TÜRKİYE İŞ BANKASI

SOSYAL MÜHENDİSLİK

İnsanların zafiyetlerinden faydalanılarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgilerin elde edildiği dolandırıcılık türüdür.

Saldırganlar en zayıf noktalarımız olan duygularımızı sömürmeyi amaçlar.

KORKU | PARA KAZANMA İSTEĞİ | TELAŞ | GÜVEN | BİLGİSİZLİK

UMURSAMAZLIK | ACIMA | EGO | HIRS | ARZU

Sosyal Mühendislik saldırılarında 4 farklı iletişim yöntemi kullanılabilir:

TELEFON | SOSYAL MEDYA | DİJİTAL ARAÇLAR | YÜZ YÜZE İLEŞİTİM

TELEFON

Kötü amaçlı kişiler sizi arayıp telefonda güveninizi kazanmaya, kişisel bilgilerinizi ele geçirmeye ve taleplerini yerine getirmenizi sağlamak üzere sizi harekete geçirmeye çalışabilir. Bunları gerçekleştirmek için en çok kullandıkları yöntemler şunlardır:

• **Panik ve telaş** ortamı yaratıp sizi düşünmeden hareket etmeye zorlarlar. Bu yolla hesap, şifre bilgilerinizi veya cihazlarınızdaki bilgileri ele geçirmeyi amaçlarlar.

• **Kızgın ve otoriter** davranarak üzerinizde baskı kurmaya ve sizi korkutmaya, bu şekilde size istediklerini yaptırmaya çalışırlar.

• Güvenilir bir kurum/kuruluştan arıyor izlenimi vererek, **kredi kartı aidat iadesi, sigorta ücret iadesi** gibi vaatlerle veya **hesabınızdan işlem yapılmış olması** gibi sizi endişelendirecek yalanlarla kişisel bilgilerinizi ve şifrelerinizi paylaşmanızı isterler.

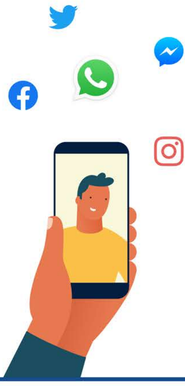
DİKKAT

- Hiçbir bankamız çalışanı sizi arayarak ya da sizinle sözlü/yazılı iletişime geçerek **müşteri/kimlik numaranızı** ve **şifrenizi** kendisiyle paylaşmanızı istemez.

- **Sizi arayanların yönlendirmesi ile** İnternet Şubemiz, İşCep ve Maximum Mobil üzerinden **işlem yapmayın.**

- Sizi **arayan kişi acil olduğunu belirtse dahi**, telefon görüşmesiyle iletilen talepleri **farklı bir kaynaktan teyit etmeden harekete geçmeyin.**

SOSYAL MEDYA



• Sosyal medyada bedava ödül (hediye internet paketi, COVID-19 evdekal para destek paketi, araba çekilişi, vb.) ya da yüksek limitli kredi, kredi kartı tahsisi vadeden **link içerikli reklamlara tıklamayın ve bu reklamların yönlendirdiği uygulamaları indirmeyin.**

Benzeri vaatlerin ardından sizden para isteyecekler ve asla iade etmeyeceklerdir. Bu nedenle, doğrudan mesaj ile sizden **müşteri/TC kimlik numaranızı veya kredi kartı/şifre bilgilerinizi isteyenlerle, isteyen kişi kim olduğunu söylerse söylesin, bu bilgilerinizi paylaşmayın.**

• Sosyal medya platformlarından gelen **tanımadığınız arkadaşlık isteklerini kabul etmemelisiniz.**

• Sosyal medya hesapları sıkça ele geçirilebildiği için arkadaşınızdan gelse dahi emin olmadığınız **bağlantılara ve dosyalara tıklamamalısınız.**

• Kişisel bilgilerinizin yalnızca arkadaş çevreniz tarafından görüntülenebilir olduğuna emin olmalısınız, aksi takdirde sosyal mühendislik saldırılarında hedef alınma ihtimaliniz artacaktır.

DİJİTAL ARAÇLAR

Siber saldırganların hedefine ulaşmak için en çok kullandığı platformlar arasında **e-posta, internet siteleri ve SMS** yer almaktadır.

Dolandırıcılar, güvenilir kurumdan gönderilmiş izlenimi veren sahte e-postalar gönderir. Bu sahte e-postalar;

- **Zararlı ek** içerebilir, sizi sahte internet sayfasına yönlendirip cihazınıza **zararlı yazılım** bulaşmasına neden olabilir.

- **Form dosyası** aracılığıyla kişisel bilgilerinizi ve müşteri numarası, kart, şifre gibi bankacılıkla ilgili bilgilerinizi almaya çalışabilir.

- **Tehdit ve şantaj** içererek sizden para talep edebilir.

- Bu yollarla **hesap, şifre bilgilerinizi** veya **cihazlarınızdaki bilgileri** ele geçirmeyi ve cihazınızın kontrolünü alarak, telefonunuzu başka numaraya yönlendirmeyi, size gelen mesajları okuyamamanızı ve telefonunuzu kullanamamanızı amaçlarlar.

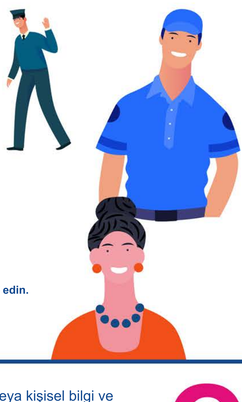
DİKKAT

Tarafınıza gelen e-posta ya da SMS'ler, tanıdığınız/bildiğiniz bir kişiden gelmiş gibi görünse dahi, gönderen kişiye telefon veya başka bir iletişim kanalıyla ulaşmadan e-posta ya da SMS içerisinde yer alan

+ dosyaları indirmemeli ve açmamalı,

+ bağlantıları tıklamamalısınız.

YÜZ YÜZE İLETİŞİM



Saldırganlar gerçek kimliklerini ve amaçlarını gizlemek için kendilerini;

• Polis, hakim, savcı ve vergi memuru gibi devlet görevlileri veya

• Sevdiğiniz birinin yakını gibi **kolay güvenebileceğiniz** kişiler

olarak tanıtabilir.

Kimliğinden emin olmadığınız kişilerle yüz yüze iletişim kurarken:

• Kişisel ve bankacılıkla ilgili **herhangi bir bilginizi paylaşmayın.**

• Onlardan öğrendiğiniz **bilgi ve haberlerin güvenilirliğini birkaç farklı kaynaktan teyit edin.**

• Sebep ne olursa olsun **bilgisayarlarınızı veya telefonlarınızı kullandırmayın.**

Aklınızda bir soru işareti kaldıysa veya kişisel bilgi ve şifre paylaşımında bulunduğunuzu düşünüyorsanız,

0 850 724 0 724 numaralı İş Bankası Telefon Şubesi'ni aramanız Müşteri Temsilcimiz ile iletişime geçebilirsiniz.