Çalışanlar için el kitabı: Kimlik avı Dolandırıcılığına aldanmayın

ESET
Digital Security
Progress. Protected.

Bir kimlik avı dolandırıcılığını alt etmeye hazır mısınız?

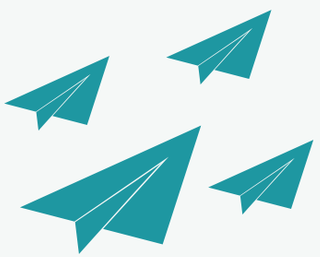
Teknoloji dijital güvenlikte önemli bir rol oynasa da, insan unsuru kritik bir faktör olmaya devam ediyor. 2022'deki ihlallerin %74 gibi şaşırtıcı bir oranı, saflık, korku ya da dikkatsizlikten kaynaklanan bir tür insan hatası içeriyor. Genellikle sosyal mühendislik saldırıları olarak bilinen bu sinsi siber tehditler, insanların zayıf noktalarından faydalanarak kurbanları, farkında olmadan bilgisayar korsanlarının sistemlerine sızması için kapıyı açmaya ikna ediyor.

Sosyal mühendislik tekniklerinin aldatıcı doğasını çözerek ve nasıl işlediklerini anlayarak, sizi bu kötü niyetli taktiklerle karşılaştığınızda güvenle yol almanız için gerekli bilgi ve araçlarla donatmayı amaçlıyoruz. Birlikte, kimlik avı saldırılarına karşı ortak savunmamızı güçlendireceğiz ve dijital güvenlik için devam eden savaşta dirençli bir cephe.

Kimlik avı ile nerede karşılaşabilirsiniz?

E-postada

PHISHING



Kimlik avı e-postaları, saldırganların sizi kandırarak parolalar, kredi kartı bilgileri veya kişisel kimlik bilgileri gibi hassas bilgileri ifşa etmeye çalıştığı en üretken siber suç tekniklerinden biri olmaya devam etmektedir. Genellikle kötü niyetli ekler veya meşru web sitelerini taklit eden bağlantılar aracılığıyla çalışırlar.

Kısa mesajda

SMISHING

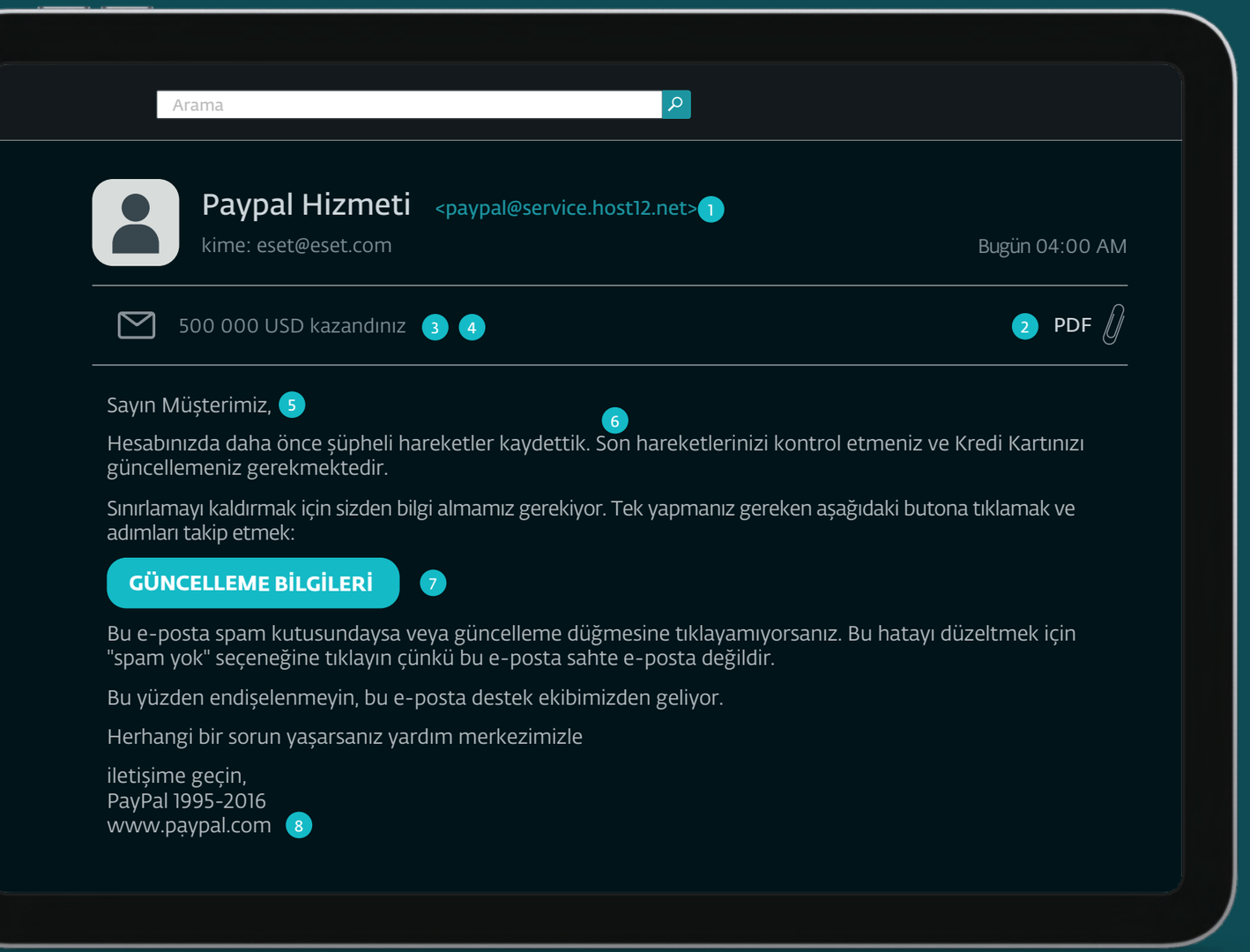
Kimlik avı mesajlarının SMS yoluyla da iletilebileceğinin farkında olmak önemlidir. Bu mesajlar genellikle sizi kötü amaçlı web sitelerine, giriş sayfalarına veya uygulamalara yönlendiren bağlantılar içerir. Erişildiğinde, bu kanallar cihazınıza kötü amaçlı yazılım bulaştırabilir ve hassas verilerinizi almak için kullanabilir.

Telefon görüşmesinde

VISHING

Dolandırıcılar ayrıca hassas bilgileri ifşa etmeniz veya hileli ödemeler yapmanız için sizi kandırmak amacıyla telefon aramalarını veya sesli mesajları da kullanabilir.
Bu saldırıların karmaşıklığı, otomatik robot aramalar üzerinden insan taklidi yapanlardan tanıdığınız bir kişinin derin taklitlerine kadar uzanmaktadır. Hatta bazı dolandırıcılar bu aldatmacayı geliştirmek için yasal telefon numaralarını kullanarak çağrı yanıltma yöntemini kullanır.

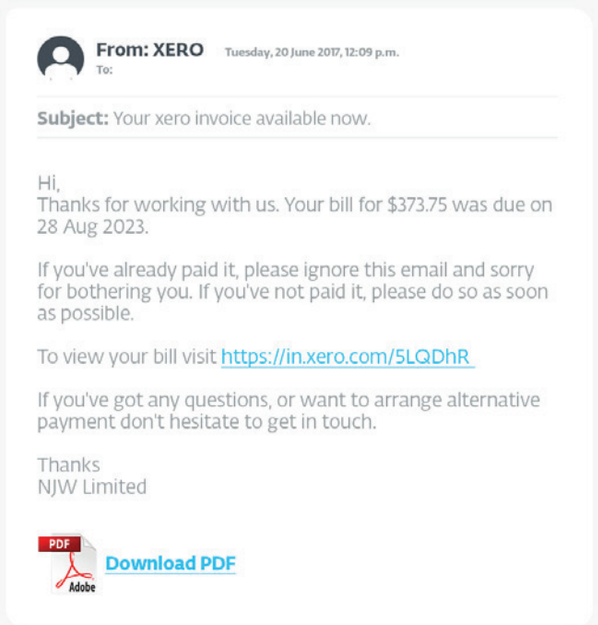
Kimlik avı e-postası nasıl anlaşılır? Bu özelliklere bakın:



1. E-posta adresine aşina değilseniz, içeriği dikkatli bir şekilde ele alın.
2. Ekli dosyalardan veya bilmediğiniz bağlantılardan en kötüsünü bekleyin. Bunlar kötü amaçlı yazılım içerebilir veya sizi kötü amaçlı bir web hedefine gönderebilir.
3. Çok mu korkutucu ya da gerçek olamayacak kadar iyi? Muhtemelen bir dolandırıcılıktır. Sosyal mühendisliğin insan zayıflıklarına odaklandığını unutmayın.
4. Konu mesajdan farklıdır.
5. Eğer selamlama çok genelse, bu sadece size değil, başka kişilere de hitap edildiğinin bir işareti olabilir.
6. Şüpheli aciliyet mi? Dolandırıcı panik yapmanızı istiyor.
7. Kötü yazım ve diğer dilbilgisi hataları, başka dillerden çevrilmiş oltalama postalarında yaygındır.
8. Homoglif saldırıları, adreslerdeki karakterleri benzer görünen ancak farklı alfabelere ait olanlarla değiştirmeye dayanır (paypal.com'daki "a" yerine "ạ" gibi).

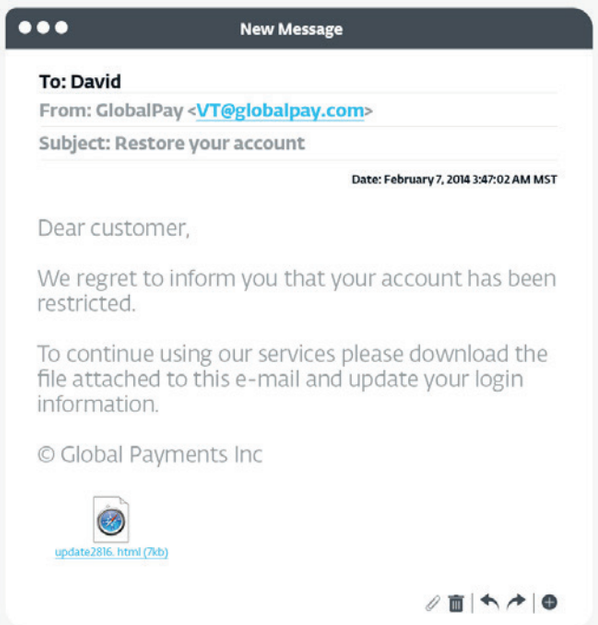
Yaygın kimlik avı planları

ÖDEME TALEPLERİ



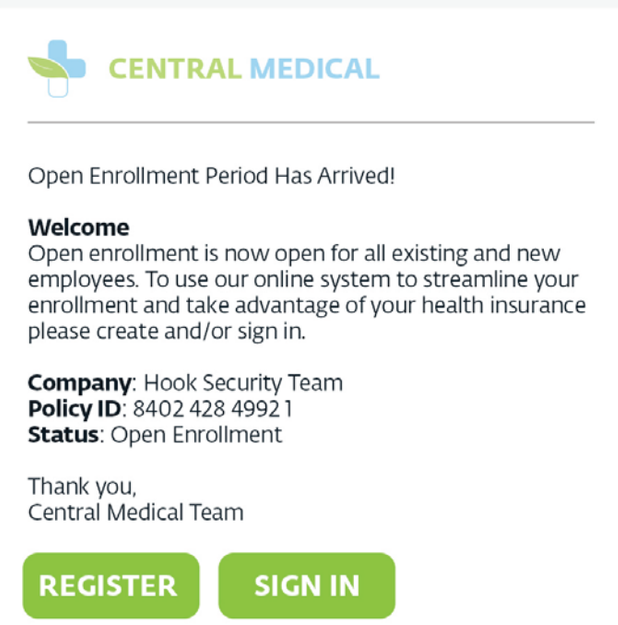
Dolandırıcılar örneğin devlet kurumu temsilcisi gibi davranarak ödeme yapılmaması halinde para cezası veya tutuklama tehdidinde bulunurlar. Diğer örnekler arasında saldırganın şirketin CEO'su gibi davranarak çalışanlardan birinden hızlı ödeme istemesi veya tedarikçilerin çalışanlarla iletişime geçerek paketler ve mallar için tazminat talep etmesi sayılabilir.

HESAP DOĞRULAMA



Dolandırıcılar, diğer finansal kurumların yanı sıra, Netflix gibi eğlence platformlarını veya kullanıcıların kişisel profillerinin bulunduğu dijital mağazaları taklit etmektedir. Hesapta olağandışı faaliyetler olduğunu iddia ediyor, kullanıcıları sahte web sitelerine yönlendiriyor ve doğrulama amacıyla giriş bilgilerini talep ediyorlar.

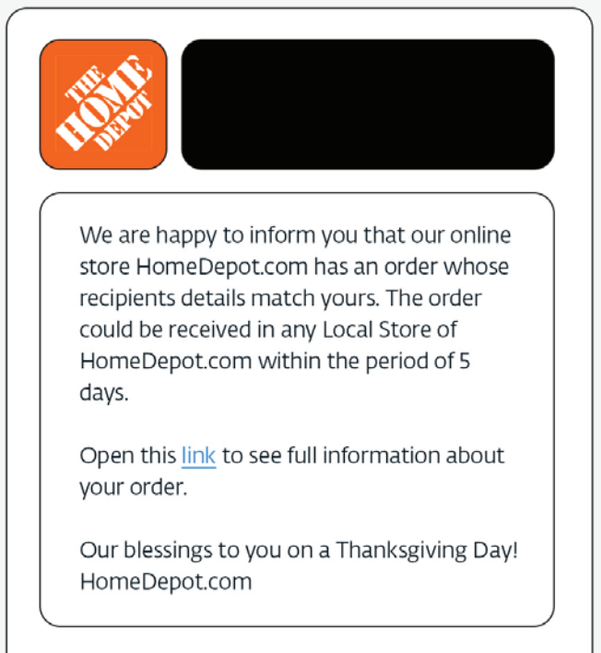
PROGRAM KAYITLARI



Dolandırıcılar, devlet programı temsilcileri gibi davranarak, kişisel ve finansal verileri toplarken kayıt konusunda yardım teklif ederler. Bu, web seminerlerine ve diğer etkinliklere davet içeren sahte e-postaları içerebilir; burada kullanıcılar aşağıdakilerle hesap oluşturur bir şifre. Bu, öncelikle kişinin farklı hesaplar için aynı şifreyi kullanması durumunda bir sorundur çünkü dolandırıcıya onları kaçırmak için serbest bir geçiş.

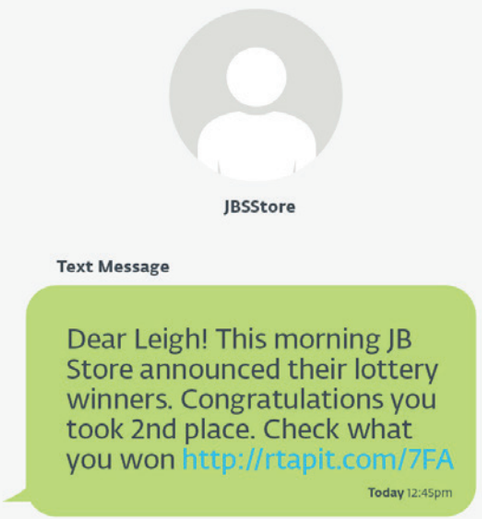
Yaygın kimlik avı planları

SİPARİŞ/NAKLİYE ONAYI



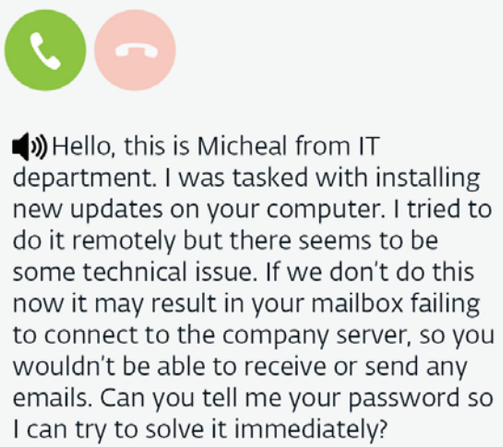
Mağdurlar, var olmayan paketleri izlemek veya siparişleri onaylamak için sahte bağlantılar alır ve bu da oturum açma kimlik bilgilerinin alınmasına veya kötü amaçlı yazılım yüklenmesine yol açar. Bu daha sonra aynı oturum açma bilgileriyle diğer web sitelerine sızmak için kullanılabilir. Tıklamamak çok önemlidir Şüpheli bağlantılar ve gelen e-postalarda dolandırıcılık belirtileri olup olmadığını kontrol etmek.

ÖDÜL KAZANMAK



Dolandırıcılar, bireyleri bir yarışma zaferi hakkında bilgilendirir ve ardından kişisel bilgilerini veya banka hesaplarına erişim talep eder. Daha sonra hesaplardan kişisel veriler çekilebilir ve potansiyel olarak önemli mali hasara neden olabilir. Herhangi bir yarışma zaferini resmi organizatör aracılığıyla doğrulamak çok önemlidir.

TEKNİK DESTEK



Dolandırıcılar kendilerini BT desteği olarak tanıtır ve bilgisayarlarındaki bir şeyi uzaktan düzeltmeleri veya güncellemeleri gerektiğini iddia ederek kullanıcılardan erişim kimlik bilgilerini vermelerini ister. Bu, dolandırıcıların kişisel verilere ve hassas bilgilere erişim sağlamasına olanak tanır. BT veya İK departmanlarının genellikle çalışanlardan telefon veya e-posta yoluyla özel bilgilerini paylaşmalarını istemediğini unutmamak önemlidir.

Şüpheli bir mesaj veya arama alırsanız nasıl tepki vermelisiniz?

1

DURUN, DÜŞÜNÜN VE HAREKETE GEÇİN

Dolandırıcılar kurbanları manipüle etmek için aciliyete güvenirler. Talepleri değerlendirmek için zaman ayırın ve aceleci davranmaktan kaçının. Kısa mesajlardaki bağlantılara tıklamaktan kaçının ve iletişimin meşruiyetini doğrulamak için kuruluşun resmi web sitesini ziyaret edin

2

BİLİNMEYEN NUMARALARDAN ŞÜPHELENİN

Tanıdık olmayan veya şüpheli numaralardan gelen aramaları veya kısa mesajları doğrulayın. Herhangi bir kişisel bilgiyi ifşa etmekten kaçının veya mesajlar içindeki bilinmeyen bağlantılara tıklamak. Bu, bu tür dolandırıcılıkların kurbanı olma olasılığınızı en aza indirmenize yardımcı olur.

3

DOLANDIRICILARLA İLETİŞİME GEÇMEYİN

Dolandırıcılar kurbanlarını istismar etmek için duygusal manipülasyon kullanırlar, bu nedenle onlarla etkileşime girmek, planlarına kanma riskinizi artırır. Bazı durumlarda, dolandırıcılar onlarla etkileşime girmeye istekli olduğunuzu hissederlerse daha agresif veya ısrarcı olabilirler. Ayrıca onlara verdiğiniz her türlü bilgiyi size karşı kullanacaklardır.
Genel olarak, dolandırıcılarla konuşmak yorucu, tehlikeli ve tamamen etkisizdir.

4

KİMLİK DOĞRULAMA

Bir şirketi veya devlet kurumunu temsil ettiğini iddia eden birinden mesaj alırsanız, doğrudan etkileşime girmekten kaçının. Bunun yerine, web sitelerinde bulunan resmi iletişim bilgilerini kullanarak kuruluşla iletişime geçerek gerçekliğini bağımsız olarak doğrulayın.

5

GÜÇLÜ GÜVENLİK ÖNLEMLERİNİ ETKİNLEŞTİRİN

Hesaplarınızı korumak için güçlü ve benzersiz parolalar kullanın. Uzun ve karmaşık parolalar oluşturmak için parola oluşturucuları ve yöneticilerini kullanmayı düşünün veya parolalar kullanın ve bunları güvenli bir şekilde saklayın. Ekstra bir koruma katmanı eklemek için mümkün olduğunda Çok Faktörlü Kimlik Doğrulama (MFA) kullanın.

Aldığınız mesajın tehlikeli olup olmadığından hala emin değil misiniz? İşte yapabilecekleriniz:

Şüpheli e-posta bir web sayfasına bağlantı içeriyorsa:
URL'yi görmek için bağlantının üzerine gelin. Adres e-postanın içeriği veya göndereni ile uyuşmuyorsa, üzerine tıklamayın. En ufak bir şüpheniz bile varsa, hiçbir bağlantıya tıklamayın. Unutmayın, bir bağlantıya tıklamadığınız veya bir eki açmadığınız sürece kimlik avı mesajı size zarar veremez.

Gönderenin adresi size tanıdık geliyorsa, ancak mesajın içeriği size mantıklı gelmiyorsa:
E-postanın gerçekliğini doğrulamak için yeni bir e-posta yoluyla gönderenle iletişime geçebilirsiniz.

Bir bulut hizmetinden gelen bir mesaja benziyorsa:
Çeşitli bulut hizmetleri sıklıkla kötüye kullanılmaktadır. Kimlik avcıları, kimlik avı web sitelerini Microsoft Azure veya OneDrive gibi meşru sunucularda barındırarak meşru alan adları sunabilir. Böyle bir e-postayı birkaç kez okuyun.

Kişisel bilgilerinizi girmeyi planladığınız tüm web adreslerinin başında "https" bulunmalıdır.
"S" harfi "güvenli" anlamına gelir. Eğer "https" görmüyorsanız, güvenli bir web oturumunda değilsiniz demektir ve herhangi bir kişisel bilgi girmemelisiniz. Ancak, "https" görüyorsanız, bu yine de dolandırılmadığınızın garantisi değildir.

Kimlik avı mesajları bariz dolandırıcılıklar olabileceği gibi oldukça karmaşık bir şekilde gizlenmiş de olabilir. Mesajın yasal olup olmadığından emin değilseniz (veya olmadığından eminseniz),
şirketinizin BT Güvenliğine veya diğer uygun yetkililere bildirmek her zaman iyi bir fikirdir.

Bu oyun kitabında yer alan içgörüler ve pratik ipuçlarıyla, kimlik avı girişimlerinin tehlikeli sularında dikkatli ve güvenle gezinmek için iyi hazırlanmış olacaksınız. Bu stratejileri benimseyip dijital uygulamalarınıza entegre ettiğinizde, kuruluşunuzun siber tehditlere karşı kolektif direncini güçlendirmede aktif bir katılımcı olacaksınız.

Digital Security
Progress. Protected.

Dijital Güvenlik Kılavuzu, küçük ve orta ölçekli işletmelerin etkili bir siber güvenlik altyapısı oluşturmalarına yardımcı olmak için bilgi birikimlerini ve deneyimlerini paylaşan ESET'in siber güvenlik uzmanları tarafından hazırlanıyor ve denetleniyor. Yüksek kaliteli dijital güvenlik çözümleri uygulayarak işinizi korumak, ilerlemenizi korumak anlamına gelir. ESET®, 30 yılı aşkın süredir dünya çapında işletmeleri, kritik altyapıları ve tüketicileri giderek karmaşıklaşan dijital tehditlere karşı korumak için sektör lideri BT güvenlik yazılımları ve hizmetleri geliştirmektedir. Daha fazla bilgi için www.antivirus.com.tr adresini ziyaret edin veya ESET'i LinkedIn, Facebook ve Twitter'da takip edin.