

OUCH!

BU SAYIDA...

- Giriş
- 5 Basit Adım
- Başkalarını Ziyaret Ederken Çocukların Güvenliğini Sağlamak

Başkalarının Güvenli Hale Gelmesine Yardım Etmek

Giriş

Birçoğumuz teknoloji konusunda, hatta onu güvenli ve emin kullanma konusunda kendimizi rahat hissediyoruz. Ancak diğer arkadaşlarımız ve aile üyelerimiz bu kadar rahat hissetmeyebilirler. Aslında, kafaları karışmış ve hatta korkmuş olabilirler. Bu onları bugünün siber saldırganlarına karşı oldukça zayıf hale getirir. Siber güvenlik korkutucu birşey olmak zorunda değildir, temel konuları anladığınızda aslında çok basittir. Çoğunlukla onların bu temel konuları anlamaları için sizin gibi bir rehber ihtiyaçları vardır.

Konuk Yazar

Randy Marchany (Twitter hesabı: [@randymarchany](https://twitter.com/randymarchany)) Virginia Tech Bilgi Güvenliği Yöneticisi (CISO) ve sertifikalı SANS Institute eğitmenidir.

5 Basit Adım

Burada başkalarına korukularını yenmek ve bugünün teknolojilerinin çoğundan yaralanmak konusunda yardım ederken kullanacağınız 5 temel adım yer alıyor. Herbir konuda daha fazla bilgi isterseniz, yazının sonundaki Kaynaklar bölümüne bakabilirsiniz.

- Sosyal Mühendislik:** Sosyal mühendislik siber saldırganların insanları yapmamaları gereken birşeyi (parolalarını paylaşmak, bilgisayarlarına virüs bulaştırmak ya da hassas verileri paylaşmak gibi) yapmaları için kandırmak amacıyla kullandıkları genel bir yöntemdir. Bu yeni birşey değil aslında, dolandırıcılar binlerce yıldır var olmuşlardır. Tek fark kötü niyetli kişilerin aynı yöntemleri artık internet üzerinden uyguluyor olmasıdır. Örneğin çok acil hissi uyandıran birisi olması, inanılmayacak kadar iyi bir şeyin konu edilmesi, ya da saldırganın bilinen biri gibi davranıp aslında o kişi gibi olmaması durumları gibi, sosyal mühendislik saldırılarının fark edebileceği genel ipuçlarını öğreterek başkalarına yardımcı olabilirsiniz. Ortalama e-postalarının ya da Microsoft teknik destek hizmeti gibi yapılan aramaların örneklerini paylaşabilirsiniz. Bunların hiçbirini yapamasanız bile aile üyelerinizin, hiçbir zaman parolalarını paylaşmaması ve hiç kimseye bilgisayarlarına uzaktan erişme izni vermemesi gerektiğini anladığından emin olun.
- Parolalar:** Güçlü parolalar hem cihazları hem de çevrimiçi hesapları korumanın anahtarıdır. Güçlü parolaların nasıl oluşturulabileceği konusunda aile üyelerinizle çalışın. Biz parolaların birden çok kelimedenden oluşturulmasını öneriyoruz, böylece hem yazması hem de hatırlaması daha kolay oluyor. Ek olarak, onlara bir parola yöneticisi yazılımı kurma ve kullanma konusunda yardım edin. Herbir cihaz ve hesabınız için farklı, benzersiz parolaları kullanmak önemlidir. Eğer bir parola yöneticisi onlar için zor olacaksa, bir yere yazıp güvenli bir yerde saklamaları gerektiğini anlatın. Son olarak, önemli kullanıcı hesapları için, iki adımlı (genellikle iki faktörlü olarak adlandırılır) doğrulama seçeneğini aktif hale getirmelerine

Başkalarının Güvenli Hale Gelmesine Yardım Etmek

yardım edin. İki adımlı doğrulama, herhangi bir hesabın güvenliğini sağlamak için en etkin yöntemlerden biridir.

3. **Güncellemeler:** Sistemleri güncel tutmak cihazların güvenliğini sağlamak konusunda önemli bir adımdır. Bu sadece bilgisayarlarınız ve mobil cihazlarınızın için değil, internete bağlanan oyun konsolları, termometreler, aydınlatma cihazları hatta hoparlörler gibi birçok şey için geçerlidir. Cihazlarının sürekli güncellendiğinden emin olmanın en basit yolu, otomatik güncelleme seçeneğini mümkün olan her yerde aktif hale getirmektir.

4. **Antivirüs:** İnsanlar hata yapabilir, bazen yapmamamız gereken ve sistemlerimizi ele geçirebilecek şeyleri kurar ya da kötü niyetli site bağlantılarına tıklarız. Antivirüs yazılımları bizleri bu tehlikelerden korumak için tasarlanmıştır. Antivirüs yazılımları tüm kötücül yazılımları durdurmasa da birçok genel saldırıyı tepit etme ve durdurma konusunda yardımcı olur. Kişisel bilgisayarlarda antivirüs uygulamalarının kurulu olduğundan ve güncel ve aktif olduğundan emin olun. Ek olarak, bugünün çoğu antivirüs yazılımı, güvenlik duvarları ve web tarayıcı koruma özellikleri gibi başka güvenlik teknolojilerini de içermektedir.

5. **Yedeklemeler:** Yedeklemeler diğer herşey başarısız olduğunda, yanlışlıkla sildiğiniz dosyalar ya da fidyeci yazılımlar tarafından şifrelenen veriler gibi kayıplarınızı geri kurtarabilmenin tek yoludur. Ailenizin ve arkadaşlarınızın ototmak bir dosya yedekleme sistemi kullandığından emin olun. Genellikle en basit çözümler bulut tabanlı, cihazlarınızın siz herhangi bir dosya değişikliği yaptığınızda ya da saatlik olarak yedeğini alan çözümlerdir. Bu çözümler sadece yedeklemeyi değil, geri kurtarmayı da kolaylaştırır.



Başkalarının bugünün teknolojilerinin çoğundan güvenle yararlanabilmesine, bu 5 basit adımı paylaşarak yardım edin.

Başkalarını Ziyaret Ederken Çocukların Güvenliğini Sağlamak

Teknolojiyle aranız iyiyse muhtemelen sadece kendinizin değil, çocuklarınızın da güvenliğini sağlamışsınızdır. Ancak çocuklar büyükbaba, büyükanne gibi teknoloji konusunda kendisi çok da rahat hissetmeyen aile üyelerini ziyarete gittiğinde, bu akrabalar çocukların çevrimiçi ortamlarda nasıl en iyi korunacağını ya da sizin beklentilerinizi bilmiyor olabilirler. Burada çocuklarınız başkalarını özellikle de akrabalarınızı ziyarete gittiğinde güvenli olmalarına yardımcı olmak için uygulayabileceğiniz bazı adımlar yer alıyor:

- **Kurallar:** Sizin çocukların güvenliği için uyguladığınız kuralları ve beklentileri onların da bilmesini sağlayın. Örneğin, çocukların çevrimiçi olduklarında uyması gereken kurallar var mı? Kimlerle konuşabilir ya da hangi oyunları oynayıp, hangi oyunları oynayamazlar? Bize güvenin, çocuklarınızın bu kuralları akrabalarınıza anlatmasını beklemeyin. Bir "Kural Sayfası" hazırlamak ve çocuklarının sıklıkla ziyaret ettiği akrabalarla paylaşmak iyi bir fikir olabilir.

Başkalarının Güvenli Hale Gelmesine Yardım Etmek

- **Kontrol:** Eğer bir çocuk, teknolojiyi kendisine bakan kişilerden daha iyi anlıyorsa, bunun avantajını kullanabilir. Örneğin, büyükbabasının bilgisayarında yönetici haklarını isteyip ya da ele geçirip, sonra da ailesinin oynamasına izin vermediği ancak kendisinin istediği bir oyunu indirip kurabilir. Akrabalarınızın çocuklarınıza ek bir erişim yetkisi vermemeleri gerektiğini anladıklarından emin olun.

Son olarak, insanlara kendi kendilerine öğrenmeye devam etmeleri için OUCH! Bülteni gibi kaynaklara üye olmalarını önerin. Bu bülten, her ay ücretsiz olarak 20'nin üzerinde farklı dilde yayınlanıyor. Üye olmak için:

<https://securingthehuman.sans.org/ouch>

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve securingthehuman.sans.org/ouch/archives adresini ziyaret ederek SxANS 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 (<https://tr.linkedin.com/in/semayuce>), Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetim/strateji, risk yönetimi, iş sürekliliği, hizmet yönetimi, altyapı hizmetleri, yazılım geliştirme ve program/proje yönetimi alanlarında yönetici ve danışman olarak 19 yılı aşkın süre görev yapmış olup, Nisan 2016 itibarıyla Trust ISC (www.trustisc.com) adıyla uzmanlık alanlarında hizmet vermekte olduğu kendi danışmanlık şirketini kurmuştur.

Kaynaklar

Sosyal Mühendislik:	https://securingthehuman.sans.org/ouch/2017#january2017
Parolalar:	https://securingthehuman.sans.org/ouch/2017#april2017
Parola Yöneticileri:	https://securingthehuman.sans.org/ouch/2017#september2017
İki Adımlı (Faktörlü) Doğrulama:	https://securingthehuman.sans.org/ouch/2015#september2015
Yedekleme ve Kurtarma:	https://securingthehuman.sans.org/ouch/2017#august2017
Bugünün Online Çocuklarını Koruma:	https://securingthehuman.sans.org/ouch/2017#may2017

OUCH!, SANS Securing The Human Programı tarafından yayınlanır ve [Creative Commons BY-NC-ND 4.0 lisansı](https://creativecommons.org/licenses/by-nc-nd/4.0/) altında dağıtılır. Bülteni değiştirmedığınız sürece, bu bülteni dağıtabilir ya da kendi farkındalık programlarınızda kullanabilirsiniz. Çeviri ya da daha fazla bilgi için, lütfen ouch@securingthehuman.org e-posta adresini kullanarak iletişime geçiniz.

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus