



İNTERNET OKURYAZARLIĞI EL KİTABI

”Kullanıcıları çevrimiçi
dünyada destekler...



Çocuklarla ve Çocuklar İçin
Bir Avrupa İnşa Etmek

www.coe.int/children



İNTERNET EL KİTABI

Çevrimiçi
Dünyada Kullanıcıların
Desteklenmesi

Avrupa Konseyi

Bu alıřmada ifade edilen grřler
yazarların sorumluluęundadır ve ‘Avrupa
Konseyi’ resmi politikalarını yansıtmak
zorunluluęunda deęildir.

Tm hakları saklıdır.

No part of this publication may be translated,
reproduced or transmitted, in any form or by
any means, electronic
(CD-Rom, Internet, etc.) or mechanical, including
photocopying, recording or any information
storage or retrieval system, without prior
permission in writing from the Directorate of
Communication (F-67075 Strasbourg Cedex or
publishing@coe.int).

Cover, layout and graphic design: Iddifix

Council of Europe Publishing
F-67075 Strasbourg Cedex
<http://book.coe.int>

Yazarlar: Janice Richardson, Elizabeth Milovidov and
Martin Schmalzried

© Council of Europe, October 2017
Printed at the Council of Europe

İçindekiler

ÖNSÖZ	7
GİRİŞ	9
1. İNTERNET – HER ZAMAN, HER YERDE	
Kılavuz 1 - Bağlanma	13
Kılavuz 2 - Çevrimiçi varlık ve bulut	19
Kılavuz 3 - Web 2.0, Web 3.0 ve daha fazlası	25
Kılavuz 4 - Bloglar ve vlog'lar	31
Kılavuz 5 - Hareket halindeyken internet	37
2. İNTERNET – İNTERNET FİKİRLERLE İNSANLARI BİRBİRLERİNE BAĞLAR	
Kılavuz 6 - E-posta ve iletişim	45
Kılavuz 7 - Sohbet ve mesajlaşma ortamı	49
Kılavuz 8 - Sosyal paylaşım ağı ve sosyal paylaşım	55
Kılavuz 9 - Gizlilik ve gizlilik ayarları	61
3. İNTERNET – BİLGİ TOPLUMUNA KATILIM	
Kılavuz 10 - Bilgi aramak	71
Kılavuz 11 - Web’de kaliteli bilgi bulma	77
Kılavuz 12 - Uzaktan eğitim ve MOOC	81
Kılavuz 13 - Çevrimiçi alış-veriş	87
4. İNTERNET – HERKES İÇİN İNTERNET	
Kılavuz 14 - İnternetteki videolar, müzikler ve resimler	93
Kılavuz 15 - Marifetler	99
Kılavuz 16 - Oyunlar	103
Kılavuz 17 - Dijital Vatandaşlık	107
Kılavuz 18 - Dijital ebeveynlik: koruyucu ve etkin	115
5. İNTERNET – PROBLEMLİ İÇERİKLER	
Kılavuz 19 - Siber Suçlar: İstek dışı e-posta, casus yazılım, dolandırıcılık ve güvenlik	123
Kılavuz 20 - Etiketleme ve filtreleme	129
Kılavuz 21 - Çevrimiçi Taciz: Zorbalık, Takip ve Kandırma	135
Kılavuz 22 - Yardım alma	141
6. İNTERNET – İNTERNETİN GELECEĞİ	
Kılavuz 23 - Nesnelerin İnterneti	147
Kılavuz 24 - Yapay zeka, otomasyon ve yıkıcı teknolojiler	151
Kılavuz 25 - Sanal ve artırılmış gerçeklik	157
Kılavuz 26 - Ürün siz misiniz? Büyük veri, veri madenciliği ve mahremiyet	163

Yazarları Tanıyalım

Janice Richardson geçen birkaç on yıl içinde çocuk hakları konusunda danışman olarak hizmet vermiş ve bu el kitabının editörler ekibine başkanlık etmiştir. 2014 yılına kadar Avrupa Komisyonunun 30 ülkesini kapsayan Güvenli şebekenin Koordinatörlüğünü, son zamanlara kadar da ENABLE zorbalığa karşı koyma ekibi koordinatörlüğünü yürütmüştür. Janice aynı zamanda Facebook'un Güvenlik Danışma Kurulunda da yer almaktadır.

Dr. Elizabeth Milovidov, J.D. Avukat olarak 20 yıllık deneyimiyle e-Güvenlik (e-Safety) danışmanı, hukuk profesörü ve çocuk hakları savunucusudur. Görevi ebeveynleri ve çocukları internet, teknoloji ve sosyal medya konularında aydınlatmaktır. DigitalParentingCoach.com'un kurucusudur.

Martin Schmalzried COFACE'nin (Avrupa Birliği Aile Örgütleri Konfederasyonu) Kıdemli politika geliştirme memurudur. Güvenli internet ve yeni teknolojiler konusunda uzmandır. SIP BENCH III Projesinin (Ebeveyn kontrol gereçleri gözden geçirimi projesi) Başkanıdır. Bu alanla bağlantılı olarak sayısız AB projesinde ve girişiminde görev almıştır.

■ İnternet okuryazarı olmak ne kadar önemlidir? Buna kısa cevap oldukça açıktır: Çok önemlidir. İnternet kullanıcı sayısı 3,5 Milyara hızla yaklaşmaktadır ve bunun yaklaşık %20'si Avrupa bölgesindedir. İnternet, deneyim elde etmek ve paylaşmak amacıyla bilgi akışı sunarken, karmaşık çevrimiçi dünyada güvenli şekilde gezinmek istenilen bir görev olabilir. Bunun için temel bir bilgi seti gerekmektedir.

■ Bu el kitabı düz ve anlaşılması kolay dil kullanan bilgi setini önermektedir. Bu yeni basılmış bir el kitabı değil, günümüzde devamlı büyüyen bilgi akışını nasıl ciddi şekilde ele almak gerektiğine dair sürekli evrilen kullanışlı ipuçlarından oluşan bir settir. El kitabının içerikleri çevrimiçinde açıklıkla eşit biçimde yer almaktadır, başarı grafikleri de bunu göstermektedir. Öyle ki incelediğimizde söz konusu bölümler sınıflardaki veya topluluk merkezlerindeki gruplara sunulabilmektedir. Bu şekilde eğitim amaçları açısından el kitabı bir gereç olarak her yaş grubu için kullanılabilir.

■ Sonsuz sayıdaki karmaşıklıkların çözülmesinde el kitabı, bilgi paylaşımına ilişkin etik değerlendirmeler ve risklere yönelik bakış açıları önermektedir: Bilgiye dönük açılımımızı gidermek için interneti kullanmayı ve bu yolla düşüncelerimizi ve görüşlerimizi paylaşmayı arzu edersek, bunu sorumlulukla yapmalıyız. İnsan hakları ilkeleri, sayısal dünyada olduğu kadar çevrimdışında da uygulanabilir. Örneğin insan hakları başkalarının çevrimiçinde ifade özgürlüğüne ilişkin olduğu kadar bizim haklarımıza da başkaları tarafından saygı duyulmasıyla da ilişkilidir. Kişisel verimizin güvende olduğundan nasıl emin oluruz? Yasadışı içerikle karşı karşıya geldiğimizde ya da haksız yere zorbalık gördüğümüzde veya nefret söylemi aldığımızda ne yaparız? Bu konular ve daha niceleri, okuyucuların çevrimiçinde gördükleri ve okudukları hakkında eleştirel düşünmeye, bilgi edinmiş şekilde ve güvenli tercihler yapmaya davet ederek kamuoyu için kolay tavsiye ve ipuçları sağlar şekilde sunulmaktadır.

■ Fikirleri paylaşmak için çevrimiçindeyse aynı zamanda bilgi ve anlayış tesis etmek için de çevrimiçindeyiz demektir. Geleneksel sağduyuya meydan okuyabiliriz ve olumlu değişim için aklar yaratabiliriz. Bu, özellikle internetin genç kuşakların kişisel gelişmesine doğrudan katkı sağlayan araştırma, öğrenme, sosyalleşme ve yaratma gibi sonsuz fırsatlar sunmasından bellidir. İnternet genç kuşakların yaşça büyürken ifade ve haber alma özgürlüğünün temel kaynağı haline gelmiştir ve çevrimiçinde kendi hak ve özgürlüklerini kullanma yollarını sunar. İnternet potansiyel olarak bazı beklenmedik tehlikeler barındırır da bunun için uyarıcı önlemler alınabilir ve duyarlı yardım sağlanabilir. Kullanıcıları (özellikle gençleri) caydırmak maksadıyla internet, tehlike ve dikkat işareti tabelalarıyla donatılarak karanlık bir yermiş gibi sunulmamalıdır. İnternetin bilgi edinilebilir, yaratıcı, güvenli ve korkusuz şekilde kullanılmasına destek sağlama amacı güden bu el kitabı, eşsiz ve değerli bir araçtır. Eğer, el kitabı yoluyla, çocuklar internetin sunduğu çok sayıdaki imkânları kucaklayabilir, aynı zamanda kendi yetenekleri ve sorumluluklarının bilincinde olarak sayısal esneklik oluşturabilirlerse, bu el kitabı amacına hizmet etmiş olacaktır.

■ Avrupa Konseyi, El kitabının yenilenmesi sürecini izlemekten dolayı övünç duymakta, ilk yayımından sonraki yıllarda bu yenilikleri takip etmekten ve müteakiben gözden geçirme ve baskısını çoğaltmaktan memnuniyet duymaktadır. Bu kitapçık, internetten azami şekilde faydalanmak ve gelecek kuşakların interneti güven içinde ve itimatla kullanabilmelerini teminen hali hazırdaki 47 üye devletin çocukları, ebeveynleri, öğretmenleri ve siyasa oluşturucuları açısından çok zengin bir kaynak sağlamaktadır.



Snežana Samardžić-Marković
Demokrasi Genel Müdürü



Christos Giakoumopoulos
İnsan Hakları ve Hukukun Üstünlüğü Genel Müdürü

Giriş

” Okuryazarlık ümitsizlikten ümide bir köprüdür. Fakirliğe karşı bir sur, gelişme için bir yapıtaşı, demokratikleşme için bir platform ve kültürel ve ulusal kimliğin gelişmesi için bir araçtır. Sonuç itibarıyla okuryazarlık, insan gelişimi için bir yol ve her erkeğin, kadının ve çocuğun potansiyelini en üst seviyeye çıkarabileceği imkânlardır.

Kofi Annan, eski BM Genel Sekreteri, Ocak 1997-Aralık 2006

Bu *İnternet Okuryazarlığı El Kitabı*'nın ikinci baskısı olup, ilk basımı 2003 yılında olmuştur. İlk baskının gözden geçirilmesi üçer yıllık aralarla 2006 ve 2009 yıllarında, çevrimiçi teknolojisi sektöründeki zorlayıcı evrilme adımına yetişme çabasıyla gerçekleştirilmiştir. Bu baskı aynı yapıda olsa da içeriği tamamen güncellenmiş ve teknolojinin geleceğine yönelik özel bir bakışla yeni kılavuzlar eklenmiştir.

■ Bu El kitabı; aileler, eğitimciler ve siyasa oluşturucular dâhil geniş çapta kamuya yönelik hazırlanmış olup, ancak konuları ayrıntılı incelemeyi arzu edenler için derin bilgi ve kaynaklara bağlantılar da sağlamaktadır. Aynı zamanda, teknolojiyi en hırslı kullananlar arasında görünen onlu ve yirmili yaşlardaki gençler, yeni akımlara biçim verenler ve oluşturanlar için öğretici olmayı amaçlamaktadır.

■ Her şeyin ötesinde, *İnternet Okuryazarlığı El Kitabı*, dünyanın birçok yerindeki insanların çoğunun yaşamında aslında böylesine büyük bir rol almış olan sayısal ve medya ile ilgili faaliyetlere bağlı daha karmaşık ahlaki, sosyolojik ve kültürel konuların bazılarını ilişkin bilgi sağlamayı ve derin düşünmeyi geliştirmeyi amaçlamaktadır. Bu el kitabını yayımlayan Avrupa Konseyi, 1949 yılından beri 47 üye devlette insan haklarını, demokrasiyi ve hukukun üstünlüğünü ilerletmek, korumak ve geliştirmek için çaba sarf etmektedir.

■ Geçen yarım yüzyıldan fazla süre içinde teknoloji, artan biçimde çoğu insanın yaşamının birçok noktasına erişirken, insan haklarını, sorumluluklarını ve özgürlüklerini de etkilemiş ve aynı zamanda da dikkate değer biçimde bunların özünde yatan okuryazarlık kavramını genişletmiştir. *İnternet Okuryazarlığı El Kitabı*, Avrupa Konseyinin birçok zorluğun üstesinden gelmeyi ve internetin doğuşunda ortaya çıkan birçok fırsattan yararlanmayı amaçlayan geniş paletli gereçlerinden birisidir. Bu gereçlerin bazılarını El kitabında atıfta bulunulmuştur.

■ Okuryazarlık, İngilizce'de 3R olarak bilinen okuma (reading), yazma (w-ritting) ve aritmatik (a-ritmetic) ifade etme ve anlama yolu olarak çağdaş iletişim gereçleri üzerinde beceri ve hâkimiyet kazanmayı kastetmektedir. Ancak kendimizi ifade etmek için sayısal gereçleri ve platformları kullandığımız zaman, bunların ileri dağıtım gücü, hızı ve anlık süresi okuryazarlığı çoğumuzun cebelleşip durduğu çok katmanlı bir kavrama dönüştürmektedir. Resimler, videolar, sınırlı karakter mesajları, emoticon'lar (ifadeler) ve pot yayınları; Instagram, Snapchat, Vine ve Periscope gibi gereçler yoluyla hakkı kendisinde olan diller haline gelmişlerdir. Bu durum özellikle, yetişkinlerin hala “gerçek dünya” diyerek atıfta bulunduğu, üstü örülmüş ve bulanıklaşmış çevrimiçi dünyada gece-gündüz metin yazan, tweet atan, elektronik oyunlar oynayan ve görüntü değişiminde bulunan genç insanlar için geçerlidir.

■ Sosyal medya kullanıcılarının belki de dünyanın bir başka tarafında olup da asla tanışamayacağı kişileri “arkadaş” veya “arkadaş değil” şeklinde ayırırken sosyal ve kültürel gelenekler alt üst olmaktadır. İş ortakları internet aracılığıyla tanışmakta ve şirketler oluşturmaktayken ve internet artan biçimde insanların hayat arkadaşlarıyla ilk kez karşılaştıkları yer olmaya başlamaktayken ilişkiler artan biçimde çevrimiçinde kurulmaktadır.

Eğer önümüzdeki tehlikelerden kaçınmak ve günümüzün toplumuna olumlu katkıda bulunmak gibi bir zorunluluğumuz varsa kendi temel insan haklarımıza ve başkalarının haklarına olan saygıya yönelik katı bir anlayış edinmeyi zorunlu kılan bu derin değişimler, okuryazarlık temel becerilerinin tam merkezine sorumluluğu ve hesap verebilirliği yerleştirmiştir.

■ *İnternet Okuryazarlığı El Kitabı*, ilk baskıya benzer bir formatta kılavuzların bir derlemesi olarak sunulmaktadır. Ancak, kılavuzlar, kullanıcıların arzu ettiği şekilde daha kolayca dosya indirme, bölüm veya tek sayfa olarak baskı alabilmelerini mümkün kılacak şekilde 6 konulu kısım olarak düzenlenmiştir. Her kısımda bir kontrol listesi sunulmakta ve içeriğe genel bir bakış sağlanmaktadır. Basit bir dizin koymak yerine bunu koymak, içeriği daha anlaşılır kılmakta ve kapsanan en ana noktalara hızlı bir rehberlik sunarak kılavuzlar hakkında bilgi edinilmesini kolaylaştırmaktadır. Kısımlar topluca, internetin nasıl çalıştığı ve verinin nereye depolandığı hakkındaki temel bilgiden tutun, kaliteli bilgiyi bulmaya ve insanlara ve bilgiye bağlanmaya, çevrimiçi teknolojinin yakında bizi nereye götüreceği konusunda yardım almaya ve geleceğe bakmaya kadar internetin ana yönlerini açıklamayı amaçlamaktadır. Kısımlar, internetin sunduğu imkânlar ağı yoluyla kullanıcılara yardımcı olmayı ve bu süreçte, kullanıcılara internetin biçim vermesinden ziyade kullanıcıların çevrimiçi dünyanın biçimlenmesine katkı sağlayabildiği yolları kazandırmayı amaçlayan birer gereç kiti oluşturmaktadırlar.

■ Sunuldukları elektronik ortama hizmet sağlamada kılavuzlar, makul oranda kısa, okunması kolay ve fikirleri, ikazları, yararlı ipuçları ve bağlantıları hızlı biçimde aramaya yardımcı olma amacı taşımaktadırlar. Her kılavuz, o gerecin, platformun veya hizmetin eğitim açısından nasıl katma değer ve fırsatlar sağlamak amacıyla kullanılabilirliğini biraz daha bütünlüklü ve doğru şekilde araştırmadan önce söz konusu konuya ilişkin en güncel bakış açısı sunarak başlamaktadır. Kullanıcının dikkati daha ileri boyutta üzerinde düşünmeye değer olan bazı etik yönlere çekilmekte, ancak yukarıda da not edildiği üzere, teknoloji sürekli olarak gelişmekte ve bu sebeple de her zaman yeni etik düşünceler ortaya çıkmaktadır. Çoğu kılavuzlardaki “nasıl” kısmı, birçok şeyin aslında nasıl çalıştığı veya çalıştırılabildiğine dair adım adım bilgi sağlamak amacı taşıyan pratik bir rehberdir. Öyle ki kullanıcıların teknolojinin nimetlerinin çoğundan istifade etmeleri mümkün olabilmektedir.

■ Her kılavuz içindeki son kısımlar, bağlantılardan makalelere ve dizinlere, o özel gereç veya hizmetin uygulamalarına kadar her şeyi sınıfta kullanmak amacıyla fikirler, iyi uygulama örnekleri ve ayrıntılı bilgi sunmaktadır. Bu sayfalar, özellikle El kitabı kullanıcıları için sosyal, eğitsel, kültürel ve küçüklerin korunması alanlarında dünya çapında çalışma yürüten kurumlardan, örgütlerden ve bireylerden toplanan “en iyi ürünlerden” oluşan bir depo olarak görülebilir. Aksi belirtilmedikçe El kitabında sunulan her şey, günümüze kadar verilen tüm tavsiyeler, tüm yaş gruplarının kullanımının güncel, ilgili ve güvenilir olmasını sağlamak için yapılmıştır. Kullanıcılar, yine de günümüzün hızla gelişen dünyasında binlerce URL’nin [Uniform Resource Locators (Özgün Kaynak Adresi) başka deyişle “bağlantı” veya “web-bağlantısı]] her gün oluşturulduğunun ve silindiğinin kesinlikle farkındadırlar. Çevrimiçi teknolojiye ilişkin hiçbir elkitabı, bu sebepten dolayı tüm bilginin geçerli kalacağı, içerdiği tüm URL’erin var olmaya devam edeceği güvencesini veremez.

■ *İnternet Okuryazarlığı El kitabı* daha çok bir fotoğraf çekimi veya belirli bir zaman noktasında kesit görüntü “alımı” olarak görülmelidir. Eğer bu elkitabı hedef kesimler için tam anlamıyla sürekli ilgili kalması gerekiyorsa, muhakkak yeni bilgilerin, fikirlerin ve rehberliklerin üstüne eklenmesi gerekecektir. Okuyucular fikirlerini, kaynaklarını ve iyi uygulama örneklerini Avrupa Konseyi’nin Çocuklar Bölümüne (Children’s Division of the Council of Europe, children@coe.int.) göndererek bu evrimsel sürece katkıda bulunmaya davet edilmektedirler.

1. İnternet: Her Zaman, Her Yerde

“Günümüzde hepimiz tıpkı dev bir beynin nöronları gibi İnternet ile bağlanıyoruz.”

Stephen Hawking, teorik fizikçi

KILAVUZ 1 – BAĞLANMAK

İnternet bağlantınızı, bir virüs koruyucu yükleyerek ve bir koruma duvarı ile ve Wi-Fi yönlendiriciniz için bir şifre oluşturarak güvenli hale getirdiğinizden emin misiniz?

İnternete sizin aığınız ve cihazlarınızı kullanan/cihazlarınız üzerinden erişen kişiler için uygun kullanım koşulları (bazen sorumlu kullanım şartları olarak adlandırılır) oluşturduğunuz mu?

Çocuklarınız tarafından kullanılan cihazlara “misafir” hesaplar oluşturduğunuz mu?

KILAVUZ 2 – ÇEVİRİMİÇİNDE OLMAK VE BULUT

Web sitenize ya da web günlüğünüze iletişim bilgilerinizi koydunuz mu?

Çevrimiçi gizliliğinizi korumak için adımlar attınız mı?

Web sitenizde/web günlüğünüzde kullandığınız içeriğin telif hakları mevzuatına uygun olduğunu gözden geçirdiniz mi?

KILAVUZ 3 – WEB 2.0, WEB 3.0 VE DAHASI

Çevrimiçinde gönderdiğiniz resim ve videolarda yer alan kişilerden düzenli olarak izin alın.

Seyahat ve ürün sitelerindeki kullanıcı tavsiyeleri faydalı olabilir, ancak bunların gerçek olduğuna emin misiniz?

Kullanıcılar tarafından oluşturulan içerik yaratıcılık ve ifade özgürlüğünü destekler, fakat İnternet daha iyi bir ortam olursa size sorumluluk da verir.

KILAVUZ 4 – GÜNLÜKLER (Blogs) VE VİDEO GÜNLÜKLER (Vlogs)

Gizliliğinizi rumuz kullanarak koruyun ve belirli kişisel bilgilerinizi saklayın.

Günlük ve video günlüklerinizi uygun güvenlik önlemleri oluşturarak, bilgisayar korsanlarına karşı koruyun ve içeriğinizi düzenli olarak kaydedin.

Gönderdiğiniz günlüğün amacını ve hedef kitlesini anlayın.

KILAVUZ 5 – İNTERNET İŞ BAŞINDA

Çocuklar kaç yaşında güvenli olarak taşınabilir cihazları kullanmaya başlayabilirler ve çok küçük çocuklar için en uygunu hangi cihazlardır?

Taşınabilir cihazlarınızın rahat ve güvenli kullanımı için coğrafi konum ve Bluetooth özelliğini yeteri düzeyde kavradınız mı?

T-eğitim (taşınabilir cihaz üzerinden eğitim) ve taşınabilir e-cüzdanlar, öğrenme, çalışma ve alışveriş yapma yöntemlerimizi değiştiren taşınabilir cihazların kullanıldığı alanlardır. Bu güncel evrim hakkında ne biliyorsunuz?

Bağlanmak



İnternet, bağlantı düğümleri işlevi gören sağlayıcılar aracılığıyla dünya çapındaki bilgisayarları birbirine bağlayan bir ağıdır¹. 2016 yılının Haziran ayı itibarıyla, 614 milyonu Avrupa'da olmak üzere, dünyada 3,5 milyar İnternet kullanıcısı olduğu tahmin edilmektedir².

- İnternet nasıl çalışır ve süreci bilmek neden önemlidir? Büyük bir olasılıkla günlük olarak İnterneti zaten kullanmaktasınız. Hatta otomobilinizi ya da bisikletinizi kullandığınızdan da daha sık bir şekilde kullanmaktasınız. İnternetin nasıl çalıştığına ilişkin olarak tüm teknik ayrıntıları bilmek durumunda olmasanız da, tıpkı bisikletinizin tekerini değiştirmek ya da otomobilinizin yağ seviyesini kontrol etmekte sahip olduğunuz bilgi gibi, en azından nasıl çalıştığına ilişkin temel kavramlara hâkim olmalısınız.
- Evde, büyük olasılıkla İnternete bir yönlendirici vasıtasıyla bağlanmaktasınız ki, bu gizemli kutu hem telefon hattınıza, hem de kablolu televizyonunuza bağlanmaktadır. Tüm cihazlarınız, akıllı telefonunuz veya bilgisayarınız bu yönlendiriciye ya bir Ethernet kabloyla ya da bir Wi-fi üzerinden bağlanır.

1. http://en.wikipedia.org/wiki/Node_%28networking%29
2. www.Internetworldstats.com/stats.htm

Şimdi, yönlendiricinizin komşunuzun yönlendiricisine bağlandığını ve komşunuzun yönlendiricisinin de onun kapı komşunun yönlendiricisine bağlandığını gözünüzde canlandırın. İşte tam olarak da bu, küçük ölçekteki bir İnternet ağıdır. İnternet basitçe devasa sayıdaki yönlendiricilerin birbirine bağlı olduğu ve bir noktadan (örneğin evinizdeki bilgisayardan) bir başka noktaya (dünyanın öbür ucunda tatilde olan bir arkadaşınızın akıllı telefonuna) bilgi (e-postalar, resimler, videolar gibi veriler) göndermenizi ve almanızı sağladığı bir ortamdır.

■ Tüm anakaralara okyanus altından ulaşan ve karadaki altyapıyı birbirine bağlayan bir kablo kara bağlantı noktasına doğrudan erişen (genellikle telefon hatları) devasa sualtı kablolarının varlığı insanı hayrete düşürebilir.

Şöyle bir kafanızda canlandırın. Bilgisayarınızdan bir arkadaşınıza resim gönderdiğinizde olan şudur: resminiz, postanedeki etiketlenmiş bir zarf gibi (gideceği yer, kaynağı ve bu veri parçalarının resminizin yeniden bir araya getirilmesi için ne şekilde tekrar birleştirileceği) paket olarak adlandırılan küçük veri parçalarına ayrılır. Cadde ismi ve ev numarası gibi bilgilerin yerine veri paketleri nereden gönderildiklerine ilişkin IP adreslerini³ ve nereye gideceğine ilişkin IP adreslerini içerir. Böylece bu parçalar telefon hattınız yoluyla İnternet omurgasına (daha önce bahsettiğimiz birbirine bağlı büyük sayıdaki yönlendiriciler) bağlı İnternet hizmet sağlayıcınızın hizmet araçlarına gider. Fakat aslında sizin resminizin varış yeri neresidir? Örneğin resminizi e-posta ile gönderirseniz, varış yeri arkadaşınızın bilgisayarı değil, arkadaşınızın kullandığı e-posta müşteri veri merkezidir.

■ Veri merkezleri, yönlendiriciler ve sabit sürücülerle dolu devasa ambarlardır. Gönderdiğiniz resminiz çoklu sabit sürücüler üzerinde (sabit disk bozulmalarına durumunda veriyi korumak için) depolanırlar. Örneğin arkadaşınız Gmail kullanıyorsa, bu durumda arkadaşınıza gönderdiğiniz resim Amerika Birleşik Devletleri, İrlanda, Belçika, Hollanda ve birçok ülkedeki⁴ Google merkezlerinden birinde fiziksel olarak depolanabilir. Böylece arkadaşınız resme bakmak istediğinde, kendi bilgisayarından yeniden İnternet omurgası üzerinden bu veri merkezine doğru bütün yollardan geçecek bir istek gönderir, bunun üzerine sizin resminizle beraber veriyi bu merkez arkadaşınızın bilgisayar ekranına yollar.

İNTERNET YÖNETİŞİMİ

□ Acaba İnternet ilk kullanıldığı yerde nasıl kurulmuştur? Mevcut altyapıların devam ettirilmesinden ve yenilerinin oluşturulmasından kim sorumludur? IP adresleri gibi standartlar hakkında kim karar verir?

□ Hiper bağlar ve birbiriyle bağlantılı web sayfaları fikri İsviçre’de CERN’de çalışırken Tim Berners-Lee ve Robert Cailliau tarafından bulunmuşken, ARPANET olarak adlandırılan ilk birbiriyle bağlantılı ağ, ABD üniversiteleri⁵ arasında kurulmuştur .

□ Bu sebeple, bir kişinin ağa bağlanmasına olanak sağlamada gerekli olan özgün “adresler” için tahsis yapmaktan sorumlu ilk kuruluş ABD’de oluşturulmuştur (IANA - Internet Assigned Numbers Authority - İnternet Tanımlanmış Adresler Otoritesi).

□ İnternet büyüdükçe, onun gelişimi, bakımı, istikrarı ve güvenliğinin daha iyi koordine edilmesi ihtiyacı artmıştır. ABD Ticaret Bakanlığının IANA’yı reforma zorlaması sonucunda IANA, 1998 yılında ICANN halini almıştır (the Internet Corporation for Assigned Names and Numbers - Tahsis Edilmiş İsim ve Numaralar İçin İnternet Kurumu). ICANN⁶, “hayırsever ve kamusal amaçlar için” kar amacı gütmeyen bir kurum şeklinde, güçlü bir “aşağıdan yukarı” yaklaşımıyla, özel sektör paydaşları, sivil toplum ve hükümetlerin de dâhil olduğu küresel çaptaki binlerce paydaşının işbirliğini içermek suretiyle resmi olarak kurulmuştur. Ancak, ICANN’ın ABD Hükümetiyle bağları ve ABD çıkarlarını öncelikle temsil etme riski nedeniyle çok fazla eleştiriye maruz kalmış ve dünyanın çeşitli bölgelerinden ülkelerin reform çağrılarına muhatap olmuştur.

□ Bunun üzerine ICANN, 111 ülke ve temel telekomünikasyon kurumları ve Avrupa Konseyi gibi bir dizi gözlemciyi içeren geniş çaplı paydaşlara açılmıştır. Ancak ICANN, paydaşlarına demokratik girdi sağlamadığı ve geniş çaplı istişare yapmadığı için eleştirilmeye devam etmiş ki bu durum 2006 yılında Birleşmiş Milletler tarafından İnternet Yönetişim Forumu’nun (IGF) oluşturulması sonucunu doğurmuştur.

□ IGF yılda bir kez toplanmakta ve gençleri de kapsayan geniş çaplı paydaşlara İnternetin geleceği üzerine görüşlerini paylaşmak için fırsat sunmaktadır.

3. https://en.wikipedia.org/wiki/IP_address

4. <http://www.google.com/about/datacenters/inside/locations/index.html>

5. https://en.wikipedia.org/wiki/World_Wide_Web

6. <https://www.icann.org/>



EĞİTİM AÇISINDAN GETİRİLERİ

- İnternet çok sayıda yeni fikirlere, kaynaklara, öğrenme fırsatlarına, bilgi ve hizmetlere erişim sağlar.
- İnternet, uluslararası sınırlar aşan kullanıcılar arasında değişik yollarla tecrübe değişimi ve iletişimi kolaylaştırır: forumlar, e-posta, sosyal ağlar, sohbet, video konferanslar ve benzeri. Böylece öğrencilere pahalı seyahate ihtiyaç duymadan diğer öğrencilerle proje ve çalışma içinde olma fırsatı sunar.
- İnternet, geleneksel kütüphaneye düzenli gitmeyen kişilere bile arama araçlarını erişilebilir kılar.
- İlave cihaz ve yazılım ile İnternet özel ihtiyaçları olanlara yeni fırsatlar açabilir.
- İnternetin nasıl yönetildiğini öğrenmek tüm vatandaşların geleceği şekillendirecek temel kararlara dâhil olmalarını sağlar.



ETİK HUSUSLAR VE RİSKLER

- İnternetin çoğu kez yanlış anonimlik duygusu sağladığının farkında olun. İnternetin nasıl işlediğine bakarsak, ne zaman internete girerseniz arkanızda daima iz bırakırsınız (IP adresiniz).
- Çevrimdışı dünyada olduğu gibi, burada da dolandırıcılık, yanlış bilgiler ve çocuklar için uygunsuz malzemeler vardır.
- İnternet bir yandan bir dizi yeni olanak sunarken, teknik çözümler her zaman geleneksel olandan daha iyi olmamaktadır. Örneğin, e-posta iletişimde devrim yaratmıştır ve her ne kadar bir video konferans size “oradaymış gibi” hissini verebilse de asla yüz yüze iletişimin yerini alamayacaktır.
- İnternet deneyiminiz üzerinde İnternet yönetimi, anonimlik veya ağ tarafsızlığı gibi muğlak ilkeleriyle büyük bir etki yaratabilmektedir. Özgür ve açık internet ilkesi ile bunu kontrol etmek arzusunda olan arasında sürekli bir mücadele vardır. Bazı şirketler, kendi web sayfaları, uygulamaları ve hizmetlerine has “ücretsiz” mobil internet planları sunarak ve diğerlerinin⁷ ziyaretini ücretlendirerek trafiği kendi web sayfalarına, uygulamalarına ve hizmetlerine yönlendirmeye çalışırlar. Örneğin Facebook, dünyanın çeşitli yerlerinden, özellikle de gelişmekte olan ülkelerden⁸ internet hizmetleri vasıtasıyla bağlanan tüm kullanıcılar için varsayılan ana sayfa olarak “Internet.org” portalını oluşturmuştur.

NASIL?



- Günümüzde satın aldığınız neredeyse tüm cihazlar, hem Wi-Fi yoluyla, hem seyyar internet erişimi yoluyla (örneğin, akıllı telefonlar ve tabletler Wi-Fi veya seyyar internet yoluyla bağlanabilirler) hem de Ethernet kablosu yoluyla (birçok bilgisayara Ethernet giriş yerleştirilmiştir) internete bağlanabilme kapasitesine sahiptir.

7. <https://en.wikipedia.org/wiki/Zero-rating>

8. <https://en.wikipedia.org/wiki/Internet.org>

- İnternete bağlanmak için iki temel seçeneğiniz vardır:

► Genellikle, bir telefon ya da kablo şirketi olan İHS (internet hizmet sağlayıcı) ile temasa geçin. Bu şirketler size telefon hattınız üzerinden ya da kablolu televizyonunuz üzerinden bir kullanıcı adı ve parola ve bazen bir modem/yönlendirici ile internete bağlantı sağlarlar.

► Cep telefonu operatörünüzden internet paketi tarifi alın. İnternette indirebileceğiniz/gönderebileceğiniz verilerin ölçüsüne dair sınırlamaların halen oldukça yüksek düzeyde olduğunu unutmayın. Ancak birçok operatör 4G ya da 5G telekomünikasyon standartlarına (hızda çok fazla artış sağlayan) geçtiğinden giderek azalmaktadır.

• Ayrıca internete ücretsiz bağlanmak için kullanabileceğiniz sayıları giderek daha da fazlaşan “açık” Wi-Fi bağlantı noktaları bulunmaktadır. Bunları, halk kütüphanesi, hatta barlar, restoranlar ve alışveriş merkezleri gibi çeşitli kamusal alanlarda bulabilirsiniz. Çoğu zaman, siz bağlanmadan önce bir ya da birden çok şu işlemleri yapmanız istenir: kullanım şartlarını kabul etmeniz, e-posta adresinizi kullanarak bir hesap oluşturma (e-postanızın bu durumda size reklam gönderilmede kullanılacağına dair dikkatli olun, bu durumlar için özel bir e-posta adresi oluşturun) veya internete bağlanmak için bir şifre girmeniz. Örneğin, barlarda, restoranlarda ve otellerde “açık” internet, genellikle sadece müşterileri için erişilebilir durumdadır. Dolayısıyla, çalışanlardan şifre istemeniz gereklidir. Hassas verilerinizi asla paylaşmayın ya da elektronik bankacılık gibi hassas işlerinizi asla kamu Wi-Fi bağlantı noktaları üzerinden yapmayınız.

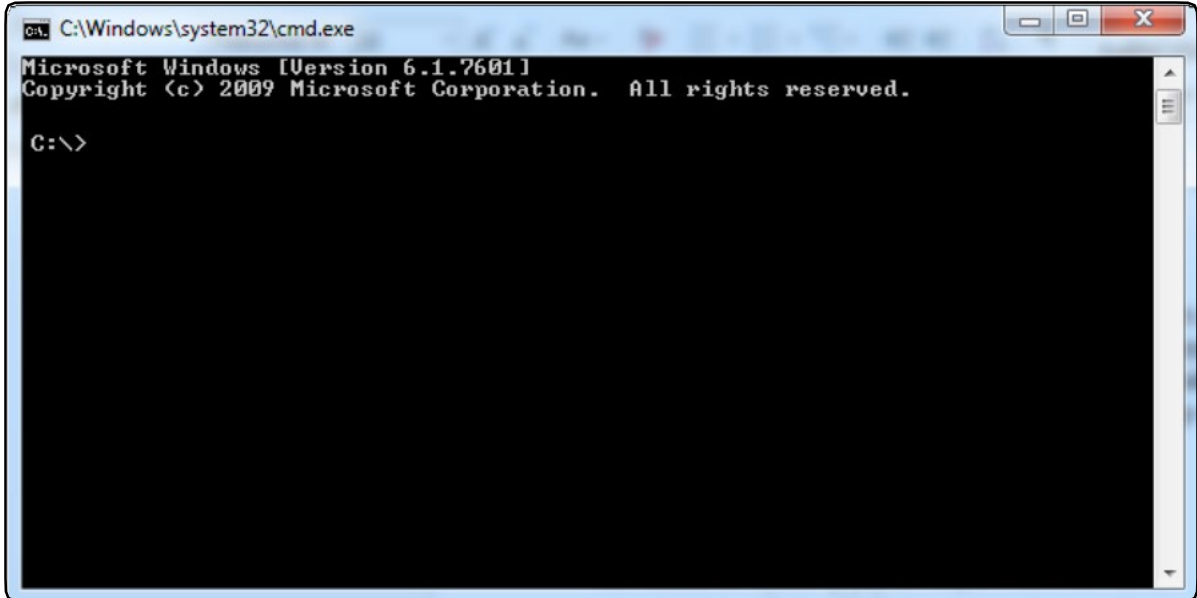
• Birçok İHS bağlantı sağlanması amacıyla sadece telefon/kablo hattınıza bağlanmanız için size önceden yapılandırılmış yönlendiriciler sağlarlar. Bazen, bir yönlendirici satın almanız gerekir ve bu yönlendiriciyi kendiniz yapılandırmanız. Sahip olduğunuz ya da almaya niyetlendiğiniz yönlendiricinin internet aboneliğinize uygun olduğunu size hizmet veren İHS ile kontrol ettiğinizden emin olun!

SINIF ÇALIŞMALARI İÇİN FİKİRLER



Windows 7 ve üzeri sürümlerde

1. Windows programında “Başlat” tuşuna basın.
2. “arama” barında “cmd” yazın ve başlatma menüsünde görünen program ikonuna basın.



3. “tracert wikipedia.org” yazın ve “enter” tuşuna basın.
4. Böylece bilgisayarınız ile erişmeye çalıştığınız web sitesi arasında bulunan “hops”u ve her “hop”un kaç kez olduğunu görebileceksiniz. Bu örnekte, Wikipedia’ya erişmek için önce yönlendiricimiz vasıtasıyla “yerel” İHS’ye gideceğimizi görürüz (bu durumda Belçika’dan Belgacom).

Washington'daki ("was" olarak kısaltılmış) bir yönlendiriciye Atlantik üzerinden gideriz ve son olarak wikipedia'nın ev sahipliğini yaptığı yere varırız. Bunu diğer web sayfalarından denemeleri için öğrenciler teşvik edilirler. Her adımın milisaniye cinsinden ne kadar zaman aldığına dikkat edin.

```
C:\Windows\system32\cmd.exe

C:\>tracert wikipedia.org

Tracing route to wikipedia.org [208.80.154.224]
over a maximum of 30 hops:

  1  12 ms   45 ms   7 ms   192.168.1.1
  2  25 ms   28 ms  175 ms  1.192-134-109.adsl-dyn.isp.belgacom.be [109.134.192.11]
  3  *        *        *        Request timed out.
  4  193 ms  39 ms   77 ms  ae-12-1000.ibrstr3.isp.belgacom.be [91.183.246.108]
  5  30 ms   43 ms   52 ms  ae2.bru21.ip4.gtt.net [141.136.102.217]
  6  126 ms  162 ms  133 ms  xe-7-3-0.was10.ip4.gtt.net [141.136.111.10]
  7  412 ms  388 ms  277 ms  xe-5-3-1.cr2-eqiad.wikimedia.org [173.241.131.218]
  8  201 ms  277 ms  185 ms  text-lb.eqiad.wikimedia.org [208.80.154.224]

Trace complete.

C:\>
```



Mac OS X ve üzeri sürümlerde

1. Mac OS X programında ağ olanağını başlatın (bunu Spotlight'a girip, "network utility" yazarak ve en üste tıklayarak yapabilirsiniz).
2. "Traceroute (iz yolu)" yazan yere tıklayın.
3. İz yolu üzerinde çalıştırmak istediğiniz şey için alan adını girin örneğin "Wikipedia.org" ve "Trace (iz)" tuşuna tıklayın.
4. Böylece bilgisayarınız ile erişmeye çalıştığınız web sitesi arasında bulunan "hops"u ve her "hop"un kaç kez olduğunu görebileceksiniz.

Öğretmenler için tercihe bağlı malzeme

- Daha fazla bilgi için, "İnternet nasıl çalışır" adlı videoyu Sadeleştirilmiş Bilim Karalama Defteri (Naked Science Scrapbook) üzerinden izleyin⁹.
- Sınıfta çevrimiçi teknolojinin özel ihtiyaçlı bireylere nasıl yarar sağlayabileceği konusunda bir tartışma başlatın ve fikirleri tetiklemek için Avrupa Konseyi eylem planına göz atın¹⁰.



İYİ UYGULAMA

- İnternet kullanımınız için uygun bir bağlantı seçin. Yüksek çözünürlüklü video gibi çok hızlı internete ihtiyaç duyan hizmeti düzenli olarak kullanıyorsanız, hızlı bir İnternet bağlantısı aldığınıza emin olun (ADSL2+ dengi en az 20 megabit/saniye). Özellikle de, indirilen verinin boyutuna sınır koymayan bir internet bağlantısı tercih edin. Eğer sadece gazete okumak, e-posta göndermek için internete ihtiyacınız varsa, bu durumda herhangi bir basit internet aboneliği sizin için yeterli olacaktır¹¹.
- Yatacağınız zaman daima cihazlarınızı (bilgisayarlarınızı) kapatın ya da akıllı telefonunuz ve tabletinizin bağlı olduğu WiFi bağlantısını kesin. Cihazlarınızı bağlı bırakmanız verilerinizin güvenliğine ilişkin riskleri artırabilir ve aynı zamanda sağlıkla ilgili riskler de içerebilir (Bkz. Güvenlik hakkındaki Kılavuz Metin 19).

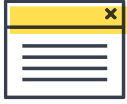
9. <https://www.youtube.com/watch?v=oj7A2YDgIWE>

10. https://www.coe.int/t/dg4/majorhazards/activites/2013/DIDRR/Action_Plan_CoE_Easy_to_Read_13nov08_EN.pdf

11. www.cnet.com/internet-speed-test

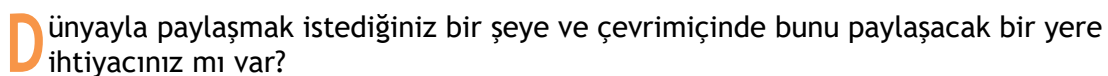
- Yönlendiricinizin kurulum sayfasına nasıl erişeceğinizi bildiğinizden emin olun. Çoğu kez, şu IP adreslerinden birini tarayıcınıza yazarsanız ona ulaşabilirsiniz: 192.168.1.0 ya da 192.168.1.1. Bu neden önemlidir? Birçok Wi-Fi kurulum sayfası çok basit kullanıcı adı ve şifreyle “tanımlanmış” kullanıcı hesaplarına sahiptir (örneğin kullanıcı adı “admin” şifre “admin”). Ayarlarınızın değiştirilmesinde kolaylıkla kullanılabilir olması ya da evinizin bilgisayar ağına kolaylıkla erişim sağlanabilecek olması sebebiyle yönlendiricinizin konfigürasyon sayfasına olan erişimi güvenli hale getirmek çok önemlidir.
- Çocuklarınız internette sörf yaparken, onların çevrimiçi deneyimleri hakkında tartışmayı teşvik etmek ve güvenlerini artırmak maksadıyla mümkün olduğunca yanında kalın; birlikte öğrenmek için fırsat yaratın.
- İnternet yönetişiyle aktif olarak ilgilenin ve anonimlik, güvenlik ya da ağ tarafsızlığı gibi temel ilkeler üzerine kamuoyu tartışmalarında sesinizi duyurun.
- Eğer sorumluluğunuz altındaki bilgisayarı veya ağı başkaları da kullanacaksa, makul bir kullanım politikası (AUP)¹² ya da sorumlu kullanım politikası (RUP) geliştirin.

DAHA FAZLA BİLGİ İÇİN



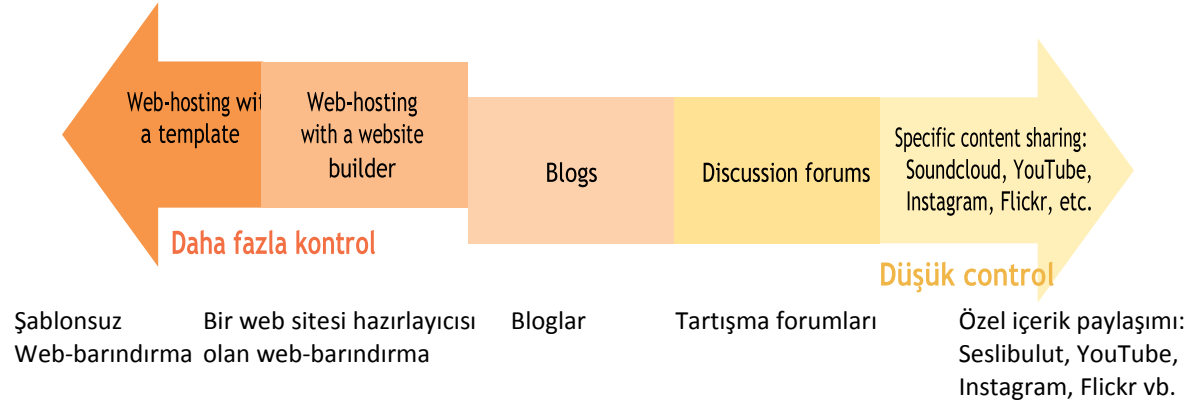
- The List adlı site, IHS’lerin dünya çapındaki rehberidir: <<http://www.thelist.com>>.
- Avrupa Okullar Ağı (European Schoolnet) <<http://www.eun.org>>, Küresel Okullar Ağı <<http://www.globalschoolnet.org/GSH/>> ve Eğitim Dünyası <<http://www.educationworld.com/>> gibi eğitim siteleri kaynak ve ortak projeler sunmaktadır.
- Bir AUP (makul kullanım politikası) yazmak için tavsiye, öğretmenler ve eğitim çalışanları için çevrimiçi bir kapı olan Eğitim Dünyası üzerinde bulunabilir: <http://www.educationworld.com/a_curr/curr093.shtml>.
- Insafe adlı ana kapı, İnternet’e nasıl güvenli bağlanılacağı ve sörf yapılacağı konularında tavsiye ve kaynak bilgiye yer vermektedir: <<https://www.betterinternetforkids.eu/>>.
- İnternet Yönetişim Forumu resmi sitesi İnternete bağlı olarak kamu politikası konularında yer alan tartışmalara fırsat sunmaktadır: <<http://www.intgovforum.org/cms/>>.
- Aşağıdaki Wikipedia sayfası ağ tarafsızlığı konusunda çeşitli bilgileri içermektedir: <https://en.wikipedia.org/wiki/Net_neutrality>.
- ICANN (İnternet Tahsisli Sayılar ve İsimler Kurumu) hakkında bilgi kurumun resmi sitesinde bulunabilir: <<https://www.icann.org/>>.

12.http://en.wikipedia.org/wiki/Acceptable_use_policy



■ Çok özel içerik mi (resimler, video, metinler vb.) paylaşmak istiyorsunuz yoksa geniş kapsamlı içerik mi paylaşmak istiyorsunuz? Yaratıcılığın bütün aşamalarında tam kontrol mü istiyorsunuz yoksa belirli bir ölçüde değişiklikler yapabileceğiniz önceden hazırlanmış şablonlar üzerinde çalışmayı mı tercih edersiniz? İçerik paylaşmadaki amacınız nedir ve buna neden ihtiyaç duyarsınız? Hedef kitleniz kimler - dünya mı, bölgeniz mi, yaşadığınız şehir mi yoksa sadece öğrenciler ve ebeveynler mi? Çevrimizde içerik paylaşmak için ödeme yapmaya ne kadar isteklisiniz?

Aşağıdaki şekil, içerik paylaşma yollarının, tam kontrol sağlanan/uyarlanandan daha az kontrol sağlanan/uyarlanana doğru giden bir devamlılık doğrultusunda hazırlanmış yüzeysel bir listesini göstermektedir.



Daha çok kontrol

Eğer hem içerik hem de tasarımla ilgili olarak tamamen serbest olmak istiyorsanız, o zaman şablonsuz web-barındırma seçmek zorundasınız. Ancak bunun bir maliyet getireceğini hatırla tutunuz zira çoğunlukla bir alan adı (örneğin <www.mywebsite.com>) satın almak zorunda kalacaksınız. Eğer nasıl kodlanacağını öğrenmek istemiyorsanız ama yine de çok çeşitli içeriği paylaşmak istiyorsanız ve tasarımda yüksek bir esnekliğe sahipseniz bir web sitesi hazırlayıcısı olan web-barındırma ya da bloğa (bazen daha kısıtlı tasarım esnekliğine sahip olan) gidebilirsiniz. Tartışma forumları zaten oldukça özelliğidir: örneğin okulunuz için tartışma forumu veya mesaj panosu oluşturabilirsiniz. Son olarak, eğer sadece resim, video ve müzik paylaşmak istiyorsanız, bu tür içeriğe yer sağlama özelliğine sahip bir hizmet için bir hesap açmayı tercih edebilirsiniz. Sonuç olarak, içeriğiniz, her ne olursa olsun, seçmiş olduğunuz yer sağlayıcının sunucusu üzerinde bir yerde bulunacaktır: söz konusu içerik “bulut” içinde yer alacaktır.

Bu hizmetlerin çoğu ücretsiz olarak verilirken, bu çoğunlukla kullanıcılarınızın az ya da çok araya giren reklamlara maruz kalabilecekleri anlamına gelir (yani, sayısız açılır pencereler, web sitesine üst üste açılan sayfaları, çok aşırı sayıda reklam bantları vb. gibi kullanıcı deneyimine büyük ölçüde engel olan reklamlar)



EĞİTİCİ DEĞERİ, NEDEN İLGİLİDİR, NEDEN ÖNEMLİDİR?

Çevrimiçinde bulunmayı ve içerik paylaşmayı geliştirmek çok büyük bir eğitici değere sahiptir ve bir dizi yeteneğin geliştirilmesine yardımcı olur.

- İçerik yönetimi/kuruluşu:** ister bir web sitesi oluşturmaya ister bir fotoğraf galerisi kurmaya karar verin, kullanıcıların aradıklarını bulmaları için içeriğinizin basit bir şekilde düzenlenmesi gereklidir.
- Tasarım:** sizin çevrimiçindeki kimliğiniz, tamamı tasarım çalışmanızın parçası olan çoğunlukla bir logoya, bir resime, tercih ettiğiniz renklere, web sayfanızın mizanpajına bağlıdır.
- Sayısal beceriler:** eğer bir web sayfası oluşturmaya seçtiyseniz, çok açık bir şekilde, çevrimiçinde ne kadar çok kalırsanız kodlama gibi belirli sayısal yetenekleriniz o kadar artar (örneğin HTML, PHP, HTML5 Javascript). Fakat diğer seçeneklerde bile, arama motorları, içeriğinizi daha görünür hale getirme ve dosya formatları konularında daha fazla bilgi sahibi olmalısınız.
- İletişim/yazma becerileri:** içeriği yorumsuz paylaşmayı planlarsanız bile kullanıcılarınızın dikkat ve ilgilerini çekmek maksadıyla iletişim/yazma yeteneklerinizi parlatmanız gerekecektir.
- Pazarlama becerileri:** çevrimiçi ortamın kalabalık olması nedeniyle fark edilemeyebilirsiniz. Ancak ün kazanmanız ve çevrimiçinde görünürlüğünüzü artırmanız, kendinizi nasıl tanıtacağınıza ve ürettiğiniz ya da paylaştığınız bir ürünü nasıl pazarlayacağınıza bağlıdır.
- Ekip çalışması:** ilave olarak, çevrimiçi ortamda eğer bir proje kapsamında arkadaşlarınız/sınıf arkadaşlarınız/öğrencilerinizle birlikteyseniz bu durumda takım çalışması yeteneğinizi de geliştirmeniz gerekecektir. Bir web sayfasını yönetmek kolay bir iş değildir ve bu iş genellikle düzenlemeyi ve birkaç kişi arasında işbölümünü gerektirir: yönetici, içerik yazarı, vb.
- İkincil getiriler:** belirli bir konuda bir web sitesi oluşturmak suretiyle, örneğin okul projeleri için matematik hakkında bir web sitesi, kaçınılmaz olarak konuyla ilgili kavrayışınız ve bilginiz de artacaktır.



ETİK HUSUSLAR VE RİSKLER

— Eğer kişisel bir içeriği paylaşmak ya da kişisel web sitesi oluşturmak isterseniz, yerleştirdiğiniz şeyler için sadece siz sorumlu olacaksınız. Siz (ve eğer küçükseniz ebeveynleriniz) birçok nedenden dolayı kendinizi sorun içinde bulabilirsiniz.



Hukuki nedenler

— “İfade özgürlüğünün” sınırları: bu hak mutlak değildir ve kullanılırken bazı sınırları vardır. İfade özgürlüğünün sınırları yasayla açıkça belirlenmelidir; demokratik bir toplumda zorunlu olmalıdır (orantılılık) ve meşru hedefleri olmalıdır (İnsan Hakları Avrupa Sözleşmesinin 10.2 Maddesi “ulusal güvenliğin, toprak bütünlüğünün veya kamu güvenliğinin korunması, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi, sağlığın veya ahlakın, başkalarının şöhret ve haklarının korunması, gizli bilgilerin yayılmasının önlenmesi veya yargı erkinin yetki ve tarafsızlığının güvence altına alınması” konularını içerir). Bu sınırlamalar bir devletten diğerine değişiklik gösterebilir ancak hatırdta tutmanız gereken bazı “genel” değerlendirmeler bulunmaktadır:

- hakaret;
- nefret söylemi²;
- başka birinin kişisel verisini paylaşma³;
- veri depolama – eğer bulut hizmetlerini seçtiyseniz, verilerinizin nerede depolanacağını önceden araştırın; verilerin kullanımı ve erişilebilirliği üzerinde kontrol sağlamak sizin hakkınız ve sorumluluğunuzdur⁴;
- terörizmin teşviki:
 - <<https://goo.gl/cv9XDR>>;
 - <<https://goo.gl/Tq3UDp>>;

fikri mülkiyet hakları: size ait olmayan bir içeriği paylaşıyor musunuz? Paylaşmanız durumunda bu içeriği paylaşma izniniz olup olmadığına emin olun. Ticari içerik telif hakları kanunu altında korunmaktadır ve bu içeriği kullanmak için telif hakkı sahibinden özel bir izin almanız gereklidir. Belirli sanatçılar ve tasarımcılar içeriği, genellikle “Creative Commons” olarak adlandırılan özel bir “lisans” altında yayımlarlar. Bu lisansa bağlı olarak, içeriği ticari amaçla kullanmanın yanı sıra yazara ödeme yapmaksızın kullanabiliyor olabilirsiniz. Telif hakkına konu olan materyale gelince, eğer bu içeriği kullanmak isterseniz, hakkı elinde bulunduran kuruluştan/bireyden (kayıt şirketi, film stüdyosu, vb.) uygun izni almanız gerekir

— Yukarıdaki eylemlerden herhangi bir sizi yasal sorunların bazı biçimlerine sürükleyebilir.



Kişisel sebepler

- Aşırı paylaşım: Paylaştığınız her türlü içeriğin bütün dünyadan herhangi biri tarafından büyük olasılıkla erişilebilir olacağını aklınızda bulundurun. Örneğin, yaz tatili fotoğraflarını yer bilgilerini de ekleyerek paylaşmanız, yabancı kişilerin sizi izlemesine ya da hırsızların sizin tam olarak ne zaman “şehir dışında” olduğunu bilmelerine fırsat sunacaktır; böylece bunlar sizin evinize gireceklerdir. Paylaştıklarınızı seçerken stratejik davranın.
- Çevrimiçi itibar: Siz bir taraftan çevrimiçinde gizli kalabileceğiniz yanılsamasına sahip olabilirken, sizin gerçek kimliğinizin bulunulmasının birçok yolu vardır. Kolluk kuvvetleri belli şartlara bağlı (çoğu durumda, bir mahkeme yetkisi) olarak internet kullanıcılarının izlerini sürmek için gerekli araçlara sahiptir. Çevrim içinde bir şeyler paylaştığınızda, bunun sizin hem çevrimiçindeki hem de gerçek hayattaki itibarınıza katkıda bulunacağının farkında olunuz.

1. <https://en.wikipedia.org/wiki/Defamation>

2. https://en.wikipedia.org/wiki/Hate_speech.

3. http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

4. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

- Saldırgan veya saçma sapan bir içeriği çevrimiçinde paylaşmanız halinde, bu sizin hâlihazırda ve gelecekteki sosyal ve mesleki hayatınız etkileyebilir. Örneğin, içinizi dökmek istediğinizde bütün dünyaya bir tweet göndermekten ziyade güvenilir arkadaşlarınızla/ailenizle konuşun ya da yastığınızı suratınıza kapatıp çılgık atın zira bu, size geri dönüp sonsuza kadar peşinizi bırakmayacaktır. Çevrimiçindeki itibarınızın korunmasına ilişkin daha fazla bilgi için bkz. Web We Want.

— Diğer içerik şekillerini paylaşmak (örneğin, okulundan bazı şeyler) ya da okulun adına resmi bir web sitesi tasarlamak isterseniz, aklınızda tutmanız gereken diğer birkaç husus bulunmaktadır:

- Resmi bir site tasarlanmadan veya web sitesi oluşturma yarışmalarına öğrenciler katılmadan önce internet güvenliği ve makul kullanım hakkındaki okul politikası açık bir şekilde tanımlanmalıdır.
- Mizanpaj ve fotoğraf kullanma şekli okulun internet güvenlik politikasını yansıtmalıdır.
- Güvenlik ve mahremiyet endişelerinden dolayı, birçok okul yayınladığı fotoğraflarda yer alanların isimlerini paylaşmamakta veya sadece ön ismini paylaşmaktadır. Web sitenizi oluştururken dikkate almanız gereken bu konudaki güvenlik protokolünüzün ne olduğudur.
- Bilgi bütünlüğünü sağlamak amacıyla diğer web sitelerine bağlanan bütün dış bağlantıların (hyperlink) taranması ve bu web sitelerinin okulun internet güvenliğine ilişkin tutumunu yeterli şekilde yansıtmayı iyi olacaktır.
- Eğer bir okulda öğretmenseniz, okulunuzun, internet erişiminizin filtrelenebileceğine (yasal olarak filtreleme zorunlu olmadığı takdirde) ya da öğrencilerinize daha “bilinçli” kullanmayı öğretmeye karar vermesi gerekecektir. Birçok okul her iki tekniğin birleşimini etkin hale getirecek bir çözüm bulmaktadır. Ayrıca öğrenciler ödev olarak bir web sitesi oluşturduğunda unutmayın ki bu web sitesi dünyanın her yerinden kullanıcılar tarafından ziyaret edilebilir. Bu web sitelerini okulunuzun bir çeşit halkla ilişkiler aracı olarak düşünün. Bu nedenle bir öğretmen olarak öğrencilerinizin çalışmalarını gözlemlemeniz ve onlara tasarım aşamasında yol göstermeniz akıllıca olacaktır.
- Öğretmenler, bazı durumlarda da ebeveynler, öğrencilerin hazırladığı bütün çalışmalardan nihai olarak sorumludurlar. Bu nedenle, öğretmenlerin web sayfalarını reddetme ya da okul veya proje sayfalarından çıkarma konusunda yetki sahibi olmaları gerekir.
- Öğrencilerin çalışmalarını uygun bir şekilde gözlemek amacıyla öğretmenler daima şifrelere, web sayfalarına ve benzerlerine erişim sağlamalıdır.



NASIL

- Profesyonel bir web-barındırma hizmetine ödeme yapmak istemiyorsanız çevrim içinde içerik paylaşımı çok da zor olmadığından kendi alan adınızı kendiniz alın.
- Web sitesi hazırlayıcıları, bloglar ya da vloglar gibi kullanacağınız birçok hizmet, (Bkz. Kılavuz 4) web sitenize başlamanızda yardımcı olacak öğretici materyalleri sunmaktadırlar.
- Bununla birlikte, bir web sitesini sıfırdan oluşturmak belli ölçüde yetenekler kazanmanızı gerektirecektir. Neyse ki, günümüzde bir web sayfası oluşturmada nasıl kodlama yapılacağını öğrenmenin kelimenin tam anlamıyla milyonlarca yolu vardır. En yaygın olanlardan bazıları şunlardır: Codeacademy³ ve W3schools⁴. Fakat asla durmayın. Daima kendi dilinizde veya ihtiyaçlarınıza uygun diğer materyalleri bulmak için çevrimiçinde bazı araştırmalar yapmaya vakit ayırın.
- Ayrıca, profesyonel bir web-barındırma hizmetine başvurmanız e-posta adresiniz yanı sıra, gerçek isminiz, adresiniz, telefon numaranız ve özellikle kredi kartı gibi bazı ödeme bilgileri türünden ilave bilgiler vermenizi gerektirir. Bu nedenle çocuklar ve gençler daima bir yetişkinden (öğretmen, ebeveyn) ön bir rehberlik ve destek alacaklarından emin olmalıdır.

5. <http://www.webwewant.eu>

6. <http://en.wikipedia.org/wiki/Password>

7. <http://en.wikipedia.org/wiki/Website>

8. www.codecademy.com

9. www.w3schools.com/



SINIF ÇALIŞMALARI İÇİN FİKİRLER

Okulunuzun çevrimiçinde görünür kılınması

■ Bir okul web sitesi, bloğu, vlogu ya da benzeri doğru kullanıldığında toplumun birçok değişik katmanlarını bir araya getirmek için güçlü bir araç olarak hizmet edebilir. Aşağıda web içeriği için bazı kullanışlı öneriler sunulmuştur:

- Öğretmenler ders planları ya da belirli bir süre aralığı boyunca öğrencilerin yaptıklarının değerlendirmelerini sunabilirler.
- Yöneticiler plan veya duyuruları postalayabilir.
- Çocuklar ve gençler sanat, şiirler, hikâyeler veya diğer çalışmalarını yayınlamak isteyebilirler.
- Ebeveynler, festivaller veya diğer toplantılar gibi ebeveyn-öğretmen faaliyetlerini duyurmak için siteyi kullanabilirler.
- Geniş ölçekte topluluk, futbol takımları, kır gezileri, polis, yol çalışmaları benzeri hakkında duyurular için bir forum olarak kullanabilirler.

■ Geniş ölçekli bir içerik, herhangi bir websitesini, blogu veya vlog'u zenginleştirebilir ancak çok sayıda katkı sağlayıcı bir Web sitesinin yönetimini karmaşık hale getirebilir. İçerik toplamak ve yazmakla sorumlu küçük bir takımın seçilmesi önemlidir. Bu görev en iyi şekilde bir öğretmen veya idareci tarafından ya da bilgi ve iletişim teknolojileri koordinatörlük görevini yapacak başka bir kişi tarafından yürütülebilir.



İYİ UYGULAMALAR

- Tüm hesaplarınızı takip ediniz. Bu hizmetlere abone olmak için kullandığınız e-posta adresinde klasörler oluşturunuz ve hesaplarınızdaki kullanıcı adı gibi önemli bilgilerinizi her zaman bulabilmek için e-postalarınızı gruplandırınız.
- Web sitesi hesapları, blog, vlog ya da benzeri gibi önemli çevrimiçi hizmetlere kayıt olurken daima e-posta adresinizi kullanınız, sosyal ağ hesabını kullanmayınız. Her ne kadar Facebook, Google+ veya diğer sosyal ağ hesaplarını kullanarak hizmetlere kayıt olmak uygun görülebilse de, bu durumda bu hizmetlerin bilgilerinizin büyük kısmına erişeceğine dair izin verdiğinizden unutmayın. Ayrıca, bazı sosyal ağlar sonsuza dek devam edecekmiş gibi görünseler de, eğer bir gün hizmetlerini sona erdirirlerse hesabınıza giremeyebilirsiniz (örneğin bir gerecin toplum tarafından yetersiz kabul edildiği durumda, o araç demode olabilir).
- Bir web sitesi, blog ya da vlog aracılığıyla bir içeriğin çevrimiçinde paylaşılması görüşlerinizi paylaşabilmek açısından büyük bir fırsattır ancak takma isim kullanarak veya belirli kişisel bilgileri geri çekerek mahremiyetinizi korumayı arzu edebilirsiniz.
- Küçük adımlarla başlayınız, çevrimiçinde aktif hale getirmeden önce ya da sınıfta tanıtmadan önce içeriğinizi öğrenmek ve deneyimlemek için zaman ayırınız. Fikir ve ilham almak için diğer web siteleri, blogları ya da vlogları ziyaret etmek bu konuda size yardımcı olabilir.
- Okulunun web sitesi, bloğu ya da vlogunda yer alan okul adresi ve okul telefon numarası gibi temel irtibat bilgilerini daima içeriğinize ekleyiniz.
- Web içeriğinin kullanıcı ve cihaz dostu olduğundan emin olunuz. Günümüzde, giderek daha fazla sayıda insan cep telefonları yoluyla web içeriğine erişmektedir ve bu durum ayrı bir düzen ve tasarım gerektirmektedir. Web içeriğini, engelli kullanıcılar için erişilebilir hale getirmeniz ayrıca iyi bir uygulama olacaktır. Bu web sayfasındaki bazı kaynaklara göz atınız: <<http://w3.org/WAI/gettingstarted/Overview.html>>.
- Türkçe konuşmayanların da içeriğinizden faydalanabilmeleri için web içeriğinizi mümkün olduğunca çoklu dilde oluşturunuz.



DAHA FAZLA BİLGİ İÇİN

- Sayısal eğitimler konulu bu makale web sitesi tasarımcıları hakkında daha fazla bilgi vermektedir:
<<http://web.archive.org/web/20160622040107/http://www.digitaltrends.com/computing/best-website-build-websites-free/>>.
- Çevrimiçi itibar yönetimi hakkındaki Wikipedia makalesi:
https://en.wikipedia.org/wiki/Online_presence_management.
- AB Komisyonunun yeni Genel Veri Koruma Düzenlemelerinden veri koruma Kılavuz listeleri “unutulma hakkı” konusunu da içermektedir:
http://ec.europa.eu/justice/dataprotection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf
- BM Çocuk Hakları Sözleşmesinin ilgili maddeleri:
- Madde 13 - Çocuklar kendilerine veya başkalarına zarar vermediği takdirde bilgi alma ve paylaşma hakkına sahiptir.
- Madde16 - Çocuklar mahremiyet hakkına sahiptir. Mevzuat çocukların yaşam tarzlarına, onurlarına, ailelerine ve konutlarına karşı saldırılardan korumalıdır.
- Madde 29 - Eğitim her bir çocuğun kişiliğini ve yeteneklerini tam anlamıyla geliştirmelidir. Eğitim çocukların ebeveynlerine, kendi kültürlerine ve başkalarının kültürlerine saygı göstermelerini teşvik etmelidir.
- Madde 31 - Bütün çocuklar dinlenme, oynama ve geniş ölçüde etkinliklere katılma hakkına sahiptir.

Kılavuz 3

Web 2.0, Web 3.0 ve dahası



Web 2.0 bize sadece veri indirme ve tüketme imkanı vermez aynı zamanda veri yükleme ve oluşturma imkanı da vermektedir. Web 2.0 terimi, kullanıcı tarafından oluşturulan içeriği, kullanılabilirliği ve birbiriyle işleyebilirliği vurgulayan web tabanlı “ikinci nesil” hizmetlerin algılanmasını ifade eder. Bunun tipik örnekleri; kullanıcılar arasında çevrimiçindeki işbirliğini ve paylaşmayı kolaylaştıran tüm sosyal ağ siteleri, wiki’ler (**kullanıcıların iş birliği yaparak doğrudan web tarayıcısı yoluyla üzerindeki içeriği ve yapıyı değiştirdiği web siteleri - Wikipedia**), iletişim gereçleri ve folksonomi’lerdir (**çevrimiçi içeriği tanımlayan ve açıklayıcı not iliştiren kullanıcı tarafından oluşturulmuş biçim/yönlendirme imleri veya anahtar kelimelerden türetilen bir sınıflandırma sistemidir – dictionary.com**). Belli teknik güncellemelerden ziyade Web 2.0, bir dizi yenilikleri içermekte ve bu yenilikleri, kullanıcıların tamamen tarayıcıları aracılığıyla yazılım uygulamalarını kullanmalarına imkan veren “platform gibi ağ” şeklindeki bilgi işlemi mümkün kılmak amacıyla “Web 1.0”in etkileşimli işlevleri üzerine bina etmiştir.

— Kullanıcılar, herhangi bir Web 2.0 sitesi üzerinde veri sahibi olabilirler ve bu siteyi kullanırlarken uygulamaya değer katmaları yönünde kendilerini cesaretlendiren bir “katılım mimarisi” yoluyla da söz konusu veri üzerinde denetim sağlarlar. Bu, ziyaretçilerin izlemesini sınırlandıran ve içeriğini ise sadece web sitesi sahibinin değiştirebildiği geleneksel web-sitelerine kıyasla devasa avantajlar sunar. Web 2.0 siteleri, akan videolar gibi ileri teknolojiyle yapılan genelde bir araya getirilmiş veya “zengin” medyaya, kullanıcıyla anında etkileşime giren indirilmiş programlara ve imleç üzerine getirildiğinde değişen içeriğe dayalı olan kullanıcı dostu bir ara-yüz özelliği sergilemektedir.

WEB 3.0 VE DAHASI

Web 3.0 (bazı yerlerde Web 4.0, 5.0, olarak da anılabilmektedir) daha geniş çapta tartışılan bir terimdir. Bazıları Web 2.0'ın evrilmesi ve genişlemesi olarak tanımlamakta iken bazı uzmanlar; verileri, kavramları, uygulamaları ve insanları birbirine bağlayan bir “bağlayıcı zeka” olarak tanımlamakta, birçok uzman ise Web 3.0'ın, sonunda kendi verilerini kendisinin oluşturmaya başlayacağını düşünmektedir. Bazıları bu terimi “Anlamsal Web” olarak tanımlamayı tercih etmekte iken bazı uzmanlar ise Anlamsal Web'i, gelecekteki büyük web evrimini tanımlayacak bir takım yakınsayan teknoloji ve akımdan sadece bir tanesi olarak tanımlamaktadır.

Başka ağ türleri de bulunmaktadır. Darknet (veya dark net) dünyayı çevreleyen ağ (World Wide web) dediğimiz ağın üzerinde bulunur ve genelde özel iletişim protokolleri ve kapıları kullanılarak sadece belli yazılım, yapılandırmalar veya yetkilendirmeye erişilebilir. Arkadaştan arkadaşına [Friend-to-friend (F2F) – sadece birbirini tanıyan kişiler arasındaki doğrudan bağlantılar] ve akranlar arası (peer-to-peer) ağlar genelde dosya paylaşımı için kullanılmaktadırlar. “Tor” gibi ağlar anonim bağlantılar dizesi aracılığıyla çalışırlar ve bundan dolayı da yasadışı faaliyetler için daha kolayca kullanılabilirler.



OKULLAR AÇISINDAN ÖNEMLERİ

Web 2.0 gereçleri; yaratıcılığı, ortak çalışmayı ve iletişimi kolaylaştırmakta ve öğrenim üzerinde derin bir etki bırakabilmektedir. Bu gereçlerle, öğrencilerin geleneksel sınıf faaliyetlerini evde¹ yapabildiği teknolojik sınıflar (flipped classrooms) gibi yeni pedagojik modeller geliştirilmiştir. Çünkü Web 2.0 gereçlerinin çoğu ücretsiz programlar olup yazılım maliyetinin düşürülmesine yardımcı olmuşlar ve okullar için lisanslama modellerinin geliştirilmesinin önünü açmıştır.

Aşağıda yer alan tabloda da görüldüğü üzere Web 1.0, 2.0 ve 3.0 birbirinden farklılık gösterirler:

Web 1.0	Web 2.0	Web 3.0
Uygulamaya dayalı	Web'e dayalı	Çoklu cihaz/dinamik uygulamalar
Yalıtılmış	Ortak çalışılabilir	Özellikli içerik dağıtılabilir
Lisanslı veya parayla alınmış	Ücretsiz	Yakınsamış çok-lisanslı medya
Tek yaratıcı	Ortak yaratma	Yaratıcılarla cihazlar etkileşir
İyi Davranış Kuralları	Açık kaynak	Ortak inşa edilmiş, uygulanabilir
Telif haklı içerik	Paylaşılmış içerik	Kullanıcı-ve-makine kaynaklı içerik

Sayırsız başka teknolojiler bulunmasına karşın Web 2.0 teknolojilerinin genelde en çok kullanılan dört kullanım sahası; sosyal ağlar (bkz. Kılavuz 8), mesajlaşma, video ve film oluşturma ve izleme [podcast aracılığıyla, MP4'ler vb.] ve wiki'lerdir.

Podcast yayını² iPod'un ortaya çıkmasıyla doğmuş olup, adı (2001 yılında Apple'ın ürettiği taşınabilir medya oynatıcısı) İngilizce “iPod” ve “broadcast” kelimelerinin birleştirilmesiyle türetilmiştir. Bu, mobil cihazlarda ve bilgisayarlarda tekrar çalmak amacıyla internet üzerinde ses dosyalarını paylaşma yöntemidir ve MP3 (ses katmanlı MPEG sayısal dosya) olarak anılmaktadır. Günümüzde MP3'ün yerini hem ses hem de görüntü depolayan bir çoklu ortam formatı olan MP4 almıştır. Podcastlar ve MP4 videoları öğretmen ve öğrencileri dış dünyayı sınıf içine taşıyabilmelerini ve olayları ve deneyimleri paylaşabilmelerini kolaylaştırmaktadır.

Video-paylaşımı 2005 yılında YouTube'un başlamasıyla birlikte oldukça popüler olmuştur ve bugünlerde birçok sosyal medya platformu aracılığıyla da yapılabilmektedir. Teachertube³,

1. https://en.wikipedia.org/wiki/Flipped_classroom

2. <http://computer.howstuffworks.com/internet/basics/podcasting.htm>

3. www.teachertube.com

YouTube⁴'a dayalı olarak öğretmenlere eğitimde kullanmaları amacıyla tahsis edilmiş bir site olup, okullar ve örgütler kendi video paylaşım kanallarını kurmak için bu siteyi de kullanabilmektedirler. Video paylaşım siteleri⁵ genelde aranabilmekte, kullanıcılarına video gönderme, yorumda bulunma, yönlendirme ve izleme imkânı sağlayabilmektedir. Ortak ilgiye sahip birçok topluluk, video üretimi ve paylaşımı amacıyla internette yer almaktadır. Son zamanlarda, kullanıcılarına çevrimiçinde kendi video kliplerini oluşturma, ses ve altyazı vb. ekleme imkânı sağlayan siteler ortaya çıkmıştır. Örneğin; Jumpcut⁶.

Wiki'ler okuyucuların başkalarıyla etkileşimde bulunması ve ortak çalışmasına imkân sağlayan web siteleridir. Bu web sitelerine herkes yazı yazabilir ve eklemede bulunabilir. Wiki, okullarda ortak çalışma içinde yazılan eserler için muhteşem bir Web 2.0 gereçidir. Örneğin; Google docs⁷ kullanıcılarına metinler, slayt sunumlar ve tablolar üzerinde beraber çalışma imkanı sunar. Wiki'ye çok bilinen bir diğer örnek ise şu anda Britannica Ansiklopedisinden daha fazla güncel bilgi girişi alan ve ortaklaşa geliştirilen bir ansiklopedi olan Wikipedia'dır.

Sosyal İmlleme, kullanıcılara kendilerinin oluşturduğu internet beğenilerini veya imlemelerini paylaşımlarına imkân sağlar. Geleneksel olarak, kullanıcıların internet tarayıcısının bir parçası olarak beğendikleri web-sitelerinden oluşan bir liste bulunmaktadır. Hâlihazırda, sosyal imleme, herkesin kullanabildiği şekilde bu listeleri kolayca paylaşabilmelerine imkân tanımaktadır. Kullanıcıların, yönlendirme imleri kullanarak daha kolay şekilde aramasını ve kullanmasını mümkün kılmak amacıyla içerik sınıflandırılabilir. Delicious⁸ web-sitesi ve uygulaması, sosyal imlemeye bir örnektir ve kullanıcılara ne kadar çok insanın belli bir siteyi kaydettiğini göstermektedir.

Fotoğraf paylaşımı, kullanıcıların ailesi ve arkadaşlarıyla fotoğraf paylaşmasına imkân sağlayan popüler bir gereçtir. Buna Flickr⁹ sitesini örnek verebiliriz. Bu site, kullanıcıların fotoğraf göndermelerine ve daha sonra da başkalarını ya tek olarak veya bir slayt gösterisi şeklinde izlemeye davet etme imkânı sağlamaktadır. Her fotoğrafa yönlendirme imi veya not eklenebilmekte ve başkalarının yorum yapmasına da imkân sağlanmaktadır.

Fotoğraf düzenleme ve geliştirme yazılımı, artık çevrimiçinde yerini almıştır ve kullanıcılara kendi fotoğraflarını düzeltip geliştirmelerine imkân sağlamaktadır. Artan biçimde popüler hale gelen bu uygulamaya örnek olarak şunları verebiliriz:

- Picasa (Google) <<http://picasa.google.com>>
- iPhoto (Apple) <www.apple.com/iphoto>
- Photo Story (Microsoft) <<http://microsoft-photo-story.en.softonic.com>>.

ETİK HUSUSLAR VE RİSKLER



- Web gereçleri herkesin internete malzeme yükleme veya yazmasına imkân vermektedirse de içerik her zaman doğru veya hakikatte olduğu gibi olmayabilmektedir. Bu da öğrenmekte olan gençlere geçerlilik ve tarafsızlık açısından siteleri ve içeriği değerlendirmeleri için gerekli medya becerilerini geliştirmeleri yönünden geniş fırsatların sağlanmasının öneminin altını çizmektedir.
- Öğretmenler her asılsız içeriğin illaki kötü olduğuna dair oldukça basit bir çizgiyi benimsememelidirler, bu belki de çevrimiçindeki uydurma bir oyunun uzantısı olabilir ve belki de eğitsel bir değeri olabilir (örneğin; sosyal ağ sitelerindeki ünlü tarihi kişilerin uydurma profilleri).
- Web gereçleri ve uygulamaları, kullanıcılara kendileri ve başkaları hakkında bilgi yayımlamaları için sınırsız fırsat sunmaktadır. Ancak bunlar yine de kendi kendini ifşa etme ve mahremiyetin kaybı risklerine yönelik tedbirli kalmaya devam etmek zorundadır. Pratik kural, tüm dünyanın bilmesi açısından anlam taşımayan hiçbir şeyi yayımlamamaktır (bkz. Sosyal ağ kurma konusundaki Kılavuz 8).
- Öğrenme sürecinde teknolojiyle bütünleşmek zaman ve çaba gerektirmektedir. Bu sebeple, bu sürece başlamadan önce, Web 2.0 ve Web 3.0 gereçlerinin kullanımının öğrenenleriniz açısından anlamlı sonuçları olacağından emin olmalısınız.
- Tüm Web 2.0 gereçleri eşit şekilde oluşturulmamıştır ve aynı felsefeye ya da iş modeline sahip değildir. Wikipedia gibi bir web sitesinin ticari olmayan, bağımsız, gönüllülük esasına dayalı, beraber çalışmaya dönük yaklaşımı bulunurken Facebook gibi birçok sosyal ağın ticari amaçları bulunmaktadır.

4. <https://support.google.com/youtube/search?q=teachers+channel>

5. <http://computer.howstuffworks.com/internet/basics/video-sharing.htm>

6. www.jumpcut.com

7. <https://www.google.com/docs/about/>

8. <https://del.icio.us>

9. www.flickr.com/

- Wikipedia'ya eklemekte olduğunuz içerik toplumun yararına kullanılacaktır, ama facebook'a eklediğiniz içerik ise diğerlerinin yanı sıra sizin kişisel reklamınızı gösterme amacıyla kullanılacaktır.
- Web 2.0/3.0 yetenekleri sayesinde rating ölçüm ürün ve hizmetleri popüler hale gelmiştir. Ancak, eleştirel yargılama her zamankinden daha da gerekli hale gelmiştir, çünkü bu tür popüler sitelerde rating ölçümleri gerektiğince güvenilir değildir, ödeme karşılığı alınan tavsiyeler artan biçimde yaygınlaşmaktadır.



SINIF ÇALIŞMASI İÇİN FİKİRLER

- **İnternet kullanımı:** İnternet kullanıcılarının %86'sı için en popüler çevrimiçi faaliyet sosyalleşmedir, bunu %50 ile bilgi alma takip etmekte, kariyer ve ticaretle ilişkili faaliyetler ise yaklaşık %25 ile¹⁰ son sırada yer almaktadır. İnternet kullanımı istatistiklerini öğrencilerinizle/çocuklarınızla tartışınız. Onların internet kullanımı, kendi ülkelerindeki ve dünyanın diğer ülkelerindeki başka gençlerle ve on yıl önceki kullanımla nasıl mukayese edilir? Bunun etkilerinin bazıları neler olabilir?
- **Video:** Verilen bir konu hakkında öğrenciler görüş ve fikirlerini daha geniş çaplı şekilde paylaşmak için kendilerine ait videolar oluşturabilirler. Öğrencileri çalışma gruplarına bölün, resimli bir taslak hazırlayın ve video yaratmak için onların cep telefonlarını kullanın. Bu görüntüleri internete yüklemekten önce ve benzeri durumlarda telif hakkı (bkz. Kılavuz 14) ve filmi çekilmiş / fotoğrafı alınmış kişinin iznini alma (veya küçük olmaları halinde ebeveynlerinin iznini alma) gibi konuları tartışma fırsatını sağlayacaktır. Öğrencileriniz milyonlarca internet kullanıcısına erişmek için sınıfınız veya okul web sitesi ya da YouTube¹¹ üzerinde tahsis edilen bir kanal aracılığıyla video görüntülerini paylaşabilir. Hali hazırda bazı okullar, gelememeleri sebebiyle dersi kaçıran öğrenciler için kaçırdıkları dersleri telafi edebilmeleri amacıyla dersleri kaydeden video cihazı kullanmaktadırlar.
- **Wikiler:** kendi eğitim düzeninize en iyi şekilde uyum sağlayan wikileri bulunuz (bkz. daha fazla bilgi), sonrasında öğrencileriniz için üzerinde beraberce çalışılabilecek bir çalışma bulun. Bireysel olarak, öğrencilerin çalışmasını faal olarak denetleyebileceksiniz ve yapılan tüm değişikliklerin bir kaydını tutabileceksiniz. Wikiler, öğrenciler için hakiki işbirliği projelerindeki okullar ve ülkeler arasında çalışma yürütmek için ideal fırsatlar sağlamaktadır.
- **Sosyal imleme:** belli bir araştırma projesi oluşturun ve görevleri münferit olarak öğrencilere veya gruplara bölün. İhtiyaçlarınıza yanıt veren bir sosyal ağ imlemesi bulmak için bir araştırma motoru kullanabilirsiniz. Her grup, ayrıntılı bir dizi ilgili bağlantılar derlemek için sosyal imlemeler kullanabilir. Bunun tek avantajı, beğeni olarak işaretledikleri çalışmalarına devam etmek istediklerinde, aynı bilgisayarı kullanmak zorunluluğunda olmadan, istedikleri bilgisayarı istedikleri zaman kullanabilmelerinin mümkün olmasıdır.

DAHA FAZLA BİLGİ

- Bu iki wiki eğitim düzenlerinde kullanılabilir: <http://mediawiki.com> ve <http://www.pbworks.com>.
- Günümüzde Avrupa'daki yüzbinlerce okulda öğretmenler, Avrupa Komisyonu'nun eTwinning ağı yoluyla başka ülkelerdeki sınıflarla güvenli bir öğrenim ortamında işbirliği içinde çalışmaktadırlar. www.etwinning.net/en/pub/index.htm.
- Okulda ve evde Web 2.0 kullanımı konusundaki güvenlik bilgisi şu adrestedir: www.betterinternetforkids.eu.
- YouTube Çocukları (Kids) videoların izlenmesi ve paylaşılması açısından YouTube.com'a göre daha az işlev sunmasına karşın, özellikle küçük çocuklar için uyum sağlanan güvenli bir ortam içinde işlev sağlamakta ve ebeveynler, öğretmenler ve bakıcılar için rehber ilkeler sunmaktadır: <https://kids.youtube.com/>.

10. <http://www.pewglobal.org/2015/03/19/2-online-activities-in-emerging-and-developing-nations/>.

11. www.youtube.com



- Sınıfta kullanımı açısından Web 2.0 gereçleri konusunda bilgi ve ücretsiz indirmeler şu adreste bulunabilir: <http://web.archive.org/web/20160413121845/http://www.solutionwatch.com/512/back-to-school-with-the-class-of-web-20-part-1/>.
- İlkokullar için yararlı Web 2.0 uygulamaları şu adreste bulunabilir: <http://web.archive.org/web/20150914224206/http://langwitches.org/blog/2007/12/22/best-web-20-applications-for-elementary-school/>.

Kılavuz - 4

Web-Günlüğü (Blogs) ve Görüntülü Web-Günlüğü (Vlogs)



Çevrimiçi günlük, 1990'lı yılların başında günümüzün bloguna evrilmiştir. “Blog” kelimesi “Weblog” kelimesinin kısaltılmışı olup, gruplar ve bireyler tarafından oluşturulan ve yayımlanan çevrimiçi bir gazete anlamına gelmektedir. “Weblog” terimi 2003 yılında Oxford sözlüğüne eklenmiştir. Bloglamayı bazı siyasetçiler ve ünlü kişiler başlatmasına karşın bloglar en çok, görüşlerini yayınlayan ve günlük hayatları hakkında konuşan daha sade insanlarla ilgili olmaya devam edegelen bir web uygulamasıdır.

Bloglar ve vloglar, blogçuların ve vlogçuların ebeveynlik veya otizmle yaşama ya da çeşitli konularda siyasi farkındalık yaratma gibi hayatlarındaki zorluklara ışık tuttıkları sosyal değişim amaçlı platformlar halini almışlardır.

Blogların popüler olması sebebiyle birçok web-sitesi içerik oluşturma ve yayınlamaya yardımcı olacak şekilde oluşturulmuştur. Bir blog içine yapılan her yazı girişine yönelik yorum yapılabilmekte, bu da tartışma fırsatları yaratmakta ve yeni fikirlerin gelişmesine yardımcı olabilmektedir.

Blogların ev sahipliği, sadece blog barındırma için oluşturulan veya sıradan web-barındırma hizmetleri ile yapılmaktadır. Günümüzde barındırma hizmeti ücretlerinin makul oranlarda olduğu düşünülmektedir.

1. <https://en.wikipedia.org/wiki/Blog>



Mobil-bloglar (Cep bloglar/moblogs)

— Moblogs olarak tanınan Cep-bloglar, bir cep telefonu ya da taşınabilir bir cihaz üzerinde bir web sitesinde veya blogda içerik yayınlama yöntemidir. Mobloglama² cep telefonlarındaki e-posta özelliğinin geliştirilmesi sayesinde ortaya çıkmıştır (Bkz. Mobil teknoloji hakkındaki 5. Kılavuz).



Vlogs

— Bir görüntü bloğu/video-loğu yukarıda da tanımlandığı üzere bir blog ile aynı şeydir, ancak postalanmaları video formatındadır. Vloglar başlangıçta YouTube üzerinde popülerdi, ama şimdi vlog'ları Vine, Instagram, Facebook ve Pinterest'te de bulabilirsiniz.



RSS (Zengin Site Özeti) beslemeleri

— RSS³ kısaltması ya da açık adıyla zengin site özeti halihazırda blogları biraraya getirmek amacıyla kullanılmaktadır. İçeriklerini başka sitelerde yayınlamak isteyenler, Web bağlantı için bir XML ya da açık adıyla genişletilebilir işaret dili kullanarak bunu sağlayabilirler.

— XML, HTML'e benzer bir kod türüdür ve de besleme olarak da bilinmektedir. Temel itibarıyla okuyucunun içeriğe "abone" olmasına yardımcı olur ve böylece kendilerine gönderilen blog güncellemelerini, bloğa tekrar ziyaret etmelerine gerek kalmadan alırlar.



Blogların ve Vlogların Eğitim açısından önemi

- Bloglar ve vloglar, oluşturucularına seslerini duyurmak için bir ortam sağlarlar. Blogçular ve vlogçular ilgi alanlarını paylaşırlar, düşünce alış-verişinde bulunurlar ve izleyicilerinde yankı uyandıran konularda izleyicilerini bilgilendirirler. Herkesin kolayca erişebileceği bir platformda yaşantılarını yazıya dökebilirler, maceralarını paylaşabilirler ve görüşlerini görsel olarak sunabilirler.
- Blogçular ve vlogçular, akıllı telefonları aracılığıyla yazarak, yayınlayarak ve içeriği internete yükleyerek aynı anda moblogçu olabilmektedirler.
- Akıllı telefonlar yaygın olarak kullanıldığından, halkın çeşitli kesimleri ve genellikle genç kitle, pahalı bilgisayar donanımına gerek kalmadan bloglama ve vloglama yapabilmektedirler.
- Önemli bir bilgi ve ifade yolu ve kaynağı olarak bloglar ve vloglar, gazeteciler, araştırmacılar ve eylemciler tarafından da kullanılmaktadır.
- Engelli insanlar ve özel gereksinimler konularında farkındalık yaratmaya ve tartışma başlatmaya odaklanan gelişmiş bloglar ve vloglar da bulunmaktadır.



Eğitim çevresinde bloglar

— Bloglar öğrencilerin öğrenme derecelerini kontrol etme şansı verir ve içinde düşünce ve duygularını paylaştıkları bir kamusal forum oluştururlar. Bloglar tartışma ve beraber çalışma yürütme için yaratıcı bir öğretme gereci olarak da kullanılabilirler. Örneğin, bir çağdaş edebiyat sınıfı "Arıların Gizli Hayatı" adlı bir romanı çalışmak için bloglamayı kullanmıştır. Yazar derse bir giriş bölümü yazmış ve öğrenciler ile ebeveynlerini günlük verdiği okuma ödevi hakkındaki izlenimlerini yazmaya davet etmiştir. Yazar daha sonra bu ödevlere verilen yanıtlara ilişkin yorumda bulunmuştur (bkz. <<http://techtraining.dpsk12.org/ilt/Bees/SLOBees.pdf>>).

— Uzmanlar bloglamanın içerdiği üç etaplı sürece dikkat çekmektedirler: izleyici tanımlama, amaç ve kapsam. Bu, şu web sitesi adresinde açıklanmaktadır <<https://macin.wordpress.com/2011/01/12/three-step-process-for-blogging/>> . Blogçular devamlı surette bakım yapmalı, filtrelemeli ve içerik göndermelidir. Öğrenciler, üzerinde yorum yapacakları içeriği araştırırken artan biçimde farklı kuramlar ve fikirleri tanımaya başlarlar ve içeriği eleştirel şekilde incelemek ve doğru içeriği farketmek için gerekli beceriler geliştirirler.

— Teknoloji eğitimde güdüleyici bir faktör olarak kullanılabilir. Blogların, yaratıcılık ve kendini ifade etme olanaklarını sunması sebebiyle öğrenciler bloglara ilgi duyarlar. Bu, çeşitli ders konularını öğretme aracı olarak da kullanılabilir.

— Çocuklara ve genç insanlara farklı bakış açıları sunan bloglar, sınıftaki her öğrenciye tartışmaya katılma şansı tanımaktadır.

2. https://en.wikipedia.org/wiki/Mobile_blogging

3. <https://en.wikipedia.org/wiki/RSS>

4. <https://en.wikipedia.org/wiki/XML>



ETİK DEĞERLENDİRMELER VE RİSKLER

- Öğrencilere herhangi bir çevrimdışı forumda ifşa etmeyecekleri kişisel bilgilerini kamuya ait internet ortamlarında da açıklamamaları gerektiğini hatırlatınız. Bu, bloglarla ilgili özel bir sorun olup, bu blogların bazıları doğası gereği genellikle kişisel özellik taşıır.
- İsimsiz blog oluşturmak bile her zaman tam anlamıyla isimsiz değildir. Bir bloğu yayından kaldırmak onun üzerindeki tüm içeriklerin silineceği anlamına gelmez.
- Çevrim-dışındayken güvenliğinizi düşünün ve şu soruyu sorun: Sağladığım bilgiye dayalı olarak birinin beni bulması ne kadar kolaydır?
- Blokçu veya vlogçu olarak kullanmayı tasarladığınız fikir ve kişiliğiniz üzerine düşünün. Bu fikriniz veya kişiliğiniz bazıları için saldırgan olarak adledilebilir mi? Okulunuz veya gelecekteki işvereniniz bu fikriniz veya kişiliğinizi saldırgan olarak değerlendirebilir mi?
- Bloglar ve vloglar nefret ve ayrımcılık içeren mesajların dağıtımı ve aşırısı, radikal ve rahatsızlık verici içeriğin geliştirilmesi için de kullanılabilir.



Nasıl?

— Teknik becerileriniz varsa sıfırdan bir blog yaratabilirsiniz. Çoğu insan bir blog içeriği oluşturmak ve yayınlamak için gereçler sağlayan siteleri kullanmaktadırlar. Okul blogları şu adrestedir: <<http://www.schoolblogs.net/wordpress/>>, Blogçu (bkz. aşağıda) ve Wordpress ücretsiz hizmet sağlayan popüler blog barınaklarıdır. Bunlar kolay, adım adım talimatlar sağlayarak size bir hesap açmanıza, bloğunuza ad vermenizi ve bir şablon seçmenize yardım ederler.

— Bloğunuzu oluşturduğunuzda ve çalıştırmaya başladığınızda merkezi bir web sitesinden girişler oluşturur ve yazarsınız. Ara-yüz olarak popüler yazılım WYSIWYG⁵ formatı olup, son derece kullanıcı dostudur. Bloğunuza uğrayan ziyaretçiler her girişin sonunda bulunan yorum bağlantılarını tıklayarak içerik hakkında yorumda bulunabilirler.

— Web sayfanızda yayınlamadan önce yorumlarınızı değiştirmeyi tercih edebilirsiniz.

— Yorumunuzu hiper-bağlantılar ve imajlarla zenginleştirdiğinizden emin olunuz. Bu özellikleri eklemek için kullanılan tuşlar, içeriğinizi girdiğiniz metin kutusunun üstündeki araç çubuğunda dahil edilmiş olmalıdır.

SINIF ÇALIŞMASI İÇİN FİKİRLER



- Öğrencileri, bir öğrencinin blogçu, diğerinin ise konu hakkında mülakat edilen kişi olacak şekilde iki takıma ayırınız. Gazeteci, blogçu mülakatı yönetsin ve daha sonra mülakat edilenin kabul edeceği bir blog yazsın.
- Engelliler, özel gereksinimler, sosyal değişme veya sosyal farkındalığa yönelik hazırlanmış üst düzey bloglar ve vlogları araştırın. Öğrencileri bir blog yorumu yaparak veya postası teslim ederek nasıl katkıda bulunabilecekleri hususunda tartışmaya davet edin.
- Öğrencilerin mesajlarını en iyi yöntemle nasıl iletecekleri hususunda düşüncelerini sağlayın: blogla mı, vlogla mı, bir dizi Tweet atarak mı, Vine videolar yoluyla mı yoksa Periscope videolar yoluyla mı? Seçenekler sınırsızdır. Eğer öğrenciler Twitter, Vine, Periscope veya başka bir uygulamayı tercih ederlerse onlara bu bağlantıları bloglarına dahil etmelerini hatırlatın.
- Öğrencilere ilgi duydukları 5 ila 10 konuya ilişkin bir liste hazırlamalarını isteyin. Daha sonra onlara tercih ettikleri konulara ilişkin blogların internette mevcut olup olmadığını araştırın.
- Popüler öğrenci ve genç blogçuları bazıları araştırın. Hangi konuları dile getiriyorlar: çevre, siyaset, moda, müzik, teknoloji?

5. "Ne görüyorsan onu alırsın": <https://en.wikipedia.org/wiki/WYSIWYG>



İYİ UYGULAMALAR

- Blog kendi görüşlerinizi yayınlamak için size büyük bir fırsat sunar, fakat takma ad kullanarak ve belli kişisel ayrıntılarınızı arka planda tutarak mahremiyetinizi korumayı arzulayabilirsiniz. Çocukların ve gençlerin blog içinde kişisel bilgilerini açıklamaları konusunda özellikle çok dikkatli olmaları gerekmektedir.
- Telif hakkı kanunlarına saygılı olunuz ve izinleri olmadan blog içerisinde başkalarının blog tasarımlarını veya fotoğraflarını kullanmayınız. Size, fotoğraflarını, kaynağı belirtilerek veya belirtilmeksizin ücretsiz olarak kullanmanıza izin veren birçok web-sitesi bulunmaktadır.
- Bloğunuzu sınıfta tanıtmadan önce uygulamalar yaparak kendi bloğunuz tanıyın. Bu, sizin fikir ve ilham almak için diğer bloglara ziyaret etmenize yardımcı olabilir. The School Blogs® web-sitesinin 4000'den fazla üyesi bulunmakta ve kullanıcılarına kendi okul bloğunu başlatma imkanı sağlamaktadır.
- Öğrencilerinize bloglama kavramını izah etmek için zaman ayırınız. Blogların neden açıldığını söyleyin ve iyi ve kötü bloglardan örnekler verin. Daha sonra öğrencilerinize postaların ve konuların uzunluğu ve sıklığı, hiper-bağlantıların ya da fotoğraf vb. hususları içerebilecek bir dizi katı kuralı anlatın. Öğrencilerden birer blog açmalarını isteyin, deneyimlerini tartışmalarını ve başkalarının blogları hakkında yorum yapmalarını isteyin.



EK BİLGİLER

- Blogger, bloglama ve şimdi ise mobloglama için gereçler sağlayan bir sitedir: www.blogger.com/start.
- Blogçular için yasal ve etik ipuçları şu adreste bulunabilir: <http://weblogs.about.com/od/bloggingethics/tp/Blogging-Best-Practices.htm>.
- Electronic Frontiers Foundation (EFF) (Elektronik Sınırlar Vakfı) blogçular için yasal bir rehber sağlamaktadır: <http://www.eff.org/bloggers/lg/>.
- Weblogg-ed- bu site halihazırda eğitimdeki mevcut bloglama akımlarını izlemektedir: www.weblogg-ed.com/.
- “Bloglama ve RSS - ‘nedir?’ ve ‘nasıl’ eğitimler için yeni güçlü web gereçleridir”: <http://web.archive.org/web/20160413030845/http://www.infotoday.com/MMSchools/jan04/richardson.shtml>.
- “Eğitilmiş blogçu: sınıfta okuryazarlığı geliştirmek için web-logları kullanma”: <http://firstmonday.org/ojs/index.php/fm/article/view/1156/1076>.
- K-12 öğrencisinin yazı yazmasını destekleyen araçlar şu sitede bulunabilir: www.readwritethink.org/student_mat/index.asp.
- Eğitimci için bloglama kaynakları şu sitede mevcuttur: <http://www.socialstudiescentral.com/>.
 - DarrenRowsetamamen bloglamadan hayatını kazanan ilk blogçuydu. Web-sitesinde bazı ipuçları ve kaynaklar sağlamaktadır: www.problogger.net/.
- Bloglarda kullanmak için ücretsiz fotoğraf sunan websiteleri şunlardır: www.pixabay.com, www.flickr.com/creativecommons/, ve www.freedigitalphotos.net.
- “Güvende olmak için beraber çalışma”, Birleşik Krallık Çocuklar, Okullar ve Aile Bakanlığı tarafından okullar için geliştirilmiş bir gereç-kiti olup, aşırıcılık ve radikalleşme konularında öğretmenlere kaynak sunmaktadır: www.preventforschools.org/download/file/mmu-learning-together-to-be-safe.pdf.
- Avrupa Konseyi’nin Avrupa İnsan Hakları Sözleşmesi Maddeleri: www.echr.coe.int/Documents/Convention_ENG.pdf:
Article 8-Özel hayata ve aile hayatına saygı gösterilmesi hakkı.
Article 10 - İfade özgürlüğü.

- BM Çocuk Hakları Sözleşmesi'nin ilgili maddeleri:

Madde 13- Kendilerine ve başkalarına zarar vermediği müddetçe, bilgiyi çocukların alma ve paylaşma hakkı vardır.

Madde16-Çocukların mahremiyet hakları vardır.Kanun onların yaşam tarzlarına, itibarlarına, ailelerine ve evlerine yönelik saldırılardan korumalıdır.

Madde 29-Eğitim tam manasıyla her çocuğun kişiliğini ve becerilerini geliştirmelidir. Eğitim çocukların ebeveynlerine, kendilerine ait ve başka kültürlere saygı göstermesini cesaretlendirmelidir.

İnternet Her Yerde



Mobil veya kablosuz ağlar aracılığıyla taşınabilir bilgisayarlardan veya cihazlardan internetin kullanımı olarak açıklayabileceğimiz “internet her yerde” yükseliştir. Çünkü, bireyler evlerinden veya işlerinden uzakta olduğu zamanlarda bağlanmadaki bu yeni yöntemlerin avantajını yaşamaktadırlar.

2012 yılında 28 üyeli AB içinde yaşları 16 ila 74 arasındaki insanların %36’sı, internete bağlanmak için mobil bir cihaz kullanmıştır. İki yıl sonra bu oran %51’e yükselmiştir. Çalışmalar’ internet bağlantıları için en yaygın şekilde kullanılan mobil cihazların cep veya akıllı telefonlar, dizüstü bilgisayarlar, notebooklar, netbooklar veya tabletler olduğunu göstermektedir.

1983 yılında cep telefonları ilk çıktığında çok az kişi satın almıştı. 1995 yılında ise AB içinde ikamet eden her 100 kişiden 5’inin cep telefonu aboneliği vardı. Eurostat’a göre 2003 yılında, 25 üyeli AB’de yaşayan her 100 kişiden 80’inin cep telefonu bulunmaktaydı.

On yıl sonra, akıllı telefon aboneliği sayısı yaklaşık olarak 400 milyon olmuştur ki bu da toplam el cihazlarının yaklaşık %40’ını temsil etmektedir. Ericsson, 2020 yılının sonlarına doğru Avrupa’daki akıllı telefon sayısının 800 milyon’a erişeceğini öngörmektedir.

1. http://web.archive.org/web/20160413105315/http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals

2. <http://web.archive.org/web/20150324081657/http://www.ericsson.com/res/docs/2014/emr-november2014-regional-appendices-europe.pdf>

— Cep telefonlarının çoğunda internet tarayıcısı ve e-posta özelliklerinin bulunması ve bilgisayarların kablosuz hale gelmesi sebebiyle mobil teknoloji ile kişisel bilgi işlem kullanımı arasındaki çizgiler ortadan kalkmıştır.

MOBİL TEKNOLOJİ



— Mobil teknoloji cep telefonu iletişimleri için kullanılan teknolojidir ve bazıları bilgi-işlemin³ geleceğinin mobil teknoloji olacağı hususunu tartışmaktadır.

SMS

— Kısa mesaj hizmetleri (SMS) telefon, Web ya da mobil iletişim sistemlerinin⁴ yazılı mesajlaşma hizmeti özelliğidir.

MMS

— Multimedya mesaj hizmetleri (MMS) kullanıcılara cep telefonlarından⁵ ve cep telefonlarına multimedya içeriği içeren mesajları gönderme imkanı veren bir özelliktir.

M-öğrenme (Mobil öğrenme)

— Mobil öğrenme ya da m-öğrenme, cep telefonları, elde taşınan bilgisayarlar ve kişisel sayısal asistanlar (PDAs⁶) gibi mobil teknolojilerin yardımıyla öğrenme anlamına gelir.

Yer Konumlama

— Yer konumlama, cep telefonu veya internete bağlı bilgisayar terminali gibi bir cihazın yeryüzündeki gerçek coğrafi konumunu belirleyebilme özelliğidir.

— Mobil teknolojisi kullanıcıları, cihazlarındaki yer konumlamanın işlevini anlamaları ve mobil cihazlarındaki standart mahremiyet ayarlarını ayarlayabilmeleri gereklidir (mahremiyet ayarları konusunda daha ayrıntılı bilgi için bkz. Kılavuz 9).

Apps (Uygulamalar)

— Bir mobil uygulaması ya da “app” akıllı telefonlar, tabletler, akıllı saatler ya da bazı durumlarda giyilebilir cihazlar⁷ gibi mobil cihazlarda özellikle çalıştırılmak için tasarlanmış bir bilgisayar programıdır. Giyilebilir cihazlar konusunda daha fazla bilgi için bkz. Kılavuz 23).

— Uygulamaların miktarı, cep telefon kullanıcılarının sayısına doğru orantılı şekilde artmış ve uygulama ekonomisinin Avrupa Birliği⁸ içinde her yıl 10 Milyar Avrodan fazla bir geliri yaratacağı tahmin edilmektedir.

— Ücretli veya ücretsiz mevcut uygulamaların devasa bir çeşitliliği bulunmakta ve indirmeden veya satın almadan önce uygulamalara ilişkin görüşlerin okunması tavsiye edilmektedir, çünkü ücretsiz uygulamalar uygulama-içi satın alımlar sırasında çok pahalıya mal olabilmektedir (Çevrimiçi satın alımlar için Kılavuz 13’e bkz.).

Mobil-Nakit (Mobicash)

— Cep telefonu kullanıcılarındaki artışla birlikte mali kurumlar, nakit kullanmadan işlem hareketleri ve mobil ödeme imkanı sunan tek bir mobil mali platform oluşturmuşlardır.

— “Orangemoney” - cep telefonu operatörü Orange’ın tarafından verilen mobil para hizmetlerine bir örnektir ve 13 ülkede kullanımdadır. Bunlar: Botswana, Kamerun, Fil Dişi Sahilleri, Mısır (Mobicash adı altında), Gine, Ürdün, Kenya, Madagaskar, Mali, Mauritius, Nijer, Senegal ve Uganda⁹.

— Birleşik Krallık tarafından hazırlanan bir rapora göre İngiliz tüketicilerinin 2021 yılına kadar mobil el-cihazları¹⁰ yoluyla yaklaşık 30.5 Milyar ABD Doları harcayacaklarını öngörmektedir.

3. https://en.wikipedia.org/wiki/Mobile_technology

4. https://en.wikipedia.org/wiki/Short_Message_Service

5. https://en.wikipedia.org/wiki/Multimedia_Messaging_Service

6. <https://en.wikipedia.org/wiki/M-learning>

7. https://en.wikipedia.org/wiki/Mobile_app

8. <http://web.archive.org/web/20160617033122/http://www.visionmobile.com/product/the-european-app-economy/>

9. <https://goo.gl/4LQvUJ>

10. <https://goo.gl/8a7Dx7>



KONULARIN ANLAŞILMASININ ÖNEMİ

- Çocukların mobil cihazları veya tabletleri çok erken yaşlarda elde etmeleri konusunda endişeler mevcuttur. Mobil cihazları veya tabletleri erken yaşlarda kullanmanın çocukların gelişmelerine nasıl etkide bulunabildiğine dair uzun vadeli herhangi bir araştırma henüz yürütülmemiştir.
- Çocuklara ilişkin diğer endişeler arasında, zararlarını anlamadan çocukların çevrimiçi alış-veriş ve e-ticaret yapmaları da bulunmaktadır.
- Uzun süre radyasyona maruz kalmanın tehlikeleri konusundaki araştırma sonuçsuzdur. Ancak bu tehlikeler en aza indirilebilir.
- Ev içinde bilgisayar kullanımı genel olarak halihazırda kurallara bağlanmış olsa da birçok ebeveyn cep telefon kullanımını “kişiyeye özel” olduğunu düşünmektedir. Bu yeni özgürlükle cesaretlenen çocuklar, “neredeyse bedava” ödüllü medya kampanyalarına veya zil sesleri gibi özelliklere para harcayarak kendilerini mali sıkıntı içine itebilmektedirler.
- Mobil cihazlar, içerdikleri coğrafi konum kolaylıkları yoluyla iz-sürme cihazları olarak da kullanılabilir. Özgürlüğün karşısında duran bu güvenlik konusu bir tezat da oluşturmaktadır.
- “Bluetooth” teknolojisi¹¹ hekleme (bilgisayar korsanlığı) ve istenmeyen mesajların alınması ve gönderilmesi gibi güvenlik sorunları doğurmaktadır.
- Moblogs,¹² mobil telefon bloglarıdır (web günlükleri). Bunlar, gençlerin bilgi ve fotoğraf göndermelerini kolaylaştırmakta ve potansiyel olarak başkalarının ve kendilerinin güvenliklerini tehlikeye sokmaktadır.
- Mobil zorbalık da giderek artan bir endişe kaynağı olmaktadır ve sadece akıllı telefonlar ve tabletlerle sınırlı değildir. Artık akıllı-saatler de önceden yüklenmiş sosyal ağ uygulamalarını içinde barındırmaktadır.
- Cep telefonu kameraları ve internete kolay erişme özellikleri mahremiyete bir tehdit oluşturabilmektedir: gençler arasında “uygunsuz fotoğraflar” çekmek gibi endişe doğuran (Ör; Jimnastik soyunma odasında veya yüz kızartıcı durumlarda başka gençlerin, sınıfta öğretmenlerin fotoğrafını çekmek gibi..), hatta internete yüklenmeden önce bu görüntülerin değiştirilerek yeniden biçimlendirilmesi gibi bir akım mevcuttur.
- Cep telefonu maliyetleri: Çocuklar genelde çevrimiçi oylama, istenmeyen yüksek ücretli kısa mesaj (SMS) hizmetleri ve uygulama-içi alımlar gibi belli hizmetlerin yüksek maliyetlerinden haberdar değildirler.
- Dikkat dağıtıcı olduklarından mobil cihazların araba kullanırken risk oluşturabildiği ve son zamanlarda yürürken bile insanlar için riskler doğurduğu tespit edilmiştir. Birçok birey yürürken mesajlaştığından, baş öne eğikken mesajlaşma sırasında yeri görmenizi sağlayan uygulamalar bile bulunmaktadır. Söz konusu yazılım Apple¹³ veya Android¹⁴’de de mevcuttur.
- 2004 yılından bu yana artık bir ev eşyası haline gelen mobil cihazları Virüsler¹⁵ etkilemektedir. Bir anti-virüs şirketi olan F-Secure, yüzlerce mobil cihaz virüsü bulunduğunu ve bunların tür ve sayı olarak sürekli arttığını tahmin etmektedir. En son virüs tehditlerini öğrenmek için “Tehdit tarifleri¹⁶”ne bir göz atınız.



ETİK DEĞERLENDİRMELER VE RİSKLERİ

- İnternet her yerde birçok risk içermektedir. Çünkü birçok kişi uygun mahremiyet ayarlarını kullanmaya pek önem vermemektedir. Tek bir kullanıcının birden fazla cihaza sahip olması ve bunları kullanma olanağı saldırıya mağruz kalma risklerini daha da mümkün kılmaktadır.
- Birçok kullanıcı kafelerde, restoranlarda ve diğer kamusal alanlardaki ücretsiz kablosuz bağlantılardan faydalanmakta ve bu çevrelerde kişisel ve mali bilgilerini vermektedirler.

11. <https://en.wikipedia.org/wiki/Bluetooth>

12. https://en.wikipedia.org/wiki/Mobile_blogging

13. <https://itunes.apple.com/en/app/type-n-walk/id331043123?mt=8>

14. <https://play.google.com/store/apps/details?id=com.biztech.typewhilewalk&hl=en>

15. http://en.wikipedia.org/wiki/Computer_virus; https://en.wikipedia.org/wiki/Mobile_virus_and_worms; http://en.wikipedia.org/wiki/Computer_worm

16. https://www.f-secure.com/en/web/labs_global/threat-descriptions

- İnternetin her zaman ve her yerde olması, çevrimiçinde ne yükleyeceğiniz veya postalayacağınız ve çevrimiçi satın alım ve diğer çevrimiçi faaliyetler hakkında karar verirken fazla düşünme süresiniz olmayacağı anlamına da gelmektedir. Örneğin; birçok uygulama olaylar gerçekleşirken canlı olarak yayınlamasına imkan tanımaktadır. Bu nedenle çocuğunuz gözü önünde cereyan eden yüz kızartıcı veya şiddet içerikli bir görüntüyü kaydetmemenin veya çevrimiçinde yayınlamamanın iyi bir fikir olmadığını düşünmeden yayınlatabilir.
- Çok küçük çocukların bile mobil cihazlar aracılığıyla satın alımlar yapabilmesinin kolay olması sebebiyle uzmanlar, paranın “sanallaşması” olarak adlandırdıkları ortaya çıkan yeni bir akım konusunda uyarıda bulunmaktadır. Bu akım yüzünden çocuklar paranın gerçek değerini kavramada güçlük çekmektedirler.



NASIL?

— Cep telefonları popülerdir ve bu telefona sahip olmak kolay ve göreceli olarak ucuzdur. Taşınabilir cihazınızı satın aldığınızda belirli dakika kullanımları için ya kontrollü tarife seçerek ödeme yapmayı ya da belli bir operatöre abone olup, hizmetleri için aylık bir ücret ödemeyi tercih edebilirsiniz.

— Akıllı telefonlar, tabletler, e-Okuyucular ve taşınabilir oyun konsolları gibi mobil cihazlar çevrimiçiye bağlanmak için sadece bir Wi-Fi bağlantısına gerek duymaktadırlar.



SINIF ÇALIŞMASI İÇİN FİKİRLER

— Gençler arasında cep telefonların çok popüler olması sebebiyle öğretmenler, öğrencileriyle ilgilenirken sınıf içi faaliyetlerine kısa mesaj hizmetlerini (SMS) ve benzeri uygulamaları da işin içine katabilmektedirler. El cihazlarının taşınabilirliği, sürekli meşgul olan öğrenciler için, grup veya okul dışı çalışması yapan öğrenciler için yararlıdır. Okul içi ve dışı öğrenimde mobil cihaz kullanımının öğrencilerin çalışmalarında sorumluluk almalarını teşvik ettiği ve tuttukları notları ve verilen ödevlerini kaybetme olasılığı azalttığı saptanmıştır.

- Bir okul gezisindeyken, öğrencilere izlenimlerini bir mobil cihaza kaydetmelerini söyleyin. Bunu yaparlarken ödevlerine fotoğraflarla ve video görüntüleriyle desteklemelerini isteyin.
- Ödevlerini ayrıntılı hale getirmeleri için öğrencilerin çeşitli uygulamalar kullanmalarını sağlayın. Örneğin; kısa video görüntüleri için Vine uygulamasını, olduğu yerde habercilik için Periscope uygulamasını veya akademik güncellemeler için Twitter veya Facebook uygulamalarını kullanabilirler.
- Öğrencilerden sınıfta mobil cihazları ve akıllı telefonları kullanmanın risklerini ve zorluklarını belirlemelerini isteyin. %100 teknolojik bir sınıfın mümkün olup olmayacağı hususunda ne düşünürlər? Neden? Neden olmasın?



İYİ UYGULAMALAR

- Düşük radyasyonlu bir cep telefonu¹⁷ kullanınız, öyle ki kulak için SAR oranı 0.56W/kg'dan daha fazla olmamalı ve vücut için ise SAR oranı 0.57W/kg'dan daha az olmalıdır. Kulaklık konusunda ise en iyileri bir frekans filtresine sahip olanlardır.
- Gençleri, cep telefonu ve tablet kullanımlarını kısıtlamaları yönünde cesaretlendiriniz ancak yasaklamayın. Cep telefonu kullanımı ve çeşitli mesajlaşma hizmetleri, onlu yaşlarda yaygın bir olgudur ve cep telefonları birçok çevrede akranlar arasında ağ üzerinden iletişim kurmada temel teşkil etmektedir.
- Güvenlik risklerinden kaçınmak amacıyla Bluetooth'u kullanmadığınızda açık bırakmayınız.
- E-postaya gelince, sadece güvendiğiniz kaynaklardan gelen veriyi kabul ediniz. Kısa mesaj hizmetleri (SMS) yoluyla gönderilen istenmeyen mesajlar (spam) konusunda dikkatli olun: cep telefonu numaranızı sadece yakından tanıdığınız insanlarla paylaşınız.
- Resimleri yayınlamadan önce, başkalarının yasal haklarını ihlal etmeyeceğinizden emin olunuz.
- Zararlı içeriklerin karşılıklı gönderilmesi konusunda çocuğunuzla konuşunuz ve bunun gençlerin korunmasına yönelik ulusal yasaları ihlal edebileceğini vurgulayınız.

17. <http://www.phonerated.com/top-rated-best-overall-low-sar-phones-global>

- Telefonunuzu ve tabletinizi kullanırken çevrenize karşı duyarlı davranın. Etrafınızdaki insanlar sizin konuşmanızı dinlemekten hoşlanmayabilirler.
- İstenmeyen aramalardan veya mesajlardan sıkıldıysanız cep telefonu operatörünüz ile veya varsa ulkenizdeki İnsafe yardım hattı ile temasa geçiniz.
- Birçok cep telefonunda filtreleme seçeneği vardır: istenmeyen numaraları engellemek için bir kara liste veya sadece seçilen numaraları aramalarını kabul etmek için bir beyaz liste oluşturup (örneğin; sadece telefon rehberinizdeki numaralar için) kullanabilirsiniz. İnternette ebeveyn kontrol filtreleri (ücretsiz yazılım) de indirebilir veya cep telefonu operatörlerinizden satın alabilirsiniz.
- Cep telefonların haberleşmede kullanılan yegane cihazlar olmadığını aklınızda bulundurun: tabletlerin ve akıllı saatlerin de mesajlaşma ve sesli iletişim özellikleri bulunmaktadır.
- Mali durumlarını henüz sorumlulukla yönetemeyen küçüklerin ve onlu yaşlardaki çocukların hoş olmayan sürprizlerle karşılaşmalarını amacıyla aylık abonelik yerine bir “ön ödemeli” plan seçiniz. Harcamalarını tartışınız ve paranın gerçek değerini anladıklarından emin olunuz.
- Çocuğunuza akıllı telefon satın alırken telefonunun ayarlarını yapılandırmayı unutmayınız. Cihazların çoğu artık tam özellikli (kamera, GPS, yakın alan iletişimi (NFC), bluetooth vb. ile) üretilmekte olup yetişkinler için varsayılan şekilde yapılandırılmışlardır. Çocuğunuzun akıllı telefonunu yapılandırma ayarları konusundaki çevrimiçi rehber ilkelerini araştırmak için tereddüt etmeyiniz. Tavsiye edilen adımların bazıları şunlardır: çocuğun hesabını şifreleme yoluyla koruma altına alınız, uygulama-içi satın alımları hizmet-dışı bırakınız, yeni uygulamaların kurulmasını (çok küçük çocuklar için) hizmet-dışı bırakınız, yer konumlamayı ve GPS’nin kullanımını hizmet-dışı bırakınız ve ebeveyn kontrolü yazılımını kurunuz.
- Mobil bir cihaz üzerinde satın almak amacıyla için parola bir kez girildiğinde parolanın 15 dakika boyunca faal kalmaya devam edebildiğini ve bunun da dikkatsizlikle bir başka satın alıma¹⁹ sebep olabildiğinin farkında olunuz.

DAHA FAZLA BİLGİ İÇİN

- GSMA raporu mobil ekonomiyi anlamamıza yardım edebilir: http://web.archive.org/web/20160411155639/http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf.
- 2014 yılında Avrupa’nın sosyal, sayısal ve mobil kapsama alanı geniş boyutlu bilgi-grafiği sunmaktadır: <http://web.archive.org/web/20151211195326/http://wearesocial.net/blog/2014/02/social-digital-mobile-europe-2014/>.
- S212 cep telefonlarının ve diğer cihazların incelemesinde bağımsız bir Birleşik Krallık sitesidir: <http://www.s21.com/mobile-phones.htm>.
- UNESCO siyasa yapımcılar ve planlayıcılar açısından mobil öğrenmenin geleceği ve bunun sonuçlarına dair bir rapor yayımlamıştır: <http://unesdoc.unesco.org/images/0021/002196/219637E.pdf>.
- “Çocuklar ve cep telefonları, eylem için bir gündem” Childnet International’ın bir çevrimiçi yayımıdır: http://www.childnet.com/ufiles/CMPAAA_A4.pdf.
- İngiliz Film Sınıflandırma Kurulu, Bağımsız Mobil Sınıflandırma Kurulu’ndan mobil operatörlerinin çalışma kurallarını (Nizamname) güçlendirecek bağımsız bir çerçeve oluşturma yetkisini devraldı: <http://www.bbfc.co.uk/what-classification/mobile-content>.
- Bluetooth’u korumayı ve nasıl çalıştığını öğrenmek : <http://web.archive.org/web/20160407133222/http://electronics.howstuffworks.com/bluetooth4.htm>.
- Cep telefonu operatörü “Vodafone” ebeveynler için rehber ilkeler hazırladı: <https://www.vodafone.com/content/parents/howto-guides.html>.

18. http://www.saferinternet.org/ww/en/pub/insafe/focus/national_helplines.htm

19. <http://www.creditcards.com/credit-card-news/whos-responsible-kids-unauthorized-charges-1279.php>

2. İnternet Fikirlerle İnsanları Birbirine Bağlar

”

“Nihayetinde herşey birbirine bağlanır - insanlar, fikirler ve nesneler. Bu bağlantının kalitesi, bizatihi kalitenin kendisinin anahtarıdır”

Charles Eames, 20.yüzyıl başı, tasarımcı

KILAVUZ 6 – E-POSTA VE İLETİŞİM

Birkaç e-posta hesabı oluşturup bunların her birine farklı parolalar verdiniz mi?

Belirlenen parola yeterince “güçlü” müdür (parolanın güçlü olması için harfler, numaralar ve sembollerden oluşan karakter sayısının sekizden fazla olması gereklidir)?

E-postalarınızda konu satırınıza ilgili anahtar kelimeleri kullanarak açıkça başlık ekliyor musunuz?

E-posta hesaplarınız üzerinde iki aşamalı güvenlik sorgulaması uyguladınız mı? (ilave güvenlik sorusu sağlayarak ve/veya cep telefonu numaranızı girerek)

KILAVUZ 7 – SOHBET VE MESAJLAŞMA MEDYASI

Websitenizde veya blogunuzda iletişim bilgilerinizi eklediniz mi?

Çevrimiçi mahremiyetinizi korumak için önlemler aldınız mı?

Websiteniz/blogunuz için kullanmakta olduğunuz içeriğin telif hakları kanunuyla uyumlu olduğunu kontrol ettiniz mi?

KILAVUZ 8 – SOSYAL AĞ İLETİŞİMİ VE SOSYAL PAYLAŞIM

İtibar bizim sahip olduğumuz yegâne şeydir: “Göndermeden önce düşün” sorusunu düzenli olarak kendinize soruyor musunuz?

Kullandığınız sitelerdeki mahremiyet ayarlarınızı en son ne zaman güncellediniz?

Demokrasi, kamuoyu tartışmalarına mümkün olduğunca fazla vatandaşın katılımına bağlıdır: ilgili sosyal ağ siteleri yoluyla sesinizi duyurmaya çalıştınız mı?

KILAVUZ 9 – MAHREMİYET VE MAHREMİYET AYARLARI

Bir sosyal ağ iletişim sitesinde yer alan işaretlenmiş bir fotoğrafı e-postayla göndermek sizce gerçekten gerekli midir?

Paylaşmakta olduğunuz şeyi anlamak için mobil uygulama sözleşmesini okudunuz mu: sizin yükümlülükleriniz nelerdir, “onların” yükümlülükleri nelerdir?

Uygulamaları yüklediğinizde hangi özel bilgilerinize erişeceklerini tam olarak bildiğinizden emin misiniz? Uygulamanın işlevselliği açısından bu tür bir erişim gerçekten gerekli midir?

Avrupa Birliği’nin Genel veri koruma Düzenlemesi’nin sizin için ne ifade ettiğini anlıyor musunuz?

Kılavuz 6

E-Posta ve İletişim



Elektronik postanın kısaltması olan e-posta¹, internet gibi ağlar üzerinde birbirine bağlı bilgisayarlar arasında mesaj göndermek için kullanılan bir sistemdir. Terim aynı zamanda mesajın kendisini de tanımlamaktadır. Bir e-posta genellikle saniyeler içinde başarıyla aktarılır ve alıcı bu postaya erişim sağlayabilip uygun olduğunda da bunu cevaplayabilir. Esnek ve etkili bir sistem olan e-posta, çalışma ve iletişim yollarını ciddi şekilde değiştirmiştir. Her gün milyarlarca mesaj gönderilmektedir.

■ Bir e-posta adresi iki bölümden oluşur: @ işareti ile ikiye ayrılan yerel isimler ile alan isimleri. Yerel isim, genellikle -her zaman değil- kullanıcının ismini gösterir. Alan ismi ise kullanıcıların kuruluşunu, şirketini veya internet hizmet sağlayıcısını gösterebilir. Alan isimleri, kuruluş çeşitlerini ve/veya ülkeleri de gösterebilir. Örneğin, isim@ox.ac.uk, Oxford Üniversitesi'nde çalışan veya okuyan birisine aittir.

■ Birçok farklı iletişim şekilleri ortaya çıksa da, çevrimiçi olabilmek amacıyla hesap açmaya yönelik en çok kullanılan tek yol olması nedeniyle e-posta adresleri, hala, kullanıcıların çevrimiçi deneyimlerin merkezinde yer almaktadır. Bu nedenle, diğer iletişim araçları (sosyal ağlar, anlık mesajlaşma vb.) e-postalara tercih edilebilirken, e-postalar, kullanılan tüm çevrimiçi hizmetlere erişim sağlamaya yönelik bir “bağlantı” şeklinde çoğunlukla hizmet ediyor olması nedeniyle kullanıcıların çevrimiçi kimlikleri için “anahtar” haline gelmiştir.

1. <https://en.wikipedia.org/wiki/Email>



Eğitimdeki Önemi

— E-posta adresleri çevrim içindeyken talep edilmekte olduğundan, e- posta hesabını uygun biçimde idare etmek eğitsel değer taşımaktadır, bu daha çok daha kolay bulabilmek amacıyla kişisel içerik ile önemli idari içeriği sınıflandırarak fiziki bir postayı ayırma işine benzetilmektedir.

— E-posta, ayrıca, farklı ülkelerdeki gençlerden ve çocuklardan oluşan sınıflar arasındaki kültürler arası projeler için değerli bir araçtır. Çocuklar ve gençler, e-postayı, yabancı dil yeteneklerini geliştirmek için kullanabilirler ve kendi kültürlerine ilişkin bilgileri paylaşabilirler.

— Daha dışa dönük olmayan çocukların ve gençlerin bazıları, yüz-yüze sınıf tartışmalarına nazaran, e-posta yoluyla kendilerini daha iyi ifade edebilmektedirler.



Etik düşünceler ve riskler

- E-postanızın tüm çevrimiçi hesaplarınız için bir “giriş kapısı” olması nedeniyle, birinin e-posta hesabınızı kırmasının sonuçları çok ciddi olabilir.
- Çevrimiçi olarak bulabileceğiniz birçok e-posta hizmeti (erişim sağlamak ve bir kullanıcının e-postasının idaresi için kullanılan bilgisayar programları)² ücretsizdir, ancak bunların çoğu e-postalarınızın içeriğini taramak için algoritmalar kullanırlar ve istenilen reklamları web posta sayfasında görüntülerler.
- Duyguların e-posta yoluyla anlatılması zordur. Mesajlarınızın yanlış anlaşılmadığına emin olmak için mesajlarınızı her zaman dikkatle yazmanızın sebebi budur. Gülen yüzler gibi küçük açıklayıcı semboller olan “duygu sembolleri³”, özellikle ironi ve mizah olmak üzere, niyetlerinizi açıklamaya yardımcı olacaktır. Bununla birlikte, dikkati mesajınızdan başka yere çekmemek için bunları mümkün olduğunca az kullanın.
- Alınan e-postaların önemli bir miktarı, alıcının rızası olmadan gönderilen ve istenmeyen postalar⁴ (istenmeyen e-postalar, kötü amaçlı yazılımlar, dolandırıcılık ve güvenlik konularına ilişkin Kılavuz 19’a bakınız). Neyse ki, istenmeyen posta filtreleri, istenmeyen postalarla düzenli e-postaları sınıflandırmada giderek daha iyi olmaktadır.
- “Eğlenceli” ya da “ilginç” bulduğunuz e-postaları tüm kişilerinize göndererek “istenmeyen posta iletimine” katkıda bulunmadığınıza emin olunuz. Bu işlemi çok sık yaptığınızda, istenmeyen posta filtreleri, kendi e-posta adresinizi, istenmeyen postaların bir kaynağı olarak algılayabilir ve kişilere erişimlerinizi imkânsız hale getirerek, adresinizi kara listeye alabilir.
- Bazı “iletirler” sahte veya hilelidir. Bir e-postanın başkalarına her iletilmesi karşılığında, bir kurum veya şirketin, insani gerekçelerle (cerrahi yardıma muhtaç hasta bir çocuğun varlığına dair iddiaları sıklıkla zikrederek) küçük bir miktar para ödemeye söz verdiğine ilişkin yalan bir iddiada bulunan e-postalar buna bir örnektir.
- Yanıltmak amacıyla bir ismi saklamak çok kolaydır. Örneğin, elvispresley@hotmail.com adresinde olduğu gibi bir posta adresi oluşturarak ya da ayarlardaki ismi kolayca değiştirerek bu yapılabilir. Hatta bir e-posta adresinin, kişilerinizden birine ait olduğunu biliyor olsanız bile, adres sahibinin bilgisayarının bir virüs veya bir korsan tarafından ele geçirilen “yaşayan ölü bilgisayar” haline getirilmiş olması mümkün olduğundan konu satırını da mutlaka kontrol edin.
- Bir bağlantı sizi bir web sitesine yönlendiriyor gibi görünürken gerçekte başka bir siteye götürebilir. Bu durum, kimlik avı (oltalama) adı verilen dolandırıcılık olaylarında sıklıkla gözükme⁶.

2. https://en.wikipedia.org/wiki/Email_client

3. https://en.wikipedia.org/wiki/Emoticon#Basic_examples

4. https://en.wikipedia.org/wiki/Email_spam

5. [https://en.wikipedia.org/wiki/Zombie_\(computer_science\)](https://en.wikipedia.org/wiki/Zombie_(computer_science))

6. <https://en.wikipedia.org/wiki/Phishing>



İYİ UYGULAMALAR

- Farklı amaçlara (sosyal ağlara erişim, çevrimiçi alışveriş yapma) yönelik olarak birkaç adet e-posta hesabı açınız. Web’te yayınlamayıp ve sadece, siz ve arkadaşlarınızın kullandığı önemli hizmetlerde kullanarak, hesaplarınızdan birini, mümkün olduğunca özel tutmaya gayret ediniz. Nadiren kullandığınız hizmetler veya bir kez kullanacağınız hizmetlere erişim için farklı bir hesap kullanınız.
- E-posta mesajlarınızı kısa ve öz tutunuz. Uzun metinlerden kaçınmaya çalışınız. Heccelemelerinize dikkat ediniz.
- Konu satırında ilgili kelimelerin bulunduğundan emin olunuz. Bu husus, mesajınızın alıcınız tarafından gerçek olarak tanınmasına yardım eder ve bir süre geçtikten sonra bulmasına da yardımcı olur.
- E-posta hesaplarınız için güçlü şifreler (harfler, rakamlar ve sembollerden oluşacak şekilde en az 8 karakter uzunluğunda) belirleyiniz ve her bir hesap için farklı şifreler kullanınız.
- Gönderdiğiniz e-postaların boyutu konusunda dikkatli olunuz ve diğerleriyle nasıl iletişim yaptığınız hususunda akıllı ve stratejik hareket ediniz. Sayıca fazla insanlarla bir grup konuşmasına ihtiyaç duyduğunuzda, birçok e-posta göndermekten, bir konferans görüşmesi organize etmeniz veya özel bir forumda bir sohbet ortamı ayarlamanız muhtemelen daha yararlı olacaktır.
- Her 10 dakikada bir e-postalarınızı kontrol etmekten kaçınınız. Birçok insan e-postalarının kendilerini sürekli meşgul etmesine izin vermektedir.
- Genel prensip olarak, banka hesapları gibi hassas bilgilere e-postalarınızda asla yer vermeyiniz. Örneğin otel rezervasyonlarında olduğu gibi, çok nadir durumlarda bu tür bilgileri göndermeye ihtiyacınız olacaktır. Şüphe durumunda, işlemlerinizi dikkatle yapınız, kullanmak istediğiniz hizmetin çevrimiçi geçmişini kontrol ediniz, kartınızı ya da işlemi iptal etme süreçlerini inceleyiniz, PayPal gibi daha güvenli ödeme hizmetlerini kullanınız ve doğrudan para transfer hizmetleri (Western Union) gibi daha az güvenli hizmetlerden sakınız. Bununla birlikte, çevrimiçi hesaplarınıza ilişkin kullanıcı isimleriniz ve şifreleriniz gibi ayrıntıları e-postalarınızla sakın göndermeyiniz. Çevrimiçi hizmetler bu bilgileri sizden asla istemezler, bu nedenle, bu türden bilgileri isteyen bir e-posta aldığınızda, bu, mutlaka bir oltaama teşebbüsüdür.
- Çok karmaşık oltaama stratejileri, kullandığınız hizmetlerden (sosyal ağ siteleri) alınan mesajlara büyük ölçüde benzeyen ve kullanıcı adınızı ile şifrenizi isteyerek sizi yanlış bir web sitesine yönlendiren “sahte” bilgilendirme e-postalarını da içermektedir. Gönderenin e-posta adresini ve web sitesinin adresini olağan dışı görünen her şey için kontrol ettiğinizden emin olunuz.
- Aldığınız e-postalar için sağlıklı bir şüphecilik geliştirin. Kaynağına güvenmediğiniz e-postalarınızı açmayınız.
- Posta eklerine karşı özellikle tedbirli olunuz. Eğer göndericiden bir ek beklemiyorsanız veya başka bir nedenden dolayı güven duymuyorsanız, mesajı açmadan siliniz. Tanıdığınız birinden ve güvendiğiniz göndericilerden gelen ekler bile önce kaydedilmeli ve açılmadan önce taranmalıdır.
- E-posta istemcinizin önerdiği güvenlik önlemlerinin hepsini uygulayınız. E-posta hesabınızın heklenmesi durumunu dikkate alarak, e-posta sağlayıcıları sizin ikinci bir e-posta adresine erişiminize genellikle imkân tanımaktadır ve e-posta sağlayıcıları, istisnai durumlara karşı, ekstra güvenlik kontrolü amacıyla, cep telefonu numaranızı girmenizi giderek önermektedirler. Hesabınız onaylandığında, hesabınızın kurtarılmasını kolaylaştırmak amacıyla güvenlik ayarlarınızı uygun bir şekilde yapılandırınız.
- E-postalara ilişkin ek tavsiyeler için, “istenmeyen e-postalar, kötü amaçlı yazılımlar, dolandırıcılık ve güvenlik” konulu Kılavuz 19’a baktığınızdan emin olunuz.



Nasıl?

- E-postalarınıza bakmak için, ya akıllı telefonlarınızda, tabletlerinizde veya Windows 8 ve üstüyle çalışan bilgisayarosanızdaki e-posta hizmetinin “resmi” uygulamalarını (Gmail uygulaması, Outlook uygulaması veya Yahoo uygulaması) kullanabilirsiniz; bu durumda, e-posta hizmetinin web sitesine (bir “web posta” hizmeti kullanarak) gidebilirsiniz, ya da e-postalarınızı e-posta hizmetinizden indiren ve postalarınızı yönetmenize/organize etmenize imkân sağlayan harici bir uygulama olan bir e-posta istemcisini de kullanabilirsiniz. En çok kullanılan e-posta istemcileri, Thunderbird ve Outlook’tur. E-posta istemcileri, çoğunlukla mesleki e-postalar için kullanılmaktadır.

- İstenmeyen e-posta filtresi kurma hakkında daha fazla bilgi için “istenmeyen e-postalar, kötü amaçlı yazılımlar, dolandırıcılık ve güvenlik” konularına ilişkin Kılavuz 19’a bakınız.



Sınıf Çalışmaları için Fikirler

- E-posta adresine sahip büyük öğrencilerden kendi e-posta hizmetine bağlanmalarını ve kendi e-posta hesaplarını, ilave bir güvenlik sorusu, ikinci bir e-posta hesabı veya cep telefonu numarası ekleyerek daha güvenli hale getirmeleri için güvenlik ayarlarına bakmalarını isteyiniz.
- Gmail, Yahoo ve Outlook’da, e-posta hesabınızı güvenli hale getirmek için izlenecek prosedürler aşağıda verilmektedir.

► <<https://support.google.com/accounts/answer/46526?hl=en>>

► <<http://windows.microsoft.com/en-us/windows/outlook-security>>

► <https://help.yahoo.com/kb/SLN8292.html>

Yukarıdaki üç "büyük" e-posta sağlayıcısının dışında çok sayıda e-posta sağlayıcısı bulunmaktadır. Neden bu üçünde ısrar edilmektedir? Zira özellikle Gmail ve Outlook/Hotmail, diğer birçok hizmete bağlantı sağlamaktadır. Örneğin, Android bir akıllı telefonunuz varsa, bir "Google" hesabınızın olması mutlaka gerekecektir ve bir Outlook hesabı da, genellikle Windows işletim sisteminize bağlantı sağlayacaktır. Bu da, tercihlerinize bakılmaksızın, yukarıda belirtilen hizmetlerin birinde bir e-posta hesabı oluşturmaya sizi “zorlayacaktır”. Ancak, Web.de veya Protonmail.com gibi daha yüksek gizlilik standartlarına sahip e-posta istemcilerini kullanma hususunda da elbette özgürsünüz. İnternet servis sağlayıcınız genelde size bir e-posta hizmeti sunsa bile çevrimiçi diğer alternatifleri araştırmada özgür olunuz.

- Öğrencilerinizden üç kişilik veya daha büyük gruplar oluşturunuz ve hayali bir e-posta hesabı için daha güvenli şifreler hazırlamalarını isteyiniz. Kendi gerçek şifrelerini paylaşmamaları hususunu açık bir şekilde belirtiniz. 10 dakikalık bir beyin fırtınasından sonra, her gruptan, hazırladıkları şifreyi söylemelerini ve bu şifrenin neden güvenli olduğunu düşündüklerini açıklamalarını isteyiniz. Güçlü bir şifrenin özelliklerini (8 karakterden uzun olan; harf, sayı ve sembol karakterlerini içeren) ve zayıf şifrelerdeki ortak tehlikeleri (bir sözlükte bulunabilmesi; bir şekilde sizinle bağlantılı olması - köpek ismi, soy isim vb) tanımlamada onlara yardımcı olunuz.



Daha Fazla Bilgi İçin

. En çok bilinen e-posta istemcileri, Microsoft Outlook <https://products.office.com/en-us/outlook/email-and-calendar-software-microsoft-outlook> veya Mozilla Thunderbird’tür. <http://www.mozilla.org/projects/thunderbird/>

. “Gerçek veya Kurgu”, gönderilen e-postaların doğruluğunu kontrol etmeleri için internet kullanıcılarına yönelik bir web sitesidir; <http://www.truthorfiction.com/>. Benzer bir web sitesi de <http://m.snopes.com/whats-new/> dir.

. En popüler webposta sitelerinin üçü; Outlook <https://office.live.com/start/Outlook.aspx>, Yahoo! <https://mail.yahoo.com> ve Google’ın Gmail’i <http://www.gmail.com>. Özellikle ülkenizdeki alternatif e-posta sağlayıcılarını araştırmada özgür olunuz.

. BM Çocuk Hakları Sözleşmesinin ilgili maddeleri:

Madde 13 - Çocuklar, bir bilginin kendilerine veya başkalarına zarar vermemesi şartıyla, söz konusu bilgiyi edinme ve paylaşma hakkına sahiptir.

Madde 16 - Çocukların mahremiyet hakları vardır. Yasa, yaşam biçimlerine, isimlerine, ailelerine ve konutlarına karşı yapılan saldırılara karşı çocukları korumalıdır.

Kılavuz 7

Sohbet ve mesajlaşma medyası



■ "Sohbet", iletişim kurmaya tahsis edilmiş bir kanalda gerçekleştirilen etkileşimli iletişimi ifade eden genel bir terimdir. Kullanıcılar, sohbet odalarındaki insan gruplarıyla konuşabildikleri gibi özel mesajlaşma hizmetlerini kullanarak tercih edilen arkadaşlarla özel konuşmalar da yapabilirler.

■ Sohbet etme, yüz yüze görüşmelere benzeyen son derece gayri resmi bir iletişim aracıdır ve iki veya daha fazla insan arasında gerçekleşir. Sohbet konuşmaları genellikle yazılı şekilde yapılır ancak kulaklık ya da web kameraları kullanılarak ses ve görüntü de içerebilir. Bu iletişim şekli anlıktır ve bu özelliği nedeniyle de göndericiyle alıcının aynı anda hazır olmalarını gerektirmeyen e-postadan farklıdır.

Sohbet etme ve anlık mesajlaşma

■ Bu terimler birbirlerinin yerine kullanılmaktadır; ancak, bir kullanıcı, anlık mesajlaşma hizmetlerini kullanarak sohbet edebilirken anlık bir mesaj gönderme (AMG) bir sohbet değildir. Sohbet oldukça popülerdir ancak anlık mesajlaşma ve diğer mesajlaşma medyası türlerine karşı konumunu kaybediyor gözükmemektedir. Birçok şirket, görevlerini yaparlarken çalışanlarının gelen mesajlarla sürekli kesintiye uğramalarından kaynaklı üretim düşüklüğüne sebep olması nedeniyle çalışma ortamında AMG'ye rıza göstermemektedir.

1. https://simple.wikipedia.org/wiki/Chat_room
2. https://en.wikipedia.org/wiki/Instant_messaging
3. https://en.wikipedia.org/wiki/Streaming_media

Diğer mesajlaşma medyası türleri nelerdir?

WhatsApp, Kik, Viber, Telegram veya iMessage gibi mesajlaşma uygulamaları, akıllı telefon sahipleri tarafından artan şekilde kullanılmaktadır. Snapchat ve Wickr gibi otomatik silme uygulamaları da akıllı telefon sahipleri için popülerdir. Bu tür mesajlaşma medyası, genel anlamda daha özgürdür ve Facebook, Twitter veya LinkedIn gibi daha büyük platformlardaki mesajlaşma türlerine nazaran görünüşte daha fazla "mahremiyet" sağlar.

Akıllı telefonlardaki bu mesajlaşma uygulamalarıyla kullanıcılar, hızlı bir şekilde video çekmekte, yazı yazmakta, fotoğraf çekmekte ve sonuçlarını düşünmeden bunları gönderebilmektedirler. Bu nedenle de, çevrimiçi taciz ve zorbalık olaylarının artışı ne yazık ki önemli bir rol oynadıkları belirtilmektedir.

Anlık mesajlaşma ve diğer mesajlaşma medyası türlerindeki büyüme, akıllı telefonların yeni pazarlara girmesi nedeniyle şüphesiz artmaya devam edecektir. Facebook WhatsApp'ı ele geçirdi, Japon şirketi Rakuten Viber'i satın aldı ve diğer mesajlaşma uygulamalarının çoğuna ilgili taraflarca finansal yatırım gerçekleştirildi. Mesaj daha açık olamazdı: mesajlaşma medyası bir süre daha etrafımızda olacak.

Sohbet ve anlık mesajlaşmayı anlamının önemi

Sohbet ve anlık mesajlaşma popüler bir aktivitedir ve gençlerin birbirleriyle iletişim kurma şeklini değiştirmektedir. Sohbet etme ve anlık mesajlaşma, öğrencilerin kendi aralarında fikir alışverişinde bulunabilme ve ev ödevleri ile diğer akademik projeleri tartışabilme gibi olumlu yönde kullanılabilir; ancak, ne yazık ki, çevrimiçi olarak başkalarına karşı zorbalık ve taciz amacıyla da kullanılabilir (zorbalık ve taciz konularına ilişkin Kılavuz 21'e bakınız).

Öğretmenler, gençler için sohbetin ne kadar önemli olduğunu çoğunlukla hafife alırlar ve bu güçten yararlanıp onu bir eğitim aracı olarak kullanma fırsatını kaçırmırlar. Örnek aktiviteler şunlar olabilir:

- beyin fırtınası oturumları ve sorun odaklı gerçek zamanlı tartışmalar
- rol üstlenme oyunları ve simülasyonlar
- görüş alışverişleri ile tartışmalar ve küçük gruplarla panel oturumları
- dersler ve rehberlik
- grup araştırması
- çevrimiçi gruplar oluşturma.



ETİK DÜŞÜNCELER VE RİSKLER

- Bir sohbet yazı temelli olduğunda, sosyal semboller, jestler ve sözsüz iletişim, yazıyla karşı tarafa iletilmez ve çevrimiçi ortamda kolaylıkla yanlış anlamalar ortaya çıkabilir. Çevrimiçi ortamda kişiler, gerçek hayatta olduğu gibi uyumlu, nazik ve iyi huylu olmalıdırlar ve iyi bir netiquette (ağ etik kuralları) kullanım alışkanlığına sahip olmalıdırlar. Mizah ve duygular, yazıların yanında yer alan ve yüze benzeyen küçük semboller gibi duygu ikonlarıyla da ifade edilebilmektedir. Gençlerin çoğu, kısa yollar ve kısaltmalar kullanmaktadır; en yaygın kullanılanlara ilişkin bir sözlüğü linkte bulabilirsiniz. <http://www.netlingo.com/acronyms.php>.
- Web'de yabancılarla sohbet ederken, insanların her zaman söyledikleri kişi olmadıklarını hatırlamanız da çok önemlidir. Bir okulda veya sınıf ortamında konferans iletişim imkânı sağlayan kapalı grup sohbetleri, erişimin belirli bir kullanıcı grubuyla sınırlandırılması nedeniyle kullanımı daha güvenlidir.
- Sohbet etme veya anlık mesaj gönderimiyle harcanan zaman, değişik formlarda (metinler, anlık mesajlar, sohbetler, e-postalar vb.) her gün yüzlerce mesaj gönderen gençler arasında büyük bir artış göstermiştir. Bilgisayar klavyeleri ve bilgisayar farelerindeki kullanım kolaylıklarına ilişkin yaşanan gelişmeyle, "yazmaya dayalı tendon rahatsızlığı" gibi yeni sendromlar ortaya çıkmıştır. Akıllı telefonlar nispeten yeni cihazlardır ancak mesaj gönderme veya uzun e-postalar yazma, başparmakların aşırı kullanımına sebep olmaktadır. Bu nedenle, sohbeti ve yazıyı sınırlama, sadece bir yaşam dengesi meselesi değil aynı zamanda bir sağlık meselesidir.

4. https://en.wikipedia.org/wiki/Etiquette_in_technology#Netiquette

5. <https://en.wikipedia.org/wiki/Emoticon>

6. https://en.wikipedia.org/wiki/Collaborative_software

- Birçok anlık mesaj uygulaması "ücretsiz" görünse de, bir şirketin kendi işletme giderlerini bir şekilde karşılamak zorunda olduğunu hiçbir zaman unutmayın. Birçok uygulama, kullanıcıları "ücretsiz" bir uygulamayla cezbederek "yap-sat" stratejisi seçer ve sonra, kullanıcı sayısı yeterince büyüdüğünde kullanıcı tabanını başka bir şirkete satar. Aynı, Facebook tarafından satın alınan Whatsapp'ta olduğu gibi. Snapchat gibi diğer uygulamalar, önce kullanıcı tabanlarını oluşturmuşlar sonra da reklam almaya başlamışlardır. Kullandığınız anlık mesaj servisinin iş modeli hakkında her zaman bilinçli olun ve hassasiyetlerinizi (daha az mahremiyet, kişisel verileriniz üzerindeki kontrol, reklamlara maruz kalma, yıllık/aylık ücretler vb.) dikkate alarak akıllıca bir seçim yapın.
- İnsanlar, mesajlaşma ve sohbet yoluyla genellikle dosya alışverişinde bulunurlar ve bu dosyaların kötü amaçlı yazılımlar içerebileceğini hatırlamak çok önemlidir. Paylaşmadan önce tüm dosyaların virüs taramasından geçirildiğinden ve aldığınız bir dosyayı açmadan önce virüs taraması yaptığınızdan emin olun. (güvenlik konusuna ilişkin Kılavuz 19'a bakınız).
- Sohbet odalarını kullanırken gençlerin karşılaşabileceği riskler konusunda çok olumsuz bir algı oluşmuştur. Bazı medyatik ceza davaları nedeniyle, ebeveynler ve öğretmenler, sohbet odalarında, özellikle de çevrimiçi oyunlar yoluyla (oyunlar konusuna ilişkin Kılavuz 16'a bakınız), çocukların pedofillerle temas kurma ihtimaline karşı sıklıkla endişe duymaktadırlar. Her ne kadar bu tehlikeler var olsa da, bu korkuları bir bütünsellik içinde ele almak önemlidir. Sohbet odalarını kullananların çoğu söyledikleri kişilerdir ve buralardaki sohbetlerin çoğu bütünüyle masumdur. Korkuyu telkin etmek ya da sohbet kullanımını yasaklamaktansa, yetişkinler, nasıl güvende olunacağını öğretmek gençleri yetkinleştirmelidirler. Çocukların ve gençlerin uyması gereken bazı temel kurallar şunlardır:
 - ▶ Canlı bir moderatör eşliğinde yaş grubunuza uygun bir sohbet odası seçin ve olumsuz herhangi bir olayı moderatöre rapor edin.
 - ▶ Her iki cinsiyet için kullanılan bir kullanıcı adı seçin ve asla kişisel bilgilerinizi vermeyin veya fotoğraflarınızı yayınlamayın (mahremiyet konusuna ilişkin Kılavuz 9'a bakınız).
 - ▶ Bir sohbet odası arkadaşıyla gerçekten buluşacaksanız, bunu önce anne-babanızla paylaşın ve güvenilir bir yetişkinle beraber gidin. Çevrimiçi tanıştığınız biriyle yaptığınız ilk fiziki buluşmada, mutlaka, şehir meydanı gibi halka açık yerleri seçin.
 - ▶ Bir sohbet oturumu sırasında sizi rahatsız eden bir şeyle karşılaştığınızda bunu bir yetişkine söyleyin. Bir sohbet odasında veya internette herhangi bir yerde bir sorunla karşılaşırsanız, bu hususu, ulusal yardım hattınızdaki deneyimli danışmanlarla her zaman konuşun.
 - ▶ Bildiğiniz insanlarla sohbet etmek istediğinizde, bir sohbet odasını kullanmaktansa, iletişim listenizi kontrol edebilmek amacıyla anlık mesajlaşma hizmetlerini (örneğin, MSN, Skype) kullanın.

NASIL?



- Web'de ücretsiz çeşitli sohbet programları mevcuttur. Bir arama motorunda "sohbet" araması yaparak, birçoğunu bulabilirsiniz. Yahoo Chat, ICQ ve AOL Chat gibi web-temelli birçok sohbet programı, gerçek-zamanlı tartışma gruplarının olduğu çok çeşitli sohbet odalarına erişim imkânı sağlar. Kullanıcılar, öncelikle, sohbete erişim sağlamak için küçük bir uygulama indirirler ve moderatörle kayıtlarını yaparlar; daha sonra, özgürce giriş yapar ve katılım sağlayabilirler.
- Seçili kullanıcılar ile özel görüşmelere imkân sağlayan anlık mesajlaşma uygulamaları, popülerlikte sohbet odalarını artık geçmektedir. Herhangi bir arama motorunda "anlık mesajlaşma" araması yaparak bu özellikteki uygulamaları bulabilirsiniz. Kullanıcılar anında mesajlaşmayı etkinleştirmek için bir uygulama indirirler ve sohbet etmek istedikleri kişilerin listesini düzenlerler. Zira, buradaki iletişim, kısıtlı bir kullanıcı grubuyla gerçekleştirilir; bu nedenle, anlık mesajlaşma, sohbet odalarındaki sohbete göre "daha güvenli" olarak sıklıkla değerlendirilmektedir.

7. www.betterinternetforkids.eu/web/portal/practice/helplines

8. https://en.wikipedia.org/wiki/Web_search_engine

9. <http://chat.yahoo.com>

10. <http://www.icq.com/>

11. <http://lifestream.aol.com>

12. https://en.wikipedia.org/wiki/Instant_messaging

Bir sohbet odası nasıl kullanılır?

- Kullanmayı seçtiğiniz sohbet programını açın.
- Gerekliyse, bir kullanıcı adı ve parola belirleyin.
- Moderatörlüğü insanlar tarafından yapılan uygun bir sohbet odası seçin. Genellikle farklı amaç ve konulara (örneğin otomotiv ilgi grupları, belirli konulardaki çalışma grupları, öğretmen sohbetleri vb.) yönelik odalar vardır.
- Giriş yaptıktan sonra, ana metin ekranında katılımcıların konuşmalarının kaydırıldığını göreceksiniz.
- Mesajınızı yazın ve katılımcıların mesajınızı görebilmesi için "başlat"a basın veya "gönder"i tıklayın.
- Belli birine mesaj göndermek istiyorsanız, ilgili penceredeki katılımcı listesinden bir kişi seçin.
- Birçok sohbet odası, bire bir dosya alışverişi için de kullanılabilir. Sohbet odaları, e-posta ile gönderilemeyecek kadar büyük dosyaların iletimine de imkân sağlar.
- İstenmeyen kullanıcıları yanlışlıkla sohbet odanıza eklememeniz için ayarlarınızı sürekli kontrol edin.

Anında mesajlaşma nasıl kullanılır?

- Anlık mesajlaşma uygulamanızı açın.
- İnternette kimin çevrimiçi olduğunu ve sohbete açık olduğunu öğrenmek için kişi listenizi kontrol edin.
- E-posta adreslerini girerek ve onları kişi listenize katılmaya davet ederek yeni kişiler ekleyebilirsiniz. Bu kişiler, bir e-posta daveti alacaklar ve kabul ederlerse listenize kayıt olacaklardır. Bu durum, her ikinizin de çevrimiçi olduğu durumlarda bu kişilerle gerçek zamanlı sohbet etmenize olanak sağlayacaktır.
- Mesaj göndermek ve iletişim kurmak için seçilen kişinin kimliğini tıklayın.
- Mesajınızı yazın ve katılımcıların mesajınızı görebilmesi için "başlat"a basın veya "gönder"i tıklayın. Bilinmeyen kullanıcılar ile iletişime geçmemek veya tanımadığınız kişilerden gelen e-posta veya anlık mesaja cevap vermemek en iyisi olur.
- İstenmeyen kullanıcıları yanlışlıkla anlık mesajlaşmanıza eklememeniz için ayarlarınızı sürekli kontrol edin.



SINIF ÇALIŞMALARI İÇİN ÖNERİLER

- . Bir konu seçin ve bir sohbet uygulamasında öğrencilerden birbirlerine soru sormalarını ve bilgi alış verişinde bulunmalarını isteyin.
- . Çalışma konusuna karar verin. Öğrencilerin ders öncesi etkinlikleri yapmalarına yardımcı olacak materyalleri toplayın. Verilen ödevlerde öğrencilerin çiftler veya küçük gruplar halinde çalışmalarını sağlayın. Bu çalışma aşaması, bir grup çalışması modeline uygun olarak düzenlenmelidir. (küçük grup etkileşimleri için en iyi sohbet çalışmaları, yani, 2-6 öğrenci).
- . Projenin sonunda öğrenciler, bir sohbet oturumu için uygun sunumlar hazırlarlar. Sohbet, farklı çalışma konuları hakkında küçük-grup sunumlarıyla başlar. Çalışma toplulukları, bu derste öğrendiklerini birlikte açıklarlar.
- . Sohbet oturumları gerçek hayatta yapılan sohbetleri modellediğinden bu ortam öğrencilere gerçek bir etkileşim fırsatı sunar ve bu nedenle, yabancı dil öğreniminde çok faydalıdır. Öğretmen öğrencilerine kısa mesajlar göndermelerini tavsiye ederek tartışmaya katılmaları için onları teşvik edebilir. Buradaki etkileşim, öğrenciler için roller yaratarak geliştirilebilir; biri yenilikçi, diğeri eleştirmen olabilir. Diğer öğrenciler tartışmaları takip edip daha sonra geri bildirimde bulunabilirler.
- . Çevrimiçi Çevre (ENO), web tabanlı uluslararası bir çevre eğitim projesidir. Kurs başında öğrenciler, konularını projenin web sayfalarından alırlar. Öğrenciler, bilimsel ve deneysel çevresel verileri toplar, farklı olayları ölçümler veya fotoğraf çekerler.

13. <https://en.wikipedia.org/wiki/Peer-to-peer>

14. <https://en.wikipedia.org/wiki/Email>

15. https://en.wikipedia.org/wiki/Instant_messaging

- Her bir ünite işlenirken, etkileşimli ve eşzamanlı gerçek-zamanlı sohbetler, elektronik anketler ve mesaj panoları şeklinde sanal dersler düzenlenir. Ders etkinliklerinin öncesinde ve sonrasında öğrenciler, görüşlerini paylaşırlar, sohbet ederek görevlerini takip ederler ve öğrendiklerini anlatırlar.



UYGUN KULLANIM

Sohbetlerde kullanılan dil, parçalı, grupsal ve karşılıklıdır; bir sohbet katılımcısı, yalnızca hızlı değil, bir konudan ve hatta bir tartışmadan diğerine geçebilecek kadar esnek olmalıdır. Öğretmenin destekleyici rolü, içeriğin kalitesini ve sohbete katkıda bulunan herkesin dengeli katılımlarını temin etmede çok önemlidir. Öğrenciler yaşça ne kadar küçükse, öğretmen kontrolünde ve moderatörlüğünde yapılan sohbet o kadar önemlidir.

Tüm sohbet oturumu süresince tartışmaları etkin bir şekilde takip edin.

- . Oturum programını önceden belirleyin; herkes aynı anda hazır olmalıdır.
- . Ağ etik kurallarına uyun; sanki yüz yüzeymiş gibi kibar, nazik ve saygılı olun.
- . Niyetiniz bu olmasa da, dikkatsizce yazılmış bir mesajın incitici olabileceğini unutmayın.
- . Kısa bir mesaj her zaman daha iyidir. Diğerlerinin okumak ve cevaplamak zorunda olduğu önceki yazışma parçalarını ekleyerek gerçek zamanlı bir sohbet oturumunu tekelinize almayın.
- . Sohbet stili, bir bilinç akış stiline yakındır. Söylemek istediklerini anlayabilmek için diğerlerinin mesajlarını dikkatlice okuyun. Bu, boşluk doldurmayı da içerebilir.
- . Kullanıcı adınızı ve şifrenizi paylaşmamayı unutmayın. Sohbet veya anlık mesajlaşmalarda tüm kişisel bilgilerinizi kişisel olarak koruyun. Ekran görüntüleri bilgilerinizi (veya yorumlarınızı) her zaman alınabilir ve başkalarıyla paylaşılabilir.



DAHA FAZLA BİLGİ İÇİN

- . Okul öğretmenlerine yönelik bazı fikirler şu adreste bulunabilir:
http://www.educationworld.com/a_tech/chat-room-get-new-life-in-classrooms.shtml
- . fSohbet, Fransızca bir sohbet odasıdır: <http://www.tchat-orange.fr/index.php>
- . "Sosyal bir araç olarak oda içi sohbet" hakkında bilgi şu adresten bulunabilir:
<http://www.openp2p.com/lpt/a/3071>
- . Temel duygu ikonları listesi için Wikipedia'ya bakınız:
https://en.wikipedia.org/wiki/Emoticon#Basic_examples
- . Pew Araştırma Merkezi mobil mesajlaşma ve sosyal medya hakkında çalışmalar yapmıştır:
<http://web.archive.org/web/20160703022409/http://www.pewinternet.org/2015/08/19/mobile-messaging-and-social-Medya-2015/>
- . "Snapchat nedir ve neden çocuklar sever ve ebeveynler korkar?":
<http://web.archive.org/web/20160619055301/http://www.forbes.com/sites/larrymaggid/2013/05/01/what-is-snapchatand-why-do-kids-love-it-and-parents-fear-it/#65fc2b447875>
- . Danimarka'da, savunmasız gençlere yardımcı olmayı ve toplumsal katılımlarının artmasını teşvik etmeyi amaçlayan Cyberhus, "grup sohbeti" kullanan değerli bir platformdur:
<http://cfdp.dk/2015-cyberhus-chat-counselling-last-year/>

16. <http://www.netlingo.com/word/real-time-chat.php>

17. http://en.wikipedia.org/wiki/Internet_forum

Kılavuz 8

Sosyal Ağ İletişimi ve Sosyal Paylaşım



Bir sosyal ağ hizmeti ya da sosyal ağ iletişim sitesi (SNS)¹ aynı çıkarları veya faaliyetleri paylaşan insanlar arasında sosyal ağlar oluşturmak için kullanılan bir platformdur. Web'e dayalı bu sistem, kullanıcıların birbiriyle sohbet etmesi, mesajlaşması, e-posta iletimi, görüntülü ve sesli sohbet etmesi, dosya paylaşması, bloglaşması ve tartışma grupları kurması, vb. gibi etkileşimlerde bulunması için çeşitli yollar sağlamaktadır.

■ Sosyal ağlar, önemli kişisel veri, ilgi alanları, ağ arkadaşları ve benzeri bilgiler içeren kişisel verilere ilişkili bilgilere dayalıdır. Sosyal ağ iletişim siteleri, ilgi alanları ve faaliyetleri paylaşan ya da başkalarının ilgi alanlarını ve faaliyetlerini araştırmaya ilgi duyan insan topluluklarını bir araya getirmektedir. Bu siteler kullanıcılarının bu faaliyetleri yapması için farklı yazılım² türleri sağlamaktadır.

■ Sosyal ağ iletişim siteleri insanların birbirleriyle bağlanmasına imkân sağlamakta (genelde her ağ üyesi için kendi tanıtım sayfalarıyla) ve kullanıcıları birbirine bağlamak için güven üzerine bina edilmiş tavsiye verici sistemler sunmaktadır. Bazı siteler, kullanıcıları belli özelliklerine göre ayırmış kategoriler içermektedir (eski sınıf arkadaşları gibi).

■ Sosyal paylaşım, sosyal bir medya sitesi veya uygulamasına³ ilişkin bir web-sitesinden kullanıcılara içerik paylaşımları için izin vermektedir.

1. https://en.wikipedia.org/wiki/Social_networking_service

2. https://en.wikipedia.org/wiki/Social_software

3. www.oxforddictionaries.com/definition/english/social-sharing

■ Popüler küresel sosyal ağ iletişim siteleri ve uygulamaları şunları kapsar: Twitter, Facebook, LinkedIn, Google+, Snapchat, Tumblr, Pinterest, Vine and Whatsapp.

■ Avrupa'da yerleşik siteler ve uygulamaları şunları kapsar: Badoo, Bebo, V Kontakte or VK (Rusya), Delphi, Draugi-em.lv (Latviya), iWiW (Macaristan), Nasza-Klasa (Polonya), Soup (Avusturya), İsviçre'de Glocals, Skyrock, The Sphere, StudiVZ (Almanya), Tagged, Tuenti (çoğunlukla İspanya'da) ve daha niceleri...

■ Sosyal ağlar, insan hakları ve temel özgürlüklerin değiş tokuşu açısından eşit biçimde önemlidir ve toplumun büyük çoğunluğuna gerekli bilgileri sağlayabilirler.

■ Sosyal ağların çoğunda hayat deneyimleri yer almaktadır, ancak şu topluluklar da mevcuttur:

- satın almayı ve satış yapmayı kolay hale getiren, emlak ve oda kiralama vb. işlem toplulukları,
- sinemalar, sağlık vb. gibi genel olarak özel bir konuya odaklanan ilgi alanı toplulukları,
- "Savaş Uçağı Dünyası" ve "İkinci hayat" gibi hayali ortamlara ve oyun-oynamaya dayalı fantezi toplulukları,
- Kullanıcıları etkileyen konularda insan hakları ve/veya eylem toplulukları,
- Engellilere, özel gereksinimlere ihtiyaç duyanlara ve diğer zorluklarla karşı karşıya kalanlara yönelik destek ve tavsiye toplulukları,
- Sosyal ağların çoğu, kişisel veri mahremiyetini yönetmek için kolay özellikler de sunmaktadır (Bkz. mahremiyet ayarları konusunda Kılavuz 9). Bu gereçler, kullanıcıların kişisel bilgilerinin bazılarını sadece arkadaşlarının veya sadece güvenilir belli grup üyelerinin erişimine açma yoluyla kısıtlama imkânı vermektedir. Bu gereçler, rastgele araştırmalarla kendilerine erişilmesini ve diğer üyelerce kendi içeriklerinin işaretlenme imkanını kısıtlamayı da üyelerine tanımaktadır.

EĞİTİMDEKİ ÖNEMİ

- Sosyal ağ iletişimi ve sosyal paylaşım ucuz olup kişisel bilgidan pazarlama bilgisine kadar uzanan birçok içeriğin paylaşılmasının hızlı bir yoludur.
- Sosyal ağ iletişimi, insanların irtibatını kaybettiği veya uzak mesafede yaşayan aile ve arkadaşlarıyla, temasta kalmasına veya yeniden temas kurmasına imkan tanır.
- Sosyal ağ siteleri önemli olayların organizasyonuna da imkân sağlamaktadır. Mücevher gösterisinden çocuk partisine kadar uzanan bazı olaylar masum olabilirken, bazılarıysa ırkçı/yabancı/eşcinsel düşmanlığı veya diğer aşırılıklar ve küçük düşürme eylemleri gibi saçma parti veya gösteriler yapma yoluyla zarar verebilmektedir.
- Birçok endüstri sosyal ağ iletişiminin ve markalaşmanın önemini görmekte ve sosyal ağ iletişimi aracılığıyla satışla sonlanabilen tavsiyeler alma amacı gütmektedir.
- Akıllı telefonlardaki websiteleri ve uygulamalar aracılığıyla yapılan sosyal paylaşımın kolaylığı sebebiyle çoğu genç insan fazla araştırma yapmaksızın anlamlı anlamsız herşeyi paylaşmaktadır.
- Potansiyel işverenler, kolejler veya üniversiteler, hatta, aile ve arkadaşlar, her bilgiye erişim sağlayabildiği için sorumlu sosyal ağ iletişimi son derece önemlidir.
- Sorumlu sosyal ağ iletişimi, sosyal bir fayda ya da tanınma (genç bir insanın son zamanlarda kazandığı bir ödül veya sertifika hakkında bilgi göndermesi) amacıyla hızla yayılan bir içerik oluşturarak öz-tanıtım (genç bir kişinin bir toplum hizmeti için herhangi bir kampanya yürütmesi) yapmaya yönelik ucuz bir yöntem olarak görülmektedir.
- Sosyal ağ iletişim siteleri, yanlış veya taraflı görüşlere dayalı bilgi tanıtımı için kullanılabilir. Bu da kullanıcılar açısından "arkadaş" seçmede ve içeriğin güvenilir olduğunu kontrol etmede fazladan itinalı olmalarını gerektirmektedir.

ETİK DEĞERLENDİRMELER VE RİSKLERİ

■ AISK İnsanlar sosyal ağ iletişim sitelerini kullanırlarken sıklıkla kendilerini daha özgür hissettiklerinden bahsetmektedirler. İnsanlar, normalde yüz yüze konuşurken sakınacağı şeyleri birilerine söyleyerek ve yorumlar yaparak kendilerini yetkili ve bazen de yenilmez olarak görmektedirler. Sanal dünyada duyguları abartmanın veya biriyle yüz yüze iletişim halindeyken söylemeyeceğiniz özel şeyleri söylemenin kolay olması gerçeği nedeniyle bu durum daha da çığırından çıkmış bir hale gelmiştir.



■ Sosyal ağ siteleri, kullanıcılarının diğer insanların kişisel bilgileri hakkında yorumlarda bulunmasına imkân tanımaktadır. Bu tür yorumların türü ve doğasına dikkat edilmesi gerekmektedir.

■ Birleşik Krallığın Get Safe Online⁴ adlı kurumunun da belirttiği üzere, sosyal ağ iletişim siteleri kullanmanın bazı riskleri vardır. Bunlar şunlardır:

- Sizin veya arkadaşlarınız/temaslarınızın sebep olduğu mahrem bilgilerin ifşası,
- Kabadayılık etme;
- Siber-tehditçilik;
- Yaşa uygun olmayan içeriğe erişim,
- Çevrimiçinde çocuklara yönelik cinsel amaçlı arkadaşlık ve çocuk istismarı,
- Doğasında şiddet, cinsellik, aşırılık ve ırkçılık veya saldırgan faaliyetler ve nefret dolu tutumlar barındıran yorumlarla karşılaşma,
- Sizi ikna veya taciz yoluyla temel inançlarınızı veya ideolojinizi değiştirmeye ya da aşırı bir ucu benimsetmeye çalışan insanlar,
- Saldırgan veya uygun olmayan yorumları göndermekten dolayı kovuşturmalara ve karşılıklı suçlamalarla karşılaşma,
- Gerçekte sizin dolandırıcı veya uygun olmayan web-sitelerini ziyaret etmeniz için cesaretlendiren ancak sosyal ağ iletişim sitelerinden gönderildiği iddia edilen kimlik avına yönelik e-postalar,
- Sizi dolandırıcı veya uygun olmayan web-sitelerine bağlanmanızı cesaretlendiren ve arkadaşlarınızdan, şirketlerden ve başkalarından gelmiş gibi görünen e-postalar,
- Hesabınızı veya sayfanızı hekleyen ya da ele geçiren insanlar,
- Mesaj ekleri veya fotoğraflar içinde bulunan virüsler ve casus yazılımlar,
- Siz ya da bir aile bireyinin tatilde olduğunu veya tatile çıkacağını e-posta yoluyla bildirmesi ve bu sebeple de evinizin boş olacağını ilan edilmesi ve bunun da evinizin soyulmasına yol açması... Eğer böyle bir şey yaparsanız ve evden uzaktayken evinizin soyulması sebebiyle tazminat talep ettiğinizde sigorta şirketiniz tazminatınızı bu sebepten dolayı pek tabii ki ödemeyebilir⁵.

■ Ancak aşağıdaki gibi başka riskler de vardır:

- Ticari içeriğe maruz kalma ve size ait mahrem verinin ticari amaçlar için kötüye kullanımı,
- Çevrimiçi itibarınıza kalıcı zarar gelmesi, bu da sizin iş bulmanızda zorluklara yol açabilir veya mali dışlanma (borç alma ve sigortadan tazminat almada yetersizlikler) gibi çeşitli başka ayrımcılıklara maruz kalabilirsiniz,
- Kişisel gelişiminizi ve evrilmenizi sınırlayabilecek inançlarınız/bilginiz/görüşleriniz doğrultusunda tek taraflı içeriğe maruz bırakılmanız;
- Mükemmel görünme, ilginç ve mutlu bir hayata sahip olma ve sürekli olarak etkileyici /hoş şeyler gönderme gibi aşırı sosyal baskıya tabi tutulabilirsiniz,

■ Çevrimiçi teknolojilere gelince, gençleri teknoloji kullanmaktan men etmek çözüm değildir. Genç insanların çevrimiçindeyken güvenle ve gözetilerek hareket etmeleri, yaş sınırlamalarına riayet etmeleri, kişisel bilgilerini mahrem tutmaları ve sorumlu yayıncılar olmaları için cesaretlendirilmeleri gerekmektedir.

■ Sorumlu yetişkinler, sosyal ağ iletişim sitelerini kullanmayı bırakmaya çalışmaktan çok, güvenli kullanım açısından karşılaşılabilecek tehlikeler ve iyi uygulamalar konusunda kendilerini eğitmelidirler. Tüm bu şeyler, doğal olarak çevrimdışı dünyada yapılacaktır – öyle ise niye çevrimiçi dünyada da olmasın?

4. <https://www.getsafeonline.org/social-networking/social-networking-sites/>

5. www.getsafeonline.org/social-networking/social-networking-sites/

Gençlerin, ebeveynleri ve öğretmenleri gibi güven duydukları yetişkinlerle çevrimiçi deneyimleri hakkında konuşmaya cesaretlendirilmeleri gerekmektedir. Tüm diğer internet güvenliği konularının yanı sıra, gençlerin çevrimiçi davranışları üzerindeki en büyük yegâne olumlu etki, ebeveynlerinin ve öğretmenlerinin onların çevrimiçi hayatlarına faal katılımlarıyla ortaya çıkmıştır.

Bunun yetişkinler üzerinde de olumlu bir etkisi olmaktadır, çünkü bu sayede yetişkinler sosyal ağ sitelerinin olumlu özelliklerini öğrenmektedirler.



SINIF ÇALIŞMASI İÇİN FİKİRLER

- Öğrencilerinizden çevrimiçi profillerinde yayınlamayı kabul etmeyi düşündükleri bilgi türlerini incelemelerini isteyin. Bir listeyle size geldiklerinde, kâğıt üzerinde bir profil oluşturmalarını isteyin. Oluşturdukları bu profillerin okuldaki tüm ebeveynlere gönderilmesinden mutlu olacaklar mı? Birçok durumda, öğrenciler bunun olmasını istemeyeceklerdir. Ancak, kişiye özel şekilde ayarlanmadıkça herkesin herhangi bir sosyal ağ iletişim sitesinde yer alan profillere bakabileceği kendilerine hatırlatılmalıdır. Gerçek dünya ile sanal dünya arasındaki bu bağı kurmak önemlidir, çünkü bu bağ çocuklar ve gençlerin çevrimiçi gönderim sonuçlarının farkına varmalarına yardımcı olur.
- Sınıfta iki ya da üç sosyal ağ iletişim sitesine bakınız ve öğrencilerinizden görebilecekleri herhangi riskli bir davranışı bulmalarını isteyiniz. Kullanıcıları riske atmakta olanın neler olduğunu tartışınız. Daha sonra da buldukları riskli noktalar ışığında kendi çevrimiçi faaliyetlerini gözden geçirmelerini isteyiniz.
- Öğrencilerinizi gruplara ayırarak bir sosyal ağ iletişim sitesinde çevrimiçi materyal yayınlamakta olduklarında dikkat edecekleri riskli noktaları içeren kendi kontrol listelerini oluşturmalarını öğrencilerinizden isteyin. Listeleri karşılaştırın ve öğrencilerin çıktısını alacakları ve bilgisayarının yanındaki duvara asmak üzere eve götürecekleri tek bir kontrol listesi haline getirin.
- Öğrencilerinizin sınıfa herhangi bir sosyal ağ iletişim sitesine yüklemek isteyecekleri sayısal fotoğraflar getirmelerini sağlayın. Küçük gruplar halinde çalışarak hangi mahrem bilginin ifşa edilmekte olduğunu saptamak için her fotoğrafı inceleyin. 1 ile 5 arası bir ölçekte her fotoğrafa bir "güvenlik notu" verin; kullanıcının mahremiyetini mükemmel şekilde koruyan fotoğrafa 5 verin.
- Bu sosyal ağ teknolojilerinin sınıf içinde nasıl kullanılacağı hakkında daha fazla öneriler getirmek için bkz. "Web 2.0, 3.0 ve dahası" başlıklı Kılavuz 3.
- Aşırılıkçı içeriğin ne olduğu ve davranış üzerinde ne etki yapabildiği konusunda bir tartışma açmak için çocuklarınız veya öğrencileriniz için uygun malzeme hazırlayın. Aşırıcılığa nasıl karşı konulacağına dair fikirler oluşturmak için onlarla beraber çalışın. Şiddet aşırılığına ve radikaleşmeye karşı Avrupa Konseyi eylem planı öğrencileri bilgilendirmede ve fikirleri tetiklemede faydalı olacaktır.
- Öğrencilerinizle Genel Veri Koruma Düzenlemesine bakınız ve Avrupa Birliği'nin belli bir yaşın altındaki çocukların sosyal ağ iletişimine erişimlerini kısıtlama isteğinin nedenlerini tartışın. Bu yaş, kaç olmalıdır?



7. İYİ UYGULAMALAR

- E-posta yoluyla gönderdiğiniz kişisel bilgiye herkes erişebilir – temel kural, aksinden emin olmadıkça, her şeyin kamuya açık olduğunu var saymaktır. Sonuç itibarıyla, çevrimdışı kamuya yayınlamakta istekli olmayacağınız hiçbir şeyi bir sosyal site üzerinde açıklamamanız gerekir. Profilinizde yapacağınız özel ayarlamaları tercih etmeniz, bu bilgileri her zaman sadece arkadaşlarınızın göreceği anlamına gelmez. Bazı hallerde, profilinize yerleştirdiğiniz her bilginin herkes tarafından halen görülebileceği anlamına gelir, fakat sadece "arkadaşlarınız" size yorum veya hızlı mesaj (IM – Instant Messaging) gönderebilir. Büyük gruplara veya ağlara (Örneğin, ülke veya şehir ağlarına) katılmanız halinde, çok büyük sayıda kişinin profilinize erişmesinin mümkün olabileceğinin farkında olmanız da gerekir.

6. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3576

7. http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf

- İlgüdülerinize güvenin – içgüdüünüz birşeylerin doğru olmadığını hissediyorsa haklı olabilir. Hoşlanmadığınız veya sizi rahatsız hissettiren bir şeyle çevrimiçinde karşılaştığınızda bilgisayarınızı kapatın ve güvendiğiniz bir arkadaşına durumu anlatın.
- Kişisel bilgileriniz konusunda dikkatli olun. Sorun; kişinin, kişisel bilgisini internete gönderir göndermez bu bilgiye kimin bakacağı ve bu bilginin nasıl kullanılacağı konusundaki denetimini kaybetmiş olmasıdır. Resimler kolayca kopyalanabilmekte ve bir düğmeye basılmasıyla binlerce kişiyle paylaşılabilir. Fotoğrafların sayısal doğası sebebiyle hem değiştirilebilmekte hem de üzerinde oynanabilmektedir. Herhangi bir isimle eşleştirilmemiş olsa bile resimler, yeni arama yazılımları yoluyla insanları teşhis etmek için de kullanılabilir. Hepimizin sadece, ebeveynler ve öğretmenler de dâhil olmak üzere, herkesin görmesinden mutlu olacağı resimleri göndermeyi öğrenmemize ihtiyacımız bulunmaktadır.
- Çevrimiçindeki hiçbir şey, görüldüğü gibi değildir. Aynı okuldan olan öğrencileri bir araya getirdiğini iddia eden belli siteler gerçekte hiçbir anlam ifade etmez. Kullanıcılar bu sitelere kaydolarak sağladıkları bilgiler kontrol edilmemektedir. Herhangi biri bir kullanıcı profili yaratabilmekte ve başka biriymiş gibi davranabilmektedir. Dahası herkes, gerçek veya uydurduğu yaşı ne olursa olsun, istediği kadar çok sayıdaki okul topluluklarına katılabilir.
- Dengede tutun – eğer sosyal medya sizin için bir takıntı haline gelirse ve profilinizi kontrol etmeden/güncellemeden, resim yollamadan ve “beğen” sayılarına bakmaktan duramıyorsanız, “sosyal medya zamanınıza” bir süre ara verebilir veya en azından sosyal ağ iletişim sitelerinde harcadığınız zamanınızı denetim altına alabilirsiniz.
- Güvenli kullanım için sosyal ağ iletişim sağlayıcılarının sitelerinde sağladıkları rehber ilkelere ilişkin materyalleri gözden geçirin.
- Çevrimiçinde gönderdiğiniz malzemeyi dikkatli şekilde ölçüp biçiniz – unutmayın ki herhangi bir şeyi bir kez gönderdiğinizde onu tamamen internetten silebilmeniz artık mümkün olamayacaktır.
- Özellikle görüntü gönderirken dikkatli olun. Görüntüyle beraber isminizi göndermeseniz bile o görüntü sizin teşhis edilmenizi sağlar ve web belleklerinde siz onu kaldırdıktan uzun bir süre sonra bile mevcut kalmaya devam edebilmektedir.
- Kişisel bilgilerinizi koruyun, özellikle de sizin kimliğinizi belirten ve konumuzu gösteren bilgiyi...
- Başkalarına asla saldırgan, karalayıcı ve küçük düşürücü hiçbir şey göndermeyin.
- Profilinizin kamuya açık veya kişiye özel şeklinde ayarlanabildiğini hatırlayın. Hangisinin en uygun kullanım ayarı olduğunu dikkatli şekilde düşünün.
- Sosyal ağ iletişim sitelerinin önerdiği mahremiyet özelliklerinden yararlanın. Kimlik bilgilerinizi kamunun görüşüne açmadan önce dikkatlice düşünün.
- Profilinizin kamuya açıksa, herkes tarafından görülebileceğini hatırlayın. Kamuya açık olmasa bile üyesi olduğunuz ağlardaki herkes tarafından görülebilmektedir. Sosyal ağ iletişim siteleri siyasalarını değiştirebildiklerinden dolayı arada sırada ayarlarınızın doğruluğunu denetlemeniz iyi bir fikirdir.
- Nefret kampanyaları, zorbalık veya ırkçı, yabancı düşmanlığı, eşcinsellik karşıtı veya diğer aşırılık içeren mesajları alma gibi sorunlar yaşıyorsanız, anlayamayacaklarını veya onaylayamayacaklarını düşünseniz bile güvendiğiniz birilerinden her zaman yardım talep edin.
- Profilinizde irtibat bilgilerinizi asla vermeyiniz.
- Çevrimiçi gönderdiğiniz içeriklerin birçok amaç için kullanılabileceğini hatırlayınız. Örneğin, size özel reklamlar, hangi işe uygun olduğunuza dair veya siyasi amaçlı mesajlar vb.
- Farklı cihazlardan sosyal ağ iletişim sitelerine eriştiğinizde, bu siteler akıllı telefonunuzdaki, tabletinizdeki veya bilgisayarınızdaki bilgilerinize erişim için izin talebinde bulunabileceğinden ayarlarınızı denetleyin.



DAHA FAZLA BİLGİ İÇİN

- Sosyal ağlar konusunda daha fazla bilgi için, bkz. “2015 yılındaki dünyanın en önemli 21 sosyal medya sitesi ve uygulamaları”:
<<http://web.archive.org/web/20160423200413/http://www.socialmediatoday.com/social-networks/2015-04-13/worlds-21-most-important-social-media-sites-and-apps-2015>>.
- Tavsiye için “Güvenli sosyal ağ iletişimi”ne bkz.:
<http://web.archive.org/web/20120602054510/http://www.getsafeonline.org/nqcontent.cfm?a_id=1459>.
- Sosyal ağ iletişim sitelerinin kullanımı ve güvenli kalmada ipuçları konusundaki bilgi şu adreste bulunabilir: <www.privacyrights.org/social-networking-privacy>.
- Onlu yaşlardakilerin sosyal ağları kullanması konusunda Sosyal Bilim Araştırma Ağı'nın bir raporu şu adrestedir:
<http://web.archive.org/web/20160703112245/http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128>.
- PEW Araştırma Merkezi, onlu yaşlar, teknoloji ve arkadaşlık konusunda bir inceleme yayımlamıştır:
<<http://web.archive.org/web/20160710143035/http://www.pewinternet.org/2015/08/06/teens-technology-and-friendships/>>.
- İlgili Avrupa Konseyi belgeleri: Avrupa Konseyi Bakanlar Komitesi'nin “Sosyal Ağ İletişim Hizmetleri Bağlamında İnsan Haklarının Korunması” konusundaki CM/Rec(2012)4 Sayılı Tavsiye Kararı: <<https://wcd.coe.int/ViewDoc.jsp?id=1929453>>.

Mahremiyet ve mahremiyet ayarları



Mahremiyet, kişinin kişisel bilgisini kullanma ve bu bilgiye erişmesi üzerinde sahip olduğu denetim düzeyini ifade eder. E-posta ve internet kullanıcılarının çoğu, kişisel bilginin izinsiz kullanılmayacağını ve söz konusu bilgi değişimlerinin özel ve güvenli olduğunu varsaymaktadır. Ancak, gerçek çok farklıdır.

Herhangi bir web-sitesine her eriştiğinizde, sosyal medya konusunda içerik gönderdiğinizde veya e-posta yolladığınızda kendinize ait fiziki ve bilgisayar adresinizi, telefon ve kredi kartı numaralarınızı, tüketici tarzı verinizi ve daha birçok bilgiyi de peşinizde bırakırsınız.

Veriniz bir kez orada olduğunda üzerindeki denetiminizi sürdürmede zorluk çekebileceğinizi ve bunun uzun vadeli sonuçları olabileceğini de hatırlamalısınız.

Çevrimiçi alış-veriş ve reklamcılık dâhil e-ticaret genelde benimsenen bir iş yürütme şekli olması sebebiyle hassas verinin, haberleşmelerin ve tercihlerin korunmasına özel önem verilmelidir.

■ İnternette çocuklar tarafından oluşturulan içerik söz konusu çocukların onuruna, güvenliğine ve mahremiyetine yönelik zorluklar doğuruyorsa ya da hâlihazırda veya yaşamlarının daha sonraki bir evresinde onları incinebilir kılıyorsa, söz konusu içeriğin hiçbir sürekli veya daimi erişilebilir kaydı olmamalıdır. (20 Şubat 2008 tarihinde kabul edilen “İnternette çocukların onurunun, güvenliğinin ve mahremiyetinin korunması” hakkındaki Bakanlar Komitesi Bildirgesi¹).

■ Mahremiyetin güvenlikle yakından ilişkisi vardır; güvenlik konusunda Kılavuz 19’un tümünü okuduğunuzdan emin olunuz.



İNTERNETTE MAHREMİYETİ

- İnternette (veya çevrimiçinde) mahremiyet, hassas ve kişisel verinin, haberleşmelerin ve tercihlerin² korunmasına yönelik kullanılan çeşitli faktörlere, tekniklere ve teknolojilere atıfta bulunan geniş bir terimdir.
- İnternette mahremiyet, herhangi bir kullanıcının bilgisayar, tablet, akıllı telefon, oyun konsolu veya diğer Wi-Fi özellikli cihaz yoluyla çevrimiçine her bağlanışında bir endişe kaynağıdır.
- İnternette mahremiyet sadece verinizi çevrimiçinde nasıl kişisel olarak koruduğunuzla değil, bilgilerinizi ele geçirmek amacıyla bilgisayar korsancılarının erişilebilirliğiyle de ilgilidir.
- Genel Veri Koruma Düzenlemesi (GVKD), kullanıcıların verileri üzerindeki denetimini ve çevrimiçi mahremiyetlerini çok daha fazla korumayı sağlamaktadır. GVKD için önemli hususlar şunlardır:

- ➔ Kullanıcı izninin yeni bir tanımı – söz konusu hizmetin sağlanması için kullanıcılar sıkı biçimde gerekenden daha fazla veri işlemine izin vermek zorunda iseler iznin serbestçe verilmekte olduğu artık düşünülemez.
- ➔ Verilerinin piktogramlar/ikonlar ve “yalın dil” ile nasıl işleme tabi tutulduğuna dair bilgilendirmede kullanıcılara daha iyi şeffaflık sunmak – bu şeffaflık kullanıcılara verilen hizmetler arasında mukayeselerini daha iyi yapmalarına ve mahremiyetlerine daha fazla saygı duyan hizmetleri seçmelerine imkân tanıyacaktır.
- ➔ Kullanıcının kendi verilerini çevrimiçinde bir yerden bir yere taşıyabilme hakkı, onların kullandıkları hizmetlerden kullanışlı bir formatta verilerini geri elde edebilmeleri anlamına gelmektedir – kullanıcıların kendi verileri üzerindeki denetimi ve veri sahipliği ilkesi bu hükümle büyük ölçüde desteklenmektedir.
- ➔ Çocukların gelişmiş şekilde korunması – 13 (en az) ile 16 (en fazla) yaşlar arasındaki her çocuk fazladan sağlanacak korumalardan faydalanacaktır örneğin, bir veri işlemde ebeveynlerinin iznini alma gereği gibi ve reklam amaçlı veri işleme karşı korunmadan da faydalanacaktır.
- ➔ Bu kuralların ihlali durumlarında ceza (şirket cirosunun 4%'üne kadar) ödemeleri,
- Bir parolanın kırılması, ele geçirilmesi ve ifşa edilmesi halinde bunun, kimlik hırsızlığından başlayarak yasadışı çevrimiçi işlemlere ve ötesine kadar uzanan çok ciddi sonuçları olabilecektir.

Mahremiyet Ayarları

■ Mahremiyet ayarları kullanıcılara kendi bilgilerine kimin erişebileceğini ve başkaları tarafından ne kadar bilginin görülebileceğini kısıtlama imkânı sağlayan denetimlerdir.

■ Birçok sosyal ağdaki mahremiyet ayarları, ilk etapta varsayılan durumuna ayarlıdır. Genelde kendi gereksinimlerinize göre bu ayarları kişisel hale getirebilirsiniz ve sosyal ağ platformu güncellemeleri uyguladığına dair sizi her bilgilendirdiğinde bu ayarlarınızı tekrardan denetleyebilirsiniz.

■ Tüm Wi-Fi özellikli cihazlarda mahremiyet ayarları düzenli olarak kontrol edilmelidir. Konum ayarlarını da kontrol etmeyi unutmayın. Çünkü sizin ya da cihazınızın konum koordinatları mahremiyetinizin önemli yönleridir (bkz. Mobil teknoloji konusundaki Kılavuz 5).

Yer Konumlama

■ Yer konumlama, radar, cep telefonu veya internete bağlı bilgisayar gibi bir cihazın konumunu teşhis edilmesidir.

■ Yer konumlama, bir cihazın konumunun belirlenmesi sürecidir. Yer konumlama uygulamaları, kullanıcılara sizin konumunuzu gösterir ve sizin konumunuzla mukayeseli olarak gerçek-dünya konumları arasındaki mesafeleri de teşhis eder. Yer konumlama uygulamaları, hizmetler ve ürünler için yeni iş modellerinin yolunu açmıştır.

¹ <https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2820.02.2008%29&Language=lanEnglish&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>
² <http://web.archive.org/web/20160703014430/https://www.techopedia.com/definition/24954/internet-privacy>
³ <https://en.wikipedia.org/wiki/Geolocation>

■ Yer konumlama nerede olduğunuzu gösterdiğinden, sizin mahremiyetinize bir tehdit de oluşturabilir. Bir çocuğun yer konumu ise söz konusu o çocuğun güvenliğine de bir tehdit oluşturabilir.

Çerezler

■ Bir çerez4 web sitesini ziyaret ettiğiniz zaman bilgisayarınızda kalan metin dosyasıdır. Çerez bilgisayara zarar vermez ancak, sizin davranışlarınıza ve ilgi duyduklarınıza ait bilgiye erişim sağlar. Bu da daha kişisel bir gezinti atmosferi verebilir. Örneğin; bir web-sitesine kayıt olduğunuzda o siteyi tekrar ziyaret ettiğinizde sizi isminizle karşılayabilir.

■ Çevrimiçi davranışınızı ne kadar özel tutmak istediğinize karar vermek önemlidir. Çünkü çerezler kullanım örneklemelerini ve temas bilginizi izlemek için kullanılabilir olduğundan sizin mahremiyetinizi ele geçirmeye yeltenme olasılığı taşırlar. Ayrıca reklamcıların davranışsal eğilimleri saptamalarını (davranışsal hedefleme) da kolaylaştırabilmektedirler⁵.

■ Sisteminizin yayınladığı verinin denetlenmesine ve istenmeyen çerezlerin temizlenmesine yardımcı olmak için bir casus yazılım engelleyici (spyware6) kullanabilirsiniz.

■ Günümüzde, Avrupa Birliğinde sahip olunan veya Avrupa Birliği vatandaşlarını hedef alan tüm websitelerinin Çerez Mevzuatı ile uyumlu olması beklenmektedir (2009/136/EC sayılı AB Yönergesi). Bu mevzuat bireylere çevrimiçi mahremiyeti azaltan çerezlerin kullanımını reddetme hakkı getirmektedir.

Veri koruma

■ Kişisel verinin korunması “Avrupa Konseyi Kişisel Verinin Otomatik İşlenmesine dair Bireylerin Korunması Sözleşmesi” ile düzenlenmiştir.

■ Bir ticari kurumun sizin hakkınızda hangi veriye sahip olduğunu bilme hakkınız vardır. Eğer doğru değilse bu veriyi de değiştirebilmelisiniz ve bu verinin nasıl kullanılıyor olduğuna dair izninizin alınması da gereklidir.

■ Verinizi korumak için en iyi rehber ilkeler, Genel Veri Koruma Düzenlemesi’nde bulunabilir⁷.

■ Kişisel bilgi⁸ sağlamanız istenen tüm web-siteleri ve uygulamalardaki feragatnameyi dikkatlice okuyunuz. Bu sizinle veri denetçisi⁹ arasındaki yasal bir sözleşmedir ve bu feragatname verinizin nerede ve ne kadar süre için saklanacağına ve nasıl silineceğine dair ayrıntıları bildirmektedir.

■ Cihazınızın ve e-posta programlarınızın şifre korumalı¹⁰ olduğundan emin olunuz. Yeni bir cihaz veya yazılım satın aldığınızda ya da bir internet hizmet sağlayıcısıyla sözleşme imzaladığınızda, size bir “varsayılan” kullanıcı ve parola ayarı muhtemelen verilecektir¹¹. Bu tür varsayılan ayarlarını hızlıca daha güvenli bir parola ve kimlikle değiştirdiğinizden emin olunuz.

■ İnternette gönderilen her tür hassas bilgiyi¹² şifrelemek en iyi yöntemdir. Neyse ki e-ticaret işlemlerinin çoğu için bu bir standart uygulamadır ancak, kredi kartı bilgilerinizi veya banka hesap numaralarınızı iletmeden önce sayfanın güvenli olduğundan hala emin olmanız gerekmektedir.

■ Bilgisayarınızın farklı kısımlarını parolalar kullanarak güvenli hale getirebilirsiniz. Gizli projeler, araştırmalar, özgün tasarımlar vb. değerli belgeler içeren dosyalarınız için parolalar oluşturun.

Unutulma Hakkı

■ Unutulma hakkı, mahremiyetle ilgili her tartışmada önemli bir unsurdur, çünkü bu hak, bireylerin mahremiyetlerini “yeniden kazanmalarına” imkân verir.

1. https://en.wikipedia.org/wiki/HTTP_cookie

2. https://en.wikipedia.org/wiki/Behavioral_targeting

3. <https://en.wikipedia.org/wiki/Spyware>

4. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

5. <https://en.wikipedia.org/wiki/Disclaimer>

6. <https://goo.gl/XEkvjh>

7. <https://en.wikipedia.org/wiki/Password>

8. <http://www.netlingo.com/right.cfm?term=default>

9. <http://en.wikipedia.org/wiki/Encryption>

10. <http://en.wikipedia.org/wiki/Ecommerce>

■ Avrupa Birliği'nde bir kişi, herhangi bir araştırma motorundan kendi adını aradığında, adının çıkmaması için arama sonucu dizininden belli sonuçları silmesini isteyebilir. Ancak, bunun sınırları vardır ve alınacak bu önlemin, ifade özgürlüğü gibi başkalarının temel haklarıyla her zaman dengelenmesi gerekir. Yine de söz konusu bilgi, yerleştirildiği web sitesinde erişilebilir olmaya devam edecektir ancak bulunmasını sadece biraz daha zorlaştıracaktır.

■ Unutulma hakkını kullanmak ve arama motorundan söz konusu bilginin çıkarılmasını talep etmek isteyen kişinin arama motorunun web sitesindeki bir formu doldurması zorunludur.

■ Ancak unutmayın ki, aslında kişisel bilgiyi göndermemek daha doğrudur, çünkü internette bir kez yer alırsa tamamıyla silmek neredeyse imkânsızdır.

Sınıfta veya evde mahremiyet hakkında konuşmanın önemi

■ Mahremiyetin teknik ve sosyal boyutları ve kişinin kendi ifşasının doğuracağı riskler değerli öğrenme konularını sağlamaktadır. Teknik boyutlar, bilişim teknolojileri (IT) derslerine dâhil edilebilir ancak hayat becerileri müfredatına da eklenmelidir.

■ Mahremiyet konusundaki eğitimin önemli bir unsuru, “profil oluşturulması” ve kişi hakkında daha ayrıntılı bir resim ortaya çıkarmak için o kişinin dağılmış haldeki bilgi unsurlarının birbirine bağlanması kavramı olmalıdır. Eğitim açısından önemli çıkarım “ikiyi ikiye bir araya getirme” yoluyla hakkımızdaki birçok bilgiyi bulabileceğimize. Örneğin, “isimsiz” bir sosyal ağ iletişim profili” kullanan kişi (takma ad arkasına gizlenen) sizin gerçek isminizle teşhis edilebilir. Bu da isimsiz bir profil ile diğer tarafta yer alan tüm bilgileri girilmiş profil arasında fotoğraflar eşleştirilerek mümkün olabilir.

■ Mahremiyetin, klasik kişisel bilginin açığa vurulmasıyla sadece ihlal edildiği fikrinin dikkatli şekilde incelenmesi gereklidir. Yeni pazarlama tekniklerinin - ki bunların bazılarının davranış özelliklerine (davranışsal hedefleme) dayalı olarak insanlar arasında ayırmacılık yapmaktadır – mahremiyete mütecaviz şekilde olduğu da düşünülebilir. İnsanları davranış özelliklerine göre ayıran ve sınıflandıran yeni pazarlama teknikleri (davranışsal hedefleme) aynı zamanda mahremiyete yönelik taciz olarak da değerlendirilebilir.

■ Mahremiyet, çocukların ve gençlerin cep telefonlardaki web uygulamaları, kamera ve MMS kolaylıkları yoluyla kolay ve hızlıca sayısal görüntüleri yayınlatabilmeleri veya oynatabilmeleri sebebiyle giderek tehlikeye düşmektedir. Pratik kural: öğretmenlerinizin veya ebeynlerinizin görmesini istemeyeceğiniz hiçbir şeyi asla yayınlamayınız...

■ Herkesin internette güvenli şekilde gezinmesi için gerekli becerilere sahip olması gerekir ki bu becerilere kendini koruma bilgisi, etkin iletişim ve başkalarına karşı sorumlu davranmak dâhildir.

Her müfredatta yer alan vatandaşlık boyutu ile çevrimiçinde mahremiyetin korunması arasında doğal bir ilinti vardır. Çevrimiçi mahremiyet hakkında ortaya atılan konular, günümüz kültürlerinin çoğunda bulunan baskın haldeki sosyal konuları tam anlamıyla yansıtmaktadır. Bilgisayar korsanları¹⁵, şifre kırıcılar ve mahremiyet aktivistlerinin güdülerini araştırma, demokratik ilkelerin değerinin tartışılması için çok sayıda fırsat sunmaktadır.



ETİK DEĞERLENDİRMELER VE RİSKLERİ

* Çevrimiçi mahremiyet, internete ilişkin olarak en karmaşık etik ve hukuki konulardan birisidir.

* Herkesin mahremiyet hakkı vardır ve bu hakkın kötü niyetten korunması gerekmektedir.

* İnternet korsanlığı riskleri şunları içerir: ortalama [(phishing) güvenli kullanıcı verisi çalmak için bilgisayar korsanlığı], sahte sitcilik [(pharming) meşru websitesi ziyaretçisini farklı bir IP adresine yönlendiren internet korsanlığı], casus yazılım [(spyware) kullanıcının izni olmaksızın çevrim içinde veri elde eden uygulama] ve kötü amaçlı yazılım [(malware) truvalar, virüsler ve casus yazılımlar¹⁶ yoluyla çevrimiçi ve çevrimdışı kullanıcılara zarar vermek amacıyla kullanılan yasadışı uygulamalardır.

* Sexting (erotik mesajlaşma) telefon, bilgisayar, web-kamerası veya başka cihazla ya da çevrimiçi cinsel içerikli yazıları e-posta yoluyla davetkâr ve açık içerik, görsel (sıklıkla öz-çekimler) mesaj ve görüntü gönderme eylemidir. Bu eylemin sadece yasalar açısından değil aynı zamanda söz konusu kişinin itibarına ilişkin riskler taşıdığından ciddi sonuçları vardır, çünkü söz konusu mesajlar, görüntüler veya videolar sosyal medya sitelerine de gönderilmekte ya da pornografik websitelerinde ve videolarda kullanılmaktadır.

• https://en.wikipedia.org/wiki/Right_to_be_forgotten
• <http://en.wikipedia.org/wiki/Hacker>
• <http://web.archive.org/web/20160703014430/https://www.techopedia.com/definition/24954/internet-privacy>

- Kendimize ait ve başkalarının hakları hakkında verdiğimiz tüm kararlar için hesap verebiliriz, örneğin; telif hakkı¹⁷ ve fikri mülkiyet hakkı¹⁸ ...
- İfade özgürlüğü bir haktır; ancak, uygulamada bu hak kolay cevapları olmayan gri bir alandır. Kabuledilebilir veya kabul edilemezler nelerdir? Konuşmacının haklarına zarar vermeyecek şekilde bu kurallar nasıl hayata geçirilebilir?



NASIL

İnternet erişimli ve Wi-Fi özellikli tüm cihazlarınızın üzerindeki mahremiyet ayarlarını kullanmak mahremiyeti korumanın en iyi yollarından biridir.

Farklı tarayıcılara göre, mahremiyet ayarlarında şu hususları nasıl yapabileceğinizi görmek için hızlı bir arama yapınız:

- Reklamları ve izlenmeyi engellemek,
- Üçüncü taraf çerezleri engellemek,
- Websitelerinin sizin konumunuza erişmelerini engellemek.

Akıllı telefonlarda, tabletlerde ve oyun konsollarındaki mahremiyet ayarlarının ayarlarını yapmayı unutmayın. Yeni kameralarda yerkonum ayarları bulunur, onları da kontrol ediniz.



SINIF ÇALIŞMASI İÇİN FİKİRLER

- Öğrencilerinize Google arama motorunda kendi adlarını arattırın. Görseller ve videoların altlarına da baktığınızdan emin olun. İsimlerine ilişkin bir Google alarmı oluşturun, böylece isimlerinin ne zaman çevrimiçi gönderilmiş olduğunu bileceklerdir.
- Sınıfınızla birlikte mahremiyet açısından temel bir bilgi çerçevesi oluşturun. Hem teknik hem de sosyal açıdan kavramları tanımlayın ve üzerinde tartışmak için önyargıları ve hikaye kalıplarını belirleyin. "Mahremiyet nedir?" ve "Mahremiyet gerekli midir?" gibi basit sorular oluşturmak bazı güçlü görüşler ortaya çıkarır.
- İnternetteki mahremiyetle ilgili siteleri araştırınız ve bunun için iz sürücü programlar kullanınız. Bu iz sürücü¹⁹ (traceroute) programlar, internetteki çeşitli yer fiziksel konularının meşruluğunu gösteren bu sitelerin fiziki adreslerini saptamak içindir. Arama izi sonuçlarından ortaya çıkan diğer konuları (kültürel, siyasi ve tarihi) araştırınız. Örneğin, tekrar-postalayıcı (remailer) bir site ya da isimsiz bir vekil sunucu (Proxy server) seçiniz, bir iz takip ediniz, daha sonra söz konusu hizmetlerin neden o ülkelerde yerleşik olduğuna dair sebepleri araştırınız.
- Veri koruma ve mahremiyet²⁰ konusunda rol oynama oyunu The Play-Decide, ulusal sınırları aşan mahremiyet kanunu, telif hakkı ve ifade özgürlüğünün farklı yaş ve kültür grupları için boyutlarını araştırmada eğlenceli bir yol sunmaktadır.
- Öğrencilere güvenli parolaları²¹ nasıl oluşturacaklarını öğretiniz.
- Öğrencilerinizle daha popüler sosyal ağ iletişim sitelerindeki kullanıcı profillerini araştırınız ve birbiriyle mukayese ediniz (Bkz. Sosyal ağ iletişim konusunda Kılavuz 8). Kullanıcılar dikkatsizlikle hangi mahrem bilgileri ifşa ediyorlar? Güvenli bir kullanıcı profili oluşturmak için bir kontrol listesi oluşturun.



İYİ UYGULAMALAR

İki altın kural:

Bilmediğiniz ve güvenmediğiniz kimseyle kişisel bilgilerinizi paylaşmayın,

İzni olmadan başka hiçbir kimsenin kişisel bilgisini veya fotoğrafını kullanmayın.

9. <http://en.wikipedia.org/wiki/Copyright>

10. http://en.wikipedia.org/wiki/Intellectual_property

11. <http://en.wikipedia.org/wiki/Traceroute>

12. <http://en.wikipedia.org/wiki/Remailer>

13. <http://paneuyouth.eu/files/2013/06/PD-kit-privacy-and-data-protection.pdf>

14. http://en.wikipedia.org/wiki/Password#Factors_in_the_security_of_an_individual_password

- Sisteminizi yedekleyin³ ve düzenli yedekleme alışkanlığı edinin.
- Sisteminizdeki güvenlik önlemlerini güncelleyin ve çevrimiçi tercihlerinizi destekleyecek ek gereçler konusunda şu adreste araştırma yapın: <http://www.epic.org/privacy/tools.html>.
- Anti-virüs⁴ ve güvenlik duvarı⁵ yazılımları kesinlikle gereklidir. Açılır pencere (pop-up) engelleyiciler⁶ ve casus⁷ (anti-spyware) yazılım engelleyici gibi diğer gereçleri de kullanmayı isteyebilirsiniz. Sisteminizi düzenli denetlediğinizden emin olun.
- Kişisel Bilgisayarınızı (PC), e-postanızı ve internet bağlantılarınızı korumak için “güçlü parolalar” kullanın. Güçlü parolalar, harflerden, numaralardan ve özel karakterlerden oluşur.
- Kişisel verinizi yayınlamadan önce, araç çubuğunda beliren asma kilit kontrol edin. Bu, işleminizin güvenli bir bağlantı üzerinden yapılmakta olduğunu gösteren bir işarettir. Çevrimiçi işlemlerinizi yapmadan önce URL'nin HTTPS içerdiğini denetleyin. “S”, üçüncü taraftan gelebilecek saldırılara karşı koruyan Hiper Metin Transfer Protokolünde (HTTP) “güvenli” anlamına gelir ve web sitesini ve ilgili web sunucusunu doğrulayarak tastik eder.
- Güvenilir olmayan websitelerindeki çevrimiçi alışverişten kaçının ve düşük güvenlik düzeyli websitelerine kişisel verinizi açıklamaktan uzak durun.
- Haklarınızı denetlediğinizden emin olun; düşündüğünüzden fazla korunabilirsiniz. Kullanıcılar mahremiyet ve veri koruma hususlarında her zaman en zayıf halkadır.



DAHA FAZLA BİLGİ İÇİN

Çerez Kanunu ve AB Yönergesi hakkında daha fazla bilgi için bkz.:

<http://www.cookie-law.org/the-cookie-law/>.

Unutulma Hakkı konusunda Avrupa Komisyonu'nun bir Kılavuz sayfası bulunmaktadır: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

Veri Koruma konusunda da Avrupa Komisyonu'nun bir Kılavuz sayfası bulunmaktadır: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf ve ilgili reformlar konusunda diğer bilgiler: http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

Elektronik Mahremiyet Bilgi Merkezi (EPIC) mahremiyet gereçleri ve makalelerinden oluşan bir liste tanzim etmektedir: <http://www.epic.org/privacy/tools.html>.

TarayıcıCasusu (BrowserSpy) kullanarak bilgisayarınızın çevrimiğinde ilettiklerini keşfedin:

<http://gemal.dk/browserspy/>.

Medeni haklara ilgi mi duyuyorsunuz? Mahremiyetle ilgili bu tartışmalar vatandaşlık dersinizi bir süre idare eder: Electronic Frontier Foundation (Elektronik Sınırlar Vakfı) <http://www EFF.org/>, Epic.org <http://www.epic.org/>, Privacy International (Uluslararası Mahremiyet) <http://www.privacyinternational.org/> ve Privacy.net <http://www.privacy.net/>.

<http://www.tucows.com/> adresindeki TuCows, 40.000'in üzerinde kısa süreli (shareware) ve ücretsiz (freeware) program yazılımı sağlayan bir web sitesidir. Hızlı, yerel ve güvenli, virüssüz ve casus yazılımsız indirmeler sunmaktadır.

<http://www.zonelabs.com/store/content/home.jsp> adresindeki Zone Alarm, tanınmış güvenlik duvarı yazılımlarından biridir. İnternet üzerinden bilgi gönderen farklı programlar için erişim denetimlerini ayarlamanıza imkân verir.

CryptoHeaven, simetrik ve asimetrik şifreli güvenli posta, dosya paylaşımı ve sohbet yapma imkânı sunan bir şifreleme paketidir: <http://www.cryptoheaven.com/>.

3. http://en.wikipedia.org/wiki/Back_up

4. <http://en.wikipedia.org/wiki/Antivirus>

5. http://en.wikipedia.org/wiki/Firewall_%28networking%29

6. http://en.wikipedia.org/wiki/Pop_up#Add-on_programs_that_block_pop-up_ads

7. <http://en.wikipedia.org/wiki/Spyware>

8. http://en.wikipedia.org/wiki/Password#Factors_in_the_security_of_an_individual_password

- Facebook Yardım Merkezi mahremiyet ayarları hakkında bilgi sunar: <https://www.facebook.com/help/193677450678703>.
- Çocukların ve gençlerin çevrimiçi mahremiyeti ve mahremiyet ayarlarını nasıl anladıkları konusundaki istatistiksel bilgi şu adreslerde: <http://web.archive.org/web/20160703155259/https://www.techopedia.com/2/30101/internet/online-privacy/do-millennials-understand-online-privacy>.
- Günümüz Avrupa'sında Genç olmak konusundaki istatistiksel bilgi için bkz.: http://web.archive.org/web/20160604111543/http://ec.europa.eu/eurostat/statistics-explained/index.php/Being_young_in_Europe_today_-_digital_world.
- Avrupa sayısal hakları konusunda bilgi için bkz.: <http://www.edri.org>.
- İlgili Avrupa Konseyi Belgeleri:

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (ETS No. 108): <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>.

İnternette çocukların onuru, güvenliği ve mahremiyetinin korunması hususunda Avrupa Konseyi Bakanlar Komitesi Bildirisi : <https://wcd.coe.int/ViewDoc.jsp?id=1252427>.

Bu Avrupa Konseyi sayfası, mahremiyet ve veri koruma alanında Avrupa Konseyi'nin çalışmaları hakkında bilgi içermektedir. : <http://www.coe.int/en/web/internet-users-rights/privacy-and-data-protection>
Bunun yanı sıra, çevrimiçi haklarınız ve sorumluluklarınız hakkında bilgi de yer almaktadır.

3.İnternet - Bilgi Toplumuna Katılım

“Bilgi güçtür. Bilgi özgürleştirir. Eğitim her toplumda, her ailede gelişimin öncüsüdür.”
Kofi Annan, Birleşmiş Milletler Genel sekreteri, Ocak 1997-Aralık 2006

KILAVUZ 10- BİLGİYİ ARAŞTIRMAK

Bir web sayfasına başvurduğunuzda kullanım şartlarını okur musunuz?

Bulduğunuz bilginin doğru ve tarafsız olduğundan nasıl emin olabilirsiniz?

Doğruları kontrol etmek için çeşitli web sayfalarına başvurur musunuz?

KILAVUZ 11-WEB'DE KALİTELİ BİLGİYİ BULMAK

Dosyaları indirmeden önce, anti-virüs programınızın faal olup olmadığını kontrol eder misiniz?

Haberleri İnternette okuyorsanız, aynı hikâyeye hakkında birden fazla bakış açısı arar mısınız?

Profilinizin arama motorlarınca “oluşturulmasını” istemiyorsanız, zaman zaman çerezlerinizi temizlemelisiniz.

KILAVUZ 12-UZAKTAN EĞİTİM VE KİTLESEL AÇIK ÇEVİRİMİÇİ DERS (MOOC)

Sizin için uygun olan bir uzaktan eğitim yöntemi seçiniz. Hedeflerinize ulaşmak için size en iyi şekilde, hangi öğrenme yönteminin (eşzamanlı, eşzamanlı olmayan, açık program, hibrid uzaktan öğrenme) yardımcı olacağına karar veriniz.

Uzaktan eğitim kursunu seçmeden önce, öğrenci ve öğretmenlerden gelen değerlendirmeleri inceleyiniz.

Bilgisayar donanımınızın ve yazılımınızın bilgisayar korsanları, virüsler ve diğer tehditlere karşı güvende olduğundan emin olmak için gerekli önlemleri alınız.

KILAVUZ 13- ÇEVİRİMİÇİ ALIŞVERİŞ

Çevrimiçi satın almalarınızı güvenli olmayan internet bağlantıları üzerinden yapmayınız.

Ürün veya hizmetler hakkında, verilen önemli bilgileri anlayınız ve kabul ediniz. Akıllı telefonunuz veya tabletinizdeki uygulama içi satın alma işlemini kapatınız.

Gördüğünüz her kullanıcı tavsiyesine inanmayınız. “Kullanıcı” tavsiyeleri hazırlamak da bir para kazanma işidir.

Bilgiyi Araştırmak



A internetin ilk yıllarında arama motorları yoktu. Arama motorlarının olmadığı bir dünyayı hayal etmeye çalışın. İnsanlar, gazete veya dergilerde yazılı web sitelerini bulmak ve adresi tarayıcı üzerine yazmak zorunda kalacaktı. Neyse ki yazılan web sitesinin bir başka web sitesiyle bağlantıları olduğu bulunacaktı ve bir bağlantıdan diğerine tıklayarak “World Wide Web”i (Dünya Çapında Ağ) “keşfedebileceklerdi”. Zaman içinde, telefon rehberini andıran internet portalları (kapı) veya rehberleri (directory)¹ oluşturulmuştu: çok sayıda web sitesinin içinde yer aldığı liste sınıflandırılmıştı. Bu rehber veya portallardan bazıları örneğin Yahoo ve MSN hala mevcuttur. Diğer portal türleri:

- Birleşmiş Milletler web sitesi veya Avrupa Konseyi web sitesi benzeri “resmi” içeriğe sahip portallar;
- Oteller için Booking.com veya alışveriş için Amazon.com benzeri özel içerik veya hizmetlerde ihtisaslaşmış portallar;

1. https://en.wikipedia.org/wiki/Web_portal

- Çok çeşitli kullanıcı tarafından oluşturulan içeriğe dayalı portallar - Facebook benzeri sosyal ağlar da bu tür bir portal olarak değerlendirilebilir.

■ Daha sonra arama motorları oluşturulmuş ve bu motorlar, insanların İnternet üzerinde içerik aramaları açısından devrim yaratmıştır. Ancak arama motorları nasıl çalışmaktadır? Günümüzde arama motorları, içeriği analiz eden, içeriği kataloglara² göre sınıflandıran ve aramalarınızda kullandığınız anahtar kelimelere bağlı olarak bu kataloglardan hangi web sitelerinin çekip alınacağına karar veren ağ gezginlerine³ ve oldukça karmaşık algoritmalara dayanmaktadır.

■ Algoritmanın nasıl kurgulandığı oldukça önemlidir, çünkü birçok insan araştırma sonuçlarının ilk birkaç sayfasına bakıp, bırakmaktadır. Günümüzde Google en bilinen arama motorudur ve bir web sitesinin önemini, kaç tane arka bağlantıları⁴ olduğuna dayalı, orijinal bir derecelendirme yöntemi kullanan algoritması sayesinde Google kendisini popüler kılmıştır. Bu, temel olarak sizin web sitenizle kaç tane harici web sitesinin bağlantı içerdiği anlamına gelmektedir. Örneğin, eğer wikipedia.org web sitesi çok sayıda diğer web sitesi ile bağlantılandırıldıysa, o durumda en yüksek dereceyi alacaktır.

■ Ancak artan gerçeklik nedeniyle algoritmalar da düzenli olarak önemli değişikliklere uğramaktadır. Örneğin Google, web sitelerinin “güvenirliliğini” içeriği Google’ın Bilgi Vault’unda depolanan gerçeklerle çapraz-ilintileyerek ölçmek için bir ekleme yapmayı planlamaktadır. Dahası ilerde göreceğimiz gibi algoritmalar ticari amaçlarla da değişikliğe uğrayabilir.

■ Arama motorunun nasıl çalıştığı hakkında Google’ın canlandırılmalı açıklamasına bakınız. <https://www.google.com/insidesearch/howsearchworks/thestory/>



EĞİTİCİ DEĞERİ NEDEN GÖRECELİ VE ÖNEMLİDİR?

■ Bir arama motorunun düzgün bir şekilde nasıl kullanılacağını öğrenmek, muhtemelen bir kişinin sadece İnternet üzerinde sorumlu bir şekilde dolaşması açısından değil aynı zamanda o kişinin eleştirel düşünme (çevrimiçi farklı kaynakları araştırmak ve karşılaştırmak suretiyle) gibi temel beceriler kazanması açısından geliştirmesi gereken en önemli beceridir. Bir arama motorunun nasıl çalıştığını bir kez anladıktan sonra, bu durum sizin diğer bin tane beceri geliştirmeniz veya İnternet üzerinde sorumlu davranmanın da içinde yer aldığı bir dizi sayısız konu hakkında bilgi edinmeniz için kaliteli bilgi bulmanıza yardımcı olabilecektir!

■ Örneğin, cihazlarınızla ilgili yaşadığınız sorunlara çözümler arayarak dijital becerilerinizi geliştirebilir veya bunların nasıl çalıştığı hakkındaki merakınızı kolayca giderebilirsiniz. Şu anda okumakta olduğunuz İnternet okuryazarlığı el kitabını bulabilmeniz bir arama motorunu kullanma sayesinde olmuştur.



ETİK HUSUSLAR VE RİSKLER

- Üyelik veya kayıt gerektiren bazı portallar ödemeli bir hizmet olabilir. Kayıt olmadan önce (“ücretsiz” hizmetler için bile) hizmetin şartlarını ve koşullarını anladığınızdan ve web sitesinin gizlilik politikasını araştırmış ve anlamış olduğunuzdan emin olunuz. (bkz.: <http://www.netlingo.com/right.cfm?term=privacy%20policy>).
- Web siteleri, arama motoru sonuçlarındaki sıralamalarını iyileştirmek için ödeme de dâhil olmak üzere çeşitli araçlar kullanırlar. Google gibi bazı arama motorları hangi sonuçların desteklendiğini açıkça belirtir. Diğer birçoğu ise böyle bir ayırım yapmamaktadır.
- Algoritmaların kendisi, hiçbir zaman tarafsız değildir, tartışmalara ve eleştirilere¹ açıktır. Örneğin Google’un, Google Shopping, Google + benzeri kendi hizmetlerinin veya YouTube’un rakiplerinin (Amazon, Facebook, Dailymotion vb.) aleyhine olacak şekilde görünürlüklerini artırdığı bilinmektedir. Arama motorları siyasi gerekçeler için de yönlendirilebilir. Temel bir kural olarak, bir arama sonucunun sadece üst sıralarda çıkmış olmasından dolayı “gerçeğin” temsilcisi olduğuna veya alt sıralarda yer alan web sitelerinin “önemsiz” veya “alakasız” olduklarına asla inanmayın.

² https://en.wikipedia.org/wiki/Web_indexing

³ https://en.wikipedia.org/wiki/Web_crawler

⁴ <https://en.wikipedia.org/wiki/Backlink>

- İşte bu nedenle, daha iyi arama gerçekliği ve tarafsızlığına katkıda bulunabilecek sağlıklı bir rekabet tesis etmek ve daha çeşitli sonuçlar almak için Web'i tarayabilecek arama motorlarına ve çeşitli geçitlere sahip olmamız şarttır. Bir kullanıcı olarak çevrimiçi ortamı şekillendirmede önemli bir rol oynuyorsunuz: Yahoo, Bing, Qwant, IXquick veya DuckDuckGo benzeri diğer arama motorlarını kullanmayı unutmayınız. Daha az bilinen arama motorlarını kullanmak suretiyle onların devamlılığına katkıda bulunur ve bu vasıta ile çeşitliliği⁶ sağlarsınız.
- Coğrafi konumunuzun⁷ ve daha önceki aramalarınızdan kalan çerezlerin arama sonuçlarınızı etkileyeceğinin farkında olunuz. Coğrafi konumunuza ilişkin verinin arama motoru tarafından alınması kaçınılmaz⁸ olsa da, çerezlerinizi düzenli olarak temizlemeniz (bkz. Kılavuz 9 gizlilik ve gizliliğin korunması hakkında) ve tarama geçmişinizi en az düzeye indirmeniz en son aramalarınızla (örneğin seyahat için gideceğiniz yerler) ilgili olarak alacağınız reklamları azaltacaktır. Bu aynı zamanda sizin önemli sosyal ve siyasi konular hakkında algıladığınız perspektifinizle⁹ sınırlanmadan makul bir şekilde çok iyi bilgilendirilmenizi sağlamaya yardımcı olacaktır. İnternet tarayıcınızdaki ayarlara bakarak çerezleri tümünden etkisiz kılabilirsiniz, buna karşılık, bazı web sitelerinin düzgün bir şekilde çalışıp çalışmadığına dikkat ediniz.
- Son olarak, aramalarınızda elde edeceğiniz sonuçların büyük oranda ne aradığınıza bağlı olacağını aklınızda tutunuz. Örnek olarak oldukça şiddet içeren bir içerik araması yaparsanız, büyük olasılıkla bunu bulabilirsiniz, ancak istediğinizden çok daha fazlasını elde edebilirsiniz. Şoke edici veya rahatsız edici içeriğe karşı mukavemet geliştirmek bir yaşam boyu süreçtir, bu yüzden aceleci davranmayın, adım adım ilerleyin.



NASIL?

Arama motorları bilgiye erişim açısından en önemli geçitler olduğundan bunların derinlemesine nasıl çalıştığını anlamak önemlidir. İlk sayfadaki arama sonuçlarına bağlı kalmak size neyin önemli ve neyin önemsiz olduğuna dair oldukça eksik bir görüş verecektir. En önemli gelişmiş arama özellikleri:

- Tırnak işaretleri: bu muhtemelen en kullanışlı ve en iyi bilinen gelişmiş arama özelliğidir. Bir arama motorunun doğru ifadeyi aramasından emin olmak istiyorsanız, kelimenin başında ve sonunda tırnak işaretleri kullanınız. Eğer doğru ifade veya cümleyi bulmak istiyorsanız, bu size faydalı olabilecektir.
- Tire işareti "-": Bu, belirli bir terimi hariç tutarak bir şeyleri aradığınız zaman kullanılır. Örneğin, "alacakaranlık" kelimesini arıyorsanız, ilk sonuçların tamamı film serisi ile ilgili olacaktır. Ancak "alacakaranlık-vampir" yazarak arama yaparsanız, "alacakaranlık" kelimesinin tanımını elde edersiniz. Bu nedenle bir kelimenin başka şeylerle çok fazla bağlantısı varsa ve aramanızda karışıklık olmasını istemiyorsanız tire işareti oldukça kullanışlı olacaktır.
- Sorgulama seçenekleri: belirli anahtar kelimeler kullanarak aramanıza özel bir seçenek ilave edebilirsiniz. Örneğin, "tanımla: kuş" yazarsanız, kelimenin genel anlamı yerine "kuş" un tanımını arayacaktır. Eğer "site:wikipedi.org.apple" yazarsanız, Google sadece "Wikipedia" web sitesini arayacaktır. Bu aşağıda göreceğimiz gibi portallar vasıtasıyla yapacağımız aramalar için çok kullanışlıdır. Çok sayıda sorgulama seçenekleri vardır bu yüzden aşağıda verilen bağlantıya giderek onları kontrol ediniz.
- İhtisaslaşmış aramalar: Aralarında IXquick, Qwant, DuckDuckGo, Google, Yahoo ve Bing'in de bulunduğu çok sayıda arama motoru, kitle iletişimi içeriği (görüntüler, videolar vb) akademik makaleler, kitaplar, haritalar ve benzeri ihtisaslaşmış arama seçeneklerine sahiptir. Bu ihtisaslaşmış arama olanaklarını öğrenin çünkü bunların kendi gelişmiş seçenekleri vardır. Örneğin görüntüleri büyüklüğü, rengi, dosya türü ve hatta telif hakkı ve lisansına göre filtreleyebilirsiniz.
- Arama araçları: bir arama yaptığınızda doğrudan arama çubuğunun altında bulunan "arama araçları" oldukça kullanışlıdır. Sonuçları ülke ve zamana göre filtreleyebilirsiniz. Bu örneğin haberleri arayacaksanız oldukça kullanışlıdır çünkü böylece aramayı en son çıkan haberler veya tam bir yıl önce yayınlanan haberler olarak sınırlayabilirsiniz.

⁵https://en.wikipedia.org/wiki/Criticism_Google

⁶https://en.wikipedia.org/wiki/Web_search_engine

⁷<https://advancedwebranking.com/blog/geo-location/>

⁸<https://allaboutcookies.org/cookies-profiling.html>

⁹<http://www.praadviser.co.uk/how-delete-cookies-web-browsing-history-3218163/>

- Gelişmiş arama: “gelişmiş arama” seçeneğini yukarıda sağda yer alan “seçenekler” düğmesine tıklayarak bulabilirsiniz. Gelişmiş arama, size yukarıda anlatılan bütün arama özelliklerini kullanıcı dostu bir yolla sunacaktır, bu nedenle eğer operatörler veya özel sorgulama seçenek terimlerinden memnun değilseniz “gelişmiş arama”yı¹⁰kullanınız.



SINIF ÇALIŞMASI İÇİN FİKİRLER

- Her bir konu için bir arama hedefi belirleyin: farklı portallar/arama motorlarını kullanan ve aynı zamanda bilgi aramak için yukarıda tanımlanan arama tekniklerinden bazılarını kullanan ekipler oluşturun. Ekiplerin, sonuçları, erişim kolaylığını ve bilgi kalitesini karşılaştırmalarına izin verin.
- Örneğin çocukları resmeden 18. yüzyıl sanatı veya belirli bir türün okyanustaki ekosistem dinamikleri gibi arama yapmak için bir konu belirleyin. Sınıfınızı, ders planını destekleyici bağlantılara yönlendiren portal URL’lerini¹¹ verin. Muhtemelen bireylerin takip edebileceklerinden daha fazla bağlantı olacağından, bağlantıları bölüştürmek ve mümkün olduğunca çoğunu kapsamak amacıyla ekipler oluşturun ve her bir ekibin bulgularını sunmalarına izin verin. Ekiplerin sonuçları değişebilir; bu nedenle öğrencilerin öğrenmesini daha da geliştirmek için daha dar kapsamlı bir arama verin.
- Önleme veya tedavi: öğrencilerin kendi adlarını bir arama motorunda aramalarını ve kendileri hakkında ne kadar istenmeyen bilgi olduğunu görmelerini sağlayın. Bu tür bilginin herkese açık olmasını nasıl önleyebilirler ve veri koruma düzenlemeleri, istenmeyen içeriği silmelerinde onlara nasıl yardımcı olabilir?



İYİ UYGULAMALAR

- Bulduğunuz bilgiye her zaman kuşkuyla bakın. İnternet, insanlara görüşlerini paylaşmaları ve fikirlerini ileri sürebilmeleri için özgür bir alan sunar. Dolaşan efsanelere inanmaktan veya yanlış iddialara kapılmaktan kaçınmak için eleştirel bir gözle değerlendirdiğinizden ve farklı görüş ve bilgileri araştırdığınızdan emin olun.
- Hazır yazıları veya çalışmalarını kullanarak intihal yapmaktan kaçınınız. Mümkün olduğu kadar yazara itibar edin ve alıntı yaptığınız veya kullandığınız bilginin kaynağını veriniz. Bu, önemlidir çünkü:
 - Yazara ve kaynağa gerekli itibarı kazandırır;
 - Bu sizi intihal suçlamalarından korur;
 - Bu durum, başkalarının bilginin güvenilirliği hakkında kendi yargılarını oluşturmalarına yardım eder;
 - İnternette bulduğunuz bir bilgiyi kullanmanız halinde telif hakkı konuları hakkında bilinçli olun (bkz aşağıda “Nasıl” bölümü ve müzik ve görüntüler hakkında Kılavuz 14).
- Çerezlerinizi ve arama tarihçesini yönetmek/temizlemek için zaman ayırınız. Geliştirilmiş gizlilik için çerezleri tamamen etkisiz kılabilirsiniz ancak bazı web sitelerinin onlar olmadan düzgün bir şekilde çalışmadıklarını akılda tutunuz.
- Aramalarınızda en fazla verimi elde etmek ve sorgulamalarınızda kaynak çeşitliliği kullanmak amacıyla her zaman çeşitli araştırma terimlerini, gelişmiş arama tekniklerini ve farklı arama motorlarını deneyiniz.
- Kullanışlı siteleri veya portalları işaretleyin böylece onları tekrar aramanız gerekmez.
- Bazen, bir kamu kuruluşunun resmi bir dokümanı, bir kelime tanımı, otel fiyatları veya uçak biletlerinin karşılaştırması veya bir ürün satın alınması gibi bir portalla ilgili bir şeyler arıyor olabilirsiniz. Bütün bu sorgulamalar için arama motorlarının bir birleşimini ve Booking.com, Wikipedia veya Amazon gibi iyi bilinen portalları kullanabilirsiniz. Portalların çoğunun kendi dahili arama motorları bulunmaktadır ancak harici bir arama motoru da kullanabilirsiniz ve aramanızı bu portalla sınırlayabilirsiniz. Örneğin “Hotel Brussels site: booking.com” araması. Her ikisini de denemek aradığınız şeyi bulmak açısından iyi bir uygulamadır.

10. https://www.google.com/advanced_search?hl=en; https://en.wikipedia.org/wiki/Google_Search#Search_options

11. <http://en.wikipedia.org/wiki/URL>

- Kullanışlı bir bilgi bulursanız ekran görüntüsü alınız veya kaydediniz. Aksi takdirde tekrar bulamayabilirsiniz veya uyarı vermeden çevrimdışı olabilir.
- Cevaplarınızı bir arama motoru vasıtasıyla bulamazsanız, sorunuzu ilgili bir mesaj panosuna, tartışma forumuna veya sosyal ağı gönderiniz.
- Çevrimiçi içerik oluşumuna katkıda bulunmayı unutmayınız. Arama motoru kullanarak aradığınız tüm cevaplar bir başkası tarafından oluşturulmuştur. Kendi bilginizi ve becerilerinizi paylaşmak bir gün bir başkasının işine yarayabilir (bkz. Yaratıcılık başlıklı Kılavuz 15).



DAHA FAZLA BİLGİ İÇİN

- Wikipedia, dünyanın dört bir tarafındaki kullanıcılar tarafından işbirliği içerisinde yazılmış ücretsiz içeriğe sahip bir ansiklopedidir. <<http://www.wikipedia.org>>.
- Europeana portalı Avrupa kültürel mirasını temsil eden çok büyük miktarda sayısallaştırılmış içeriğe ev sahipliği yapmaktadır. <http://www.europeana.eu/portal>.
- Avrupalı arama motorları yüksek standartlarda gizlilik korumasına sahiptir: <http://www.qwant.com/> ve <http://ixquick.com/>
- Benzer şekilde yüksek standartlarda gizlilik koruması olan bir ABD arama motoru da vardır: <http://duckduckgo.com/>
- Aşağıdaki site size Google arama motorunda nasıl arama yapacağınızı anlatmaktadır: <http://support.google.com/websearch/answer/134479?hl=en>
- Window 8 üzerinde Microsoft'un Bing programını kullanımı ile ilgili ipuçları için bkz.: <<http://onlinehelp.microsoft.com/en-us/bing/jj684589.aspx>>.
- Arama motorları nasıl çalışır? Bkz.: <<http://web.archive.org/web/20160509142554/http://www.bbc.co.uk/guides/ztbjq6f>>.
- BM Çocuk Hakları Sözleşmesinin ilgili maddeleri:

Madde 13 – Çocukların, kendilerine veya başkalarına zarar vermediği sürece, bilgi alma ve paylaşma hakkı vardır.

Madde 16 – Çocukların mahremiyet hakkı vardır. Yasa onları, yaşam tarzlarına, namuslarına, ailelerine ve evlerine karşı yapılacak saldırılardan korumalıdır.

Madde 17 – Çocuklar kitle medyasından güvenilir bilgi alma hakkına sahiptir. Televizyon, radyo ve gazeteler çocukların anlayabileceği bilgi sunmalı ve çocuklara zarar verecek içeriği sunmamalıdır.
- İlgili Avrupa Konseyi dokümanları:
 - Bakanlar Komitesinin üye Devletlere yönelik “Arama motorları ile ilgili olarak insan haklarının korunması” hakkındaki CM/Rec (2012)3 sayılı Tavsiye Kararı: <https://wcd.coe.int/ViewDoc.jsp?id=1929429&Site=CM&BackColorInternet=C3C3&BackColorIntranet=EDB021&BackColorLogged=F5Q383>.
 - Bakanlar Komitesinin üye Devletlere yönelik “İnternet filtreleri ile ilgili olarak ifade ve haber alma özgürlüğüne saygı duyulmasını teşvik edecek önlemler” hakkındaki CM/Rec(2008)6 sayılı Tavsiye Kararı: <<https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282008%296&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFB-B55&BackColorLogged=FFAC75>>.

Web’de kaliteli bilgiyi bulmak



İnternetin icadının arkasında yatan temel fikir, bilginin kolaylıkla erişilebildiği ve dağıtıldığı elektronik bir kütüphane geliştirmektir. Bu amaca birçok şekilde ulaşılmıştır: günümüzde internet, dünyanın dört bir tarafındaki kamu ve özel kütüphanelerden oluşan muazzam bir kütüphane olarak işlev görmektedir. Bunlar, hizmetler, programlar ve faaliyetler hakkında bilgi vermekte ve kataloglarında yer alan ve internet üzerinde sipariş edilebilen kitaplara erişime imkan vermektedir. Sayısal kütüphaneler, genellikle web sayfasının görüntüsünü veren html script şeklinde, Word veya PDF dosyası olarak veya düz metin (ASCII) olarak sayısallaştırılan çevrim içi kitaplara ve koleksiyonlara erişim vermektedir. Bazı önemli kütüphaneler ve müzeler nadir kitapların ve koleksiyon eserlerin sayısal versiyonlarını taramanıza izin vermektedir⁷.

1. http://www.livinginternet.com/i/ij_summary.htm

2. http://www.livinginternet.com/i/ij_summary.htm

3. <https://en.wikipedia.org/wiki/HTML>

4. <http://en.wikipedia.org/wiki/Html>

5. <http://www.census.gov/main/www/pdf.html>

6. <http://en.wikipedia.org/wiki/ASCII>

7. <http://www.bl.uk/manuscripts/Default.aspx>

■ İnternet, bilgi sunmada kütüphanelerin de ötesine giderek, sizin ilgilendiğiniz güncel olaylar, teknoloji, hobiler, eğlence, sanat, spor ve daha fazlası hakkında ne varsa güncellenmiş ve güvenilir bilgi sunabilmektedir. Bu durum, aralarında 24 saat yayın yapan haber kanalları, gazeteler, dergiler ve çoğunlukla haber kaynakları veya RSS kaynakları (zengin site özetleri, bkz. www.whatissrss.com) olarak bilinen çok sayıda web siteleri ve sosyal medya platformları vasıtasıyla çalışan haber toplayıcılarının bulunduğu geniş çaplı kaynaklar kullanmak vasıtasıyla mümkün olmaktadır. Kullanıcılar, çevrimiçi gazeteler, bloglar, podcastler ve videobloglardan (vlogs) elde edilen web içeriğini tek bir noktadan kolayca düzenli bir şekilde alabilmek amacıyla bunlara abone olurlar.

■ Günümüzde birçok Avrupalı ulusal ve uluslararası haberleri internet üzerinden takip etmekte ve interneti sağlıklı bilgi almak için kullanmaktadır. Haberleri sosyal medya platformlarından almak giderek büyüyen bir akımdır. Haber tartışma forumları ve haber grupları, tartışma için verimli ortamlar ve güncel konular hakkında çeşitli bakış açıları almak açısından bir araç olarak hizmet etmekte ve aynı zamanda öğrencilerin tartışma becerilerini geliştirmektedir. Bu tür yüzlerce binlerce forum bulunmaktadır ve daha faal olan gruplar her gün yüzlerce haber mesajı almaktadır. Mesajlar, gönderenin adının ve mesajın gönderildiği zamanın kaydedildiği ve gösterildiği konulara göre ayrılmaktadır. Günümüzde birçok sunucu ve tarayıcı sizi öğrencileriniz için ilgi çekici olacak forumlara yönlendirebilir¹¹.

■ Twitter, internetten güncellenmiş bilgileri alma yollarından birisidir. Kendi Twitter adresinizi, ilgilendiğiniz alandaki haber kuruluşlarını, gazetecileri, uzmanları takip etmek için kullanabilir veya bir Twitter listesine kaydolup isimsiz bir şekilde takip edebilirsiniz. Google Alerts, benzer şekilde belirli konulardaki haberleri takip etmek için kullanılabilir ancak anahtar kelimeler dikkatli ve açık bir şekilde tanımlanmadığı takdirde faydalı olabilecek çok sayıda uyarı alabilirsiniz. Sosyal medya platformları, devamlı olarak sizin dünya haberlerini takip etmenizi sağlayacak yeni işlevler eklemektedirler.



EĞİTİMDEKİ ÖNEMİ

- Geleneksel ve çevrimiçi kütüphanelerde dolaşmak için gerekli araştırma becerileri benzerdir. Çocukların internete ilk adım attıkları andan itibaren bu becerileri öğrenmeleri ve uygulamaları için ebeveynleri ve öğretmenleri tarafından yönlendirilmeleri çok önemlidir.
- Web üzerinde özellikle müfredat alanlarını ve konuları ile ilgili <http://viib.org> ve <http://sldirectory.com/libsf/resf/libplans.html> binlerce özel kategorilerde kütüphaneler bulunmaktadır. Esas itibarıyla WebQuests, girdi ve materyallerin çok büyük bir yüzdesinin internet tarafından sağlandığı küçük projelerdir. Webquests, üzerinde öğretmenin karar verdiği öğrenme faaliyetine bağlı olarak öğretmen tarafından veya öğrenen kişi tarafından yapılabilir. <<http://webquest.org/>> adresindeki model, sınıftaki katılımcılar için internet üzerindeki kütüphane imkânları kullanmalarında ve aynı zamanda araştırma, arşivleme, okuryazarlık, analiz ve değerlendirme gibi bir dizi temel becerileri geliştirmek açısından faaliyetler tasarlamalarında çok faydalı olabilir.
- Haber grupları ve tartışma forumları, gençleri çeşitli farklı kaynaklara başvurmak suretiyle kendi doğrularını kontrol etmeye teşvik etmek şartıyla eleştirel düşünme ve tartışma becerilerini geliştirmek açısından oldukça faydalı kaynaklardır. Gençler aynı zamanda başkalarının tecrübelerinden öğrenmek ve bilgi paylaşmak için bir platform da sunabilirler.

1. http://wwitv.com/news_tv_live/

2. <http://www.onlinenewspapers.com>

3. <http://www.e-journals.org>

4. <http://www.newsforum.com>

5. <https://en.wikipedia.org/wiki/Twitter>

6. <https://www.teachingenglish.org.uk/article/webquests>



ETİK HUSUSLAR VE RİSKLER

- Çerezler (çevrimiçi cihazınızda siz ve tercihleriniz hakkında bilgi depolamak için bırakılan küçük dosyalar) tercihlerinizi hatırlayarak veya belirli sitelere yapacağınız her ziyarette kaydolmanızı önleyerek tarama tecrübenizi geliştirebilir. Buna karşılık, çerezleri kullanan arama motorları sizi sadece benzer mantıktaki sitelere yönlendirecek ve sizin haber hikâyeleri ve güncel konularla ilgili bakış açınızı zamanla daraltacaklardır.
- İnternet, her yaştan insana aktif olarak içeriğe katkıda bulunma fırsatı vererek demokratikleşmiş bir gazeteciliğe imkân tanır. Bu nedenle internette sunulan bilgi sonsuz hale gelmektedir, bu nedenle, kaliteli olan ile güvenilir olmayan içerik arasında ayırım yapabilmenin ve bilgi ile hedeflenen bilgiye benzer reklam türü olan ticari tanıtım arasında ayırım yapabilmenin önemi de vurgulanmalıdır.
- Haber grupları veya tartışma forumlarının çok azı bir moderatör tarafından bütünüyle yönetilmekte ve kullanıcılar izlenmemektedir. Bu nedenle, bu tür forumlar, telif hakkına tabii materyalin dağıtımı, ırkçı propaganda, aşırıcılık veya çocukların cinsel istismarını içeren materyallerin dağıtımı gibi yasadışı faaliyetler amacıyla istismar edilebilirler. Sundukları sözde anonimlik, çirkin ve saldırgan (*flaming*) mesajlar göndermek ve zorbalık (*bullying*) benzeri anti-sosyal bir davranışa yol açabilmesi sebebiyle bu tür platformları kullanmak belli bir düzeyde sorumluluk ve makul toplumsal uzlaşılardan farkındalığını gerektirir. Öğrenciler bu tür forumları¹⁵ kullandıklarında mahremiyet konularını da hatırlamaya yönlendirilmelidirler.
- Birçok kütüphane erişime belirli kurallara göre izin vermektedir. Bu kurallar en azından kullanıcının materyalin telif hakkı ilkesine saygı göstermesini gerektirir. Eğer materyaller kamuya açık değilse, yayıncının izni olmadan dağıtamayacağınızı veya yayınlamayacağınızı aklınızda tutun. Telif hakkı aynı zamanda kişisel bir sorumluluktur. İntihal bir başkasının çalışmasını kaynak belirtmeden kullanmaktır. Kaynaklarınızı belirttiğinizden emin olunuz ve öğrencilerinize bu alışkanlığı aşılayınız.



NASIL?

- Usenet¹⁷, isimleri hiyerarşik olarak konularına göre sınıflandırılmış bir dizi “haber gruplarından” oluşan dünya çapında yaygın bir tartışma sistemidir. Bu haber gruplarına erişim, internet service sağlayıcınız¹⁸ (ISS) veya okul, üniversite veya işyeri sunucunuz tarafından tanımlanmaktadır. Bazı platformlara erişim ücretsizken, bazıları “özel tarifeli” hizmetler abonelik esasına göre çalışır.
- Bir haber veya RSS bildirimi sayfası oluşturmak için çeşitli araçlar mevcuttur. “Hazırlanın: haberleriniz için bir akış oluşturun¹⁹” başlıklı video ihtiyaçlarınıza en iyi uyacak araçları nasıl kullanacağınızın adım adım açıklamasını sunmaktadır.
- Google Alert programını kurmak için öncelikle bir Google hesabı yaratmanız gerekir. Daha sonra bir kelime listesi hazırlayabilirsiniz, diğer birkaç parametreyi belirleyin ve bu terimler çevrimiçinde görüldüğünde Google Alert elektronik posta yoluyla sizi bilgilendirecektir. Teriminizle ilgili güncellemeleri gösteren bir URL listesi alacaksınız ya da bir RSS bildirimine tercihinize bağlı olarak bir alarm ekleyebilirsiniz.
- Sınıfınızda güncel bir konu kullanarak, bir kütüphane kategorisini <http://vlib.org> adresinde belirleyiniz. Bu kütüphanedeki kaynaklardan bir webquest programı oluşturduğunuz veya <http://webquest.org/> ve <http://www.spirited.ca/teacherresources/default.asp> adreslerindeki mevcut bir webquest programını kullandığınızı düşünün. Bir arama motoru kullanarak webquest programlarını bulabilirsiniz. Webquest programınızı Google Alert programını kurarak veya bir Twitter listesine bağlanarak zenginleştirebilir ve her birinden elde ettiğiniz bilginin kalitesini karşılaştırabilirsiniz.
- Yetişkinler, çocuklar ve gençler, İskoçya’da yerleşik Uluslararası Kütüphaneler Dernekleri ve Kuruluşları (IFLA) adresi üzerinden kaliteli haber web sitelerine ve faaliyetlerine ulaşabilirler. Bu haber web siteleri, sanat ve tarihten, bilim ve matematiğe kadar çok geniş bir yelpazede konu sunmaktadır. Diğer konuları Amerikan Kütüphaneler Derneğinin bir bölümü tarafından geliştirilen “Great websites for kids/Çocuklar için Büyük web siteleri” başlıklı sitede bulabilirsiniz. Kütüphane ve bilişim hizmetleri hakkında daha fazla bilgi, kütüphane ve bilişim mesleğinin küresel sesi olarak kabul edilen IFLA’nın sitesinde bulunmaktadır.

8. <http://en.wikipedia.org/wiki/Flaming>

9. <http://www.webwewant.eu/information>

10. http://web.archive.org/web/20160102210205/http://www.gallowglass.org/jadwiga/SCA/libraries.html#Copyright_Plagiarism

11. <http://en.wikipedia.org/wiki/Usenet>

12. [https://en.wikipedia.org/wiki/Server_\(computing\)](https://en.wikipedia.org/wiki/Server_(computing))

19. <http://web.archive.org/web/20151231202307/http://www.pcmag.com/article2/0,2817,2458165,00.asp>

20. http://en.wikipedia.org/wiki/Search_engine

21. <http://media.twitter.com/best-practice/create-and-use-twitter-lists>

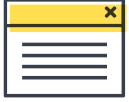
22. <http://www.ifla.org/activities-and-groups>

23. <http://gws.ala.org>



İYİ UYGULAMALAR

- Öğrencileri çevrimiçi kütüphaneleri kullanmaya teşvik etmeden önce, temel kütüphane becerilerini ve araştırma stratejilerini²⁴ gözden geçirdiğinizden emin olunuz. Öğrencilerin telif hakkının korunması konusunda sağlam bir anlayışa sahip olduklarından da emin olunuz.
- Dosya indirmek için kullanılmakta olan her cihazda, anti-virüs filtresi olduğundan emin olunuz. Dosyaları okulun sunucusuna indirmeden önce²⁵, okul ağ yöneticinizle yeterli koruma ile dosyaları depolamak ve uygun bir şekilde arşivlemek²⁶ için yeterli alan olup olmadığını kontrol ediniz.
- Sınıfınız için bilgi araştırma ödevleri belirlerken, kullanmaları için kendi URL²⁷ listenizi vermeniz akıllıca olacaktır. Bu şekilde adreslerin çalıştığından ve içeriğin uygun olduğundan emin olabilirsiniz.
- Telif hakkını korumak amacıyla indireceğiniz birçok dosya Adobe PDF formatında olacaktır. Bu nedenle, öğrencilerinizin bu dosyaları açabilmesini sağlamak için Acrobat Reader programının en son sürümünü indirdiğinizden ve yüklediğinizden emin olunuz. Bu Adobe Systems²⁸ sitesinden yapılabilir.
- İnternet kullanırken uygulayacağınız temel güvenlik ilkeleri çevrimiçi kütüphaneleri kullanırken de uygulanmalıdır. Gizlilik açıklamalarını ve kullanım koşullarını kontrol ediniz ve dosyaları virüslere karşı tarayınız.
- Bir haber grubuna katıldığınızda, rehber ilkeler açısından sıkça sorulan soruları²⁹ kontrol ettiğinizden emin olunuz. Bu size haber grubunun kuralları hakkında bir fikir verecektir. Farklı haber gruplarının farklı kuralları vardır.
- Mesajlarınızı mümkün olduğu kadar kısa tutunuz, ancak tüm ilgili bilgileri verdiğinizden emin olunuz. Örneğin teknik bir soruyla ilgili bir cevap arıyorsanız, kullandığınız donanım ve yazılım hakkında açık ayrıntılar veriniz.



DAHA FAZLA BİLGİ

- Google haber gruplarının <http://groups.google.com/> adresinde haber gruplarının tamamının bir listesi ve 1 milyardan fazla posta kaydının arşivi bulunmaktadır.
 - David Lawrence ve Russ Albery, Big 8 haber grubu oluşturma hakkında tavsiyeler vermektedir:
<<http://web.archive.org/web/20140330141231/http://www.faqs.org/faqs/usenet/creating-newsgroups/part1/>>.
 - Wikipedia'nın haber grupları için girişi vardır: <<http://en.wikipedia.org/wiki/Newsgroups>>.
 - İngiliz Kütüphanesi (British Library) dijitalle geçirilmiş koleksiyonlarını sunmaktadır: <<http://www.bl.uk/manuscripts/Default.aspx>>.
 - Dünya e-kitap Vakfı binlerce metni sunmaktadır: <<http://www.netlibrary.net/>>.
 - Library Spot ücretsiz sanal kütüphane merkezidir: <<http://www.libraryspot.com/>>.
 - "Teacher tap" 1000'den fazla webquests ve ilgili kaynakların listesine sahiptir: <<http://eduscapes.com/tap/topic4.htm>>.
- Gençlik yayınlarında "the Web we want" sitesinin "Malumat bilgi değildir" bölümü, <http://www.wewant.eu/web/guest/information> onlu yaşlardakilerin eleştirel düşünme ve gazetecilik becerilerini güçlendirmeleri için gerekli etkileşimli faaliyetleri sağlar.

24. <https://www.pinterest.com/explore/library-skills/>

25. <http://www.walthowe.com/glossary/d.html#download>

26. http://en.wikipedia.org/wiki/Archiving#Computing_sense

27. <http://en.wikipedia.org/wiki/URL>

28. <http://www.adobe.com/products/acrobat/readstep2.html>

29. <http://en.wikipedia.org/wiki/Faq>

Uzaktan Öğrenim ve MOOCs



Uzaktan öğrenim, öğrenci ve öğretmenlerin fiziksel olarak bir sınıf içinde bir arada bulunmadıkları resmi bir eğitim sistemidir. Teknolojinin gelişmesine bağlı olarak uzaktan eğitim de geliştiği için eğitim süreci elektronik medya vasıtasıyla gerçekleşmektedir. Artık öğretmen ve öğrencilerin; e-posta, mesajlaşma, video-konferansı, sohbet odaları, ilan panoları vb. vasıtasıyla içerik değişimi yaptıkları sanal sınıflar görmekteyiz.

■ Kullanılan teknolojiye bakılmaksızın, uzaktan eğitim her ülkeden ve her yaştan öğrencilere yaşam boyu öğrenme fırsatları sunan ve onların dünyadaki hemen hemen bütün çevrimiçi üniversitelerden diploma, sertifika ve ünvan almalarını mümkün kılan kanıtlanmış bir yöntem olarak görülmeye devam etmektedir. Öğrenciler ayrıca yüzlerce veya hatta binlerce kilometre uzakta yerleşik olan diğer öğrencilerle -veya öğretmen(ler)le öğrenimi kesinlikle zenginleştiren bir öge olan tartışmaları yapabilmektedirler.

Uzaktan öğrenim 1800'lü yılların ortalarında evde, orduda veya işte çalışıp, ileri eğitim arayan yetişkin nesillerle başlamıştır. Dersler eskiden geleneksel posta sistemi yoluyla, malzeme gönderip alarak yapılan yazışmalarla gerçekleştirilmiştir. Buna karşılık günümüzde, uzaktan öğrenim güncel teknolojinin avantajını kullanarak evrilmiştir. Uzaktan eğitim, internet vasıtasıyla gelişmiş ve öğrenciler, fiziki bir sınıfa ayak basmadan derece için çalışabilmektedir.

■ Uzaktan öğrenim günümüzde, yukarıdaki klasik tanımdan, kitlesel açık çevrimiçi kurslara, bire bir You Tube eğitimi ve web seminerlerinde (webinar), Periscope ile sanal alan gezilerine kadar değişen farklı biçimlerde mevcuttur. Her ne kadar teknoloji hızla gelişse de, uzaktan öğrenimin temeli, eğitim vermek olarak kalmaya aynen devam etmektedir.



UZAKTAN ÖĞRENİM TÜRLERİ

MOOCs (Kitlesel açık çevrimiçi dersler)

- MOOCs ilk olarak 2008 yılında devam kısıtlaması olmadan ders almak isteyen herkese Internet vasıtasıyla içerik sağlamak amacıyla başlatılmıştır. Öğretmenler ve öğrenciler arasında değişime izin vermek üzere etkileşimli topluluk forumları oluşturulmuştur.
- 2012 yılı itibarıyla MOOC dersleri resmi eğitim kuruluşları tarafından desteklenmeye başlanmıştır ve kar amaçlı bir eğitim teknoloji şirketi olan Coursera aracılığıyla Stanford Üniversitesi, Princeton Üniversitesi, Michigan Üniversitesi ve Pennsylvania Üniversitesi gibi benzeri üniversitelerde MOOC dersleri bulunabilir.
- Diğer başarılı MOOC programları arasında yer alan ve bir diğer Stanford Üniversitesi paydaşı olan Udacity, ile Massachusetts Teknoloji Enstitüsü ve Harvard Üniversitesi tarafından kurulan bir MOOC sağlayıcı olan edX'i de kapsamaktadır.
- MOOC dersleri öğretmen-öğrenci modeline dayalıdır. Buna karşılık You Tube ise eşitler arası (peer to peer) uygulanan bir başka uzaktan öğrenim modeli geliştirmiştir.

Eşitler Arası Eğitim (Peer to peer)

- Eşitler arası eğitim, bireylerin kendilerine benzer geçmişleri olan meslektaşlarından öğrendikleri oturumlar olarak tanımlanabilir. Örnek olarak çocukların çocukları eğitmesi, avukatların avukatları eğitmesi vb.
- Bu ortak öğretme modülü, milyonlarca aboneli You Tube “öğretmenlerinin” yazılım öğreticileri, web sitesi tasarım öğreticileri, makyaj öğreticileri, yazma öğreticileri ve binlerce diğer konunun öğreticileri You Tube üzerinde kolaylıkla bulunabilir.

Web seminerleri (Webinar)

- Webinar veya web tabanlı seminerler da internette bulunabilir. Koçlar, eğitimciler, guru'lar ve bilgi paylaşmak isteyen herkes bir web semineri sunabilir.
- Web semineri formatları; sunumlar, dersler, Power Point sunumları, video, atölye çalışması malzemeleri ve diğer hususları içerebilir.
- Web seminerleri daha sonraki bir tarihte çalışmak üzere indirilebilecek malzemeleri de içerebilir.

Periscope

- Periscope, insanların sizin gördüğünüzü gerçek zamanda görmesine izin veren bir yayıncılık uygulamasıdır. Uygulama ilk yıllarında benzersiz bir başarı kazanmıştır ve eğitimciler hala kullanışlı uygulamaları araştırmaktadır.
- Bazı eğitimciler, sanal alan gezilerinin, sınıflarını paylaşmanın veya öğrenci izleyicilerden gerçek zamanda sorular almanın kullanışlı olduğuna inanmaktadır. Buna karşılık bu gelecekte izlenecek bir uzaktan öğretim aracıdır.

■ Uzaktan öğrenimdeki gelişmeler ilkokuldan yüksek öğretime kadar ki öğrenme ortamlarında köklü değişiklik yapmıştır. Örneğin;

- Dersler, kesintisiz ortam vasıtasıyla veya eğitimcinin sunucusundaki² dosyalara kaydedilen basılı malzemelerle verilebilmektedir.

1. http://en.wikipedia.org/wiki/Streaming_media
2. http://en.wikipedia.org/wiki/Web_server

- Öğrenciler öğretmenle ve birbirleriyle mesaj panosu³, e-posta⁴ veya sohbet⁵ vasıtasıyla iletişim kurmaktadır.
- Açık eğitim kaynakları, eğitim, öğretim ve değerlendirmenin yanı sıra araştırma amaçları için kullanışlı belgeler ve medyadan (genellikle açık-lisanslı) oluşmaktadır. Açık eğitim kaynakları, öğretmenlerin diğer okullarla, eğitimcilerle ve kıtalarla içerik kullanmalarını ve değişim yapabilmelerini mümkün kılmamanın bir diğer yoludur. Açık eğitim kaynakları, öğretmen olmayan uzmanlar tarafından da belirli konularda üretilebilir ve açık eğitim kaynakları havuzundan kolaylıkla seçilebilir ve paylaşılabilir⁶.
- Yukarıda bahsedilen araçlar “teknolojik sınıfların” artışına yol açmıştır; öğretici bir strateji ve karşık bir eğitim türü, geleneksel eğitim düzenlemesini sınıf dışında genellikle çevrimiçi öğretici bir içerik sağlamak suretiyle tersine çevirmiş ve geleneksel anlamda ev ödevi olarak değerlendirilenler de dâhil olmak üzere etkinlikleri sınıfa taşımıştır. Edutopia⁷’daki araçlar hakkında daha fazla bilgi alın.
- Öğrenciler ödevlerini, genellikle ücretsiz bir hizmet olan ve kayıtlı kullanıcıların güvenle dosyalarını sakladıkları, senkronize ettikleri ve seçtikleri herhangi biriyle kolaylıkla paylaştıkları bulut tabanlı dosya paylaşım programı drop box’a indirebilirler. Hatta ani sınavlar ve yazılı sınavlar bilgisayar ortamında yapıp çevrimiçi alınabilir.
- Kitlesel açık çevrimiçi dersler (MOOC) ve uzaktan öğretim ile ders malzemeleri her zaman kolayca bulunabilmekte ve kolaylıkla güncellenebilmektedir. Bunun yanı sıra bu yeni eğitim ortamı formatları kendi kendine eğitim için eşsiz bir esneklik sağlamaktadır.



UZAKTAN ÖĞRETİMİN ÖNEMİ

- İnternet sanal bir eğitim ortamı kurmak için mükemmeldir. Örneğin, öğrenciler yurtdışında sanal bir üniversitede eğitim görürken kendi şehirlerinde oturabilir veya çalışan öğrenciler ise eğitim zamanlarını okul ve iş yeri arasında farklı yerlerle geçirebilirler.
- Öğrencilerin öğrenme malzemelerinin tümüne erişim sağlamaları, onlara öğrenme süreçlerinde daha bağımsız olma fırsatı verecek ve ne öğrendiklerini ve niçin öğrendiklerini daha iyi kavramalarını sağlayacaktır.
- Öğrenciler kendi eğitimlerine daha fazla sahiplenecekler ve öğretmenin görevi de bir koçun görevine dönüşecektir.
- Dersler “normal” okul veya üniversitelerin açılış saatleri ile kısıtlı olmadığından herkes yaşam boyu öğrenci haline gelmek için daha çok fırsattan faydalanacaktır.
- Uzaktan öğretim, hem öğrencinin hem de öğretmenin davranışını değiştirmektedir. Başarılı öğrenciler devamlılık ve organizasyona dayalı becerilerini geliştirir ve dolayısıyla öğretmenler ise teknoloji konusunda daha deneyimli olmak zorundadırlar.



ETİK HUSUSLAR VE RİSKLER

Onay Belgesi

- Onaylanmış ve onaylanmamış programları ayırt etme becerisi dersi verenin yasal olup olmadığını belirlemek açısından faydalıdır.
- Uzaktan öğretim için onay kimlikleri çok geniş bir alanda ortaya çıkmaktadır ve eğitim fırsatlarının eşitliğinde önemli bir adımı temsil etmektedir.
- Programlar, gerçek bir onayları olmaması ancak çok iyi bilinen ve yerleşmiş üniversitelerle ortak olmaları durumunda genellikle bir tür beceri doğrulaması gerçekleştirirler.

3. https://en.wikipedia.org/wiki/Internet_forum

4. <https://en.wikipedia.org/wiki/Email>

5. https://en.wikipedia.org/wiki/Online_chat

6. <https://www.oercommons.org>

7. <http://www.edutopia.org/blog/flipped-learning-lets-talk-tech-jon-berghman>

8. <https://wiki.mozilla.org/Badges>

Öğretmen ve fakülte

- Uzaktan öğrenim ehil öğretmenlere sahip olma temel gereksinimini değiştirmez. Esasen, eğitimde ortaya çıkan eğilimlere ayak uydurabilmek için daha fazla eğitim fırsatları verilen öğretmenlere ihtiyaç olduğunun altı eskisinden daha fazla çizilmektedir.
- Yüz yüze eğitimin değeri inkâr edilemez ancak teknolojinin faydaları ve eğitim de önemlidir.
- Herkesin kendi seminer web sitesini (webinar) veya eşitler arası (peer to peer) çevrimiçi ders açması ve hatta kendilerini “uzman” olarak tanımlamaları nedeniyle eleştirel düşünme kullanıcılar için olduğu kadar web içeriğinin diğer çeşitleri için de çok önemlidir.



NASIL

■ Bir derece veya başka bir uzaktan eğitim programı seçerken belirli önlemleri alma hususunda kullanıcı olarak kendinizin sorumlu olduğunuzu bilmelisiniz. İzlemeniz gereken bazı hususlar şöyledir:

- Yasal olanların yanında güvenilirmez uzaktan öğretim kuruluşları olduğunu da unutmayınız. Kayıt olmadan önce programı/kuruluşu araştırdığınızdan emin olunuz;
- İnternet’te yapılan her tür bilgi alışverişinde, güvenlik konuları her zaman kilit durumdadır. Virüsler (Güvenlik hakkındaki Kılavuz 19’a bakınız) ve bilgisayar korsanları uzaktan öğretim sistemi üzerinde büyük zarara yol açabilirler. Bu yüzden hangi önlemleri almanız gerektiği hususunda mahremiyet hakkındaki Kılavuz 9’a, güvenlik hakkındaki Kılavuz 19’a başvurunuz.
- Telif hakkı¹⁰ genellikle öğrencinin kendi ülkesindeki kanunlarla korunur. Buna karşılık diğer ülkelerdeki uzaktan öğretim programlarını takip ederken eğitim kaynaklarının uluslararası telif hakkı ile korunduğundan emin olunuz.



SINIF ÇALIŞMASI İÇİN FİKİRLER

- Öğrencileri bir grupta “öğretmen” ve diğer grupta “öğrenci olmak üzere iki gruba ayırınız. Öğrencilerin bir ders konusunu araştırmalarını ve belirlenen konu ile ilgili olarak bir uzaktan öğrenim çeşidinin diğerinden neden daha iyi olduğunun sebeplerini bulmalarını sağlayınız.
- Öğrencilerin araştırma konusu ve uzaktan öğrenim yöntemi üzerine karar vermelerinden sonra, “öğretmen” grubunun ideal ders gereksinimlerini araştırmalarını sağlayın ve “öğrenci” grubundan da aynıyı yapmalarını isteyin. Öğrencilerin ve öğretmenlerin ihtiyaçlarını mukayese edin.
- Bir uzaktan öğrenim yöntemi seçin ve ne tür bir sertifika verildiğini araştırın ve kontrol edin. Saygıdeğer bir kuruluş mu? Hangi göstergeler bir kuruluşun saygıdeğer olduğunu gösterir? Kuruluş sertifika veya kimlik kartı veriyor mu?
- Eğitim uygulamaları ve dersleri arasındaki farkı tartışınız. Her ikisi de engelli bireyler için yeni öğrenme fırsatlarını nasıl sağlayabilir?
- Öğrencileri sevdikleri bir alanla ilgili bir başlık hakkında kendi kısa eğitim kursunu oluşturmaya davet edin ve diğer öğrencileri de bu kursu almaya teşvik edin. Bu tecrübeden yola çıkarak sınıfın çevrimiçi eğitimi daha etkili hale getirecek kıstaslar listesini hazırlamasını sağlayın.



İYİ UYGULAMALAR

- İnternet öğrenme şeklimizi değiştirmektedir ve öğrencilerin öğrenmelerine yardımcı olacak bütün bilgilere ve araçlara erişiminin olması çok önemlidir.

9. [https://en.wikipedia.org/wiki/Hacker_\(computer_security\)](https://en.wikipedia.org/wiki/Hacker_(computer_security))

10. <http://en.wikipedia.org/wiki/Copyright>

- Sayısal uçurum, birçok ülkenin ekonomik ve sosyal büyümesinde en önemli konu olarak görülmektedir ve uzaktan öğretimin kullanılması bu eşitsizliği azaltacaktır. Buna karşılık, muhalif görüşe göre, eğer sayısal bir eşitsizlik varsa ve insanlar İnternete (ve uzaktan eğitime) erişemiyorlarsa, uçurum genişleyecektir.
- Uzaktan öğretim, öğrenci eğitimini ölçülebilir şekilde artırabilir. Bu, ayrıca öğrenciler, onların ailelileri ve öğretmenleri için uygulama yaparak İnternet eğitimi de sağlar.
- Uzaktan öğretim öğrencilerin yeni beceriler ve nitelikler geliştirmesi ve yeni yönlerle doğru gelişmesi için fırsat sağlar.
- Uzaktan öğretim, ayrıca daha önce sınıfa devam edememiş engelli öğrencilere erişim sağlayabilir. Öğrenciler çevrimiçi sınıfa katılabilir ve diğer öğrenciler ve öğretmenle fikir alışverişini yapabilirler.



DAHA FAZLA BİLGİ

- Uzaktan Öğrenim Portalı dünyadaki uzaktan öğretim programları ve kuruluşları hakkında bilgi sağlar: <http://www.distancelearningportal.com/>.
- Uluslararası Açık ve Uzaktan Eğitim Kurulu, uluslararası kuruluşlar hakkında bilgi sağlar: <http://www.icde.org/>.
- Avrupa Eğitim Bakanları konsorsiyumu olan European Schoolnet, öğretmenler için Açık Eğitim Kaynakları (OER) havuzu sağlar: <http://reforschools.eun.org/web/guest>. Ayrıca özel ihtiyaçlar için eğitim kaynakları sağlar: <http://reforschools.eun.org/web/guest7sennet>.

11. https://en.wikipedia.org/wiki/Digital_divide

ÇEVİRİMİÇİ ALIŞ-VERİŞ



E-ticaret; ürünlerin çevrimiçi satışına izin veren hizmetlerin, yazılımın ve yöntemlerin birleşimi olarak tanımlanabilir. Kitaptan tatile, giysiden elektroniğe kadar neredeyse her şey çevrimiçinde satın alınabilir. Somut eşyalardan ayrı olarak çevrimiçi içeriğe erişim gibi hizmetler için de ödeme yapabilirsiniz.

■ E-ticaret şüphesiz olumlu faydalar getirmiştir çünkü alışveriş kolaylaşmış ve daha güvenilir olmuştur, ancak e-ticaret işlemleri risksiz değildir. Endüstri büyüdükçe faydaları ve riskleri de artmaktadır.

■ Son günlerdeki bir eğilim, giderek daha fazla çocuğun 18 yaşına ulaşmadan veya bir öğrenci için uygun yarı zamanlı bir işi olmadan çevrimiçi satın almalar (sıklıkla bir ebeveynin kredi kartı hesabını kullanarak) yaptığını göstermektedir. Çocukların parayı “sanallaştırdıkları” ve değerini anlayamaz hale geldikleri, ki bu durum onların gelecekleri açısından çok önemli bir ekonomik etkisi olabilecektir, hakkında bir endişenin artmasına yol açmıştır.



UYGULAMA-İÇİ SATIN ALIM

- Uygulama-içi satın alım (in-app purchasing) belirli bir uygulama veya “app” içerisindeki ürünlerin veya hizmetlerin satışını kolaylaştıran akıllı bir telefon veya mobil cihaz özelliği anlamına gelmektedir.
- Her ne kadar uygulama-içi satın alım işletmelere karlılık getirse de, bu uygulamanın nasıl çalıştığını anlamayanlar için sorun olabilmektedir.
- Uygulama-içi satın alımlar, satın alım yapmaya ehil olmayan ancak sadece birkaç tıkla bunu yapabilen çocuklar ve genç tüketiciler için bir sorun teşkil etmektedir.



TÜKETİCİ HAKLARI

- Çevrimiçi bir ürün veya hizmet satın alırsanız, teslimatın belirlenen zamanda yapılması, beğenilmeyen ürünlerin iadesinin yapılması ve sadece açık bir şekilde satın almaya karar verdikleriniz için ödeme yapılmasının da dâhil olduğu tüketicinin korunması kurallarından faydalanırsınız. Örneğin, Avrupa Birliği içerisinde beğenilmeyen ürünleri teslim alındıktan sonra 14 gün içerisinde iade hakkınız vardır.
- Çevrimiçi bir ürün veya hizmet satın alırsanız, satıcı, satın alımı yapmanızdan önce ürün veya hizmet hakkındaki açık, doğru ve anlaşılabilir önemli bilgileri size vermek zorundadır.
- Önemli bilgilerin bir listesi için aşağıda yazılı Avrupa Birliği web sitelerine bakınız.



KONULARIN ANLAŞILMASININ ÖNEMİ

Çocuklar ve gençlerin tüketiciler olarak iyi bilgilendirilmeleri, çevrimiçi alışveriş yapmak için uygun olup olmadıklarını, alışveriş için gereken kural ve şartları ve bir sorun olması durumunda haklarını nasıl koruyacaklarını bilmeleri gerekmektedir. Çevrimiçi alışveriş önem kazandıkça çocuk ve gençlerin, nasıl çevrimiçi alışverişle bağlantılı riskleri önleyecek ve faydalarından yararlanabilecek sorumlu tüketiciler olacaklarını anlamaları önemlidir.

- Bilgilendirilmeyen tüketiciler, özellikle gençler ve yaşlılar çevrimiçi sahtekârlıklara ve çevrimiçi alışveriş dolandırıcılığına karşı daha korunmasız olabilirler.
- E-ticaret içindeki alıcılar ve satıcılar genellikle birbirlerini tanımazlar ve bu durum insanları doğruyu yanlıştan ayırt etme hususunda duyarsızlaştırabilir.



ETİK HUSUSLAR VE RİSKLER

- Kredi kartı bilgilerinizi, telefon numaranızı ve diğer kişisel bilgilerinizi koruyunuz. Bilgisayar korsanları bilgisayarınıza erişerek veya bilgilerinizin bulunduğu güvensiz web sitelerini kırarak kredi kartı bilgilerinizi elde edebilirler. Kredi kartı bilgilerinizi kaydetmeyi soran web sitelerinden sakınınız çünkü bu bilgi çalınabilir.
- Kamuya açık Wi-Fi bağlantısı kullanarak ödeme yapmaktan kaçınınız. Kahvehaneler, oteller, havaalanları ve hatta kamuya açık parklara yerleştirilen bağlantı noktaları birçok yerde mevcut olması sebebiyle, korsanlar bu bağlantı noktalarına sızabilir ve kişisel bilgilerinizi çalabilirler.
- Aynı zamanda suçlular da insanları aldatarak kredi kartı veya banka bilgilerini gönüllü olarak vermelerini sağlayabilirler. Avlamak bu kategoriye girer. Bu tür saldırılar genellikle çevrimiçi alışveriş veya ödeme sitelerinin kullanıcılarını ayrıntıları “tekrar onaylamalarını” isteyerek hedef alır.
- Çevrimiçi alışveriş genelde kredi kartı ile ödeme yapılmasını içerdiğinden, tüketiciler aşırı harcamadan kaçınmak için harcamalarını dikkatlice yönetmelidir. Dikkatsiz bir şekilde alışveriş yapmadığınızdan ve izniniz dışında bir alışveriş olmadığından emin olmak için düzenli olarak kredi kartı ekstrenizi gözden geçiriniz.

1. <http://www.techopedia.com/definition/27510/in-app-purchasing>
2. <http://en.wikipedia.org/wiki/Phishing>

- “Gerçek olamayacak kadar güzel” tekliflere dikkat edin. Teklifin geçerli olup olmadığını teyit etmek için satıcının sitesine bakınız.
- İnternet; PayPal, Bitcoins, Para Transferi, mobil ödemeler vb. değişik birçok ödeme yöntemlerini içerir. Hiçbir ödeme yönteminin tamamen güvenli olmadığını aklınızda bulundurun ve böylece herhangi bir ödemeyi çevrimiçinde yaparken daima dikkatli olun.



NASIL?

— Güvenli bir şekilde çevrimiçi alışveriş yapmak için tüketiciler çevrimiçi alışverişte ilave önlemlere ihtiyaç olduğunu hatırlamalıdır.

- Sadece bilinen satıcılardan alışveriş yapın. Giderek daha fazla satıcının pazara girmesi nedeniyle bu zor olabilir ancak araştırmanızı yapın.
- Bilgisayarınızın, tabletinizin veya akıllı telefon ayarlarınızın en iyi düzeyde olduğundan emin olunuz.
- Sipariş kontrol alanınızın şifreli olup olmadığını doğrulayınız. Birçok site SSL (güvenli soket katmanları) teknolojisini kullanır. Güvenli olduğunu gösteren kilit ikonu ve web sitesi adresine bakınız. “http” yerine “https” olmalı.
- Siparişinizin bir kopyasını ya bir çıktı ya da ekran görüntüsü almak suretiyle saklayınız. İtiraz durumunda bunu kanıt olarak kullanabilirsiniz.
- Yapmadığınız bir satın alımın tarafınıza faturalandırılmaması için belgelerinizi sıklıkla kontrol ediniz.



SINIF ÇALIŞMASI İÇİN FİKİRLER

- Öğrencileri satıcı ve satış koşulları hakkında araştırma yapmaları için eğitiniz.
- Öğrencileri tek başına veya gruplar halinde, belli bir amaç dâhilindeki ürün veya hizmetler için özel ticari web sitelerini ziyaret etmelerini isteyiniz. Örneğin, sabit bir bütçeye uygun bir tatil planlaması (Bkz. Kılavuz 10 Bilgi araştırması).
- Öğrencilerinizle bir e-ticaret sitesi (örneğin okul ürünlerini satmak için) veya okul kapsamında daha önceden başlatılmış bu tür mevcut girişimler hakkında gelişmiş bir çalışma planlayınız. İyi bir e-ticaret web sitesinin yapısını çalışınız.



İYİ UYGULAMALAR

- Satıcı veya tedarikçi hakkında araştırma yapınız. Örneğin eBay tedarikçilerin geçmiş performanslarına ve geri bildirimlerine uygun olarak ticari güvenilirlik oluşturmalarına izin verir. Güvenilir olmayan kaynaklardan, özellikle spam yoluyla reklamı yapılanlardan alışveriş yapmayınız (Bkz. Kılavuz 19).
- Kredi kartlarınızın hileli kullanıma karşı sigortalı olduğundan emin olunuz. Yetkiniz dışındaki her türden alışverişler için, hesap özetlerinizi dikkatli bir şekilde kontrol ediniz.
- Kuralları ve şartları okuyunuz. Metin uzun ve teknik olabilir ancak eğer okumadıysanız, okudum ve anladım kısmını tıklamayınız.
- Gizli maliyetleri kontrol ediniz. Satıcı tarafından ödenmesi gereken vergiler veya kargo ücretleri olabilir. Eğer yurt dışından sipariş veriyorsanız, gümrük vergi ödemeleri de kapsamda yansıtılabilir.
- Site güvenli mi? Web tarayıcısının sağ alt köşesindeki asma kilit veya anahtar sembolü güvenli siteleri gösterecektir. Verinin gönderilmeden önce şifrelenmesini güvence altına alan SSL (güvenli soket katmanları) sertifikalarını arayınız.

3. http://en.wikipedia.org/wiki/Secure_Sockets_Layer

- Kişisel verilerinizin kontrolünüz altında olduğundan emin olunuz ve daha iyi anlamak için Genel Veri Koruma Düzenlemesine başvurunuz. Satıcının verilerinizi saklama veya pazarlama amaçlı sizinle temas kurma seçenekleriyle ilgili kutulara dikkat ediniz.
- Eğer bir web sitesinin ciddiyeti hakkında şüphemiz varsa çevrimiçinde bazı araştırmalar yapmak için tereddüt etmeyiniz ve diğer tüketicilerin görüşleri, değerlendirmeleri ya da deneyimlerini araştırınız. Trustpilot gibi web siteleri, genelde web sitelerinin ve müşteri deneyimlerinin ciddiyeti hakkında iyi bir göstergedir⁴.



DAHA FAZLA BİLGİ İÇİN

- Avrupa Birliği'nin çevrimiçi alışveriş ile ilgili web sitesini ziyaret ediniz: http://europa.eu/youreurope/citizens/shopping/buy-sell-online/rights-e-commerce/index_en.htm.
- Öğrencilerinize örneğin Microsoft'un sitesinden çevrimiçi alışveriş yapmayı öğretiniz: <http://web.archive.org/web/20050405134258/http://www.microsoft.com/office/previous/frontpage/columns/edcolumn04.asp>.
- ECC-Net, AB tüketicilerinin haklarının anlaşılmasını teşvik etmekte ve ağı içindeki bir başka ülkeden seyahat esnasında veya çevrimiçi alışverişle yapılan satın alımlar hakkındaki şikâyetlerin çözülmesine yardımcı olmaktadır: http://ec.europa.eu/consumers/solving_consumer_disputes/non-judicial_redress/ecc-net/index_en.htm.
- TrustArc (önceden TRUST), çevrimiçi işlemlerde itimat ve güvenilirlik tesis etmeyi amaçlayan bağımsız, kar amacı gütmeyen küresel bir girişimdir: <https://www.trustarc.com>.
- Europa.eu sitesi çevrimiçi alışverişle ilgili bilgi sunmaktadır: http://europa.eu/youreurope/citizens/consumers/shopping/index_en.htm.
- Genel Veri Koruma Yönetmeliği hakkında bilgi için bkz.: http://ec.europa.eu/justice/data-protection/index_en.htm.
- Paypal dolandırıcılık önleme tavsiyeleri: <https://www.paypal.com/eBay/cgi-bin/webscr?cmd=p/gen/fraud-tips-buyers-outside>.
- Ekonomik İşbirliği ve Kalkınma Örgütü'nün (OECD) 2016 yılında kabul ettiği E-Ticarette Tüketicinin Korunması hakkında Tavsiye Kararı hakkında bilgi için bkz.: <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>.

4. <https://www.trustpilot.com/>

4. Herkes için İnternet

”Yaratıcılık bilinenlerden kopma cesaretini gerektirir”

Erich Fromm, Psikolog

KILAVUZ 14, İNTERNET ÜZERİNDE VİDEO, MÜZİK VE GÖRÜNTÜLER

Tekrar kullanmak istediğiniz her içeriğin lisansını kontrol ediniz.

Çevrimiçi oluşturduğunuz ve postaladığınız içerik üzerinde Creative Commons sınıflamasını kullanınız.

Beğendiğiniz sanatçı, müzisyen veya içerik oluşturucusunun içeriği için ödeme yapmanıza imkân verecek adil çevrimiçi iş modellerini destekleyiniz.

KILAVUZ 15 YARATICILIK

Bir görüntü binlerce kelime ifade eder, özellikle kendimizin veya başkalarının özel bilgileri hakkında dikkatli değiliz.

Sahip olduğunuz yaratıcı esere yönelik başkalarının saygı göstermesini nasıl güvence altına alacağınızı biliyor musunuz?

İntihal, eser oluşturanın sahipliğine saygı duymamakta ve toplumun çeşitli katmanlarında sorunlara sebep olabilmektedir. İntihalin toplum üzerinde oluşturabileceği çok çeşitli etkilerinin farkında mısınız?

KILAVUZ 16 – OYUNLAR

Yaşamın dengesi önemlidir. Çevrimiçinde oyunlara harcadığınız zaman dışarıda veya yüz yüze yapacağınız faaliyetlerinize zarar veriyor mu?

Çevrimiçi oynadığınız oyunlar sizin yabancılarla tanışmanızı ve iletişim kurmanıza yol açtığında herkesin kendini tanıttığı kişiler olmayabileceğini unutmayın. Küçük yaştaki çocuklar için önceden seçilebilecek tümcecikler vasıtasıyla “İnsan tarafından yönetilen oyunları” veya “güvenli sohbet” içeren oyunları seçiniz.

Uygulama içi satın alımlar bazı oyunlarda sizin dikkatsizliğinize yönelik bir tuzak olabilir. Kılavuz 13’deki ipuçlarını kontrol ettiniz mi?

KILAVUZ 17 - SAYISAL VATANDAŞLIK

Çevrimiçi haklarınızı ve sorumluluklarınızı biliyor musunuz?

Sayısal parmak izinizi son zamanlarda kontrol ettiniz mi? İsminizi bir arama motoruna yazınız ve neler çıktığına bakınız.

Tam anlamıyla bir sayısal vatandaş olmak için gerekli sayısal beceriler nelerdir?

KILAVUZ 18 – SAYISAL EBEVEYNLİK: OLUMLU VE ETKİN

Bu yeni sayısal çağda ebeveynlik yaparken olumlu olun ve çocuklarınızın arkadaşlarıyla çevrimiçinde neler yaptıkları, çevrimiçi nerelere gittikleri ve kimlerle konuştukları hakkında olabildiğince en iyi iletişimi kurun.

Her ne kadar teknoloji büyük bir hızla gelişmiş olsa da, ebeveynlik büyük oranda aynı kalır: çocuklarınızın yaşamında faal olmak, onları iyi birer “sayısal” vatandaş olmaya teşvik etmek ve nezaket ve empatiyi vurgulamak.

İster küçük bir çocuğun ister bir ergenin ebeveyni olun, teknolojiyle ilgili olarak çocuğunuzun gelişiminde karşılaşılabilecek sıkıntıların farkında olun. Teknolojiyi, çocuğunuzun gelişimine engelleyecek şekilde değil, yardım edecek şekilde kullanın.

İnternet Üzerinde Video, Müzik ve Görüntüler



Çoklu iletişim ortamı olarak İnternet, ses dosyaları, görüntü dosyaları ve sayısal fotoğrafların da dâhil olduğu çok sayıda iletişim şekli sunar. Uygulamalar ve çevrimiçi platformlar, dil, kültür ve ulusal sınırları aşmak ve sadece kişisel bilgilerin (bkz.: Kılavuz 9 - Mahremiyet) açığa çıkarılmasını değil, aynı zamanda telif hakkı ihlalleri ve yasadışı veya zararlı içerik benzeri önemli hususlarda farkındalığı artırmak suretiyle bu tür içeriğin üretimini ve dağıtımını büyük ölçüde kolaylaştırmıştır.



TELİF HAKKI

- Çok sayıda uluslararası yasa ve anlaşma yürürlüktedir. 1996'da 100'den fazla ülke, sayısal içeriğe¹ hitap eden Dünya Fikri Mülkiyet Kuruluşu (WIPO) anlaşmalarının ikisini imzalamıştır: <<http://www.wipo.int/treaties/en/>>.
- Görsel-işitsel malzemelerin yaratıcısı olan bir kişi, kendisi feragat etmediği takdirde otomatik olarak telif hakkına sahiptir.

- Ülkelerin birçoğunun yasası, yaratıcının ölümünden 50-70 yıl sonrasına kadar telif hakkını muhafaza etmektedir.
- Bir müzik parçasının genellikle birden fazla telif hakkı sahibi vardır. Söz yazarı, icracı, plak şirketi ve yayımcı bütün haklara veya “komşu haklara” sahip olabilir.
- Ekonomik unsurun yanı sıra, görsel-işitsel bir içeriğin yaratıcısının “etik hakları” da vardır. Bu eserin yaratıcısı olarak tanınma hakkı ve eserin izin alınmadan değiştirilme veya yayınlanması hakkı ile ilgilidir.
- Müzik eserleri ve filmler çevrimiçi satın alınabilirler (Bkz. Kılavuz 13 çevrimiçi alışverişi). Çevrimiçi müzik eseri satın almak için çok sayıda site vardır; örneğin iTunes ve Amazon. Müzik, görüntü veya video satın almak için başka çevrimiçi mağazalarda bulunmaktadır. Bu nedenle, bunları bulmak için arama yapma konusunda kendinizi özgür hissediniz⁵.
- Çevrimiçi film veya müzik eseri satın almak, genellikle sınırlı bir şekilde kopyalama veya dağıtma hakkı verir veya hiçbir hak vermez. Örneğin, Apple firmasının çevrimiçi müzik mağazası iTunes, satın alınan bir müzik eserinin bir hanede en fazla beş tane bilgisayara indirilmesine izin vermektedir.
- Çoklu medya içerik tüketimi değiştikçe yeni iş modelleri ortaya çıkmaktadır. Bir şarkıyı satın almak yerine bir çevrimiçi akışlı platforma aylık abonelik ücreti ödeyebilir ve o platformda mevcut her şarkıyı dinleyebilir veya her filmi seyredebilirsiniz. Bu tür hizmetlere örnek olarak, filmler için Netflix ve müzik için ise Spotify’ı gösterebiliriz. Ayrıca birçok farklı platform olduğundan arama yapma hususunda rahat olunuz.
- Müzik endüstrisi, hem eşitler arası yazılım firmalarına hem de bireysel dosya paylaşıcılara karşı hukuki işlem başlatmıştır. Dosyaları indirmeye uygun hale getirenlerin, dava edilme olasılığı bu dosyaları bilgisayarlarına indirenlere nazaran daha fazladır.
- Creative Commons⁸, telif hakkının tümünü karşılamak amacıyla alternatif sunan kâr gütmeyen bir kuruluştur.



ETİK HUSUSLAR VE RİSKLER

- Hâlihazırda sayısal müzik satışları, 2014 yılında % 6,9’luk bir artışla plak endüstrisinin toplam satışlarının %46’sına karşılık gelmektedir. Bu durum, sayısal müzik satışları veya akışlı yayınları için olan yasal kuruluşların çoğalmasından dolayıdır. (Bkz: <https://www.ifpi.org/facts-and-stats.php>)
- Müzik endüstrisi korsanlıkla mücadele için web sitelerine ve bireysel kullanıcılara karşı çok sayıda dava açmıştır.
- Eşitler arası yazılımları kullanmak bilgisayarınız açısından güvenlik riski oluşturabilir çünkü kötü amaçlı yazılım programları müzik ve görüntü dosyalarına eklenerek dağıtılmaktadır.
- Çoklu medya içeriği tüketimi İnternetle beraber oldukça değişmiştir. En beğendiğiniz CD’yi tekrar tekrar dinlemek yerine, İnternet kullanıcıları İnternetin kendilerine sunduğu muazzam seçenekler arasında çok çeşitli şarkı ve melodileri dinlemek isterler. Ortalama bir Amerikalı her gün üç buçuk saat müzik dinlemektedir. İşin garip yanı, korsanlık, bir albümün tamamını satın alma şeklindeki “geleneksel” iş modelini abonelik usulüne dayalı sınırsız akışlı yayın platformlarına tercih etmeye zorlayarak endüstriye katkıda bulunmuştur. Akışlı bir yayın platformu seçiminde alacağınız kararların bu iş modelini desteklemeye yardımcı olacağını unutmayınız.

1. https://en.wikipedia.org/wiki/Moral_rights

2. <http://www.apple.com/itunes/>

3. <http://www.amazon.com/>

4. <http://www.apple.com/itunes/overview/>

5. <https://www.netflix.com>

6. <https://www.spotify.com>

7. <http://creativecommons.org/>

8. <https://en.wikipedia.org/wiki/Peer-to-peer>

9. http://www.digitalstrategyconsulting.com/intelligence/2014/10/us_media_consumption_trends_music_tops_the_charts.php



EĞİTİM

Eğitim kuruluşlarının, bazı durumlarda, eserleri yeniden uyarlamalarına ve kamuya iletmelerine izin verilir. Ulusal mevzuatınıza veya 22 Mayıs 2001 tarihli 2001/29/EEC numaralı Direktife bakınız. Bu durumda aşağıdaki koşulların karşılanması gerekir:

- Kullanılacak eserler, yalnızca eğitim veya bilimsel araştırma amaçlı olmalıdır.
- Kaynaklar, yazarın adı da dâhil olmak üzere, mümkün olmayan haller dışında belirtilmelidir.
- Bu tür bir içeriğin kullanılmasından dolayı hiçbir şekilde doğrudan veya dolaylı olarak ekonomik kazanç elde edilmemelidir.

Çocukların veya gençlerin çevrimiçi fotoğraflarını yayınlamadan önce ebeveynlerinden veya velilerinden yazılı izin alınız.

İçeriğin okul web sitesinde yayınlanması durumunda, bütün içerik, çocukların ve gençlerin yaptıkları da dahil olmak üzere, okulun yetkisi ve sorumluluğu altındadır.



SINIFTA

- Etik konular üzerinde tartışma yapınız. Görsel-işitsel eser korsanlığı hırsızlık mıdır?
- Çocuk ve gençleri, Internet'ten dosya indirme durumunda virüslerin ve casus yazılımların riskleri hakkında bilgilendirin.
- Çocuk ve gençleri, telif hakkı olan müzik ve film eserlerini Internet'ten indirmeleri durumunda para cezası olasılığı hakkında bilgilendirin.
- Çocuk ve gençlerin takımlar halinde sanatsal/yaratıcı çalışma yapmalarını sağlayın. Bu bir şiir yazma, resim yapma, hikâye yazma, video hazırlama veya şarkı bestelemek olabilir. Onlara Creative Commons lisansına bakmalarını ve içeriklerine uygulamak istedikleri lisansı seçmelerini söyleyin. Bunu yaptıklarında, seçtikleri lisansı ve neden seçtiklerine ilişkin kararlarını paylaşmalarını sorun. Örneğin, ürettikleri eserleri satma niyetinde oldukları için çok sınırlı bir lisans seçmiş olabilir veya eserlerini değiştirilmeye ve yeniden kullanmaya açık bırakmayı tercih etmiş ve eserlerinin bir başkası tarafından yeniden kullanılacağı veya değiştirileceğini tam olarak kavramış olabilirler.



YASADIŞI İÇERİK

- Yasadışı içeriğin tanımı ülkeden ülkeye değişmektedir ancak çoğunlukla çocuk pornografisi veya çocuk istismar malzemesi, aşırı şiddet, siyasi aşırılık, hakaret veya azınlık gruplarına karşı nefrete kışkırtmak anlamlarına gelmektedir.
- Birçok ülkede yasadışı içeriği rapor etmek için özel telefon hattı vardır. Inhope, ulusal şikâyet telefon hatları ağıdır. Yasadışı içeriğe karşı eyleme geçmek, içeriğin yapısı ve sunucunun bulunduğu yerden dolayı zor veya yavaş olabilir. Şikâyet hatları, Internet Servis Sağlayıcıları ve polis ile birlikte çalışırlar ve yasadışı içerikle mücadelede en iyi yerlerdir.
- Çoğu çevrimiçi platform yasadışı içeriği tanımlamak ve etkisiz hale getirmek için insan ve/veya otomatik moderasyon, foto/video DNA teknolojisi ve raporlama mekanizmaları gibi çeşitli yöntemler kullanmaktadırlar.
- Zararlı ve yasadışı içeriği tartışın. Araştırmalar, öğrencilerin çoğunun bu tür içeriği Internet'te bilinçli olarak veya tesadüfen bulunduğunu, ancak çok azının bunu yetişkinlere söylediğini göstermektedir

ETİK HUSUSLAR VE RİSKLER



- Yasadışı içerik telif hakkından daha ciddi kriminal bir suçtur. Telif hakkında “adil kullanım” gibi ve kar gütmeyen veya eğitsel amaçlar için istisnalar olsa da yasadışı içerik, özellikle çocuk cinsel istismarı veya terörizm malzemeleri her zaman ciddi bir kriminal suç olarak kabul edilecektir. İfade özgürlüğü gibi çeşitli özgürlüklerin sınırlarının sınanması insanoğlunun doğal bir özelliğidir ancak özellikle çocuk ve gençler için geçilmemesi gereken belirli sınırlar vardır.
- Yasadışı içerik genellikle yasadışı silah veya hap satışı gibi diğer yasadışı eylemlerle bağlantılıdır. Bu faaliyetlerin çoğu “dark net” olarak adlandırılan ve internetin geleneksel arama motorları ile erişilemeyen bölgesinde gerçekleşmektedir. Yasadışı içerik yayınlama, paylaşma veya arama kolaylıkla kartopu misali ciddi bir suça dönüşebilir.

- Okulunuzda veya şirketinizde, telif hakkı ve yasadışı materyal hakkındaki konuları içeren kabul edilebilir bir kullanım politikası veya alternatif olarak sorumlu kullanım politikası olmalıdır.
- Kullanmak istediğiniz bir içerik bulduğunuzda lisansını kontrol ettiğinizden emin olunuz. Çok çeşitli lisanslar bulunmaktadır. Düzenli internet kullanıcıları tarafından üretilen içerik çeşitli lisanslarla birlikte gelir. En “açık” lisans, sahibini bilgilendirme ihtiyacı olmadan ticari projelerde bile içeriği yeniden kullanmanıza ve değiştirmenize izin verir. Uygun kredi tahsisine tabi diğer lisanslar, kullanımı kar gütmeme şartına bağlamakta veya değişiklikleri yasaklamaktadır. Google veya Bing benzeri arama motorları görüntü ve video aramalarını lisansa göre filtrelemeyi önermektedir. Bunun yanı sıra projelerinizde kullanacağınız içeriği satın alabileceğiniz çok sayıda platform bulunmaktadır.
- İçeriğinize telif hakkı lisansı uyguladığınızdan emin olunuz. Örneğin bir plak şirketi gibi geleneksel telif hakkı içinden seçebilirsiniz veya oluşturduğunuz materyal için başkalarının nasıl kullanacağını açıklamak üzere Creative Commons sınıflandırmalarını kullanabilirsiniz.
 - Her ne kadar “ücretsiz” çevrimiçi müzik, görüntü veya video aramak çekici olsa da, unutmayın, öyle ya da böyle ya sınırsız reklama maruz kalma ya da verilerinizi çalabilecek kötü amaçlı yazılımları bilgisayarınıza bulaştırma veya hak sahiplerinin dava açması sonucu her zaman bir ödeme yaparsınız. İyi hizmet sunan ve ödenen paranın karşılığını veren platformları desteklemek, internetin biçimlendirilmesine, zaman harcayan reklamlarla, düşük kaliteli ve zararlı içerikle doldurulmasından kaçınmaya ve sanatçıların çalışmalarından dolayı adil şekilde ödüllendirilmelerine katkı sağlamaktadır.
- Günümüzde dünya üzerindeki kullanıcılar her gün yoğun şekilde içerik üretmektedirler. Bunlar, You Tube veya Dailymotion benzeri video platformlarına yüklenen kısa videolar, sosyal ağlara konulan resim ve görüntüler veya müzik platformlarına yüklenen müzik parçaları olabilmektedir. Bunları yükleyen kullanıcının bir lisans belirtmiş olup olmamasına bakılmaksızın, yüklenen her içeriğin korunduğunu aklınızda tutunuz. Ancak yazarın açık bir şekilde üretmiş olduğu içerik üzerindeki haklarını kaldırdığını belirtmesi halinde, telif hakkı kanunu uygulanmaz.
- İçerik kullanımı üzerindeki bir diğer sınırlama veri korumadır. Örneğin, utanç verici bir video veya resmi birisine göndermek, bir başkasının veri mahremiyetini ihlal etmek ve siber zorbalık anlamına gelebilir. Genel bir kural olarak, eğer içeriği kullanacak, değiştirecek, başkasına gönderecekseniz, daima söz konusu içeriği yerleştiren kullanıcının iznini alın. İzin almak ve gerekli hakkın verilmesi, yasal bir yükümlülüğün ötesindedir. Bu, çevrimiçi yaratıcı ve katılımcılık için olumlu ve cazip bir ortam yaratılmasına yardımcı olur. Veri koruması ile ilgili ayrıntılı bilgi için AB’nin “AB veri koruma kuralları reformu¹³” başlıklı Adalet sitesini ziyaret ediniz.



İYİ UYGULAMALAR

- Yazılım filtreleri bazı yasadışı web sitelerini engellemeye yardımcı olabilir ancak hiçbir zaman gerçek çözüm değildir. Yasadışı içeriği önceden önlemek isterseniz hiçbir filtre sizi koruyamaz.
- Bir ebeveyn, öğretmen veya daha büyük kardeş olarak çevrimiçi tecrübeler hakkında aile ve sınıf tartışmalarını harekete geçirdiğinizden emin olun. Yasadışı içerik sadece bir telif hakkı konusu değildir, genellikle zararlı veya şok edici içerik, kötü amaçlı yazılım, spam veya benzer şeylerden oluşur.
- Yasadışı bir içeriği bir yardım hattına (bkz aşağıda INHOPE) bildiriniz veya kullandığınız platform tarafından sağlanan bildirim mekanizmalarını kullanınız.
- Okulunuzun yasadışı içerikle ilgili katı bir politikası olmasını ve çocuk ve gençlerin yasadışı içeriği yayınlama, paylaşma veya izlemenin olası sonuçları hakkında uygun bir şekilde bilgilendirilmesini sağlayınız.
- Zararlı ve yasadışı içeriği tartışınız. Araştırmalar birçok çocuk ve gencin bu tür içeriği internette bilerek veya tesadüfen bulunduğunu ancak çok azının bunu bir yetişkine söylediğini göstermektedir.

10. <http://creativecommons.org/>

11. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

FURTHER INFORMATION



- Telif hakları ve benzeri konular için Dünya Fikri Mülkiyet Örgütü (WIPO) web sitesini ziyaret ediniz: <http://www.wipo.int>.
- Beğendiğiniz müzik grubunun müzik korsanlığı hakkında ne söylediğini:” Sanatçılar müzik korsanlığı hakkında konuşuyor” sitesinden öğreniniz: <https://www.upvenue.com/article/1590-musician-stances-on-music-piracy.html>.
- INHOPE, İnternet’te yer alan yasadışı içeriği bildirmek için kullanılan şikâyet hatları ağıdır: <http://www.inhope.org/gns/home.aspx>.
- Avrupa Konseyi’nin medya sayfası, telif hakkı alanındaki çalışmalar ile ilgili bilgi içermektedir: <http://www.coe.int/media>.
- Avrupa Komisyonu web sayfası fikri mülkiyet hakları ile ilgili bilgi sağlamaktadır: http://europa.eu/youreurope/business/start-grow/intellectual-property-rights/index_en.htm.
- Dünya çapında kayıt endüstrisini temsil eden Uluslararası Fonografik Endüstrisi Federasyonu (IFPI) internet üzerinde güvenle ve yasal bir şekilde müzik arama konusunda ebeveynlere ve öğretmenlere yardım etmek için rehberlik sunmaktadır: <http://www.ifpi.org/music-and-the-internet-guide.php>.
- Avrupa Komisyonunun Avrupa için Sayısal Gündemi, telif hakları konusunda daha fazla tavsiye sunmaktadır: <https://ec.europa.eu/digital-agenda/en/copyright>.
- Dark net (karanlık ağ) ile ilgili daha fazla bilgi için Wikipedia sayfasına bkz.: <https://en.wikipedia.org/wiki/Darknet>.
- BM Çocuk Hakları Sözleşmesinin ilgili maddeleri:

Madde 13 - Çocukların, kendilerine veya başkalarına zarar vermediği sürece bilgi alma ve paylaşma hakkı vardır.

Madde 17 - Çocukların kitle medyasından güvenilir bilgi alma hakkı vardır. Televizyon, radyo ve gazeteler çocukların anlayabilecekleri bilgi sunmalı ve çocuklara zarar verecek içeriği desteklememelidir.

Madde 33 - Hükümetler çocukları tehlikeli ilaçlardan koruyacak yolları temin etmelidir.

Madde 34 - Hükümetler çocukları cinsel istismardan korumalıdır.

Madde 36 - Çocuklar kendi gelişimlerine zarar verebilecek her türlü faaliyetlerden korunmalıdır.

Madde 37 - Hiç kimsenin çocukları zalimce ve kötü bir şekilde cezalandırmasına izin verilmez. Suç işleyen çocuklar acımasız bir şekilde muamele görmemelidir. Yetişkinlerle aynı hapisaneye konmamalı ve aileleriyle görüşmelerine izin verilmelidir.

Madde 40 - Kanuna karşı gelmekle suçlanan çocukların yasal yardım alma ve haklarına saygılı bir adalet sistemi içerisinde adil yargılanma hakları vardır. Hükümetlerin, kriminal olarak sorumlu olmayacak çocuklar için asgari bir yaş sınırı belirlemeleri ve adil ve hızlı yargılama veya alternatif süreçler için asgari garantileri sağlamaları gerekmektedir.



İNTERNET YARATICILIĞI NASIL GELİŞTİRİR?

— Internet'in esnek yapısından dolayı, günümüz sınıf ortamı eskisinden daha az katıdır. Hızla gelişen teknoloji öğrencilere ilgilendikleri konuları araştırmaları ve geleneksel olmayan şekillerde öğrenmeleri için gereğinden fazla olanak tanımaktadır (bkz. Kılavuz Metin 3 -Web 2.0, 3.0 ve dahası).

— Öğrenciler, modern teknolojinin sağladığı araçları kullanarak, dünyanın her yerindeki izler kitle için yayınlanmak üzere profesyonel standartlarda malzeme yaratabilirler. Kendi çevrimiçi ürünlerini üretebilir ve sınıf içerisinde veya Internet aracılığıyla diğer öğrencilerle etkileşimli olarak her tür deneyi ve canlandırmayı gerçekleştirebilirler.

— Internet, küreselleşmiş bir eğitime sahiptir ve öğrencilere dünya üzerindeki bütün akranlarına eş zamanlı olarak erişme imkânını sağlamaktadır. Genç internet kullanıcılarının bu imkânları tam olarak kullanabilmeleri için sadece tüketici değil, aynı zamanda yaratıcı olmaları önemlidir. Bu günümüzde birçok ülkede uygulanmakta olan kodlama girişimlerinin (örneğin bkz. <http://codeweek.eu>) altında yatan amaçtır.



EĞİTİMDE YARATICI SÜREÇLERİN DESTEKLENMESİ

- Teknolojinin sınıf ile başarılı bir şekilde bütünleşmesi, öğrencilere icatlarını, bireyselliklerini ve yaratıcılıklarını gösterme ve girişimcilik kapasitelerini geliştirme fırsatı sunar.
- Yaratıcı yazılımlar ve internetin kullanımı sınıfta motivasyonu artırır ve öğrenmeyi anlamlı bir şekilde geliştirir. Kodlama, teknolojinin nasıl çalıştığı hakkında daha derin bir anlayış geliştirilmesine yardımcı olur, ve dolayısıyla daha sorumlu kullanıcı stratejilerin geliştirilmesine katkıda bulunur.
- Yaratıcılığın ifade edilmesi ve öğrenme sürecinde daha faal bir görev alma fırsatı, bağlılığı ve katılımcılığı teşvik eder - ki bunlar, vatandaşlığın iki önemli temel taşıdır.
- İnternet ve mobil teknoloji öğrenciler ve öğretmenler için kendi görsel-işitsel içeriklerini yaratmak ve yüklemek açısından heyecan verici imkânlar sunmaktadır. Aynı zamanda, interneti dünyanın her yerindeki sanatçılarla temas kurmak, eserleri hakkında tavsiye ve görüş almak için kullanabilirler. Sanatçılar, atölye çalışmaları düzenlemek için video konferans araçlarını ve sanal toplantıları kullanabilir (bkz Kılavuz 12 Uzaktan Eğitim).
- Sınıf içi öğrenimde sosyal medya ve belirli sosyal platformların kullanılması, öğrencileri ortak projelerde birlikte çalışmaya ve çevrimiçi işbirliği yapmaya teşvik eder. Bu durum, yaratıcı duygularını gösterme şansı sağlar ve bu şekilde yapacakları beyin fırtınası, yaratıcı süreci canlandırabilir.



ETİK HUSUSLAR VE RİSKLER

- **Eşitlik konuları:** Herkesin internete erişim için gerekli donanımı ve bağlantısı var mı? Yaşlarına, becerilerine ve özel ihtiyaçlarına bakılmaksızın, dünyadaki bütün çocuk ve gençler yaratıcı olmak için fırsatlardan eşit faydalanabiliyorlar mı? Bir başka deyişle, yaratıcı olmak için gerekli mevcut teknolojiyi nasıl kullanacaklarını biliyorlar mı?
- **Çevrimiçi güvenlik faktörü:** Genç kullanıcıları, özellikle çok küçük yaşlardaki çocukları ve özel ihtiyaçları olanları korumak için yerleştirilen filtreler, yaratıcı olmak için gerekli materyale erişimi engelliyor mu? Öğrencilerin ihtiyaç duydukları güvenli erişimin tadını çıkarabilmeleri için bu durumla nasıl başa çıkılabilir? (Bkz. sınıflandırma ve filtreleme başlıklı Kılavuz 20).
- **Öğretmenlerin eğitim ihtiyaçları:** Öğrencilerin internet bilgisi çoğunlukla öğretmenlerden daha fazla olabilir. Öğretmenlerin, mobil telefon kullanımı da dâhil olmak üzere, bilişim ve iletişim teknolojisinin (BIT) bütün unsurları ile ilgili olarak öğrencilerini doğru bir şekilde yönlendirebilmeleri için kendilerine sunulan bütün eğitim fırsatlarından yararlanmaları gerekir (bkz. Mobil teknoloji başlıklı Kılavuz 5 ve uzaktan eğitim başlıklı Kılavuz 12).
- **Teknik destek unsuru:** Program ve projelerin engellenmemesi amacıyla okullarda yeterli teknik destek olması gereklidir.
- **Ara Bellek Ortamı:** Yaratıcılık kişinin duygularını birey olarak ifade etmesine imkân tanır. Her ne kadar, gençlerin yaratıcı süreçlerinin önüne her türlü sınırlama getirmekten kaçınmamız gerekse de, onların yarattıklarıyla ilgili olarak özellikle beyin fırtınası yapılan grup ortamlarında hoşgörü, empati ve saygı ilkelerinin altının çizilmesi önemlidir. Bir çalışmanın yapıcı bir şekilde yönlendirilmesi için bir öğretmen veya sınıf başkanının hazır bulunması gereklidir.
- **Mahremiyet:** Web 2.0 ve 3.0, fotoğrafların ve görüntülerin internete yüklenmesini oldukça kolaylaştırmıştır. Öğrenciler, tek bir görüntünün binlerce kelimeyi anlattığını ve kendilerinin ve başkalarının özel bilgilerinin riske girebileceğinin farkında olmalıdırlar.
- **Telif Hakkı:** Gençler, küçük yaşlardan başlayarak yaratıcı ürünlerin sahipliğine saygı duymayı öğrenmelidir ve intihalin topluma neye mal olduğunu anlamalıdır.⁵

1. <http://web.archive.org/web/20080614214250/http://www.netlingo.com/right.cfm?term=video%20conferencing>

2. <http://www.eun.org/teaching/smile>

3. <http://www.etwinning.net>

4. https://en.wikipedia.org/wiki/Content-control_software

5. <https://www.teachingcopyright.org/handout/copyright-faq.html>



SINIFTA YARATICILIĞI ÜST SEVİYEYE YÜKSELTMEK

- Webquest⁶ programı, İnternet’i sınıfla bütünleştirmek için sorguya dayalı bir yaklaşımdır.
- Öğrenciler, kodlamanın temellerini öğrenmek suretiyle kendi web sitelerini kurarak, yaratıcılıklarını zorlayabilirler. Bu, onların yaratıcı düşünme süreçlerini, grafikler ve içeriğe yönelik girdiler talep etmeleri suretiyle farklı şekillerde destekler.
- Öğrenciler, çevrimiçi hikâyeler ve diğer içeriği üretme yoluyla yazma ve görsel-ışitsel yapım becerilerini geliştirecek projelerde kendi aralarında işbirliği yapabilirler. Örneğin, cep telefonları yabancı ülke öğrencileriyle birlikte kendi ülkelerinin kültürel ve mesleki unsurlarının video ve görüntülerini kaydetmek ve birbirleri arasında paylaşmak için kullanılabilir. Bu öğrencilerin; mahremiyet, fotoğraf izinleri ve benzeri konulara ilişkin pratik yapmaları yoluyla öğrenmelerine yardımcı olur.
- Öğrencileri “Hot Potatoes” gibi yazılımı olan web siteleri için etkileşimli sınavlar ve faaliyetler veya at Quita’s web sitesinde mevcut olan yazılımı kullanarak çok çeşitli sonuçları olan etkileşimli hikâyeler yaratmaları için teşvik ediniz
- Orta öğretim ve üniversite öğrencileri, kendi üç boyutlu öğrenme ortamlarını, Active Worlds¹⁰ gibi yazılımlar kullanarak yaratabilirler. Kendi ideal alanlarını veya sanal yerleşkelerini inşa edebilirler. Ayrıca başka öğrencilerle farklı konularda projelerde işbirliği yapabilirler.



İYİ UYGULAMALAR

- İnternet farklı konularda gerekli bilgi edinmek için temel bir araştırma aracı olarak kullanılabilir. Öğrenciler, yaratıcılığı teşvik eden ödevlerde kazandıkları bilgiyi, daha sonra uygulamaya koyabilirler. Teknoloji, öğrencilere daha üst düzeyde düşünme yeteneği geliştirmeleri için fırsat ve özgürlük sağlar.
- İnternet ve diğer modern teknolojiler, farklı ülkelerden ve kültürlerden gelen öğrenciler arasında güçlü bir iletişim ve işbirliği sağlar. Öğrencilerin, geçmişe nazaran daha fazla, kendi yaşlıları ile yaratıcı çözümler bulmaya yönelik beyin fırtınası yapma fırsatları vardır.
- Açık kaynaklı yazılımlar, dünyanın her yerindeki öğrencilerin, özellikle imkanları daha dar olan ailelerin çocuklarının yaratıcılıklarını ücretsiz olarak ortaya koymalarına imkân sağlamaktadır. Open Office, Gimp, Audacity veya Blender benzeri yazılımlar, çocukların belgeler yaratmasına, görüntüleri ve ses dosyalarını düzenlemelerine ve hatta 3 boyutlu animasyonları ücretsiz almalarına imkân tanımaktadır. Ayrıca açık kaynaklı yazılımlar, kullandığınız yazılımı geliştirmeniz ve güncelleniz amacıyla gönüllü kodlayıcılar topluluğuna katılarak kodlamayı öğrenme ve becerilerinizi paylaşma fırsatı sunar. Çocuklarınız/öğrencilerinize bu tür seçenekleri gösteriniz.
- Öğretmenler, sınıfta uygulamalı alıştırma yoluyla teknolojiyi uygulamanın öğrencilere problem çözümü ve yenilikler açısından fırsatlar sunduğunu tespit etmişlerdir.
- Öğrenme hedeflerini akılda tutmak gereklidir: bu hedeflere ulaşmanın yolu, ürünün kendisinden ziyade nasıl elde edileceği sürecine odaklanmaktır.
- Öğrenciler çevrimiçi yaratıcı faaliyetlerini yayınladıklarında, telif haklarına saygı göstermeleri ve Creative Commons¹² hakkında daha fazla şey öğrenmeleri gerekmektedir. Öğrencilerinize başkalarının ürettiği materyalleri kullandıklarında kaynaklara atıf yapmaları konusunda uyarınız.

6. <http://webquest.org>

7. <https://scratch.mit.edu/educators/>

8. <http://hotpot.uvic.ca/>

9. <http://www.quia.com/>

10. <http://www.activeworlds.com/>

11. <https://en.wikipedia.org/wiki/Copyright>

12. https://en.wikipedia.org/wiki/Creative_Commons



DAHA FAZLA BİLGİ İÇİN

İşbirliğinin gerekli olduğu ve yaratıcılığın desteklendiği projelere öğrencileri dâhil etmek için, bir çok web sitesi bir başlangıç noktası olarak kullanılabilir:

- International Schools Cyberfair, ebeveynlerin, öğrenci ve eğitimcilerin işbirliği yapacakları, birbirleriyle temas kuracakları, eğitim kaynaklarını keşfedecek, geliştirecek ve yayımlayacakları bir çevrimiçi toplanma yeridir:
<<http://www.globalschoolnet.org/GSH/>>. European Schoolnet okullar için benzer kaynaklar sunmaktadır:
<<http://www.eun.org>>.
- Future Problem Solving Program International (Geleceğin Problem Çözücüleri Programı): Öğrencileri, eleştirel ve yaratıcı düşünme becerilerini harekete geçirerek, yaratıcı problem çözmeye yönlendirir: <<http://www.fpsp.org>>.
- Yaratıcılığı geliştirecek fikirler ve kaynaklar Education Scotland sitesinde bulunabilir: <<http://www.educationscotland.gov.uk/learningandteaching/approaches/creativity/>>.
- John Hopkins Eğitim Okulunun Öğrenmede Yeni Ufuklar <<http://education.jhu.edu/PD/newhorizons/>> yaratıcı öğrenmeyi geliştirmek için yeni eğitici uygulamaları içerir.
- Web We Want başlıklı el kitabının “İçinizdeki Sanatçı” başlıklı 6. Bölümü <<http://www.webwewant.eu>> kendi yaratıcılıklarını incelemek ve intihal, telif hakları ve dahası hakkında daha fazla bilgi sahibi olmaları hususunda gençleri yönlendirecek bir dizi faaliyet sunmaktadır.

Oyunlar



Video oyunları, televizyon ekranı, bilgisayar, tablet veya akıllı telefon benzeri bir video aracı üzerinde görsel geri bildirim üretmek üzere kullanıcı ara yüzüyle birlikte insan etkileşimi içeren bir ortam olarak tanımlanabilir. Kavram, atari ve rol oyunundan, strateji oyunlarından fantastik dünyalara kadar çok geniş bir yelpazede türler içermektedir. E-spor, katılımcıların (genellikle yarı profesyonel oyuncular) hızla artan canlı ve çevrimiçi izleyiciler önünde para ödülü için rekabet ettikleri oyun müsabakalarına verilen terimdir. Bu sadece spor olmak zorunda değil, her türlü oyun olabilir. Oyunlar yalnız oynanabilir, kapalı alanda eşlerle oynanabilir veya binlerce ve hatta bazen milyonlarca yabancıyla birlikte oynanabilir. Bu tür kitlesel, çok oyunculu çevrimiçi oyunlar (MMOGs) arasında “World of Warcraft” ve “Game of Thrones” bulunmaktadır. Video oyunları, günümüzde yayıncılık ve kablo televizyonu takip eden dünya eğlence pazarının üçüncü en büyük sektörü olup, 2013 ve 2014¹ yıllarında gelirini iki katı artırdıktan sonra 2015 yılı itibarıyla 74 milyar ABD Doları satış yapmıştır.

1. https://en.wikipedia.org/wiki/Video_game

— Akıllı telefonların, tabletlerin ve küçükten büyüğe kullanıcıların internette yer alması, oyun eğilimleri üzerinde dikkate değer bir etki yapmıştır. 2015 yılında yapılan bir araştırma,² 18 yaşında altındaki her üç çocuktan birinin çevrimiçi oyun oynadığını, ancak çevrimiçi oyuncuların ortalama yaşının 31 olduğunu göstermiştir. Geçmişte daha erkek egemen olan bu alanda bugün kadınlar, tüm alımların %50 sini yapmaktadır. Dünya çapında elektronik oyuncuların %48'i ve İngiltere'de ise %52'si kadındır. Oyun konsollarının kullanımı da gelişmiştir. Kullanıcılar zamanlarının yarısından fazlasını televizyon izleyerek, internet³ üzerinde video ve Blu-ray diskleri izleyerek, araştırma yaparak harcamaktadır³.

— Oyunlar hem aile hem de sınıf içi faaliyet olarak geniş bir alanı kaplamaktadır. İlkokul öğretmenlerinin %74'ü, beşte dördünü "eğitici" oyunların teşkil ettiği çevrimiçi oyunlarını sınıf içi faaliyetlere dâhil ettiklerini söylemektedirler. Aynı zamanda ebeveynlerin %56'sı, oyunların çocuklarını olumlu etkilediğini söylemektedir. Oyunların artan popülerliği ve insan hakları üzerinde olabilecek etkileri göz önüne alındığında, Avrupa Konseyi oyun sağlayıcıları için oyun sağlayıcıları ve çocuk koruma, eğitim ve insan hakları sektörlerinden⁴ uzmanlarla işbirliği içerisinde geliştirilen bir dizi rehber ilke yayınlamıştır.

— Bu durum esasen çevrimiçi oyunların internet üzerinden ve cep telefonları ile her gün milyonlarca kullanıcının keyif aldığı çok çeşitli oyunların yer aldığı büyük bir iş alanı olduğunu göstermektedir.



KİŞİSEL GELİŞİM VE EĞİTSEL YÖNDEN DEĞERİ

- Oyun oynamak eğlencenin ötesinde bir şeydir; Çocuklar ve her yaştan yetişkinler arasında işbirliğini geliştirici bir faaliyettir. Oyunlar yaratıcılığı ve etkileşimi geliştirir, sosyal ve entelektüel gelişim açısından önemli bir rol oynar.
- Oyunlar yetişkinlerin ve çocukların eşit şartlarda (kuşaklar-arası iletişim) fikir alışverişi yapabildikleri ender durumlardan birini temsil ederler.
- Çocuklar, kurallar ve değişkenler içinde sınırlanmış ortamda, farklı sosyal yapılar içinde oynayarak demokrasiyi öğrenirler.
- Oyunlar, genellikle başkalarının haklarına saygı duymayı ve mallarını paylaşmayı içerir. Bazen oyuncuların diğer kültürler ve kültürler-arası uygulamalarla ilişki kurmalarını sağlar. Çocuklar, başarısızlık korkusu olmadan ve kontrol duygusu ile birlikte sosyal becerilerini kullanabilirler. Oyunlar çocukların kurallara uymalarını ve talimatları takip etmelerini gerektirdiği için, onların öz-disiplin ve bağımsızlık açısından kapasitelerini artırır.
- Bulmacalar, oyun tahtası üzerinde oynanan oyunlar, macera oyunları ve araştırma oyunları, oyuncular için stratejik düşünme ve problem çözme yeteneklerini artırma fırsatı sunarlar. Belirli oyunlar, daha küçük çocuklarda motor ve uzamsal becerilerini artırmak ve fiziksel engellilerde ise tedavi edici amaçlarla kullanılabilir.
- Bazı araştırmalar oyun oynamanın otizmde faydalı olduğunu göstermektedir, Minecraft benzeri oyunlar özellikle vurgulanmıştır.
- Çevrimiçi oyunlar yeni kullananlara teknolojiyi ve kodlamayı tanıtmak açısından kullanışlıdır ve genellikle bilgi ve iletişim teknolojilerine (BİT)⁵ olan ilgiyi ve anlayışı artırabilir.
- Oyunlar, matematikten sosyal bilimlere ve dil eğitimine kadar neredeyse müfredatın her alanına yerleştirilebilir.

2. <http://web.archive.org/web/20160420163852/http://www.bigfishgames.com/blog/2015-global-video-game-stats-whos-playing-what-and-why/>

3. <http://web.archive.org/web/20151023082205/http://www.nielsen.com/us/en/insights/news/2015/game-consoles-in-2015-one-stop-shop-for-games-and-entertainment.html>

4. <http://www.coe.int/en/web/portal/guidelines-for-providers>

5. https://en.wikipedia.org/wiki/Information_technology



ETİK HUSUSLAR VE RİSKLER

- Video oyunları ile bağımlılık, saldırganlık, şiddet, yetersiz sosyal gelişim ve çok sayıda kalıp yargılar ve cinsel ahlak konuları arasındaki bağlantılar uzun yıllardır tartışılmakta olup, oyunlardaki bu hususların diğer medya⁶ araçlarından daha fazla etkili olduğuna dair hiçbir kesin delil bulunmamaktadır.
- Oyunların yaşlara uygunluğu, özellikle çok küçük yaşlardaki çocuklar için önemlidir.
- Bağımlılık genellikle bir risk olarak kabul edilir. Amerikan Psikiyatri Derneği (APA) 2013 yılında oyun bağımlılığının düşünsel bir rahatsızlık olarak kabul edilmesi yönünde yeterli kanıt olmadığına hükmetmiş, bunun yerine “internetten oyun oynama bozukluğu” kavramını önermiş ve bunun ölçütlerini tanımlamak için daha fazla çalışma yapılmasını teşvik etmiştir. Her ne kadar internetten oyun oynama bozukluğu bir bozukluk olarak tanımlanmış olsa bile, bu bozukluğun ne kadarının oyun oynama faaliyetinin kendisinden veya diğer bozuklukların⁷ etkisinden kaynaklandığı tartışılmaktadır.
- İnternette yer alan tüm faaliyetler arasında oyunlara baktığımızda, yaşam dengesi önemli bir husustur. Oyunlara harcanan zaman, dışarda ve yüz-yüze yapılacak faaliyetleri etkilememelidir.
- Çevrimiçi oyunların bazıları, yabancılarla tanışma ve iletişim kurma olasılığına izin vermektedir. Kullanıcı etkileşimini teşvik eden, özellikle küçük çocuklara yönelik oyunların insan denetimi (human moderation) yoluyla kontrol edilmesini veya önceden seçilmiş ifadelerle “güvenli bir sohbet” sunmasını sağlayınız.
- Uygulama için satın alımlar vasıtasıyla, bazı oyunlarda çocuklar için ebeveynlerin büyük miktarlarda paralarını bilmeden koleksiyon ve araçlar için harcama potansiyeli bulunmaktadır.



İYİ UYGULAMALAR

- Sınıflandırma ve ölçüm sistemleri, oyun endüstrisi aktörlerinin, ürünlerine tanımlama ve açıklama gerektirerek sorumlu davranmaya teşvik etmektedir. Bu durum oyun satın alanların, oyunlara ilişkin yaş ve içerik uygunluğunu değerlendirmelerine ve oyun pazarında daha güvenli dolaşmalarına yardımcı olmaktadır. PEGI (Pan Avrupa Oyun Bilgilendirme) Avrupa çapında oyun içeriklerinin ve uygulamalarının⁸ yaşa uygunluğu hakkında ayrıntılı tavsiyeler sağlayan tek sınıflandırma sistemidir. Yaklaşık 20.000 oyunun değerlendirmesi kendi web sitesinde www.pegi.info bulunabilir. PEGI aynı zamanda Uluslararası Yaş Sınıflandırma Koalisyonu’nun (IARC) bir parçasıdır. IARC, sayısal olarak indirilen oyunlar ve uygulamalar için küresel sınıflandırma ve yaş sınıflandırması sistemi sunmaktadır. Sonuç olarak, Google Play Store ve Mozilla Firefox Marketplace’de yer alan bütün ürünlerin PEGI değerlendirmeleri hâlihazırda mevcuttur. Microsoft ve Windows 10 uygulaması için de yakın zamanda sınıflandırma yapılacaktır.
- Oyun oynamaya harcanan saatlerin süresini gözlemleyin. Diğer sosyal faaliyetlere zaman ayrılmaması veya çocuk ile gençlerin oyuna zaman ayırmak için okulu asmaları halinde eyleme geçin.
- Oyun toplulukları aidiyet duygusunu destekler ve çocukların bunlara çok rahatça güvenmelerine yol açabilir. Çocuklara, çevrimiçinde edindikleri arkadaşlarının her zaman kim olduğunu söyledikleri kişiler olmayabileceğini hatırlatınız. Kişisel bilgilerin çevrimiçinde başkalarına verilmemesi önemlidir.
- Çevrimiçi oyun oynamak giderek daha popüler bir aile etkinliği olmaya başlamış olup, sorumlu internet kullanımı hakkında yapılacak aile sohbetlerine de vesile olmaktadır. Ebeveynler ve öğretmenler çocuklarının zamanlarının çoğunu elektronik oyunlara harcadığı konusunda kaygı duyuyorlarsa, bir arama motoru vasıtasıyla bulabilecekleri birçok “oyun oynama bağımlık testleri”ni kontrol edebilirler. Bunlar aynı zamanda ideal sohbet başlatıcılardır.
- Avrupa Konseyi çocukların haklarını iyileştirmek ve onları şiddetin her türünden korumak amacıyla cezbedici etkileşimli bir çevrimiçi oyun geliştirmiştir.

6. https://en.wikipedia.org/wiki/Video_game_controversies#Crime_and_violence

7. https://en.wikipedia.org/wiki/Video_game_addiction

8. <http://www.globalratings.com>

9. <http://www.wildwebwoods.org>

Sınıfınızla veya ailenizle <<http://www.playdecide.eu>> adresinden bulacağınız bir konu hakkında rol oynama oyunu seçiniz.

- Oyun-içi satın almalarda; yeni içerik, oyunun işlevselliği, belirli bir oyunun veya uygulamanın özellikleri ve/veya güncellemelerin yanı sıra çevrimiçi mağazalarda satılan oyun dışındaki ayrı unsurlar özellikle ebeveynler için giderek daha fazla endişe uyandırmaktadır. Ebeveyn kontrol filtreleri genellikle bunu önleyebilmektedir.



DAHA FAZLA BİLGİ İÇİN

- Video oyunları hakkında bilgi sahibi olmaya yardımcı olmak için “Ask about games”e bkz.: <<http://www.askaboutgames.com/>>.
- Hâlihazırdaki oyun çalışmaları için Uluslararası Bilgisayar Oyun Araştırmaları Bültenini okuyunuz: <<http://www.gamestudies.org/>>.
- Video oyunları ile ilgili mevzuat; adli, düzenleyici, anayasal, idari, şirketler, sözleşme ve bazı yargı alanlarında rekabet hukukunu da kapsayan devasa bir konudur. Avrupa Etkileşimli Yazılım Federasyonunun (Interactive Software Federation of Europe) - (ISFE) web-sitesi <<http://www.isfe.eu/objectives/public-policy>> kamu politikası ile ilgili bölümü, AB ve küresel mevzuata ışık tutmaktadır.
- Pan-Avrupa Oyunlar Bilgilendirme (PEGI) web sitesi ölçümleme ve sınıflandırma bilgilerini içerir: <<http://www.pegi.info/pegi/index>>. PEGI Online, bu sistemin eki olarak güvenli bir çevrimiçi ortam sağlamayı amaçlamaktadır. PEGI Online sınıflandırmasıyla lisanslanan oyun sağlayıcıları, PEGI Online Güvenlik İlkeleri <www.pegionline.eu> web sitelerini yasadışı ve kullanıcı tarafından hazırlanmış saldırgan içerik ile istenmeyen bağlantıların olmadığı ve özel hayatın gizliliğinin korunduğu ve bağımsız bir şikâyet mekanizmasının da dâhil olduğu standartları karşılamalıdır.
- Yaş doğrulaması küçük yaştaki çocuklara cazip gelen diğer çevrimiçi sektörlerde olduğu gibi oyun endüstrisinde de tartışılmaktadır. Yaş-sınırlaması olan ürün veya hizmetleri satan veya bunlara erişim sağlayan şirketlerin, yaş doğrulamasını daha etkili yapabilmek için bilgi toplayabileceği ve değiş tokuş yapabileceği “değer değiş tokuşu” tesis etmenin mümkün olup olmayacağını görmek için Avrupa’da pilot projeler yürütülmektedir.
- En hızlı büyüyen eğlence pazarı olması sebebiyle çevrimiçi oyunlarla ilgili haber yazıları her hafta yayınlanmaktadır. En fazla satan oyunlar, oyun haberleri, tanımlar, araştırma raporları ve istatistikler hakkında dengeli bir görüş sahibi olmak için çeşitli siteleri ziyaret ediniz. Faydalı başlangıç noktaları Bigfishgames, IFSE, PEGI ve Nielsen web siteleridir. Ayrıca, haberdar olmak için bu sitelerin sunduğu haber bültenlerine/haber akışlarına abone olabilir veya net bir şekilde tanımlanmış Google alarmı ayarlayabilirsiniz.

Sayısal vatandaşlık



İnternet'in ve yeni iletişim teknolojilerinin yaygın kullanımı, büyüme ve istihdam için itici bir güç olmuştur ve birçok vatandaşın hayat kalitesini arttırmıştır. İnternetin günlük kullanımı birçokları için ortak bir olgu haline gelmiştir; buna karşılık sayısal vatandaşlık ve sayısal haklar konusunda derin bir anlayış eksikliği bulunmaktadır.

■ Sayısal ortam olarak bilinen konulara tüm vatandaşların bilgi sahibi olarak katılması, okuryazarlığın daha geniş çapta geliştirilmesine bağlıdır. Bu konu, maruz kaldığımız bilgi çeşitliliğini (görsel-işitsel içerik) eleştirel olarak analiz etme, bağımsız görüşler oluşturma ve sosyal etkileşimle faal olarak ilgilenme ile yeni sosyal etkileşim biçimlerinde uzmanlaşma yeteneğini içermektedir. Yirmi yıl önce yapılan bir araştırmada UNESCO bu becerileri eğitimin dört temel ayağı olarak tanımlamıştır: bilmek için öğrenmek, yapmak için öğrenmek, birey olmayı öğrenmek ve birlikte yaşamayı öğrenmek. Bunun yanı sıra, sayısal vatandaş olabilmek web araçlarını (bkz. Kılavuz Metin Web 2.0, Web 3.0 ve dahası) kullanabilmeyi ve e-mahremiyet konularını (Bkz. Kılavuz 9) anlamayı gerektirmektedir.

1. http://www.unesco.org/education/pdf/15_62.pdf



SAYISAL VATANDAŞLIK NEDİR?

- Sayısal vatandaşlık, bir kişinin çevrimiçi sayısal teknoloji³ kullanırken nasıl davranması² gerektiğini tanımlayan kavramdır.
- Bazı uzmanlar, sayısal vatandaşlığı oluşturan dokuz öge bulunduğunu belirtmektedir. Bunlar; sayısal erişim, sayısal tüketicilik, sayısal iletişim, sayısal okuryazarlık, sayısal görgü kuralları, sayısal hukuk, sayısal haklar ve sorumluluklar, sayısal sağlık ve sıhhat ve sayısal güvenliktir⁴.
- Sayısal vatandaşlığın kompozisyonu ne olursa olsun internetin bütün kullanıcılarının bir sorumluluğunun olduğu ve internet ve iletişim teknolojilerini kullanırken sorumlu davranma görevi olduğu açıktır.

Sayısal ayak izi

- Sayısal ayak izi kullanıcıların sayısal hizmetleri kullandıklarında arkada bıraktıkları verilerdir.
- Pasif bir sayısal ayak izi, veri toplanırken sahibinin haberi olmadan yaratılır, buna karşılık aktif sayısal ayak izleri web siteleri veya sosyal medya⁵ aracılığıyla bir kişi hakkında bilinçli olarak kullanıcı tarafından bilgi paylaşmak amacıyla kişisel veri sağlandığında oluşturulur.

Sayısal kimlik

- Sayısal kimlik, bilgi sistemleri ve ağlarındaki⁶ insanları, örgütleri veya makinaları temsil etmek üzere kullanılan bilgidir.

Sayısal okuryazarlık

- Sayısal okuryazarlık; akıllı telefonlar, tabletler, dizüstü bilgisayarlar ve masaüstü bilgisayarları⁷ benzeri çok geniş bir aralıktaki sayısal cihazlarda kullanılan bilgi, beceri ve davranışlardır.
- Bilgi ve iletişim teknolojileri, toplumun faal birer üyesi olmak için gereken beceri türlerini değiştirerek günlük yaşantımızın her köşesine çoktan girmiş bulunmaktadır.
- İnternet kablosuz ağların yaygınlaşmasına bağlı olarak evrilmeye devam ettilçe, medya okuryazarlığı ve internet okuryazarlığını açacak şekilde etkin biçimde bilgiyi alma ve iletme amacıyla insanların günümüz teknolojisini kullanma becerisi giderek daha önemli hale gelecektir.

Sayısal haklar

- Avrupa Konseyi, sayısal hakları ve sorumlulukları kullanıcı dostu formatında açıklayan ve insan haklarının çevrimiçi ve çevrimdışı⁹ ortamlara eşit şekilde uygulandığının önemini vurgulayan “İnternet Kullanıcıları için İnsan Hakları” başlıklı bir rehber hazırlamıştır.
- “Sayısal haklar”¹⁰ kavramı bireylerin sayısal medyaya erişmelerine, kullanmalarına, üretmelerine ve yayınlamalarına veya bilgisayarlara ve diğer elektronik cihazlara veya iletişim ağlarına erişmelerine ve kullanmalarına izin veren insan hakları olarak tanımlanmaktadır.
- “Sayısal haklar” kavramı, yeni sayısal teknolojiler ve özellikle internet¹³ bağlamında mahremiyet¹² hakkı benzeri mevcut hakların korunması ve uygulanması ile özellikle ilgilidir.
- Avrupa’daki gençlerin sayısal haklarına ilişkin AB Gençlik Manifestosu, internetin nasıl daha iyi hale getirileceği¹⁴ hususunda Avrupalı gençler tarafından hazırlanmış çevrimiçi bir “bildiri”dir.

2. https://en.wikipedia.org/wiki/Digital_citizen

3. https://en.wikipedia.org/wiki/Digital_electronics; https://en.wikipedia.org/wiki/Etiquette_in_technology#Online_etiquette

4. http://www.digitalcitizenship.net/Nine_Elements.html

5. https://en.wikipedia.org/wiki/Digital_footprint

6. https://en.wikipedia.org/wiki/Digital_identity

7. https://en.wikipedia.org/wiki/Digital_literacy

8. https://en.wikipedia.org/wiki/Wireless_network; <http://en.wikipedia.org/wiki/3G>

9. <https://www.coe.int/en/web/internet-users-rights/guide>

10. https://en.wikipedia.org/wiki/Digital_rights

11. https://en.wikipedia.org/wiki/Human_rights

12. https://en.wikipedia.org/wiki/Right_to_privacy_or_freedom_of_expression https://en.wikipedia.org/wiki/Freedom_of_speech

13. <https://en.wikipedia.org/wiki/Internet>

14. <http://www.youthmanifesto.eu/>

Sayısal vatandaşlık ve e-demokrasi

- E-demokrasi, demokratik bir cumhuriyet veya temsili demokrasi içerisindeki demokratik süreçlerin iyileştirilmesinde internet benzeri elektronik iletişim teknolojilerinin kullanımını içermektedir. Bu durum kullanıcıların ilgili konularda kendi seslerini ve yorumlarını “açıklamalarına” izin veren sosyal ağların kullanımıyla desteklenen bir siyasi gelişmedir. Bir teoriye göre sosyal ağların e-demokraside kullanımı, daha fazla insanın yer alması daha akılcı politikalara ve şeffaflık ile hesap verilebilirliğin artmasına yol açacağından siyasa sonuçları üzerinde daha geniş bir etkiyi mümkün kılmaktadır.
- Günümüzde birçok ülkede politikacılar gençlerle irtibat kurmak ve onların görüşlerini almak için sosyal ağ sitelerini kullanmaktadır. Bazıları bu duruma karşı gelse de gençlere ulaşmak için onların olduğu yerlere gitmek önemlidir.
- E-demokrasıyla ilgili bir başka endişe ise medyaya erişemeyenlerin yer aldığı sayısal uçurumun etkisidir. Ancak başlı başına internete erişen her yaştaki insan sayısının artması bile e-demokrasi içindeki sosyal ağ sitelerin yararlarını tanımama anlamı taşıyan bir düşünce olarak görülmemelidir.
- Çevrimdışı iletişimde yetki genellikle hiyerarşik olarak görünürken, çevrimiçinde ise yaygın ve sürekli el değişmektedir. Benzer şekilde, çevrimiçi sınırlar geçirgenleşmekte, roller esnek ve değişebilir olmakta ve sözel olmayan özelliklere veya hiyerarşiye güvenmemektedir. Yalnız başına bu sebepler dahi e-demokrasiyi geliştirmek için sosyal ağ sitelerini kullanmanın faydalarını göstermektedir.
- Buna karşılık e-demokrasinin olumlu bir etkisi olması için kullanıcılar, şiddet içermeyen ve çelişkili olmayan görüşlere açık olmalı, uzlaştırıcı ve saygılı tartışmalarda yer almayı istemelidirler. Benzer düşüncedeki insanların oluşturdukları topluluklar, diğer bakış açılarını dikkate almaksızın konuları şekillendirdikleri ve tartıştıklarında, bu durum e-demokrasiyi güçlendirmekten ziyade zayıflatmakta ve hatta fikirlerin radikalleşmesine sebep olmaktadır.



EĞİTİMDEKİ ÖNEMİ

- Internet daha fazla bilgiyi daha hızlı yayımlamayı mümkün kılmının yanı sıra vatandaşların herhangi bir ilgi alanındaki son gelişmelerden haberdar olmaları için bu bilgiyi sürekli olarak günceller.
- Bilgiye erişim hakkı ve katılım hakkı, Birleşmiş Milletler Çocuk Hakları Sözleşmesinin 13 ve 17nci maddeleri kapsamında bütün çocuklara tanınmış haklardır.
- Geçmişte basının bizi bilgilendirmek için yayımlamayı seçtiği açıklamalara güvenmek zorundayken günümüzde çoğunlukla kaynağa giderek birinci elden bilgimizi elde edebilmekteyiz.
- Dünya üzerindeki vatandaşlar, video çekebilen akıllı telefonlarıyla günlük gazeteciler haline geldikçe, gözlerimizin önünde gelişen “canlı” sahnelerin içine gömüleceğiz. Filmin ne sunmakta olduğunu ve film çekimi başlamadan önce ve sonra nelerin olduğunu araştırma yeteneği genelde bu tür günlük gazetecilikte eksik olup, bunun göstergeleri Twitter, You Tube, Vine videoları ve diğer sosyal medya platformlarında mevcuttur.
- Vatandaşların daha iyi bilgilendirilmeleri, kendi ülkelerinde, pan Avrupa boyutunda ve uluslararası ölçekte demokratik hayata daha iyi katılımları için onları yetkinleştirecektir. Ayrıca vatandaşlar birçok konu ile ilgili tarafsız ayrıntıları araştırmak için interneti kullanabileceklerdir.
- Kamu ve özel sektör kurumları tarafından toplanan coğrafi, kültürel, turistik ve trafiğe ilişkin bilgiler vatandaşların hayatlarını büyük ölçüde zenginleştirmektedir. Bazı ülkelerde vatandaşlar, adreslerini resmi olarak değiştirmek, pasaport yenilemeye başvurmak veya eskiden oldukça zaman alan faaliyetler için interneti kullanmaktadır. Ancak, unutmayınız ki, özel bilgiyi çevrimiçinde verirken belli bazı önlemler alınmalıdır. (Bkz. mahremiyet başlıklı Kılavuz 9 ve güvenlik başlıklı Kılavuz 19).

- İnternet ayrıca vatandaşların kamu veya gündelik hayatla ilgili konularda çevrimiçinde görüşme ve tartışmalara katılmalarını ve hatta e-oylama¹⁵ ile seçimlerde yer almalarını mümkün kılar.
- Siyasi katılımın yanı sıra vatandaşlar çevrimiçi alışveriş yapabilir, eğitim alabilir (bkz. Kılavuz 12 uzaktan eğitim), kültürel tartışmalar, meditasyon, yoga benzeri çevrimiçi olabilecek her türlü faaliyette bulunabilirler.



ETİK HUSUSLAR VE RİSKLER

- Devamlı olarak güncellenen nitelikli bilgiye erişmek, temel insan haklarının kullanılmasında vatandaşları daha iyi bir konuma getirir. Öte yandan, özellikle aşağıda belirtilen teknolojinin bu haklar üzerinde olumsuz etkileri konusunda tedbirli olmalıyız:
- Herkes bilgiye eşit şekilde erişim sağlayamamaktadır. Sayısal uçurum, günümüz toplumunun ikiye bölünmüşlüğü ve bilgiye “sahip olanlar” ile “sahip olmayanlar” arasındaki uçurumu tanımlamaktadır. Bu durumun devam etmesi halinde, dezavantajlı olanlar ifade özgürlüklerini zamanla kaybedeceklerinden demokrasi yara alacaktır. Bilgiye doğrudan erişim olmazsa kendi görüşlerimizi daha az oluşturabilir ve bu yüzden yeni teknolojilerin kullanımında daha iyi olanlar tarafından daha kolaylıkla yönlendirilebiliriz. Buna ilave olarak, kamu sektörüne ilişkin bilgiler demokratik ve sivil yaşam için çok önemlidir ve özellikle ekonomik faaliyetler için temel bir kaynaktır. Herkes için eşit fırsatları sağlayabildiğimiz takdirde; herkesin bilgiye eşit erişimi ve eleştirel düşünce için sağlam bir zemin oluşturulması da gerekli olacaktır.
- Bilgiye erişim açısından, teknoloji ve çevrimiçi platformlar her zaman eşit olmayabilirler. Arama motorları tarafından kullanılan algoritmalar veya sosyal ağlardaki sansür, ortaya çıkan ilk bilgiyi belirgin bir şekilde şekillendirmektedir.
- Günümüzde bilişim ve iletişim teknolojileri hayatımızda o kadar önemli roller oynamaktadır ki yalnızca bunların kullanımında becerikli olanlar gerçekten seslerini duyurabilecek olanlardır. Barışçıl tartışma ve konuşma, eleştirel düşünme ve açık fikirlilik ile benzeri değerler, olumlu bir çevrimiçi ortam ve ifade özgürlüğünü desteklemek için gereklidir.
- Bilginin aktarımı ve değişimi araçlarındaki büyük artış, kendimiz hakkındaki verileri dolayısıyla mahremiyet hakkımızı korumamızın gerekliliğini gösterir (aşağıdaki “İyi Uygulamalar” kısmına bakınız).



NASIL?

- Bilinçli bir e-vatandaş olabilmek için, bütün internet kullanıcılarının temel hak ve sorumluluklarını bilmeleri gerekmektedir. Kullanıcılar sadece kendilerine ne yapmalarına izin verildiğini değil aynı zamanda endüstri, hükümet ve diğer internet kullanıcılarının da ne yapmalarına izin verildiğini bilmelidirler.
- Çerezler hakkında temel bir bilgiye sahip olunması ile diğer web sitelerinin kişisel verilerinizi nasıl toplayıp kullandıklarına ilişkin bilgi sahibi olunması gereklidir (Bkz. mahremiyet hakkında Kılavuz 9).
- Konuların çocuklar için karmaşık hale gelmesini önlemek için, iyi vatandaşlığın temel ilkeleri çevrimiçi faaliyetleri de kapsayacak şekilde genişletilmelidir: saygı, kibarlık ve harekete geçmeden önce düşünme.

15. https://en.wikipedia.org/wiki/Electronic_voting



SINIF İÇİ ÇALIŞMALAR İÇİN FİKİRLER

- Öğrencilerin Birleşmiş Milletler Çocuk Hakları Sözleşmesi üzerinde çalışmalarını ve hangi bölümlerin sayısal haklarla¹⁶ ilgili olduğunu incelemelerini sağlayın.
- Öğrencilerden, vatandaşlık hakkında program yapan çeşitli Twitter, Facebook ve/veya Periscope konuşmacılarını seçmelerini ve tartışmalara katılmalarını isteyin. Konuşmacılara sayısal vatandaşlık ve kullanıcıların sorumlulukları hakkındaki görüşlerinin ne olduğunu sorun. Öğrencilerden sormak için başka sorular oluşturmalarını isteyin.
- Öğrenciler sayısal haklar hakkında destek sunan Avrupa web sitelerini tecrübe etmelidirler. Öğrencilerden Avrupa Konseyi, Avrupa Komisyonu ve Avrupa sayısal hakların bir değerlendirmesini yapmalarını isteyin.
- Avrupa Konseyi'nin çevrimiçi insan hakları faaliyet programı, medeni haklar çalışma programınız için iyi bir kaynak teşkil eder. Ayrıca sınıfınızdan kendi insan hakları sözleşmesini hazırlamasını isteyebilirsiniz. Öğrencilerin insan hakları hakkındaki yeni bilgilerini sanal ortamlara uygulamalarını sağlayın. Örneğin çalışmaları ve oynamaları amacıyla interneti nasıl daha iyi bir yer haline getirebilirler.
- Fransız Devrimini anlatan bir tarih programının ilgili bölümü çerçevesinde, Bastille Hapishanesinin ele geçirilmesine dair kahramanlık dolu ihtilal resimleri ile günümüz bilgilerini karşılaştırarak, öğrencilerinizin gerçekler ile varsayımları ayırt etmelerine yardımcı olunuz. Öğrenciler, "Bastille Hapishanesi'nin ele geçirilmesine ilişkin yorum farklılıklarını sebepleriyle açıklayabilmelidirler". Bu durum, gerçeğin nasıl değişik amaçlarla tanımlandığı ve delillerin güvenilirliği gibi medya eğitimi kavramları ile ilişkilendirilebilir.
- "dünya pasaportu" isimli coğrafya projesi örneğinde olduğu gibi öğrencilerinizden, internet üzerinde bölgelerin nasıl gösterildiğine ilişkin tartışmalarını ve belli bir bölge hakkında web siteleri arasındaki yaklaşım ve tutum farklılıklarını incelemelerini isteyin.
- Öğrencilerinizin içerik analizini öğrenmelerine yardımcı olmak için bir konu seçiniz, değişik kaynaklardan haber sitelerine bakınız ve sınıfta onları inceleyiniz. Farklı kuruluşlar farklı yaklaşımlar mı kullanıyor? Neden böyle olduğunu düşünüyorsunuz?
- Öğrencilerin toplumla ilgili bilgi toplamaları ve demokrasiye aktif olarak katılmaları için okul dışındaki yaşamlarının ayrılmaz bir parçası olan cep telefonlarının nasıl kullanılabileceğini sınıfta değerlendirin. Cep telefonlarının sunduğu hizmetleri listeleyin ve mahremiyet ile demokrasi üzerindeki etkilerini tartışın (mobil hizmetler hakkında bilgi için "internet iş başında" adlı Kılavuz 5'e bkz).
- Akıllı tahtaya bir mesaj göndererek ve öğrencilere hatırlatma notları dağıtarak çevrimiçi bir tartışma başlatın. Her öğrenciye bir numara verilecek ve kendi numarasına karşılık gelen süre bitiminde not kâğıdını okuyacak. Gönderilen mesajı okuduktan ve gelen tüm yorumları dinledikten sonra öğrencilerin kendi yorumlarını yazıp göndermelerine ve diğer mesajlara gelen cevaplara ilişkin tartışmayı izlemelerine izin verilecektir. Öğrencilerin, ilk orijinal mesajın hemen yanına daha belirgin bir şekilde yerleştirilen bir başka öğrenciden gelen mesajı "destekleme" seçeneği de olacaktır. Bu alıştırma, öğrencilere çevrimiçi bir tartışma ile gerçek yaşamdaki bir tartışma arasındaki farklılıklar ile "ifade özgürlüğü" konularını sorgulamayı ve saldırgan veya diğer uygunsuz çevrimiçi davranışlardan kaçınmayı öğretmeyi amaçlamaktadır.

16. <http://web.archive.org/web/20160501101507/http://blogs.lse.ac.uk/mediapolicyproject/2014/09/12/sonia-livingstone-digital-media-and-childrens-rights>

17. https://www.coe.int/t/dg4/youth/Training/Training_courses/HRE_Youth_Programme_en.asp



İYİ UYGULAMALAR

- Her vatandaş kendi kişisel verilerini kontrol etme hakkına sahiptir ancak bu bilgilerin bazıları, kendileri hakkında hangi bilgilerin toplandığını bilmeyi gerektirir. Genel Veri Toplama Düzenlemesi, Avrupa Birliğinde 2016 yılında vatandaşlara mahremiyet ve veri koruma ile ilişkili bu hakları ve diğer temel hakları kullanmalarında yardımcı olmak için çıkarılmıştır. Vatandaşlar için önemli noktalar 15 Aralık 2015¹⁹ tarihli Avrupa Komisyonu basın bülteninde özetlenmiştir.
- Kendiniz hakkında verdiğiniz bilginin nasıl kullanılacağını görmek için anketlerin satır aralarını her zaman okuyunuz ve daha fazla tavsiye için mahremiyet ile ilgili Kılavuz 15'e bakmayı unutmayınız.
- Demokratik sürece katılımın artırılması isteniyorsa, okuryazarlık becerilerinin yaygınlaştırılması ve bunların okullara, yükseköğretime ve tüm topluma aktarılması gereklidir.
- Sayısal vatandaşlık veya sayısal haklar hakkında çevrimiçi kurslara katılmayı planlayın.
- Çok sayıda okul, hâlihazırda, günümüz bilgi toplumunda öğrencilerinin yaşamak, çalışmak ve oynamak için gerekli beceriler geliştirmesini sağlayacak internet yeterlilik programları üzerinde çalışmaktadır. Bu programlar aşağıdaki konuları içermektedir:
 - ▶ İnternette yer alan bilgi labirentinde dolaşma becerileri;
 - ▶ Bilgiyi yanlış bilgidan ayırt etme kapasitesinin geliştirilmesi;
 - ▶ Bilginin uygunluk ve geçerlilik açısından incelenmesi;
 - ▶ Demokrasi hakkındaki çevrimiçi araçların etik göstergelerinin anlaşılması;
 - ▶ Proje temelli öğrenmede bilginin kullanımı;
 - ▶ Tarayıcı ve internetin sunabileceği çoklu fırsatların anlaşılması ve kullanımı.



DAHA FAZLA BİLGİ İÇİN

- Genel Veri Koruması Düzenlemesi için bkz.: http://ec.europa.eu/justice/data-protection/reform/index_en.htm.
- AB Gençlik Manifestosu internetin nasıl daha iyi hale getirileceğine dair Avrupa Gençliği tarafından hazırlanmış çevrimiçi bir bildiridir: <http://www.youthmanifesto.eu>.
- Avrupa sayısal hakları hakkında daha fazla bilgi için bkz.: <https://edri.org>.
- Uluslararası Af Örgütü <http://www.amnesty.org/> ve İnsan Hakları İzleme Örgütü <http://www.hrw.org/> insan hakları konusunda çalışmalar yürüten sivil toplum kuruluşlarıdır. Uluslararası Af Örgütü'nün, özellikle Merkez ve Doğu Avrupa ülkelerindeki gençlerin insan hakları hakkında bilgi edinmelerine yardımcı olması için çeşitli dillerde öğretmenlere yönelik olarak hazırlanmış "ilk adımlar" başlıklı bir el kitabı bulunmaktadır.
- Avrupa Komisyonu'nun görsel işitsel hizmetlerde çocukların korunması ve insan onuru hakkında bilgileri için bkz.: http://ec.europa.eu/avpolicy/index_en.htm.
- Çocuk haklarında daha fazla bilgi BM Çocuk Hakları Sözleşmesinde bulunabilir: <http://www.ohchr.org/en/professionalinterest/pages/crc.aspx>.
- AB Çevrimiçi Hakları Yasası, çevrimiçi ağlara ve hizmetlere erişiminde ve bunları kullanırken vatandaşları korumayı amaçlayan AB hukukunda yer alan bir dizi temel haklar ve ilkelerdir <http://ec.europa.eu/digital-agenda/en/code-eu-online-rights>.

18. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

19. http://europa.eu/rapid/press-release_IP-15-6321_en.htm

- Sayısal vatandaşlığın dokuz unsuru için bkz.:
<http://www.digitalcitizenship.net/Nine_Elements.html>.
- Avrupa Komisyonu ve Avrupa Bakanlar Konseyi tarafından 2015 yılında kabul edilen Paris Bildirisi; vatandaşlığı, ortak özgürlük değerlerini, hoşgörüyü, ayrımcılık yapılmamasını ve bunların eğitim yoluyla insanlara kazandırılmasını teşvik etmektedir:
<http://ec.europa.eu/education/library/study/2016/neset-education-tolerance-2016_en.pdf>.
- İlgili Avrupa Konseyi dökümanları “İnternet kullanıcıları için insan hakları”:
<<http://www.coe.int/en/web/internet-users-rights/guide>> (temel başlıklar aşağıda):
 - ▶ Erişim ve ayrımcılık yapılmaması
 - ▶ Haber alma ve ifade özgürlüğü
 - ▶ Toplantı, dernek ve katılım
 - ▶ Mahremiyet ve veri koruma
 - ▶ Eğitim ve okuryazarlık
 - ▶ Çocuklar ve gençler
 - ▶ Etkili önlemler ve çareler

Dijital Ebeceynlik: Koruyucu ve etkin



“Sayısal yerliler” sayısal çağda, teknoloji çağında doğan çocuklardır. Onlar bir tableti veya akıllı telefonu birkaç dakika tuttuktan sonra teknolojinin ustalıkla kullanılmasında hiçbir korku veya kaygı duymayan çocuklardır. Ne yaptıklarını her zaman anlamadan ancak ekranda bir şeyler olduğunun bilinciyle dokunmatik ekran üzerinde parmaklarını hareket ettirmekte, ekranı kaydirmakta ve tıklamaktadırlar. Marc Prensky’e göre “bugün öğrencilerimizin tamamı internet, bilgisayar ve video oyunlarının sayısal dillerini “ana dilleri” gibi konuşmaktadırlar” (Prensky, M. (2001) “Sayısal Yerliler, Sayısal Göçmenler Bölüm 1” *On the Horizon* 9(5) syf 1-6, 1.

<<http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>>).

“Sayısal göçmenler” teknolojinin gelişimden önce doğan insanlardır. Bu tanım da Prensky tarafından 2001 yılında türetilmiş ve Sayısal çağda büyümemiş insan neslini tanımlamak için kullanılmıştır. Prensky “sayısal çağda doğmamış ancak yaşamının ilerleyen yıllarında yeni teknolojinin birçok veya çoğu yönünden etkilenen bizler, yani sayısal göçmenler her zaman onlarla mukayese edileceğiz” diyerek bu durumu mükemmel bir şekilde tanımlamaktadır (Prensky, 2001),1-2<<http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>>).

■ “Sayısal ebeveynlik”, “sayısal göçmen ebeveynlerin” “sayısal yerli çocuklarının” bugün neler yaptıklarını anlamalarına yönelik rehberlik kavramıdır. Tek amaç çocukları korumak, ebeveynleri yetkinleştirmek ve her iki taraf arasındaki iletişimi açık tutmaktır.

Sayısal ebeveynlik:

- İnternetin riskleri ve faydaları hakkında çocuğunuzla açık iletişim kurmaktır;
- Çocuğunuzun internet faaliyetlerine düzenli olarak katılımınızdır;
- Çocuğunuzun sayısal itibarının ve sayısal kimliğinin etkin bir şekilde korunmasıdır;
- İnternetin sunabileceği fırsatları çocuğunuzla beraber öğrenmektir;
- İnternetin yol açacağı tehlikelere karşı çocuğunuzun korumasıdır;
- Çevrimdışı ebeveynlik becerilerinizi çevrimiçi dünyaya aktarmaktır.

Yapıcı ebeveynlik ise:

- Çocuğunuza yapıcı disiplin ve rehberlik sağlamaktır;
- Çocuğunuzun, sert davranmadan terbiyeli olarak yetiştirmektir;
- Çocuğunuza, “kötü” davranışların etkilerini ve “iyi” davranışların faydalarını göstererek küçük yaştan itibaren uygun bir şekilde nasıl davranacağını öğretmektir;
- Çocuklarınızdan ne yapmalarını istediğiniz hususunda açık olunmasıdır;
- Belirli ve uygun sınırların çizilmesidir;
- Her zaman tutarlı olunmasıdır.

■ Sayısal ebeveynler ve bakıcılar, proaktif ve yapıcı olabilmek ve çocuklarının interneti ve wi-fi bağlantılı bağlı araçları sorumlu bir şekilde kullanmalarını sağlayabilmek için mevcut tüm araçlara ihtiyaç duymaları nedeniyle bu yukarıdaki iki husus arasında açık bir bağlantı bulunmaktadır.



KONULARIN ANLAŞILMASININ ÖNEMİ

- İnternet, cep telefonları ve kablosuz ağa bağlı araçların aynı anda her yerde bulunmasına bağlı olarak ebeveynler kendi teknik bilgi ve uzmanlıklarının eksik olmasından dolayı hüsrana uğramış gibi hissedebilirler. Ayrıca “teknoloji meraklısı” ebeveynler, çocuklarının internet ve teknolojiyi sahiplenme hızından dolayı endişeli hissedebilirler.
- Ebeveynler, pijamalarıyla saatlerce Minecraft oynayan çocuklarıyla nasıl başa çıkacaklarını veya 17 yaşındaki bir gence akşamları mesajlaşma konusunda nasıl sınır koyacaklarını veya 2 yaşındaki çocukları için tuvalet eğitimi uygulaması kullanıp kullanmayacaklarını bilemeyebilirler. Bu tür sorular teknoloji ilerledikçe ve cihazlar daha fazla modernleştikçe ve teknoloji merakı arttıkça bitmeyecektir.
- Aile yapıları değiştikçe, ebeveynler, partnerlerinin evlerinde, büyükannelerin evlerinde veya diğer aile ortamlarında aynı teknoloji kurallarını muhafaza etmekte zorluk yaşayabilirler.
- Teknoloji geliştikçe, çocuk gelişimi ile çevrimiçi kullanımına ilişkin araştırmalar da artmaktadır, ancak uzun vadeli bulgular için birkaç yıl daha beklemek gerekecektir.



ETİK HUSUSLAR VE RİSKLER

- İlk araştırmalar, çocukları “sakinleştirmek” için akıllı bir telefon veya cihaz kullanımının onların özdenetim¹ yeteneklerine zarar verebildiğini göstermiştir.
- Çocukların interneti ve teknolojiyi güvenle ve akıllıca nasıl kullanacaklarını bilmeye ihtiyaçları olduğundan, günümüzde çocuk yetiştirmek aynı zamanda sorumlu bir sayısal vatandaş yetiştirmek anlamına gelmektedir.
- Ebeveynler, bilgiyi iyi kullanma becerisi, medya ve sayısal teknolojileri etkin kullanma becerisi ve sayısal vatandaşlığın gelişimi olarak tanımlanan sayısal okuryazarlığı anlamaları hususunda çocuklarına yardımcı olmalıdır.
- Sayısal dünya ve internetin, “çevrimdışı” ebeveynlik üzerinde de önemli bir etkisi vardır. “Çevrimiçi” dünyayı “çevrimdışı” dünyadan ayrı olarak algılamak bir yanılsamadır. Çocuklar çevrimiçi dünyanın sunduğu sayısız fırsatlar nedeniyle belirli içerik ve tecrübelerle “çevrimdışı” dünyada karşılaşabileceklerinden daha erken yaşlarda karşılaşabilmektedirler. Buna daha erken okumayı öğrenmek, müzik yapmayı öğrenmek ve yabancı bir dille tanışmak gibi “olumlu” diğer konular da dahil olabilir. Aynı zamanda çocuklar cinsel açıdan açık içeriklere, şiddete, korkuya, zorbalığa ve benzeri içeriklere de maruz kalabilirler.
- İnternetin ticari boyutu konusunda dikkatli olun. “Ücretsiz” çevrimiçi hizmetlerin çoğu, maliyet yapıları şeffaf olmayan iş modellerine veya kişisel verilerin reklam amacıyla istismarına dayalıdır. Belirli “ücretsiz” oyunlar, oyunda ilerlemek için çocuğunuzu çokça para harcamaya ayartacaktır. Buna karşılık “oyunreklamları” oyun içerisine bir ürün veya markayı ayrı bir şekilde ilişkilendirmek suretiyle oyun ve reklam arasındaki sınırı bulanıklaştırmaktadır.
- Sayısal vatandaşlığın dokuz unsuru için “sayısal vatandaşlık: teknolojinin uygun bir şekilde kullanımı” na bkz. ve sayısal vatandaşlık hakkındaki Kılavuz 17’i okuyunuz.
- Avrupa Komisyonu Ortak Araştırma Merkezi tarafından yapılan küçük çocuklu ailelerin teknoloji kullanımına odaklanan son araştırmaları bulguları, konu ve risklerin³ anlaşılmasında faydalı olacaktır.
- AB Çevrimiçi Çocuklar sitesi, kendi ebeveyn blogunda⁴ Avrupa çapındaki ebeveynlerin kaygılarına ilişkin raporları içermektedir.



NASIL?

- Çocuklarınız için rol model olun ve kendi teknoloji kullanımınıza sınırlar koyun.
- Güncel çevrimiçi konular hakkında sürekli bilgi edinin ve çocuklarınızın çevrimiçi faaliyetlerini tartışın.
- Çevrimiçi güvenlik programı olup olmadığına karar vermek için çocuklarınızın okulu ile görüşün.
- İstenmeyen sonuçlar doğurabilecek olması nedeniyle ergen çocuğunuzun cihazını bir disiplin önlemi olarak elinden aldığınızda ve çocuğunuzu sosyal bağlantılardan ve ağlardan izole ettiğinizde dikkatli olun.
- Her yaşa ilişkin iyi uygulamalar hakkında bilgi toparlamak amacıyla diğer ebeveynlerle konuşun.
- Çocuklarınıza çevrimiçi zamanını nasıl dengeleyeceğini öğretmek için cep harçlığını nasıl kullanacağını öğrettiğiniz gibi aynı şekilde çevrimiçi zaman sınırlamaları koyun. Her hafta “harcayabilecekleri” bir miktar süre tanıyın ve onların bunu yönetmesine izin verin.
- Çevrimdışı aile zamanının önemini vurgulayın ve haftalık aile faaliyetlerinizi sürdürün.

1. <http://web.archive.org/web/20160424230408/https://www.theguardian.com/technology/2015/feb/01/toddler-brains-research-smartphones-damage-social-development>

2. http://www.digitalcitizenship.net/Nine_Elements.html

3. <http://publications.jrc.ec.europa.eu/repository/handle/JRC93239>

4. <http://web.archive.org/web/20160415215157/http://blogs.lse.ac.uk/parenting4digitalfuture/2015/06/26/svenjas-post-on-little-kids-european-comparison/>



SINIF ÇALIŞMALARI İÇİN FİKİRLER

- Öğrencilerinizden sayısal çağda ebeveynlik hakkında ipuçları veren kısa bir blog yazısı yazmalarını isteyin.
- Öğrencilerinizle günümüz teknolojinin kullanımı hakkında bir tartışma yapın. Faydaları nelerdir? Riskleri nelerdir? Öğrencilerin faydaları artırmak ve riskleri önlemek için yapabilecekleri bir şey var mıdır?
- İnterneti kullanmanın iyi uygulamaları hakkında yapılacak bir tartışmanın ardından öğrencilere küçük kardeşleri, kuzenleri, yeğenleri veya daha genç komşularıyla paylaşabilecekleri en iyi ipuçlarını sıralamalarını isteyin. Daha küçük yaştaki çocukların, öğrencilerin tecrübelerinden nasıl yararlanabilirler?
- Öğrencilerden 1960'ların teknolojisi ile günümüz teknolojisini değerlendirmelerini isteyin. Ebeveynler aynı kaygılara sahip miydi? Neden veya neden olmasın?



İYİ UYGULAMALAR

- Çocuklarınızla çevrimiçinde kiminle konuştuklarını, ne yaptıklarını, hangi siteleri ziyaret ettiklerini ve ne zaman çevrimiçi olduklarını konuşun.
- Konu sizin için rahatsız edici olsa dahi diyaloga açık olun, bu sizin çocuğunuzun çevrimiçi faaliyetleri hakkında haberdar olmanızın en iyi yoludur.
- Çocuklarınızla yapacağınız “güvenli seks” konuşmalarınızın yanı sıra, “güvenli teknoloji” ve “güvenli içerik” benzeri internet konuşmaları da yapın ve cinsel içerikli veya aşırılık içeren fotoğraflar, konuşmalar veya mesajların uygunsuzluğunu ve risklerini açıklayın.
- Şiddet, kışkırtma, zorbalık, cinsellik, toplumsal cinsiyet kalıp yargıları ve rolleri ve benzeri konular hakkında konuşmaya hazırlıklı olun çünkü çocuklarınız bunlarla çevrimiçinde beklenmedik bir zamanda karşılaşabilecek ve başa çıkmak ve karşılığında olumlu bir çevrimiçi davranış geliştirmek için sizin rehberliğinize ihtiyaç duyacaktır.
- Kişisel güvenlik (mahremiyet) ayarlarının nasıl kullanılacağını öğrenin ve çocuğunuza bunları nasıl uygulamaya koyacaklarını ve bunu yapmanın neden gerekli olduğunu açıklayın.
- Çocuğunuzun kullandığı oyunlar, hizmetler veya web sitelerinin gerisindeki iş modeli hakkında bilgi alın. Küçük çocuklar için içeriğin reklamsız olduğundan, gizli bir maliyeti veya ödül özellikleri olmadığından emin olun. Çocuğunuzun ticari suiistimal denemelerine maruz bırakmak yerine bir oyun için küçük bir ücret ödemek veya kaliteli bir hizmete aylık abonelik yaptırmak daha iyidir.
- Çocuklarınızın kullandıkları hizmetler veya oyunların veya okudukları içeriğin arkasındaki iş modellerini anlamalarını sağlayınız.
- Çocuklarınızın, gereği dışında paylaşım (kişisel bilgi, tanımlayıcı özellikler, uygun olmayan fotoğraflar vb) yapmadığından emin olunuz.
- İnternet kullanımı ve ekran süresi ile ilgili sağlıklı bir denge bulunuz ve iyi bir sayısal rol model oluşturunuz.
- Çocuklarınıza yazdıkları, gönderdikleri veya paylaştıkları her şeyin süresiz olarak internet üzerinde kalacağını ve bunların aynı zamanda değiştirilebileceğini ve başkalarına gönderilebileceğini hatırlatın.
- Çocuklarınıza bildirim araçlarının nasıl kullanılacağını öğretin böylece uygunsuz her içeriği işaretleyebilirler.



DAHA FAZLA BİLGİ İÇİN

- iPadlerin çocuk gelişimi üzerindeki etkisi için ilgili rapora bakınız: <https://www.youtube.com/watch?v=VrQhmcPrhFw>.
- Marc Prensky'nin "Sayısal yerliler, sayısal göçmenler" (2001) makalesini okuyunuz: <http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>.
- Avrupa Aileler Konfederasyonu (COFACE) aileler için faydalı bilgiler sunmaktadır: <http://www.coface-eu.org/>.
- The Parent Zone (Ebeveyn Hattı) çok değerli bilgiler sunan bir İngiliz sitesidir: <http://www.theparentzone.co.uk/>.
- Çevrimiçi Aile Güvenliği Enstitüsü'nün yayınlarına bakınız: <https://www.fosi.org/good-digital-parenting/>.
- Vodafone, sayısal ebeveyn dergilerinin yanı sıra ebeveynler için rehber ilkeler hazırlamıştır: <https://www.vodafone.com/content/parents/howto-guides.html>.
- Boston Üniversitesi Tıp Merkezi cep telefonu kullanımı hakkında bir rapor yayınlamıştır: http://web.archive.org/web/20160607121811/http://www.eurekalert.org/pub_releases/2015-01/bumc-mai013015.php.
- Avrupa Komisyonu Ortak Araştırma Merkezi genç çocuklar ve sayısal teknoloji hakkında bir rapor yayınlamıştır: <http://publications.jrc.ec.europa.eu/repository/handle/JRC93239>.
- "Oyna ve öğren: çevrimiçi olmak", sorumlu internet kullanımı hakkında ebeveyn ve öğretmenleri çocuklarıyla yapacakları konuşmalarda desteklemek amacıyla 04-08 yaş arası çocuklar için faaliyetleri içermektedir: <https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=198308>.
- Küçük çocuklarınızı kendi yaşlarına uygun sitelere yönlendirin, bu tür çok çeşitli siteler vardır, bunlar arasında "Junior: çocuklar için güvenli arama" <https://www.juniorsafesearch.com/> ve YouTube Kids <https://kids.youtube.com/>.
- Avrupa Konseyi'nin ilgili mevzuatı Avrupa Konseyi'nin "Sayısal ortamda çocuklar" başlıklı Avrupa Konseyi web sayfasının altında yer almaktadır: <http://www.coe.int/en/web/children/the-digital-environment>.

5. İnternet- Problemlİ İerikler

“İnsan haklarını insanlara tanımamak onların insanlığına karşı gelmektir.”



Nelson Mandela, 1993 Nobel Barış Ödülü sahibi, ırkçılık karşıtlığı savunucusu, 1994-1999 Güney Afrika Cumhurbaşkanı.

“Bir kişinin hakları tehdit altında olduğunda herkesin haklarında azalma olur.”

John F. Kennedy, 1961-1963 ABD Başkanı

KILAVUZ 19 - SİBERSUÇ: İSTEK DIŞI E-POSTA, KÖTÜ AMAÇLI YAZILIM, DOLANDIRICILIK VE GÜVENLİK

Hesaplarınız için güçlü değişik şifreler oluşturdunuz ve ikili güvenlik unsurunu yapılandırdınız mı?
Araçlarınız / hesaplarınız için güvenlik ayarlarını araştırdınız mı?
İşletim sisteminiz ve uygulamalarınız güncel mi?
En önemli verilerinizi yedeklediniz mi?

KILAVUZ 20 – SINIFLANDIRMA VE FİLTRELEME

Filtrelemenin kültürel ve ahlaki etkileri hakkında düşündünüz mü?
“Kara liste” ve “Beyaz liste” arasındaki farkı biliyor musunuz?
Çocuk içeriği için en sık kullanılan sınıflandırma sistemleri ve ne anlama geldikleri hakkında ilginiz var mı?

KILAVUZ 21 – ÇEVİRİMİÇİ TACİZ: ZORBALIK, SATAŞMA, KANDIRMA

Çevrimiçi bir tacize karıştıklarında çocukların etkilerini anlamaları için açık bir aile veya okul politikanız bulunuyor mu?
Kişisel bilgilerinizi yeterince koruyor musunuz? Birçok çevrimiçi sorun, yanlış yönlendirilmiş fotoğraflar ve bilgilerin paylaşımıyla ortaya çıkmaktadır.
Zorbalık, trolleme ve genel olarak tacizi kolaylaştıran çevrimiçi iletişimin “anonimlik” ve “yüzünü gizlenmesini” aşmak için daha iyi sosyal ve duygusal becerilerin (sosyal okuryazarlık olarak da bilinir) nasıl oluşturulacağını araştırdınız mı?

KILAVUZ 22 – YARDIM ALMAK

Siz ve çocuklarınız/öğrencileriniz yasadışı içeriği nereye bildireceğinizi biliyor musunuz?
Gelişmekte olan eğilimleri ve riskleri anlamak için yardım hatları tarafından bildirilen istatistikleri hiç kontrol ediyor musunuz?
Sizi çevrimiçinde en iyi şekilde koruyacak ilk beş sayısal beceriler nelerdir?
Mobil cihazlarınızı rahat ve güvenli bir şekilde kullanmak için coğrafi konum ve Bluetooth'u yeterince anlıyor musunuz?
M-öğrenme ve mobil cüzdanlar, mobil cihazların kullanımının öğrenme, çalışma ve alışveriş yapma biçimimizi değiştirdiği alanlardır. Bu son gelişmeler hakkında ne biliyorsunuz?

Siber Suçlar: İstek Dışı E-Posta, Kötü Amaçlı Yazılım, Dolandırıcılık, Güvenlik



İnternet kaliteli içeriğe ve hizmetlere erişmenin harika bir yolu olmasına rağmen, istek dışı içerik, virüsler, kötü amaçlı yazılımlar ve aldatmacaların/scam dağıtılması yoluyla kötü niyetli kişilere de hizmet edebilir.

- Siber suç, bir bilgisayara yasadışı erişim (saldırı/hacking olarak da adlandırılır), iletişimin durdurulması, bir bilgisayarın çalışmasına engel olmak veya hasar görmesine ya da verileri silmek gibi bilgisayarlara ve verilere karşı suçların yanı sıra dolandırıcılık veya çocuklara yönelik cinsel şiddet gibi bilgisayarlara işlenen suçları da kapsar. Kötü amaçlı yazılım, istek dışı e-posta ve oltalama/phishing ve diğer kimlik hırsızlığı türleri, siber suç işleyenlerin kullandığı araçlardan bazılarıdır.
- Kötü amaçlı yazılım¹ (Malware), virüsleri, truva atlarını ve diğerlerini içeren çeşitli düşman veya saldırgan yazılım biçimlerini ifade etmek için kullanılan şemsiye bir terimdir. Kötü amaçlı yazılımların hedefleri çok çeşitlidir. Yazılıma zarar vererek veya donanımını bozarak bilgisayarınızın işlevini bozmayı amaçlayabilir ya da bir şekilde para kazanılabilecek bilgi ve verileri çalabilirler. Virüslü bilgisayarınız, bilginiz olmadan suçlular tarafından kontrol edilen bir "bot" haline gelebilir; daha sonra, istek dışı e-postaları yaymak, dolandırıcılık yapmak veya hastaneler, havaalanları veya bankalara yönelik saldırıları gerçekleştirmek için "botnet" in bir parçası olarak milyonlarca diğer virüs bulaşmış bilgisayarla birlikte kullanılabilir.

1. <https://en.wikipedia.org/wiki/Malware>

- Spam², çoklu alıcılara istenmeyen iletilerin toplu olarak gönderilmesidir. En çok e-posta ile ilişkilendirilir, ancak sosyal ağlar, anında mesajlaşma, cep telefonları ve diğerleri için de geçerlidir. Neyse ki, çoğu e-posta hizmetinde etkin istek dışı e-posta filtreleri bulunmaktadır. İstek dışı bir e-posta aynı zamanda, bir alıcının istek dışı bir e-postada belirtilen bir ek veya bağlantıyı açması gibi, farklı türdeki kötü amaçlı yazılımları yaymak için bir vektör görevi görebilir.
- Oltalama³, "şifre için oltalama" türüne dayanmaktadır ve kimlik hırsızlığının bir biçimidir. Örneğin, alıcılar, banka veya sosyal ağ gibi bilinen bir kurumdan yasal posta olarak gizlenmiş istek dışı e-posta alırlar. Bu postalarda genellikle, kredi kartı numaraları veya şifreler gibi hassas kullanıcı bilgilerini toplamak için kullanılan sahte web sitelerine bağlantılar bulunur. Çalınan kimlik bilgileri dolandırıcılık yapmak için sıklıkla kullanılır.
- İnternet dolandırıcılığı⁴, son birkaç yıldır e-ticaret imkânları ve çevrimiçinden ödeme yapılmasının artmasıyla büyük ölçüde gelişti. İnternet dolandırıcılığı, sahtecilik, emlak dolandırıcılığı, SMS çağrı/zil sesleri, para transferi dolandırıcılığı ve benzeri dolandırıcılık gibi çeşitli dolandırıcılıkları kapsar.



NASIL GÜVENDE KALABİLİRSİNİZ?

— Çevrimiçi güvenliğiniz ev güvenliğiyle karşılaştırılabilir. Pencereyi kapalı ve kapıyı kilitli tutarak içerdekileri korursunuz. Sağlıklı ölçüde şüphecilik, eleştirel düşünme ve BİT becerileri, dolandırıcılık, kimlik avı, kötü amaçlı yazılım veya çevrimiçi aldatmacalara/scam yakalanmanızı önlemeye de yardımcı olacaktır.

— Güvenlik için olan birçok husus, mahremiyetle de ilgilidir (Bakınız Kılavuz 9).



KİŞİSEL GELİŞİM VE EĞİTİM DEĞERİ

— Güvenlik, tüm internet kullanıcılarının olduğu kadar sizin güvenliğiniz için de önemlidir. Kötü amaçlı yazılımlar, virüsler ve istek dışı e-posta, çoğunlukla kullanıcıların kendileri tarafından yayılır! Bilgisayarınız veya cihazınız güvende değilse, tüm arkadaşlarınız ve irtibatlı olduğunuz kişiler güvenlik risklerine maruz kalabilir!

— İnternet güvenliği ve emniyetine ilişkin bilgiler, kullanıcıları, cihazlarının parametre ve ayarlarını ve kullandıkları çevrimiçi hizmetleri daha derin incelemeye ve onları cihazlarının işletim sistemlerinin ve internetin çalışması konusunda daha iyi teknik bilgi edinmeye zorladığı için sayısal okuryazarlık becerilerinin daha da gelişmesi açısından çok değerlidir.



OLASI RİSKLER

İstek dışı e-posta (Spam)

- İstek dışı e-posta genellikle zararsızdır ve sonuçta sıralama sırasında çoğunlukla büyük bir zaman kaybı olur veya bağlantıları tıklamakla zaman boşa gider.
- İstek dışı e-posta genellikle sahte veya hileli bilgi içerir. Gönderen isimsiz olduğu için, sahte bilgilere dava açmak mümkün değildir.
- İstek dışı e-posta gönderenler, genellikle veri tabanlarına posta adresleri toplamak için alıcıların iyi niyetini istismar ederler. Örneğin, bir dilekçe veya davayı desteklemek için alıcıların kişisel bilgilerini bir listeye eklemelerini isteyen postalar gönderilebilir. Çoğu zaman ameliyat gerektiren hasta bir çocuk gibi bir nedenden dolayı, gönderilen her seferde paranın ödeneceğini bir şirketin veya kuruluşun vaat ettiğini yalan olarak iddia etmektedir.

2. <https://en.wikipedia.org/wiki/Spamming>

3. <https://en.wikipedia.org/wiki/Phishing>

4. https://en.wikipedia.org/wiki/internet_fraud

- Her gün istek dışı e-postaların yeni teknikleri görünmektedir. Örneğin, sosyal ağlarda istek dışı e-posta, arkadaşların paylaştığı "kilo vermenin en iyi 10 yolu" veya "bu kızın web kamerasının önünde ne yaptığını inanmayacaksınız" gibi akılda kalıcı başlıkları içeren mesajlar ile "tıklama/click jacking"⁵ şeklinde olabilir. Bunun sonuçları, sizi gelir edinmek için çok sayıda reklama maruz bırakan bir web sitesini ziyaret etmeye veya sizi daha çok mesaj ile istek dışı e-postası olan bir sayfayı beğenmeye zorlayabilir.
- Birçok çevrimiçi dolandırıcılık türü vardır ve teknoloji geliştikçe her geçen gün yenileri ortaya çıkmaktadır. Yaygın bir dolandırıcılık türü, bu tür mağduriyetleri yasaklayan bir Nijerya yasasının ardından "419" olarak adlandırılmaktadır. Bu, genellikle, banka transferleriyle ilgili yardım karşılığında çok miktarda bir paranın bir kısmının söz verilmesini içerir. Başka bir dolandırıcılık ta, mağdura, kiralık bir daireyi ziyaret etmeden önce Western Union aracılığıyla kiralık depozito garantisi olarak para göndermesini istemekten oluşur.

Oltalama ve kimlik hırsızlığı

- Oltalamaya ve kimlik hırsızlığına yakalanma riskleri çok daha ciddidir. Oltalama girişimi yoluyla sağladığınız bilgilere bağlı olarak, zarar, çevrimiçi forum gibi nispeten önemsiz bir çevrimiçi hesabın kontrolünü kaybetmekten, tüm çevrimiçi hesaplarınızın tehlikeye düşmesine yol açabilecek ana e-posta adresiniz gibi son derece önemli hesapların kontrolünü kaybetmeye kadar olan herhangi bir şey olabilir!
- Hesaplarınız tehlikeye girince verileriniz de tehlikede olabilir. Örneğin tüm e-postalarınızın içeriği indirilebilir. Bu veriler, sizden veya bağlantılı olduğunuz kişilerden para sızdırmak, çevrimiçi sipariş vermek için hesaplarınızı kullanmak, kredi kartınızı kullanmak, çevrimiçinde sizin kimliğinize bürünmek vb. için çok değerli olabilir.

Kötü amaçlı yazılım

- Kötü amaçlı yazılım yüklemenin riskleri, oltalamaya ve hatta istek dışı e-postaya benzer veya daha kötüdür. Kötü amaçlı yazılım, oltalama amaçlı olarak, hesaplarınız hakkında bilgi çalmak için (örneğin bir anahtar kaydedici⁶ kullanarak), sizi pop-up'lar, bildirimler veya tarayıcılarınız içindeki varsayılan ana ekranlarla bombardıman etmek için istek dışı e-posta gönderme amaçlı olarak ve ayrıca bilgi ve verileri doğrudan bilgisayarınızdan çalmak veya bilgisayarınızın işleyişini bozmak, suç işlemek için bilgisayarınızı kontrol altına almak, cihazlarınızın mikrofonlarını veya kameralarını size karşı casusluk yapmak için etkinleştirmek ve potansiyel olarak içeriği tamamen yok etmek gibi başka amaçlar için kullanılabilir.
- Kullanıcıları kötü amaçlı yazılım yüklemelerine kandırmaya yönelik yöntemler de hızla gelişmektedir. Buna bir örnek, bilgisayarınızın antivirüs taramasını gerçekçi bir şekilde taklit eden sahte açılan bir penceredir. Sahte taramanın sonunda, tehlikeli virüslerin bilgisayarınızda tespit edildiği söylenir ve onlardan kurtulmak için - aslında kötü amaçlı bir yazılım veya bir virüs olan bir yazılım yüklemelisiniz!



SINIF ÇALIŞMASI İÇİN FİKİRLER

- Çocuklar ve gençlerden üçer veya dörder kişilik gruplar halinde çalışmalarını ve sahte bir çevrimiçi hesap için güçlü bir şifre önermelerini isteyin. Kullandıkları mevcut bir şifre değil, yeni bir şifre oluşturmaları gerektiğini açıkça belirtin! Farklı takımların şifrelerini sunmalarını ve geri kalan grubun, tekliflere bakarak güçlü bir şifrenin özelliklerini belirlemelerini isteyin.
- Güçlü bir şifre:
 - en az sekiz karakter uzunluğundadır;
 - sözlükte bulunan bir kelimeyi içermez, kişisel hayatınıza veya kullanıcı adınıza, gerçek adınıza veya şirket adına bir gönderme içermez;
 - aşağıdaki kategorilerin her birinden karakterler içerir: büyük harfler, küçük harfler, sayılar ve semboller.

5. <https://en.wikipedia.org/wiki/Clickjacking>

6. https://en.wikipedia.org/wiki/Keystroke_logging

• CSIRT (bilgisayar güvenlik olayı müdahale ekibi) olarak da bilinen bir CERT (bilgisayar acil durum müdahale ekibi), bilgisayar güvenlik olaylarıyla ilgilenen uzman bir gruptur. Öğrencilerinizin ulusal CERT / CSIRT'nizi bulmalarını sağlayın ve bu takımların rolü ve işleyişi hakkında daha fazla bilgi edinin.

► Siber suçların kurbanları, genellikle suçu polise bildirmezler ve bu nedenle suçlular işlerine devam eder ve yeni kurbanlar bulurlar.

► Öğrencilerinizden bir suçun, şikayet hatları yolu da dahil olmak üzere, polise veya diğer kamu otoritelerine nasıl bildirileceğini öğrenmelerini isteyin.

► Öğrencilerinizden ülkelerinin yasaları uyarınca neyin siber suç oluşturduğunu öğrenmelerini isteyin.



İYİ UYGULAMA

- İnternet kullanıcılarının her şeyi çevrimiçi "ücretsiz" olarak almasını beklemelerinin sonuçlarından birisi de, çevrimiçi kullanılan "ücretsiz" yazılım veya hizmetlere eklenen kötü amaçlı yazılımların veya istek dışı e-postanın sürekli olarak gelişmesidir. Çevrimiçi ortam, paylaşılan bir sorumluluktur ve kullanıcıların kendi çevrimiçi davranış ve tercihlerinin sonucudur. Kaliteli hizmetleri/içeriği/ yazılımı maddi olarak destekleyerek (açık kaynak girişimleri için bağışlar yoluyla veya ticari kuruluşlara lisanslar veya abonelik satın alarak) çevrimiçi ortamın daha güvenli hale getirilmesine katkıda bulunursunuz.
- • Kullanıcı dostu olma durumu güvenlik düşmanı olabilir. Örneğin, işletim sisteminizi, önemli bir işlem gerçekleştirildiğinde (örneğin, yeni bir yazılımın yüklemesi) bir yönetici şifresi isteyecek şekilde yapılandırabilirsiniz. Son derece sınır bozucu ve sıkıcı olabilir, ancak daha fazla güvenlik için ödeyeceğiniz fiyat budur! İşletim sisteminizin güvenlik ayarlarını yaparken bunu göz önünde bulundurun.
- • Bir bilgisayarın veya ağın birden fazla kullanıcıyı yönetiyorsanız, her kullanıcının uygun haklara sahip olduğundan emin olun. Gereksiz kullanıcı haklarını kısıtlamak, yanlışlıkla veya kasıtlı güvenlik problemlerinden kaçınmanıza yardımcı olabilir.
- Bilgisayarınıza herhangi bir şey indirmeden önce kaynağa güvendiğinizden emin olun. Özellikle, kötü amaçlı yazılımların dağıtımına yardımcı olmak için bilinen bir noktadan bir noktaya (peer-to-peer) yazılımlardan⁷ haberdar olun (müzik ve görüntülere ilişkin Kılavuz 14'e bakın). Yazılımı yüklediğinizde "sonraki" düğmesini tıklamadan önce tüm adımları okuduğunuzdan emin olun. Bilgisayarınıza kötü amaçlı yazılım yükleyebilecek olan önceden işaretlenmiş kutulara özel dikkat gösterin!
- Anti-virüs yazılımı yükleyin⁸ ve bunu güncel tutun.
- Mevcut oldukları anda güvenlik yamalarını veya işletim sistemi güncellemelerini yükleyin. Bazı işletim sistemlerini ve programları otomatik olarak güncelleştirecek şekilde veya karşıdan yükleyebileceğiniz bir yama hazır olduğunda sizi bilgilendirecek şekilde ayarlayabilirsiniz.
- Bilgisayarınıza gelen veya giden trafiği kontrol etmek için bir güvenlik duvarı⁹ yükleyiniz.
- "Kişisel" e-posta adresinizi her zaman vermekten kaçınmak için (örneğin, forumlara kaydolma, formları doldurma vb.) farklı amaçlar için farklı e-posta hesapları kullanın ve e-posta adresinizi büyük ölçekte dağıtmayın. Bir web sitesine e-posta adresinizi eklerseniz, web tarayıcılarının bunu alıp istek dışı e-posta amaçlı dağıtım listelerine ekleyebileceğini unutmayın. Ayrıca istek dışı e-postayı yanıtlamayın. Bu, istek dışı e-posta gönderene, sizin e-posta adresinizi teyit etmek olacaktır. Sizi posta listesinden çıkartma sözü veren bağlantıların gerçek olmayabileceğini unutmayın.
- E-posta adresinizi mutlaka göndermeniz gerekiyorsa, Tom (nokta) Smith (@) gmail (nokta) com gibi karakterleri ekleyerek veya otomatik olarak kopyalanamayacağı şekilde resim olarak göndererek gizleyebilirsiniz.

7. <https://en.wikipedia.org/wiki/Peer-to-peer>

8. https://en.wikipedia.org/wiki/Antivirus_software

9. [https://en.wikipedia.org/wiki/Firewall_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing))

- Aldığınız e-postalar hakkında bir şüphe duyun. Kaynağa güvenmiyorsanız e-postaları açmayın. Aldığınız herhangi bir bildirimin e-posta adresini gerçekliğini daima kontrol edin.
- Özellikle eklentilere dikkat edin. Şüpheli görülen veya talep etmediğiniz bir şey alırsanız, açmadan hemen silin.
- Güvenmediğiniz alıcılardan gelen bağlantıları ve özellikle de "orijinal" URL adresini görmenin imkânsız olduğu kısaltılmış URL'leri kullanan bağlantıları asla tıklamayın. Hesapları veya cihazları tehlikede altında olan güvendiğiniz alıcıların bile virüslü mesajlar gönderebileceğini unutmayın.
- Asla bir kullanıcı adı, şifre veya kredi kartı numarası gibi özel bilgileri e-posta ile göndermeyin veya postalamayın. Hiçbir çevrimiçi hizmet sizden e-posta yoluyla kullanıcı adınızı ve şifrenizi göndermenizi istemeyecektir ve sadece çok nadir durumlarda sizden kredi kartı numarası gibi bilgileri paylaşmanız istenecektir (örneğin, bu bilgiyi otelin resmi rezervasyon e-posta adresine bir otel odasını ayırırken göndermeniz gerekebilir).
- En önemli hesaplarınız için farklı şifreler kullanın ve mümkün olduğunda ikili güvenlik önlemlerini ayarlamayı unutmayın (cep telefonu numaranızı veya fazladan bir güvenlik cümlesi/sorusu ekleyerek). Şifrelerinizin sizinle açık bir bağlantısı olmadığını, en az sekiz karakter uzunluğunda olduğundan ve harf (küçük ve büyük harfli), rakam ve sembollerin birleşiminden oluştuğundan emin olun.
- Harici bir sabit disk üzerinde tüm verilerinizi düzenli olarak yedekleyin. Birçok yedekleme yazılımı programı bulunmaktadır ve bunlar otomatik ve düzenli olarak verilerinizi yedekler. Bunların bazıları işletim sisteminiz (Windows, MacOS, Linux vb.) içinde bile bulunmaktadır. Bunlar hakkında bilgilerinizi sürekli yenileyin¹⁰.

DAHA FAZLA BİLGİ

- Gerçek veya Kurgu İnternet kullanıcılarının yaygın olarak iletilen e-postalarla yapılan talepleri kontrol etmesi için bir web sitesidir: <<http://www.truthorfiction.com/>>.
- Spam ile mücadele hakkında daha fazla bilgi: <<http://spam.abuse.net>> and <<http://www.spamhelp.org/>>.
- Microsoft güvenliği hakkında bilgi için bkz: <<http://www.microsoft.com/security/>>.
- Apple güvenliği hakkında bilgi için bkz: <<http://www.apple.com/support/security/>>.
- Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA), sayısal güvenlik konularında düzenli olarak güncelleme yapar: <<http://enisa.europa.eu>>.
- Avrupa Konseyi'nin "Siber Suçlara Karşı Eylem" adlı bir web sayfası bulunmaktadır: www.coe.int/cybercrime
- TechTarget bir bilgi güvenliği dergisidir: <http://informationsecurity.techtarget.com/>
- Çerezlerden IP adreslerine, tarayıcı kontrollerine kadar konular hakkında faydalı bilgiler ve kullanıcı testleri şu adresten bulunabilir : <<http://www.2privacy.com/>>.
- Birleşik Krallık hükümetinin çevrimiçi güvenlik önerileri şu adreste bulunabilir: <<https://www.getsafeonline.org>> ve Birleşik Devletler için: <<http://www.us-cert.gov/>>.
- CERT ve ülke adınızı kullanarak bir web araması yoluyla ulusal bilgisayar acil durum müdahale ekibinizi bulun.
- Doğrudan Pazarlama Derneği tarafından sunulan bilgi güvenliği rehber ilkeleri <<http://www.the-dma.org/guidelines/informationsecurity.shtml>> doğrudan pazarlamacılar için tasarlanmışsa da çevrimiçi güvenlik konusunda endişe duyan herkes için yararlı ipuçları sağlamaktadırlar.

10. https://en.wikipedia.org/wiki/List_of_backup_software

- **BM Çocuk Haklarına dair Sözleşmenin ilgili maddeleri:**

Madde 16 - Çocuklar mahremiyet hakkına sahiptir. Yasa, onları hayat tarzlarına, adlarına, ailelerine ve evlerine yapılan saldırılardan korumalıdır.

Madde 17 - Çocuklar, kitle iletişim araçlarından güvenilir bilgi alma hakkına sahiptir. Televizyon, radyo ve gazeteler çocukların anlayabileceği bilgileri sağlamalı ve çocuklara zarar verebilecek materyalleri tanıtmamalıdır.

Madde 34 - Hükümet çocukları cinsel istismardan korumalıdır.

Madde 36 - Çocuklar ,gelişmelerine zarar verebilecek her türlü faaliyetten korunmalıdır.

Sınıflandırma ve filtreleme



Sınıflandırma ve filtreleme

Sınıflandırma ve filtreleme her ikisi de video, görüntü, web sayfası ve oyun gibi İnternet içeriğine erişimi kısıtlamak için kullanılan yöntemlerdir. Teknik ve çocuk yardım kurumlarının on yıl kadar önce, filtreleme amacıyla web sitelerine yerleştirilebilecek bir elektronik sınıflandırma sistemi yaratma yönündeki ilk umutlarına rağmen, günümüzde sınıflandırma çıplak gözle görülebilen ve belirli yönetmelikler veya standartların karşılandığını belirten bir simge şeklini almaktadır.

Bununla birlikte, çocukların ve ailelerinin uygun çevrimiçi içeriğini tanımasına ve bu alandaki uluslararası iyi uygulamaların paylaşılmasına imkân tanıyan güven markası ve sınıflandırma sistemleri için kriterler geliştirilmesi Avrupa Konseyi için özellikle de her yıl Birleşmiş Milletler¹ tarafından düzenlenmekte olan İnternet Yönetişim Forumu yoluyla ön planda olmaya devam etmektedir. Sitelerin sınıflandırılması sadece küçükleri koruma ve çevrimiçi işlemlerin kullanımında halkın güvenliğini arttırmanın bir yolu değil, aynı zamanda içerik sağlayıcıların yasal standartlara uygunluğunu teşvik etmektedir.

1. www.intgovforum.org

■ PEGI, oyunlarda ve uygulamalarda bulunacak yaş sınırlamaları ve içerik türlerine ilişkin rehberlik sağlaması nedeniyle, Avrupa Komisyonu tarafından desteklenen bir Avrupa çevrimiçi sınıflandırma sistemidir (Oyunlara ilişkin Kılavuz Metin 16'ya bakın). Oyunların, uygulamaların ve belirli çevrimiçi içeriğin yaş sınırlamaları ve içerdikleri içeriğin türünün belirtilmesi hakkında rehberlik sağlar. Ayrıca, içerik sağlayıcılarının, diğer şeylerin yanında, web sitelerinin kullanıcı tarafından üretilen yasadışı ve rahatsız edici olmayan içerik ve istenmeyen bağlantılar bulundurmamaya çalışma yükümlülüğü, mahremiyeti korumak ve bağımsız şikâyet mekanizmalarına sahip olmak gibi kalite standartlarına saygı duyduğunu da gösterir.

■ Kalite ve güven markası sınıflandırmaları, alışveriş ve diğer çevrimiçi işlem sitelerinde, güvenli işlemler için düzenleme ve kurallara saygı duyduklarını belirtmek için bulunabilir (çevrimiçi alışveriş hakkında Kılavuz 13'e bakın). Görebileceğiniz en sık sembollerden biri, üzerinde bulunduğunuz web sitesindeki sayfanın SSL (güvenli yuva katmanı) protokolünü (verileri şifreleyen ve sunucuyu ve mesajın bütünlüğünü doğrulayan bir veri aktarım güvenlik standardı) veya TLS (taşıma katmanı güvenliği) protokolünü belirten bir asma kilit simgesidir. Dolayısıyla, verilerinizin, özellikle bankacılık bilgilerinizin güvenli olduğunu varsayabilirsiniz.



FİLTRELEME

■ Filtreleme, genellikle, İnternet'teki uygun olmayan platformları ve/veya içeriği tespit etme ve engelleme işlemi olarak anlaşılır. Tarayıcılar ve Proxy'ler (vekil sunucular) içinde veya ebeveyn denetimleri gibi yazılım denetleyicileri yükleyerek yapılabilir. Filtreler; ebeveynler, okullar, işletmeler, hükümetler ve diğerleri tarafından oluşturulan kurallara göre oluşturulmuştur. Bunlar genellikle "kara" listeler (engellenecek içerikler) veya beyaz listeler (bunlar, filtrenin onayladığı öğeler dışında tüm İnternet içeriğine erişimi engeller) aracılığıyla çalışırlar. Bazen, taşıyıcı veya servis sağlayıcının uygulamalar, içerik ve medya üzerinde kontrol sahibi olduğu ve onaylanmayan uygulamalara veya içeriğe uygun erişimi kısıtladığı bir yazılım sistemi içinde beyaz listeler bir araya getirilir. Çocuklar için böyle bir sistem kurulduğunda, tüketicilerin uygulamalara, içeriğe ve daha fazlasına sınırsız erişime sahip olduğu açık bir platformun aksine "duvarlı bahçe" veya "kapalı platform" ² olarak ifade edilir.

■ Başka bir filtreleme yöntemi; kurallar, anahtar sözcükler veya terimlerle girildiğinde, yasaklanmış sözcükleri veya cümleleri içeren herhangi bir web sayfasına erişimi kısıtlaması veya tamamen engellemesidir. Filtreleme kurallarını belirleyen kişi bir şifreyle sitelere geçici (ad hoc) erişime izin verebilir³.

■ Günümüzde çoklu cihaz filtreleri mevcuttur. Filtreleme yazılımı veya uygulaması bir dizüstü bilgisayar, tablet, akıllı telefon, televizyon veya e-Okuyucu gibi çeşitli cihazlara yüklenebilir ve merkezi olarak, örneğin ebeveyn tarafından kontrol edilebilir. Farklı yaşlardaki çocuklar için farklı kurallar belirlenebilir ve bunlar, çocuğun yaşına göre otomatik olarak gelişebilir. Filtreleme kuralları çevrimiçinde geçirilen zamanı ve irtibatlara erişimin yanı sıra coğrafi konum ve çok daha fazlasını izlemek için de uygulanabilir.



EĞİTİM

- Beyaz listeler, çocukların en sevdikleri siteleri tanımalarını ve hızla erişmelerini sağlamalarında İnternette ilk adımlarını attığı zaman özellikle değerlidir. Bu sadece onların, okuma öncesi bir gereklilik olan, görsel ayırt edişlerini geliştirmelerine yardımcı olmaz, aynı zamanda çocuğunuzun çevrimiçi ortamdaki güvenliğini sağlamada çok önemli bir unsur olan internet faaliyetlerinin ortak aile faaliyetleri haline gelmesine yardımcı olur.
- Filtreleme, küçük yaştakileri internetteki uygun olmayan içerikten korumak veya kullanımını izlemek için çok yararlı bir tamamlayıcı unsur olabilir, ancak ebeveynlerin, öğretmenlerin ve çocuk bakıcıların uygun rehberliğiyle birlikte kullanılmalıdır.

2. https://en.wikipedia.org/wiki/Closed_platform

3. <http://internet-filter-review.toptenreviews.com>

- Sınıf ortamında, filtreler öğrencilerin uygunsuz veya zararlı materyallere erişim riskini azaltmak için değerli olabilir. Bununla birlikte, internet tabanlı ödevleri belirlemeden önce öğrencilere önerilen siteleri kontrol etme ihtiyacını azaltmazlar.
- Daha Güvenli İnternet Programı kıyaslama çalışması (SIP Bench) bugünün filtreleme araçlarının, İnternet'in çocuklara ve gençlere sunduğu fırsatlara ciddi olarak zarar vermeden olası zararlı içeriği filtreleme kapasitesine sahip olduğunu göstermektedir. Daha fazla ayrıntı Daha Güvenli İnternet Programı sitesinde mevcuttur⁴.
- Sınıflandırma ve filtreleme uygulamalarıyla gündeme getirilen konular vatandaşlık ve / veya sosyal çalışmalar temaları açısından zengin niteliktedir. Çevrimiçi filtreleme konusuyla ilgili bir tartışma başlatın. Çevrimiçi filtreleme sansürün kabul edilebilir ve gerekli bir biçimi midir?



KONULAR

- İçerik filtreleme, değerli bilgi ve kaynaklara, örneğin içerdikleri belirli anahtar kelimeler nedeniyle Dünya Savaşı tarihi veya cinsel eğitime erişimi engelleyebilir.
- Ülkelerin web sitelerinin sınıflandırması ve derecelendirmesi, ülkelerin bazı standartları uygulamak için yasalara sahip olduğu durumlar haricinde, büyük ölçüde gönüllü bir uygulama olarak kalır. Küresel bir dünyada yaşıyoruz ve bu standartların etkisi, platform ve içerik sağlayıcıları, ortak bir sınıflandırma ve derecelendirme sisteminin olmaması sebebiyle sınırlı artışlarla bir ölçüde tesir altında kalmıştır.
- Mevzuat teknolojik gelişime ayak uyduramamaktadır ve bugün hala filtreleme yazılımı hizmetleri, sayfaları kendi değer sistemleri ve sosyal gündemlerine göre sınıflandırma eğilimi içermektedir.
- Belirli yaştaki çocuklar için hangi içeriğin gerçekten zararlı olduğuna, içerik sağlayıcıların gözlemleyeceği genel kurallara kimin karar vereceğine ve bu kuralların uygulanması konusunda kimlerin karar vermesi gerektiğine karar vermek zordur. Bu sebeple, çocuk bakıcıların filtreleme kurallarını aile değerlerine göre şekillendirmelerini sağlamak için filtreleme araçlarının çok esnek olması gerekmektedir. Filtre tedarikçileri, bu kriterlere uygun filtrelemelerini sağlamak için teknikler geliştirmelidir.
- Filtreler aynı zamanda kamuoyunu şekillendirmek ve siyasi muhalefeti bastırmak için kullanılan bir sansür aracı olabilir. Bazı ülkeler muhalif siyasi partilerin veya ideolojilerin sitelerini engellemektedir; bu sınıfta insan haklarını ve demokrasiyi tartışmak için ilginç bir başlangıç noktası olabilir.
- Bazı insanlar filtrelemeyi bir sansür şekli olarak, dolayısıyla bunun internetin ruhuna karşı olduğunu değerlendirir. Bazıları ise eğer filtre yazılımı bulunmasaydı, hükümetlerin çevrimiçi içeriği düzenlemek için baskı altına gireceğini iddia ederler.
- Filtreleme yazılımı satıcıları; sosyal medyanın, mobil cihazların ve giderek daha genç yaştaki çocukların İnternet kullanımının zorluklarıyla başa çıkmak için uğraş vermektedir.
- Potansiyel olarak zararlı, kötü amaçlı veya uygun olmayan çevrimiçi içeriklerden korumak amacıyla çocuklar için uyarlanmış siteler için “.org,” “.com” ve benzeri yerini alacak bir “.kids” alanı yaratmaya yönelik uluslararası tartışmalar sürmektedir. Kayıt kurallarına uymak için “.kids” alan adını kullanan siteler gerekli olduğundan, uluslararası kabul gören standartları oluşturmak, uluslararası bir izleme ajansı seçmek vb. birçok zorluklar içindedir.

⁴.<http://www.sipbench.eu>



NASIL

- Yaratınızın, ulusal veya uluslararası standartlara göre puanlandırılmasını isteyen bir oyun veya uygulama geliştiriciyseniz veya sadece süreci anlamak isteyen bir ebeveyn veya bakıcıysanız, Uluslararası Yaş Derecelendirmesi Koalisyonu web sitesindeki (IARC) "nasıl " videosunu izleyin⁵. Tarayıcı ve işletim sistemlerinin çoğu, istenmeyen içeriği filtrelemek üzere ayarlayabildiğiniz yerleşik ebeveyn denetimlerini içerir. "Tüm aygıtlarımda sinir bozucu olmayan ebeveyn denetimlerini nasıl kurarım?" adlı blog⁶, bunu geniş bir aygıt ve yazılım yelpazesinde nasıl yapacağınız hakkında bilgi sağlamaktadır. Çoğu filtre programıyla, filtrelemek veya izin vermek istediğiniz içerik türlerini belirtebilirsiniz. Bununla birlikte, önceden kurulmuş filtreler, özellikle iki veya daha fazla kullanıcı için farklı kurallar belirlemek isterseniz tüm gereksinimlerinizi karşılamayabilir. Siteleri filtrelemek ve kullanımı izlemek için daha karmaşık bir yaklaşım için özel bir program satın almanız gerekecektir. En güncel daha Güvenli İnternet Programı raporu⁷ ve İnternet yazılımı değerlendirmeleri⁸ piyasadaki mevcut geniş ürün yelpazesinden seçim yapmada faydalı olabilir.



İYİ UYGULAMA

- Bir filtrenin kurulumundan önce nasıl çalıştığını yakından inceleyin. Filtrelemesinde, aynı fikirde olmadığınız herhangi bir ideolojik veya kültürel karar öneriyor mu?
- Elektronik yardım malzemelerini ayırt ederek kullanın ve yutturmacaya/hype inanmayın. Ürün iddialarını kişisel deneyim karşısında test edin. Bütün internet kullanıcılarının yaşları ne olursa olsun geliştirmeleri gereken "eleştirel düşünme filtresinin" yerini alacak hiçbir filtre olamaz.
- Öğrenciler, veliler ve çalışanlarla kullanımları ve ihtiyaçları hakkında konuşun ve bunu düzenli olarak yapın. Açık bir tartışma ortamı yaratmak, öğrenenlerin İnternet deneyimine değer katmak için sansür veya cadı avlarından çok daha fazlasını yapacaktır. Uzmanlar, çocukların sorumlu İnternet kullanımını geliştirmenin anahtarı olarak, ebeveynlerin çocuklarının çevrimiçi etkinliklerine ilgi göstermelerini ve onlarla çevrimiçinde vakit geçirmelerini önermektedir.
- En genç İnternet kullanıcıları için "sadece onaylanmış sitelere erişime izin veren" "beyaz listeleme" seçeneklerini göz önünde bulundurun. Favori ve diğer çocuk dostu web sitelerini tarayıcınıza yerleştirerek çocuklarınız için kişisel bir liste hazırlayın ki böylece daha önce kullandıkları güvenli sitelere kolayca erişebilsinler.
- Çocuklar ve gençler İnternette buldukları uygunsuz materyal hakkında konuşmaya teşvik edilmelidir. Gençler, çevrimiçi ortamda karşılaştıkları ahlaki konularda aileleri ile konuşamamalarının kendileri için büyük bir zorluk olduğunu defalarca iddia etmektedir. Olası yasadışı olan içeriği bir şikâyet hattına bildirin⁹.
- Çocuklarınızın oyun web sitelerindeki etkinliklerini izleyin ve güvenli siteleri ayırt etmek için PEGI Çevrimiçi sınıflandırmasını arayın.
- Giderek artan sayıda çevrimiçi topluluk içeriği sınıflandırmaya yardımcı olmak açısından kendilerine olan güvenleri, özellikle de içerik kullanıcı tarafından üretildiğinde, daha da artmaktadır. Yüklediğiniz tüm içeriği sınıflandırdığınızdan ve uygunsuz şekilde sınıflandırılmış içeriğin işaretlenmesine yardımcı olduğunuzdan emin olun.

4. <https://www.globalratings.com>

5. <http://web.archive.org/web/20160528132556/http://liferhacker.com/5868750/how-do-i-set-up-non-annoying-parental-controls-on-all-my-devices>

6. <http://www.sipbench.eu/>

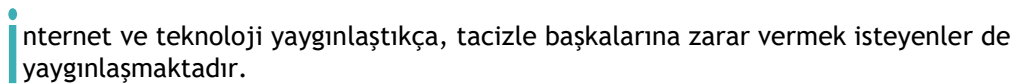
7. <http://internet-filter-review.toptenreviews.com>

8. <http://www.inhope.org>



DAHA FAZLA BİLGİ

- Wikipedia'da siberuzayda sansürün girişi bulunmaktadır:
<http://en.wikipedia.org/wiki/Censorship_in_cyberspace>.
- Avrupa Konseyi medya bölümü web sitesi, öz-denetim ve kullanıcı güçlendirmesini teşvik eden çalışmalar hakkında bilgi vermektedir: <<http://www.coe.int/media>>.
- NetNanny at <<http://www.netnanny.com>> ve Cyberpatrol at <<http://www.cyberpatrol.com>> en iyi tanınan ticari filtreleme ürünleri arasındadır.
- Electronic Frontier Foundation (EFF), internette sivil özgürlükleri savunmayı amaçlamaktadır: <<http://www.eff.org/>>.
- AB tarafından finanse edilen SIP-Bench projesi, her yıl dokuz dilde filtreleme ürünlerine ilişkin karşılaştırmalı anket sonuçlarını yayınlamaktadır: <<http://www.sipbench.eu/>>.
- Avrupa Konseyi'nin gençler, esenlik ve çevrimiçinde risk (2006) araştırması, bilgi toplumunda çocukların ve gençlerin korunmasında zararlı içeriğin anlamını araştırıyor:
<<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680483b30>>.
- PEGI Çevrimiçi sınıflandırma sistemi web sitesi, çevrimiçi oyun, kategoriler, riskler, güvenlik ipuçları ve sınıflandırılmış web sitelerinin listesi hakkında bilgi sunmaktadır :
<<http://www.pegonline.eu>>.
- İnternet filtreleri ile ilgili olarak ifade ve haber alma özgürlüğüne saygının arttırılmasına yönelik tedbirler konusunda Bakanlar Komitesinin üye devletlere CM/Rec (2008) 6 sayılı Tavsiye Kararı:<[https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec\(2008\)6&Language=lanEnglish&Ver=original&direct=true](https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&direct=true)>.
- İlgili Avrupa Konseyi belgeleri: sınıflandırma ve filtreleme hakkında daha fazla bilgi için:
<www.coe.int/en/web/freedom-expression/internet-standard-setting>.



1. Görüşülen kişilerin% 40'ı kişisel olarak çevrimiçinde tacizi yaşadı.
2. Genç yetişkinler, çevrimiçi tacizi yaşamaları en muhtemel demografik gruptur.
3. Erkekler ve kadınlar çevrimiçi taciz ile farklı deneyimlere sahiptir.
4. Çevrimiçi taciz edilenlerin yarısı bunun arkasında kimin olduğunu bilmemektedir.
5. Sosyal medya taciz sahnesinin en fazla görüldüğü yer olmuştur.

— Çevrimiçi taciz, hedeflenen bireylere karşı aşağılayıcı veya rahatsız edici yorumları sürekli olarak yöneltmeyi içerir. Sözelimi, siber zorbalık, siber taciz, trolleme veya nefret yaymak gibi çeşitli biçimlerde olabilir. Örneğin;



SİBER ZORBALIK

- Dünya Sağlık Örgütü, zorbalık davranışını, "kendine, başka bir kişiye karşı ya da bir gruba ya da topluluğa karşı, yaralanma, ölüm, psikolojik zarar, kötü gelişim ya da yoksunlukla sonuçlanması veya olasılığı yüksek olan, tehdit edici ya da gerçek, kasıtlı fiziksel ya da psikolojik güç ya da kuvvet kullanımı olarak kabul eder." (Dünya Sağlık Örgütü - 2002) Dünya şiddet ve sağlık raporu: özet¹.
- Zorbalık, zarar vermek için başka bir kişiye karşı yapılan ve belirli bir süre boyunca çeşitli şekillerde tekrarlanan bir eylemdir. Ebeveynler ve çocuklar genellikle bu sorunun ölçeği ile ilgili aynı algıya sahip değildir.
- Zorbalık birçok biçime sahip olabilir: fiziksel zorbalık, sözel zorbalık, ilişkisel saldırganlık, cinsel zorbalık, önyargısal zorbalık, gasp ve siber zorbalık gibi birçok biçime sahip olabilir.
- Siber zorbalık, saldırgan veya kötü niyetli mesajlar, e-postalar, sohbet odaları veya mesaj panosu yorumları, hatta en aşırısı, bir kişiye veya belirli bir grup insana yönelik zararlı bir niyetle kurulmuş web sitelerini içeren, İnternet veya cep telefonu yoluyla zorbalık yapmaktır.
- Siber zorbalık, cep telefonlarını, başkalarının utanç verici görüntülerini almak veya can sıkıcı SMS veya MMS mesajları göndermek için kullanılmaktadır. Çevrimiçi zorbalığın her biçimi, normal zorbalığa göre daha büyük etkiye sahiptir, çünkü yazarlar **anonimlik/isimsizlik/tanınmama** hissiyle güçlenmekte ve mağdurların zorbadan saklanacak yerleri bulunmamaktadır- sanal olarak nerede olurlarsa olsunlar gece ve gündüz kurban olabilirler.
- Siber takip, bir kişiyi, bir grubu veya bir organizasyonu takip etmek veya taciz etmek için İnternet'in veya diğer elektronik araçların kullanılmasıdır².
- Trolleme, bir haber grubu³ veya blog gibi çevrimiçi bir topluluğa tahrik edici, ilgisiz veya konu dışı mesajlar göndererek tartışmalar başlatarak veya insanları rahatsız ederek internette sorunlara neden olma eylemidir.
- Trolleme, okuyucuları duygusal bir tepki için provoke etmek veya konuyla ilgili normal tartışmayı bozmak amacıyla bilinçli bir niyetle yapılır⁴.
- Siber takip, trolleme ve zorbalık genellikle daha geniş çevrimiçi taciz şemsiyesi altında değerlendirildiği için, aşağıdaki rehber ilkeler ve bilgi, münferit durumlara göre uyarlanabilir.



DAYANIKLILIĞIN ÖNEMİ VE SOSYAL VE DUYGUSAL ÖĞRENME

- Sosyal ve duygusal dayanıklılık ve **iyilik durumu**, gençlerin zorbalık ve diğer saldırgan çevrimiçi davranışlara karşı korunma geliştirmeleri için önemli faktörlerdir.
- Pozitif bir okul iklimi veya olumlu bir toplumsal çevre, çevrimiçi ve çevrimdışı zorbalığın ve daha genel olarak çevrimiçi tacizin **etkisini düşürebilir**.
- Ebeveynler, çocuklarının dayanıklılık geliştirmelerine; onların kendilerini tanıma ve benlik saygısını artırmalarına yardımcı olarak, onlara, oldukları gibi kabul edildikleri ve sevildiklerini göstererek; zor durumlara uyum sağlama, ele alma ve bunları aşmayı öğreterek; olumlu duyguları teşvik ederek, yaşamda zevk ve mizah bularak; problem çözme becerilerini geliştirerek; yanıtlarında esnek olmayı öğrenerek ve onlara empatinin önemini göstererek yardımcı olabilirler.

1. http://www.who.int/violence_injury_prevention/violence/world_report/en/summary_en.pdf

2. <https://en.wikipedia.org/wiki/Cyberstalking>

3. https://en.wikipedia.org/wiki/Usenet_newsgroup, forum, chat room <https://en.wikipedia.org/wiki/Chat_room

4. https://en.wikipedia.org/wiki/Internet_troll



ETİK DÜŞÜNCELER VE RİSKLER

- Sınıfta zorbalık ve taciz, korku ve güvensizlik ortamı yaratarak bütün sınıfın moralini düşürebilir ve öğrenmeyi neredeyse imkânsız hale getirir.
- Zorbalığa maruz kalanlar veya taciz kurbanı olanlar için en sık görülen etkiler arasında depresyon, kaygı, düşük benlik saygısı, sosyal uyum zorlukları ve yalnızlık bulunmaktadır.
- Failller için en sık görülen etkiler arasında kaygı artışı, okulda başarısızlık riski ve sıklıkla kabahatli davranışlar ve yetişkin suçluluğu olasılığı artışı bulunmaktadır.
- Zorbalık veya tacizin bir sorun haline gelmesini önlemeye yönelik önleyici bir tedbir olarak, müfredatınıza sosyal ilişkiler yönetimi, öfke yönetimi ve uyuşmazlık çözümünü koymaktır. Bu tür iyi seçilmiş programlar çocukların ve gençlerin uyuşmazlıklarda potansiyel araçlar olarak kendi yeteneklerini keşfetmelerini sağlayacaktır. Bu şekilde, küçük çaplı uyuşmazlıkların tehdit eden davranışlara dönüşme riski çevrimdışı ve çevrimiçi olarak azaltılacaktır.
- Okulunuzun, öğrencilerin ve çalışanların okulda interneti ve cep telefonlarını ne zaman ve nasıl kullandıklarını izlemek için açık bir politikası olmalıdır - genelde sorumluluk sahibi veya kabul edilebilir kullanım politikası (RUP veya AUP)⁵ - olarak bilinir. Bu belge, kaba, zorba veya taciz edici dile ve eylemlere müsamaha gösterilmeyeceğini açıkça belirtmelidir. İnternet veya cep telefonunu uygun olmayan bir şekilde kullanan herkesin doğrudan sonuçları hakkında açıkça bilgilendirilmesi gereklidir.
- Bazı veri koruma sorunlarına neden olabileceği halde, kimlerin çevrimiçinde olduğu, ne zaman ve nerede olduğu dahil olmak üzere İnternet kullanımını belgeleyen bir işlem süreci bulunmalıdır.
- Öğrencilere, onları taciz eden veya çevrimiçi olduğunda onları herhangi bir şekilde rahatsız eden herhangi biriyle görüşmeyi kesmeleri tembihlenmelidir.
- Öğrenciler derhal güvenilir bir yetişkine neler olup bittiğini söylemeli ve mümkünse saldırgan malzemeyi göstermelidir. Daha sonra yetişkin, okulun AUP veya RUP'da belirtilen işlemleri takip etmesi gereklidir.
- İşlem süreci, gerçek hayatta, birisi tarafından taciz edilen bir çocukta olduğu gibidir. Çocuk fail ile olan temasını kesmeli ve güvenilir bir yetişkine olan olayı söylemelidir. Çocuk, sanki yalnızmış gibi veya kendi kendine baş etmeliymiş gibi hissetmemelidir.

Özetlemek gerekirse, okul İnternet ve cep telefonu kullanımı politikası, çatışma çözümü, öğrenci ve çalışanlarına çevrimiçi taciz durumunda ne yapılması gerektiği konusunda eğitim verilmesi, istismar hedeflerine olumlu destek sağlanması ve mümkün olan yerlerde istismarcılara davranışlarını değiştirmek için yardım gibi müdahale yöntemlerini içermelidir. Böyle bir politika uygulandığında, okulların zorbalık veya tacizle uğraşma konusunda çok az bir problemi olacaktır.



NASIL

Eğitmciler her zaman sınıfta ve sınıf dışında zorbalık ve tacizle uğraşmak zorunda kalmışlardır. Şimdi bu tür tacizin İnternet'i de nasıl içerdiğini anlamak zorunlu hale gelmiş bulunmaktadır.

- Öğrencilerin kendi eylemleri için sorumluluk alabilmeleri gerekir; ancak zorbalık ve taciz, güven ve benlik saygısını zayıflatır. Bir kişi taciz edildiğinde veya zorbalığa maruz kaldığında odaklanmadığı için öğrenme kısıtlanır, tehdit altında hisseder ve kendine güvenini yitirir.
- Tehdit altında hisseden öğrenciler (çevrimiçi veya çevrimdışı) güvenilir bir yetişkinin yardımına ihtiyaç duyarlar. Ayrıca, zorbalığı veya tacizi yapan kişinin de, bu davranışın gelecekte tekrarlanmaması için rehberlik edilmeye ihtiyacı olduğunu unutmamalısınız.
- Zorbalık ve tacizin ele alımı kabul edilemez davranışın doğası ve potansiyel nedeni ile birlikte uygulanabilecek düzeltici adımlar hakkında ailede veya sınıfta açık tartışmalar yoluyla küresel bir yaklaşım gerektirir.

5. https://en.wikipedia.org/wiki/Acceptable_use_policy

- Zorbalık ve taciz toplumsal sorunlardır. Öğretmenler ve ebeveynlerin sorumluluğu bu davranışın iddialarını araştırmak ve ailede ya da sınıfta çalışarak, sınıfta, oyun alanında ya da çevrimiçi çalışmada mümkün olan en iyi öğrenme ortamını sunmaktır.
- Zorbalık ve taciz sürecinin dinamikleri ve bunun için İnternet ve cep telefonlarının kullanım biçimleri hakkında öğretmenleri eğitin. Onlara, mağdurların yanı sıra saldırgan davranıştan sorumlu kişinin belirtilerinin/sinyallerinin nasıl okunacağını ve bu gibi belirtiler/sinyalleri fark ettiklerinde nasıl tepki verileceğini öğretin.
- Okulların belirli kuralları olmalıdır. Zorbalık ve tacizle baş etmek için okulunuzun İnternet politikasında önleyici tedbirlerin alınması iyi bir fikir olabilir.
- Öğrencilere, siber zorbalık veya siber tacize karşı dört altın kural öğretilmelidir:
 1. Mümkünse saldırgan malzemenin bir kopyasını oluşturun.
 2. Saldırgan malzemeyi başkalarına iletmeyin.
 3. Alıcı cihazı kapatın (bilgisayar veya cep telefonu).
 4. Olayı güvenilir bir yetişkine bildirin.



SINIF ÇALIŞMASI İÇİN FİKİRLER

- Rol canlandırma: Öğrenciler gerçek olmayan bir uyuşmazlık çözümü süreci canlandırmasına katılırlar. Öğretmen, rolleri belirler ve bir anlaşmazlığı çözmek için öğrencilerin sorumlu olduğu grupları düzenler. Bir sonraki adım, öğrencilerin konuya farklı bir perspektiften yaklaşmalarına izin vererek rolleri tersine çevirmektir.
- Tartışma grupları: Öğrenciler, genel olarak zorbalık, İnternette yapacakları ve yapmayacakları ve sorumlulukları gibi konulardaki izlenimlerini, grup çalışmalarına katılımlarını değerlendirmek için tartışma gruplarına katılırlar.



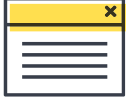
İYİ UYGULAMA

Çevrimiçi her türlü zorbalık ve taciz e-postaları veya mesajlarının nasıl ele alınacağıyla ilgili bazı fikirler aşağıda verilmiştir:

- Öğrencilere bilinmeyen kaynaklardan gelen e-postaları açmamaları söylenmelidir.
- Eğer bir e-posta veya metin mesajı açılıp saldırgan/hakaret edici bulunursa, güvenilir bir yetişkine göstermek için rahatsız edici materyalin bir kopyasını çıkarın. Bununla birlikte, mağdur saldırgan mesajlara asla tepki vermemelidir, çünkü bu yalnızca diğer kişiyi saldırgan davranışa teşvik eder.
- Bir kişi saldırgan veya taciz edici e-postalar veya mesajlar göndermeye devam ederse ve nereden gönderildiğini öğrenmek (bir e-posta adresi aracılığıyla) mümkünse, tacizi bildirmek için hemen o servis sağlayıcıya⁶ veya mobil operatöre başvurun.
- Bir okulun zorbalığa ilişkin politikaları ve/veya kabul edilebilir kullanıcı politikası, öğrenciler tarafından çevrimiçi tacizin nasıl ele alınacağı konusunda hükümler içermelidir.
- Öğrenciler, çevrimiçi ya da cep telefonlarından her ne zaman taciz edilirlerse, bir ebeveyn, öğretmen ya da başka bir güvenilir yetişkine gidebileceklerini bilmelidirler. Bu güvenilir yetişkinin hikâyeyi ciddiye alma ve mağduru rahatlatma rolü bulunmaktadır.
- Zorbalara veya tacizden sorumlu olanlara, davranışlarının müsamaha edilemeyeceğini ve derhal durması gerektiğini söyleyin ve aynı zamanda, onların motivasyonları hakkında neler bulabileceğinize bakın. Gerçek hayatta aynı şeyleri söylemeye veya yapmaya cesaret edebilirler miydi?
- Her zaman ebeveynler, kendi çocuklarının zorbalığa uğrayıp, uğramadığı ya da birine zorbalık yapıp yapmadıkları konusunda farkındalık sağlamak için daima gayret göstermelidir. Bir zorba, İnternet veya cep telefonunu zorbalık için kullandığında saldırgan davranışlar genellikle okul kapısında kalmaz, muhtemelen evden de devam eder.

6. https://en.wikipedia.org/wiki/Internet_service_provider

- ENABLE⁷ (Öğrenme ve Boş Zaman Ortamlarında Zorbalığa Karşı Avrupa Ağı), Avrupa Komisyonu tarafından finanse edilen ve zorbalıkla mücadeledeki en başarılı yaklaşımların yanı sıra sosyal ve duygusal öğrenme hakkında derinlemesine bilgi veren bir projedir ve okullar için ebeveyn paketleri ve akran eğitimi araç takımları sağlar.



DAHA FAZLA BİLGİ

- Avrupa Konseyi "Zorbalığı yenin" web sayfası zorbalığa karşı araçlar sunmaktadır: www.coe.int/en/web/edc/beat-bullying.
- Nobullying.com zorbalık ve siber zorbalık kaynaklar sağlar. <http://nobullying.com/>.
- Yunanistan'da bulunan Çocuk Gülümsemesi web sitesi, çocukların yaşadığı günlük sorunlarla ilgili yardımlar sunmaktadır: <http://www.hamogelo.gr/1.2/home>.
- "Zorbalığa Son Verin": <http://www.stompoutbullying.org> "Zorbalığa şimdi son verin!" ABD'li bir internet sitesinde zorbalık oranını azaltmayı amaçlamaktadır: <http://www.stompoutbullying.org> <http://www.stopbullyingnow.com/>.
- "#DeleteCyberbullying" siber zorbalık konusunda tavsiyeler veren etkileşimli bir Android uygulamasıdır: <https://deletecyberbullying.wordpress.com/app/>.
- "Riskleri bilin: siber zorbalığı zorlamak" ebeveynlere ve öğretmenlere yöneliktir: http://web.archive.org/web/20100923133231/http://www.media-awareness.ca/english/teachers/wa_teachers/safe_passage_teachers/risks_bullying.cfm.
- "Siber zorbalık nedir?" Ailelere tavsiyelerde bulunan Avustralya Hükümeti web sitesidir: http://web.archive.org/web/20090703064421/http://www.netalert.gov.au/advice/risks/cyber-bullying/What_is_cyber_bullying.html.
- Zorbalık ve zararlı içerikleri Insafe ağına bildirin: <http://www.betterinternetforkids.eu>.
- Pew Araştırma Merkezi, "Çevrimiçi taciz" konusundaki bulgularının 2014 yılı özetini yayınlamıştır. <http://web.archive.org/web/20160703044152/http://www.pewinternet.org/2014/10/22/online-harassment/>.
- Nefret Söylemine Hayır Hareketi, Avrupa Konseyi'nin gençlik kampanyasıdır: <http://www.nohatespeechmovement.org/>.
- Zorbalık hakkında daha fazla bilgi edinin ve ders planları, ebeveyn paketleri ve akran eğitim setlerini indirin: <http://enable.eun.org>.

7. <http://enable.eun.org>

Yardım almak



İnternet, milyarlarca cihazı dünya çapında bağlamak için İnternet Protokol Paketini (TCP / IP) kullanan birbirine bağlı küresel bir bilgisayar ağları sistemidir¹. Bu sebeple diğer medyadan çok farklıdır. Çünkü mevcut iletişim ortamları arasında en fazla tek merkezde kontrol edilemeyen bir ortamdır. Bu milyarlarca gevşek bağlı cihazın, iletişim ve bilgi aktarımına izin vermek için çok çeşitli yollara sahip olması nedeniyle tek bir kontrol noktası bulunmamaktadır. Buna ek olarak, Web 2.0'in ortaya çıkmasından bu yana da çevrimiçi ağ kullanıcıları sadece izleyiciler değil aynı zamanda bilgi üreticisidirler. (bkz. Bağlanmak Kılavuz 1).

Günümüzde, herkes çevrimiçinde herşeyi yayınlayabildiğinden ve verilerimizin çoğu "bulut" olarak bilinen bulunması zor yerlerde saklandığı için İnternet'in geleceği ve bu bilgi akışının küçük parçalarını bile kontrol etmenin nasıl mümkün olabileceği konusunda bir çok soru sorulmaktadır. Sıklıkla kendimize, hangi konuşma ve bilgilerin çocuklarımız, ailemiz ve bizim için rahatsız edici veya tehlikeli olduğunu kimin belirleyebileceğini sorarız. Ve daha önemlisi, kendimizi ve sevdiklerimizi bundan nasıl koruyabiliriz?

1. <https://en.wikipedia.org/wiki/Internet>



YASADIŞI İÇERİK

Her ülke, ulusal mevzuatıyla yasal ve yasadışı olan içeriği ve eylemleri tanımlamaktadır. Buna göre, bir iletişim aracı olarak İnternet, düzenlenmiş bir alan olarak işlemektedir. "Gerçek hayatta" yasadışı sayılan herhangi bir işlemin İnternette de yasa dışı sayılması gerekir. Bununla birlikte, internetin büyük erişimi, başkalarının haklarına saygı ihlallerini artırabilir ve etkiyi çoğaltabilir; Örneğin, çevrimiçi "alay etme", hakarete veya daha kötüsüne dönüşebilir.

Yasaya aykırı olan veya bir kişi ya da varlık üzerinde zarar verebilen ve/veya önyargı oluşturabilen bir faaliyet, malzeme, bilgi ya da benzeri herşey, yasadışı içeriğin geniş kapsamı içinde yer alabilir.

Yasadışı içerik, çocuk istismarı görüntülerini ve web sitelerini, sohbet odalarındaki yasadışı faaliyetleri (grooming/kandırma gibi), çevrimiçi nefreti ve yabancı düşmanlığı mesajlarını, web sitelerini ve benzerlerini kapsar. Bu ve diğer yasadışı davranış biçimleri, İnternet ve diğer bilgisayar ağları yoluyla işlenen suçlarla ilgili ilk uluslararası sözleşme olan Avrupa Konseyi Siber Suç Sözleşmesi² ve bilgisayar sistemleri yoluyla işlenen ırkçı ve yabancı düşmanlığı niteliğindeki faaliyetlerin suç kapsamına alınmasına ilişkin Siber Suç Sözleşmesi Ek Protokolü³ içinde yer almaktadır. Çocukların Cinsel Sömürü ve Cinsel İstismara karşı korunmasına ilişkin Avrupa Konseyi Sözleşmesi (veya Lanzarote Sözleşmesi)⁴, verilerin yetkisiz olarak toplanmasını ve saklanması ile bilgi madenciliğini de kapsar. Bu Sözleşme, kandırma da dahil olmak üzere çocuklara yönelik her türlü cinsel şiddete ceza getiren ilk uluslararası sözleşmedir.



YARDIM ALMAK TEMEL BİR HAKTIR!

İnternet her yerden ve herkes tarafından erişilmesi kolay bir araçtır ve bu nedenle zararlı veya uygun olmayan içerik, çocuklara, gençlere ve diğer savunmasız gruplara kolayca erişebilir. Evrensel İnsan Hakları Beyannamesi⁵ uyarınca, her tür zarar ve ziyana karşı ayrımcılığa veya ihlale karşı, korunma hakkı temel bir insan hakkıdır. BM Çocuk Hakları Sözleşmesi (UNCRC), yetişkinlerin çocuğun çıkarlarını en iyi şekilde korumak üzere davranmalarına ilişkin rollerini -ve dolayısıyla onu zararlı içerik ve eylemlerden koruyarak- vurgular ve hükümetlere ile ailelere, çocuk haklarına saygı gösterilmesini, korunmasını ve bunların uygulanmasını sağlamak için tüm önlemleri almaları sorumluluğunu verir. Bu, sosyal hizmetleri ve çocukları desteklemek için hukuk, sağlık ve eğitim sistemlerini temin eder ve onların büyüyüp olgunlaşmalarına ortam sağlamayı da içermektedir. Bu sistemler içinde, yardım hatları ve diğer bildirim mekanizmaları da önemli bir unsurdur.

Diğer uluslararası örgütlerin yanı sıra özellikle uluslararası İnternet Yönetişimi Forumundaki faaliyetler kapsamında Avrupa Konseyi, çocukların ve gençlerin internette korunması ile ilgili sosyal ve aile bilincini geliştirmeye çabalamaktadır. Bu çabalar, uygun yardımı elde etmek için mevcut araçlar ve prosedürler konusunda kolay bulunabilir bilgi sağlamayı da içermektedir.



NASIL

- İnternette bulunan herhangi bir yasadışı nitelikteki içerik bir şikayet hattına bildirilebilir. Bu hat⁶, internette yasadışı olduğu düşünülen herhangi bir içeriğin herkes tarafından şikayet edilebileceği bir hizmettir. INHOPE, dünyadaki birçok ülkedeki internet şikayet hatlarını koordine eden bir dernektir⁷. INHOPE'un ilgilendiği yasal olmayan içerik türü hakkında web sitelerinden daha fazla bilgi edinebilirsiniz⁸.
- Yasadışı içeriği bildirmek için <<http://www.inhope.org/tns/contact-us/details.aspx>> adresine gidin ve belirtilen adımları izleyin. Şikayet hattı, içeriğin yasadışı olup olmadığını görmek için raporu araştırır⁹ ve eğer varsa, bu içeriğin kaldırılması için kaynağını inceler ve ev sahibi ülkedeki kolluk kuvvetleri ile internet servis sağlayıcısına başvurur.

2. <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185>

3. <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>

4. <http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=12/18/2008&CL=ENG>;

<http://www.coe.int/en/web/children/lanzarote-convention>

5. <http://www.un.org/en/universal-declaration-human-rights/index.html>

6. <http://en.wikipedia.org/wiki/Hotline>

7. <http://inhope.org/gns/who-we-are/at-a-glance.aspx>

8. <http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/illegal-content.aspx>

9. <http://www.inhope.org/en/about/faq.html>

Yardım hattından yardım istemek

- Çocuklar ve gençler, e-posta, web veya sms yoluyla telefonla destek ve/veya danışmanlık hizmeti sunan bir yardım hattını¹⁰ arayarak yardım talep edebilirler.
- Birçok ülkede, Insafe farkındalık merkezleri¹¹, gençlerin çevrimiçi deneyimleri veya karşılaştıkları zararlı veya yasadışı çevrimiçi içeriği ile bağlantılı sorularını ve endişelerini yanıtlamak için ulusal yardım hatlarıyla işbirliği yapmaktadır. İnternetle ilgili sorunları ele alan birçok yardım hattı da, gençlere daha geniş kapsamlı diğer "gerçek dünya" sorunlarında da yardımcı olabilir.
- Uluslararası Çocuk Yardım Hattı (Child Helpline International)¹², birçok Avrupalı ve Avrupa dışı ülkede önemli bir irtibat noktasıdır. Bu küresel çocuk yardım hatları ağı, çocukların haklarını korumak için yaklaşık 150 ülkede faaliyet göstermektedir.
- Normal olarak, yardım hatları günde 24 saat, haftanın 7 günü açıktır. Hizmetlerinin tümü ücretsiz ve gizli olup aramaları, e-postaları veya metinleri izlememektedirler. Çocuklar ve gençler çok çeşitli konularda yazabilirler ve gençlerin daha geleneksel yöntemlerin yanı sıra sohbet, e-posta ve forumlar yoluyla iletişim kurmalarını sağlayan olanaklar bulunmaktadır. Yardım hattı personeli, onları dinlemek ve kendi çözümlerini geliştirmelerine yardımcı olmak için oradadır.
- Ülkenizde bir yardım hattı bulmak için, ülke adı ve "bildirim/report" ve "yardım hattı" sözcükleri ile ağ üzerinde arama yapabilirsiniz.

Sosyal medya platformlarıyla ilgili özel rapor hizmetlerinin kullanılması

- Facebook, Twitter, Instagram veya Google gibi çoğu sosyal medya platformunda kullanıcılara rehberlik edecek bir güvenlik merkezi ve uygunsuz içerik veya etkinlikleri bildiren çevrimiçi bir raporlama hizmeti bulunmaktadır. Bu genellikle "Destek" veya "Yardım" menüsünde bulunur. Örneğin zorbalık olaylarını sosyal paylaşım sitelerine bildirmek, rahatsız edici içeriğin kaldırılmasına ve hatta kullanım şartlarını ihlal eden kişilerin hesaplarının silinmesine neden olabilir. Çoğu site benzer şekilde çalışmaktadır: Örneğin, Facebook'ta her içerik, kullanıcıların bir yazı veya fotoğrafı bildirmesine ve neden onu görmek istemediğini söylemesine olanak tanıyan bir açılır menü içerir. Bu sayfada bildirim yapma/raporlama hakkında bilgi bulunmaktadır¹³.
- Tüm cep telefonu operatörleri, telefon, web sohbet veya e-posta yoluyla yardım sağlamaktadır ve birçoğu da özellikle ailelere ve çocuklara yönelik tavsiyeler vermektedir. Örneğin Vodafone, ebeveynlere ve çocuklara tavsiyelerde bulunan bir "sayısal ebeveynlik" web sitesi¹⁴ ve ebeveyn kontrolleri kurmak için "nasıl" kılavuzlarının yanı sıra SecureNet¹⁵ aracılığıyla ebeveyn denetimleri ve diğer güvenlik özelliklerinin sunumunu sağlamaktadır. Android cihazlardaki Vodafone Guardian uygulaması, istenmeyen kişilerin engellenmesine de izin verir.



DAHA FAZLA BİLGİ

- UNCRC <<http://www.ohchr.org/en/professionalinterest/pages/crc.aspx>> ve/veya UNICEF tarafından geliştirilen genel değerlendirme belgesi <http://www.unicef.org/crc/files/Rights_overview.pdf> çocukların korunma ve yardım hakkına ilişkin daha fazla bilgi için danışın.
- Şiddete karşı korunma ve şiddeti haber vermeye ilişkin ayrıntılı bilgi için Avrupa Konseyi'nin şiddete karşı birleşik stratejisi faydalı bilgiler içermektedir: <<http://www.coe.int/en/web/children/integrated-strategies>>.
- Yasadışı içeriği bildirmek için INHOPE ile temasa geçebilirsiniz : <<https://www.inhope.org/>>.

10. <http://en.wikipedia.org/wiki/Helpline>

11. <http://www.betterinternetforkids.eu>

12. <http://www.childhelplineinternational.org>

13. <https://www.facebook.com/help/181495968648557/>

14. <http://www.vodafone.com/content/digital-parenting.html>

15. <https://securenet.vodafone.com/>

- İnternet güvenlik merkezleri Avrupa ağı olan INSAFE'in portalı <http://www.betterinternetforkids.eu/> Avrupa'daki ulusal irtibat noktaları ve yardım hatları hakkında bilgi sunmaktadır.
- Siber zorbalığı bildirmek veya yardım almak için Childline ile iletişime geçebilirsiniz <http://www.childline.org.uk/>, çocuklar ve gençler için 24 saat ücretsiz yardım hattı (Telephone: 0800 1111).
- Befrienders.org <http://www.befrienders.org> yardıma gereksinim durumunda en yakın intihar destek yardım hattınızı bulabileceğiniz bir web sitesidir.
- Europe Direct http://ec.europa.eu/europedirect/index_en.htm Avrupa Birliği konularında genel sorulara anında cevap ve ulusal yardım hatları gibi ilgili kuruluşların iletişim ayrıntılarını alabileceğiniz ücretsiz bir hizmettir.

6. İnternet – İnternetin Geleceđi

”Özgür ifade, insan haklarının temeli, insan doğasının kökü ve gerçeğın anasıdır. İnsan haklarını aşğılamak, insan doğasını ezmek ve gerçeđi bastırmak özgür konuşmayı öldürmektir.”

Liu Xiaobo, 2010 yılı Nobel Barış Ödülü sahibi ve insan hakları savunucusu

KILAVUZ 23 – NESNELERİN İNTERNETİ / INTERNET OF THINGS

Bilgisayarınızı ve diğeri cihazlarınızı güvenliklerine yönelik müdahalelerden halihazırda koruduğunuz şekilde "Nesnelerin İnterneti" cihazlarınızı da aynı önlemlerle koruduğunuzdan emin olunuz.

Her bir aygıtı korumanın zor olduğunu, ancak ağıınızı koruyabileceğınızı ve savunmasız alanlarınızı azaltabileceğınızı unutmayın.

Evinize ve çocuğunuza tanıtmayı planladığınız herhangi bir "Oyuncakların interneti" ürününü dikkatlice düşünün. Oyunağın güvenlik ve gizlilik parametrelerini kontrol edin ve kendinize şu soruyu sorun: "Bu oyuncak ne kadar gerekli?"

KILAVUZ 24 - YAPAY ZEKA, OTOMASYON VE YIKICI TEKNOLOJİLER

Yapay zeka ve otomasyon alanındaki en son gelişmeler hakkında kendinizi bilgilendirdiniz mi?

Kişiler arası, sosyal ve duygusal becerilerinize yatırım yaptınız mı?

Uygun seviyede güvenlik ve kullanıcı koruması sağlamak için "akıllı" cihazlarınızı kurdunuz mu?

KILAVUZ 25 - SANAL VE ARTTIRILMIŞ GERÇEKLİK/AUGMENTED REALITY

Cinsiyetçilik, cinsellik, ırkçılık, zorbalık, basmakalıplar ve ayrımcılığın diğeri biçimleri gibi temel konular hakkında çocuğunuzla / öğrencinizle konuştunuz mu?

Çocuğunuzun / öğrencinizin kullandığı cihazların, yüksek gizlilik ve güvenlik korumasıyla doğru şekilde kurulduğundan emin misiniz?

Sanal veya arttırılmış teknolojiyi kullanırken çocuğunuzun / öğrencinizin sağlıklı bir yaşam dengesini koruduğünü kontrol ettiniz mi?

KILAVUZ 26 - ÜRÜN SİZ MİSİNİZ? BÜYÜK VERİ, VERİ MADENCİLİĞİ VE MAHREMİYET

Özel verilerinizin kullandığınız çevrimiçi hizmetler tarafından işleme biçimini incelemek ve uygun ve yeterli gizlilik ayarlarını yapmak için zaman ayırdınız mı?

Son zamanlarda çevrimiçi yayınladığınız içeriğın hâlâ doğru olduğundan ve hâlâ paylaşmayı isteyip istemediğınızden emin olmak için gözden geçirdiniz mi?

Bu değişikliklerin sizi nasıl etkileyebileceğini ve bu konuda neler yapabileceğınızı öğrenmek için "büyük veri" hakkındaki son gelişmelerden haberdar mısınız?

Nesnelerin İnterneti



İnternetteki son gelişmeler ve veri özellikli cihazlara kablosuz bağlanmanın getirdiği teknolojik gelişmeler pek çok alanda heyecana neden olmaktadır. Şirket verimliliğini artıran ve yeni yaşam tarzına uygunluğu destekleyen web bağlantılı cihazlardan oluşan "Nesnelerin İnterneti" olarak bilinen bu yeni gelişme alanı, ebeveynlerde ve yakınlarında büyük endişe yaratabilir.

■ Güvenlik, mahremiyet ve veri toplama konusundaki endişeler, giderek daha fazla cihazın tasarlanıp satılmasıyla uzmanların ve politika yapımcıların ele aldığı hususlardır. Bununla birlikte, nesnelerin interneti, riskleri kısıtlamak ve hatta azaltmakla birlikte, bu yeni teknolojinin faydalarını desteklemek için uzmanlar ve politika yapımcılarına benzersiz yollar bulmaları konusunda özel bir fırsat sunmaktadır.

■ Tüketiciler sadece "nesnelerin birşeyler düşünmeye başlamalarından" endişelenmemeli aynı zamanda "nesnelere" erişen korsanlardan da endişelenmelidirler. Bir aracın motorunu durdurmadan önce, iki korsanın klima, radyo ve ön cam sileceği ile uzaktan oynadıkları "Korsanlar otoyolda bir cipi uzaktan öldürüyor"¹ adlı son makaleyi okuyun. Bu iki bilgisayar korsanının eylemleri, otomobiller ve kamyonlar için sayısal güvenlikle ilgili tartışmalara yol açtı.

1. <http://web.archive.org/web/20160703222843/https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway>

■ Bir diğer tartışma konusu ise nesnelerin internetinin bir sonraki endüstriyel devrim olduğu fikridir. Bugün yaklaşık olarak 10 milyar birbirine bağlı cihaz bulunmakta, ancak bu yeni akımın piyasadaki cihaz sayısındaki tahmini artışının 2020 yılına kadar 26 milyar ila 30 milyar arasında olacağı, piyasa değerlerinin ise 6 trilyon ABD doları ila 9 trilyon ABD doları arasında olacağı beklenmektedir².

■ Bu gelişme, bağlı cihazların sayısında bir patlamaya ve bunun sonucunda ise veri patlamasına sebep olacaktır. Veriler yaygınlaştıkça, Genel Veri Koruma Yönetmeliği mahremiyeti korumak için yeni zorluklarla karşılaşacaktır.



NESNELERİN İNTERNETİ

- “Nesnelerin İnterneti” kavramı ilk 1999 yılında ortaya çıkmış, ancak bizler birkaç yıl sonra, internete bağlı nesnelerin gerçek varlığını görebildik.
- “Nesnelerin İnterneti”³, veri toplamak ve değiştirmek için elektronik cihazlarla, yazılımlarla, sensörlerle ve bağlantılarla birbirleriyle ilişkilendirilmiş fiziksel nesneler veya eşyalar ağıdır.
- “Nesnelerin İnterneti”, eve gitmeden önce ısıtmayı sağlayan akıllı termostatlardan, bittiğinde portakal suyu sipariş eden buzdolaplarına kadar her şeyi tanımlamak için kullanılmaktadır. İnsanlar sağlık ve zindelik durumlarını takip eden cihazlar takmakta, hayvanlara ise sağlık ve yerlerini takip eden cihazlar takılmaktadır⁴.
- “Nesnelerin İnterneti” basitçe ifade etmek gerekirse, işleri kontrol etmeyi ve otomatikleştirmeyi ve veri toplamayı kolaylaştırarak aygıtların birbirleriyle konuşabileceği internet bağlantısı anlamına gelmektedir.
- Pew Araştırma Merkezi, “Nesnelerin İnterneti” ve “takılabilir” ürünlerin 2025 yılına kadar yaygınlaşacağına ve faydalı etkileri olacağına inanmaktadır⁵.



TAKILABİLEN TEKNOLOJİ

- “Takılabilir teknoloji” veya “takılabilir ürünler”, bilgisayar ve gelişmiş elektronik teknolojileri içeren kıyafetler ve aksesuarlardır.
- Takılabilir ürünler, aynı zamanda moda uygun teknoloji, takılabilir cihazlar, teknoloji elbiseleri veya moda elektroniği olarak da anılmaktadır⁶.
- Takılabilir ürünler kullanıcıya anında veri sağlar ve kullanıcı teknolojiyi anında izleyebilir, daha sonra kullanmak üzere indirebilir veya çıktı gönderebilir.



OYUNCAKLARIN İNTERNETİ

- Nesnelerin İnterneti, çocuk oyuncaklarına da uygulanabilir. Kablosuz bağlantı, bir oyuncağın diğer veri özellikli cihazlarla veya diğer oyuncaklarla etkileşime geçmesine izin verecektir.
- Oyuncakların İnterneti, gençlere teknolojiyi tanıtmak için yeni yollar sunmakta ve genellikle oyuncakla etkileşime girmelerini teşvik etmektedir.
- 2015 yılında kurulan ve Barbie'nin çocukları dinleyebildiği Mattel şirketinin bir “oyuncakların interneti” girişimi olan “Merhaba Barbie”, bu tür oyuncakların kendi başlarına yaratma, hayal etme ve öğrenmelerini etkileyerek çocuklarda gelişim sorunlarına neden olup olmadığını merak eden başlıca psikologlar, mahremiyet konusu uzmanları ile ebeveynler için endişelere neden olmuştur. 2011 yılında kurulan ToyTalk şirketi, farklı bir görüş sunarak konuşan oyuncakların ve Wi-Fi özellikli oyuncakların çocuklara öğrenme fırsatları sağlayabileceğini savunmaktadır⁷.

2. <https://securityintelligence.com/data-protection-in-the-internet-of-things/>

3. https://en.wikipedia.org/wiki/Internet_of_Things

4. <http://web.archive.org/web/20160310125239/http://www.theguardian.com/technology/2015/mar/30/internet-of-things-convenience-price-privacy-security>

5. http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf

6. https://en.wikipedia.org/wiki/Wearable_technology

7. http://web.archive.org/web/20150604014333/http://www.nytimes.com/2015/03/29/technology/a-wi-fi-barbie-doll-with-the-soul-of-siri.html?_r=0

- Nesnelerin interneti ve takılabilir ürünlerin getirdiği kolaylıklar ile oyuncakların internetinin getirdiği eğlence ve hoşça vakit geçirme imkânlarına rağmen kullanıcılar, nesnelerin interneti ile akıllı telefonlar ve bilgisayarlar gibi oyun cihazlarının güvenlik ve mahremiyet riskleri doğurabileceğinin yeterince farkında olmayabilirler. Oyuncaklar söz konusu olduğunda, çocuk gelişimine yönelik riskler bile muhtemelen ortaya çıkabilir.



KONULARI ANLAMAMANIN ÖNEMİ

■ Nesnelerin interneti, birçok kullanıcının "bilgi işlem aygıtı" olarak düşünmeyebileceği takılabilir ürünleri içerir; bu nedenle de birçok kullanıcı mahremiyet sorunlarını göz ardı etme riski taşır.

■ Nesnelerin internetinin ve takılabilir ürünlerin barındırdığı geleceğe dönük teknolojik vizyonlar, birçok kişiye cazip gelmektedir. Bununla birlikte, nesnelerin internetinin ilk piyasaya girişi, daha çok araştırmanın yapılması gerektiği anlamına gelmektedir. Geçmişte siber güvenlik firmalarının tecrübe ettikleri gibi, suç amacı güden insanlar, nihai hedeflerine ulaşacak yeni yollar yaratmak için daha sıkı ve daha hızlı çalışmaktadırlar.

■ Oyuncak şirketlerinin nesnelerin interneti alanına girmesi, gençler için harika yeni oyuncaklar anlamına gelmektedir, ancak anne-babaların, açık mikrofon cihazlarının gençlerin elinde olmasının ve kendi evlerinde açık veri bağlantıları olmasının risk taşıdığını anlamaları gerekmektedir.



ETİK DÜŞÜNCELER VE RİSKLER

■ Nesnelerin internetinin nihai hedefi verimliliği artırmaktır, ancak bu artan verimliliğin beraberinde getirdiği "karşılıklı bağlantılılık" (interconnectivity) hali önemli riskler doğurabilir.

- İnsanların cihazlarınıza ve verilerinize uzaktan erişebileceği fikri korkutucu bir olasılıktır.
- Takılabilir ürünlerin ve cihazların çoğu, en uygun güvenlik veya mahremiyet göz önünde bulundurularak tasarlanmamıştır.
- Son saldırılar, bilgisayar korsanlarının bebek monitörleri ve web kameraları vasıtasıyla insanları evlerinde izlediğini göstermiştir⁸.
- Tüketiciler, evlerinde fiziksel saldırı altında olabildikleri gibi, siber saldırı "riski altında da" olabilirler.
- Tüketiciler, Genel Veri Koruma Yönetmeliği'nin kendi verilerini kontrol etme imkânı verdiğinin bilincinde olmalı ve uygulamada bu kontrolün nasıl yapıldığı konusunda birbirlerini bilgilendirmelidir.



NASIL

- Nesnelerin interneti cihazlarının tasarım ve işlevleri farklıdır. Cihazın düzgün bir şekilde kullanılmasıyla ilgili en önemli husus, talimatları okumak ve cihazın işlevlerini anlamaktır.
- İstedığınız yerde mahremiyeti sağlayacak uygun ayarları devre dışı bırakmak veya etkinleştirmek için ayar işlevlerine bakmanız gerekir.
- Bazı takılabilir ürünlerin, piyasadan çekilmiş olması veya piyasaya sürüldüğü gibi çalışmıyor olması ihtimali sebebiyle satın almadan önce bu ürünler hakkında araştırma yapın.
- Unutmayınız ki bu alan, gelişmekte olan bir alandır ve birkaç hafta veya ay beklerseniz, piyasada daha yeni, daha iyi ve genellikle daha az pahalı bir şey bulma olasılığınız vardır.

SINIF ÇALIŞMASI İÇİN FİKİRLER



- Öğrencilerin, bir evde birbiriyle bağlanabilecek olası tüm cihazların bir listesini oluşturmalarını sağlayın. Ardından, potansiyel güvenlik veya mahremiyet risklerini listelemelerini isteyin. Kullanıcılar, riskleri azaltmak için ne yapabilirler? Cihaz sağlayıcısı ne yapabilir? İnternet hizmet sağlayıcısı ne yapabilir?

8. <http://web.archive.org/web/20160406200102/http://www.bbc.com/news/technology-30121159>

- Nesnelerin interneti ile ilgili bir tartışma sonrasında, öğrencilerden tüketicilerin güvenlik risklerini anlamalarına yardımcı olmak amacıyla tüketiciler için taslak bir talimatname hazırlamalarını isteyin.
- Genel Veri Koruma Yönetmeliğinin bir özetini okuyun ve öğrencilerden nesnelerin interneti⁹ ile ilgili tüm maddelerini listelemelerini isteyin.
- Tüketici hakları farkındalığı kampanyasına¹⁰ ilişkin video klipini indirin ve öğrencileri tüketici hakları ve nesnelerin interneti hakkında tartışmaya davet edin.
- Gençlerden oyuncakların interneti için yeni oyuncaklar “geliştirmelerini” isteyin. Oyuncakların faydaları nelerdir? Riskleri nelerdir? Genç kullanıcıları nasıl koruyabilirler? Ebeveynlere, oyuncakların güvenli olduğuna dair nasıl güven verebilirler?



İYİ UYGULAMA

Bu yeni teknolojiyi benimsemek için fikren açık olmak önemlidir, ancak verilerinizi ve mahremiyetinizi korumak için uygun güvenlik önlemleri aldığınızdan emin olun.

- Veri özellikli cihazlar üzerindeki kişisel bilgileri sınırlayın.
- Evinizin kablosuz ağındaki güvenliği güçlendirin.
- Güçlü parolalar seçin.
- Mümkün olduğunda, bazı cihazları birbirinden ayrı tutun.
- Oyuncakların İnternet'inin diğer cihazlarınızla etkileşimlerini sınırlayın ve onların kapasitelerini takip ettiğinizden emin olun.

Tüketiciler herhangi bir nesnelerin interneti cihazını seçerken birçok konuda dikkatli olmalıdır:

- Uyumluluk ve birlikte işleyebilirlik: Cihazınız diğer üreticilerin cihazlarıyla uyumlu mu ya da cihazınızı kullanabilmek için aynı "ekosistem" de mi kalmanız gerekiyor? Bu son derece önemlidir, aksi takdirde o üreticiye "kapalı kalarak" diğer üreticilerin diğer cihazlarına geçme veya entegre olmak imkânsız hale gelecektir.
- Bağlantılılık: Nesnelerin interneti cihazı, düzgün çalışabilmek için sadece İnternet bağlantısına mı dayanmaktadır? İdeali, İnternet'e bağlanmak zorunda kalmadan cihaza erişebilmelisiniz. Bu özellikle önemlidir, çünkü cihaz üreticiniz, cihazınıza erişmek için çevrimiçi platformu kapatırsa cihazınız fiilen kullanım-dışı hale gelecektir.



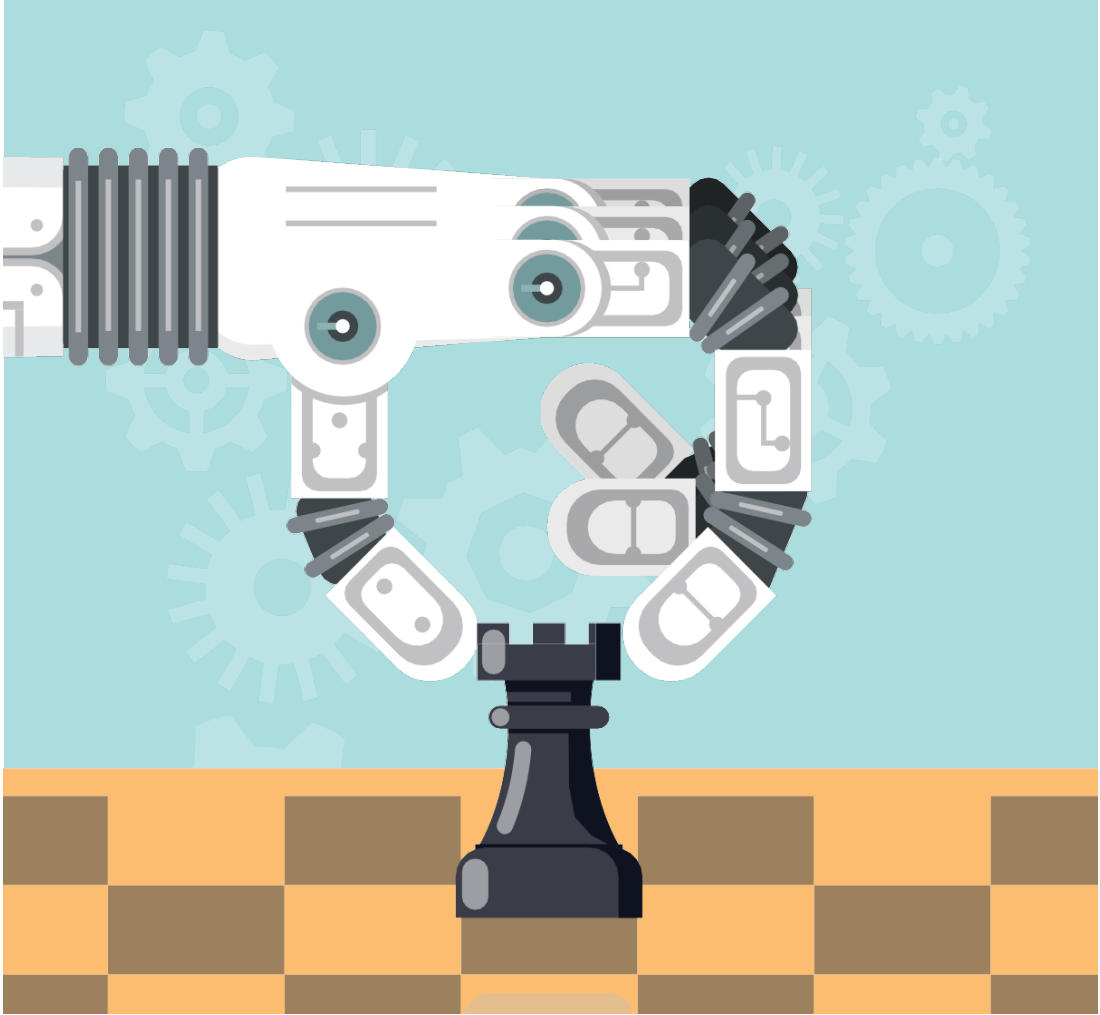
DAHA FAZLA BİLGİ

- AB "Tüketici Hakları ve Hukuku" hakkında daha fazla bilgi şu adresten bulunabilir: http://ec.europa.eu/consumers/consumer_rights/index_en.htm.
- Guardian nesnelerin internetine ilişkin haberi: <http://www.theguardian.com/technology/internet-of-things>.
- Intel'in bilgi grafiklerinde nesnelerin interneti hakkında daha fazla bilgi bulunabilir: www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.
- Disney, oyuncakların interneti üzerine araştırma yapmıştır: <http://www.disneyresearch.com/project/calipso-internet-of-things/>. Oyuncakların interneti rehberi şu adreste bulunabilir: <http://www.mutualmobile.com/posts/iot-internet-toys>.
- Çocukların Sayısal Medya Merkezi'nden de ayrıntılı bilgi bulunmaktadır: <http://cdmc.georgetown.edu/publications-and-papers/textbooks/>.
- İlgili Avrupa Konseyi belgeleri: "İnternet kullanıcıları için insan hakları - Çocuklar ve gençler": <http://www.coe.int/en/web/internet-users-rights/children-and-young-people>.

9. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

10. http://ec.europa.eu/justice/newsroom/consumer-marketing/events/140317_en.htm

Yapay Zeka, Otomasyon ve Yıkıcı Teknolojiler



■ "Otomasyon"¹, bir insan tarafından yapılan herhangi bir eylem veya işlevin bir makine tarafından yapılmasıdır. "Yapay zeka"² ise, makineler veya yazılımlar tarafından sergilenen zekâdır.

■ Tarihte teknolojik gelişmeler bazı işlerin kaybolmasına sebep olmuş, bazılarını ise yaratmıştır. Örneğin, telekomünikasyon teknolojisi geliştikçe tamamen ortadan kaybolan telefon operatörlerini ele alalım. Teknolojik devrimlerin neden olduğu işgücü piyasasındaki bozulmalar yeni bir olgu olmamakla birlikte her seferinde toplum kayıp olanları telafi edecek kadar yeni iş bulunamayacağı korkusuna kapılır.

1. <https://en.wikipedia.org/wiki/Automation>

2. https://en.wikipedia.org/wiki/Artificial_intelligence

■ Kaybolan işleri telafi etmede şimdiye kadar kimsenin hayal edemediği kadar yeterli sayıda işler yaratıldığından, bu tür korkular büyük ölçüde yersiz çıkmıştır. Örneğin, yirmi yıl önce hiç kimse "sosyal medya yöneticisi" veya "arama motoru iyileştiricisi (search engine optimiser)" gibi bir iş olacağını öngörmemişti.

■ Yapay zeka, otomasyon ve makine öğrenmesi alanlarındaki güncel teknolojik gelişmeler, yalnızca düşük vasıflı işleri değil, aynı zamanda işgücü piyasasının daha büyük bir bölümünü de tehdit etmektedir.



YENİ GELİŞMELER

Sürücüsüz arabalar

■ Sürücüsüz otomobillerin sunulmasına ve seri üretime hazır olmasına daha uzun bir yol olsa da, bu alandaki ilerleme inkar edilemez. Örneğin, Tesla, halihazırda otobanda sürücüsüz şekilde seyreden otomobiller üretmektedir. 2016 yılının Mayıs ayında bir Tesla otomobilindeki yazılım hatasından kaynaklanan ilk ölümcül kazanın incelenmesi, sürücüsüz otomobil teknolojisinin geleceğinin belirlenmesine katkıda bulunacaktır. En büyük engel, teknolojinin kendisi değil, kaza durumunda sorumluluk sorunu ile makinelerin kritik durumlarda karar vermesi durumlarına yasanın gereken şekilde uyarlanmasıdır. Ancak bu tür engellerin kalkmasıyla, taksi şoförleri, kamyon şoförleri ve toplu taşıma sürücüleri (metro, otobüs, tramvay) gibi meslekler kaybolacaktır. AB'de ulaştırma endüstrisi toplam istihdamın % 4,5'ini oluşturmaktadır.

Otomatik oluşturulan web siteleri, uygulamalar ve oyunlar

■ Web tasarımı yeni bir meslektir ancak telefon operatörlerinden çok daha hızlı ortadan kalkabilir. Günümüzde, web sitesi oluşturucuları tarafından bir web sitesinin oluşturulması, kullanıcının bir içeriği basitçe değiştirmesi için ekranda sürükleyip bırakmasıyla daha kolay hale gelmiştir. Karmaşık algoritmalar artık web sitenizi tercihlerinize göre otomatik olarak oluşturabilmektedir. "The Grid"³, tercihlerinize dayalı otomatik web sitesi üretimi sunan ilk hizmettir. Tüm ekranlar için uyumlu (bilgisayarlardan akıllı telefonlara kadar tüm ekranlar için uyumlu) bir web sitesi oluşturmak için web sitenizin amacı ile tercihlerinize uygun resim, içerik ve bazı bilgiler yeterli olacaktır. Bu sadece başlangıçtır. Yapay zeka, makine öğrenmesi ve algoritmalar geliştikçe programlama becerilerini gerektiren pek çok iş otomatik hale gelecek, yalnızca çok yaratıcılık, kişiye uygunluk veya yenilikçilik gerektiren işler kalacaktır.

Rastgele üretilen sanat

■ Makine öğrenmesinin gelişmesiyle bilgisayarlar artık görüntülerden resimlere ve müziğe kadar sanatsal üretimler yapabilmektedir. Google'ın "Derin Rüya"⁴ uygulaması, görüntünüzü analiz etmekte ve sanki bulutlara baktığınızda bir köpek ya da çiçek görüyormuşsunuz gibi size hayali nesneleri göstermektedir. Diğer programlar, Van Gogh veya Picasso gibi bir ressamın tarzını taklit edebilmekte ve çektiğiniz herhangi bir resme uygulayabilmektedir⁵. Müzikte, Emily Howell⁶, müziklere ait beğenileri analiz ederek, müzikteki "kuralları" veya "kalıpları" çıkaran ve benzer bir tarzda müzik besteleyen bir programdır. Bu sanatçıların sonunun geldiği anlamına gelmese de, bunun kesinlikle sanat üzerinde bir etkisinin olacağı aşikardır.

Robotlar ve selfservis

■ Amazon gibi büyük çevrimiçi perakendeciler, ürünlerin sınıflandırılması ve organize edilmesi veya dağıtım amacıyla ürünün teslim edilmesi gibi görevleri yerine getirmek için robotlara yoğun bir şekilde yatırım yapmaktadır. Tamamen robotlar tarafından yönetilen ilk otel, Japonya'da kapılarını açmıştır. Süpermarketlerde kendi kendine tarama istasyonları, lokantalarda self servis, robotlarla dolu endüstriyel montaj hatları, sağlık ve yaşlı bakımında robot yardımcılar, çevrimiçi alışveriş için otomatik nakliye süreçleri ve otel gibi hizmetler robotlar tarafından yönetilmeye başlandı. Otomasyon konusunda giderek daha fazla örnek sayısı dünyada artacaktır. Üç boyutlu yazdırmanın başlamasıyla inşaat işleri bile otomasyona geçebilecektir!

3. <https://thegrid.io/>

4. <http://deepdreamgenerator.com/>

5. <http://web.archive.org/web/20160114142911/http://arxiv.org/pdf/1508.06576v2.pdf>

6. <http://artsites.ucsc.edu/faculty/cope/Emily-howell.htm>

Öngörebilen ve hatasız algoritmalar

■ Büyük veri, süper bilgisayarlar ve güçlü algoritmalar sayesinde, sağlık hizmeti gibi birçok sektör yeni bir evrilmeye uğrayacaktır. Sağlıkla ilgili büyük miktarda verilerin mevcut olması sebebiyle algoritmalar; belirtilere, gerçek zaman sensörlerine ve geçmiş tıbbi kayıt verilerine dayanılarak tanı konulmasında doktorlardan daha iyi hale gelmektedir.

YZ-Yapay Zeka ve makine öğrenmesi

■ İleri yazılım ve bilgisayarlarla, günümüzde makinelerin, insan hareketlerini gözlemleyerek ve belirli "kurallar" ya da "kalıplar" türeterek ve bunları taklit ederek veya basitçe yapma yoluyla öğrenerek ve belirli eylemlerin sonuçlarını inceleyip, "kurallar" koyarak öğrenmeleri mümkündür. Örneğin, bilgisayar programlarının düşmanları yenmeyi, engellerin üzerinden atlamayı vs. "öğrenerek" video oyunlarını başarıyla bitirmeleri mümkün olmuştur. Gelecekte makinelerin ne kadar "öğrenebileceğine" dair birşey söylenemez, ancak şimdiden tekrar edilen görevlerde başarılı oldukları ortadadır.



EĞİTİMİN GETİRİLERİ

- Kodlamayı öğrenmek, temel YZ-Yapay Zekâ ve otomasyon da dâhil olmak üzere, robotik ve yazılım hakkında daha derin bir anlayışa kapı açmaktadır. Bu, halen bilgisayarların ve makinelerin erişiminde olmayan becerileri tanımlamak ve netleştirmek ve bu teknolojileri daha da ileri götürmek amacıyla gerekli olan becerileri geliştirmek için son derece önemlidir. Düşük beceri ve tekrar edilen işler, makineler tarafından devralınınca, geriye daha eğitilmiş olmaktan başka bir şey kalmamıştır.
- Aynı zamanda, otomasyon ve YZ-Yapay Zekâ hakkında bilgi edinilmesi, toplumun bir bütün olarak bunların etkisinden faydalanmasını temin edecek politikaların oluşturulmasına yardımcı olacaktır. Örneğin, otomasyon ve YZ-Yapay Zekâ hakkında yazan birçok yazar, temel bir evrensel geliri ve daha düşük çalışma saatlerini savunmaktadır. Bir grup biliminsanı, araştırmacı ve Stephen Hawking gibi önde gelen isimler, bir gün makineler tarafından köleleştirilmekten kaçınmak için YZ-Yapay Zeka'nın gelişimine yönelik net bir yönlendirme çağrısında bulunan açık bir mektup imzaladılar⁷.



ETİK DÜŞÜNCELER VE RİSKLER

İşsizlik

■ YZ-Yapay Zeka ve otomasyonun en belirgin riski, yerini aldığı iş sayısından daha az iş kolu yaratılmasıdır. Bu teknolojiler ilerledikçe yaratılabilecek işleri öngörmek mümkün olmasa bile, bu yeni iş kolları çok vasıflı iş gücü gerektirecek ve bu sebeple orta öğretime sahip kişilerin istihdamına az sayıda fırsat yaratacaktır.

Eşitsizliklerin Artması

■ Düşük vasıflı iş kolları daha da azaldıkça, pazarlanabilir becerilere sahip olanlar ile becerileri aşamalı olarak makineler tarafından yeri alınanlar arasında giderek artan bir eşitsizlik olacaktır. Otomasyona ve YZ-Yapay Zeka yeniliklerine geçmek için teknolojik bilgi birikimine sahip olan bazı ülkeler ile işgücünde el emeğine dayanan diğer ülkeler arasında başka bir eşitsizlik biçimi de ülkeleri vuracaktır. Uygun sosyal, istihdam, eğitim ve öğretim politikaları olmaksızın, bu tür eşitsizlikler toplumsal huzursuzluğa neden olabilir.

Makinelere aşırı bağımlılık

■ Otomasyon ve YZ-Yapay Zeka, sihirli değnek değildir. Bunlar, günümüzde halen insan denetimine ihtiyaç duymakta ve insanlara daha karmaşık bir görevi yerine getirmekte yardımcı olmaktadır. Örneğin, uçuş irtifasında seyir halindeyken otopilotta bir uçağı uçurmak yazılım için herhangi bir sorun teşkil etmezken, iniş ve kalkışın hala insan eliyle yapılması zorunludur. Bununla birlikte, pilotlar gittikçe daha az eğitim ve uygulama aldıklarından, otopilot tarafından idare edilemeyen "kritik" bir durumu yönetmeleri daha az mümkün olabilir. Aynı şey sürücüsüz otomobiller için de söylenebilir. Taşımanın otomatik olduğu bir gelecekte, yazılım başarısız olursa ve hiç bir insan araç kullanmadığında ne olacak? Daha da önemlisi, eğer makineler bizim için her şeyi yapacaklarsa ve hatta kendilerini yaratma ve onarma yeteneğine de sahip olacaklarsa, biz insanların, yapmamız gereken şey nedir? Bu durum, daha fazla eşitsizlik ve sosyal gerilimi besleyecek şekilde bilgi ve beceriler arttırılırken, eğlence arayan insanların bir kısmında ise toplu bir gerilemeyi başlatabilecektir.

Becerilerin yavaş ve uygun olmayan uyumu ve gelişimi

■ Otomasyon ve YZ-Yapay Zekanın gelecekte neler başaracağını hiç kimse tahmin edememektedir ve bu nedenle "gelecekle uyumlu" oldukları için hangi becerilerin artırılması gerektiğini hayal etmek çok zor bir iştir. Örneğin, eğitim dünyasında yavaş yavaş okullarda programlama ve kodlama öğretimi düşüncesi uyanmaktadır, ancak YZ-Yapay Zekadaki son gelişmeler, mantığa ve açık kurallara dayanması nedeniyle makinenin kendi kendine program yapabilmenin otomatik hale gelmesinin mümkün olduğunu göstermektedir. Web tasarımının otomatik olarak yapılması bu duruma basit bir örnektir.

Güvenlik

■ İnternete bağlı veya yazılıma dayalı herhangi bir cihazda olduğu gibi, YZ-Yapay Zeka ve otomasyon da hekimlere karşı savunmasızdır. Fakat bunların sonuçları, kişisel verilerinizi çalmaktan veya tahrip etmekten daha ciddi olabilir. Güvenlik uzmanlarından oluşan bir ekip, internet bağlantılı bir otomobilin heklenmesi ve ele geçirilmesi ve motorunun kapatılması veya hatta yavaş hızlarda direksiyon hakimiyetinin devranılması gibi eylemlerin gerçekleştirilebileceğini göstermiştir. Direksiyonu olmayan sürücüz bir otomobilin heklenmesinin sonuçlarını hayal edin.

Sıkıcı bir işin sonu; sıkıcı bir dünyanın başlangıcı

■ Belki de YZ-Yapay Zeka ve otomasyonun getirdiği en büyük güçlükler özünde felsefidir. Dünyamızı ilginç kılan nedir? İnsanlar, tamamen anlaşılmış, öngörülebilir ve optimize olmuş, her şeyi "plana göre" çalışan bir dünyada mutlu olabilir mi? İnsanın kendiliğindenliği, bilerek yanlış bir karar verme ve ondan ders çıkarma durumu ile mantıksız karar verme seçimi hakkında ne düşünüyorsunuz? "Otomatik" kararlar getirmek bilim, gerçekler ve akılla yönlendirilen toplumlarımızın mantıksal sürekliliğidir, ancak bu durum insanlar için sağlıklı mıdır? Bir yüzyıl önce birçok bilim adamı ve aydın, bilim yoluyla aydınlanma nedeniyle dinin sona ereceği öngörüsünde bulunmuş olsalar da şimdi maneviyata ve dine olan ilginin geri geldiğini görüyoruz. Belki de bu durum, insanların yaşamlarına bir anlam yüklemelerine imkan tanımayan bir dünya ile bizi insan yapan hisler, duygular, dürtüsellik ve mantıksızlık gibi şeylerle savaş halinde olan bir dünyanın belirtisidir.



SINIF ÇALIŞMASI İÇİN FİKİRLER

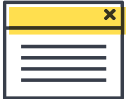
Sınıfta Yapay Zekayı tanıtmak için iyi bir başlangıç etkinliği, "akıllı bir kağıt parçası" denilen etkinliktir. Bu, herhangi bir çocuğu ya da genç insanı dokuz kare (noughts-and-crosses/tik-tac-toe) oyununda yenebilecek üzerinde yazılı talimatlar bulunan bir kağıt parçası sunmaktan ibarettir. Ayrıntılı talimatlar için bkz: <http://web.archive.org/web/20160326100226/http://csunplugged.org/artificial-intelligence/>.

- Bu temel etkinliğin devamında, çocuklarınıza veya öğrencilerinize günlük yaşantılarında kullandıkları herhangi bir Yapay Zekanın farkında olup olmadıklarını sorunuz.
- Öğrencilerinizin her biri büyük olasılıkla bir akıllı telefona sahiptir ve akıllı telefonların çoğunda da özel uygulamalar (IOS/Apple için Siri, Android / Google için Google Now ve Windows/Microsoft için Cortana) bulunmaktadır. Bu üç uygulamanın hepsi de Yapay Zeka özelliklerini sunar: milyonlarca insan sesini dinlerken daha iyi hale gelen bir ses tanıma özelliğine, sorduğunuz soruları cevaplamak için bir algoritmaya sahiptirler ve sizin kendilerine sağladığınız verilere göre (arama verileri, iletişim bilgileri, konum verileri, vb.) size sundukları bilgileri kişiselleştirme özelliği bulunmaktadır. Bu aynen, kelimeyi otomatik düzeltme gibi temel özelliklerde de geçerlidir. Bu da aynı zamanda YZ-Yapay Zeka teknolojisidir.



İYİ UYGULAMA

- Yapay zeka, otomasyon ve öğrenen makineler çok yararlı olabilir, ancak başarısız olmaları durumunda bazı el becerilerinizi korumayı asla unutmayın. Örneğin, GPS uygulamaları şimdi akıllı telefonlarda yaygın olsa bile, harita okumayı öğrenebilmeniz ve yön bulma duyularınızı geliştirmeniz gereksiz bir faaliyet değildir.
- Her şeyi kontrol altında tutun. Pek çok otomasyon seviyesi vardır, en aşırı olanı insanlar tarafından herhangi bir girdi ya da doğrulama yapılmadan kararlar alabilen bir makinedir. Tıpkı kullanıcının yazılım tarafından yapılan öneriyi kabul veya reddetme seçeneğine sahip olduğu akıllı klavyelerde olduğu gibi, doğrulama alabilmeniz için herhangi bir otomatik veya YZ-Yapay Zeka destekli cihazı veya yazılımı yapılandırmanız gerekir.
- Değişime hazır olun ve farklı birçok beceriyi geliştirmede çok yönlü olun. Bu yıkıcı teknolojiler pazara girdikçe, uyum sağlayabilecek olanlar çok yönlülüğü en fazla olan ve en esnek olan çalışanlardır. Gelecekte, işçilerin yeni beceri setleri geliştirmek için sıklıkla "yeniden eğitilmeleri" veya eğitimlerine geri dönmeleri gerekecektir. Hayat boyu öğrenmek kural olacaktır.
- Kişilerarası, sosyal ve duygusal becerilerinizi artırın; çünkü bunlar, otomasyonun herhangi bir biçimine karşı güvencededir. Robotlar ve algoritmalar birçok düşük vasıflı işin yerini alabilecekken, kalitenin ve insan etkileşiminin yerine hiçbir zaman geçemeyeceklerdir.
- YZ-Yapay Zeka ve otomasyon yazılımlara dayanmaktadır. Güncellemeleri düzenli olarak kontrol ederek sahip olduğunuz "akıllı" bir cihazın en yeni yazılım sürümünü çalıştırdığınızdan emin olun ve yüksek güvenlik ayarlarına göre uyarlayın. Eğer cihazınız çalışması için internete sürekli bağlanmayı gerektirmiyorsa, saldırı olasılığını azaltmak için bağlantısının kesildiğinden emin olun.
- Noktaları birbirine bağlamak ve geleceğin neler getirebileceği hakkında genel bir bakışa sahip olmak için, büyük veri, arttırılmış ve sanal gerçeklik ve nesnelerin interneti hakkındaki Kılavuzları okuduğunuzdan emin olun. Büyük verinin yapay zekayı ve otomasyonu beslediğini, arttırılmış ve sanal gerçekliğin YZ-Yapay Zeka ve makinelerle etkileşimde bulunmanın yeni yolları olduğunu, nesnelerin internetinin sadece YZ-Yapay Zeka ve makinelerle etkileşime geçmenin başka bir yolu olmadığını, aynı zamanda onlara daha fazla gelişmesini sağlayacak değerli verileri sunan bir besleme aracı olacağını anlayın. Vatandaşlar, ancak büyük resmi anladıklarında, bu değişiklikleri daha iyi bir toplum için kullanmak hakkında bilinçli ve bilgili kararlar verebilirler.



DAHA FAZLA BİLGİ

- Bu BBC'den yapay zeka ile ilgili bir makaledir: <http://web.archive.org/web/20160509115227/http://www.bbc.com/news/technology-34224406>.
- Google, yapay zeka ve öğrenen makine hakkındaki araştırma sayfasına bkz.: <http://research.google.com/pubs/ArtificialIntelligenceandMachineLearning.html>.
- Otomasyon hakkında haberler burada mevcuttur: <http://www.automationworld.com/>.
- Bu, teknoloji alanlarındaki en son yenilikleri sergileyen Tüketici Elektronik Fuarı'nın resmi web sayfasıdır: <https://www.cesweb.org/>.
- BİT alanındaki en son araştırma ve yeniliklerle ilgili haberler, AB Komisyonu Araştırma ve Yenilik Dergisi'nden edinilebilir <http://horizon-magazine.eu/topics/ict>.

Sanal ve arttırılmış gerçeklik



Sanal gerçeklik¹, gerçek dünyadaki fiziksel varlığı taklit eden bir ortamı canlandıran yoğun bir multimedya deneyimidir. Yaratılan duysal deneyim, görme ve işitme başta olmak üzere dokunma, koku ve tat duyularını içerebilir;

■ Arttırılmış gerçeklik², gerçek dünyadaki ortamlara ses veya görüntüler gibi bilgisayar tarafından üretilen duysal girdilerin eklenmesidir.

■ Sanal ve arttırılmış gerçeklik fikrinin doğuşu onlarca yıl geriye giderken, teknolojinin sanal ve arttırılmış gerçeklik cihazları, hizmetleri ve yazılımlarının ticarileştirilmesi noktasına kadar ilerlemesi ancak yakın geçmişe uzanmaktadır. Arttırılmış gerçeklik uygulamaları akıllı telefonlar, mobil internet ve coğrafi konumlandırma teknolojisi yoluyla hızla büyümüştür.

1. https://en.wikipedia.org/wiki/Virtual_reality

2. https://en.wikipedia.org/wiki/Augmented_reality

Sanal ve arttırılmış gerçeklikteki son gelişmelere ilişkin bazı örnekler şunlardır:

- özellikle Android ve iOS mobil platformları, PlayStation 4, Xbox One ve geleneksel PC veya Mac bilgisayar oyunları yoluyla başlatılmaya ayarlanmış birçok oyunla Oculus Rift, Samsung Gear VR, HTC Vive veya Sony Playstation VR gibi sanal gerçeklik kulaklıkların artan mevcudiyeti;
- arttırılmış gerçeklik kulaklıklarının veya Google Glass ve Microsoft HoloLens gibi gözlüklerin artan mevcudiyeti; Microsoft, oturma odasında oynanabilen, Minecraft'ın bir arttırılmış gerçeklik sürümünü çıkarmayı planlamaktadır;
- Akıllı telefonunuzla (iOS ve Android) gerçek dünyada Pokemons'u yakalamanızı sağlayan Pokemon Go gibi ana akım arttırılmış gerçeklik oyunlarının piyasaya sürülmesi.



EĞİTİMİN FAYDALARI

- Sanal gerçeklik, gerçek dünya deneyimini canlandırma imkânı ile öğrenmek için çok sayıda fırsat sunmaktadır. Örneğin, arabanın nasıl kullanılacağı birebir canlandırılabilir.
- Sanal gerçeklik yoğunluğunun derecesi göz önüne alındığında, deneyimler, örümcek korkusundan kurtulmak veya post-travmatik stres bozukluklarının (PTSD) üstesinden gelmek gibi tedavi edici amaçlar için sanal gerçekliği kullanma konusunda ümit vaat etmiştir. Aynı zamanda bir kullanıcının bir başkasının yerinde olmanın nasıl bir duygu olduğunu hissetmesini sağlayarak diğer kişiler hakkında empati ve anlayış düzeyini arttırmak için başarıyla kullanılmıştır: engelliliği olan bir kişi olmak (görme engelli bir kişi, tekerlekli sandalyede bir kişi) ya da ayrımcılığa uğrayan bir azınlık olmak.
- Her ne kadar herkes seyahat etme fırsatına sahipse de hiç birşey gerçeğin yerini tutamaz. Sanal gerçeklik, bir anıtı veya başka bir yeri ziyaret etmenizi "sanki" kendiniz fiziksel olarak oradaymışınız gibi canlandırabilir. Ancak daha da ileri gidebilir ve size ay veya uzay veya bir yanardağın içi gibi normalde asla gitmeyeceğiniz yerleri ziyaret ettirebilir veya hatta sizi bir 18.yüzyıl savaş alanına geri götürebilir ya da dinozorların yanında yürüyüş yaparken canlandırabilir.
- Arttırılmış gerçekliğin sıralayacak çok fazla faydalı uygulaması bulunmaktadır. Gerçek dünya üzerine "fazladan" bilgi veya nesnelerin yüklenmesinden oluştuğu için, olanaklar sınırsızdır. Bir anıt, heykel ya da gerçek başka bir şeye baktığınızda arttırılmış gerçeklikle bir tur rehberine gerek duyulmaksızın bu nesnelerin üzerine faydalı bilgiler bindirilebilir. Üst üste bindirilen bilgilerin gerçek sınırları yoktur. Bu, bir restoran için bir menü veya bir eleştiri yazısı, insanların isimlerini veya gördüğünüz zaman onlar hakkında bilgi veren hatırlatma notları vb. olabilir. Öğrenme açısından da, sınırsız olasılıklar taşımaktadır. Örneğin; sırasıyla atmanız gereken adımları vererek bir araba parçasının nasıl takılacağını/değiştirileceğinin gösterilmesi, ameliyat sırasında bir cerraha yardım edilmesi, malzemelerin nasıl kesileceği ve bunların nasıl karıştırılacağı canlandırılarak bir tarif hazırlanmasını size göstermek olabilir. Baktığınız her şey ek bilgilerle "arttırılabilir". Örneğin, bir sınıf, sanal nesnelerin eklenebileceği, insan vücudunun yarı saydam bir modelini gösteren bir sahne haline dönüştürülebilir.



ETİK DÜŞÜNCELER VE RİSKLER

Davranışsal risk

Bir dizi çalışma, video oyunları oynamak ile şiddet ve saldırganlıktaki artış gibi gerçek hayat davranışları arasındaki bağlantıyı incelemiştir. Bununla birlikte, sonuçlar hala tartışmalıdır. Bazı çalışmalar şiddetli bir video oyunu oynadıktan sonra "kısa vadeli" saldırganlık ve şiddet davranışlarına işaret etmektedir, diğer çalışmalar bu oyunların çocuklar üzerindeki "deşarj" etkisinin altını çizmektedir. Oyunun bir işbirliği unsuru ile birlikte çok oyunculu olup olmadığı gibi diğer ayrıntılar da sonuçları etkiler. Gerçek şu ki, video oyunlarının çocuklar ve genç yetişkinler üzerindeki uzun vadeli etkilerini hâlâ anlamaktan uzaktayız. Sanal gerçeklik ve arttırılmış gerçeklik, video oyunlarına daha ileri bir gerçekçilik katmanını ekleyerek onu "gerçekliğe" daha da yakın hale getirmekte ve bunun çocukları nasıl etkileyeceği konusunda hemen hemen hiç birşey/hiç denecek kadar az şey bilinmektedir.

Son zamanlarda, GTA V gibi video oyunları üzerine birçok tartışma oldu; bu oyunda bireyler tarafından geliştirilen bir üçüncü taraf eklentisi, oyuncuların sanal bir kadın karakter üzerinde tecavüzü canlandırmasına izin vermiştir. Video oyunlarında cinsiyet ayrımı, tacizden kaçınmak amacıyla kadın oyuncuların genelde "erkek" gibi davranması iyi bilinen bir olgudur. Ve bu sadece video oyunlarının biçimsel içeriği ile ilgili değildir. Video oyunları yoluyla canlı sohbet, aşırıcılık içeren içerik, cinsiyet ayrımı, zorbalık, nefret söylemi ve benzerlerini yaymak için kullanılmıştır. Sanal ve arttırılmış gerçekliği kullanan video oyunları, çocukların gelecekte tüketebilecekleri medyanın bir parçası olacak ve onların tutum ve davranışlarını belirli bir ölçüye kadar şekillendirmeye kaçınılmaz olarak katkıda bulunacaktır. Sorumsuz oyun geliştiriciler oyunlarında aşırı şiddet, aşırıcılık, cinsiyet ayrımı, ırkçılık, homofobik içerikler bulunduruyorsa, bu durum kullanıcıları olumsuz yönde etkileyebilir.

Mahremiyet/gizlilik

■ Arttırılmış gerçeklik, sanal öğelerle doğru olarak "arttırılması" için fiziksel dünyanın daimi gerçek zamanlı analizine dayanır. Bu, neyin gösterilmesi gerektiğinin doğru bir şekilde hesaplanması için yerleşmenin ve neye baktığının süper bilgisayarlara (genellikle çevrimiçi) beslenmesi gerektiği anlamına gelir. Bu, ekranınızda neyin gösterileceğinin doğru bir şekilde hesaplanması için bulunduğunuz konum ve yaptığınız araştırmalar (genellikle çevrimiçi) süper bilgisayarlara bilgi sağlanması gerektiği anlamına gelmektedir. Uygun mahremiyet/gizlilik koruması olmadan, arttırılmış gerçeklik, gerçek zamanda insanlar üzerinde daha derin bir şekilde casusluk yapmanın bir yoluna dönüşebilir olabilir.

Güvenlik

■ İnternete daimi olarak bağlı cihazlarla, uzak mesafeden canlı saldırı daha kolay hale gelmiştir. Gözlük camları ve hatta kontakt lensler gibi arttırılmış ve sanal gerçeklik cihazlarını kullanmaya başlayacağımız için, potansiyel olarak çok tehlikeli yeni saldırı durumları ortaya çıkabilir. Örneğin, bir sürücü, yön sağlamak için arttırılmış gerçeklik ekranı kullanıyorsa, bu ekran, onu yoldan çıkarmak için saldırıya uğrayabilir.

Manipülasyon ve tüketicilik

■ Arttırılmış ve sanal gerçeklik kendileriyle birlikte yeni reklamcılık stratejileri de doğuracaktır. Neye izin verilip verilmediğine dair bir düzenleme olmadığından, reklamcılığın bir sınırı yoktur ve bu sebeple evinizdeki reklamlarda, "arttırma" gibi teknikler kullanılacağını kolayca varsayabiliriz. Örneğin, buzdolabınızı açtığınızda bir reklam cihazı buzdolabınızda bulunması "gereken" ürünleri size "arttırarak" gösterir. Süpermarkette, akıllı telefonunuzla bir ürünü tararken, gelecek bir bildirim başka bir ürün satın almanızı önerebilir.

Bağlılık ve bağımlılık

■ Nörobilimler son yıllarda ilerleme kaydetmiş ve beynimiz hakkında çok şey keşfedilmiştir. Beyin hızlı hareket, eylem ve benzeri gibi hızlı uyaranlardan çok zevk alır. Video oyunları ve hızlı tempolu aksiyon filmlerini bu kadar başarılı kılan şey budur. Maalesef, "gerçek" dünya, sınırlama, öz denetim, sabır, azim ve proaktiflik gibi becerilerin edinilmesini ve uygulanmasını gerektirir. Her şey teknoloji yoluyla "oyunlaştırılmaz" ya da veya "hoş" hale getirilemez. Keman öğrenmek sadece bir örnektir. Çocuklar sanal ve arttırılmış gerçeklikle büyürken, "sanal" gerçeklikleri kadar uyarıcı, "arttırılmamış" veya "zengin" olmayan bir dünya ile başa çıkamayacak olmaları tehlikesi bulunmaktadır. MMORPG'ler (geniş olarak çok oyunculu çevrimiçi rol yapma oyunları) buna iyi bir örnektir. Bunlar örgütlenme, planlama, liderlik ve işbirliği duygusu gibi çok sayıda beceri geliştirmeye yardım ederken, oyuncuların ilgisini çekecek kadar zorlu ancak onları vazgeçirecek kadar fazla zor olmayan "eğlenceli" bir öğrenme eğrisi ile gelmektedirler. Arttırılmış ve sanal gerçeklik, bu sorunun daha da kötüleşmesine neden olacak ve başa çıkmanın daha kolay ve daha az sinir bozucu olduğu bir dünyaya ve gerçek dünyadan çok daha uyarıcı bir dünyaya bağlılık ve bağımlılık yaratabilecektir.

Kişiler arası becerilerin kaybedilmesi ve asosyal davranışlar

■ Japonya gibi bazı ülkelerde halen sınırlı bir olgu olmakla birlikte, "Hikikomori" olarak adlandırılan ergen ve yetişkinlerin toplumsal yaşantıdan kopması giderek artan bir olay haline gelmiştir. Medya, televizyon ya da internet ile doğrudan ilgili olmasa da, bu araçlar, "gerçek" yaşam zorluklarından uzaklaşma sağladıkları için bu sosyal yaşantıdan kopuşu daha katlanılabilir kılmaktadırlar. Sanal ve artırılmış gerçeklik, bu olguyu daha da şiddetlendirebilir çünkü sanal gerçekler başa çıkılması daha kolay ve "karışık" insan etkileşimlerinden daha tatmin edici olabilir. Cinsellik ve cinsel ilişkilerin beraberinde getirebileceği olumsuz duygular, başarılı olma baskısı ve vücut görüntüsünden doğan utanç payı, kullanıcının herşey üzerinde tam kontrole sahip olduğu bu sanal dünyada tamamı yok olmaktadır.

Fiziksel sağlık

■ Arttırılmış gerçeklik ve sanal gerçeklik, aynı zamanda kullanıcıların saatler boyunca ekranların arkasında pasif bir şekilde oturmaları gibi fiziksel hareketsizlik sorunlarını çözme fırsatı da getirmektedir. Örneğin, konuma-dayalı oyunlar, arttırılmış bir gerçeklikle gerçek dünyada yerini alabilir ve projeler sanal gerçeklik ortamları için özel alanlar oluşturabilir. Aynı zamanda, sürükleyici deneyimler, tüm dikkatimizi çekmek için sanal veya arttırılmış içeriğin gücü nedeniyle ağır belirtilerini veya aşırı kullanımı görmezden gelmek gibi yeni sorunlar ortaya çıkarmaktadır. Bir oyun içindeki tekrarlanan hareketler, bazı Wii oyunlarında görüldüğü gibi tendonitlere yol açabilir. Ayrıca, kafaya takılı bir ekran aracılığıyla beyne yöneltilen görüntüler, iç kulaktaki hareket sensörlerinden gelen girdiyle çakıştığı için, taşıt tutması ve mide bulantısı, arttırılmış gerçekliğin sürükleyici deneyiminin güçlü bir yan etkisi olabilir. Son olarak, birçok beta test kullanıcısı, o sırada gerçek dünyada arttırılmış gerçeklik oyunları oynarken, akıllı telefon ekranlarına bakmalarından dolayı sanal gerçeklik ve hatta arttırılmış gerçekliğe dalarak yere düşme veya bir nesneye çarpmak suretiyle yaralandıklarını belirtmişlerdir.

Zorbalık, siber taciz ve iletişim bağlantılı riskler

■ Gerçek olan ile sanal olan arasındaki sınır belirginliğini yitirdiği için, sanal ve özellikle arttırılmış gerçeklik, örneğin bir insanın yüz görüntüsünün üstüne bir fare başının koyulmasını programlamak, veya bir kişiyi küçük düşüren bir durumun naklen yayınının paylaşmak suretiyle o kişiyi hemen o anda canlı yayında aşağılamak mümkün olabilir.

■ Arttırılmış gerçeklik ve buna nispeten daha az derecedeki sanal gerçeklik, "temas" ile ilgili riskler taşımaktadır. Yoğun arttırılmış gerçeklik oyunları, gerçek dünyada tanımadığı gerçek insanlara karşı oynanmaktadır. Problemler durumlar, gerçek hayatta gasp edilme veya saldırıya uğramayı içerebilir.

SINIF ÇALIŞMASI İÇİN FİKİRLER



- Arttırılmış ve sanal gerçeklik büyük ölçüde donanım ihtiyacı duyar. Örneğin okul veya öğrenim kurumunuzda tabletler bulunmuyorsa, bu durumda bu teknolojilerden tam olarak yararlanamayacağınız anlamına gelir. Bazı durumlarda, çocukların ve gençlerin kişisel cihazları (akıllı telefonları gibi) kullanılabilir. Ancak bazı okullar, okul saatleri boyunca akıllı telefon kullanımını yasakladığı için okul politikası ile ilgili sorunlar yaratabilir ve bazı öğrencilerin arttırılmış veya sanal gerçeklik etkinliğini gerçekleştirecek kadar güçlü bir cep telefonları olması ve bazılarının da olmaması ayrımcılığa neden olabilir.
- Bununla beraber sınıfta arttırılmış ve sanal gerçekliği kullanmanıza yardımcı olmak için çevriminde sunulan birçok kaynak bulunmaktadır. Arttırılmış gerçeklik kullanımı daha kolaydır, çünkü tamamen yoğun bir deneyim sunan ve akıllı telefonlar ve tabletler gibi mevcut cihazlarla çalışacak "kafa başlığı" gerektirmemektedir.
- Arttırılmış gerçekliği kullanmakla ilgileniyorsanız, Kathy Schrock'un "Her şeye bir rehber"³ web sitesinde⁴ öğreticiler, kılavuzlar ve uygulamalar listesini bulabilirsiniz.

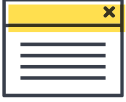
3. <http://web.archive.org/web/20160318145342/http://www.schrockguide.net/augmented-reality.html>; OnlineUniversities.com

4. <http://www.onlineuniversities.com/blog/2012/09/20-coolest-augmented-reality-experiments-education-so-far/>



İYİ UYGULAMALAR

- Her zaman olduğu gibi, bu yeni teknolojileri uzun süreli kullanmanın veya maruz kalmanın etkileri hakkında çok az şey biliniyor olduğundan sağlıklı bir yaşam dengesinin korunması şarttır. Sizin ve/veya çocuğunuzun "bağlı", sanal veya arttırılmış faaliyetlerinizi "geleneksel" spor veya diğer hobiler ile dengelediğinizden emin olun. Bu, sınıflar için de geçerlidir. Arttırılmış ve sanal gerçeklik, gelişen iş alanlarıdır ve onları eğitimde kullanmanın faydaları hakkında birçok iddia gerçek olsa da, kaliteli eğitim sağlamak için sihirli değnek yoktur. Geleneksel ve yeni öğretim yöntemleri arasındaki sağlıklı bir denge, ilerlemenin yoludur.
- Çocuklarınızın sanal veya arttırılmış gerçeklik cihazlarını kullanmaları durumunda onlar için satın aldığınız içeriği dikkatli bir şekilde seçin ve neye eriştiklerini kontrol edin. Yaş sınırlamalarını ve sınıflandırmaları, örneğin PEGI sınıflandırmalarını (sınıflandırma ve filtrelemeye ilişkin kılavuz metin 20'ye ve oyunlara ilişkin kılavuz metin 16'ya bkz.) okuyun ve daha küçük yaşta çocukların kullandıkları cihazlarda içeriğe özgürce erişemeyeceklerinden emin olmak için ebeveyn kontrol araçlarını etkinleştirin. Küçük çocuklar için, eğer ülkenizde/dilinizde mevcutsa kaliteli beyaz listeler kullanın; zira bu hem onları korumanın en iyi yoludur hem de uzmanlar tarafından incelenen olumlu içerikle karşılaşmalarını sağlar.
- Şiddet, siber zorbalık, cinsellik ve hak ve sorumluluklar konusunda çocuklarla ve gençlerle açık konuşmak her zamankinden daha önemlidir. Çocuklarınızın bir noktada çevrimiçi ya da sanal ve arttırılmış gerçeklik cihazlarıyla karşılaşabilecekleri cinsiyet ayrımı, ırkçı ya da diğer ayrımcı ya da olumsuz mesajları etkisizleştirmek için en erken yaştan itibaren güçlü ahlaki standartlar koymak en etkili yoldur.
- Küçük çocuklar için mahremiyet/gizlilik ve güvenlik ayarlarını en üst düzeye getirin. Bkz. Kılavuz 9. Bu cihazların saldırıya maruz kalma riskiyle karşı karşıya olduğunu unutmayın.
- Siz veya çocuğunuz müdahaleci reklamcılık faaliyetlerine maruz kalabileceğinden, sanal ve/veya arttırılmış gerçeklik için kullandığınız içerik veya cihazın arkasındaki iş modelini kontrol ettiğinizden emin olun.



DAHA FAZLA BİLGİ

- Sanal gerçeklikteki son gelişmelere ilişkin haberler Venture Beat'da mevcuttur: <http://venturebeat.com/tag/virtual-reality/>.
- Stanford Üniversitesi'nden sanal gerçeklik ve eğitim ile ilgili bir makale bulunuyor: <https://teachingcommons.stanford.edu/teaching-talk/virtual-reality-and-education>.
- Arttırılmış gerçeklikteki son gelişmelere ilişkin haberler Venture Beat'da mevcuttur: <http://venturebeat.com/tag/augmented-reality/>.
- Arttırılmış gerçeklikle ilgili genel bilgi Dartmouth College Kütüphanesi Araştırma Rehberi'nden edinilebilir: <http://researchguides.dartmouth.edu/AR>.

Ürün siz misiniz? Büyük veri, veri madenciliği ve mahremiyet



Büyük veri¹, geleneksel yöntemlerle (örneğin bir bilgisayar veya basit bir uygulama kullanarak) analiz edilemeyecek veya işlenemeyecek kadar geniş verilere işaret eden geniş bir terimdir.

■ Aşağıdakilerin birleşimi büyük verinin köklerini oluşturur:

- sayısal depolama kapasitesinin giderek muazzam bir şekilde büyümesi;
- toplumlarımız tarafından üretilen verilerdeki artış (artan bir şekilde yaptığımız her şey sayısal bir iz bırakır);
- tüm verilerin birbirine bağlanmasını sağlayan internet yoluyla birbirine bağlı bir dünya;
- üretilen tüm verilerin analiz edilmesi ve anlamlandırılması için artan bir yetenek.

1. https://en.wikipedia.org/wiki/Big_data

■ Büyük veriyi kullanan çevrimiçi hizmetlere örnek olarak Facebook gibi sosyal ağlar, Google veya Bing gibi arama motorları ve Amazon gibi çevrimiçi alışveriş siteleri bulunmaktadır. Ancak büyük veri "çevrimiçi" bir şeyden çok daha fazlasıdır; günlük, çevrimdışı hayatlarımıza da uzanmaktadır.

- Süpermarketler alışveriş modellerini analiz etmek, envanterlerini gerçek zamanlı olarak ayarlamak veya özel bir mağaza etkinliği (pazarlama, satış, vb.) programlamak için mağaza kartlarını kullanmaktadır.
- Sürücülerden, arabalarının sensörleri ve GPS cihazlarından elde edilen veriler gerçek zamanlı trafik bilgisi sağlamaya yardımcı olmaktadır.
- Hastanelerde, sensörlerden gelen kalp atımı sayısı gibi verilerin incelenmesine, gerçek zamanlı olarak herhangi bir dıştan işaret ve belirti tespit edilmeden önce enfeksiyonları veya diğer sağlık sorunlarının tespit edilmesine yardımcı olabilir.

■ Ayrıca veri, en popüler çevrimiçi para birimlerinden biri haline gelmiştir. Sosyal ağlar veya arama motorları gibi kullandığınız çevrimiçi hizmetler için nakit ile ödeme yerine, bu hizmetleri beslediğiniz verilerle "ödeme yaparsınız". Bu veriler, hizmetlerin reklamları ve pazarlamayı tercihlerinize göre uyarlamasına ve böylece daha etkili olmasına olanak tanımaktadır. Bununla birlikte, verilerle "ödeme yapmak", zayıf bir karşılaştırmadır. Parayla karşılaştırıldığında, veriler çok daha duyarlıdır. Birden fazla defa tekrar kullanılabilir ve yeniden satılabilir. Bir hizmete erişme karşılığında evinizin anahtarını vermek, daha doğru bir karşılaştırma olacaktır!

■ Veriler nesnelerin interneti yoluyla daha kapsamlı (nesnelerin interneti ile ilgili kılavuz 23'e bkz.) ve veri analizi tekniklerindeki ilerlemeler (yapay zekâ, vb.) ve bilgi işlem gücündeki artış yoluyla daha da verimli hale geldiğinden bu devrimin henüz çok başındayız.



EĞİTİMİN FAYDALARI

- Büyük veri, hayatınızın birçok bölümünü en iyi hale getirme ve kolaylaştırma potansiyeli taşımaktadır: arama sorgularınızın daha doğru sonuçlar verdiğinden, iş veya okula gidiş/geliş zamanlarınızı mümkün olduğunca etkin kullanmanızdan, bölgedeki mağazalarda istediğiniz yiyecekleri her zaman bulabileceğinizden emin olun.
- Büyük verinin gücünden faydalanmak ve size karşı değil, sizin yararınıza çalıştığından emin olmak için büyük veriyi ve nasıl çalıştığını öğrenmek gereklidir. Bu, hangi tür verileri paylaşmaya istekli olduğunuzu dikkatle seçmenizi ve verilerin kullanımlarına dayalı olarak hizmetleri ve ürünleri seçmeyi gerektirir.
- Büyük veri aynı zamanda, insanlık tarihinde ilk kez insanların yarattığı büyük veri yığınlarını analiz etmeyi ve anlamlandırmayı mümkün kılarak, toplumlarımızı anlamaya yardımcı olma amacına hizmet edebilir. Sosyal bilimler, psikoloji, davranış bilimleri, sağlık hizmetleri, pazarlama ve daha birçok araştırma alanı için büyük veri gerçek bir dönüm noktasıdır. Bu alanlardaki bulgular, öğretmenler tarafından bazı sosyolojik kavramları gerçek hayat örnekleri ve tablolarıyla birlikte göstermek için kullanılabilir.
- Ana gelir kaynakları olarak nakitten ziyade veriye dayalı çevrim içi iş modellerinin hakim konumu, kişisel iş yönetimi ve mahremiyet koruma becerileri gibi yeni becerilere yönelik bir ihtiyaç doğurmaktadır. Tıpkı kişisel bütçenizi ve hesaplarınızı yöneteceğiniz ve aşırı harcamayacağınız gibi kişisel verilerinizi de sorumlulukla yönetmeyi ve aşırı paylaşmamayı öğrenmek zorunda kalacaksınız.



ETİK DÜŞÜNCELER VE RİSKLER

Mahremiyet ve verinin korunması

Her ne kadar birçok yasa bireylerin verilerini ve gizliliklerini korusa da, gerçek hayatta uygulanmaları zordur. Genel Veri Koruma Düzenlemesi (GSYİH) kullanıcıların açık iznini talep edecek hizmetleri gerekli kılmakta ancak bu, "hizmet koşullarını" kabul etmeye benzer şekilde büyük olasılıkla sadece işaretlenecek "onay kutucuğu" uygulamasını getirmektedir: kabul et veya vazgeç! Kullanıcılar genellikle verilerini teker teker ve ayrıntılı olarak kontrol etmezler ve her şeyi ya da hiçbir şeyi paylaşmayan seçeneklerle karşı karşıya kalırlar. Genel Veri Koruma Düzenlemesi (GSYİH), orantılılık ilkesini getirerek (bir tüketicinin verisine erişim talep eden hizmet gerçekten bu hizmetin sunulması için tür verileri gerektirirse bile) tüketici onayı konusunu ele almaya çalışsa da, uygulamadaki yorum ve uygulama, kullanıcıları korumak için yeterli olmayabilir. Örneğin sosyal ağlar, haberlerinizi sıralamak için verilerinizi kullanmayı gerektiriyor mu?

Mahremiyet ve veri korumaya ilişkin kavramlarının önümüzdeki yıllarda daha da geliştirilmesi gerekecektir. Mahremiyet ne demektir? Sizin veri izinize tekrar erişilmediği müddetçe verileriniz kötüye kullanılabilir mi? Günlük olarak kullanıcılar tarafından üretilen verinin tümü göz önüne alındığında, verilerinizin ne ölçüde paylaşıldığını ve kullanıldığını daha detaylı olarak nasıl kontrol edebilirsiniz?

Standardizasyon, uyumluluk ve tepkisizlik

Büyük veri, hayatı kolaylaştırmak için bir nimettir. Toplu taşıma, sağlık ve hastaneler, kentsel planlama, bu sektörlerin tümü daha etkili olabilmek için kullanıcılar, hastalar ve vatandaşlar tarafından üretilen verilerin analiz edilmesinden fayda sağlayabilir. Peki ya siz farklıysanız? Eğer ya olağandışı saatlerde işe gidiyorsanız, eğer ender görülen bir hastalığınız varsa, eğer "genel" yaşam tarzına uymak istemiyorsanız? Etrafınızdaki tüm hizmetler büyük veri temelinde daha verimli bir şekilde tasarlanırsa, siz bir birey olarak alışılmadık özlem ve ihtiyaçlarınızla birlikte bunların dışında kalabilirsiniz.

Ancak büyük veri, ihtiyaçlarınıza özel olarak uyarlanabilmesi için de kullanılabilir: örneğin, arama motorları, arama sonuçlarını önceki aramalara ve hakkınızdaki diğer tüm verilere dayalı olarak kişiselleştirir; sosyal ağlar size beğenebileceğiniz mesajları gösterir. Bununla birlikte, sadece görmek istediğiniz veya görmekten hoşlandığınız şeylerin gösterilmesi, kişisel tepkisizlik şeklinde ters etki yapabilir. Örneğin, siyasi tercihleriniz ve görüşleriniz daha sağ veya daha sol kanattaysanız görüşlerinizi destekleyen bilgi ve içerikle düşüncelerinizi beslemek egonuzu tatmin edebilir, ancak demokrasi, tartışma ve kişisel gelişim gibi temel değerlerin gelişmesi açısından korkunç olabilir - yani bu durum "sizin içinize kapanmanıza sebep olacaktır".

Dışlanma

Bir hayat sigortası yaptırttığınızda, bir iş başvurusunda bulunduğunuzda, kredi talep ettiğinizde ya da araç sigortası yaptırttığınızda, sahip olduğunuz geri ödeme yeterliliğiniz veya risk durumunuz değerlendirilmektedir. Bu değerlendirme, sigara kullanıp kullanmadığınızı veya spor yapıp yapmadığınızı soran bir sağlık anketiyle, becerilerinizi test etmek için bir iş görüşmesi veya bütçenizi son zamanlarda nasıl yönettiğinizle veya aldığınız herhangi bir krediyi geri ödeyip ödemediğiniz ile ilgili bir araştırma yoluyla olabilir. Ancak, "adil" bir değerlendirme ile mahremiyetinizin açık ihlali arasındaki ayrım nerededir? Birçok işveren zaten işe alım kararlarını vermek için iş adayları hakkında çevrimiçi bilgileri kullanmaktadır ve sigorta şirketleri ile bankaların, bir kredinin geri ödenmemesi olasılığını ya da ciddi bir sağlık sorununun olup olmadığını değerlendirmek için çevrimiçi verilerin analizine yöneldiklerine dair pek çok ipucu bulunmaktadır. Büyük veri, öngörü güçleri sayesinde hayat kurtarabilir, ancak bazı insanların temel finansal veya sağlık hizmetlerine erişimini de engelleyebilir.

Dışlanmaya karşı itibar satışı

Çevrimiçi itibar yönetim şirketleri internette ortaya çıkmaya başlamıştır. İşletmeler ve bireyler, bu şirketlere itibarlarını yönetmeye ve verilerinin kredi/yatırım, sigorta veya istihdam gibi belirli hizmetlere erişimin dışında kalmamalarını sağlamak için ödeme yapabilir. Bu, bir nehri kirlilemek, zehirlenmiş vatandaşlara ilaç satmak ve nehri temizlemek için bir işletmeye ödeme yapmak gibi bir dışsallık döngüsünün ticari sömürüne bir örnektir.

Manipulasyon ve tüketicilik

■ Uygulamalar ve çevrimiçi hizmetler için en popüler iş modelinin genellikle kullanıcı verilerinin kullanımına dayanan "ücretsiz" reklamcılık olduğu göz önünde bulundurulursa, tüketicilerin, tüketimi teşvik eden daha fazla mesaja giderek maruz kalma riski vardır. Çevrimiçi reklamcılık her yıl büyümektedir ve tüketicileri reklamlara bakmaya veya tıklamaya zorlayan yeni teknikler hızla evrilmektedir. Örneğin, ön tarama videoları sadece birkaç yıl önce ortaya çıkmıştır.

Büyük veri, bir yandan reklamcılığı daha etkin hale getirerek ve bireylerin alışkanlıkları ve ilgi alanlarına göre özelleştirerek, bir yandan da kitle verilerinden bir reklamın görülmesi ve onunla etkileşime geçilmesi için kullanılan en etkin tasarımı, yeri ve yöntemi de öğrenerek reklamcılıktaki büyümeyi beslemektedir.

Siyasi zulüm

■ Bazı hükümetler mahremiyete saygı duymakta ve vatandaşlarına yönelik casusça gözetlemeler yürütmese de, çoğu böyle değildir. Edward Snowden'ın yaptığı açıklamalar, dünyanın her yerinde hükümetlerin internet kullanıcılarını gözetlediğini göstermiştir. Bazı durumlarda bu tutum, terörle mücadele ve terör saldırısının önlenmesi gibi güvenlik nedenlerinden ötürü haklı sebeple olabilir ancak bu tür eylemlerin orantılılığının her zaman sorgulanması gerekir. Örneğin, polis bir protesto yürüyüşüne katılan vatandaşları belirlemek için sosyal ağ profillerini araştırabilir.

Tüketici hakları

■ Büyük veri yeni çevrimiçi para birimidir, ancak kullanıcılar bu birim değişimi karşılığında ne almaktadırlar? Taciz ve rahatsız eden reklamlarla dolu bir çevrimiçi hizmeti kullanma hakkını mı? Kullanıcılar bir hizmeti kullanmak için aylık bir ücret ödediğinde, tüketici hakları yasalarıyla korunmaktadırlar ve hizmet veya içerik beklentilerinin karşılanmadığı veya ciddi kusurlar olması halinde, tazminat alma hakkına sahiptirler. Kullanıcı, filmi izleyemiyorsa çevrimiçi video platformundan para iadesi alabilir, ancak tercih ettiğiniz sosyal ağda hatalar varsa veya kullanım dışı ise ne olacaktır? Ne tür bir tazminat hakkına sahipsiniz? Sonuçta, sosyal ağ, verilerinizi sizin reklamlara bakmanız için kullanmış ve bundan para kazanmıştır. Para birimi olarak veriye dayanan bu yeni iş modeli, tüketici hakları bakımından birçok sorun oluşturmaktadır. Sözde "ücretsiz" olduğu için, kullanıcıların genelde herhangi bir tazminat hakkı yoktur, mevcut hakları ise çok kısıtlıdır.

İsim Gizlemenin Sonu

■ Rumuzlar ve takma adlar henüz daha ortadan kaybolmamışken, büyük verinin ortaya çıkışıyla isim gizleme ciddi tehdit altına girmiştir. Birkaç adet isimsiz veri parçası arasında bağlantı oluşturarak, bir kişiyi çevrimiçinde ismiyle tanımlamak mümkündür. Verdiğimiz bilgiler konusunda çok temkinli davransak bile, iyisiyle veya kötüsüyle yakın gelecekte herkesin çevrimiçinde isimsiz olarak kalması zor olacaktır.

İnternet asla unutmaz

■ Avrupa Birliği, gerçekleşmesi için yasal adımlar attığından bu yana "unutulma hakkı" ilgi görmektedir. Ancak, bunun uygulanması hâlâ zordur. Sayısal içerik, otomatik internet botları ya da araçları tarafından kolaylıkla yeniden gönderilebilir, tanınmayacak şekilde hafifçe değiştirilebilir veya AB yasaları kapsamı dışındaki çevrimiçi sunucularda veya servislerde barındırılabilir. Artık herkes kolayca akıllı telefonlarıyla istediği zaman fotoğraf veya videolarını çekebilmektedir. Bu da siz bir festivaldeyken çevrimiçine yüklendiğinizi görme ve tüm dünyanın sizinle dalga geçme riski olmadan artık kendinizi aptal yerine koyamaz ve sorumsuzca davranamazsınız anlamına gelmektedir. Hesap verebilirlik hakkı ile unutulma hakkı arasında hâlâ ince bir denge kurulması gerekiyor.

Kalitesiz içerik ve hizmetler

■ Çevrimiçi hizmetler ve içerik oluşturucuları, gelir için reklamlara giderek daha fazla dayandıklarından, hizmet veya içeriklerinin çekiciliğini en iyi duruma getirmeye çalışacaklardır. Büyük veri, bir makaleyi, fotoğraf veya videoyu neyin cazip hale getirdiğinin belirlenmesinde yardımcı olur; ancak bu, kaliteli içerik veya hizmetlerin leyinde mi yoksa aleyhinde mi olacaktır?

Çevrimiçinde giderek artan sayıda makale, bağlantıyı veya mesajı tıklamak ve reklamlarını dolduran sayfalara kullanıcıları çekmek için "yemleme tıklamasını" kullanmaktadır. "Zayıflamanın ilk üç sırrı", "bu kızın kamera karşısında ne yaptığına inanamayacaksınız" veya "internette en sevimli ilk 10 kedi" gibi başlıklar giderek daha sık çevrimiçinde yer almaktadır. Her ne kadar eğlence ve hikâyelerle ilgili içeriklerde bir sorun bulunmasa da, reklamcılığa dayalı bu tür iş modelleri, gerçeğe dayalı güvenilir içeriği veya eğitsel içeriği yok sayarak sadece bu türde içerik yaratılmasını büyük ölçüde teşvik etmektedir.



SINIF ÇALIŞMASI İÇİN FİKİRLER

14 yaş ve üstü gençler için: gençleri kendi adları için bir arama yapmaya ve/veya internette onlarla ilgili mevcut verileri incelemeye davet edin, sonra bunları bir işveren, bir sigortacı ve bir hükümetin kanun uygulama birimleri açısından analiz etmeye davet edin. Kendileriyle ilgili mevcut verileri analiz edip etmediklerini, bu kuruluşların kendilerini nasıl gördüklerine dair tartışma yapmalarını sağlayın? Örneğin, vakit öldürmenin faydaları hakkında makaleler paylaşan mesajlar veya birçok imla hatası içeren durum güncellemeleri bir işveren açısından çok kötü görünebilir. Sigara veya içki içtiğinizi veya tehlikeli faaliyetler yaptığınızı gösteren resimler sigortacınıza kötü görünecektir. Ve son olarak, hükümetinizi eleştiren ve radikal değişim çağrısı yapan mesajlar kolluk kuvvetlerinde şüphe uyandırabilir.



İYİ UYGULAMALAR

- İnternet ve büyük veri, nihayetinde teknik devrimin sadece daha ileri adımlarıdır. Nihai sonuçların insanlık ve toplum için iyi ya da kötü olup olmadığı, onları nasıl kullandığımıza bağlıdır. Bir vatandaş ve bir İnternet kullanıcısı olarak, büyük verinin nasıl kullanılacağını şekillendirebilir, toplum yararına çalışan girişimleri teşvik edebilir ve kamu yararına aykırı olanları önleyebilirsiniz. Örneğin, vatandaş olarak, verinin kullanımına ilişkin güçlü etik standartları destekleyen politikacılara oy verebilirsiniz; İnternet kullanıcısı olarak, verilerinizi etik ve sorumlu bir şekilde ele alan hizmetler ve şirketleri destekleyebilirsiniz.
- Büyük veri hakkındaki en son gelişmelere ilişkin bilgi sahibi olunuz, çünkü bunların günlük hayatınız üzerinde derin etkileri olacaktır. Bu, yalnızca paylaşmayı istediğiniz veya seçtiğiniz verilere karar vermenize yardımcı olmakla kalmaz, aynı zamanda, özel verilerinizin nasıl ele alınılacağına ilişkin etik standartlarınızla uyumlu politikacıları ve şirketleri tanımlamanıza ve desteklemenize yardımcı olur.
- Özellikle genç yaşta başladıysanız, çevrimiçi varlığınızın en başlangıcından itibaren kullandığınız tüm hizmetleri ve çevrimiçi yayınladığınız tüm içeriği izlemeye devam edin! Çocuk ya da gençken gönderdiğiniz yorumlar ya da mesajlar, yetişkin hayatınızda sizi rahatsız etmek için kolayca bulunabilir. Yayınladığınız içeriği incelemek için biraz zaman ayırın ve bugün artık kim olduğunuzu temsil etmeyen içeriği arşivleyin veya silin.
- Çevrimiçi hizmetlerin özel verilerinizi kullanma biçimini incelemek için zaman ayırın ve bunları uygun biçimde seçin. Verileriniz için doğru korumayı belirlemek için her zaman mevcut tüm mahremiyet ayarlarınızı kontrol edin.



DAHA FAZLA BİLGİ

- Toplumun yararına kullanılan büyük veriye ilişkin örnekler, AB Komisyonu web sitesinde bulunabilir: <https://ec.europa.eu/digital-agenda/en/what-big-data-can-do-you>.
- Unutulma hakkına ilişkin AB mevzuatı hakkında da bilgi bulunmaktadır: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.
- Data & Society, veri merkezli teknolojik gelişmeden doğan sosyal, etik ve kültürel konular üzerine odaklanan bir Amerikan düşünce kuruluşudur: <http://www.datasociety.net/>.
- Sivil haklar, büyük veri ve algoritmik geleceğimiz" hakkında bir rapor mevcuttur: <https://bigdata.fairness.io/>.
- Electronic Frontier Foundation, sayısal dünyadaki haklarınızı koruma konusunda bilgi sunmaktadır: <http://www EFF.org>.
- Avrupa Sayısal Hakları, sayısal ortamda hak ve özgürlüklerin savunulması hakkında bilgi de sunmaktadır: <http://www.edri.org>.

İnternet Okuryazarlığı El Kitabının ilk baskısı 2003 yılında yayınlandığından Bu yana İnternet dünyası çok büyük bir değişim geçirdi. İnternet kullanıcılarının sayısı arttı; kullanıcılar giderek daha gençleşiyor, insanların İnternet'i nasıl kullandığı ve ne aradıklarının eğilimleri gelişiyor ve birden bire görünen o ki örneğin kişisel güvenlikte yeni tuzaklar ortaya çıkmaktadır.

Bu yeni baskı, sayısız değişikliği gözönüne alıyor olmasına rağmen, El Kitabının amacı hâlâ, ailelere, eğitimcilere ve politika yapıcılara, genç insanlarla iletişim teknolojisi yoluyla gezinmelerine izin verecek yeterli teknik bilgi birikimini sunmaktır. Yeni baskı, daha önce "yeni" sayısal vatandaşlık ve sayısal ebeveynlik kavramlarını getiren Kılavuz Metinlerinin kapsamını genişletiyor. Bu baskı, özel olarak ayrılmış, İnternet'in geleceğine yönelik "İleriye Bakmak" başlığı da dahil olmak üzere 6 konu başlığı altında düzenlenmiş 26 Kılavuz Metnini içeriyor. El Kitabı, "Web'de kaliteli bilgi bulma" başlıklı Kılavuz Metninde gösterildiği gibi, kullanımı kolay ve faydalı olacak şekilde tasarlanmıştır. Ayrıca, tam formatta veya kılavuz metinleri tek tek indirilebilecek şekilde çevrimiçinde de mevcuttur.

www.coe.int

Avrupa Konseyi, kıtanın önde gelen insan hakları örgütüdür. İçinde 28'si Avrupa Birliği üyesi olan 47 üye devlet bulunmaktadır. Avrupa Konseyi'ne üye tüm ülkeler, insan hakları, demokrasi ve hukukun üstünlüğünü korumak için tasarlanan Avrupa İnsan Hakları Sözleşmesi'ni imzalamıştır. Avrupa İnsan Hakları Mahkemesi, Sözleşmenin üye devletlerde uygulanmasını denetlemektedir.