



EKİM 2026 · FARKINDALIK SERİSİ



İŞ YERİNDE VE SOSYAL MEDYADA

Kullanıcıyı Hedef Alan Saldırılar ve Dolandırıcılık Yöntemleri

Sahte İK hesapları ve çalışan profilleri · Yönetici ve iş ortağı taklitleri
Ele geçirilen hesaplar · Ses ve görüntü kopyaları
Para, veri ve erişim talepleri · Güvenli doğrulama yöntemleri

İÇİNDEKİLER

03 Editörden

04 Bu Mesajda Bir Tuhaflık Var

05 Yönetici mi, Dolandırıcı mı?

06 Tedarikçinin Hesabı Gerçekten Değişti mi?

07 İK mı, Sahte İK mı?

08 Çalışan Gerçekten O Çalışan mı?

09 Hesap Gerçek, Talimat Sahte

10 Bilgi İşlem Sizden Bunu İster mi?

11 Hangisi Gerçek Profil?

12 Arkadaşınız mı, Hesabını Ele Geçiren Biri mi?

13 Arayan Gerçekten Yöneticiniz mi?

14 Dolandırıcının Bastığı Dört Düğme

15 Bu Talebi Nasıl Doğrularsınız?

Mini test ve masanızda kalacak doğrulama kartı

Para, bilgi veya erişim isteyen bir talep geldiğinde birkaç saniye durun.

Editörden

**“Bugün öğleden önce şu hesaba ödeme yapar mısın?
Sonra anlatırım.”**

İlk tepki çoğu zaman işi geciktirmeden halletmek oluyor. Dolandırıcının güvendiği şey de tam olarak bu refleks.

Birini taklit etmek için kimi zaman sosyal medyadan alınmış bir fotoğraf ve isim yeterli. Kimi zaman da ortada sahte bir hesap bile yok. Gerçek hesap ele geçirilmiş, mesaj gerçekten bildiğiniz adresten gelmiş olabilir. Ekrandaki kişi tanıdık görünür, talep makul gelebilir. Tehlike de burada başlar.

Üstelik konu yalnızca yöneticiden gelen ödeme mesajlarıyla sınırlı değil.

- Sahte İK hesapları iş başvurusu bahanesiyle belge topluyor.
- Çalışan adına maaş hesabı değişikliği isteniyor.
- Arkadaşınızın hesabından para talebi geliyor.
- Bilgi işlem gibi davranan biri MFA kodunuzu soruyor.

Ekim sayısını, bir solukta gözden geçirilebilecek şekilde hazırladık. Mesaj örnekleri, kısa senaryolar ve küçük testler var.

Okurken kendinize şu soruyu sorun:

Bu talep bugün bana gelse ne yapardım?

Her mesaja kuşkuyla bakarak yaşanmaz. Ancak bir talep ödeme, belge paylaşımı veya hesap erişimi içeriyorsa acele etmeyin.

Ekrandaki isme değil, talebin kendisine bakın.

Gerekirse konuşmayı kesin, bildiğiniz numarayı kendiniz arayın ve sorun.

Bazen bir dakikalık teyit, uzun süre uğraşacağınız bir zararın önüne geçer.

SPARTA SİBER GÜVENLİK

BU MESAJDA BİR TUHAFLIK VAR

Gerçek bir vakadan uyarlanan bu e-postayı siz alsaydınız, nerede durup sorardınız?

GİZLİ SATIN ALMA İŞLEMİ

Çin'de bir şirket satın alıyoruz. İşlem henüz kamuya açıklanmadı.

SEC düzenlemelerini ihlal etmemek için bu konuyu **başka kanallardan konuşmayın.**

Denetim firmamızdan bir yetkili ödeme bilgilerini size iletecek. İlk transfer tutarı

780.000 dolar.

Neresinde durmalıydı?

1 Adı doğruydu, adresi değil

E-posta CEO'nun adıyla geldi ama her zaman kullandığı kurumsal adresten gelmedi.

2 Gizliliğin gerekçesi hazırdı

Siber suçlular mevzuatı bahane ederek başka bir kanaldan doğrulama yapılmasını engellemeye çalıştı.

3 Denetim firması da, çalışan da gerçekte

Ödeme bilgilerinin geleceği firma, şirketin gerçek denetim firmasıydı. Adı kullanılan kişi orada gerçekten çalışıyordu ve Scoular'ı hiç duymamıştı. E-posta adresi ve telefon numarası ise siber suçlulara aitti.

4 Arama yapıldı, teyit yapılmadı

Finans yöneticisi e-postadaki numarayı aradı ve beklediği isimle karşılaştı. Şüphesi dağıldı. Oysa numara bağımsız bir kaynaktan alınmamıştı.

GERÇEK VAKA: ÜÇ TRANSFER, 17,2 MİLYON DOLAR

Haziran 2014'te ABD'li tahıl ticareti şirketi Scoular'ın finans yöneticisine, CEO'dan ve denetim firmasından geliyormuş gibi görünen e-postalar gönderildi. Hikâye makuldü. Şirket gerçekten Çin'de büyümeyi değerlendiriyordu. Para Çin'deki bir banka hesabına gönderildi.

26 Haziran

780 bin dolar

27 Haziran

7 milyon dolar

30 Haziran

9,4 milyon dolar

TOPLAM: 17,2 MİLYON DOLAR

FBI soruşturma başlattı. Şirket de iç sistem ve kontrollerini sıkılaştırdığını açıkladı.

Mesajın dili tuhaf değildi. Kontrol etmek için kullanılan e-posta ve telefon da siber suçlulara aitti.

Teyit için mesajdaki numarayı değil, kendi kayıtlarınızdaki numarayı arayın.

E-posta örneği, gerçek vakadan uyarlanmıştır. Birebir mesaj metni değildir.

Kaynak: Reuters, CSO Online ve The Guardian

SPARTA SİBER GÜVENLİK

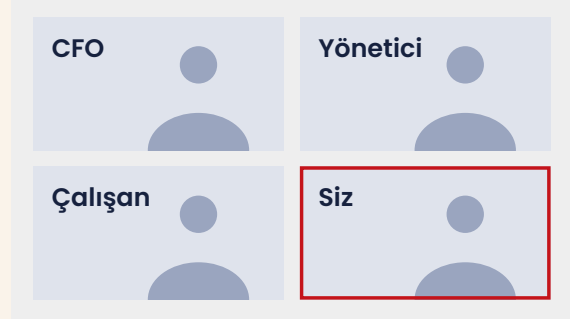
YÖNETİCİ Mİ, DOLANDIRICI MI?

Görüntülü toplantıdaydılar. Ancak toplantıdaki tek gerçek kişi, para transferini yapan çalışandı.

Finans ekibindesiniz.

CFO'dan gizli bir işlem için para transferi isteyen bir mesaj geliyor. Önce şüpheleniyorsunuz. Ardından CFO'nun ve birkaç çalışma arkadaşınızın bulunduğu görüntülü toplantıya katılıyorsunuz.

Yüzler tanıdık. Sesler tanıdık. Görüşme uzun sürmüyor. Katılımcılar talimatı veriyor ve toplantı sona eriyor.



Görüntülü toplantı talebi doğrulamış sayılır mı?

- A. Evet. CFO ve diğer yöneticiler görüntülü toplantıdaysa talep doğrulanmıştır.
- B. Hayır. Talep, şirket kayıtlarındaki numara kullanılarak ayrıca doğrulanmalıdır.
- C. Evet. Görüntü ve ses tanıdıksa ikinci bir kontrole gerek yoktur.

DOĞRU CEVAP: B

Birini görmek ve sesini duymak, o kişinin gerçekten toplantıda olduğunu kanıtlamaz. Talebi ileten toplantı, aynı talebin doğrulanması sayılamaz.

GERÇEK VAKA: TOPLANTIDAKİ HERKES SAHTEYDİ

Ocak 2024'te mühendislik şirketi Arup'ın Hong Kong ofisindeki bir finans çalışanı, şirketin CFO'sundan geliyormuş gibi görünen gizli işlem mesajı aldı.

Çalışan önce mesajdan şüphelendi. Ancak CFO'nun ve çalışma arkadaşlarının yer aldığı görüntülü toplantıya katılınca talebin gerçek olduğuna inandı. Hong Kong polisinin açıklamasına göre toplantıdaki diğer katılımcıların görüntüleri ve sesleri yapay zeka ile oluşturulmuştu.

Çalışan, beş banka hesabına 15 ayrı transfer yaptı.

15

TRANSFER

5

BANKA HESABI

200 MİLYON

HONG KONG DOLARI

Yaklaşık 25,6 milyon ABD doları

Dolandırıcılık, çalışan şirket merkezine ulaşip işlemi sorduğunda anlaşıldı. Arup, sahte görüntü ve seslerin kullanıldığını doğruladı. Şirketin iç sistemleri ele geçirilmemişti.

EKRANDA GÖRMEK, KİMLİĞİ DOĞRULAMAK DEĞİLDİR.

Beklenmedik bir ödeme veya yetki talebinde görüşmeyi sonlandırın. İlgili kişiyi şirket kayıtlarındaki numaradan arayın ve mevcut onay sürecini uygulayın.

Açılış senaryosu, gerçek vakadan uyarlanmıştır. Birebir toplantı kaydı değildir.

Kaynak: The Guardian, World Economic Forum ve China Daily

SPARTA SİBER GÜVENLİK

TEDARİKÇİNİN HESABI GERÇEKTEN DEĞİŞTİ Mİ?

Tedarikçi aynıydı. Bekleyen ödeme gerçekleşti. Değişen yalnızca banka hesabıydı.

KONU: BANKA BİLGİLERİMİZ DEĞİŞTİ

Merhaba,

Banka hesap bilgilerimiz güncellenmiştir. Bundan sonraki ödemelerin ekte yer alan yeni hesaba yapılmasını rica ederiz.

İyi çalışmalar.

Bu e-postadan sonra ilk adım hangisi olmalı?

- A. E-postadaki belgeye göre yeni hesabı sisteme tanımlamak.
- B. Aynı e-posta zincirinden hesap değişikliğini yeniden sormak.
- C. Eski kayıtlardaki numarayı arayıp değişikliği ayrıca doğrulamak.

DOĞRU CEVAP: C

Aynı e-postaya yanıt vermek, talebi doğrulamak değildir. Mesaj sahte bir adresten gelmişse yanıt yine siber suçlulara gider. Gerçek hesap ele geçirilmişse aynı e-posta zinciri de siber suçluların kontrolünde olabilir.

GERÇEK VAKA: ÜÇ ÖDEME, 11,8 MİLYON KANADA DOLARI

2017'de Kanada'daki MacEwan University, büyük tedarikçilerinden birinden geliyormuş gibi görünen e-postalar aldı. Mesajlarda tedarikçinin banka bilgilerinin değiştiği belirtiliyordu.

Talep gerçek kabul edildi ve yeni hesaba üç ayrı ödeme yapıldı. Ödemelerin toplamı 11,8 milyon Kanada dolarına ulaştı.

Dolandırıcılık, gerçek tedarikçinin ödemesinin neden yapılmadığını sormasıyla ortaya çıktı. Üniversite, olay sırasında bilgi sistemlerinin ele geçirilmediğini açıkladı.

Üniversitenin ilk incelemesi, ödeme süreçlerindeki kontrollerin yetersiz olduğunu ortaya koydu.

10 Ağustos

İlk ödeme yapıldı

17 ve 19 Ağustos

İki ödeme daha yapıldı

23 Ağustos

Gerçek tedarikçi aradı, dolandırıcılık fark edildi.

11,8 MİLYON KANADA DOLARI

Üç ayrı ödeme yanlış hesaba gönderildi.

Üniversite, olayın ortaya çıkmasının ardından paranın 10,92 milyon Kanada dolarlık bölümünü geri aldı.

HESAP DEĞİŞİKLİĞİ E-POSTAYLA ONAYLANMAZ.

Ödeme yapmadan önce tedarikçiyi mevcut kayıtlarınızdaki numaradan arayın. Değişikliği yetkili kişiyle doğrulayın ve kurumunuzdaki ikinci onay sürecini tamamlayın.

E-posta örneği, gerçek vakadan uyarlanmıştır. Birebir mesaj metni değildir.

Kaynak: TIME ve Global News

SPARTA SİBER GÜVENLİK

İK MI, SAHTE İK MI?

Sahte işe alım süreci, zararlı bir teklif dosyasıyla tamamlandı.

YENİ İŞ FIRSATI

Merhaba,

Profiliniz açık pozisyonumuzla örtüşüyor. Ücret paketimiz mevcut koşullarınızın oldukça üzerinde.

Kısa bir görüşme yapabilir miyiz?

Görüşmeler tamamlandı. Teklifinizi ekteki PDF’te bulabilirsiniz.

İş_Teklifi.pdf

Teklif dosyasını açmadan önce ne yapmalısınız?

- Şirketin kariyer sayfası ve resmi iletişim kanalı üzerinden süreci doğrulamak.
- Profilin bağlantı sayısına bakıp teklif dosyasını açmak.
- PDF dosyaları güvenli olduğu için dosyayı doğrudan açmak.

DOĞRU CEVAP: A

Görüşme yapılması, profilin eski görünmesi veya dosyanın PDF olması teklifin gerçekten o şirketten geldiğini göstermez. Şirketi kendi internet sitesi, kariyer sayfası ve yayımlanmış iletişim bilgileri üzerinden kontrol edin.

GERÇEK VAKA: SAHTE İŞ TEKLİFİ, 540 MİLYON DOLAR

2022’de Axie Infinity’nin geliştiricisi Sky Mavis’in kıdemli bir mühendisine LinkedIn üzerinden yeni bir iş

The Block’ın haberine göre siber suçlular, gerçekte var olmayan bir şirketin temsilcileri gibi davrandılar. Birden fazla görüşme yaptılar ve yüksek ücretli bir teklif sundular.

Teklif PDF olarak gönderildi. Mühendisin dosyayı indirmesinin ardından casus yazılım şirket sistemlerine sızdı. Siber suçlular işlem onay anahtarlarını ele geçirerek 173.600 ETH ve 25,5 milyon USDC çaldılar.

Varlıkların olay sırasındaki değeri yaklaşık 540 milyon dolardı. ABD makamları saldırıyı Kuzey Kore bağlantılı Lazarus grubuna atfetti.

LinkedIn mesajı

Cazip iş fırsatı sunuldu.

Birden fazla görüşme

Güven oluşturuldu.

Teklif PDF’i

Zararlı dosya indirildi.

Sistem erişimi

İşlem onay anahtarları ele geçirildi.

540 MİLYON DOLAR

Çalınan varlıkların olay sırasındaki yaklaşık değeri

İŞ TEKLİFİ, DOSYAYI GÜVENLİ YAPMAZ.

Beklemediğiniz bir iş teklifi geldiğinde şirketi ve işe alım yetkilisini resmi kanallardan doğrulayın. Dosyayı kurumsal cihazda açmadan önce bilgi güvenliği ekibine bildirin.

Mesaj örneği, gerçek vakadan uyarlanmıştır. Birebir mesaj metni değildir.

Kaynak: The Block, Ronin ve CISA

SPARTA SİBER GÜVENLİK

ÇALIŞAN GERÇEKTEN O ÇALIŞAN MI?

Dört görüntülü görüşme ve geçmiş kontrolü, bilgisayarları gerçekten kimin kullandığını göstermedi.

ONBOARDING KAYDI

4 görüntülü görüşme — TAMAMLANDI

Kimlik ve geçmiş kontrolü — TAMAMLANDI

Referans kontrolü — TAMAMLANDI

Kurumsal cihaz — TESLİM EDİLDİ

**İLK BAĞLANTI: Yetkisiz yazılım
çalıştırma girişimi**

**Bu kontroller tamamlandıysa
çalışanın kimliği doğrulanmış
sayılır mı?**

- A. Evet. Dört görüntülü görüşme ve geçmiş kontrolü yeterlidir.
- B. Evet. Cihaz doğru adrese teslim edildiyse süreç tamamlanmıştır.
- C. Hayır. Kimlik, cihazın bulunduğu yer ve ilk bağlantı birlikte doğrulanmalıdır.

DOĞRU CEVAP: C

İşe alım sırasında doğrulanan kişiyle kurumsal cihazı kullanan kişi aynı olmayabilir. Uzaktan erişim ve "laptop farm" düzenekleri, başka bir kişinin cihazı farklı bir ülkeden kullanmasını sağlayabilir.

GERÇEK VAKA: DÖRT GÖRÜŞMEYİ GEÇTİ, CİHAZ 25 DAKİKADA DURDURULDU

Temmuz 2024'te güvenlik farkındalığı şirketi KnowBe4, iç yapay zeka ekibi için bir yazılım mühendisi işe aldı. Aday dört görüntülü görüşmeye katıldı. Kimlik, geçmiş ve referans kontrollerinden geçti.

Daha sonra kullanılan kimliğin ABD'de yaşayan gerçek bir kişiden alındığı, başvuru fotoğrafının ise yapay zekayla değiştirilmiş bir stok fotoğraf olduğu anlaşıldı.

Kurumsal Mac bilgisayar teslim edildikten sonra güvenlik yazılımı şüpheli hareketleri algıladı. Kullanıcı oturum kayıtlarını değiştirmeye, zararlı olabilecek dosyalar aktarmaya ve izinsiz yazılım çalıştırmaya başladı.

KnowBe4'ün güvenlik ekibi cihazı yaklaşık 25 dakika içinde izole etti. Şirket, hiçbir sisteme yetkisiz erişim sağlanmadığını ve veri kaybı yaşanmadığını açıkladı. Mandiant ve FBI ile yapılan inceleme, kişinin Kuzey Kore bağlantılı sahte bir uzaktan çalışan olduğunu ortaya koydu.

ÇALINMIŞ KİMLİK → **DÖRT GÖRÜNTÜLÜ GÖRÜŞME** → **KURUMSAL CİHAZ TESLİMİ** → **EDR ALARMI VE İZOLASYON**

4**GÖRÜNTÜLÜ GÖRÜŞME****25 DAKİKA****İÇİNDE İZOLASYON****0****VERİ KAYBI****KİMLİK DOĞRULAMA, İŞE ALIMLA BİTMEZ.**

Uzaktan işe alımda kimlik, teslimat adresi ve çalışma konumunu birlikte kontrol edin. Yeni çalışanlara ilk günden tam yetki vermeyin. İlk bağlantıları güvenlik ekibiyle izleyin.

Senaryo, gerçek vakadan uyarlanmıştır. Birebir kayıt değildir.

Kaynak: KnowBe4

SPARTA SİBER GÜVENLİK

HESAP GERÇEK, TALİMAT SAHTE

Adres doğruydu. Mesaj gerçekten kurum hesabından gönderilmişti. Ancak mesajı hesabın sahibi değil, siber suçlular yazmıştı.

Çalışma arkadaşınızın kurumsal hesabı

Pakistan sağlık merkezleri – güneş paneli ödemesi

Ekli sipariş ve fatura belgeleri tamamlandı. **997.400 dolarlık** ödemenin Japonya'daki tedarikçiye aktarılması gerekiyor.

İşlemi **bugün** tamamlayıp dekontu bu zincirden paylaşır mısınız?

Gönderen adresi doğruysa hangi kontrol gerçekten işe yarar?

- A. Ekleri kurumun kullandığı belge formatlarıyla karşılaştırmak.
- B. Talebi kayıtlı numaradan arayarak ve ödeme kaydı üzerinden doğrulamak.
- C. Aynı e-posta zincirinden gönderene yeniden sormak.

DOĞRU CEVAP: B

Siber suçlular gerçek hesaba eriştiğinde e-posta adresi, imza, geçmiş yazışmalar ve aynı zincirde verilen yanıtlar güvenilir kanıt olmaktan çıkar. Böyle bir talepte ilgili kişiyi kayıtlı numarasından arayın.

GERÇEK VAKA: ÇALIŞANIN HESABINDAN 997.400 DOLARLIK TALİMAT

2017'de Save the Children USA çalışanlarından birinin e-posta hesabı ele geçirildi. Siber suçlular çalışan gibi davranarak sahte faturalar ve destekleyici belgeler hazırladı.

Belgelerde, Pakistan'daki sağlık merkezleri için güneş panelleri satın alınacağı yazıyordu. Kuruluş, bu talimata dayanarak Japonya'daki sahte bir kuruluşa 997.400 dolar gönderdi.

Dolandırıcılık fark edildiğinde transferi geri çağırmak için geç kalınmıştı. Kuruluşun sigortası 885.784 doları karşıladı. Save the Children güvenlik kontrollerini güçlendirdiğini açıkladı.

ÇALIŞANIN HESABI
ELE GEÇİRİLDİ

→ SAHTE FATURA VE
BELGELER
HAZIRLANDI

→ 997.400 DOLAR
GÖNDERİLDİ

→ DOLANDIRICILIK
SONRADAN FARK
EDİLDİ

997.400 DOLAR
AKTARILAN TUTAR

885.784 DOLAR
SİGORTANIN KARŞILADIĞI
TUTAR

111.616 DOLAR
KALAN KAYIP

DOĞRU HESAP, DOĞRU KİŞİ DEMEK DEĞİLDİR.

Mesaj doğru hesaptan gelse bile ödeme, hesap veya erişim talebini bağımsız bir kanaldan doğrulayın. Aynı e-posta zincirindeki yanıtı doğrulama saymayın.

E-posta örneği, gerçek vakadan uyarlanmıştır. Birebir mesaj metni değildir.

Kaynak: The Boston Globe ve BleepingComputer

SPARTA SİBER GÜVENLİK

BİLGİ İŞLEM SİZDEN BUNU İSTER Mİ?

Parola siber suçlulardaydı. Erişim için eksik olan yalnızca bir onaydı.

BİLGİ İŞLEM DESTEK

VPN hesabınızda doğrulama hatası görüyoruz.

Telefonunuza **birkaç onay bildirimi** gelebilir. **Onaylayın**, bağlantınızı düzelteceğiz.

Peş peşe MFA bildirimi alırken "Bilgi İşlem"den bu mesaj gelirse ne yaparsınız?

- A. Bildirimleri reddeder ve kayıtlı destek kanalından olayı bildiririm.
- B. Gönderen çalışan bilgilerimi biliyorsa son bildirimi onaylarım.
- C. Sorunu çözmek için gelen bildirimlerden yalnızca birini onaylarım.

DOĞRU CEVAP: A

MFA bildirimi yalnızca sizin başlattığınız girişim için onaylanır. Siber suçlular parolayı biliyor olsa bile ikinci adımı geçmek için onayınıza ihtiyaç duyar. Beklenmeyen her bildirim reddedilmeli ve kurumun kayıtlı destek kanalına bildirilmelidir.

GERÇEK VAKA: UBER'DE TEK ONAYLA AÇILAN ERİŞİM

Eylül 2022'de siber suçlular, Uber için çalışan harici bir yüklenicinin kurumsal parolasını ele geçirdi. Uber'e göre parola, yüklenicinin kişisel cihazına bulaşan zararlı yazılımın ardından karanlık ağda satışa çıkarılmış olabilir.

Siber suçlular yüklenicinin hesabına tekrar tekrar giriş yapmayı denedi. Yüklenici her denemede iki faktörlü doğrulama bildirimi aldı ve başlangıçta talepleri reddetti.

WIRED'in aktardığına göre siber suçlular, WhatsApp üzerinden bilgi işlem görevlisi gibi davranarak yükleniciyi bildirimlerden birini onaylamaya ikna etti. Bu onayın ardından Uber'in iç sistemlerine erişildi.

Siber suçlular başka çalışan hesaplarına, G-Suite ve Slack dahil çeşitli iç araçlara erişti. Uber, üretim sistemlerine, müşteri hesaplarına veya hassas kullanıcı verilerini tutan veri tabanlarına erişildiğine dair kanıt bulmadığını açıkladı.

PAROLA ELE
GEÇİRİLDİ

→ MFA BİLDİRİMLERİ
PEŞ PEŞE
GÖNDERİLDİ

→ SAHTE BİLGİ İŞLEM
MESAJI GELDİ

→ TEK ONAYLA İÇ
ARAÇLARA ERİŞİLDİ

NEDEN PEŞ PEŞE GELDİ?

Amaç, bildirimlerin bir sistem hatasından kaynaklandığını düşündürmek ve kullanıcının sonunda birini onaylamasını sağlamaktır. Bu yöntem "MFA yorgunluğu" olarak bilinir.

SİZ BAŞLATMADIYSANIZ ONAYLAMAYIN.

Beklemediğiniz MFA bildirimlerini reddedin. Mesajdaki numaraya veya hesaba dönmeyin. Olayı kurumunuzun kayıtlı destek kanalından bildirin ve parolanızı güvenli bir cihazdan değiştirin.

Destek mesajı, gerçek vakadan uyarlanmıştır. Birebir mesaj metni değildir.

Kaynak: Uber ve WIRED

SPARTA SİBER GÜVENLİK

HANGİSİ GERÇEK PROFİL?

Gerçek fotoğraflar ve kopyalanmış bilgilerle uzun süre kullanılan sahte bir kimlik oluşturuldu.



PROFİL A

Temsili profil

- 500'den fazla bağlantı
- Birkaç yıllık hesap geçmişi
- Birden fazla sosyal medya hesabı
- Ayrıntılı eğitim ve iş bilgileri



PROFİL B

Temsili profil

- 186 bağlantı
- Dört ortak bağlantı
- Düzenli paylaşımlar
- Şirket ve görev bilgileri

Hangisine güvenirsiniz?

- Geçmişi daha dolu görünen Profil A'ya
- Ortak bağlantısı bulunan Profil B'ye
- Kimliği doğrulanmadan ikisine de güvenmem

DOĞRU CEVAP: C

Bir profilin eski, ayrıntılı veya tutarlı görünmesi kimliği doğrulamaz. Ortak bağlantılar da hesabın sahibini gerçekten tanımıyor olabilir. Dosya açmanızı, bağlantıya tıklamanızı veya iş bilgisayarında bir işlem yapmanızı isteyen kişiyi kurumun resmi kanallarından kontrol edin.

GERÇEK VAKA: BİR YILDAN UZUN SÜREN SAHTE KİMLİK

SecureWorks araştırmacıları 2017'de "Mia Ash" adıyla kullanılan sahte bir kimliği ortaya çıkardı. Profil, LinkedIn, Facebook, Blogger ve WhatsApp üzerinde destekleniyor ve uzun süredir kullanılıyormuş gibi görünüyordu.

Fotoğraflar gerçek bir fotoğrafçıdan alınmıştı. İş tanımı başka bir kişinin LinkedIn profilinden kopyalanmıştı. Çok sayıda bağlantı ve farklı platformlardaki tutarlı hesaplar, oluşturulan kimliği inandırıcı gösteriyordu.

Sahte profil, Ocak 2017'de hedef alınan bir kurumun çalışanıyla LinkedIn üzerinden iletişim kurdu. Konuşma daha sonra Facebook, WhatsApp ve e-postaya taşındı. Yaklaşık bir ay sonra çalışana bir fotoğrafçılık anketi olduğu söylenen Excel dosyası gönderildi ve dosyayı iş bilgisayarında açması istendi.

Dosyadaki makro, bilgisayara uzaktan erişim sağlayabilecek PupyRAT adlı zararlı yazılımı indirmeye çalıştı. Kurumun güvenlik kontrolleri kurulumu engelledi.

PROFİL HAZIRLANDI

Çalınmış fotoğraflar ve kopyalanmış bilgiler kullanıldı.



GÜVEN KURULDU

Haftalar boyunca farklı platformlarda konuşuldu.



İSTEK

NORMALLEŞTİRİLDİ

Fotoğrafçılık anketi gibi görünen bir dosya gönderildi.



KURUMSAL CİHAZ

HEDEFLENDİ

Dosyanın özellikle iş bilgisayarında açılması istendi.

PROFİLİ DEĞİL, KİMLİĞİ DOĞRULAYIN.

Bağlantı sayısı, ortak kişiler ve eski paylaşımlar kimlik kanıtı değildir.

Profil örnekleri eğitim amacıyla hazırlanmıştır. Gerçek kişileri veya gerçek sosyal medya hesaplarını temsil etmez.

Kaynak: Sophos/SecureWorks ve WIRED

SPARTA SİBER GÜVENLİK

ARKADAŞINIZ MI, HESABINI ELE GEÇİREN BİRİ Mİ?

Mesaj gerçek hesaptan geldiği için para talebi sorgulanmadı.

MESAJ

Merhaba, çok acil bir ödeme yapmam gerekiyor. Bankacılığa giremiyorum. 7.500 TL gönderebilir misin? Akşama geri yollarım.

Gönderen: Kayıtlı bir arkadaşınız

Mesaj arkadaşınızın kayıtlı hesabından geldiyse ilk ne yaparsınız?

- A. Önceki konuşmalarla uyumluysa parayı gönderirim
- B. Arkadaşımı bildiğim başka bir kanaldan ararım
- C. Hesap sahibinin adını kontrol edip ödemeyi yaparım

DOĞRU CEVAP: B

Profil fotoğrafı, ad ve kayıtlı numara gerçek kişiye ait olabilir. Ancak hesabı kullanan kişi değişmiş olabilir. Aynı sohbet içinde yanıt vermek kimliği doğrulamaz. Para, kod veya bilgi talebini bildiğiniz başka bir iletişim kanalından doğrulayın.

GERÇEK VAKA: KARDEŞİNİN HESABINDAN GELEN MESAJ

Surrey Police'in Eylül 2025'te yayımladığı dolandırıcılık bülteninde, Sussex'te yaşanan gerçek bir olaya yer verildi.

Bir kişi, kardeşinin WhatsApp hesabından gelen para talebine güvendi. Talebi başka bir kanaldan doğrulamadan yaklaşık 500 sterlin gönderdi. Daha sonra kardeşinin WhatsApp hesabının ele geçirildiği ortaya çıktı.

Para, bir kod kullanılarak Afrika'daki bir alıcıya gönderilmişti. Mesaj yabancı bir hesaptan değil, mağdurun kardeşine ait gerçek WhatsApp hesabından gelmişti.

HESAP ELE GEÇİRİLDİ

Kardeşine ait WhatsApp hesabının kontrolü siber suçlulara geçti.

→ PARA İSTENDİ

Ele geçirilen hesaptan tanıdık kişilere mesaj gönderildi.

→ TALEP**DOĞRULANMADI**

Hesabın gerçek sahibine başka bir kanaldan ulaşılmadı.

→ YAKLAŞIK 500**STERLİN GİTTİ**

Dolandırıcılık para gönderildikten sonra anlaşıldı.

TANIDIK HESAP, GÜVENLİ TALEP DEMEK DEĞİLDİR.

Para, kod veya bilgi isteniyorsa kişiyi başka bir kanaldan doğrulayın.

Mesaj örneği eğitim amacıyla hazırlanmıştır. Gerçek vakadaki mesajın birebir metni değildir.

Kaynak: Surrey Police

SPARTA SİBER GÜVENLİK

ARAYAN GERÇEKTEN YÖNETİCİNİZ Mİ?

Numara farklıydı. Ses aynıydı. Doğrulama sorusu oyunu bozdu.

ARAYAN: GENEL MÜDÜR



Planladığımız satın alma için yardımına ihtiyacım var. Farklı bir numaradan arıyorum çünkü konu gizli. Birazdan hukuk ekibinden bilgi gelecek.

Ses, yöneticinizin sesine tamamen benziyor.

Böyle bir aramada ilk ne yaparsınız?

- A. Görüşmeyi kapatıp kayıtlı numaradan geri ararım
- B. Ses tanıdıksa işlemin ayrıntılarını dinlerim
- C. Talep yazılı gelirse işleme devam ederim

DOĞRU CEVAP: A

Tanıdık bir ses, arayan kişinin kimliğini kanıtlamaz. Ses kayıtlarından yöneticilerin sesleri taklit edilebilir. Beklenmedik bir para, bilgi veya işlem talebinde görüşmeyi sonlandırın ve yöneticiyi kayıtlı iletişim bilgilerinden geri arayın.

GERÇEK VAKA: FERRARİ'DE ARAMAYI BİTİREN SORU

Temmuz 2024'te bir Ferrari yöneticisi, şirketin CEO'su Benedetto Vigna'dan geliyormuş gibi görünen beklenmedik WhatsApp mesajları aldı.

Mesajlar Vigna'nın kullandığı iş numarasından gelmiyordu. Profil fotoğrafı da farklıydı. Buna rağmen kullanılan fotoğraf ve mesajlardaki gizli satın alma hikâyesi inandırıcı görünüyordu.

Ardından yönetici telefonla arandı. Arayan kişinin sesi, Vigna'nın sesini ve Güney İtalya aksanını oldukça başarılı biçimde taklit ediyordu. Görüşmede gizli bir satın alma işleminden ve Çin bağlantılı sorunlardan söz edildi.

Ferrari yöneticisi sestten şüphelendi. Arayan kişiye, Vigna'nın birkaç gün önce kendisine önerdiği kitabın adını sordu. Siber suçlular bu soruyu yanıtlayamadı ve görüşme aniden sona erdi. Ferrari herhangi bir kayıp yaşamadı.

FARKLI NUMARA

Mesajlar CEO'nun kayıtlı iş numarasından gelmedi.

→ TANIDIK SES

CEO'nun sesi ve aksanı yapay olarak taklit edildi.

→ GİZLİ İŞLEM

Satın alma hikâyesiyle gizlilik ve yetki algısı oluşturuldu.

→ KİŞİSEL SORU

Arayan cevap veremedi ve görüşmeyi sonlandırdı.

SESE DEĞİL, DOĞRULAMA KANALINA GÜVENİN.

Beklenmedik bir talepte görüşmeyi kapatın ve kayıtlı numaradan geri arayın.

Görüşme örneği eğitim amacıyla hazırlanmıştır. Gerçek konuşmanın birebir metni değildir.

Kaynak: Bloomberg/Moneyweb ve WIRED

SPARTA SİBER GÜVENLİK

DOLANDIRICININ BASTIĞI DÖRT DÜĞME

CEO, tedarikçi ya da arkadaş fark etmiyor. Acele etmemiz ve kimseye sormamamız isteniyor.

Dolandırıcılık mesajları her zaman kusursuz değildir. Yine de tanıdık bir isim, gizli bir konu ve zaman baskısı bir araya geldiğinde düşünmeden hareket edebiliriz.

1. YETKİ

Üst düzey bir yöneticinin adı, talimata ağırlık kazandırır.

2. GİZLİLİK

'Kimseye söylemeyin' denildiğinde sizi uyarabilecek kişiler devreden çıkar.

3. ACİLİYET

'Bugün' ve 'hemen' baskısı düşünmek için ayıracağınız süreyi kısaltır.

4. GÜVEN

Gerçek isimler, belgeler ve iş süreçleri şüpheyi azaltır.

GERÇEK VAKA: PATHÉ'DE 19,2 MİLYON AVROLUK ZİNCİR

8 Mart 2018'de Pathé'nin Hollanda yönetimine, şirketin Fransız ana merkezindeki CEO'dan geliyormuş gibi görünen bir e-posta ulaştı. Mesajda önce bir KPMG yetkilisinin kendileriyle iletişime geçip geçmediği soruldu.

Ardından Dubai'de yapılacak gizli bir şirket satın alımı için ödeme istendi. Talimatın hemen yerine getirilmesi ve işlemin kesinlikle gizli tutulması söylendi. Siber suçlular, gerçekten KPMG'de çalışan bir kişinin adını kullandı. İmzalı faturalar ve kurumsal görünen belgeler de gönderildi.

İlk olarak 826.521 avro ödendi. Sonraki günlerde yeni faturalar ve ek ödeme talepleri geldi. 9-27 Mart arasında yapılan transferlerin toplamı 19.244.304 avroya ulaştı. Fransa'daki merkez, şirketin nakit havuzundan çekilen paraları sorunca dolandırıcılık ortaya çıktı.

İLK TALEP

826.521 AVRO

TOPLAM

19.244.304 AVRO

BASKI HİSSETTİĞİNİZ ANDA İŞLEMİ DURDURUN.

Bir talepte yetki, gizlilik veya acele baskısı varsa durun. İlgili kişiye kendi kayıtlarınızdaki numaradan ulaşın.

Kaynak: Amsterdam Mahkemesi ve NOS

SPARTA SİBER GÜVENLİK

BU TALEBİ NASIL DOĞRULARSINIZ?

Teyit için mesajdaki numarayı değil, kendi kayıtlarınızdaki numarayı kullanın.

Mesaj, ses veya görüntü ne kadar gerçek görünürse görünsün, beklemediğiniz bir ödeme, belge veya hesap işlemini teyit etmeden yapmayın.

- 1. DURUN** Bir şey göndermeden veya işlem başlatmadan önce talebi beklemeye alın.
- 2. MESAJDAN ÇIKIN** Yanıt vermek yerine konuşmayı kapatın. Mesajdaki bağlantıyı veya telefon numarasını kullanmayın.
- 3. NUMARAYI KENDİNİZ BULUN** İlgili kişiye kurum rehberindeki, sözleşmedeki veya daha önce kaydettiğiniz numaradan ulaşın.
- 4. SORUYU AÇIKÇA SORUN** "Bu ödemeyi siz mi istediniz?" diye sorun. Alıcıyı, tutarı ve hesap değişikliğini ayrıca teyit edin.
- 5. İKİNCİ ONAYI ALIN** Ödeme, hesap değişikliği veya erişim talebini ikinci bir yetkilinin onayı olmadan tamamlamayın.

GERÇEK VAKA: MATTTEL'DE DOLANDIRICILIĞI ORTAYA ÇIKARAN KONUŞMA

30 Nisan 2015'te Mattel'in bir finans yöneticisine, şirketin yeni CEO'sundan geliyormuş gibi görünen bir e-posta ulaştı. Mesajda Çin'deki yeni bir tedarikçiye 3 milyon dolar gönderilmesi isteniyordu.

Mattel'de transfer için iki üst düzey yöneticinin onayı gerekiyordu. Talep CEO'dan gelmiş gibi görüldüğü için finans yöneticisi, kendi onayıyla birlikte iki onayın da tamamlandığını düşündü ve transferi gerçekleştirdi.

Aynı gün finans yöneticisi ödemedi CEO'ya söz etti. CEO böyle bir talimat vermediğini söyledi. Şirket bankasıyla, FBI'la ve Çinli yetkililerle hemen iletişime geçti. Çin'de 1 Mayıs nedeniyle bankaların kapalı olması zaman kazandı. Alıcı hesap donduruldu ve 3 milyon dolar geri alındı.

Bu konuşma transferden önce yapılsaydı para şirketten hiç çıkmayacaktı.

İŞLEMİ YAPTIYSANIZ BEKLEMİYİN

Bankanızı ve kurumunuzdaki güvenlik veya bilgi işlem ekibini hemen bilgilendirin. Mesajları, arama kayıtlarını ve ödeme bilgilerini silmeyin.

TALEBİN GELDİĞİ KANAL, DOĞRULAMA KANALI DEĞİLDİR.

Mesajı kapatın. Kayıtlı numarayı kendiniz bulun. Soruyu doğrudan sorun.

Kaynak: Atlanta Fed / FRASER ve IRMI