Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...



# CEO Dolandırıcılığı

## CEO Dolandırıcılığı Nedir?

Siber suçlular sinsidir, istediklerini almak için yeni yollara başvururlar. En etkili yöntemlerden biri sizin gibi insanları hedef almalarıdır. Siber suçlular habersiz kişilerin şirketteki en zayıf halka olduğunu öğrenmiş iken OUCH! okuyucuları gibi bilgili kişilerin bir şirketin en iyi savunucuları olduğunu unutuyorlar.


### Konuk Yazar

Angela Pappas, Thomson Reuters'da bilgi güvenliği eğitimi ve farkındalığının yöneticisidir. Angela, oltalama ile ilgili e-öğrenme ve çalışanların eğitimini içeren elçilik programından sorumludur.


Siber suçlular, İş E-postası Ele geçirme (İEE, Business Email Compromise (BEC)) olarak da bilinen CEO dolandırıcılığı ile isimlendirilen yeni bir saldırı geliştirdiler. Bu tür saldırılarda siber suçlular, bir CEO (başkan) ya da şirketinizdeki üst düzey bir yönetici gibi davranır. Bu suçlular sizin gibi çalışanlara, yapmamanız gereken bir şeyi yaptırmak için sizi kandırmayı amaçlayan bir e-posta gönderir. Siber suçlular tahkikatlarını yaptıkları için bu tür saldırılar son derece etkilidir. Şirketin nerede olduğu, yöneticilerinizin kim olduğu ve birlikte çalıştığınız şirketlerin kimler olduğu gibi bilgileri, şirketinizin web sayfasından araştırırlar. LinkedIn, Facebook ve Twitter gibi sayfalardan iş arkadaşlarınızla ilgili alabildikleri kadar çok bilgiyi öğrenirler. Bir kez şirket yapısını öğrendiler mi belirli çalışanları araştırır ve hedef alırlar. Hedeflerini belirli amaçları temel alarak seçerler. Eğer paranın peşinde iseler muhasebe bölümündeki çalışanları hedef alabilirler. Eğer vergi bilgisi arıyorlarsa insan kaynaklarını hedef alabilirler. Eğer veri tabanı sunucularına ulaşmak istiyorlarsa, bilgi sistemlerinden herhangi birini hedef alabilirler.

Bir kez ne istediklerini ve kimi hedef aldıklarının kararını verdikten sonra saldırılarını ustalıkla yaparlar. Daha çok mızrak saplama kullanırlar. Oltalama, bir saldırganın kişilerin virüslü bir dosyayı açmaları ya da kötü niyetli bir web sitesini ziyaret etmeleri gibi bir şeyi yaptırmak için onları kandırmak amacıyla milyonlarca kişiye bir e-posta göndermesidir. Mızrak saplama, oltalamaya benzer, ancak milyonlarca kişiye genel bir e-posta göndermek yerine ufak ve seçilmiş bir grup kişiyi hedef alan uyarlanmış bir e-posta gönderirler. Bu mızrak saplama e-postaları gerçekçi görünür ve teşhis edilmesi zordur. İş arkadaşınız ya da belki müdürünüz gibi birlikte çalıştığınız ya da tanıdığınız birinden geliyor gibi görünürler. Iş arkadaşınızın kullandığı jargonu, şirketin logosunu ya da hatta bir yöneticinin resmi imzasını kullanabilecekleri için gerçekçi görünürler. Bu e-postalar çoğunlukla sizin hemen harekete geçmenizi ve kimseye bir şey söylememenizi isteyerek büyük bir aciliyet algısı yaratırlar. Siber suçluların amacı sizi hata yaptırmaya

## CEO Dolandırıcılığı

sevk ederek bir işe düşünmeden hızla girmenizi sağlamaktır. Üç yaygın örnek senaryo aşağıda verilmiştir:

- **Banka Havalesi**: Bir siber suçlu paranın peşindedir. Bu onların şirketinizin muhasebede çalışanı ya da şirketinizin mali işleri ile ilgilenen takımdaki kişileri araştırdığı ve öğrendiği anlamına gelir. Bu suçlular daha sonra ustalıkla bir e-posta oluşturur ve yöneticileri gibi davranan e-postayı gönderirler. Bu e-posta bir aciliyetin olduğunu ve tanımlı bir hesaba hemen para transfer edilmesi gerektiğini belirtirler.

- **Vergi Dolandırıcılığı**: Siber suçlular, iş arkadaşlarınız gibi davranarak vergi dolandırıcılığı yapmak için onların bilgilerini çalmak istemektedirler. Şirketinizi araştırırlar ve kimin çalışan bilgilerine sahip olduğunu öğrenirler, örneğin insan kaynaklarından herhangi biri. Buradan siber suçlular üst düzey bir yönetici ya da tüzel bir kişilik gibi davranarak çalışanların, birtakım dokümanları hemen göndermelerini isteyen sahte e-postalar gönderirler.


*CEO Dolandırıcılığı, birçok güvenlik korumasını atlatabilen çok güçlü bir saldırıdır. Sonuçta siz bizim en iyi savunmamızsınız.*

- **Avukat Taklidi**: CEO Dolandırıcılığı saldırılarının hepsi sadece e-postayı içermez, telefon gibi diğer yöntemler de kullanılabilir. Bu senaryoda suçlular kıdemli bir yönetici gibi davranarak bir avukatın acil bir konu hakkında arayacağını haber veren bir e-posta göndererek işe başlarlar. Suçlu daha sonra avukat gibi davranarak sizi arar. Gizli ve zamana duyarlı konular ile ilgili konuşarak sizde büyük bir aciliyet algısı yaratırlar. Bu aciliyet algısı sizin hemen harekete geçmenize neden olarak sizi aldatır.

## Kendinizi Korumak

Peki, şirketiniz ve kendinizi korumak için ne yapabilirsiniz? Sağduyu sizin en iyi savunmanızdır. Eğer müdürünüzden ya da iş arkadaşınızdan bir mesaj aldıysanız ve size doğru gibi gelmiyorsa bu bir saldırı olabilir. Büyük bir aciliyet algısı, doğru görünmeyen bir imza, beklemediğiniz belirli bir tavır veya sizi hitap eden kişinin hitap edişinden farklı bir ismin kullanılması ipuçları olabilir. Bir diğer ipucu ise saldırgan sizin daha önce bilmediğiniz bir e-posta adresi ya da telefon kullanıyor olması olabilir, ya da belki iş arkadaşınız ya da müdürünüzün kullandığı e-posta adresine çok benziyor olabilir ancak aynısı değildir. Şüpheye düştüğünüzde, güvenilir bir

## CEO Dolandırıcılığı

telefondan o kişiyi arayın ya da yüz yüze buluşun (e-postaya cevap vermeyin) ve ilgili e-postayı gönderip göndermediğini teyit edin. Hiçbir zaman güvenlik süreçlerini ve politikalarını atlamayın. Şirketiniz, para transferinde yetkilendirme ya da gizli bilginin yayımlanması ile ilgili uygun süreçler, tanımlayan politikalara sahip olabilir. Bu politikaların pas geçilmesine çabalayan istekler, görünen kaynağın ne olduğuna bakılmaksızın, şüpheli olarak nitelendirilmeli ve harekete geçmeden önce doğrulanmalıdır. Böyle bir istek alırsanız ve ne yapacağınız konusunda emin değilseniz, hemen danışmanınızla, yardım masasıyla ya da bilgi güvenliği takımı ile iletişime geçin.

## Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve securingthehuman.sans.org/ouch/archives 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.

## Kaynaklar

| | |
|---|---|
| Sosyal Mühendislik: | https://securingthehuman.sans.org/ouch/2014#november2014 |
| Oltalama: | https://securingthehuman.sans.org//ouch/2015#december2015 |
| Kötü Amaçlı Yazılım Nedir?: | https://securingthehuman.sans.org/ouch/2016#march2016 |
| İki adımlı doğrulama: | https://securingthehuman.sans.org/ouch/2015#september2015 |
| Günün ipucu: | https://www.sans.org/tip-of-the-day |



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