OUCH! | Eylül 2019

Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

Sosyal Medya Yolu ile Dolandırılmak

Giriş

Birçoğumuz evde ya da iste dolandırıcılık e-posta saldırılarına maruz kalmışızdır. Bunlar örneğin bankanızdan, patronunuzdan ya da en çok sevdiğiniz cevrim-içi alışveriş mağazasından gelen meşru ve gerçek gibi görünen e-postalarıdır. Ancak bunlar sizi aceleye getirerek harekete geçmenize neden olup sizi kandırmaya çalışan saldırılardır, örneğin virüs bulaşmış bir e-posta eklentisini açmanız, şifrenizi paylaşmanız ya da para göndermeniz gibi. Buradaki zorluk sudur: biz ne kadar deneyimli hale geliyorsak insanları dolandırmak için siber suçlular da o kadar farklı yollar deniyorlar.

Skype, WhatsApp ve Slack'dan Twitter, Facebook, Snapchat ve hatta oyun uygulamalarına kadar hemen hemen her tur iletişim seklinde kandırılmanız ve dolandırılmanız mümkündür. Bu platform ve kanallar ile iletişim kurmak daha gayri resmi ve güvenilir olarak görülür, iste tam bu yüzden saldırganlar bunları diğerlerini kandırmak için kullanırlar. Ayrıca bugünün teknolojileri ile dünyanın herhangidir yerinde olan herhangi bir saldırgan için istedikleri gibi başkası ya da başka bireymiş gibi davranmak çok daha kolaydır. Unutmamalısınız ki herhangi bir iletişim yolu ile karsınıza çıkan kişiler göründükleri gibi ve söyledikleri kişiler olmayabilirler.

Alınacak Dersler

Aldığınız bir mesajın ya da gönderilmiş bir yazının ir saldırı olabileceğini gösteren en yaygın ipuçları şunlardır

Acillik: Bir hesabınızın kapatılması ya da hapse gitmeniz ile ilgili bir tehdite benzer, bir şey kotu gitmeden önce "Acil bir eylem" gerektiren ve acil hissiyati yaratan bir mesajdır. Saldırgan sizin hata yapmanıza neden olacak şekilde sizi aceleye getirir.

Baskı; İşte uygulamanız gereken tedbir ve prosedürleri pas geçmenize neden olacak şekilde baskı yapılması

Merak: İnanılmayacak kadar iyi olan bir şey ile ilgili güçlü bir merak hissini uyandıran. Hayır, o piyangoyu siz kazanmadınız.

Hassas: Kredi kartı numaranız, şifreniz ya da paylaştığınızda kendinizi rahat hissetmeyeceğiniz hassas bir bilginin istenmesi.

Resmi mesajlar: Kotu bir dil yapisi ve yazımı olmasına rağmen resmi bir kurumdan geldiğini söyleyen bir mesaj. Birçok ülke kurumu resmi yazışmalar için sizinle direk iletişime geçmek için sosyal medyayı kullanmaz. Eğer mesajın meşru ve gerçek olduğundan emin değilseniz, kurumu arayın ancak örneğin kendi web sitelerinde yazan güvenilir bir telefon numarası kullanın.

Taklit Etme: Bir arkadaşınızdan ya da beraber çalıştığınız bir kişiden bir mesaj aldınız, ancak yazım ve üslup sanki onlar değilmiş gibi. Eğer şüphe ediyorsanız, teyit etmek için mesaj gönderen kişiyi telefonla arayın. Bir siber saldırganın, sizin tanıdığınız birinden geliyormuş gibi görünen bir mesaj oluşturması kolaydır. Bazı durumlarda bir arkadaşınızın hesabını ele geçirirler ve arkadaşınız gibi davranarak sizinle iletişime geçerler. Gönderenin kişiliğini çok yansıtmayan Twitter ve diğer kıs mesaj formatları ile yazılan metin mesajları konusunda daha dikkatli olun.

Dolandırıcılıklara ve bunun gibi saldırılara karşı en iyi savunma kendinizsiniz. Bir yazı ya da mesaj garip ya da şüpheli görünüyorsa, sadece görmezden gelin ve silin. Ya da bu metin kişisel olarak tanıdığınız birinden geldiyse, bu kişiyi telefonla arayın ve gerçekten bu mesajın ona ait olup olmadığından emin olun.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup Hawaii Üniversitesinde yazılım mimarileri ve yazılım güvenliği üzerinde doktora sonrası araştırma yapmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetişim/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 Editor

Dr. Jessica Barker *(@drjessicabarker) siber güvenliğin insani tarafı ile ilgili konularda bir liderdir. Cygenta'nin yönetici ortaklarından olup tüm dünyada siber güvenlik farkındalığı, tutumu ve kültürünü olumlu etkileme tutkusunun pesinden gitmektedir. Ayrıca ClubCISO'in başkanı ve bilinen bir ana tema konuşmacısıdır.*

Kaynaklar

Sosyal Mühendislik:	https://www.sans.org/u/Uz6
Telefon Sahtekârlığı:	https://www.sans.org/u/Uzb
Dolandırıcılıkları Durdurun:	https://www.sans.org/u/Uzg
Kişiselleştirilmiş Sahtekârlık:	https://www.sans.org/u/Uzl