



1- İnternette Alışveriş Dolandırıcılığı Yöntemleri

Dolandırıcılar, aslında hiç var olmayan ya da kendilerine ait olmayan mal veya hizmetleri satmak için reklam yaparlar ya da gerçek bir şirket gibi görünebilmek için mevcut itibarlı markaların internet sitelerini taklit etmeye çalışırlar.

İnternette Alışveriş Dolandırıcılığı Nasıl Yapılır?

Dolandırıcılar tamamen gerçek görünen sahte alışveriş internet sitesi yaparlar ya da gerçek bir alışveriş sitesinin sahtesini hazırlarlar.

Sosyal medya üzerinden reklamlar vererek ilgili sahte internet sitelerine yönlendirme yapılabilirler.

Sahte internet siteleri üzerinden sattıkları ürünlerin fiyatını kampanyalarla cazip hale getirirler.

Dolandırıcılar, ödemelerinizi EFT ve havale gibi yöntemlerle doğrudan doğruya banka hesaplarına göndermenizi isteyebilirler. Bedelini ödediğiniz bu ürünleri siz ödeme yaptıktan sonra yayından kaldırıp izlerini tamamen yok ederler.

Dolandırıcılar kart bilgileriniz ile ödeme yapmanızı isteyebilir bu durumda kart bilgilerinizi ele geçirebilirler.

İnternette Alışveriş Dolandırıcılığından Nasıl Korunuruz?

- ✓ URL'sinin başında 'https' bulunmayan bir siteden asla hiçbir şey satın almayın – ve bir asma kilit ikonunu arayın. Bu, o internet sitesinin güvenli olduğunu gösterir.
- ✓ Ödeme sayfasında SSL sertifikası bulunmayan sitelerden hiçbir ürünü satın almayın. SSL sertifikası o internet sitesine girilen bilgilerin şifrelendiğini gösterir, sitede SSL sertifikası varsa adres çubuğunda firma ismi yeşil renkle belirtilerek yeşil renkte bir kilit görünür.
- ✓ Banka veya kredi kartı ile yapmış olduğunuz internet alışverişlerinizde sanal kart kullanabilir ya da ödemelerinizi 3D Secure/ GO Güvenli Öde seçenekleri ile yapın. Bu tedbirler sizin dijital olarak güvenliğinizi sağlayacaktır

Alışveriş yaptığınız internet sitesinin yasal ve gerçek olduğundan emin olunuz. Gerçek site adresine benzer ancak harf ya da rakamlar eklenerek oluşturulmuş taklit edilmiş sahte sitelere karşı dikkatli olunuz. Beklenmedik bir e-posta ile gelen hiçbir linke güvenmeyiniz.

Alışveriş yapmak istediğiniz site ile ilgili araştırma yapınız. Sitenin iletişim bilgilerini kontrol ederek ulaşılabilir olduklarından emin olunuz.

İnternette alışveriş yaparken dolandırıldığınızı düşünüyorsanız veya kart bilgilerinizi sahte site üzerinden paylaştığınızı düşünüyorsanız durumu hemen **Banka Müşteri İletişim Merkezine** bildirebilirsiniz



2- Sosyal Mühendislik Yöntemleriyle Dolandırıcılık

Bu yöntemde dolandırıcılar, sizden bilgi almak ya da istenilen işlemleri yapmasını sağlamak amacıyla taklit (polis, savcı, banka), etkileme (kampanya, chip puan, aidat iadesi) ve ikna etme kabiliyetleri kullanırlar.

Sosyal Mühendislik Dolandırıcılığı Nasıl Yapılır?

- ✓ Dolandırıcı, kendini kamu çalışanı olarak (polis, savcı, hâkim vb.) tanıtır ve size terör örgütü ile ilişkinizin olduğunu ya da banka hesabınızın terör örgütü tarafından kullanıldığını ve bunun gibi söylemlerle sizi korkutarak para transferi yapmak, kart şifrenizi tuşlatmak, kimlik bilgilerinizi vermek için ikna etmeye çalışır.
- ✓ Hesap bilgilerinizin, kimlik bilgilerinizin örgütün eline geçtiği veya SIM kartınızın kopyalanarak örgüt tarafından kullanıldığını söyleyerek ilettikleri hesaba para göndermenizi talep ederler. Taleplerini yerine getirinceye kadarki süreçte telefonu kapatmamanız için çeşitli zorlama ve korkutma yöntemlerini kullanırlar. Bazı durumlarda "uydu aracılığı ile tüm hareketlerinizi izlediklerini" veya "örtülü ödenekten hesabınıza para gönderildiğini" belirterek sizi ikna etmeye çalışırlar.
- ✓ "ÖDÜL KAZANDINIZ" (Örn: Forma, saat vb. para ödülü vb.) tarzında SMS mesajları göndererek ödül gönderimi için ön ödeme talep ederler.
- ✓ Banka çalışanı gibi sizi arayarak ücret, komisyon iadesi, faiz iptali, borç erteleme, aidat iptali vb. vaatlerle sizden kart bilgilerinizi (CVV, son kullanma tarihi, şifreniz) isteyebilir ve/veya telefona tuşlamanız için yönlendirebilirler.
- ✓ Bazı vakalarda daha önce dolandırdıkları müşterileri yeniden arayarak "kart itirazınız için aramıştık" diyerek ikinci kez dolandırıcılık girişiminde bulunmaktadırlar.
- ✓ COVID-19 salgınının gündemde olduğu bu günlerde dolandırıcılar banka temsilcisi, kamu görevlisi, Sağlık Bakanlığı yetkilisi vb. olduklarını iddia ederek, COVID-19 konulu gerekçelerle sizleri yanlış yönlendirmeye çalışabilir.

Sosyal Mühendislik Dolandırıcılığından Korunmak için Alacağınız Önlemler

- ✓ Unutmayın, üzerinizde baskı kurarak ya da cazip teklifler sunarak yapılan bu aramalar dolandırıcılıktır.
- ✓ Kamu görevlileri ve banka çalışanları kişisel bilgilerinizi ya da finansal bilgilerinizi isteyemez, para transferi yapmanızı talep edemez.
- ✓ Böyle bir durumla karşılaştığınızda arayan kişiye kesinlikle bilgi vermeyin ve telefonu hemen kapatın.

- ✓ Sizi arayan numaraya asla geri arama yapmayın.
- ✓ Bankalar tarafından yapılan aramalarda hiçbir zaman internet bankacılığı şifresi, SMS ile iletilen mobil onay kodu, kredi kartı şifresi, kimlik detayları gibi bilgiler talep edilmez.
- ✓ Şifreleriniz size özeldir, en yakınlarınız dahil kimseyle paylaşmamanız gerektiğini her zaman hatırlayın
- ✓ Ödül, faiz ücret iadesi, kart ücret iadesi veya farklı nedenlerle kartınız üzerinde yazan herhangi bir bilgiyi, kartınızın şifresini, Mobil veya İnternet bankacılığı bilgilerinizi, kendinize SMS ile gelen şifrelerinizi talep eden, tuşlanmasını isteyen,
- ✓ Hesabınıza yanlışlıkla ya da dolandırıcılık yoluyla para gönderildiğini ve bunu verilecek bir başka hesaba göndermenizi isteyen,
- ✓ E-posta üzerinden sizinle iş ortağıymış gibi irtibata geçerek daha öncekilerden farklı bir hesaba/IBAN'a transfer talimatı iletmenizi isteyen,
- ✓ Şüpheli işlemler nedeniyle hesaplarınızın güvence altına alınması gibi nedenler belirterek para transferi talebinde bulunan, şahıslara inanmayınız.
- ✓ Bu ve benzeri yöntemlerle bilgi ve menfaat talepleriyle karşılaşmanız durumunda, dolandırıcılık mağduru olmamak için sözkonusu taleplere itibar etmemeniz ve en yakın polis merkezine giderek müracaatta bulunmanız önem taşımaktadır.



Facebook, YouTube, Twitter, MySpace, WhatsApp, Messenger gibi çeşitli sosyal ağlar aracılığıyla kullanıcı ile iletişime geçilerek inandırıcı bir senaryoyla güvenlik açısından kritik olan kişisel ve finansal bilgilerin alınması yoluyla gerçekleştirilen, insan faktörüne dayanan dolandırıcılık türüdür.

Hangi Şekillerde Karşılaşılm?

Nasıl Çalışırlar?

Dolandırıcılar sosyal medya hesaplarını ele geçirerek kendilerini ilgili hesap sahibi gibi gösterebilirler. Hesaba girdikten sonra, gerçek hesap sahibinin arkadaşları ve ailesiyle irtibat kurabilirler ve onların dostluk ve yakınlık duygularından yararlanarak para, kredi kartı veya banka detaylarını paylaşma konusunda kandırabilirler. Bunun pek çok yolu olabilir.

Örneğin;

- ✓ Dolandırıcılar tanıdığınız bir kişinin ele geçirdikleri sosyal medya adresi üzerinden sizinle iletişime geçerek acil ve çok önemli bir sebeple paraya ihtiyaç olduğunu söyler.
- ✓ Kaza geçirdiğini ve hastane faturasını ödemek için paraya ihtiyacı olduğunu söyler.
- ✓ Sizden bu masraflar için bir hesaba para havale etmenizi ya da banka detaylarınızı paylaşmanızı ister.
- ✓ hediye çekilişi kampanyasına katılım,
- ✓ belirli hesaba para gönderimi,
- ✓ kredi puanınızı yetersiz belirterek adınıza kredi çekme için para gönderimi talebi, vb. çeşitli senaryolarla sizi etkileyip ikna ederek kişisel ve finansal bilgilerinizi (kart bilgisi, internet bankacılığı şifresi, SMS ile iletilen mobil onay kodu, tek kullanımlık cep anahtar şifresi vb.) isteyebilmektedir.

Sizden Ne İsterler?

Kopya hesap oluşturan dolandırıcılar genellikle bildirdikleri bir hesap numarasına para transferi yapmanızı isterler

Ne Yapılması Gerekilmektedir?

- ✓ Sosyal medya hesaplarında belirtilen bankaların internet site isimlerine dikkat edilmesi gerekir.
- ✓ Banka hesapları güvenli internet sitelerine sahip olup https olarak domain adresleri olması gerekir. Https olmayan banka sitelerine hiç bir şekilde giriş yapmayınız.
- ✓ Bankaların sosyal medya hesapları mavi tik işareti ile belirtilmektedir. İlgili sosyal medya hesabı aracılığı ve size yönlendirilen internet bankacılığı linki ile sizden kişisel bilgiler talep ediliyor ise, bu hesaplara güvenmeyiniz
- ✓ İnternet ortamında bir kişinin gerçekten arkadaşınız olup olmadığını anlamanız çok zordur. Bu nedenle arkadaş listenizde olsa bile kimseyle hesap bilgilerinizi, şifrelerinizi paylaşmayın, para transferi yapmayın.
- ✓ Sizden para talep edecek kadar yakın olan bir kişinin size sosyal medya hesabınızdan değil, yüz yüze iletişim kurabileceğiniz kanallardan ulaşacağını hep aklınızda tutun.
- ✓ Bütün sosyal medya hesaplarınızın “Gizlilik” ve “ Güvenlik” ayarlarını kontrol edin. Güvenliğiniz içi belirtilen bütün işlemleri yaptığınızdan emin olun. Kontrol işlemi belirli aralıklarla tekrar edin.
- ✓ Kendi rızanızla dolandırıcılara yapacağınız para transferlerinde aracı bankaların hiçbir sorumluluğu olmayacağını unutmayın.



'Phishing' Yöntemi

Kimlik, anne kızlık soyadı, şifre, parola, müşteri numarası, kredi kartı numarası ve benzeri kişisel veya kurumunuza ait bilgilerin elde edilmesine yönelik dolandırıcılık yöntemidir. Dolandırıcılar hedef aldıkları finansal kurumun internet sitesinin görünüşte aynısını oluştururlar. Son olarak da elde ettikleri e-posta adreslerine o finansal kurumdan geldiği izlenimini verdikleri bir e-posta mesajını gönderirler.

Bu tür e-posta mesajları genellikle bir sistem çalışması ya da benzeri bir yapısal değişiklik ya da belki bir sorundan dolayı kişisel bilgilerinizi girmeniz gerektiğini bildirirler. Bu e-posta mesajlarında yer alan link'leri tıkladığınızda hesabınızın bulunduğu kurumun sitesi yerine sahte siteye yönlendirilirsiniz.

Phishing (Oltalama Saldırıları) Dolandırıcılık Nasıl Yapılır?

Dolandırıcılar oltalama saldırılarında; internet aracılığıyla, finansal kurum ve kuruluşlar, resmi kurumlar veya alışveriş şirketlerinden gönderilmiş gibi görünen, acil ve çok önemli konular içeriyormuş izlenimi veren sahte e-postalar gönderirler.

E-postanın konusu, müşteri bilgilerinin güncellenmesi veya şifrelerin değiştirilmesi olabilir ve içinde ilgili kurumların sayfalarının birebir aynısı şeklinde görünen internet sayfalarına giden linkler yer alabilir.

Cep telefonunuza gelen bir SMS bildiriminin içinde yer alan link, sizi sahte internet bankacılığı sayfalarına yönlendirebilir.

Örneğin;

- ✓ Tanınmış bir kimseden veya bir şirketten gerçek görünen bir e-posta gelir.
- ✓ Bu e-posta sizden daha fazla bilgi almak veya para iadesi, kargo takibi, ödenmemiş fatura vb. işlemler için bir linke tıklamanızı ister.
- ✓ Sizden bir şey indirmeniz istenir. İndirmeniz istenen linkteki dosya, kendisini normal bir dosyaymış gibi gösteren kötü niyetli bir yazılımdır (malware).

- ✓ Bu yazılım ise bilgisayarınıza/telefonunuza yerleşerek dolandırıcıların sizin kişisel bilgilerinize, hesap detaylarınıza ve veya paranıza erişmesini sağlar.
- ✓ Son olarak acil, önemli gibi ibareler de kullanarak daha önce e-posta sahibi ile aranızda iş ilişkisinden kaynaklanan para trafiğini başka bir hesaba yönlendirmeye çalışır.

Tanımadığınız bir numaradan bir kısa mesaj mı geldi? Ya da sizden bir şey yapmanızı isteyen bir şirketten? Bu bir 'dolandırıcılık' kısa mesajı olabilir.

- ✓ Hiç beklemediğiniz bir kısa mesaj gelir.
- ✓ Bu mesaj bir internet sitesi linki içerir ve sizden o linke tıklamanızı ister.
- ✓ Linke tıkladığınızda ya da numarayı aradığınızda, Direkt İnternet şifreniz gibi kişisel bilgilerinizi vermeniz, tuşlamanız istenir.

E-Posta ve SMS ve Dolandırıcılarına Avlanmayın!

Nasıl Çalışırlar?

- ✓ Ortalama adını verdiğimiz bu yöntemde dolandırıcılar sosyal medya, e- posta ve kısa mesajlar aracılığı ile bankaların unvanlarını ve logolarını kullanarak sahte kampanya ve reklam linklerine tıklamanız için çalışırlar.
- ✓ "İnternet Bankacılık Süreniz Dolmuştur", "Bilgilerinizi Güncellemeniz İstenmektedir", "Hesaplarınızda Şüpheli İşlemler Tespit Edilmiştir", "Araba Çekilişine Katılmak İçin Tıklayın", "Kart Aidatınızı Geri Almak İçin Tıklayın" gibi mesajlar ve yönlendirmeler kullanırlar.
- ✓ Bu linklere tıklamanız durumunda sizi sahte banka hesaplarına yönlendirebilir, güvenliğiniz açısından kritik bilgileri paylaşmanıza neden olabilirler.
- ✓ Tıkladığınız linkler aracılığı ile siz bankanın internet sitesine girmiş olduğunuzu düşünebilirsiniz.

Sizden Ne İsterler?

Dolandırıcılar bu yöntemle kart bilgilerinizi, kimlik bilgilerinizi, internet/mobil bankacılık kullanıcı adı ve şifrenizi talep ederek finansal bilgilerinize ve hesaplarınıza ulaşabilirler.

Phishing metodu ile yapılan online sahtekarlıkta çalınan bilgiler:

- ✓ Kredi, Banka Kartı / ATM kart numaraları / CVV2
- ✓ Şifreler ve parolalar
- ✓ Hesap numaraları
- ✓ İnternet Bankacılığı'na girişte kullanılan kullanıcı kodu ve şifreleri

E-Posta ve SMS Dolandırıcıları İçin Alacağınız Önlemler

- ✓ Bu tür postalar, kısa mesajlar aldığınızda ya da kullandığınız sosyal medya hesaplarında bu tür reklamlar gördüğünüzde dikkatli olmalısınız.

- ✓ Dolandırıcılar açtıkları sahte hesaplarda ya da elektronik posta ve SMS aracılığı ile gönderdikleri linklerde banka adını küçük değişiklikler yaparak kullanırlar. Paylaşılan linklerde harf eksikliği, fazlası ya da hatası olup olmadığını kontrol etmeyi unutmayın.
- ✓ Bankalar, elektronik posta ya da SMS ile bilgi güncellemesi talep etmez, internet şubesi giriş sayfasına yönlendiren bir link paylaşımı yapmaz.
- ✓ Elektronik posta ve SMS aracılığı ile gelen mesajlarda bulunan linklere kesinlikle tıklamayın.
- ✓ Şüphe duyduğunuz bir durumla karşı karşıya kalırsanız Müşteri İletişim Merkezimizi arayarak bilgi verin.
- ✓ Banka adı ve görseli kullanılarak hazırlanan kişisel ve finansal (şifre, kart numarası vb.) bilgilerinizi isteyen e- postalara cevap vermeyiniz. Bu tür e-postalar aracılığıyla gönderilen linklerle İnternet Bankacılığına giriş yapmayınız.
- ✓ Ödenmemiş fatura, yüksek tutarlı borç bilgileri, hesap bilgilerinizin ele geçirildiği, acil, kargo takibi vb. konularda gönderilen e-postalara karşı dikkatli olunuz. Bu e-postalara genellikle çok kullanılan, tanınmış firmalardan geldiği izlenimi verilmektedir. Bu sahte e-postalarda içinde yer alan linki tıklamanız ya da dosyayı indirmeniz istenerek zararlı yazılımların telefonunuza / bilgisayarınıza yerleşmesi sağlanır. Dolandırıcılar böylelikle kişisel ve finansal bilgilerinize erişebilirler.
- ✓ Cazip kampanya, indirim kuponu, puan kazanımı vb. içerikli sms bildirimlerine karşı da dikkatli olunuz. Bu sms içeriklerinde yer alan linkler ile sahte internet bankacılığı sayfalarına yönlendirilebilirsiniz. Bu sayfalarda internet bankacılığı şifrelerinizi girmeniz için sizi yönlendirir.
- ✓ Kaynağından emin olmadığınız e-posta ve sms'lere karşı dikkatli olunuz.



Uzaktan erişim, dolandırıcıların size onlara erişim imkânı tanımanız için ikna ederek bilgisayarınızın kontrolünü ellerine geçirebildikleri bir yoldur.

Bunu uzak bir mesafeden de yapabilirler.

Peki, tüm bunlar sizin başınıza nasıl gelebilir?

- ✓ Beklenmedik bir anda telefonunuz çalar – arayan kişi bir teknik destek hizmeti sağlayıcısından, büyük bir telekomünikasyon veya bilgisayar şirketinden aradığını iddia eder.
- ✓ Bilgisayarınızda teknik problemler olduğunu ve bu problemi onarmak için bilgisayarınıza uzaktan erişimleri ve girmeleri gerektiğini söyler.
- ✓ Sizden bir yazılım satın almanızı ya da bilgisayarınızın onarımı için bir servis istasyonuna başvurmaınızı ister.
- ✓ Kişisel bilgilerinizi ve banka veya kredi kartı detaylarınızı sorar.
- ✓ Arayan kişi çok ısrarcı olabilir.

Bir an durun ve düşünün, Böyle bir telefon alırsanız, telefonu hemen kapatın.

Ne yapmalısınız?

- ✓ Aramayı siz yapmadığınız sürece ve telefon çağrısı güvendiğiniz bir kaynaktan gelmediği sürece – kişisel bilgilerinizi, ödeme detaylarınızı veya internet hesap bilgilerinizi telefonda, asla, hiç kimseye paylaşmayın.
- ✓ Bilgisayarınızın güncellenmiş anti-virüs ve anti-casus yazılımlarıyla ve iyi bir güvenlik duvarıyla korunduğundan emin olun. Önce araştırma yapın ve sadece bildiğiniz ve güvendiğiniz bir kaynaktan yazılım satın alın. Mobil telefon ve tabletlerinize, cihazınızın uygulama marketi (Google Play, App Store, Windows Store vb.) dışındaki ortamlardan uygulama indirmeyin. Uygulama marketi dışından indirilen uygulamalar telefonunuza/tabletinize zararlı yazılımlar bulaşmasına neden olabilir.



6- İnternet ve Mobil Cihaz Dolandırıcılık Yöntemleri

Virüsler, kötü amaçlı yazılımlar ve truva atı, vb. zararlı programları bilgisayar ya da cep telefonuna bulaştırma yoluyla kişisel ve finansal bilgileri (internet bankacılığı şifresi, SMS ile iletilen mobil onay kodu, vb.) ele geçirmeyi amaçlayan dolandırıcılık türüdür.

İnternet ve Mobil Cihaz Dolandırıcılığı Nasıl Yapılır?

- ✓ Güvenli olmayan internet siteleri vasıtasıyla finansal kurum müşterilerine ulaşan dolandırıcılar bu siteler üzerinden kişilere çeşitli dosya, fotoğraf ya da uygulamayı cihazlarına indirme konusunda ikna ederler.
- ✓ Akıllı telefonların uygulama marketleri üzerinde yayınladıkları zararsız gibi görünen ve güncel konulara hitap eden (virüs testi, kur çevirici, oyun v.b) uygulamaları sunarak kişilerin cihazlarına yüklemeyi sağlarlar.
- ✓ Bilgisayar, dizüstü bilgisayar, akıllı telefon ya da tablete kurulan bu uygulamalar kişilerin şifrelerini, kişisel bilgilerini ve tek kullanımlık şifreleri ele geçirmenin yanında gerçek kişinin bankacılık uygulamasına erişimini de engellerler.

İnternet ve Mobil Cihaz Dolandırıcılığından Nasıl Korunuruz?

- ✓ Güvenliğinden emin olmadığınız kaynaklardan bilgisayarınıza veya mobil cihazınıza uygulama yüklemeyiniz.
- ✓ Güvenliğinden emin olmadığınız kaynaklardan gelen e-postaları ve eklerini açmayınız. E-posta ayarlarınız yaparken eklerin otomatik olarak açılmayacağından emin olunuz.
- ✓ Mobil cihazınıza uygulama indirirken her zaman resmi uygulama mağazalarını kullanınız.
- ✓ Sürekli yeni virüslerin piyasaya çıkması ve anti-virüs programının bu virüsleri tanımama ihtimaline karşı anti-virüs programını düzenli olarak güncelleyiniz.
- ✓ Mobil cihazınıza yüklediğiniz uygulamaların, erişmek istediği izinleri kontrol ediniz. Özellikle bilinmeyen kaynaklardan uygulama yüklenmesine ve telefonunuza ait yönetici izni (admin) isteyenlere izin vermeyiniz.
- ✓ Şifreniz size özeldir, lütfen banka çalışanları ve en yakınlarınız dahil kimseyle paylaşmayın, herhangi bir yere yazmayın.
- ✓ İnternet şubesinden çıkmak için mutlaka "Çıkış" butonunu kullanın. "Çıkış" butonu; oturumunuzun ve internet şubesi işlem penceresinin güvenli bir şekilde kapatılmasını sağlayacaktır
- ✓ İnternet Şube ve mobil cihaz güvenliğinizden şüphe duyduğunuz bir durumla karşı karşıya kalırsanız bankanızın Müşteri İletişim Merkezini arayarak bilgi veriniz.



7- Güncel Tehditler

Covid-19 Salgınına Kullanan Atak Türleri

Dolandırıcılar her zaman güncel gelişmeleri takip ederler; son dönemde ülkemizi ve Dünya'yı etkisi altına alan Covid-19 salgınına da kullanarak geliştirdikleri yöntemlerle kişisel bilgilerinizi ele geçirmeye çalışıyorlar. Covid-19 aşı çalışmalarının da Dünya üzerinde başlamasıyla dolandırıcılar aşı için başvuru aldıklarını iddia ettikleri sahte mesajlar gönderip, sahte uygulama ya da siteler üzerinden kişisel ya da finansal bilgilerinizi hedef alıyorlar.

Zararlı Yazılım

Akıllı telefon, tablet ve kişisel bilgisayarlara uygulama marketlerinden indirilen; “ateşölçer”, “covid 19 önlemleri”, “salgından korun”, “covid testi”, “covid aşı”, “aşı başvuru” ve benzeri ibareli uygulamalar aracılığıyla zararlı yazılımları cihazlarınıza yükleyebilirler.

İpuçları

- ✓ Tanınmamış bir uygulamacı tarafından geliştirilmiş ve kısa süre içinde çok fazla olumlu yorum ve puan almış uygulamaları indirmemenizi öneririz.
- ✓ Özellikle çok bilinmeyen uygulamamaları indirmeden önce her seferinde uygulama hakkında araştırma yapmanızı tavsiye ederiz.
- ✓ Uygulama marketlerde aşı ve benzeri konulardaki uygulamalar için üretici olarak T.C Sağlık Bakanlığı ibaresi dışındaki hiçbir kaynağa güvenmeyin.

Ölülama

Güvenilir kurumların ya da kişilerin ele geçirilmiş/kopyalanmış verileri üzerinden gelen “covid 19 önlemleri”, “salgından korun”, “covid testi” covid testi”, “covid aşı”, “aşı başvuru” gibi ibareler içeren bir e-posta ya da SMS ile finansal kurum müşterilerini zararlı yazılımı indirmek için ikna etmeye ve uygulama vasıtasıyla finansal varlıklarına dair güvenlik bilgilerini ele geçirmeye çalışabilirler.

İpuçları

- ✓ Güvenilir kurumların ya da kişilerin ele geçirilmiş/kopyalanmış verileri üzerinden gelen e-posta ya da SMS'ler konusunda dikkatli olun.
- ✓ Bu tip şüpheli kaynaklardan gelen linkleri kesinlikle açmayın.
- ✓ Devlet kurumları ya da finansal kurumlar kesinlikle e-posta ya da SMS yolu ile link paylaşmaz.
- ✓ Devlet kurumları ya da finansal kurumlar kesinlikle sizden finansal ya da kişisel verilerinizi talep etmez.



KAYNAKÇA

<https://www.akbank.com/tr-tr/genel/akbankguvenlik/dolandiricilik.html>

<https://www.akbank.com/tr-tr/genel/akbankguvenlik/guncel-tehditler.html>

<https://www.aktifbank.com.tr/tr/bize-ulasin/hizmet-noktalarimiz/internet-sube/dolandiricilik-yontemleri>

<https://www.hsbc.com.tr/direkt-bankacilik/dijital-bankacilik/online-guvenlik/phishing>

<https://www.hsbc.com.tr/direkt-bankacilik/dijital-bankacilik/online-guvenlik/sosyal-muhendislik>

<https://www.icbc.com.tr/tr/guvenlik/detay/En-Sik-Karsilasilan-Dolandiricilik-Yontemleri/407/1118/0>

<https://www.isbank.com.tr/dolandiricilik-yontemleri>

<https://www.teb.com.tr/guvenlik/dolandiricilik-yontemleri/>

<https://www.turkiyefinans.com.tr/tr-tr/dijital-bankacilik/guvenlik/Sayfalar/dolandiricilik-yontemleri.aspx>

<https://www.ziraatbank.com.tr/tr/dijital-bankacilik/guvenlik/yaygin-dolandiricilik-turleri>