

OUCH!

Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

Sosyal Medyayı Güvenli Bir Şekilde Kullanmanın İpuçları

Giriş

Snapchat, Facebook, Twitter, Instagram ve LinkedIn gibi sosyal medya siteleri, insanlarla tanışmaya, iletişim kurmaya ve paylaşım yapmaya olanak veren muhteşem araçlardır. Ancak bu etki ve güç riskleri de beraberinde getirir, sadece sizin için değil, aileniz, arkadaşlarınız ve çalışanlarınız için de. Bu sayıda, sosyal medyayı daha güvenli ve emniyetli hale getirmenin anahtar adımlarından bahsedeceğiz.

Gönderim

Gönderim yapmadan önce bir kere daha düşünün ve dikkatli olun. Yaptığınız gönderim büyük ihtimalle bir noktada halka açık hale gelecektir, ki nerede okula gideceğinizi ve iş bulacağınızı kapsayacak şekilde bu, sizin itibarınızı ve geleceğinizi etkileyecektir. Eğer ailenizin ve patronunuzun gönderiminizi görmelerini istemiyorsanız, büyük ihtimalle bu gönderimi yapmamalısınız. Ayrıca başka insanların sizinle ilgili yaptıkları gönderimlerden de haberdar olmalısınız. Belki onlardan sizinle ilgili yaptıkları paylaşımları kaldırmalarını isteyebilirsiniz.

Gizlilik

Hemen hemen tüm sosyal medya siteleri size güçlü gizlilik seçenekleri sunarlar, mümkün olduğunca bunları etkinleştirin. Örneğin, kullandığınız sitenin gerçekten sizin bulunduğunuz yeri (lokasyonunuzu) takip etmesine gerek var mı? Ayrıca, gizlilik seçenekleri kafa karıştırıcı olabilir ve sık sık değişir. Bu seçeneklerin sizin istediğiniz gibi çalıştığını kontrol etmeyi ve onaylamayı bir alışkanlık haline getirin.

Parolalar

Sosyal medya hesabınızı uzun ve eşsiz bir parola ile koruyun. Parola, birden fazla kelimedenden oluşan, kolayca tuşlayabileceğiniz ve hatırlayabileceğiniz ancak siber saldırganların tahmin ederken zorlanacağı bir şifredir.

Oturumunuzu Kilitlemek

Daha iyisi, tüm hesaplarınız için iki-adımlı doğrulamayı aktif hale getirin. Bu yöntem, hesabınız ile oturum açmak istediğinizde parolanızın yanına tek seferlik bir kodu ekler. Bu gerçekten çok kolaydır ve en güçlü koruma yöntemlerinden biridir.

Dolandırıcılık

E-postalardaki gibi kötü niyetli kişiler, sizi sosyal medya mesajlarıyla kandırmaya çalışacaklardır. Örneğin, parolanız ve kredi kartınızla sizi kandırmaya çalışabilir. Neyi tıkladığınıza dikkat edin: Eğer bir arkadaşınız size tuhaf gelen

bir mesaj gönderdiyse ya da arkadaşınızdan gelmiş gibi görünmüyorsa, bu kişi arkadaşınız gibi davranan bir siber saldırgan olabilir.

Kullanım Koşulları

Sitelerin kullanım koşullarının farkında olun. Herhangi bir gönderim ya da yüklemeniz sitenin malı haline gelebilir.

İş Yeri

Eğer iş yerinizle ilgili herhangi birşey hakkında gönderim yapmak isterseniz, öncelikle bunun halka açık hale gelmesinin uygun olup olmadığını amirinizle kontrol edin.

Daha güvenli bir çevrim-içi tecrübe için bu ipuçlarını takip edin. Sosyala medya sitelerinin daha güvenle nasıl kullanılacağını ya da yetkisiz erişimleri nasıl raporlayacağınızı öğrenmek için sosyal medya sitesinin güvenlik sayfasını ziyaret edin.

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, 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 yaptıktan sonra, Truth ISC (www.truth-isc.uk) adıyla kurduğu Türkiye ve İngiltere'de faaliyet gösteren danışmanlık şirketinde hizmet vermeye devam etmektedir.

Konuk Yazar

Jessica Barker siber güvenliğin sosyal mühendislik (insani) tarafında bir dünya lideridir. Dünya genelindeki müşterilerine danışmanlık servisi verdiği [Redacted Firm](#), firmasının kurucu ortağı ve çok iyi bilinen bir konuşmacıdır. [@drjessicabarker](#) ile twitter'dan takip edebilirsiniz.



Kaynaklar

Parolalar:	https://www.sans.org/u/B6E
İki-Adımlı Doğrulama:	https://www.sans.org/u/B6J
Bugünün Çevrim-içi Çocuklarını Güvende Tutmak:	https://www.sans.org/u/B6O
Oturumunuzu Kitlemek:	https://www.lockdownyourlogin.org/

Lisans

OUCH!, SANS Securing The Human Programı tarafından yayınlanır ve [Creative Commons BY-NC-ND 4.0 lisansı](#) altında dağıtılır. Bülteni değiştirmedığınız sürece, bu bülteni dağıtabilir ya da kendi farkındalık programlarınızda kullanabilirsiniz. Çeviri ya da daha fazla bilgi için, lütfen www.sans.org/security-awareness/ouch-newsletter e-posta adresini kullanarak iletişime geçiniz. Yayın Kurulu : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley