Dolandırıcılık Yöntemleri

Telefon Dolandırıcılıkları

Nedir?

Telefonla polis, savcı, avukat, TAM ATM platformu yetkilisi ve bankacı arıyor izlenimi verilerek, inandırıcı bir senaryo ile güven kazanıp ikna ederek kişisel ve finansal bilgilerin paylaşılmasını sağlayan dolandırıcılık türüdür.

Hangi Şekillerde Karşılaşırım?

Dolandırıcı, telefonla sizi arayarak benzer şekilde inandırıcılığı sağlamak için arka fonda polis telsizi, yazıcı sesi ya da bankadan/ TAM ATM yetkilisi olarak aradığına ilişkin sesleri taklit edebilmektedir. Genellikle,

- ATM' de sıkışan paranın iadesi,
- Üyelik aidatı iadesi,
- Suç örgütleri listesinde adının olduğuna ilişkin sahte bildirim yapılması ve silinmesi için para gönderimi istenmesi, vb.

iyi hazırlanmış ve inandırıcı senaryolarla telefonda güveninizi kazanıp kişisel ve finansal bilgilerinizi (internet bankacılığı şifresi, kart şifresi, SMS ile iletilen mobil onay kodu vb.) paylaşmanız istenmektedir.

Kendimi Nasıl Korurum?

• Platform üyesi bankalarımız tarafından aranarak hiçbir zaman internet bankacılığı şifresi, SMS ile iletilen mobil onay kodu ya da tek kullanımlık cep anahtar şifre bilgisi istenememektedir. Bu tarz bilgi istenmesi durumunda bilgilerinizi vermeyerek telefon görüşmesini sonlandırınız.

• Her zaman için bilmediğiniz kişiler sizi aradığında dikkatli olunuz.
• Şüphe duymanız halinde, bilgi girişinde bulunmayarak konuyu 0 850 222 0 826 telefon numaralı müşteri hizmetlerine bildiriniz.

Sosyal Medya Dolandırıcılıkları

Nedir?

Instagram, YouTube, X, 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 Karşılaşırım?

Dolandırıcılar, genellikle sosyal medya aracılığıyla arkadaş listenizde bulunan hesabı ele geçirip arkadaşınız gibi davranarak

- 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.

Kendimi Nasıl Korurum?

- Sosyal medya üzerinden yayınlanan reklam ve kampanyalarımız, sadece platform üyesi bankaların resmi kurumsal sosyal medya hesapları üzerinden yapılmaktadır.

- İnternet ortamında bir kişinin kendisini tanıttığı kişi olduğundan emin olmak son derece zor olduğundan güvenliğiniz açısından kişisel ve finansal bilgilerinizi bu kişilerle kesinlikle paylaşmayınız.

- Gerçekten acil bir durum olma ihtimaline karşı farklı bir kanaldan (örneğin telefon ederek) tanıdığınızla temas kurmayı deneyiniz.

İnternet ve Mobil Cihaz Dolandırıcılıkları

Nedir?

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.

Bilgisayar ve Mobil Cihaz Zararlı Yazılımları
Bilgisayar ve mobil cihazlara zarar vermek, bilgi çalmak, vb. amaçlarla hazırlanmış kötü amaçlı yazılımlardır. Örnek olarak virüsler, truva atları, solucanlar verilebilir.

Site Trafiği Yönlendirme (Pharming)
Farming, adres çubuğuna doğru internet adresi yazılmasına rağmen, dolandırıcıların DNS (Alan Adı Sistemi) ayarlarını bozarak internet sayfasını sahte bir internet sayfasına yönlendirmesi yoluyla gerçekleştirilen dolandırıcılık türüdür.

Bilgisayar ve Mobil Cihaz Zararlı Yazılımları

• Güvenliğinden emin olmadığınız uygulama dükkanlarından uygulama yüklemeyiniz. Resmi marketlerden uygulama indirmeye özen gösteriniz. Güvenilmeyen veya bilinmeyen kaynaklardan bilgisayarınıza veya mobil cihazınıza uygulama yüklemeyiniz.
• Mobil cihazınıza yüklediğiniz yeni uygulamaların erişmek istediği izinlere dikkatli edin. Özellikle bilinmeyen kaynaklardan uygulama yüklenmesine ve telefonunuza ait yönetici izni (admin) isteyenlere izin vermeyiniz.
• Lisanslı işletim sistemi, yazılım ve antivirüs programları kullanın ve sürekli güncel tutunuz.
• Bilgisayarınızda yüklü değilse Microsoft Security Essentials programını ücretsiz indiriniz.
• Eğer cihazınıza virüs bulaşmışsa, cihazınızın teknik servisinden destek almanızı öneririz.
• Tanımadığınız kişilerden gelen e-postaları ve eklerini açmayınız. E-posta ayarlarınız yaparken eklerin otomatik olarak açılmayacağından emin olunuz.
• İnternetten cihazınıza yüklediğiniz yazılım, resim, video,vb. dosyaları anti- virüs taramasından geçirdikten sonra açınız.
• Şüphe duymanız halinde, bilgi girişinde bulunmayarak konuyu 0850 222 0 826 telefon numaralı Bankamız müşteri hizmetlerine bildiriniz.

Site Trafiği Yönlendirme (Pharming)

• Arama motorlarına TAM ATM platformuna üye bankaların kurum ismini yazarak arama sonucu çıkan linklere tıklamayınız. Bunun yerine adres çubuğuna ilgili bankanın URL adresini yazarak giriş yapınız.
• İnternetten cihazınıza yüklediğiniz yazılım, resim, video, vb. dosyaları anti- virüs taramasından geçirdikten sonra açınız.
• Tanımadığınız kişilerden gelen e-postaları ve eklerini açmayınız. E-posta ayarlarınızı yaparken eklerin otomatik olarak açılmayacağından emin olunuz.
• TAM ATM platformuna üye bankaların internet şubesine girişte karşılama mesajının doğru olup olmadığını kontrol ediniz.
• TAM ATM platformuna üye bankaların internet sitesinde olduğunuzdan emin olmak adına, giriş yaptığınız internet sitesinin Güvenlik sertifikasının ilgili banka güvenlik sertifikası ile aynı olup olmadığını kontrol ediniz.