DOLANDIRICILIK TÜRLERİ ve KORUNMA YÖNTEMLERİ

Dolandırıcılığın nasıl yapıldığını, dolandırıcılıktan nasıl korunacağınızı ve neler yapmanız gerektiğini öğrenmek için aşağıdaki bilgileri dikkatle okuyunuz.

Dolandırıcılık Türleri

Ön Ödeme Dolandırıcılığı

Dolandırıcılar ellerinde olmayan veya kendilerine ait olmayan ürün ve hizmetleri satmak için internet/sosyal medya üzerinde reklam vererek bilinen markaların internet sitelerini taklit ederler veya farklı internet siteleri oluştururlar.

- ✓ Alışveriş yaptığınız sitenin, kişinin, kurumun güvenilir olup olmadığını kontrol etmelisiniz. Alışveriş yaptığınız internet sitesinin SSL sertifikasının var olduğundan ve güncel olduğundan emin olunuz.
- ✓ Sosyal medya ve internet üzerinden yaptığınız alışverişlerde, gelen ürünü kontrol etmeden teslim almayınız.
- ✓ Sosyal medyada gördüğünüz otel, tatil rezervasyonu kampanyaları için para transferi yaparken dikkatli olmalısınız. Para gönderdiğiniz kişi veya kişiler dolandırıcı olabilir. Otel, tatil rezervasyonu yaparken güvenilir siteler ve şirketleri kullanmanız işlem güvenliğiniz açısından oldukça önemlidir.
- ✓ Noter vasıtası ile alım satım yaparken, noter işlemleri tamamlanmadan para transfer işleminin gerçekleşip gerçekleşmediğini ve alım satımı yaptığınız kişinin gerçek kişi/kurum olup olmadığını kontrol etmek sizi koruyacaktır.

Sosyal Mühendislik Yöntemleriyle Dolandırıcılık

Bu dolandırıcılık yönteminde dolandırıcılar, sizden kişisel bilgilerinizi almak ya da istedikleri işlemleri yapmanızı sağlamak için kendilerini kamu görevlisi (polis, savcı, bankacı vb.) olarak tanıtır veya çeşitli vaatler ile (kampanya, chip puan, aidat iadesi, işe yerleştirme, yurtdışına çıkarma vb.) ikna etmeye çalışırlar.

- ✓ Dolandırıcılar kendilerini kamu görevlisi olarak (polis, savcı, hâkim vb.) tanıtır ve terör örgütü ile ilişkinizin olduğu ya da banka hesabınızın terör örgütü tarafından kullanıldığını söyleyerek sizi korkutup, para transferi yapmak, kart bilgilerinizi elde etmek (kart şifresi tuşlatmak da dahil) veya kimlik bilgilerinizi vermek için ikna etmeye çalışır.
- ✓ Banka hesaplarınız/ kredi kartlarınız ile ilgili bir sorun olduğu veya paranızın iade edileceği gibi konularda arama yaparlar.
- ✓ Çok ikna edici olabilirler ve kaçırılmayacak fırsatlar sunarlar.
- ✓ Teklifin sadece sizin için geçerli olduğunu söyleyebilirler.
- ✓ Güveninizi kazanmak için dışarıdan elde edilen kredi kartı numaranızı ya da gerçekleştirdiğiniz bankacılık işlemlerinizden örnek verebilirler.
- ✓ Sizi oyalamak için uzun süre telefonda tutarlar.
- ✓ Dolandırıcılar size ulaşarak yasa dışı bahis/kumar sitelerinde yüksek meblağlar kazanabileceğinizi söyleyebilirler. Hatta onlara güvenmenizi sağlamak için size bir miktar para bile yollayabilirler, paranın iadesini talep edebilirler. Size bu ve benzeri taleplerle gelen kişilere para göndermeyin, bilgilerinizi paylaşmayın.

- ✓ Arkadaşlık siteleri veya sosyal medya üzerinden evlenme, işe yerleştirme, yurtdışına çıkarma, para kazanma vb. vaatlerde bulunan tanımadığınız kişilere para göndermeyin ve bilgilerinizi paylaşmayın.
- ✓ Dolandırıcılar, bildiğiniz veya alışkın olduğunuz çağrı merkezi numaralarına benzer numaralar edinerek sizi arayabilirler. Arayan kendini kamu ya da banka çalışanı olarak tanıtabilir ve sizden özel bilgilerinizi isteyebilir veya SMS ile gelen bir linke tıklamanızı talep edebilirler.
- ✓ Sizinle telefonla, SMS veya sosyal medya kanallarından iletişime geçerek kazanç/indirim vaadiyle "Bize referans numarasıyla para gönderin, daha sonra misliyle geri alın veya indirim kazanın" gibi ifadeler kullanan ve talepte bulunan kişilere güvenmeyin; para göndermeyin ve kişisel bilgi veya kart bilgilerinizi paylaşmayın.

Bu gibi durumlarla karşılaştığınızda arayan kişilere kesinlikle itibar etmeyin ve görüşmeyi sonlandırın.

Zararlı Yazılım Yöntemiyle Dolandırıcılık

Çeşitli internet siteleri, akıllı telefon uygulama marketleri, SMS bildirimleri üzerinde yayınladıkları, genellikle güncel konulara hitap eden, zararsızmış gibi görünen uygulama, dosya veya link ile kişilerin cihazlarına erişim sağlayabilirler.

Böyle bir dolandırıcılığa maruz kalmamak için;

- ✓ Cihaz yazılımlarınızı ve güvenlik uygulamalarını her zaman güncel tutun.
- ✓ Mutlaka iyi bir zararlı yazılım engelleyici uygulama edinin.
- ✓ Gönderilen kaynağın güvenilir olduğundan emin olun.
- ✓ Güvenmediğiniz hiçbir kaynaktan dosya, oyun, uygulama vs. indirmeyin, hiçbir linke tıklamayın.

Oltalama Yöntemiyle Saldırı

Oltalama saldırılarında, dolandırıcılar farklı kaynaklardan (SMS, eposta, sosyal medya mesajı, vb.) size ulaşarak, sizin kişisel veya kart/hesap bilgilerinizi ele geçirmek için ikna etmeye çalışırlar. Gönderilen mesaj ya da bildirim bilinen veya güvenli görünen bir mail adresinin taklidi olabilir.

- ✓ Gelen bildirimlerdeki bir linki tıklamanız veya sizden bildirime cevap vermeniz istenebilir.
- ✓ Böyle bir durum ile karşılaştığınızda; hiçbir şekilde linki tıklamayın ve bilmediğiniz bağlantılarda kişisel bilgi/şifre girmeyiniz.
- ✓ Bilmediğiniz bir kaynaktan gelen bildirimlerde dikkatli olunuz, size ait kişisel bilgilerinizi paylaşmayınız.

Kayıp&Çalıntı Kart Üzerinden Dolandırıcılık

Bu tür dolandırıcılıklarda kaybedilen veya çalınan kartlarla, kart sahiplerinin bilgileri dışında işlem gerçekleştirilebilir.

- ✓ Kartlarınızın ve şifrelerinizin güvenliğinin sağlanması sorumluluğunun sizde olduğunu unutmayınız.
- ✓ Kart veya şifrelerinizin güvenliğinden şüphe duymanız halinde derhal bankanızı ve United Payment'ı bilgilendiriniz.
- ✓ Kart hamilleri, yapacakları kayıp ya da çalıntı bildiriminden önceki yirmi dört saat içinde kartları ile gerçekleştirilen hukuka aykırı kullanımdan doğan zararlardan 250 TL'ye kadar sınırlı olmak üzere sorumludur. Hatalı ve yetkisiz işlem sebebiyle alıcı ve/veya alıcının Ödeme Hizmeti Sağlayıcısından bedelin geri alınması halinde United Payment işlemden doğan zararına ilişkin tutar, tespit ve ispat edilmiş olmadıkça ilgili bedelden mahsup edilemeyecektir.

KOLAYCA ALABİLECEĞİNİZ ÖNLEMLER

Şifrenizi, kartınızı ve bilgilerinizi koruyun

- ✓ Kimlik doğrulama bilgilerinizi (kullanıcı adı, şifre, SMS ile cep telefonunuza gönderilen tek kullanımlık şifre, parola, kart şifresi, PIN vb.) kimseyle paylaşmayın ya da tuşlamayınız.
- ✓ Unutmayın; devlet kurumları, emniyet, savcılık, polis ve finansal kurumlar sizden şifrenizi herhangi bir şekilde tuşlamanızı ya da söylemenizi istemez.
- ✓ ATM, kiosk ya da akıllı kasalardan işlem yaparken 3.kişilerden yardım almayın.
- ✓ Kartınızı ATM'nin ya da kioskun alıkoyması halinde derhal müşteri hizmetlerimizi arayın.
- ✓ ATM, kiosk ya da akıllı kasalarda, olağan dışı bir durum, cihaz, aparat tespit etmeniz halinde ATM/kiosk sahibi kuruma bilgilendirmede bulunun.

Şifre belirlerken şifre güvenlik standartlarına uygun bir şekilde;

- ✓ Ardışık rakamlar içermeyen,
- ✓ Sizin veya yakınlarınızın doğum tarihini çağrıştırmayan, tuttuğunuz takımın kuruluş yılı olmayan,
- ✓ Milli günler ve bayramların tarihini içermeyen bir kombinasyon tercihi sizi güvende tutacaktır.

Bilgisayarınızı ve Telefonunuzu Güncel Tutun

- ✓ Kişisel cihazlarınızın sistem güncellemelerini düzenli yapmalı ve cihazlarınıza uygulama marketi (Google Play, App Store, Windows Store vb.) dışındaki ortamlardan uygulama indirmemelisiniz.
- ✓ Uygulama marketleri üzerinden indireceğiniz uygulamalar için de onaylı ve tanınmış yazılımcılar tarafından üretilmemiş ürünleri indirmeden önce iyice araştırın.
- ✓ Cihazlarınızı korumak için zararlı yazılım engelleyici program edinin.
- ✓ İzniniz olmadan size gönderilen e-posta ve SMS iletilerini açmayın.
- ✓ İzniniz olmadan size gönderilen bir e-posta ya da SMS iletisinin eklerini açmayın. United Payment'tan gelmiş gibi görünüp, bilgilerinizi güncellemenizi isteyen ya da ödül kazandınız, gibi ibareler ile linklere yönlendirme yapan e-postaları ya da SMS'leri asla dikkate almayın.
- ✓ United Payment, müşterilerini arayarak, hiçbir nedenle herhangi bir kişisel bilgi istemez.

Kişisel bilgileriniz, kart/hesap şifre bilgilerinizin korunması sorumluluğu tarafınızda olup, diğer sorumluluklarınız hakkında bilgi edinmek için kullanıcı sözleşmenizi kontrol edebilirsiniz.

HERHANGİ BİR ŞÜPHELİ İŞLEM VEYA DOLANDIRICILIK İŞLEMİ İLE KARŞILAŞMANIZ, KULLANMIŞ OLDUĞUNUZ CİHAZLARDA, YAZILIMLARDA, MOBİL UYGULAMADA HERHANGİ BİR KİŞİSEL BİLGİNİZİN ÇALINMASI, 3. KİŞİLER TARAFINDAN ELE GEÇİRİLMESİ DURUMLARINDA VE/VEYA TARAFINIZA AİT HASSAS VERİLERİN DEĞİŞTİRİLMESİ VE SİLİNMESİNİN GEREKMESİ DURUMLARINDA, DERHAL UNITED PAYMENT MÜŞTERİ HİZMETLERİNİN 0850 252 22 22 TELEFON NUMARASINDAN BİZE ULAŞABİLİRSİNİZ.

.