Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

- Giriş
- Temeller
- Ziyaret Eden Çocuklar

Siber Nesil Farkını Dikkate Alarak Çocuklarınızı Çevrim-içi Güvenli Hale Getirmek

Giriş

Bir çoğumuzu teknolojiyi nasıl güvenli bir şekilde kullanacağımız konusunda kendimizi rahat hissetmekteyiz. Ancak, diğer aile üyeleri kendilerini bu konuda rahat hissetmeyebilir, özellikle de bilgisayar ya da internet çağında büyümediyse. Güvenlik konusunda kuşak farkını nasıl kapatabileceğiniz ile ilgili alabileceğiniz önlemleri burada bulabilirsiniz. Ayrıca çocuklarınızı evdeyken nasıl koruyabileceğiniz konusunda önlem alıyor olabilirsiniz ancak çocuklarınız akrabanızın evini ziyaret ettiğinde aynı güvenlik önlemleri alınmamış olabilir. Çocuğunuz bu akrabalarınızı ziyaret etiğinde onlara nasıl güvenli bir çevrim-içi ortam yaratabileceğiniz konusuna da değineceğiz.

Konuk Yazar

Brian Honan (Twitter'da **@brianhonan**) Dublin, İrlanda'da bağımsız olarak güvenlik danışmanlığı yapmaktadır. Europol'un Bilişim Suçları Merkezi (E3) özel danışmanı olup İrlanda'nın ilk Computer emergency response team (CERT) yapısının kurucusu ve başkanıdır. Ayrıca Bilgi Güvenliği konusunda Dublin Üniversitesinde ders vermektedir. Birçok kitabın yazarıdır ve endüstriyel yayınlar yapmaktadır.

Temeller

Sadece bir kaç temel adım, bir kişinin dijital hayatını korumak için çok yararlı olacaktır. Aile üyelerine her zaman önerdiğimiz temel adımlar bulunmaktadır. Ancak eğer bir aile üyesi bu adımları anlamamışsa sizin bu adımlar üzerinden geçerek gerçekleştirmeniz gereklidir.

- **Sosyal Mühendislik**: İlişkili olabilecek herkese sosyal mühendislik kavramlarını basit ifadelerle anlatın. Sahtekarlar ve dolandırıcılar binlerce yıldır kol gezmektedirler, bu tür saldırılar yeni değildir. Şu andaki tek fark, kötü niyetli kişilerin aynı kavramları bugün internete uygulamasıdır. En yaygın sahtekarlık saldırıları ile ilgili örnekler verin, yaygın oltalama e-postaları ya da adı kötüye çıkmış Microsoft teknik destek telefon çağrıları gibi. Hiçbir şey olmasa bile aile bireylerinin kesinlikle kimseye şifrelerini ya da bilgisayarlarına uzaktan erişim yetkilerini vermemeleri gerektiğini anladıklarından emin olun. Son olarak e-posta ya da birilerinin onları aramaları konusunda rahatsız olduklarında ya da kafalarında sorular oluştuğunda, herhangi bir bilgi vermeden önce sizi arayacaklarından emin olun.
- **Evdeki Kablosuz Ağlar**: Evde kullandıkları kablosuz ağın güvenli olduğundan emin olmak için vakit harcayın. En azından ön tanımlı yönetici şifresinin değişmiş olduğundan. Kablosuz ağa erişmek için güçlü bir şifre tanımlanmış olduğundan ve ağ bağlantısının en güncel şifreleme yöntemlerini kullandığından emin olun. Ayrıca, kablosuz ağı www.opendns.org gibi güvenli bir DNS kullanacak şekilde yapılandırmayı dikkate alabilirsiniz. Bunun gibi güvenli DNS servisleri sadece bulaşmış ağ sitelerinden ziyaretçileri engellemeye yardım etmekle kalmaz, aynı zamanda size kişilerin hangi ağ sitelerini ziyaret edip edemeyeceğini kontrol etmenizi sağlar ki bu da ziyarete gelen çocuklar için çok kıymetlidir.

Siber Nesil Farkını Dikkate Alarak Çocuklarınızı Çevrim-içi Güvenli Hale Getirmek

- **Yamalama**: Sistemleri tamamıyla güncel tutmak herhangi bir teknolojiyi güvenli hale getirmek için alınabilecek en temel önlemdir. Bunun gibi, tüm ev cihazlarını (mobil cihazlar dahil olmak üzere) ve uygulamalarını tamamiyle yamalayın. Bundan emin olmanın en kolay yolu, otomatik güncelleme şeçeneğini etkinleştirmektir.
- **Anti-Virus**: İnsanlar hata yapabilir, bazen yapmamız gerektiği halde bazı uygulamalara tıklayıp yükleriz. Anti-virüs programları tüm kötü amaçlı yazılımları engelleyemez, daha çok yaygın saldırıların tespit edilmesine ve engellenmesine yarar. Tüm ev bilgisayarlarında anti-virüs programı yüklendiğinden, güncel ve aktif olduğundan emin olun.
- **Parolalar**: Güçlü parolalar, hem cihazların hem de çevrim-içi hesapların korunmasında kilit bir rol oynar. Aile bireylerin güçlü parolalar tanımlaması konusunu detaylı bir şekilde açıklayın. Parolalar tanımlanırken sözcük ya da cümlelerin kullanılması, parolaların hatırlanmasını kolaylaştırabilir. Bir diğer seçenek ise parola yöneticilerini yükleyerek nasıl kullanılacağını anlatmaktır. Eğer bu da işe yaramazsa, şifrelerini bir yere yazarak, sadece onların ulaşabilecekleri gizli bir yerde saklamaklamaları gerektiğini anlatabilirsiniz. Herhangi bir hassas çevrim-içi hesap için iki-aşamalı doğrulama kullanmayı seçebilirsiniz.
- **Yedekleme**: Tüm çareler tükendiğinde yedekler hayatınızı kurtarır. Basit ve güvenilir bir yedekleme sistemine sahip olduklarından emin olun.

Eski nesillerin kendi evlerindeki teknolojileri koruma ve evlerini ziyaret eden çocuklar için güvenli bir ortam yaratma konusunda yardıma ihtiyaçları olabilir.

Bu önlemlerin alınıp alınmadığını her ay ya da 3 ayda bir kontrol etmek isteyebilirsiniz. En kötü senaryoda bir cihaza uzaktan yönetim yazılımını kurmayı düşünebilirsiniz. Eğer bu şekilde bir yol izlerseniz, erişimin şifreleme ve güçlü ve eşsiz bir parola ile korunduğundan emin olun.

Ziyarete Gelen Çocuklar

Çoğu zaman çocuklar büyükanne ve büyükbabaları gibi akrabalarının evini ziyarete gittiğinde evinizdeki kurallar artık geçerliliğini kaybeder. Bunlar, çocuklarınızın çevrim-içi olduklarında korunmalarına yardımcı olacak kuralları içerebilir. Aşağıda çocuklarınızı korumak için alabileceğiniz önlemleri bulabilirsiniz.

Kurallar. Çocuklarınızın güvenliği için yakınlarınızın bilmesi gereken kuralların ya da beklentilerin olup olmadığından emin olun. Örneğin, çocuklarınızın ne kadar süre ile çevrim-içi oyun oynayacaklarını belirleyen bir kuralınız var mı? Ya da mobil cihazlara erişimleri olup olmadığı konusunda. Çocuklarınızın büyükanne, büyükbaba ya da diğer akrabalarınıza açıklama yapacaklarını farz etmeyin. Bir fikir kuralların yazılı olduğu bi sayfa hazırlamak ve bunu çocuklarınızın sıklıkla ziyaret ettiği diğer akrabalarınızla paylaşmaktır.

Siber Nesil Farkını Dikkate Alarak Çocuklarınızı Çevrim-içi Güvenli Hale Getirmek

Kontrol: Eğer çocuklarınız teknolojiyi kendi bakıcılarından daha iyi anlıyorlarsa, bundan yararlanabilirler. Örneğin, çocuklar büyükanne ya da büyükbabalarına ait bilgisayarların yönetim parolalarını isteyebilir ya da elde edebilirler ve daha sonra sizin oynamalarını istemediğiniz bir oyunu yükleyip oynamak gibi istediklerini yapabilirler. Akrabalarınızın çocuklara verilmemesi gereken erişimleri bildiğinden emin olun.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve http://www.securingthehuman.org adresini ziyaret ederek SANS güvenlik farkındalığı çözümleri hakkında daha fazla bilgi edinin.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup SOSoft Bilişim Teknolojilerinde biyometrik güvenlik sistemleri üzerinde çalışmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, telekomünikasyon, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, iş sürekliliği, risk yönetimi, altyapı hizmetleri, yazılım geliştirme ve proje yönetimi alanlarında yönetici ve danışman olarak 15 yılı aşkın süredir görev yapmaktadır.

Mustafa Emrah Ünsür, Güvenlik Araştırmacısı olarak araştırmaları, makaleleri ve çevirileri vardır. Beyaz Şapkalı Hacker olarak kendisi tarafından kodlanan ve kodlanmakta olan 'exploit'ler ve 'tool'lar bulunmaktadır. Ayrıca, Sızma Testi Uzmanı olarak özel şirketlere ve devlet kurumlarına Zafiyet ve Sızma Testi yapmış ve yapmaya devam etmektedir.

Kaynaklar

Sosyal Mühendislik:	http://www.securingthehuman.org/ouch/2014#november2014
Ev Ağınızı Güvenli Hale Getirmek:	http://www.securingthehuman.org/ouch/2014#january2014
Parolalar:	http://www.securingthehuman.org/ouch/2015#april2015
Anti-Virus:	http://www.securingthehuman.org/ouch/2014#december2014
Çocuklarınızı çevrim-içi olduklarında korumak:	http://www.securingthehuman.org/ouch/2013#april2013
Teknik destek hizmeti sahtekarlığı:	http://www.onguardonline.gov/articles/0346-tech-support-scams
Siber güvenli bir ev için (poster):	http://www.securingthehuman.org/resources/posters

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis