TÜRKİYE BANKALAR BİRLİĞİ

Dolandırıcılık Eylemleri ve Korunma Yöntemleri

Bu Rehberde yer alan bilgiler, Türkiye Bankalar Birliği tarafından kamuoyunun bilgilendirilmesi amacı ile hazırlanmıştır. Bu çalışmada bilişim suçları ile bugüne kadar karşılaşılan sahtecilik ve dolandırıcılık eylem girişimleri hakkında genel bilgi verilmek suretiyle müşterilerin karşılaşılacağı olası eylemlerde ne şekilde hareket edilmesi gerektiği hakkında bilgilendirilmesi amaçlanmıştır. Ayrıca yaşanan dolandırıcılık ve sahtecilik örneklerine ilişkin detaya da yer verilerek bilgilerin daha etkin ve kalıcı olması amaçlanmıştır. Yeni dijital finansal dünya dolandırıcıların yeni teknikler geliştirmesine imkan verdiğinden dolandırıcılar tarafından farklı yöntemlerin geliştirilmesi de mümkündür. Müşterilerin bankalarımızın bu konudaki uyarı ve açıklamalarını titizlikle takip etmesi gerekmektedir.

Çalışmada bazı internet adresi bağlantılarına yer verilmiştir. Ancak, söz konusu internet bağlantıları üzerinden erişilen adres ve sayfaların varlığı, yer alan bilgi ile içeriğin doğruluğu ve hukuka uygunluğu hususunda garanti vermemektedir ve sorumluluk kabul etmemektedir.

Burada yer alan bilgilerin, yaşanabilecek dolandırıcılık ve sahtecilik olayları ve alınacak tedbirler açısından yeterli olduğu hususu garanti edilmemektedir. Tüm açıklamalar yaşanan somut olaylara dayanarak hazırlamış olup, Türkiye Bankalar Birliği'nin sorumluluğu bulunmamaktadır.

ÖNSÖZ

Bu kitabın amacı, bankacılık ve finans sektörü ile bireyleri tehdit eden dolandırıcılık tiplerinin analizi, sektör açısından değerlendirilmesi, dünyadan ve Türkiye'den örnekler verilerek korunma önerileri hakkında bilgi sağlamaktır.

Bu bağlamda, bir bütün olarak bilinen olası yöntemlerin çerçevesi çizilmiş, Türkiye'de ve dünyada karşılaşılan dolandırıcılık yöntemlerine ve çeşitlerine değinilmiş ve bunlar analiz edilmiş, örnek olay senaryoları ile irdelenerek, önümüzdeki dönemlerde banka ve bireyler açısından ele alınabilecek dolandırıcılıktan korunma yöntemlerine yer verilmiştir.

Türkiye Bankalar Birliği Bankacılık Dolandırıcılık Önleme Çalışma Grubu temsilcilerinden oluşturulan uzman bir ekip tarafından hazırlanan bu çalışmanın sektördeki güvenlik uygulamaları ve dolandırıcılık engelleme çalışmaları açısından bir kaynak olarak kullanılacağına ve banka çalışanlarına önemli katkı sağlayacağına inanıyoruz.

Saygılarımızla.

Amaç ve Genel Bilgi

Dolandırıcı kelimesi Türk Dil Kurumu Sözlüğünde "birini aldatarak mal veya parasını alan kimse" olarak tanımlanmaktadır. Dolandırıcılık eylemlerine hemen her ülkede ve kültürde rastlamak mümkündür. Son yıllarda teknoloji kullanımının ve uzaktan işlemlerin daha da yaygınlaşması nedeniyle dolandırıcılık eylemleri teknolojik yöntemlerin kullanıldığı daha karmaşık bir yapıya bürünmüştür.

Dolandırıcıların veya dolandırıcılık amacıyla kurulmuş olan çetelerin hedefinde şahısların yanı sıra kurumlar da yer alabilmektedir.

Son yıllarda Türkiye'de ve dünyada dijital bankacılık kanal kullanımının artması, özellikle mobil bankacılık yoluyla verilen hizmetlerde çeşitlilik, birçok işlemlerde ödemelerin bankalar üzerinden yapılmasına yönelik düzenlemeler ve bu ödemelerin dijital kanallar üzerinden yapılması amacıyla sunulan hizmetler sonucunda, bankalar ile çalışan müşteri sayılarında ve kullanılan ürünlerde kayda değer artışlar meydana gelmiştir.

İşlemlerin uzaktan yapılabilmesi, müşteri tanımlamada kullanılan kişisel bilgiler ile yöntemlerin önemini daha da artırmış, işlem doğrulama konusunda yeni tedbirler alınmış ve düzenlemeler yapılmıştır. Ayrıca, banka kullanımının ve hizmet çeşitliliğinin artması dolandırıcıların bankalara ve müşterilere yoğunlaşmalarına neden olmuştur.

Teknoloji kullanımının ve uzaktan işlemlerin yaygınlaşması, teknoloji kullanılanak yapılan dolandırıcılık eylemlerini karmaşık bir yapıya bürünmesine neden olmuştur

Banka müşterileri, dolandırıcılık eylemlerine en çok hedef olan kesimlerin başında gelmektedir. Bu kapsamda; gerekli tedbirlerin alınması, yeni hizmetlerin yarattığı ortamlara uygun düzenlemelerin yapılması, teknolojik altyapıların düzenlemelere uygun bir şekilde yapılandırılması, denetimi ve hepsinden önemlisi bankaların bankacılık işlemlerinin gerçekleştirilmesi konusunda basiretli hareket etmeleri büyük önem taşımaktadır.

Bankacılık sektöründe BDDK tarafından hazırlanan ve ilk olarak 2008 yılında yürürlüğe giren "Bankaların Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliği" ile Bilgi Sistemleri aracılığı ile gerçekleştirilebilen dolandırıcılık türlerine karşı alınacak tedbirlere ilişkin düzenleme gerçekleştirilmiştir. Daha sonra, bankaların faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetimi ile elektronik bankacılık hizmetlerinin sunulmasında ve bunlara ilişkin risklerin yönetiminde esas alınacak asgari usul ve esaslar ile tesis edilmesi gereken bilgi sistemleri kontrollerinin düzenlendiği "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" 1 Temmuz 2020 tarihinde yürürlüğe girmiştir. Telefon bankacılığı yeni Yönetmelikle birlikte özel şartlara tabi tutulmuştur. Bu sayede gelişen teknolojik imkanlar doğrultusunda vatandaşın uzaktan finansal varlıklarını görüntüleyip işlem yaptıkları elektronik bankacılık kanallarından daha güvenli bir şekilde işlem yapabilmeleri için güvenlik standartları getirilerek düzenlenmesi sağlanmıştır.

Ayrıca "Bankalarca Kullanılacak Uzaktan Kimlik Tespit Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik" 1 Mayıs 2021 tarihinde yürürlüğe girmiştir. Uzaktan Müşteri Edinimi, fiziksel olarak hiç banka şubesine gitmeden mobil cihazlar veya web sitesi aracılığı ile banka müşterisi olunmasına imkan tanımaktadır.

Banka müşterileri, dolandırıcılık eylemlerine en çok hedef olan kesimlerin başında gelmektedir

Gelişen teknolojiler sayesinde bankalar, kişilerin kimliklerini ve cihazlarını teyit edebilir hale gelmiştir. Bu da yapılan talep ya da işlemlerin standart bir kontrol ile doğrulanabilmesi, kimlik tespitinin dijital ortamda gerçekleştirilmesi anlamına gelmektedir. Ayrıca, 30 Nisan 2021 tarihli Resmî Gazete'de yayımlanan Mali Suçları Araştırma Kurulu Genel Tebliği (Sıra No: 19) ile müşteri kimliğinin doğrulanması amacıyla kullanılacak uzaktan kimlik tespiti yöntemlerine ilişkin usul ve esaslar düzenlemiştir. Buna göre, müşterileri ile yüz yüze gelinmeksizin kimliğinin doğrulanmasına imkân verecek yöntemlerle sözleşme kurulmasına cevaz verilmiş olması halinde, sürekli iş ilişkisi tesisinde müşteri kimliğinin doğrulanması amacıyla uzaktan kimlik tespiti yöntemleri kullanılabilmektedir.

Açık Bankacılık, 27 Haziran 2013 tarihinde 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri ve Elektronik Para Kuruluşları Hakkındaki Kanun ve 2019 yılında yapılan düzenlemeler ile yasal alt yapısı oluşturulmaya başlanmıştır. Açık Bankacılık hizmeti, farklı Bankalardan alınan belirli bankacılık ürün ve hizmetlerinin, Açık Bankacılık ile tek bir bankadan veya Yetkili Ödeme Servis Sağlayıcılarından güvenli bir şekilde alınması olarak tanımlanmıştır. Yetkili Ödeme Servis Sağlayıcıları, T.C. Merkez Bankası tarafından lisans verilmiş kuruluşlardır.

BDDK tarafından yürürlüğe koyulan yeni düzenlemeler ve tüm dünyada yaşanan Pandemi nedeniyle Bankacılık sektöründe çok daha geniş bir Dijital Dünyanın kapısı açılmıştır. Hem Uzaktan Müşteri Edinimi hem de Açık Bankacılık, gelişen teknolojilerin kullanılması, finansal hayatın kolaylaştırılması, müşteri deneyiminin iyileştirilmesi, sektörde yeni ürünlerin çıkartılması gibi faydalar sağlamaktadır. Yaşanan bu gelişmeler sonucunda dijital ortamda tutulan verilerin güvenliği çok büyük öneme sahip olmaktadır.

Oluşan yeni dijital finansal dünya dolandırıcılar için de yeni alanlar yaratmaktadır. Bu çalışmada, daha çok dolandırıcılık şebekelerinin nasıl çalıştığına, bilinen dolandırıcılık eylemlerinde kullanılan yöntemlerin neler olduğuna ve karşılaşılacak olası eylemlerde ne şekilde hareket edilmesi gerektiğine yer verilmektedir. Ayrıca, bilişim suçları, dolandırıcılık türleri, banka şubelerinde yaşanması muhtemel sahtecilik ve dolandırıcılık eylem girişimleri hakkında temel bilgi verilmekte birçok yöntem ve girişimle ilgili detaylı örneklerle verilen bilgilerin daha etkin ve kalıcı olması amaçlanmaktadır.

İÇİNDEKİLER

BÖLÜM 1

Elektronik Bankacılık Kanallarına Genel Bakış

I. Elektronik Bankacılık Kanallarına Genel Bakış

Dünyada ve ülkemizde gelişen teknolojiler ile birlikte Bankacılık sektöründe yeni teknolojiler kullanılmaktadır. Banka şubelerinde yüz yüze verilen bankacılık hizmetleri farklı ortamlarda sağlanmaya başlanmıştır. Bankacılık faaliyetlerinin yürütülmesinde kullanılan bilgilerin girildiği, iletildiği ve işlendiği, ortamlarda gizliliği sağlayacak önlemlerin alınması büyük önem taşımaktadır. Kişisel ve finansal veriler kâğıt veya elektronik ortamdan bağımsız olarak korunmalıdır.

"Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" ile internet bankacılığı, mobil bankacılık, telefon bankacılığı, açık bankacılık servisleri ile ATM ve kiosk cihazları gibi müşterilerin, uzaktan bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri her türlü banka kanalı elektronik bankacılık kapsamında değerlendirilmiştir. Bu kanallar aracılığı ile yapılan finansal işlemlerin güvenliği için özellikle kimlik doğrulaması ve banka çalışanlarının yetkisiz erişimlerinin engellenmesinin üzerinde özellikle durulmuştur. Telefon bankacılığı bu yönetmelikte ilk defa ayrı bir kanal olarak düzenlenirken, sorgulama ve finansal işlemler dahil olmak üzere, tüm işlemler için bir kimlik doğrulama standartı getirilerek müşteri işlem ve bilgi güvenliğinin sağlanması hedeflenmiştir. İnternet ve mobil bankacılık kanallarından yapılan işlemlerin de elektronik bankacılık kapsamında güvenlik standartları belirlenmiş, mobil bankacılıkta cihaz eşleştirmesi yapılarak SMS OTP gibi ek bir doğrulama olmadan işlemlerin yapılabilmesi gibi deneyim iyileştirici önemli hükümler eklenmiştir.

Günümüzde bankacılıkta en yaygın olarak kullanılan kanalların tanımlarına aşağıda kısaca yer verilmiştir.

A) İnternet Bankacılığı

1997
İnternet bankacılığı Tükiye'de ilk uygulanmaya başladığı yıl

Bankaların kendi ticaret unvanı, işletme adı veya herhangi başka bir ad altındaki bir web sayfası üzerinden sundukları hizmetlere müşterilerin, kullandıkları cihaz veya platformdan bağımsız olarak, internet yoluyla ulaşabildiği ve kendilerine ait finansal veya kişisel verileri görüntüleyebildiği, değiştirebildiği veya finansal sorumluluk yaratacak işlemlerin 7/24 gerçekleştirebildiği elektronik bankacılık kanallarıdır.

Ülkemizde ilk olarak 1997 yılında başlatılan İnternet Bankacılığı uygulaması sektörde faaliyet gösteren bankalar tarafından ürün ve hizmetlerin sunulduğu önemli bir kanal haline gelmiştir.

İnternet Bankacılığı üzerinden verilen hizmetler nakit para yatırma/çekme işlemleri dışında bankacılık hizmetlerininin çoğunu kapsamaktadır.

B) Mobil Bankacılık

2010
Mobil uygulama hizmetlerinin başlangıç tarihi

Akıllı telefon veya tablet gibi mobil bir cihaz üzerinde yüklü, bankaya ait mobil uygulama üzerinden müşterilerin bankacılık işlemlerini gerçekleştirebildikleri özelleşmiş internet bankacılığı dağıtım kanalıdır. Bilişim teknolojilerinin gelişimi ile bankacılık sektörü de ülkemizde 2010 yılından itibaren mobil uygulama hizmeti vermeye başlamıştır.

Kişilerin kullanmış oldukları mobil cihazlar yaygınlaştıkça bankacılık mobil uygulamaları ve verilen hizmetlerin çeşitliliği de artmıştır. Tablet, telefon gibi mobil cihazlara yüklenen bankacılık uygulamaları aracılığı ile giriş yapılan bu kanalda, günlük bankacılık işlemlerinin neredeyse hepsinin tek bir uygulama üzerinden yapılabilmesi sağlanmaktadır. Bankaların bu uygulamaları tüm platformlara ait **güvenli** uygulama marketlerinden indirilebilmektedir.

C) Telefon Bankacılığı (Çağrı Merkezi)

1996
Türkiye'de çağrı merkezlerin ilk kez hayata geçtiği tarih

Başta temel bankacılık hizmetleri olmak üzere, bankaların sunmuş olduğu ürün ve hizmetlere ilişkin olarak işlem yapılması ile bilgilendirme, pazarlama, yönlendirme, tahsilat işlemlerine telefonla aracılığı ile hizmet verilebilmektedir. Çağrı merkezi uygulamasına dünya genelinde ilk olarak bankacılık sektörünün geçtiği bilinmektedir. Günümüzde neredeyse tüm sektörlerde kullanılan çağrı merkezi hizmeti, ülkemizde bankacılık sektöründe ilk olarak 1996 yılında Citibank tarafından hayata geçirilmiştir.

Telefon ile arayan banka müşterilerinin kimlik doğrulama aşamalarından geçirildikten sonra bankacılık hizmeti verilmesidir.

Dijital cihazlarda verilen internet şube ve mobil uygulama hizmetleri ile birlikte çağrı merkezleri üzerinden verilen hizmetler azalmıştır.

D) ATM Bankacılığı

Otomatik para çekme işleminin yanı sıra diğer bankacılık işlemlerinin tamamının veya bir bölümünün gerçekleştirilmesine imkân veren elektronik işlem cihazıdır. İlk ATM (Automated Teller Machine) 1967 yılında Barclays Bank tarafından İngiltere'nin başkenti Londra da hizmete açılmıştır. Türkiye ilk ATM 1982 yılında Türkiye İş Bankası A.Ş. tarafından Bankamatik adı ile hizmete sunulmuştur.

Müşterilerin daha çok para çekme, yatırma gibi nakit ihtiyacını karşılamak amacıyla kullanılan ATM cihazları, son yıllarda diğer bankacılık hizmetleri (EFT, havale, fatura ödeme, vergi ödemesi, şifre edinimi gibi) için de sıkça kullanılan bir kanal haline gelmiştir.

Kartlı işlemlerin yanı sıra kartsız işlem menüsünden de hizmet veren ATM'lerde sadece ilgili bankanın değil diğer tüm bankaların (yurt dışı bankaları da dahil olmak üzere) kartları ile işlem yapılabilmektedir. Nakit çekim işlemleri kartlı menüden yapılabildiği gibi bankaların mobil uygulamaları kullanılarak Karekod doğrulaması ile de tamamlanabilmektedir.

E) Üye İşyeri (POS)

Ülkemizde ilk POS terminali 1991 yılında kullanılmaya başlanmış olup ödemelerin kredi kartı ya da banka kartı aracılığı ile yapılabilmesinin sağlandığı kanaldır. Fiziki ortamda alınan ödemelerde fiziki POS cihazları kullanılırken, internet ortamından yapılan alışverişlerde ve ödemelerde sanal POS uygulamaları kullanılmaktadır. Ayrıca son zamanlarda, mobil uygulama aracılığı ile POS ödemelerinin alınması da yaygınlaşmaktadır.

Günümüzde ise, mevcut yazar kasalar ile banka POS cihazları birleştirilmiştir. 01 Nisan 2016 tarihinden itibaren Yeni Nesil Ödeme Kaydedici Cihaz (ÖKC) kullanılması zorunlu hale gelmiştir.

POS kanalı aracılığı ile Karekodlu ödeme gibi alternatif ödeme yöntemleri de mevcut olup, belirlenmiş sektör limitlerine kadar olan işlemler için herhangi bir PIN girişi yapmadan temassız ödemeler kabul edilmektedir. Harcama belgelerinin elektronik ortamda düzenlenerek kâğıt kullanımında tasarruf edilmesi yönünde çalışmalar devam etmektedir.

BÖLÜM 2

Elektronik Bankacılık Kanallarında Karşılaşılan Dolandırıcılık Türleri

II. Elektronik Bankacılık Kanallarında Karşılaşılan Dolandırıcılık Türleri

A) Zararlı Yazılım Kaynaklı Dolandırıcılıklar

Zararlı yazılım, programlanabilir herhangi bir aygıta, hizmete veya ağa zarar vermek veya bunlardan yararlanmak üzere tasarlanmış her türlü kötü amaçlı yazılım için kullanılan kapsamlı bir terimdir. Siber suçlular genellikle bunu, mali kazanç için mağdurlardan veri elde ederek baskı yapmak üzere kullanır. Bu veriler finansal verilerden sağlık kayıtlarına, e-postalara ve parolalara kadar değişebilir.

Banka Müşterileri Gelişen teknolojiler ile ortaya çıkan Zararlı Yazılımların en büyük hedeflerindendir. Zararlı yazılım geliştiren kişilerce bu zararlı kodlar karanlık internet ağı olarak adlandırılan illegal dijital ortamlarda satılabilmekte ve bu kodları satın alan kişilerce dağıtılmaktadır.

Türkiye de Bankacılık sektöründe karşılaşılan zararlı yazılımlardan ilk olarak İnternet Bankacılığı Müşterileri etkilenmiştir. Buna yönelik BDDK tarafından 2008 yılında yürürlüğe giren Tebliğ ile bankaların sistemleri üzerinde gerekli tedbirleri almaları amaçlanmıştır. Değişen yöntemlere sektörel olarak önlemler alınabilmesi amacıyla 2020 yılında yeni Yönetmelik yürürlüğe girmiştir.

Zararlı Yazılım Türleri

Trojan atı genellikle bilgisayarla e-posta yoluyla bulaşır ve tespiti zordur.

İnternet bilgi hırsızları çeşitli yöntemlerle müşterilerin özel bilgilerini ele geçirmektedirler. Bu yöntemlerden en çok kullanılanlar aşağıda yer almaktadır:

1. Truva Yazılımları (Trojan)

Truva yazılımları ismini "Truva Atı"ndan almaktadır. Bir bilgisayar programına bağlanarak saklanan, tahribatını yaparken ise, programın olağan çalışmasına izin veriyormuş gibi gözüken virüslere "Truva atı" denir. Truva atları çoğunlukla, bulaştıkları bilgisayarlarda kullanılan şifre, kullanıcı adı gibi özel bilgileri ele geçirmek amacıyla kullanılır.

Tespit edilmesi oldukça zor olan Truva atı, genellikle sistemlere e-posta yoluyla bulaşmaktadır. Bunun dışında yoğun disklerden (cd), sayısal çok yönlü disklerden de (DVD), e-posta ekindeki (.jpg, .gif, .txt, .doc, .xls gibi) dosyalara, bilgisayar oyunlarındaki ".exe" uzantılı uygulama dosyaları gibi pek çok yere gizlenebilir.

2. Tuş ve Ekran Kaydediciler (Keylogger ve Screenlogger)

Tuş kaydediciler, bilgisayarda, klavye vuruşlarını anlık olarak kopyalayabilen ve bunları kaydederek e-posta yoluyla korsanın eline geçmesini sağlayan programlardır. Bu tür programlar klavye ile yazılan her şeyi kaydedebilme yeteneğine sahiptir. Elde edilen kayıtlar sistemde ".txt" uzantılı metin dosyası olarak tutulur. Yapıları itibariyle kurbanların her türlü şifre ve özel yazışmalarını ele geçirmek için kullanılabilir.

Ekran kaydediciler ise, ekran görüntülerini kopyalayan ve bunları e-posta ile saldırgana ulaştıran programlardır. Yakalanan anlık görüntüler sayesinde, o anda ekranda ne yapıldığı veya şifrelerin nereye yazıldığı kolaylıkla görünebilir. Tuş kaydediciler ve ekran kaydediciler dolandırıcılık eylemlerinde birbirlerini tamamlayan iki bileşen gibi çalışırlar.

3. Pop-Up Ekranlar

Bir arıza, geliştirme, erişim sorunu, yardım teklifi gibi içerikle kullanıcı karşısına çıkarılan ekranlara, kullanıcı kodu ve şifresi girilmesi istenerek erişim yetkileri çalınır.

Bu dolandırıcılık tipinde, kullanıcı bir pop-up mesajı ile makinesinde tespit edilen bir eksiklikten dolayı bazı programların çalışmayacağına dair bir mesaj çıkarır. Aynı mesaj kendisine "şimdi yükleyin" diye ücretsiz yardımcı bir program teklif eder.

4. Spam E-Postalar

Çoğu zaman istenmeyen mesajlar olarak adlandırılan bu elektronik postalar, içeriğinde zararlı yazılımlar taşıyabildiği gibi, zararlı yazılım yayan sitelere de yönlendirme yapabilmektedirler.

Özel bilgiler, teknolojik olanaklar kullanarak casusluk, dinleme gibi yöntemlerle ele geçirilebilir.

5. Teknolojik Donanımlar

Kötü niyetli kişiler, kurbana ait özel bilgileri teknolojik imkânlar kullanarak casusluk, dinleme gibi yöntemler ile ele geçirir. Özellikle kurumlarda çalışan temizlik hizmet personeli veya kurbana yakın görünen güvenini kazanabilen kötü niyetli kişiler, klavye kablosunun ucuna takacağı bir kopyalama aparatı (donanımsal keylogger) ile gün boyu çalışanın yazdıklarını veya ekranını kopyalayacak, bir sonraki temizlik gününde bilgiler şirket dışına çıkarılmış olacaktır.

Zararlı yazılımın hedefi kişinin kendine özel bankacılık işlemleri için kullandığı kişisel bilgileri ile kendisi tarafından belirlemiş olduğu şifrelerdir. Bu bilgileri ele geçiren dolandırıcının ayrıca müşterinin telefonuna giden tek kullanımlık SMS OTP bilgisini de ele geçirmesi gerekmektedir.

2021 yılı Ocak ayı itibariyle İnternet Bankacılığı kullanımı Mobil Uygulama onayına tabi tutulmuştur. Yeni Yönetmeliğe göre sadece mobil uygulamasını aktive etmemiş olan müşteriler SMS OTP ile işlemlerine devam edebilmektedirler.

Zararlı Yazılımdan Korunma Yöntemleri

Hediye, Reklam ve Haber Linkleri: Para veya hediye vaat eden kısa mesaj (SMS), sosyal medya reklamları, anlık haberleşme uygulamalarından gelen mesajları ve e-posta iletilerini açmayınız ve ilgili linklere tıklamayınız. E-posta ayarlarınız yaparken eklerin otomatik olarak açılmayacağından emin olunuz.

Uygulama Yükleme: Bilinen yaygın uygulamalar haricinde, güvenliğinden emin olmadığınız yeni uygulamaları yüklemeyiniz.

Resmî Kurum Uygulamaları: Mobil cihazınıza uygulama indirirken her zaman resmî uygulama mağazalarını kullanınız.

İnternette Seçicilik: İnternette ziyaret ettiğiniz siteler konusunda seçici olunuz.

Anti-Virüs: Sürekli yeni virüslerin piyasaya çıkması ve anti-virüs programının bu virüsleri tanımama ihtimaline karşı anti-virüs programını düzenli olarak güncelleyiniz.

Uygulama Yükleme Özelliği: Mobil cihazınıza bilinmeyen kaynaklardan uygulama yükleme özelliğinin kapalı olduğundan emin olunuz.

Erişim İzinleri: Mobil cihazınıza yüklediğiniz uygulamaların, erişmek istediği izinleri kontrol ediniz. Özellikle bilinmeyen kaynaklardan uygulama yüklenmesine ve telefonunuza ait yönetici izni (admin) isteyenlere izin vermeyiniz.

İşletim Sistemi: Mobil cihazlarınızın işletim sistemini güncel tutunuz.

Arama Motorlarından Giriş: Banka internet şubelerine arama motorlarını kullanarak giriş yapmayınız. Adres çubuğuna www.xxxbank.com.tr yazarak giriş yapınız.

Güvenlik Ayarları: İnternet ve mobil bankacılığı güvenlik ayarlarınızı ihtiyaçlarınız ve kullanım alışkanlıklarınız doğrultusunda belirleyiniz. (IP sınırlaması, saat sınırlaması, yurtdışı harcamaya kapama vb.)

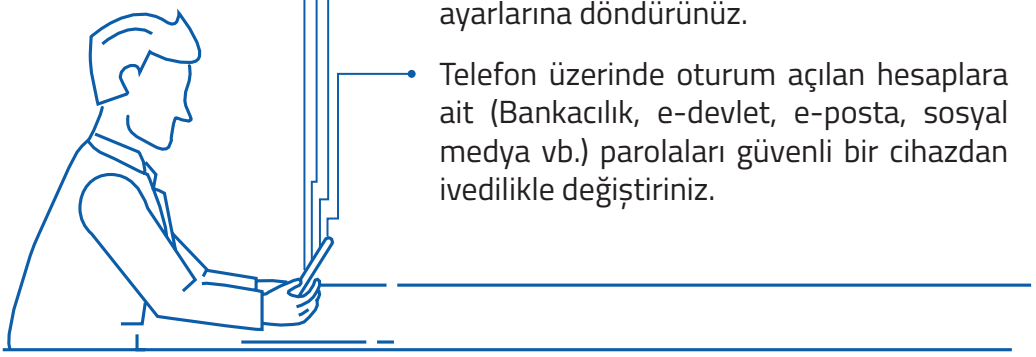
Halka Açık Bilgisayarlar: İnternet salonları, ortak kullanıma açık, iş yeri bilgisayarı gibi başkalarına ait ya da başkalarının erişimine açık bilgisayarlarda internet bankacılığı işlemi yapmayınız.

Zararlı Yazılım Şüphesi: Cihazda zararlı yazılım olabileceğinin şüphesi olması durumunda aşağıdaki durumların yaşanıp yaşanmadığı kontrol ediniz.

- Telefon veya tabletinizde herhangi bir nedeni olmadan aniden yavaşlama, donma, ya da aşırı ısınma,
- İndirilen uygulamanın kullanım amacı dışında çok sayıda izin istemesi,
- İşlem yapılmamasına rağmen pilde hızlı azalma,
- Kullanılan uygulamaların ya da uygulama sekmelerinin istem dışı kapanması,
- SMS bildirimlerinin gelen kutusunda görüntülenememesi.

Zararlı Yazılım Saldırısına Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler

Cihazınıza bulaşan zararlı yazılımdan ancak bu zararlı yazılımın silinmesi/temizlenmesi ile kurtulabilirsiniz. Zararlı yazılımın aktif olarak veri çalmaya devam etmesini engellemek amacıyla şunlar yapılmalıdır:



- Çok hızlı bir şekilde mobil cihazınızın internet erişimini engelleyiniz.
- Mobil cihazınızda bulunan SIM kartı çıkartınız.
- Kişisel bilgilerinizi yedekledikten sonra telefondaki zararlı yazılımın etkisiz hale getirilmesi için yetkili bir servise başvurunuz, ya da cihazınızı zararlı yazılım taraması sonrası yedekleyerek fabrika ayarlarına döndürünüz.
- Telefon üzerinde oturum açılan hesaplara ait (Bankacılık, e-devlet, e-posta, sosyal medya vb.) parolaları güvenli bir cihazdan ivedilikle değiştiriniz.

Senaryo 1

Dilek asgari ücret ile çalışan bir sekreterdir. Ortaya çıkan pandemi ile iş yerinde de sıkıntılar yaşamaktadır. Bu sıkıntılarını giderebilmek amacıyla devlet tarafından asgari ücretlilere verilmesi planlanan yardım paketine başvurmuştur.

Aradan geçen bir kaç haftadan sonra cuma günü kendisine gelen sms ile "**Pandemi destek için başvurunuz onaylanmıştır. Aşağıda yer alan link üzerinden talebinizi güncelleyebilirsiniz"** mesajını gördüğünde hemen linke tıklamış, link üzerinden cihazına herhangi bir güvenli uygulama marketine yönledirilmeksizin bir uygulama indirmiştir.

İndirilen uygulama sırasında istenen tüm izinlere onay vermiştir. Ancak tüm yönlendirmelere uyduğu halde herhangi bir bildirim almamış buna da şaşırmıştır. Hafta sonu gece geç saatte telefonunun ekran ışığının açıldığını fark etmiştir. Gün içerisinde de telefonu sürekli donmuş ve bir uygulamayı kullanabilmek için uzun süre beklemesi gerekmiştir. Telefonundaki bu anormallikleri cihazının eski bir model olmasına bağlamış artık bunun da ömrü tükendi diye düşünmüştür.

Pazartesi sabah iş yerine gittiğinde yeni bir sms almıştır. SMS de **"1.000 TL destek tutarınız GÜVEN BANK hesabına yatırılmıştır"** yazdığı için hiç vakit kaybetmeden bankasının mobil uygulamasına girmiştir. Ancak hesabına gelen herhangi bir tutar olmadığını gördüğünde sorunu işlerini hafiflettiği zaman araştırmaya karar vermiştir. İki saat sonra bankadan bir görevli kendisini arayarak, **30.000 TL'lik birikim hesaplarının bozdurulduğu ve bazı yüksek tutarlı fatura ödemeleri yapıldığını** belirtmiş ve işlemlerin kendisine ait olup olmadığını sormuştur. Dilek panikle böyle bir işlem yapmadığını belirtmiş, banka görevlisi ayrıca kendisi adına **Mobil Şube üzerinden 20.000 TL kredi kullanıldığını ve hesaplarına aktarıldığını** bu işlemin kendisine ait olup olmadığını sormuştur. Dilek böyle bir işlemden haberi olmadığını, hesaplarından hiçbir ödeme yapmadığını hatta mobil uygulamaya son iki saat içerisinde hiç girmediğini banka görevlisine anlatmıştır.

Banka görevlisi Dilek'e cep telefonu cihazında zararlı bir yazılım olabileceğini, telefonu kapatarak bu zararlının çalışmasını engellemesi gerektiğini, banka tarafından kendisine ulaşılabilecek başka bir numara vermesini istemiştir. Dilek banka görevlisine yanında çalışan arkadaşının telefon numarasını verdikten sonra cihazını hemen kapatmıştır. Banka görevlisi diğer numaradan Dilek' e ulaşarak hesaplarından yapılan ödeme işlemlerinin iptal edileceğini, kullanılan kredinin iptal edileceğini kendisinin en kısa sürede suç duyurusunda bulunarak belgelerini bankaya ulaştırması gerektiğini iletmiştir.

Dilek büyük panik içerisinde en yakın şubeye giderek hesaplarında bulunan bakiyeyi kontrol etmiş, yapılan ödemeler ve iptal edilen işlem detaylarını alarak savcılığa suç duyurusunda bulunmaya gitmiştir.

Senaryo 2

Yapı Limited Şirket yetkilisi Koray Bey'in masa telefonu çaldığı sırada kendisi bir faturanın onayı için bilgisayarının başındadır. Telefonu açtığında sekreteri, Güven Bank'ın Dijital Müşteri temsilcisinin kendisini aradığını iletir. Koray Bey sabah İnternet Şube üzerinden şirket hesaplarına gelen 500.000 TL ödeme işlemini teyit etmiştir. Telefondaki kişi kendisinin Güven Bank'ın Dijital Müşteri temsilcisi Burak olduğunu, bankalarının müşterilerine özel artık Dijital Müşteri Asistanı atadığını, kendisinin de Koray Bey'in firmasının Dijital Müşteri Asistanı olduğunu anlatır. Koray Bey, ben Şube ile görüşüyorum ilave bir ihtiyacım yok demesine karşın kendisini Dijital Müşteri Asistanı olarak tanıtan Burak Bey, evet biliyorum Şubede görevli Aliye Hanım sizin müşteri temsilciniz diyerek konuşmasını sürdürür.

Telefonda **Koray Bey'e bankasının Yapı Limited Şirketine özel hazırladığı bir kart teklifi olduğunu, 1 milyon TL limitli bu kart ile ticari harcamalarının hiçbir komisyon ödemeden 3 ay ertelemeli ekstreye yansıtılacağını** anlatır. Koray Bey'in teklif edilen kartın kullanım şekli dikkatini çekmiştir. Teklifi kabul ettiğini söyler, hemen arkasından Burak Bey, Koray Bey'e kendisine bir SMS gönderdiğini ve kart tanımları için bu bilgiyi kendisine okuması gerektiğini belirtir. Koray Bey gelen SMS içeriğine dikkat etmeksizin gördüğü 6 haneli şifreyi Burak Bey'e okur. Daha sonra gelen 2 SMS şifreyi de Burak Bey ile paylaşır. Bu esnada Koray Bey'in cep telefonu numarasına 0850 222 XX XX numaralı banka hattından bir arama gelmiştir. Koray Bey zaten bankanın Burak Bey ile görüştüğü için telefonunun sesini kısarak yanıtlamamıştır.

Telefonuna bu kez şubede bulunan müşteri temsilcisi tarafından bir arama gelir. Koray Bey telefonunu yanıtlar. Şube müşteri temsilcisi Aliye Hanım, hesaplarından yüksek tutarlı iki adet para transferi gerçekleştirildiğini, genel müdürlük birimleri tarafından kendisinin arandığını bu işlemleri Koray Bey'in yapıp yapmadığını teyit etmek istediğini belirtir. Koray Bey büyük şaşkınlık içerisinde kesinlikle işlemleri yapmadığını ve bankanın Dijital Müşteri Temsilcisi ile yaptığı görüşmeyi anlatır. Aliye Hanım bu kişilerin dolandırıcı olduğunu, firma hesaplarına giriş yaparak yüksek tutarlı para transferlerini onların gerçekleştirmiş olabileceklerini anlattığında Koray Bey büyük panik yaşar. Daha sonra Koray Bey masaüstü bilgisayarını teknik ekiplerine incelettiğinde daha önce gelen spam e-postayı açması sonucunda cihazına zararlı bir yazılımın yüklendiği, kendisinin yapmış olduğu her türlü işlemin bu zararlı yazılım üzerinden dolandırıcılara gittiğini öğrenir.

Senaryo 3

Can cafede çalışan bir servis görevlisidir. Pandemi sebebi ile işyeri kapandığından, vaktini evde internete girerek geçirmektedir. Bu nedenle Can'ın mobil internet kullanımı artmış ve internet paketi yetersiz gelmeye başlamıştır. Yine sosyal medyada vakit geçirdiği esnada telefonuna gelen **"Tüm vatandaşlarımıza Covid-19 sebebi ile #EvdeKal içinde tüm operatörlerde geçerli 10 GB dağıtma kararı alındı. Hemen indir kur hattına tanımlansın"** mesajı ile hemen linke tıklamış ve telefonuna güvenli uygulama marketine yönlendirilmeksizin bir uygulama indirmiştir. Uygulamanın yüklenmesi esnasında tüm izinlere onay vermiştir. Tüm bu onaylara istinaden hediye internet paketi tanımlanmamıştır.

Can bu durumun yoğun talepten olabileceğini düşünerek beklemeye başlamıştır. Gün içerisinde telefonunda donmalar meydana gelmiş, ekranı kendi kendine kapanmış, bunu telefonun donanımsal özelliklerinin zayıf olmasına bağlamıştır. Ertesi gün kısa çalışma ödeneğinin yatıp yatmadığını kontrol etmek için kullandığı bankanın mobil bankacılık uygulamasını açmıştır. Öncekilerden farklı olarak uygulamada bu sefer kart bilgilerini istemiştir. Can bu duruma bir anlam verememiş olmasına rağmen önce kart bilgilerini, ardından dijital bankacılık bilgilerini uygulamaya girmiştir.

Kısa çalışma ödeneğinin yattığını görünce uygulamadan çıkış yapmıştır. Yarın sabah gider paramı çekerim diyerek telefonunu şarja takmış ve uyumuştur. Sabah telefonun çalması ile uyanmıştır. Arayan banka görevlisi gece boyunca kartı ile 3D işlemler gerçekleştirildiğini ve dijital bankacılığı üzerinden de kredi başvurusunda bulunularak para transferi gerçekleştirilmek istendiğini söyleyince Can kısa bir şaşkınlığın ardından bu işlemlerin kendisi tarafından yapılmadığını banka görevlisine söylemiştir.

Banka görevlisi bunun üzerinde Can'a **telefonunda zararlı yazılım olabileceği bilgisini vererek telefonu kapamasını, hattını farklı bir cihazda kullanmasını ve banka şubesinden işlemlerin detayını alarak savcılığa suç duyurusunda bulunarak belgeleri en kısa zamanda bankaya ulaştırması gerektiğini** iletmiştir.

Zararlı Yazılım / Uzaktan Kontrol

Uzaktan Kontrol yani bir cihaza uzaktan erişim, bulunduğunuz yerden bağımsız olarak internet üzerinden bilgisayarınıza ve/veya mobil cihazınıza bağlanmanızı ve yönetmenizi sağlayan ve özel protokoller üzerinden işleyen uygulamalardır.

Uzaktan erişim sağlanacak cihazın aktif ve çalışır durumda olması gerekmektedir. Uzaktan erişim sürecinde iki bilgisayar arasında kriptolu bir iletişim kurulmaktadır.

Son dönemde müşteri cihazlarına dolandırıcı kişilerce uzaktan kontrol edebilmek için zararlı yazılım ve/veya sosyal mühendislik yöntemlerinin kullanıldığı vakalara oldukça sık rastlanmaktadır.

Senaryo 1

Ahmet 48 yaşında, iki çocuk babası, lise matematik öğretmenidir. Son dönemde pandemi nedeniyle uzaktan eğitim vermekte ve çok da aşina olmadığı dijital ortamlarda bir takım uygulamaları indirmektedir. Kullandığı cihazın birazda eski olması nedeniyle bazen dersler sırasında bağlantısı donmakta ve bu zamanlarda kendisini yetersiz hissetmektedir.

O gün aldığı e-posta da cihazına hız kazandıracak bir web adresi olduğuna dair gördüğü reklam onun için umut olmuştur. Hemen ilgili adrese girerek istenen tüm izinleri onaylamıştır. Ancak yapılan tüm yönlendirmelere harfiyen uymasına rağmen bilgisayarı bu sefer tamamen kilitlenmiş ve uzun süre hiç kullanamamıştır.

Aradan geçen iki saatin sonunda bankadan bir görevli hesaplarından yapılan 40.000 TL'lik para transfer işleminin kendisine ait olup olmadığını sormuştur. Ahmet bu soru karşısında paniklemiş ve kesinlikle kendisinin böyle bir işlem yapmadığını işlemi durdurmaları gerektiğini belirtmiştir.

Bankadan aradığını söyleyen şahıs, Ahmet'e telefonuna bir şifre geleceğini kendisine okuması gerektiğini söylediğinde, Ahmet gelen şifreyi hiç tereddüt etmeden okumuştur.

Telefonda görüştüğü banka görevlisi işlemin iptal edildiğini endişe edecek bir durum olmadığını belirtmiş ve telefonu kapatmıştır. Ahmet'in bilgisayarı on dakika sonra normale döndüğünde hemen İnternet üzerinden banka hesaplarını kontrol etmiş ve hesabından 75.000 TL para transfer edildiğini görmüştür. Hemen banka çağrı merkezini arayarak yapılan işlemin iptal edilmesini bu işlemin kendisi tarafından yapılmadığını anlatmıştır.

Ancak banka çağrı merkezi görevlisi işleme ait SMS şifrenin kendi numarasına gönderildiği ve bu şifre ile işlemlerin gerçekleştirildiğini belirtmiştir. Ahmet telefonunu eline aldığında on dakika önce kendisini banka görevlisi diye tanıtan kişiye okuduğu SMS şifre mesajının 75.000 TL'lik para transferinde kullanıldığını görmüştür.

Banka ile yaptığı görüşmeyi bitirdikten sonra kendisine yakın olan mahalle karakoluna giderek şikâyetçi olmuştur. Daha sonra kendisini arayan banka görevlisi giden paranın alıcı hesapta tutulduğunu ve şikâyet dilekçesini kendilerine iletmelerini istemiştir. Ayrıca hesabından çıkan paranın kendisine geri ödenebilmesi için mahkemeden karar çıkartması gerektiğini de öğrenmiştir.

Senaryo 2

Evinde emekliliğinin tadını çiçekleri ve torunları ile geçiren Ayşe teyzeye beklenmedik bir arama gelmiştir. Ayşe teyze telefonu açtığında kendisini ABC Bank'ın müşteri temsilcisi olarak tanıtan Ahmet ile konuşmaya başlamıştır.

Müşteri temsilcisi Ahmet, Ayşe teyzenin hesabından 5.000 TL ve 7.000 TL tutarında para transferlerinin gerçekleştiğini bu işlemlerin kendine ait olup olmadığını sormuştur. Ayşe teyze paniğe kapılarak işlemlerin kendisine ait olmadığını büyük bir üzüntü ve telaş içerisinde hesabından böyle bir işlem yapmadığını iletmiştir.

Bunun üzerine Ahmet Ayşe teyzeye üzülmemesini, sakin olmasını ve tutarların hesabına iade edilmesi için kendisine yardımcı olacağını ileterek güven kazanmıştır. Ahmet Ayşe teyzeye telefonunun uygulama mağazasından quicksupport adlı uygulamayı indirmesi durumunda hesabından çıkan tutarların kendisine iade edebileceğini iletmiştir. Bunun üzerine Ayşe teyze torunu Sude Naz'ın yardımı ile uygulamayı indirip Ahmet' in yönlendirmesi ile tüm izinleri onaylamıştır. Daha sonra telefonun diğer ucundaki Ahmet Ayşe teyzeden mobil bankacılığına girmesini istemiştir.

Uygulama indirilip mobil bankacılığa girildikten sonra tüm kontrolü ele geçiren Ahmet Ayşe teyzenin hesabındaki yüklü miktardaki birikimini farklı hesaplara transfer etmiştir, ayrıca Ayşe teyzenin ön onaylı 50.000 TL tutarındaki kredisini de kullanıp hesabına aktarmış ve bu tutarları da yine 3 farklı hesaba transfer etmiştir.

Birkaç saat sonra durumu kızı Nazan' a anlattığında, Nazan şüphelenerek annesi ile birlikte banka şubesine giderek durumu şubedeki gişe personeline anlatmıştır. Şube personeli hesapları kontrol ettiğinde Ayşe teyzenin hesaplarının boşaltıldığının hesabındaki 80.000 TL'nin yanı sıra 50.000 TL tutarında kredi kullanıldığını ve tutarların birden fazla hesaba transfer edildiğini iletmiştir. Ayşe teyze hemen en yakın savcılığa giderek şubeden aldığı dekontlardaki alıcılar hakkında suç duyurusunda bulunmuştur.

> …en büyük tehlike siz olabilirsiniz. Şahsen, insanı yanıltmanın teknolojiyi yanıltmaktan daha kolay olduğunu gördüm…
>
> *Kevin Mitnick – Bilgisayar Korsanı*

B) Sosyal Mühendislik Temelli Dolandırıcılıklar

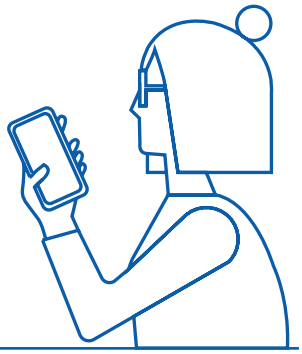
Tüm sosyal mühendislik yöntemleri, insan davranışlarındaki önyargılar üzerine kurgulanır. Bu önyargılar insana dair "sistem açıkları" olarak da tanımlanabilir. Bu yöntemleri kullanan kişi, insan davranışlarında etkili olan önyargıları harekete geçirecek yöntemleri büyük bir beceri ile kullanabilen kişidir.

"…en büyük tehlike siz olabilirsiniz. Şahsen, insanı yanıltmanın teknolojiyi yanıltmaktan daha kolay olduğunu gördüm…" (Kevin Mitnick – Bilgisayar Korsanı)

Sosyal mühendislik yöntemlerini kullanan dolandırıcılar, kişi ve kurumlara ait bilgi ve materyalleri (fiziki, sistemsel çevreleri, organizasyonel yapıları, kullanıcı kod ve şifreleri, çalışma koşulları, iş akışları, güvenlik organizasyonu vb. materyalleri) teknolojiyi kullanarak ya da kullanmadan, haksız çıkar elde etmek amacıyla ele geçirme yöntemleri ve organizasyonlarıdır.

Sosyal mühendisliğin temeli kandırmaya dayanır. Sosyal mühendislik vakası karşı tarafı kandırma ve yanıltma yoluyla bilgilerin ele geçirildiği andan itibaren, elde edilen haksız çıkar da dâhil olmak üzere sürecin tamamını ifade eder.

Aşağıdaki senaryolar, insanların karar verme becerilerini etkileme (manipüle etme) amacıyla en çok kullanılan yöntemlerdir:



Otorite korkusu "emniyetten arıyoruz", "terör örgütü ile bağlantınız tespit edilmiştir", "tehdit mesajı atmışsınız..."

Yardımcı olma arzusu "derhal..."

Zafer kazanma duygusu "ödül kazandınız" mesajları...

Tembellik "işlemler için şubeye gelemeyecekseniz, biz buradan hemen yapalım siz zahmet etmeyin..."

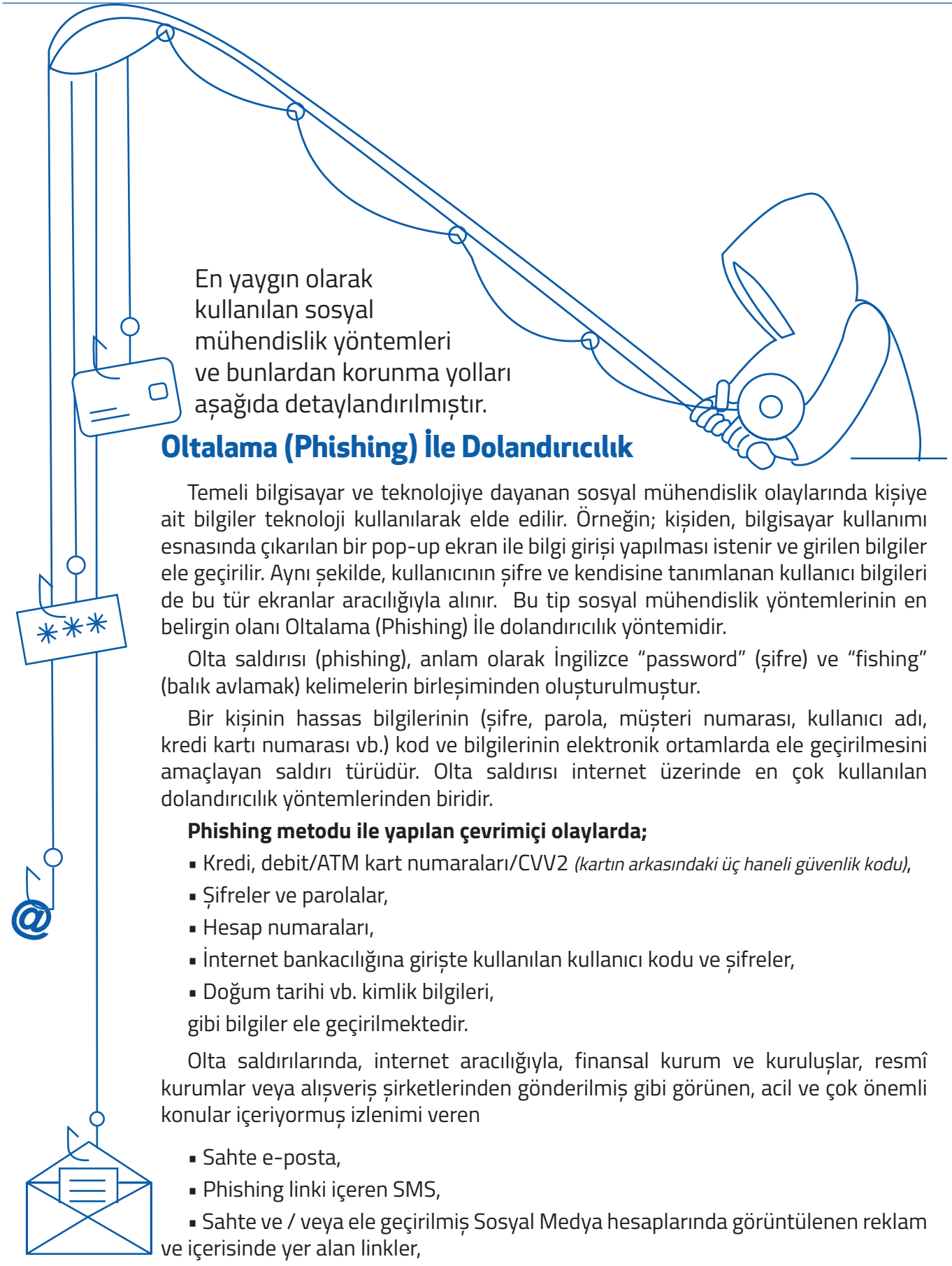
Değer verilme arzusu; ego "sizin gibi değerli bir çalışan ile iş yapıyoruz, şahsi numaranızı alabilir miyim?"

Vaadcilik "kredi kart aidatı ve kredi dosya masraflarını alırız..."

Güvenlik endişesi "hesabınızdan bilginiz dışında işlemi iptal etmek için şifrenizi paylaşır mısınız?"

Yetersiz bilgi: "Kart numaramı versem ne olacak ki?"

Kaybetme korkusu:
"Bu fırsat sadece bugün için sunulmuştur..."



En yaygın olarak kullanılan sosyal mühendislik yöntemleri ve bunlardan korunma yolları aşağıda detaylandırılmıştır.

Oltalama (Phishing) İle Dolandırıcılık

Temeli bilgisayar ve teknolojiye dayanan sosyal mühendislik olaylarında kişiye ait bilgiler teknoloji kullanılarak elde edilir. Örneğin; kişiden, bilgisayar kullanımı esnasında çıkarılan bir pop-up ekran ile bilgi girişi yapılması istenir ve girilen bilgiler ele geçirilir. Aynı şekilde, kullanıcının şifre ve kendisine tanımlanan kullanıcı bilgileri de bu tür ekranlar aracılığıyla alınır. Bu tip sosyal mühendislik yöntemlerinin en belirgin olanı Oltalama (Phishing) İle dolandırıcılık yöntemidir.

Olta saldırısı (phishing), anlam olarak İngilizce "password" (şifre) ve "fishing" (balık avlamak) kelimelerin birleşiminden oluşturulmuştur.

Bir kişinin hassas bilgilerinin (şifre, parola, müşteri numarası, kullanıcı adı, kredi kartı numarası vb.) kod ve bilgilerinin elektronik ortamlarda ele geçirilmesini amaçlayan saldırı türüdür. Olta saldırısı internet üzerinde en çok kullanılan dolandırıcılık yöntemlerinden biridir.

Phishing metodu ile yapılan çevrimiçi olaylarda;

- Kredi, debit/ATM kart numaraları/CVV2 *(kartın arkasındaki üç haneli güvenlik kodu)*,
- Şifreler ve parolalar,
- Hesap numaraları,
- İnternet bankacılığına girişte kullanılan kullanıcı kodu ve şifreler,
- Doğum tarihi vb. kimlik bilgileri,

gibi bilgiler ele geçirilmektedir.

Olta saldırılarında, internet aracılığıyla, finansal kurum ve kuruluşlar, resmî kurumlar veya alışveriş şirketlerinden gönderilmiş gibi görünen, acil ve çok önemli konular içeriyormuş izlenimi veren

- Sahte e-posta,
- Phishing linki içeren SMS,
- Sahte ve / veya ele geçirilmiş Sosyal Medya hesaplarında görüntülenen reklam ve içerisinde yer alan linkler,
- Arama motorlarından yayınlanan kampanyaları içeren linkler

aracılığı ile yayılır.

Oltalama (Phishing) İle Dolandırıcılık Türleri

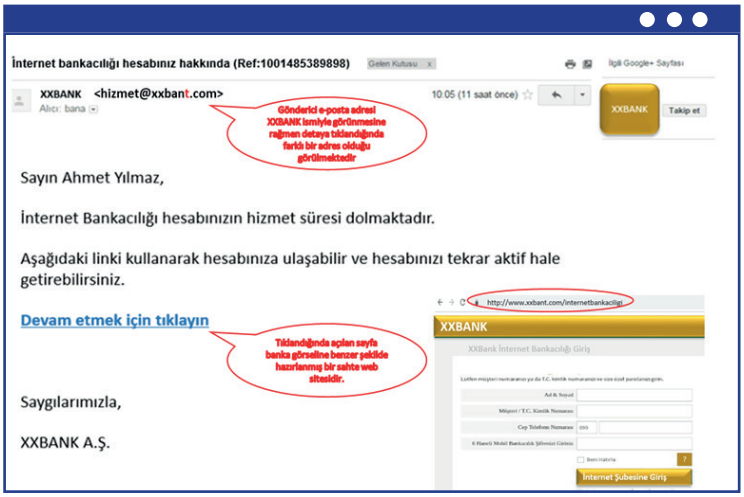
1. Sahte E-posta

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. Örnek vermek gerekir ise;

"Tarafınıza x adlı kişiden y tutarında para transferi yapılmıştır. Lütfen aşağıdaki linke tıklayarak, internet bankacılığınıza giriş yapın ve bilgilerinizi kontrol edin" gibi ifadeler içeren e-postalar gönderilir.

"Eğer internet bankacılığına girerek işlemi onaylamazsanız para transferi gerçekleştirilmeyecektir" gibi tuzağa düşürücü anlatımlar da bulunabilir.

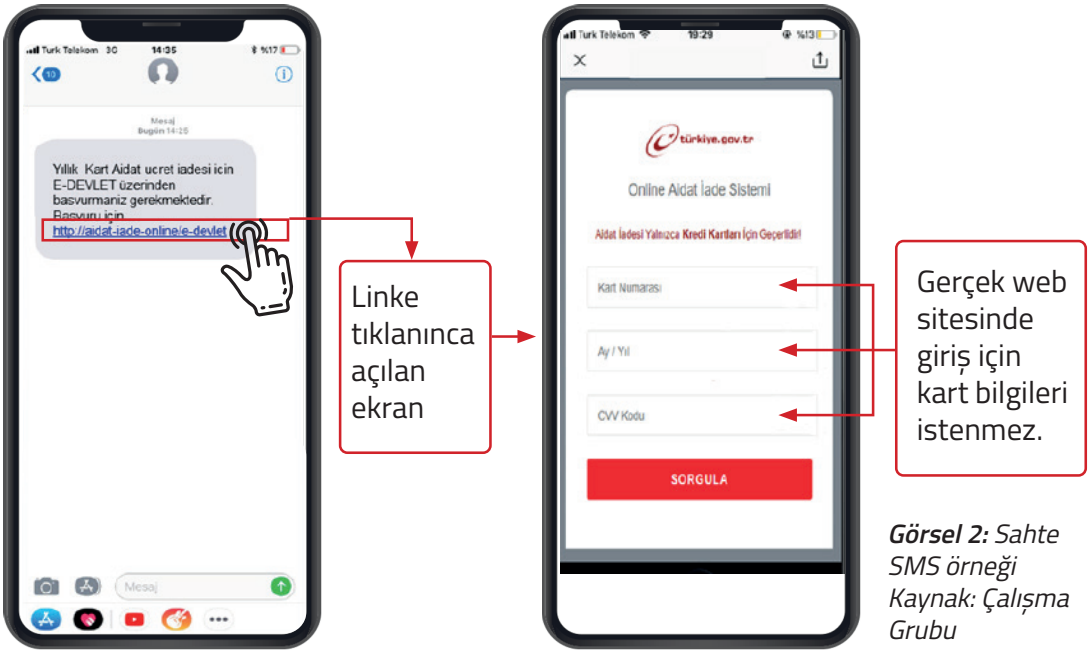
Bu mesajlarda kişilerin; şifre, parola, müşteri numarası, kullanıcı adı, kredi kartı numarası ve kodları sanki kurum tarafından isteniyormuş gibi yazılır. Bu e-postalarda verilen linklere tıklayıp, kişisel bilgilerini ekrana giren kullanıcı bu sitelerin gerçek siteler olmadığını fark etmemekte ve özel bilgileri çaldırmaktadır.



Görsel 1: *Sahte e-posta örneği*
kaynak: Çalışma Grubu

2. Oltalama Linki İçeren SMS ve Diğer Anlık Haberleşme Uygulamaları

Dolandırıcılar ele geçirdikleri telefon numaralarına SMS ler ve diğer anlık haberleşme iletileri ile ödül, kart aidat iade gibi çeşitli vaatlerde bulunmak suretiyle oltalama amaçlı açılmış site adreslerini iletirler. Banka adresi gibi gösterilen oltalama sayfasına giren müşteri İnternet Bankacılığı bilgilerini bu sayfaya girdiği anda, dolandırıcı müşteri ile eş zamanlı olarak müşterinin ilgili bankadaki hesaplarına erişim sağlar.



Görsel 2: *Sahte SMS örneği Kaynak: Çalışma Grubu*

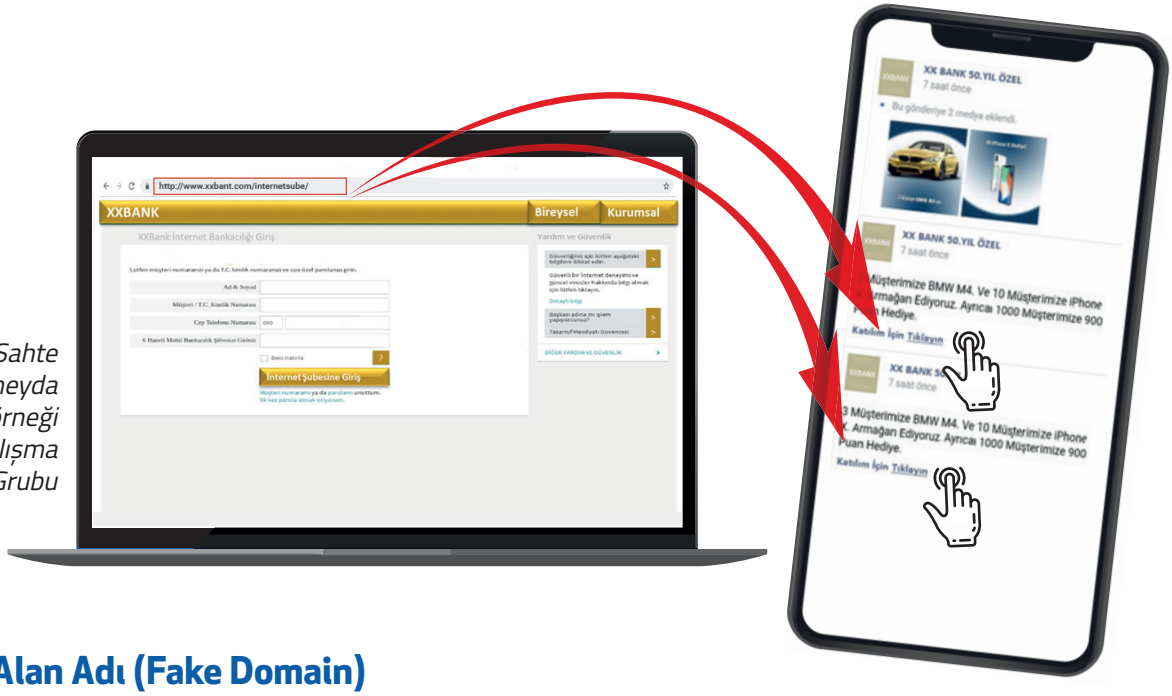
3. Sahte ve/veya Ele Geçirilen Sosyal Medya Hesapları Üzerinden Verilen Reklamlar

Daha çok finansal kurumlar ve resmî kurumların görselleri kullanılarak tamamen sahte bilgiler ile dolandırıcılık amacı ile açılmış veya gerçek bir kişiye ait kullanıcı bilgileri ele geçirildikten sonra dolandırıcılık amaçlı kullanılmaya başlanmış sosyal medya hesapları üzerinden çeşitli reklamlar ya da ödül/vaatlerde bulunularak kişilerin bu yayınların altında bulunan oltalama sayfalarına girmeleri sağlanmaktadır.

Görsel 3: *Sahte internet sitesi örneği kaynak: Çalışma Grubu*

Dolandırıcılığı gerçekleştirecek kişi(ler) olta saldırısı yöntemi ile edindikleri bilgileri kullanarak müşterilerin banka hesaplarına erişmekte ve varlıklarını ele geçirmektedir. Ele geçirilen hesaptan paranın çekilmesi aşamasında, daha az şüphe çekebilecek üçüncü kişiler kullanılır.

Para çekme işlemlerinde kullanılan üçüncü kişiler internet üzerinden sahte iş ilanları yoluyla bulunduğu örneklerle karşılaşılabilmektedir. Bu kişilere menfaatler karşılığı görevler verilir. İş ilanlarında çaba harcamadan kolay para kazanılacağı şeklinde bilgi verilir, başvuruda bulunan kişilerin hesap bilgileri alınır ve bu kişilere ait hesaplar kullanılarak olta saldırısı yöntemi ile ele geçirilen hesaplardan para transferi yapılır. Bu yöntemle, müşteri ve hesap bilgilerini ele geçiren ve dolandırıcılık olayının asıl faili olan kişiler kimliklerini gizler ve aracı olarak kullandıkları üçüncü kişilere suçu yükleyerek zaman kazanmış olurlar.

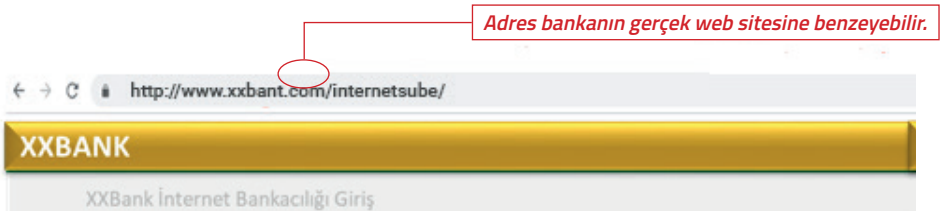


Görsel 4: *Sahte sosyal meyda kampanya örneği*
Kaynak: Çalışma Grubu

4. Sahte Alan Adı (Fake Domain)

Kurumların web site adreslerine benzer şekilde oluşturulmuş alan adlarının edilinerek müşterilerin oltalama amaçlı bu sitelere yönlendirilmesi hedeflenmektedir. Örneğin bilinen adı **www.xxbank.com** olan bir alan adının **www.xxbant.com** olarak kullanımı sahte siteye güçlü bir işarettir.

Firmanın markanın ismini yayması, tanıtması çok büyük bir emektir. Durup dururken bunu farklılaştırılması mantığa uygun değildir.



Görsel 5: *Sahte alan adı örneği*
Kaynak: Çalışma Grubu

Oltalama Saldırılarından Korunma Yöntemleri

Sosyal medya üzerinden kart aidatı/sigorta iadesi, ödül kazandırma gibi vaadler ile, banka ya da resmî kurum logosu kullanarak kart bilgilerinizi ve şifrelerinizi ele geçirmeyi amaçlayan, sahte kampanya mesajlarına itibar etmeyiniz. Bu mesajlardaki linklere tıklamayınız.

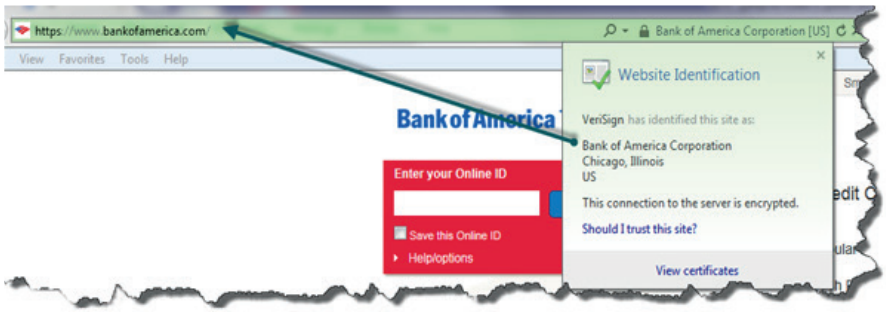
Tanımadığınız ve güvenmediğiniz göndericilerden gelen e-posta ve mesajlardaki bağlantıları açmayınız. Karşınıza çıkan web sitesi linklerine tıklamadan önce doğruluğunu, harf hatalarını, kampanya bilgilerini kontrol ediniz. İnternet/mobil bankacılık girişlerinde kullanılmayan cep telefonu, kart numarası, CVV2 gibi bilgiler sahte sitelerde sıkça istenir. Bu bilgileri kesinlikle girmeyiniz.

Tanıdığınız kişilerden, resmî kurumlardan geliyor gibi görünse de, zamanlaması ve içeriği bakımından beklenmeyen, güven vermeyen mesajlar, e-posta iletilerine de dikkat ediniz, bunlarda yer alan linklere tıklamayınız.

SSL (Secure Socket Layer) sertifikası ile korunan sitede sertifika kilidinin olup olmadığına dikkat ediniz

Zorunlu olmadıkça internet bankacılığı hesabınıza, bankanın resmî web sitesinde yer alan "İnternet Şube" butonuna tıklayarak giriş yapınız. İnternet bankacılığı hesabınıza, arama motorları üzerinden giriş yaptığınızda ya da SMS, e-posta, farklı web siteleri üzerinden yönlendirildiğinizde, bilgilerinizi girmeden önce internet tarayıcınızın adres çubuğunda doğru adresin yazdığından emin olunuz.

Sürekli kullanılan ve SSL (Secure Socket Layer) sertifikası ile korunan sitede sertifika kilidinin olup olmadığına dikkat ediniz. SSL sertifikasının görsel olarak olması durumunda bile, sertifikanın kimin ismine verildiği ve o an hangi sitenin içinde olduğunuzu karşılaştırınız. SSL tek başına web sitesinin tamamen güvenliği olduğu anlamına gelmez bilgilerinizi girmeden önce bu başlık altında yer alan diğer uyarıları da dikkate alınız.



Görsel 6: *Sahte internet sitesi örneği*

Kaynak: TBB – Dolandırıcılık Rehberi (Aralık 2015)

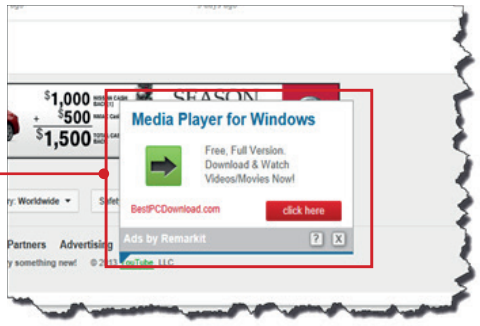
Bir sitedeki kullanıcı adı/şifre gibi özel bilgilerin sorulduğu formlar ile ilgili olarak kuşku oluşması durumunda, yanlış bir kullanıcı adı ve parolası ile sisteme, iki kere hatalı girilmesi denendiğinde, genelde sahte siteler kuşku uyandırmamak amacıyla doğru siteye yönlendirirler. Bu şekilde yönlendirme yapan sitelere bilgilerinizi girmeyiniz.

Giriş yapmış olduğunuz web sitesinin adres çubuğu üzerinde sağ tıklayarak (klik) özellikler (properties) seçeneğinde yer alan görsel ile site ismi ile aynı olup olmadığını karşılaştırınız.

İsim benzerliğinden faydalanarak sahte e-posta tespiti yapılabilir, ancak çoğu zaman kötü niyetli kişi elektronik posta adresini birebir yazdırabilmektedir. Bilinçli bir kullanıcı e-posta ile talep edilen şahsına ait bilgileri vermekten uzak durur. Mesela, bir banka müşterilerinden özel bilgilerini e-posta vasıtasıyla istemez.

Değerinin çok altında bir satış bedeli ile ilana çıkmış ürünler için iletilen linklerden uzak durunuz. Tanımadığız ve güvenliğinden emin olmadığınız web sitelerine kart numarası, güvenlik kodu, kişisel bilgilerinizi ve şifrelerinizi girmeyiniz.

UYARI



İnternet ortamında karşınıza çıkan güvenliğinden emin olmadığınız Bannerlar (Afiş), reklamlar, pop-up ekranlara tıklamayınız. Tıklamanız durumunda açılan sayfalara bilgilerinizi girmeyiniz.

Görsel 7: *Sahte reklam örneği Kaynak: TBB – Dolandırıcılık Rehberi (Aralık 2015)*

Sahte Site Örnekleri

Aşağıda bazı sahte site örnekleri görsellerinden de anlaşılabileceği gibi genel olarak, kullanıcıları kandırabilmek için sanki resmî, yasal bir site izlenimi verebilmek amacıyla banka logoları, benzer alan adları kullanılabilmektedir. Bu tarz sahte sitelerin hepsinin ortak noktası, bir şekilde kullanıcıyı tuzağa düşürmek suretiyle, kullanıcının özlük bilgileri veya finansal bilgileri ile kredi kartı bilgilerinin ele geçirilmek istenmesidir.

Görsel 8-9: *Sahte bir internet sitesi örneği*

Kaynak: TBB – Dolandırıcılık Rehberi (Aralık 2015)

Oltalama Saldırısına Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler

1. Bankacılık bilgilerinizi sahte bir siteye girdiğinizi farketmeniz durumunda vakit kaybetmeden şifrenizi değiştiriniz, hesap/kart hareketlerinizi kontrol ederek bankanızı arayınız.

2. Çalıştığınız kurum e-posta adresinize gelen ve sahte siteye yönlendiren link içeren bildirimleri vakit kaybetmeden kurumunuzun teknik ekiplerine bildiriniz. Link üzerinden banka kullanıcı, şifre bilgisi girişi yaptıysanız bankanız ile iletişime geçiniz.

Senaryo 1

Pandemi döneminde yaşanan ekonomik durumlardan dolayı işten çıkarılan Elif evinde bir yandan iş ilanlarına bakıyor bir yandan da yine internet üzerinden, pandemi sürecinde işten çıkarma vakalarına göz atıyor ve durumun etkilerine bakıp haklarını almanın yollarını araştırıyordur.

Aynı günün sonuna biraz kafa dağıtmak için girmiş olduğu sosyal paylaşım sitesi üzerinde günlük paylaşımlara göz atarken birden karşısına Cumhurbaşkanlığı logosu olan ve devletin pandemi sürecinde işten çıkarılanlara sağlamış olduğu ödenek üzerinden pay dağıtımı yapmaya başlandığı bilgisini içeren bir metin ve devamında da içeriği e-devlet olan bir link çıkmıştır. Karşısına çıkan linki kendisine maddi bir ek gelir olur umuduyla tıklayan Elif, girdiği sitenin güvenli olduğuna kanaat getirmiş ve açılan sayfada istenen tüm internet bankacılığı bilgilerini yazmış ve sonrasında hesabına para geleceğine dair umuduyla biraz daha rahatlamıştır. Tam o sırada çalan telefonunu açtığında, banka güvenlik biriminden arayan Yusuf, Elif'in hesabından kredi kullanıldığını ve kullanılan kredi tutarından hesaba geçen miktarın başka birine gönderilmeye çalışıldığını söyleyerek bu işleme onayının olup olmadığını sormuştur.

Hemen telaşa kapılan Elif kesinlikle hiçbir işlem yapmadığını ve işlemi onaylamadığını belirtmiştir. Yusuf da hemen her gün karşılaştığı bu vakanın nasıl olduğunu anlamak için Elif'e; "sizi gün içinde arayan işlem yaptırmaya çalışan oldu mu? Ya da internet üzerinden herhangi bir sayfada bilgi paylaşımı sağladınız mı?" diyince Elif durumu anlamıştır. Kendisine maddi bir ek kaynak sağlamak umuduyla bilgi girişi sağladığı, e-devlet sayfası olduğuna inandığı sayfanın aslında dolandırıcılar tarafından hazırlanmış bir sahte site olduğunu, son anda banka güvenlik biriminin uyarısıyla maddi zarara dönüşmeden önlendiğini tecrübe etmiştir.

Senaryo 2

Erdi; o gün işin tüm yoğunluğunu ofiste bırakmıştır, artık alıştığı trafiğin kalabalığına bile aldırış etmeden otoban gişelerine kadar gelmiştir. Gişe çıkışında polislerin rutin yapmış oldukları kontrole denk gelmiş ve kendinden emin şekilde ehliyetini ruhsatını vermiştir. Yapılan kontrol sonrası kendisini yanına çağıran Polis Memurunun; **"Aracınızın muayenesi eksik görünüyor. Cezai işlem yapacağız"** uyarısıyla adeta şaşkına dönmüştür.

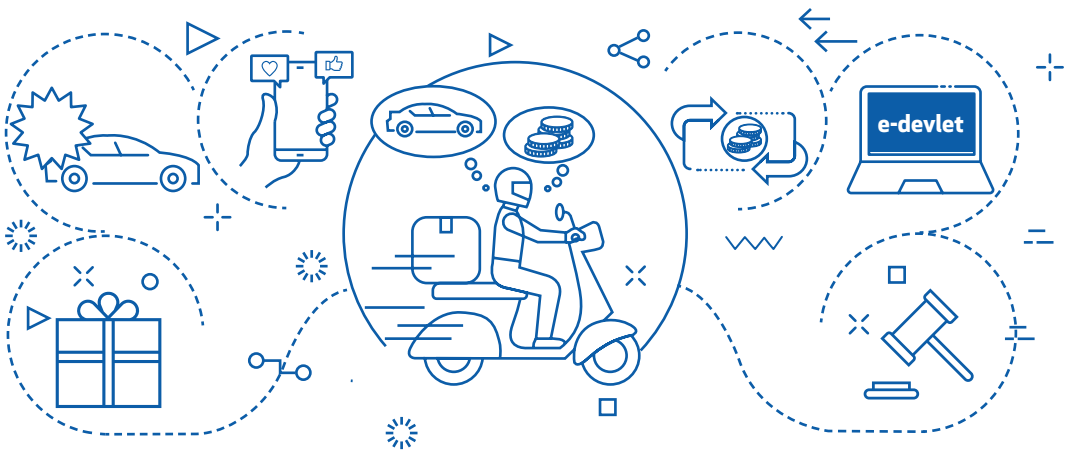
Ceza yediğine mi yansın araç muayenesini unutmuş olduğuna mı bilemeden evine gelip kendini koltuğa atar atmaz hemen muayene randevusu olmak için internete girip arama motoruna araç muayenesi yazdıktan sonra gelen ilk muayene içerikli linki tıklamıştır.

Daha önce böyle bir işlem yapmadığı için karşısına çıkan ekranlarda istenen kart numarası, kart güvenlik kodu (CVV2) ve kimlik bilgileri içeren alanlar kendisinde herhangi bir şüphe uyandırmadı ve tereddüt etmeden bu bilgileri web sitesine girmiştir. Girmiş olduğu sahte web sitesi üzerinden randevu işlemlerini yaptığını düşünen Erdi kendisine gelen bildirimlerde kredi kartından yapılan harcamaları görünce hemen bankasını aradı ve yapılan işlemlerin, biraz önce vermiş olduğu bilgilerle dolandırıcılar tarafından yapıldığını öğrenmiştir. Erdi, dikkatsizliğinin faturasını biraz ağır ödemiştir.

Senaryo 3

Harun, 25 yaşında pizzacıda çalışan bir kuryedir. Yorucu ve kısıtlı imkanlarına rağmen her ay kenara ayırdığı parasıyla internet bankacılığı üzerinden altın almakta ve hayalini kurduğu orta seviyede arabanın peşinatı için birikim yapmaktadır. Bir gün yemek molasından sonra sosyal medya platformuna giriş yaparak hoşuna giden gönderilere beğeni atarak zaman geçirmektedir.

Bu sırada içerisinde çalıştığı bankanın adının geçtiği sponsorlu bir sayfasının "Bankanın 50'nci yılına özel 5 müşterisine son model otomobil,10 müşterisine de son model telefon" hediye ettiğini görür ve heyecanla sayfanın paylaştığı linke tıklar. Tıklama sonrası açılan sayfada çalıştığı bankaya ait internet bankacılığı ekranını görür ve hemen bilgilerini girer. Bilgilerini girdikten sonra sayfanın aynı şekilde kaldığını ve giriş yaptığı sayfanın uzantısında harf farklılıklarının olduğunu anlar. Çalıştığı bankanın çağrı merkezini arayan Harun, biriktirdiğini 50 gr altının bozdurularak tutarın tamamının Ahmet Yılmaz adında hiç tanımadığı bir kişiye EFT yapıldığını öğrenir. Banka görevlisi, banka şubesinden işlemlerin detayını alarak savcılığa suç duyurusunda bulunup belgeleri en kısa zamanda bankaya ulaştırması gerektiğini Harun Bey'e iletir.



Telefonla İkna İle Dolandırıcılık

Sosyal Mühendislik yetenekleri kullanılarak gerçekleştirilen bu eylemler ilk olarak 2007 yıllarında kontör/TL yükleme dolandırıcılığı olarak ortaya çıkmıştır. O tarihlerde basit senaryolar kullanılarak ikna edilen kişilere kontör kart üzerinde bulunan kod okutularak GSM kontör bakiyeleri çalınmıştır. Telefon üzerinde ikna yeteneklerini geliştiren dolandırıcılar, zaman içerisinde aradıkları kişileri banka hesaplarından kendilerine para transferlerini yaptırmaya ikna etmişlerdir. Çığ gibi büyüyen bu dolandırıcılık eylemleri nedeniyle Emniyet ekipleri başta olmak üzere, bankalar ve kurumlar tarafından insanların bilinçlendirilebilmesi amacıyla çok çeşitli kampanyalar başlatılmıştır. İkna ile dolandırıcılıklar, bugün çok çeşitli senaryolar kullanılarak yapılmaktadır ve insanlar, anlatılan olayı yaşadıklarına inandırılarak ciddi para kayıpları yaşamaktadır.

2007
Türkiye'de sosyal mühendislik kullanılarak yapılan ilk dolandırıcılık eylemi kontör/TL yükleme olmuştur.

Temeli insana dayanan sosyal mühendislik girişimlerinde ise kişiden bilgi almak ya da istenilen işlemleri yapmasını sağlamak amacıyla taklit, etkileme ve ikna etme kabiliyetleri kullanılır. Kurumun bir şubesinden arıyormuş gibi davranıp, şubeye ait bir müşterinin herhangi bilgisini istemek bunun için bir örnektir.

Temeli insana dayanan sosyal mühendislik girişimlerinde en belirgin yöntemlerden biri telefonla İkna ile aldatma yöntemidir. Bu yöntemde teknolojilerin getirdiği imkânlarla da desteklenerek aranılan kişiden daha kolay bilgi alınmasını hedeflemektedir. Buradaki teknolojik imkân yurt dışı internet servis sağlayıcılardan (proxy) faydalanarak aranılan kişiye, arayan olarak istediği numarayı göstermesidir.

Telefonla ikna dolandırıcılık yöntemi ile, müşterilerinin hesap numaraları, kredi kartı bilgileri ve bunun gibi kişisel bilgilerini elde etmeye yönelik gönderilen e-postalar ve bu e-postaların içeriklerinde verilen çeşitli telefon numaralarına yönlendirmeler yapılır. Bu sahte telefon numaraları, mağdur tarafından arandığında dolandırıcının daha önceden hazırladığı banka sesli yanıt sistemini ve çağrı merkezini taklit eden bir sistem çıkmakta ve dolandırıcılar bu yöntem sayesinde kurbana ait kişisel bilgileri ele geçirebilmektedir.

Telefonla ikna yöntemi türleri

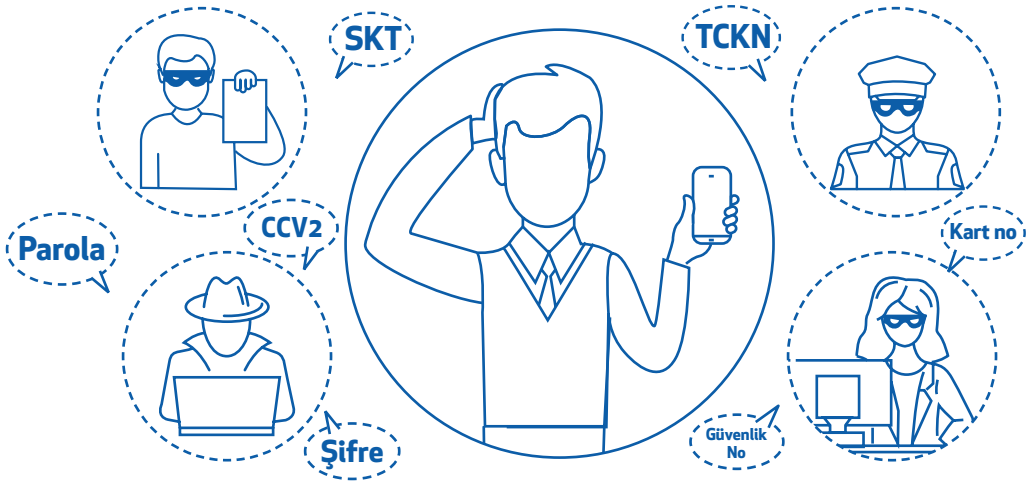
Dolandırıcılar tarafından müşterileri ikna etmek amacıyla en sık kullanılan yöntemler şöyle:

Banka Adı Kullanılarak Arama

Bu tür aramalar genellikle banka numarasına benzeyen numaralarla yapılmaktadır. Banka adına aradığını söyleyen dolandırıcı önceden ele geçirdikleri bilgileri kullanarak müşterinin güvenini kazanmaya çalışır.

Dolandırıcılar, kart ücreti iadesi, sigorta/ücret iptali, daha yüksek faizden bağlamak için vadeli bozumu, kampanya çekilişine katılım gibi gerekçelerle müşterilerin dikkatini çekerek bilgilerini ele geçirmeyi hedefleyebilir. Bu kişiler bankanın güvenlik ekibinden aradığını söyleyerek işlem iptali yapılması için şifre isteyebilirler.

Yukarıdakiler haricinde, bankadan aradığını söyleyen kişiler müşterinin hesabına yanlışlıkla para geldiği ve iadesinin yapılması için müşteriye uzaktan erişim uygulaması indirtip bu uygulama üzerinden işlem yapmaya çalışırlar.

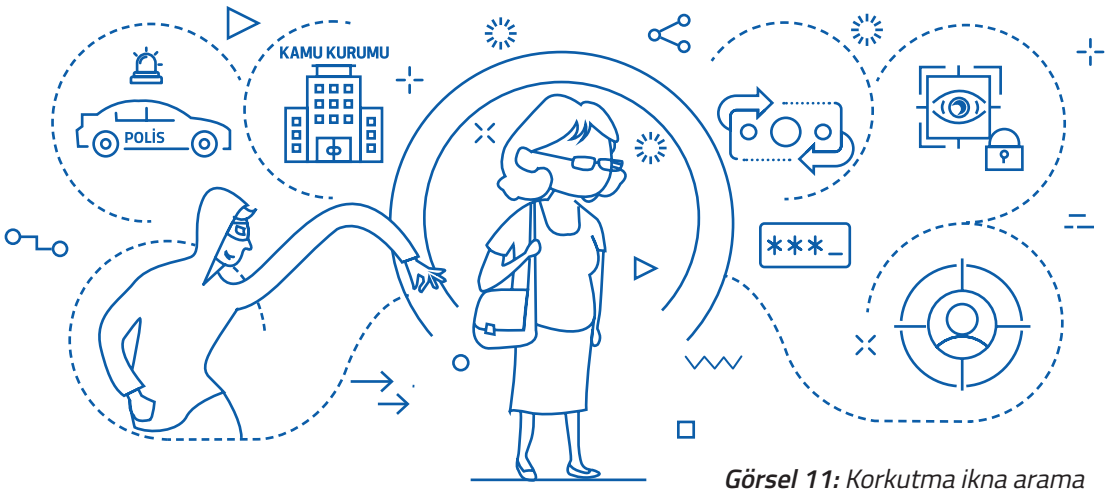


Görsel 10: *Banka adı kullanılarak sahte arama Kaynak: TBB – Çalışma*

İkna

Dolandırıcılar emniyet, jandarma gibi resmî kurumlar adına arayarak terör örgütü üyeliği nedeniyle hesaplarını güvenceye alma bahanesiyle müşterilerin şifrelerini ele geçirmeye ya da müşterinin tanımadığı kişilere para transfer etmesini sağlamaya çalışırlar.

Müşteriler kendilerinin ve hesaplarının tehdit altında olduğu psikolojisi ile karşı tarafın şifre dahil istediği tüm bilgileri paylaşabilmekte, istenen işlemleri yapabilmektedir. Müşterinin baskı altında kalmaya devam etmesi ve durumun farkına varamaması için dolandırıcılar müşterileri görüşmeye devam etmesi için zorlamaktadırlar.



Görsel 11: *Korkutma ikna arama Kaynak: TBB – Çalışma Grubu*

Yakını Adına Talepte Bulunma

Müşterilerin yakınlarına ait sosyal medya hesaplarının ele geçirilerek, yakını adına çekilişe katılma amacıyla kart bilgilerini isteme, para isteme, bir hesaba para gönderilmesi isteme gibi vakalar yaşanabilmektedir.

Bu tür vakalarda sosyal medya üzerinden gelen talepler dikkate alınmamalı, mutlaka ilgili kişi ile farklı bir kanaldan iletişime geçilerek bu talebi kendisinin yapıp yapmadığı sorgulanmalıdır. Sosyal medya hesapları ele geçirilen kişi ise en kısa sürede sosyal medya hesabını geri alarak şifrelerini güncellemesi yönünde bilgilendirilmelidir.

Görsel 12: *Ele geçirilen sosyal medya hesabı üzerinden bilgi elde etme*
Kaynak: TBB – Çalışma Grubu

Telefonla İkna Saldırılarından Korunma Yöntemleri

Saldırılardan korunmanın en etkili yöntemi şifre ve parolaların üçüncü kişilerle paylaşılmamasıdır.

Telefon numaralarının başında +1, +00 gibi rakamlar olan aramaları dikkate almayınız.

Telefonla ikna saldırılarından korunmanın en etkili yöntemi üçüncü kişilerle şifre/parola bilgileri paylaşılmamasıdır. Şifre ve parola bilgileri size özeldir, sizi arayan üçüncü kişilerle bu bilgileri kesinlikle paylaşmayınız. Bankanız sizi arayarak hiçbir koşulda şifrenizi istemez.

Ücret iadesi, yanlışlıkla gelen paranın iadesi, işlem iptali, terör örgütü üyeliği gibi bahanelerle, banka, resmî kurum, emniyet güçleri adına sizi arayan kişiler ile kişisel bilgilerinizi, internet bankacılığına giriş bilgilerinizi, kart bilgilerinizi veya şifrelerinizi paylaşmayınız/telefonda bu bilgileri tuşlamayınız.

Sizi arayan kişilerin yönlendirmesi ile tanımadığınız kişilere para göndermeyiniz, cihazınıza uzaktan erişim uygulaması indirmeyiniz.

Tarafınıza gelen aramalarda numaranın başında +1 +00 gibi rakamların olup olmadığına dikkat ediniz. Bu yönde gelen aramalar karşısında söylenenleri dikkate almayınız. Dolandırıcıların aradığı numaralar genellikle bankaların numaralarına benzerlik göstermekle birlikte detaylı incelendiğinde farklılıklar tespit edilebilmektedir. Bu yönde gelen aramalarda numara geri arandığında asla ulaşılamamaktadır.

Değersiz olarak nitelendirdiğiniz, üzerinde kimlik, iletişim, bankacılık gibi bilgileriniz bulunan her türlü materyalleri uygun şekilde imha ediniz.

Telefonla İkna Saldırısına Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler

1. İnternet bankacılığı, kredi kartı ya da şifre/parola bilgilerinizi üçüncü kişilerle paylaştığınızda bu kişilerin yönlendirmeleri ile tanımadığınız kişilere para gönderdiğinizi anladığınız anda vakit kaybetmeden bankanızı arayarak hesaplarınız ve kartlarınızda gerekli güvenlik aksiyonlarının alınmasını sağlayınız.
2. Aynı şifreyi birden fazla bankada kullanıyorsanız, dolandırıcılarla o anda üzerinden işlem yapmadığınız bankalarınızı da arayarak varlıklarınızı güvenliğe alınız.
3. Bankanız tarafından güvenlik aksiyonları alınana kadar, üçüncü kişilerle paylaştığınız şifrelerinizi değiştirerek, geçici bir çözüm üretebilirsiniz.
4. Bankanızı aradığınızda olaya ilişkin tüm bilgeleri vakanın detaylı incelenmesi için paylaşınız.

Senaryo 1

Bir gün telefonu çalan 1941 doğumlu Adnan Bey telefonu açtığında karşıda kendini emniyet müdürü olarak tanıtan Feridun Bey ile karşılaşmıştır. Dolandırıcı olan Feridun, Adnan Bey'e adının Terör Örgütü soruşturmasına karıştığını bu konuyla ilgili yürüttükleri operasyon sırasında isminin dinlemeye takıldığını ama kendilerinin bu durumun doğru olmadığını bildiklerini iletmişlerdir.

Kendisini de bu operasyona dahil edip terör örgütü üyelerini yakalamak için bir şans vermişlerdir. Bu konudan kimseye hiçbir akrabasına ya da eşine daha da önemlisi banka çalışanlarına bahsetmemesi, bankadan bir arama gelirse oğlunun evinin tadilatını yaptırmak için işlem yaptığını söylemesi istenmiştir. Yaşından dolayı kolayca ikna edebilecekleri için seçtikleri Adnan Bey'in, böyle bir durumu olmadığını ispatlamak için her şeyi yapabileceğini anlamışlardır.

Dolandırıcılar operasyonun ikinci aşaması olarak belirttikleri bir transfer işlemi yapılması gerektiğinden bahsetmişlerdir. Feridun Bey'e hesabındaki tüm parayı örgüt üyeleri tarafından kullanılmaması için, X banka Mecidiyeköy şube müdürü olarak tanıttıkları Serdar Bey'in hesabına **"TADİLAT"** açıklamasıyla aktarmasını, operasyon bittikten sonra verdikleri 555XXX1234 numaralı telefonu arayıp yatırdığı parasını geri alabileceğini iletmişlerdir. Her şeyin kılıfına uygun olduğunu düşünen Adnan Bey transferi yapmak için internet şubesinden hesabındaki tüm parayı dolandırıcıların verdiği hesaba transfer etmiştir. Olaydan bir gün sonra verilen banka müdürünün telefonuna ulaşıp parasını almak istediğinde telefonun sahte olduğunu ve onu aradıkları numaraya da ulaşamadığını gördüğünde dolandırıldığını anlayıp bu kez gerçek savcılığın yolunu tutmak zorunda kalmıştır.

Senaryo 2

Kadir Bey 56 yaşında orta ölçekli bir giyim firmasının sahibidir. O gün sabah ofisine giderken tanımadığı bir numaradan aranmış ancak çok acelesi olduğu için telefona cevap verememiştir. Ofisinin kapısında bekleyen güvenlik görevlisi Kadir Bey i karşıladıktan sonra eşinin kendisini aradığını ve çok acil telefon beklediğini iletir. Kadir Bey eşinin neden ofisi aradığını cepten kendisini aramadığını düşünse de durumun acil olduğunu düşünerek paltosunu bile çıkartmadan ofis telefonundan evini arar.

Kadir: Merhaba Defne beni aramışsın,

Defne: (Nefes nefese) Aradım aradım ama ulaşamadım. Lütfen beni çok dikkatli dinle, şu anda evimizde polisler var. Söylediklerine göre savcılık talimatı ile gelmişler. Senin tehdit altında olduğunu hesaplarındaki paraların her an terör örgütünün eline geçebileceğini söylüyorlar.

Kadir: Sakin ol canım olur mu hiç öyle şey ben bu işin aslını bir öğreneyim.

Tam o sırada ofisin kapısından üniformalı polis memuru girer.

Polis: Kadir Bey çok acele benimle adliyeye gelmeniz gerekiyor. Savcı bey talimat verdi sizi alıp derhal kendisine götürmem gerekiyor.

Kadir: Neler oluyor hiç anlamadım. Savcı neden beni çağırsın ki.

Polis: Devam eden bir soruşturma kapsamında sizin çok kritik bir konumda olduğunuzu söyledi ben de başka bir şey bilmiyorum.

Telefonda bekleyen Defne de konuşmaları duymuştur.

Kadir: Defne sen oradaki polislere söyle ben Savcı beyin yanına gidiyorum. Çıkınca seni ararım.

Defne: (Telaşla) Tamam tamam sen git

Kadir bey polis ile birlikte ofisinden ayrılır. Arabasına bindikleri sırada polisin telefonu çalar.

Polis: Buyrun Savcı Bey, tamam anladım, tamam o zaman biz direk banka ya gidiyoruz. Tamam bekler misiniz sorayım. Kadir Bey siz hangi banka ile çalışıyorsunuz?

Kadir: XX Bank

Polis: XX Bankmış efendim, tamam ben iletiyorum, tamam bankaya geçiyoruz. Kadir Bey kara banka gidelim.

Kadir: Tamam hemen gidiyorum. Telaş içerisinde arabasını kara bankın önüne çeker.

Polis: Ben sizi arabada bekleyeceğim Kadir Bey, Savcının verdiği talimata göre paranızı size yazdığım hesaba göndermeniz gerekiyor. Çok hızlı hareket etmemiz lazım aksi takdirde bütün operasyonun boşa gideceğini özellikle anlattı Savcı Bey.

Kadir banka şubesine girdikten sonra vadeli hesabını kapatarak 150.000 TL'yi polis memurunun kendisine yazdığı hesaba havale etmek ister. Bankoda çalışan görevli Kadir Bey'in telaşlı hallerinden bir sorun olduğunu anlamıştır.

Bankacı: Kadir Bey hayırdır bugün biraz telaşlı görünüyorsunuz.

Kadir: Yok canım bir sorun yok. Biraz acelem var yetişmem gereken bir randevuma geç kaldım.

Bankacı: Tamam anladım, peki bu ödemenin açıklamasına ne yazmamı istersiniz?

Kadir: Ev ödemesi

Bankacı: Hayırlı olsun yeni bir ev mi alıyorsunuz

Kadir: Yok bir arkadaşıma borç gönderiyorum.

Bankacı: Sizi biraz bekleteceğim, arka ofisten çıktı almam lazım.

O sırada polis de bankaya gelir. Arka ofise geçen banko görevlisi yetkilisi ile görüşerek Kadir Bey'in dolandırıcılık yaşıyor olabileceğini davranışlarının oldukça tedirgin olduğunu, parayı gönderdiği kişi ile ilgili çelişkili beyanları olduğunu anlatarak destek ister. Banka yetkilisi bankoya geldiğinde Kadir Bey in yanında görevli polis memurunu görünce konunun detaylarını öğrenmek ister. Polis memuru, görevli Savcı dan talimat aldığını Kadir Bey'in işlemlerini tamamlamalarını rica eder.

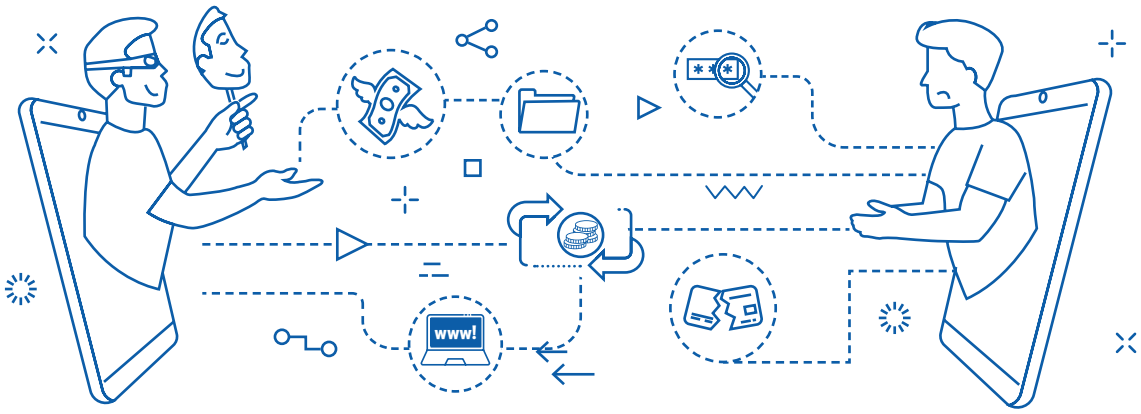
Banka yetkilisi polis memuruna Savcı Bey ile yüz yüze görüşüp görüşmediğini sorar. Memur kendisinin telefon ile görüşme yaptığını belirtince banka yetkilisi savcıyı adliye santralinden aramasını rica eder. Görüşmeyi yapan polis arayan kişinin savcı olmadığını öğrenir. Bu sırada eşi ile görüşen Kadir Bey aslında evlerinde herhangi bir polisin olmadığını eşini arayan kişilerin kendisine böyle bir bilgi vermesini istediklerini öğrenir.

Senaryo 3

Fazıl Bey, 57 yaşında SGK emeklisi bir bireydir. Geçmişte hem kendi ihtiyaçları hem de çocuklarının evlilik ihtiyaçları için farklı bankalardan kredi kullanımları yapmıştır.

Bir Pazar günü evinde kahvesini yudumlayıp bulmacasını çözerken 0850 222 XX XX'li bir numaradan kendisine bir arama gelir. Bu aramaya yanıt verdiğinde; kendisini bankada yetkili olarak tanıtan Murat adında şahıs ile görüşmeye başlar. Murat, Fazıl Bey'in geçmişte kredi kullanımları yaptığını ve bu kullanımlara bağlı olarak birikmiş 900 TL sigorta alacağının olduğunu söyler.

Maddi açıdan zor günler geçiren Fazıl Bey için, bu tutar hiç de az değildir. Hemen bu fırsattan yararlanmak istediğini söyler. Bunun üzerine Murat, Fazıl Bey'e şuan hangi bankalar ile çalıştığını sorar. Fazıl Bey, Murat'ın nazik ve yumuşak tavırlarından etkilenip güven duyduğu için tereddütsüz bir şekilde çalıştığı bankaya ait internet bankacılığı bilgilerini paylaşır. Bu bilgiler ile Fazıl Bey'in internet bankacılığına giriş yapan Murat, 5.000 TL nakit avans kullanımı yaparak bu tutarı eşleştirmiş olduğu cihaz ile kendisine en yakın ATM'den QR kod kullanımı yaparak çeker. Fazıl Bey görüşmeyi sürdürürken telefonuna yapılan finansal işlemler için SMS'ler geldiğini fark edip görüşmeyi sonlandırır. Panik şekilde bankasına ait çağrı merkezini arayan Fazıl Beye, kendisine herhangi bir iade yapılmadığını ve dolandırıcılığa maruz kaldığı söylenir. Bunu duyan Fazıl Bey, soluğu savcılıkta alır.



Telefonla İkna / Uzaktan Kontrol

Banka müşterisini telefon ile arayan dolandırıcı, daha önce illegal yollardan elde ettiği bilgileri kullanarak bankadan aradığına ikna etmekte ve yaptığı yönlendirmeleri müşterinin gerçekleştirmesini sağlamaktadır.

Dolandırıcı telefonda ikna ettiği müşteriye cihazında bulunan uzaktan erişim uygulamasını aktif ettirerek, müşteri cihazına bağlanmakta ve banka hesaplarına erişerek işlemleri kendisi gerçekleştirmektedir. İkna dolandırıcılıkları ile uğraşan kötü niyetli kişiler, toplumumuzda artan farkındalıklar nedeniyle yöntemlerini güçlendirmişlerdir. Teknolojik imkanların kullanımı, mağdurun aile bireylerinin de dolandırıcılık eylemine dahil edilmesi son dönemde karşımıza daha sık çıkmaktadır.

Senaryo 1

Telefonunuza program indirmenizi isteyerek bilgisayarınıza uzaktan erişime açabilmek mümkündür. Bu yolla sizin bilgisayarınızdan adınıza işlem yapılabileceğini unutmayın.

Parlak boya fabrikasının muhasebe bölümünde çalışan Ekrem'in öğle molasında telefonu çalar. Kendisini savcı Ferit olarak tanıtan kişi Ekrem'in hesaplarının terör örgütü tarafından ele geçirildiğini ve kendisine vereceği talimatları sorgusuz bir şekilde yerine getirmesini söyler. Telaşlanan Ekrem hangi bankada hesabı olduğunu telefonda kendisini savcı olarak tanıtan kişiye iletir.

Savcı çok gizli bir operasyon içinde olduklarını, çevresinde bulunan hiç kimseye bu bilgileri vermemesi gerektiğini ve telefonunu sürekli açık tutmasını kendisinin sivil bir ekip tarafından takip edildiğini söyler. Telaştan eli ayağı titreyen Ekrem savcının kendisine vereceği talimatları sorar. Savcı Ferit Ekrem'e telefonuna **TeamViewer Host** isimli uygulamayı indirmesini bu uygulamayı açıp istenilen tüm izinleri onaylamasını ister. Bu sayede sivil ekibin kendisini uzaktan takip edebileceğini iletir.

Birazdan terörle mücadele ekipleri tarafından aranacağını bu kapsamda kendilerine yardımcı olmalarını isteyen Savcı Ferit telefonu kapatır. Savcı ile görüşmeyi sonlandırdıktan hemen sonra tekrar telefonu çalan Ekrem bu kez kendini terörle mücadele ekibi komiseri olarak tanıtan Cemil ile görüşmeye devam eder. Komiser Cemil savcının talimatı ile kendisine yardımcı olmak için aradığını kendisinin bu terör örgütü ile bağlantısının bulunmadığını ancak hesaplarını kullandıkları için kendisi ile işbirliği yapmasını ister.

Az sonra telefonuna SMS'ler geleceğini bu SMS'lerin terör örgütü tarafından hesabından yapılan bir saldırı sonucu geleceğini ancak her şeyin kontrolleri altında olduğunu belirtir. Ekrem'in telefonuna bir süre sonra **"Hesabınızdan 35.000 TL, 40.000 TL ve 50.000 TL tutarında para transferi işlemleri gerçekleştirilmiştir işlemler tarafınıza ait değilse bankanızı arayınız"** şeklinde SMS'ler gelmeye başlamıştır.

Komiser Cemil tutarların şubede polis kontrolünde bir hesaba gönderileceğini banka tarafından aranması durumunda da işlemin kendisi tarafından yapıldığını doğrulamasını ister. Bankanın güvenlik birimleri tarafından aranan Ekrem telefondaki Komiser Cemil'in talimatı ile kendisini bekletmeye alır ve banka personeline işlemi kendisinin yaptığını, transferin gerçekleşmesini istediğini iletir. Transfere onay verdikten sonra tekrar komiser ile konuşmaya başlar. Komiser Cemil terör örgütüne mensup kişilerin şubeden parayı çekeceği anda suçüstü yapılacağını bu gizli operasyon sonunda parasını savcılıktan gelip alacağını belirtmiş ve kendisini arayacağını söylemiştir.

Ekrem uzun süre bekledikten sonra komiserden ve savcıdan telefon gelmeyince kendisini arayan numaralara ulaşmaya çalışır fakat sonuç alamayınca savcılığa gidip durumu anlatır. Savcılıktan bu şekilde bir arama olmadığını ve dolandırıldığını anlayan Ekrem kendisini arayan ve paranın gönderildiği kişilerden şikâyetçi olur ancak iş işten geçmiştir ve tüm birikimini bir telefonda kaybetmiştir.

Senaryo 2

Yoğun bakım hemşiresi olan Duygu Hanım gece mesaisini bitirip evinin yolunu tutmuştur. Evine vardığında uykusuzluk ve yorgunluğun da etkisiyle koltuğa uzanmıştır. Tam uyumak üzereyken 0850 222 XX XX numaralı hattan aranır. Telefonu açınca kendisini XX bankın müşteri temsilcisi olarak tanıtan Arzu ile görüşmeye başlar. Arzu, Duygu Hanıma yapılan son yasal düzenleme çerçevesinde kredi kartından kesilen aidat ücretlerinin toplu olarak ödeneceğini bunun için kendisini rahatsız ettiğini iletir. Son derece kibar ve tatlı dilli bir kızla konuşan Duygu Hanım alacağı parayı da duyunca son derece mutlu olur.

Arzu, önce kısa bir doğrulama adımından geçeceğini ilettiği Duygu Hanıma şimdi telefonunuza bir şifre gönderiyorum şifreyi telefonda tuşlamanızı rica ederim der. Gelen şifrenin mobil bankacılık aktivasyon şifresi olduğunu fark etmeden paylaşır. Arzu şimdi sizinle telefonunuzda birkaç tuşlama yapmamız gerekiyor, bu tuşlamadan sonra gün içinde arkadaşlarının kendisini arayacağını ve beklemeden parayı hesabına aktaracağını iletir.

Duygu Hanıma telefonundan sırasıyla **33*5422222222# tuşlamasını ister. Tuşlamayı yaptıktan sonra Arzu iyi günler dileyerek telefonu kapatır. Görüşmeden sonra uyuyan Duygu Hanım kapının çalması ile uyanır. Kapıyı açtığında kızını görünce şaşırır ve senin işte olman gerekmiyor muydu diye sorar.

Kızı Gökçe telefonuna ulaşamadığını merak ettiğini ondan eve geldiğini söyleyince Duygu Hanım telefonuna bakar, telefonum açık gelen aramada yok der. Bir tuhaflık olduğunu anlayan Gökçe telefonun ayarlarını kontrol eder ve telefonunun yönlendirildiğini bunu neden yaptığını sorar. Duygu Hanım kendisinin böyle bir şey yapmadığını hatta uyumadan önce bankadan arandığını belirtir.

Telefon ayarlarını normale çeviren kızı, ardından hemen bankanın çağrı merkezini arayıp hesaplarını kontrol etmesini ister. Telaşla bankanın çağrı merkezine ulaşan Duygu Hanım, temsilcinin hesaplarınızdaki tutarlar transfer edilmiş demesiyle sarsılır. Vakit kaybetmeden suç duyurusunda bulunmak üzere yola çıkar.

Daha sonra bankanın güvenlik birimlerince aranan Duygu Hanım hesabından gerçekleştirilen 48 bin TL tutarındaki EFT işleminin teyidi için arandığını telefonunun yönlendirilmiş olması sebebi ile dolandırıcıların işlemi teyit ettiğini öğrenir.

Senaryo 3

Mehmet Bey, günlük iş temposunda yoğun bir şekilde çalışırken bir yandan ay sonunda yapılacak olan tedarikçi ödemeleri ve personel maaşlarını düşünmektedir. Bu yoğunlukta kafasını iş dışında bir konuya veremeyecek durumda iken, birden çalıştığı bankanın numarasına benzer bir numaradan arama gelir. İlk etapta telefonu meşgule atmasına rağmen, telefon ısrarla çalmaya devam ettiğinde, daha önce yapmış olduğu kredi başvurusunun durumu için aranmış olabileceğini düşünüp telefonu açar.

Telefondaki kişi kendisini bankada çalışan Nazan Hanım olarak tanıttığında, Mehmet Bey heyecanla araya girip kredi başvurusu hakkında arandığını tahmin ettiğini, sonucunu çok merak ettiğini söyler. Bu durum karşısında telefonda kendisini Nazan Hanım olarak tanıtan kişi, kısa bir duraklama sonrası başvurusunun onaylandığını, kullandırım işlemini tamamlamak için kendilerini aradığını söyler. İşlemleri tamamlamak için öncelikle mobil bankacılık uygulamasına giriş yaparak onay vermesi gerektiğini, dilerse işlemleri hızlandırmak için şifresini bu arama üzerinden iletebileceğini söyleyip kendisini şifrelerini tuşlaması için sesli yanıt sistemine aktarır.

Şifreleri telefonda tuşlayan Mehmet Bey'e kredinin hesabına 1 saat içerisinde geçeceği, bu süre zarfında kendisinin bankadanmış gibi tanıtıp işlemleri reddetmek amacıyla şifrelerini ele geçirmeye çalışabilecek kişilerin olabileceği, önlem amaçlı telefonunu kısa bir süreliğine kendilerine yönlendirmesi gerektiği bilgisi verilir. Bu talimatlara uyan Mehmet Bey, çalışmaya geri döner, ancak bir süre sonra gelen SMS'lere baktığında işlemlerin kredi kullandırımı değil para transferi olduğunu anlar.

Vakit kaybetmeden bankayı aradığında, güvenlik izleme birimi tarafından şifre ve hesapları için güvenlik aksiyonlarının zaten alındığını anlar. Yapılan işlemler, güvenlik izleme biriminin kontrollerine takılmış ve teyit aramasında telefonun yönlendirilmiş olduğu fark edildiği anda güvenlik aksiyonları alınmıştır. Mehmet Bey ise görüşme sırasında alınan önlemler için teşekkür ederek, bundan sonra daha dikkatli olacağını ifade etmiş, kredinin durumunu sorarak görüşmeyi sonlandırır.

C) Çağrı Merkezi Dolandırıcılıkları

Bankalar, çağrı merkezi kanallarını şubelerine en büyük alternatif dağıtım kanalı olarak, internet bankacılığı ve mobil bankacılık gibi dijital kanalların yaygınlaşmasından çok önce kullanmaya başlamıştır.

Günümüzde de, nakit işlemler hariç, neredeyse tüm bankacılık işlemlerinin yapılabildiği bu bankacılık kanalında müşteriler akıllı yönlendirmeler ve sesli yanıt sistemi menüleri ile mümkün olan en kısa sürede hizmet almak istediği işleme yönlendirilmekte, işlemleri banka çalışanı aracılığıyla ya da sesli yanıt sistemi üzerinden kendileri yapabilmektedir.

Ses tanıma gibi biyometrik doğrulama yöntemlerinin kullanılabildiği çağrı merkezi kanalında, internet ve mobil bankacılık kanallarına ait şifrenin kullanımı müşteri deneyimi açısından bankaların en sık tercih ettiği yöntemdir. Bu kanaldan yapılabilen işlem çeşitliliği ve doğrulama yöntemlerinin diğer kanallar ile ortak olması, farklı yöntemlerle ele geçirilen müşteri bilgileri üzerinden dolandırıcılık girişimlerinin yaşanmasını da beraberinde getirmektedir.

Çağrı merkezi dolandırıcılığı, müşteri bilgilerinin (kimlik, kart, internet bankacılığı, sim kart vb.) ele geçirilerek 3. kişiler tarafından çağrı merkezinin aranması ile gerçek müşteri adına işlem yapılmasıdır.

Bankaların telefon aracılığı ile bankacılık hizmetlerini yürüttükleri Çağrı Merkezleri üzerinden bağlanan dolandırıcı kişiler müşteri hesaplarından yetkisiz işlemler gerçekleştirebilmektedirler.

Bu dolandırıcılık eylemleri yıllar içerisinde değişiklik gösterse de günümüzde halen yeni teknolojileri alet eden kötü niyetli kişiler Çağrı Merkezi aracılığı ile müşteri hesaplarına erişebilmektedirler.

Çağrı Merkezi Dolandırıcılıklarından Korunma Yöntemleri

Çağrı Merkezi aracılığıyla yapılan işlemlerde doğrulama adımında internet/mobil bankacılık şifresi, kart şifresi, parola gibi müşteri tarafından bilinen bilgiler ve SMS OTP, mobil onay gibi sahip olunan bileşenler kullanılır. Bu bilgilerin tamamı size özeldir ve sadece sizin bankanızı aradığınız durumlarda güvenliğiniz için istenir.

Bankanız sizi arayarak işlem onayı için şifrenizi tuşlamanızı, paylaşmanızı, mobil onay vermenizi istemez. Sizi arayarak tanımadığınız kişilere para göndermenizi, şifrenizi tuşlamanızı, paylaşmanızı isteyen kişilere itibar etmeyiniz.

Bankanın diğer kanallarında olduğu gibi bu kanaldan yapılan işlemler sırasında ve sonunda banka tarafından iletilen SMS OTP/mobil onay ve SMS bilgilendirme içeriklerine dikkat ediniz.

Çağrı Merkezi Dolandırıcılıklarına Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler

1. Şifrelerinizi üçüncü kişilerle paylaştığınızda, bilginiz dışında adınıza farklı bir cihazda mobil onay için aktivasyon yapıldığında ya da bankacılık ürünlerinize ait bilginiz dışında bir işlem olduğunda zaman yitirmeden bankanız çağrı merkezini arayarak bilgilerinizi ve ürünlerinizin güvenlik altına alınmasını sağlayınız.
2. Üçüncü kişilerle paylaştığınız şifrelerinizi değiştirerek geçici çözüm üretebilirsiniz.
3. Hattınız ile ilgili sinyal problemi var ise operatörünüz ile görüşerek hattın durumunu kontrol ettiriniz.
4. Bilginiz dışında ses imzası oluşturuldu ise bu ses imzasını sildirmek üzere Bankanız ile iletişime geçiniz.

Senaryo 1

Sosyal medyada son derece aktif olan Ali Bey, Bankanın hesabına benzer bir sosyal medya hesabından hediye çekilişi kampanyasına ait linke tıklar ve açılan sayfada kart, iletişim ve kimlik bilgilerini girer. Banka çekilişine katıldığını düşünen Ali Bey bilgilerini aslında dolandırıcılar ile paylaşmıştır. Bilgileri ele geçiren dolandırıcı önce çağrı merkezini arayıp kartın aktifliğini kontrol etmiştir. Kartın aktif olduğu teyit edildikten sonra VOIP ile müşteri numarası taklit edilerek Banka aranmıştır.

Çağrı merkezi parolası oluşturmuş ve güvenlik teyidinden geçen dolandırıcı kendi hesabına transfer sağlamıştır. Ali Bey yine sosyal medyada dolaşırken cep telefonuna bir SMS gelir. SMS içerisinde hesabından tanımadığı bir kişiye 2.000 TL transfer gerçekleştiği bilgisi yer almaktadır. Ali Bey önce bir yanlışlık olduğunu zanneder. Çok şaşırır. Hemen internet bankacılığına girer ve hesabını kontrol eder. Gerçekten hesabından 2.000 TL transfer gerçekleşmiştir. Bunun üzerine hemen Banka görevlisi Handan Hanım'a ulaşır ve işlemin kendisine ait olmadığını iletir. Banka görevlisi tutarın alıcı hesaptan çekildiği bilgisini verir ve Ali Beyi savcılığa yönlendirir.

Senaryo 2

Zeynep XX Bankda yöneticidir. Sabah başlayan yoğun iş temposu sırasında tanımadığı bir numaradan arama gelir.

Zeynep: Alo

Dolandırıcı: Merhaba Benim adım Ali, sizi XX Bank Uyum Biriminden arıyoruz.

Zeynep bir anda dikkat kesilir

Zeynep: Buyurun

Dolandırıcı: İnternet Bankacılığınız üzerinden şüpheli işlemler kaydettik. Bunları teyit etmek amacıyla sizi arıyoruz. Bugün hesaplarınızdan 48.000 ve 15.000 TL'lik EFT ler yaptınız mı?

Zeynep: Hayır?

Dolandırıcı: Size ait olmadığını tahmin ediyoruz, bu işlemleri iptal etmek istiyor musunuz?

Zeynep: Evet!

Dolandırıcı: Peki şimdi sizi sesli yanıt sistemine aktarıyorum, dijital parolanızı sesli olarak söylemenizi isteyeceğim.

Zeynep hiç tereddüt etmeden çıkan sinyal den sonra dijital parolasını söyler.

Dolandırıcı: Tamam Zeynep Hanım, şimdi mobil uygulamanızı açar mısınız?

Zeynep: Evet açtım
Dolandırıcı: Size bir onay işlemi düşecek lütfen onu sağa doğru çekiniz.
Zeynep paniklemiştir. Mobil uygulamada yanlışlıkla onay yerine işleme red verir.
Dolandırıcı: Zeynep Hanım işlemi onaylayamadınız. Bekleyin lütfen birazdan yeniden onay göndereceğim. Gönderdim şimdi onaylar mısınız?
Bu sefer gelen mobil onaya evet demiştir.
Zeynep: Tamam Zeynep Hanım ilk işlemi onayladınız şimdi sırada ikinci işlem var.

Bu esnada Zeynep in ofis telefonu ısrarla çalmaktadır. Yan tarafında bulunan arkadaşından telefonunu cevaplamasını ister. Arkadaşı masasına gelerek bankanın güvenlik biriminden aradıklarını, konuştuğu kişinin dolandırıcı olabileceğini belirtince Zeynep bir an şaşırır. O esnada söylenenleri duyan dolandırıcı **"Zeynep Hanım onlar dolandırıcı dikkate almayın"** diyerek hala ikna etmeye çalışmaktadır. Zeynep hiçbir şey söylemeden telefonu kapatır.

Diğer hatta bekleyen ve sistemden kontrol ettiği Eda hanım ile yaptığı görüşme sırasında, aslında kendisini arayanların dolandırıcı olduğu, telefonda verdiği dijital şifre ve mobil onaylar ile adına çağrı merkezine bağlanıldığı, çağrı merkezine bağlanan kişilerin kendi telefon numarası gibi gösterdikleri VOIP arama ile işlem denediklerini öğrenir. Neyse ki hesabından gönderilmeye çalışılan 55.000 TL bankasının Güvenlik Bölümü tarafından fark edilmiş ve kendisine ulaşılmıştır. Yapılan işlem iptal edilerek hesabına aktarılır. Kendisinden beklenen savcılık suç duyurusunu da hemen yaparak Güvenlik Bölümüne iletir.

D) SIM Kart Kopyalama

Müşteri adına düzenlenen sahte kimlikle, telefonunun çalındığını veya kaybolduğunu beyan eden dolandırıcıların GSM operatör bayilerinden yeni SIM kart alarak kullanıcıların banka hesap bilgilerini ele geçirmeyi amaçlayan dolandırıcılık şeklidir.

SIM Kart Kopyalama Saldırılarından Korunma Yöntemleri

SIM Kart Kopyalama vakalarında, SIM kartlar GSM operatör bayilerinden sahte kimlik ile çıkartılabildiği için kimlik belgesinin ve bilgilerinin 3.kişiler veya kurumlarla paylaşımı konusunda dikkatli olunmalıdır.

SIM Kart Kopyalama Saldırısına Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler

1. SIM kartınızın çalışmadığını fark ettiğinizde vakit kaybetmeden operatörünüz üzerinden adınıza çıkarılmış SIM kartın olup olmadığını kontrol ediniz ve var ise iptalini sağlayınız.
2. Çalıştığınız bankalar ile iletişime geçip SIM kartınızın kopyalandığını ve adınıza yapılacak işlemlerin durdurulması ve önlem alınması için bildirimde bulununuz.

Senaryo 1

Evinin bodrum katında ayakkabı imalatçılığı yapan Ahmet Bey, sabah telefonuna gelen SMS bilgilendirmesi ile ihtiyaç duyduğu krediye başvurmak ister. SMS'de yer alan link aracılığı ile açılan sayfada kart ve kimlik bilgilerini paylaşır. Ardından kredi başvurusunun değerlendirmeye alındığı bilgisini SMS ile alan Ahmet Bey, bodrum katındaki atölyesine geçerek işine devam eder.

Bu sırada dolandırıcı, Ahmet Bey'in adına düzenlediği sahte kimlik ile bir operatör bayisinden yeni bir SIM kart alır. SIM kartı dolandırıcı tarafından kopyalanması Ahmet Bey'in bankacılık işlemlerinde kullandığı telefon hattında kesintiye neden olur. Ahmet Bey atölyesinde ara ara şebeke sorunu yaşandığı için bu durumu çok fazla önemsemez.

Paralelde kimlik, kart bilgileri ve SIM kartını ele geçiren dolandırıcı çağrı merkezi üzerinden SIM kart aktivasyonunu tamamlar ve internet bankacılığı için yeni parola alır. Yeni alınan parola ile Ahmet Bey adına internet bankacılığı girişi yapılarak kredi kullandırımı yapılır ve dolandırıcılığa aracılık eden hesaplara para transferi yapılır.

Öğlen yemeğini yemek için yukarı kattaki evine çıkan Ahmet Bey oğlunu aramak istediğinde telefonundaki şebeke sorununun devam ettiğini görür. Evindeki sabit hattından oğluna ulaşıp telefonundaki sorunu ilettiğinde oğlu şüphelenir ve ne zamandan itibaren hattındaki sorunu yaşadığını sorar. Ahmet Bey sabah hattında sorun olmadığını ve telefonundan krediye başvuruduğunu söyler.

İyice şüphelenen oğlu Ahmet Bey'in bankasını arayarak bilgi almasını ister. Bankasını aradığında gün içerisinde adına kredi kullanıldığını ve aynı zamanda kredi kartından da nakit avans kullanılarak hesabına aktarılan tutarların tanımadığı hesaplara transfer edildiğini öğrenir. Bankası ile yaptığı görüşmede, hesapları ile ilgili gerekli güvenlik önemlerini aldıran Ahmet Bey, banka personelinin yönlendirmesi ile Savcılığa suç duyurusunda bulunur.

E) ATM Dolandırıcılıkları

Banka müşterilerinin şubeye gitmeden para yatırıp çekebilmesi için geliştirilen ATM kanalı, günümüzde para transferi, kredi başvurusu, bilgi güncellemesi gibi diğer temel bankacılık işlemleri için hizmet veren bir kanal haline dönüşmüştür. Müşterilerin ihtiyacı olduğu anda kısa süre içerisinde temel bankacılık hizmet ihtiyacını karşılayabilmek için şubelerin bulunduğu konumlardan çok uzak bölgelere ATM kurulumu yapılmaktadır. Dolandırıcılar tarafından ATM kanalına özel yöntemlerle müdahale edilerek müşteri kart ve hesap bilgilerininin ele geçirilmesi hedeflenmektedir.

Bu dolandırıcılıkları, yetkisiz yazılım ve donanımlarla ATM'nin manipüle edilmesi sonucu müşteri kartının, müşteri bilgilerinin veya ATM sisteminin ele geçirilmesi şeklinde özetleyebiliriz.

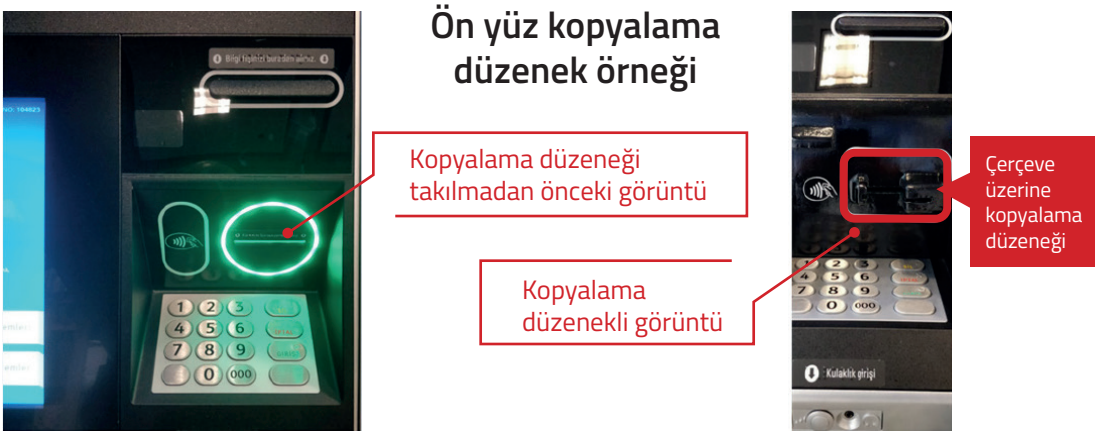
• ATM Kart Kopyalama

Dolandırıcılar tarafından ATM üzerine veya içerisine yerleştirilen kopyalama aparatları ile kart manyetik verilerinin ele geçirilmesidir. Bu yöntemde kart şifresinin ele geçirilmesi ise ATM klavyesi üzerine yerleştirilen sahte bir klavye düzeneği ile veya ATM'ye yerleştirilmiş klavyeye odaklı gizli bir kamera ile yapılmaktadır.

o Ön yüz kopyalama

ATM'de ön yüz kopyalama, dolandırıcılar tarafından ATM'nin kart okuyucu bölümünün üzerine yerleştirilen aparat aracılığı ile kart manyetik verilerinin ele geçirilmesidir. Kart okuyucu bölmesinin girişi dolandırıcılar tarafından taklit edilerek benzeri üretilir ve içine kopyalama cihazı yerleştirilir veya kopyalama cihazı direkt olarak ATM üzerinde mevcut olan kart girişinin içerisine yerleştirilir.

Müşteriler ATM'den işlem yaparken kartlarını taklit edilmiş ve içerisinde kopyalama aparatının bulunduğu kart girişine yerleştirdiklerinde kartın manyetik verileri kopyalama aparatı tarafından ele geçirilir. Bu yöntem ile elde edilen manyetik veriler başka bir plastik karta aktarılarak asıl kartın kopyası oluşturulur. Kart şifresi ise sahte klavyeler veya kameralar yardımı ile ele geçirilir.



Görsel 13: *Ön yüz kopyalama*
Kaynak: TBB – Çalışma Grubu

Kopyalamada kullanılan kamera ile şifre alma düzeneği örnekleri

Kamera takılıp söküldüğünü gösteren yapışkan kalıntıları

Görsel 14: *Kamera takılıp söküldüğünü gösterir kalıntılar*
Kaynak: TBB – Çalışma Grubu

Monte halde kamera düzeneği

Görsel 15: *Kamera ile şifre alma*
kaynak: TBB – Çalışma Grubu

Kopyalamada kullanılan sahte klavye ile şifre alma düzeneği örneği

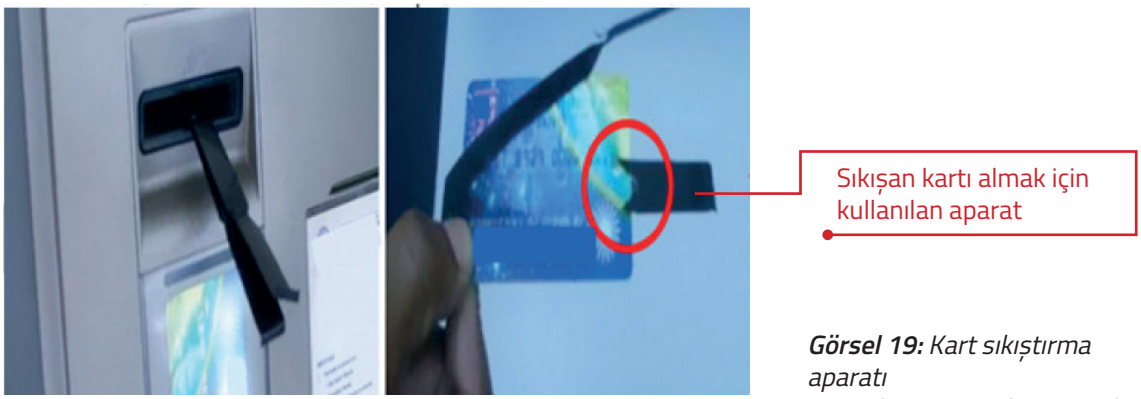
Şifre ele geçirmek için hazırlanan sahte klavye

Görsel 16: *Sahte klavye*
Kaynak: TBB – Çalışma Grubu

• ATM Kart Sıkıştırma

ATM'nin kart okuyucu bölümüne dolandırıcılar tarafından yabancı cisimler yerleştirilmesi ve kartın 3. Kişilerce ele geçirilmesi durumudur. Bu yöntemde dolandırıcılar genellikle sıkıştırılan kartın müşterisi ile temas halindedir. Müşteriyi ATM'de problem olduğuna inandırıp müşteriye yardımcı olmaya çalışıyormuş gibi görünerek kart şifresini girmeye ikna ederler, bu esnada şifreyi müşteriden direkt veya dolaylı olarak (omuz sorfü yöntemi gibi) öğrenirler. Dolandırıcılar tarafından ATM'de teknik bir aksaklık olduğuna ikna edilen müşteri ATM'den ayrılır veya ayrılmaya zorlanır. Daha sonra kart cımbız veya benzeri aparatlar ile sıkışan ATM'den alınarak dolandırıcılar tarafından şifresi ile kullanılır.

Kart sıkıştırma düzenek örneği:



Görsel 19: *Kart sıkıştırma aparatı*
Kaynak: TBB – Çalışma Grubu

Senaryo 1

Yaklaşık 3 yıl önce emekli olan Recep, alışkanlık gereği fatura ödemelerini yıllardır elden yapmaktadır. Emekli maaşı henüz yatmış olan Recep, elindeki doğalgaz faturası ile borcunu ödeyeceği fatura ödeme merkezinin önünde bulunan ATM'de sıra beklemektedir. ATM'de bulunan genç bir adam bir yandan telefonla konuşmakta bir yandan da ATM'de işlem yapmaktadır. Genç adam telefonu kapatıp arkasını döner ve Recep'e kardeşinden hesap numarası beklediğini, dolayısıyla işlem için daha vaktinin olduğunu belirtir ve sırasını Recep'e verir.

Sırasını verdiği için önündeki genç adama teşekkür eden Recep gözlüklerini takar ve kartını ATM'ye yerleştirir. Kısa bir süre bekledikten sonra ATM'nin kartına tepki vermediğini fark edip tuşlara basmaya başlar. Ne kartını alabilmektedir ne de parasını çekebilmektedir. O sırada sırasını vermiş olan ve Recep'in arkasında bekleyen genç adam bir sorun olup olmadığını sorar. Recep kartının ATM'de kalmış olabileceğini ve hiçbir işlem yapamadığını paylaşır. Yardımcı olmak isteyen adam izin isteyerek ATM'ye yanaşır ve yardımcı olmak maksadıyla tuşlara basmaya başlar.

Bu sırada ATM'nin arızalanmamış olmasını işinin acil olduğunu belirterek Recep ile bağ kurmaya, sohbet etmeye başlar. Güvenini kazandıktan sonra Recep'e kartının şifresini tuşlamasını, belki kartın iade olabileceğini söyler. Genç adamın niyetinden şüphe etmeyen Recep onun da görebileceği bir şekilde şifresini tuşlar.

Kendi işleminin de acil olduğunu belirten genç adam Recep'e ATM'nin arızalanmış olabileceğini ve mesai saatlerinde gelip kartını görevlilerden alabileceğine ikna eder, kendisinin de başka ATM arayacağını ileterek Recep'in oradan kendisiyle birlikte ayrılmasını sağlar.

Ertesi gün öğleden önce şubede sırası gelen Recep durumu veznedeki çalışana anlatır. Kartının ATM'de kaldığını ve onu almak istediğini, faturasını ödeyemediğini belirtir. Banka çalışanı Recep'in hesabını kontrol ettiğinde tüm paranın dün az ileride farklı bir ATM'den çekildiğini söyler.

Durumu anlayamayan Recep, banka personeline yaşadıklarını anlatır. Bunun üzerine banka personeli Recep'e, kendisine yardımcı olmaya çalışan genç adamın aslında kartının ATM'de sıkışmasına sebep olduğunu ve bizzat kendisinden öğrendiği şifre ile kartı kullandığını ve tüm parasını çektiğini anlatır. Recep Banka personeli tarafından suç duyurusu yapmak üzere Savcılığa yönlendirilir.

• ATM Para Sıkıştırma

Para çekme haznesinin kapağına benzer sahte bir kapağın üzerine sürülen yapıştırıcı ya da dışarıdan hazneye müdahale ile eklenmiş bir aparat yardımıyla ATM'nin içerisinden çıkan paraların, dolandırıcılar tarafından sonradan alınmasıdır. Müşterinin hesabından çektiği para, para çıkış haznesi kapağı ile sonradan eklenen sahte kapak arasında sıkıştırılmış veya gizlenmiş durumdadır. Müşteri ATM'den para çekmiştir fakat hazne açıldığında hesabından düşen miktar hazne içerisinde görünmemektedir. Müşteri ATM'den ayrıldıktan sonra dolandırıcı sahte kapaktaki yapıştırıcı tarafından tutulan banknotları ele geçirir.

Para sıkıştırma düzenek örneği:

Görsel 20: *Para sıkıştırma aparatı*
Kaynak: TBB – Çalışma Grubu

ATM Dolandırıcılıklarından Korunma Yöntemleri

1. ATM'den işlem yaparken kart giriş yuvasının veya klavyenin hasarlı olup olmadığı, ATM üzerinde normalden farklı bir aparatın takılı olup olmadığına dikkat ediniz.
2. Kurcalanmış, delinmiş veya herhangi bir yeri hasar görmüş ATM'den işlem yapmayınız.
3. ATM'den işlem yaparken şifrenizi elinizle gizleyerek giriniz ve kimseye göstermeyiniz.
4. Kartınızın sıkışması durumunda, varsa banka görevlisinden yoksa çağrı merkezini arayarak yardım alınız. Bankanızdan bilgi alana kadar ATM başından ayrılmayınız.
5. Kartınızın ATM'de sıkışması, alıkonulması gibi durumlarda size yardımcı olmak isteyen kişilerden yardım almayınız.

ATM Dolandırıcılıklarına Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler

Kartınızı muhafaza ederek hemen bankanıza bilgi verip hemen kullanıma kapattırınız.

F) POS Dolandırıcılıkları

Basit bir ödeme aracı olarak kullanılan POS (Point Of Sale) sistemleri, yaygın kullanımı nedeniyle dolandırıcılar tarafından da hedeflenen önemli bir kanal haline gelmiştir. POS cihazları kart kopyalama işlemlerinde kullanılabildiği gibi, sanal ortamda ele geçirilen kart bilgileri ile işlem yapma amacıyla da dolandırıcılar tarafından kullanılabilmektedir. POS aracılığı ile gerçekleştirilen dolandırıcılıklardan en sık karşılaşılanlar aşağıda yer almaktadır.

• POS Kart Kopyalama

Dolandırıcılar tarafından POS cihazlarına kopyalama programları yüklenerek veya kullanıcıların görmeyeceği bir yerde saklanan kart kopyalama cihazı ile kart manyetik verilerinin ele geçirilmesidir.

Senaryo 1

Son derece başarılı bir yatırım uzmanı olan Erdem akşam eşi ve çocukları ile yemeğe çıkmıştır. Yemekten sonra biraz yürümek için ailecek deniz kenarına inmişlerdir. Bu sırada Erdem'in küçük oğlu Eğmen babasından kâğıt helva ve içecek bir şeyler ister. Biraz ilerde büfeden kâğıt helva içecek ve mısır alan Erdem yanında nakit olmadığı için kartla ödeme yapmak ister.

Büfeci POS cihazının şarjının çok az olduğunu şarjdan çıkaramayacağını bundan dolayı kartını vermesini ister. POS cihazı Erdem'in göremeyeceği ve ulaşamayacağı bir noktada olduğu için şifresini büfedeki satıcıya söyler ve satıcı şifreyi girip ödemeyi aldıktan sonra kartını teslim eder.

Yaklaşık iki hafta sonra pazar günü saat 10 gibi uyanan Erdem telefonuna gelen mesajları kontrol ettiğinde bir anda şok olur, çünkü akşam saat 11'de uyumuştur ama gece boyu hesabından para çekildiği yönünde mesajları görmüştür. Hemen hesaplarını kontrol etmek için mobil bankacılığına girer. Hesabına baktığında ise kartı ile farklı ATM'lerden 11.600 TL çekildiğini görür. Ancak kartını kontrol ettiğinde kartının da cüzdanında olması nedeniyle bu işe bir anlam veremez ve bankasını arayarak kartını kullanıma kapattırır. Banka personelinin yönlendirmesi ile gerekli işlemleri başlatan Erdem savcılığa da suç duyurusunda bulunur.

Yine bir Pazar günü evinde tabletinden haberleri takip eden Erdem gördüğü bir haber sonrasında birkaç ay önce başından geçen olayı anlamlandırır. Haberde, İstanbul'da bir büfede müşterilerinin kartlarını alarak POS cihazında kopyalayan şebeke çökertildi, şebekenin yaklaşık 300 adet kartı kopyaladığı ve 3,5 milyon TL tutarında bir vurgunda bulunduğu bilgisi verilmektedir. Erdem kendisinin de bu mağdurlardan biri olduğunu anlar.

• CNP (Card Not Present) İşlem Dolandırıcılığı

Üye işyerlerimizde en sık karşılaşılan dolandırıcılık olaylarının başında CNP işlem dolandırıcılıkları gelmektedir. CNP işlem, kartın fiziki olarak kullanılmadığı işlemlerdir. CNP işlem dolandırıcılıkları mail order işlemlerinde öne çıkmaktadır. Sadece kart bilgileri girilerek gerçekleşen, yüz yüze satış niteliği taşımayan işlemlerin tamamı CNP işlemleri kapsamaktadır.

Senaryo 1

Anıl Bey işyerinde yoğun bir şekilde çalışırken öğlen vakti bir telefon gelir. XX Bank'tan aradıklarını söyleyen dolandırıcı kart aidatlarının iadesinin yapılacağını söyleyerek bu işlemi tamamlaması için Anıl Beyden kart bilgilerini ve şifresini talep eder. O sırada kafası işle meşgul olan Anıl Bey çok fazla düşünmeden bilgilerini paylaşır. Dolandırıcılar gün içerisinde kendisine dönüş yapılacağını söyleyerek görüşmeyi sonlandırır. Anıl Bey ile beraber 20 farklı kişinin aynı yöntemle bilgilerini ele geçiren dolandırıcı bu kartlar ile harcama yapabileceği uygun bir yer bulmak için araştırma yapmaya başlar. Dolandırıcı, bu esnada gezindiği sitelerin birinde Ada Otel reklamını görür ve hemen arayarak kendini acente olarak tanıtıp Ada Otel sahibi Bekir Bey'den oteline rezervasyon yaptırmak için tarih ve oda bilgilerinin müsaitlik durumunu iletmesini ister.

Bekir Bey Antalya'da uzun yıllardır otel işletmeciliği gerçekleştirmektedir. Yaz sezonunun başlayacak olması ve işlerinin açılacağı için heyecanlıdır. Bekir Bey, rezervasyon talep edilen tarihler ve oda bilgileri için otelinin müsait olduğunu iletir. Dolandırıcı 20 farklı kişi adına farklı tarihler için yaklaşık 300.000 TL işlem gerçekleştirmek istediğini yurtdışı kart ile mail order POS işlemi yapıp yapamayacağını sorar. Bekir Bey, yapabileceğini iletir. Dolandırıcı ele geçirdiği kart bilgilerini Bekir Bey'e iletir. Bekir Bey mail order POS üzerinden işlemleri gerçekleştirerek rezervasyonları tamamlar.

Dolandırıcı aynı zamanda rezerve edilen odaları internet üzerinden farklı kişilere uygun fiyatlarla satarak kazanç sağlar. Gerçek kart hamilleri, kartlarından gerçekleşen Ada Otel işlemlerini görür ve kendilerinin yapmadığı işlemler olması nedeniyle kart bankalarına "ben yapmadım" nedenli itirazlarda bulunur. İtirazlar gelmeye başlayınca hem Banka yetkilileri hem de Bekir Bey işlemlerin dolandırıcılık kaynaklı olduğunu anlar. Mağdur olan tüm taraflar konu ile ilgili savcılığa giderek suç duyurusunda bulunurlar.

• Sahte/Kayıp/Çalıntı Kart Kullanımı

POS/ATM aracılığı ile kopyalanan kartlar ile ya da çalıntı/kayıp kartların üye işyerlerindeki POS cihazlarında kullanılması ile gerçekleştirilen dolandırıcılık işlemleridir. Bilgileri ele geçirilen kartlar ile hem fiziki (sahte kart üretilerek), hem de fiziki olmayan (mail order, sanal pos, vb kartsız işlem yapılan kanalar üzerinden) POSlar üzerinden işlemler gerçekleştirilebilir.

POS Dolandırıcılıklarından Korunma Yöntemleri

POS'dan işlem yapılırken kart şifresi kimsenin görmeyeceği şekilde giriniz, POS cihazının kart girişinde normal olmayan bir donanım ya da aparat varsa işlem yapmayınız. Kart bilgilerini güvenilmeyen e-ticaret sitelerine girmeyiniz, güvenli olmayan ortamlarda ya da arayan kişilerle paylaşmayınız.

POS'dan işlem yapılırken şifrenizi kendiniz giriniz, kimseyle paylaşmayınız. Alış veriş esnasında asla kartınızı satıcıya verip kendisinin işlem yapmasına izin vermeyiniz.

POS cihazının bir ürün/hizmet karşılığında ödeme yapılırken kullanıldığını unutmayınız. Bunun haricinde nakit/komisyon karşılığı yapılan işlemler yasal olmadığı için ne POS sahibi ne de kart sahibi olarak buna aracılık etmeyiniz.

POS Dolandırıcılıklarına Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler Yapmalı

Kartınız ile ilgili bir dolandırıcılık durumuna maruz kaldığınızda vakit kaybetmeden Bankanız ile iletişime geçerek kartlarınızı ve hesaplarınızı güvenlik altına alınız.

BÖLÜM 3

Bilgi ve Belge Sahteciliği

III. Bilgi ve Belge Sahteciliği

Kötü niyetli kişiler tarafından düzenlenen sahte bilgi ve belgeler (kimlikler, sahte hesap cüzdanları, talimatlar vb.) yoluyla bankalara sahte başvurular yapılarak, bazı işlemler gerçekleştirilebilmektedir. Teknolojideki gelişmeler ve bankacılık sistemlerinde kullanımının yaygınlaşması ile birlikte banka sistemlerinde birçok başvuru kontrol mekanizması kurulmuş olmasına rağmen kötü niyetli kişilerin de gelişen teknolojiye ayak uydurarak tekniklerini geliştirdikleri görülmektedir.

A) Kimlik Belgesi Türleri ve Özellikleri Kimlik Belgesi

Bir insanın kim olduğunu kanıtlayan belge olarak kullanılmakta olan kimlik, geçmişten günümüze nitelikleri değişerek gelmiş; önemi ve güvenlik ögeleri gün geçtikçe artmıştır.

Osmanlı Devleti zamanında "Devleti Aliyye-i Osmaniyye Tezkiresi" adıyla kullanılmaya başlayan kimlik belgesi, kişinin adı, anne adı, baba adı, milleti, mesleği, göz rengi ve boyu ile ilgili bilgileri içerecek şekilde düzenleniyordu.

Daha sonraları 1926 yılında defter biçimini alan "Nüfus Cüzdanı", 1976 yılında tek sayfalık bir belge halini almıştır.

4 Mart 2016 tarihi itibari ile pilot olarak belirlenen illerde, 2 Ocak 2017 tarihi itibariyle de ülke genelinde uluslararası standartlara uygun "Türkiye Cumhuriyeti Kimlik Kartı" kullanılmaya başlanmıştır.

> Üzerinde T.C. kimlik numarası olan ve özel kanunlarında resmî kimlik hükmünde olduğu açıkça belirtilen belgeler göre bankacılık işlemlerinde kullanılabilmektedir

Bankacılık sektöründe gerçek kişilerde kimlik tespiti için Türkiye Cumhuriyeti Kimlik Kartı (TCKN), nüfus cüzdanı, ehliyet ve pasaport başta olmak üzere, birçok kimlik tipi kullanılabilmektedir.

Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmeliğinin **"Gerçek Kişilerde Kimlik Tespiti"** başlıklı 6'ncı maddesinde; kimlik doğrulamasının hangi tür belgeler ile yapılabileceği belirtilmiştir. 14.12.2017 tarihinde Resmî Gazete'de yayımlanan değişiklikle ise bu maddede yer alan kimlik bilgilerinin teyit edilebileceği belgeler arasına **"Üzerinde T.C. kimlik numarası bulunan ve özel kanunlarında resmî kimlik hükmünde olduğu açıkça belirtilen kimlik belgelerinin eklendiği"** bilgisi iletilmiştir. Buna göre, avukat kimliği başta olmak üzere, bazı mesleki kimlikler, geçici koruma belgeleri de bankacılık işlemlerinde kabul görmeye başlamıştır.

Türkiye Cumhuriyeti Kimlik Kartı (Yeni Kimlik) Özellikleri

Türkiye Cumhuriyeti Kimlik Kartı, dünyadaki teknolojik gelişmelere uygun olarak güvenli kimlik doğrulama alanında sayısız fayda sağlamakla birlikte yeni kullanım alanlarına açık bir mimaride tasarlanmış olup temaslı ve temassız yongaya sahiptir. Yonga içerisindeki bilgilerin okunması suretiyle elektronik bankacılık kanal aktivasyonu ve biyometrik kimlik doğrulaması yapılabilmektedir. Kimlik ve biyometrik veriler yüksek güvenlikle muhafaza edilmektedir.

Türkiye Cumhuriyeti Kimlik Kartı Ön Yüz Üzerinde Yer Alan Bilgiler:

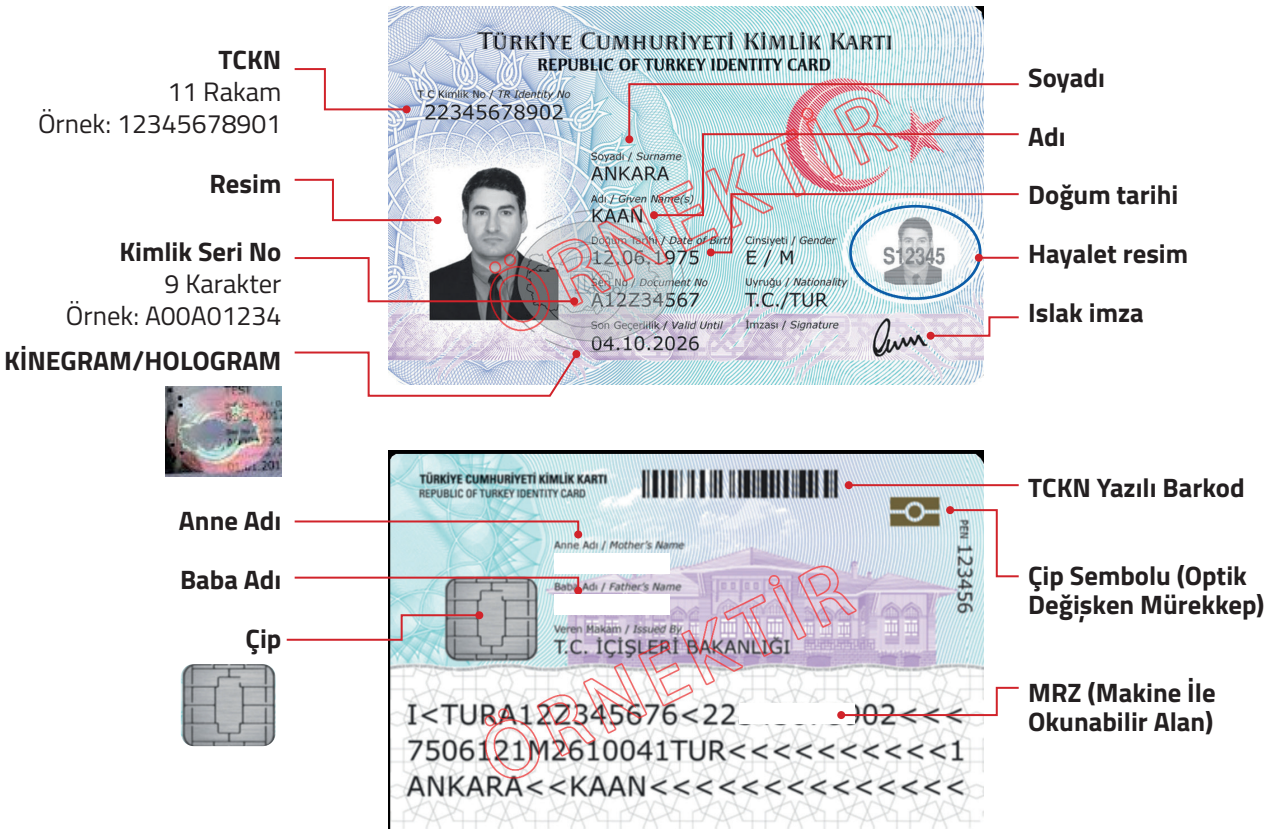
11 Haneli TCKN
Adı /Soyadı
Doğum Tarihi (Gün/Ay/Yıl)
Belgeyle Bütünleşik Biyometrik Fotoğraf
9 Haneli Kimlik Seri No
Ay Yıldız/TC Teması İçeren Kinegram/ Hologram
Kimlik Son Geçerlilik Tarihi (Gün/Ay/Yıl)
Biyometrik Fotoğraf ile Aynı Olan, Belgeyle Bütünleşik Hayalet Resim
Islak İmza

Türkiye Cumhuriyeti Kimlik Kartı Arka Yüz Üzerinde Yer Alan Bilgiler:

Anne Adı
Baba Adı
Yonga (Çip)
TCKN Bilgisini İçeren Barkod Yonga (Çip) Sembolü (Optik Değişken Mürekkep)
Rakamsal Karakterleri Harf Karakterinden Büyük MRZ Alanı

Görsel 22: *Yeni kimlik kartı*
Kaynak: TBB – Çalışma Grubu
Kaynak: (https://www.nvi.gov.tr/tc-kimlik-karti)

Örnek Kimlik Kartı Görseli



Görsel 23: *Yeni kimlik kartı*
Kaynak: TBB – Çalışma Grubu

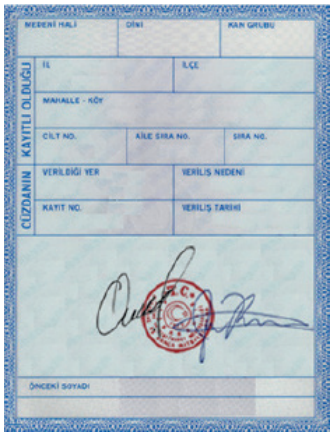
Nüfus Cüzdanı (Eski Kimlik) Özellikleri

Nüfus cüzdanı, vatandaşlarına devletçe verilen, kimlikleriyle kişisel durumlarını gösteren resmî belgedir. 29 Ekim 2000 tarihinde bilgisayar ortamında tutulan nüfus kütükleriyle eşleştirilerek 10,9x7,8 cm ebatlarında kart şeklindeki nüfus cüzdanları basılmaya başlanmıştır. Kadınlar için pembe erkekler için mavi renkteki nüfus cüzdanlarına 2001 yılında TC kimlik numaraları yazılmaya başlanmıştır.

Nüfus Cüzdanı (Eski Kimlik) Ön Yüz Üzerinde Yer Alan Bilgiler:

- 9 Haneli Kimlik Seri No
- 11 Haneli TCKN
- Adı - Soyadı
- Baba Adı
- Ana Adı
- Doğum Yeri ve Tarihi
- Belge üstüne yapıştırılmış fotoğraf
- Ay Yıldız/TC teması

Nüfus Cüzdanı (Eski Kimlik) Arka Yüz Üzerinde Yer Alan Bilgiler:



- Medeni hali
- Dini
- Kan grubu
- Cüzdanın kayıtlı olduğu il, ilçe, mahalle-köy
- Cilt No / Sıra No/ Aile Sıra No
- Verildiği Yer / Tarihi
- Veriliş nedeni
- Kayıt No
- Nüfus Müdürü Adı Soyadı, İmzası
- Önceki Soyadı

***Görsel 24**: Eski kimlik kartı Kaynak: TBB – Çalışma Grubu*

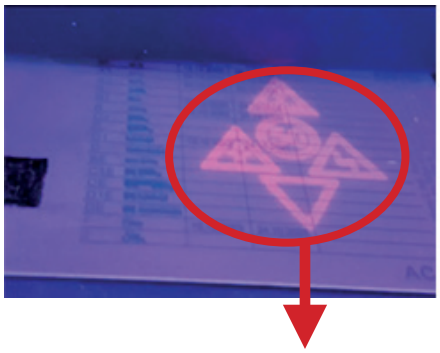
Görsel 25: *Güvenlik ögeleri Kaynak: TBB – Çalışma Grubu*

Yeni Sürücü Belgesi (Ehliyet) Özellikleri

Uluslararası standartlara uygun şekilde polikarbonat malzemeden lazer baskı ile üretilen sürücü belgeleri, özel renk ve mikro harfler içeren karmaşık bir tasarıma sahiptir. Kartın içerisinde, ultraviyole ışığa tutulduğunda görülen yazı ve şekiller bulunmaktadır. Kartta renkli güvenlik mürekkepleri ile gökkuşağı ve giyoş baskı (Banknot baskısında da kullanılan çok ince çizgi ve yazılardan oluşan bir teknik) kullanılmaktadır. Fotoğraf, karta lazer baskı ile işlenmiş olup fotoğraf üzerinde oynamaya veya kopyalamaya karşı özel hologram kullanılmıştır. Böylece tarama, baskı ya da kopyalama yoluyla kartın taklit edilmesinin önüne geçilmesi amaçlanmıştır.

Yeni Ehliyet Ön Yüzünde Yer Alan Bilgiler

Belgeyle Bütünleşik Biyometrik Fotoğraf	11 Haneli TCKN Belge Numarası
Adı ve Soyadı	İmza
Doğum Tarihi/Yeri	Beyaz Işık Hologramlı
İlk Veriliş Tarihi	Türkiye Haritası
Geçerlilik Tarihi	Mor Işıkta Parlayan "TR" ve Al Bayrak
Verildiği Yer	



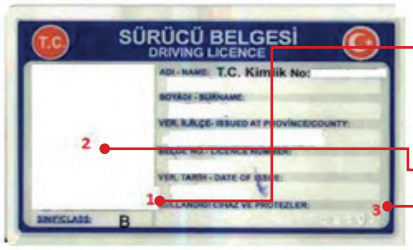
Yeni Ehliyet Arka Yüzünde Yer Alan Bilgiler

TCKN ve Belge No İçeren QR Kod
Ehliyet Sınıfı
Alınış Tarihi
Geçerlilik Tarihi
Kan Grubu

Eski Sürücü Belgesi Ehliyet Özellikleri

Türkiye sınırları içerisinde motorlu araç kullanımı için gerekli bir belge olan sürücü belgeleri, aynı zamanda bankalarda gerçek kişi kimlik tespitinde önemli bir kimlik belgesi olarak kullanılmaktadır.

Üzerinde yer alan kimlik bilgileri, ehliyet sınıfı ve fotoğraf bilgilerinin sert plastik üzerine pres baskı ile aktarılması ile oluşan kimlik türünde kontroller belge numarası üzerinden değil kimlik bilgileri ve fotoğraf eşleşmesi ile yapılabilmektedir.



- Fotoğrafın sağ alt köşesinde parmakla hissedilecek şekilde soğuk mühür bulunmalıdır. Mührün ortasında ay-yıldız simgeleri, çeperinde ise TC İç İşleri Bakanlığı Emniyet Gn. Md.lüğü yazısı yazıldığı şekliyle bulunmalıdır
- Fotoğrafın kenarları oval olmalıdır.
- Sağ alt köşede parmakla hissedilen 5 haneli numara yer almalıdır.

- Sağ kenarda seri numarası yer almalıdır.

Görsel 27: Ehliyet Belgesi kaynak: TBB – Çalışma Grubu

Eski Sürücü Belgesi (Ehliyet) Ön Yüz Üzerinde Yer Alan Bilgiler:

Belgeyle Bütünleşik Fotoğraf
11 Haneli TCKN
Adı, Soyadı
Verilen il/ilçe
Belge No
Veriliş tarihi
Kullandığı cihaz ve protezler
Sınıfı

Eski Sürücü Belgesi (Ehliyet) Arka Yüz Üzerinde Yer Alan Bilgiler:

Doku ve organ bağışı alanı
Nüfusun kayıtlı olduğu il, ilçe,
mahalle/köy
Cilt No
Sayfa
Kütük
Ana - Baba adı
Doğum yeri/tarihi (gün/ay/yıl)
Kan grubu
Düzenleyen sicil
Belge sahibinin imzası ve tarih
Seri No

Passaport Özellikleri

Pasaport; **"Kanunda belirlenen yetkili makamlarca verilen ve hamillerine bir ülkenin milli hudutlarından diğerine geçmeyi sağlayan belgedir."** Ülkemizde Pasaport, yurt dışına çıkmak isteyen kişilere, yerel Emniyet Müdürlükleri'nin, içerisinde bulunan Pasaport Şube Müdürlükleri'nce verilmekte ve aşağıda yer aldığı üzere 4 çeşitten oluşmaktadır.

Mevcut pasaportlara ek olarak, yurt dışında pasaportunu kaybeden kişilerin kişisel olarak T.C. Büyükelçiliği ya da konsolosluklarına başvurmaları halinde geçici (pembe) pasaport düzenlenebilmektedir.

Görsel 28: *Pasaport Kaynak: TBB – Çalışma Grubu*

HUSUSİ (Yeşil)
Devlet memurlarına ya da eski bürokratlara verilir.

UMUMİ (Bordo)
Standart olarak vatandaşlara verilir.

HİZMET (Gri)
Resmî bir kurum tarafından yurt dışına bir görev nedeni ile gönderilen kişilere verilir.

DİPLOMATİK (Siyah)
Devletteki üst düzey görevlere sahip olan kişilere verilir.

E-Pasaport Özellikleri

E-pasaportlar, "Çipli Pasaport" ya da "Biyometrik Pasaport" olarak da tanımlanabilir. Biyometrik bilgileri saklayabilen yongalı (çipli) pasaportlardır. Bu pasaportlar, 01.06.2010 tarihinden itibaren verilmeye başlanmıştır. Polikarbonat malzemeden lazer baskı ile üretilmektedir.

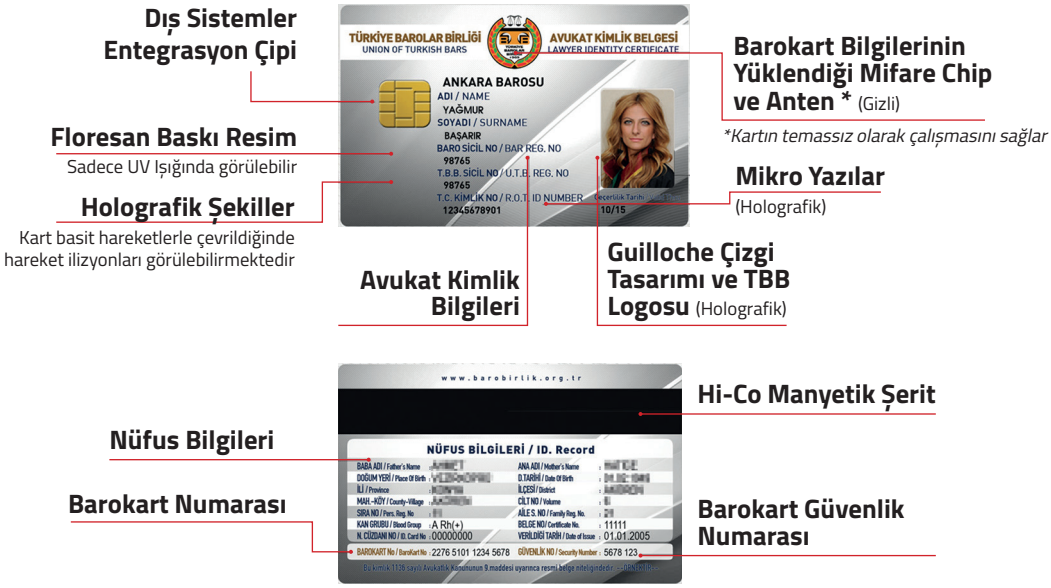
Görsel 29: Pasaport kaynak: TBB – Çalışma Grubu

E-Pasaport İçinde Yer Alan Bilgiler

Parmak izi
Biyometrik fotoğraf
İsim, Soyisim
Cinsiyet
Düzenleme ve geçerlilik tarihi
Uyruk
TCKN
Pasaportu düzenleyen makam
Fotoğraf
Doğum yeri ve tarihi
Dijital imza

Avukat Kimliği Özellikleri

Barolar birliği tarafından çıkarılan ve üzerinde avukatlık bilgileri ile kişinin kimlik bilgilerinin yer aldığı resmî kimlik statüsünde olan kimlik türüdür. Avukat kimliklerinin teyidinde **https://www.barobirlik.org.tr/** ana sayfasında yer alan aşağıdaki sorgulama alanından avukat ad soyadı ile arama yapılıp eğer kayıtlı ise fotoğraf kontrolü yapılabilmektedir.

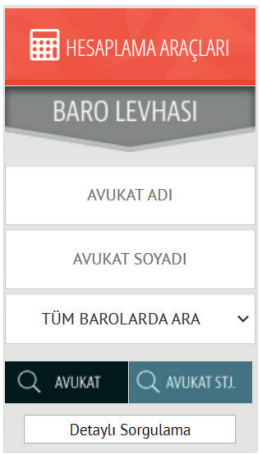


Görsel 30: *Avukat Kimliği Özellikleri Kaynak: https://www.barobirlik.org.tr*

Avukat Kimlik Belgesi Üzerinde Yer Alan Bilgiler

Baro Bilgisi	Baba Adı
Baro Sicil	Anne Adı
TCKN	Nüfus İl
Uyruk	Nüfus İlçe
Ad	Mahalle-Köy
İkinci Ad	Cilt No
Soyadı	Aile Sıra No
Doğum Yeri	Sıra No/Kütük No
Doğum Tarihi	Medeni Hali

Avukat Bilgileri Sorgulama Ekranı



Görsel 31: *Barolar Birliği internet sitesinden sorgulama*
Kaynak: TBB – Çalışma Grubu

B) Sahte Kimlikle İle Yapılan Dolandırıcılıklar

Kaybolan kimlikler veya ele geçirilen kimlik belgeleri ile oluşturulan sahte kimlikler üzerinden en sık yapılan kötü amaçlı işlemler aşağıdadır;

- Kredi, kredi kartı, esnek hesap/KMH ve limit arttırım başvurularında bulunulması
- Şirket/şirketler kurularak Bankalardan çek karnesi talep edilmesi
- Borç taahhütlerine girilmesi/Kefalet verilmesi
- İnternet Bankacılığına başvurulması
- Cep telefonu ekleme/güncelleme/silme işlemi yapılması
- Para transferi ve nakit çekim gibi parasal işlemler yapılması

Bu tür sahte kimlikle yapılan işlemlerin önüne geçmek kimlik türleri ve özellikleri başlığında anlatılan hususlara dikkat edilmesi önem arz etmektedir.

Sahte Kimlikle İle Yapılan Dolandırıcılıklardan Korunma Yöntemleri

Kimlik kopyasının istenmesi durumunda amacı sorgulanmalıdır.

Kimliğin kaybolması/çalınması durumunda vakit kaybetmeden nufüs il/ilçe müdürlüğünde kayıp başvurusunda bunulmalı ve kimlik belgesi güncellenmelidir.

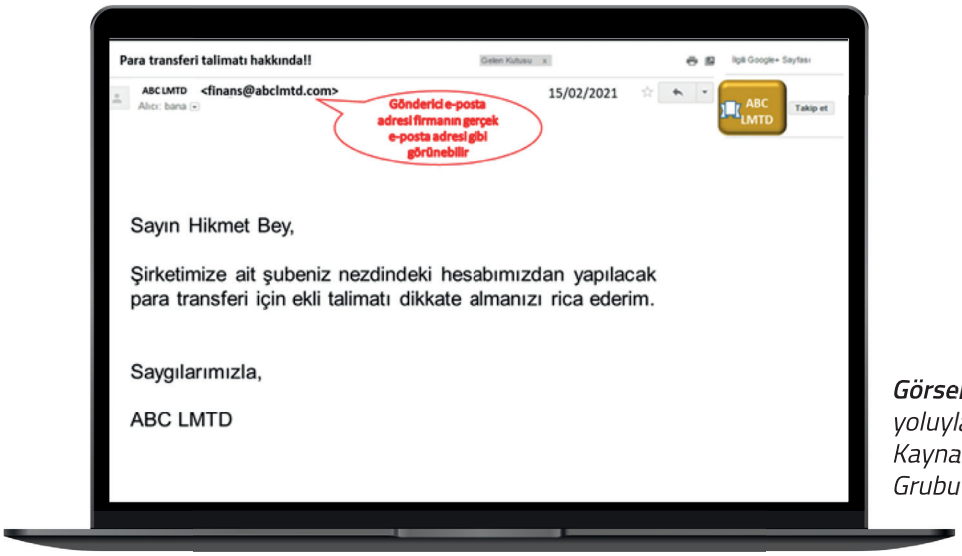
Sahte Kimlikle İle Yapılan Dolandırıcılığa Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler

Müşteri kendisi adına sahte kimlikle işlem yapıldığını öğrendikten sonra işlemin kendisi tarafından yapılmadığını yönünde itirazını Bankasına iletmeli ve Savcılığa Suç Duyurusunda bulunmalıdır.

C) Sahte Talimatla İle Yapılan Dolandırıcılıklar

Günümüzde bankacılık işlemlerinin uzaktan yapılması konusu önem kazanmakla birlikte, müşterilerin internet ve mobil bankacılık gibi bankacılık kanallarından yapamayacakları tutarda işlemler için de uzaktan talimat verme yöntemiyle işlem yapabilmeleri sağlanabilmektedir. Bu tür talimatlar müşterilerin bankalarda kayıtlı olan e-posta ya da fax numaraları üzerinden alınabilmektedir. Özellikle ticari müşteriler ve şahıs işletmelerinin ticari faaliyetlerine ait ödemeler talimatlı para transferleri ile yapılmaktadır.

Sahte talimat ile yapılan dolandırıcılıklar, müşteri e-postasının ele geçirilmesi/taklit edilmesi ile şube personeline sahte talimat iletilmesi ya da müşteri adına şubeye faks ile sahte bir talimat gönderilmesi suretiyle müşteri hesabından para transferi yaptırılmak istenmesi durumudur. Banka tarafında gerekli sistemsel kontroller yapılsa da e-posta hesabının güvenliği gibi müşterilerin de dikkat etmesi gereken konular bulunmaktadır. Aşağıda e-posta aracılığı ile bankaya iletilmiş olan sahte bir talimat örneği (e-posta bildirimi ve Ek'inde yer alan talimat dokümanı) yer almaktadır.



Görsel 32: *E-posta yoluyla sahte talimat*
Kaynak: TBB – Çalışma Grubu

Alıcı firma ve IBAN numarası, müşterinin daha önceki talimatlarda kullanmadığı ve ilk defa bu talimatta ilettiği bilgilerdir.

Görsel 33: *Sahte talimat*
Kaynak: TBB – Çalışma Grubu

Sahte Talimatla İle Yapılan Dolandırıcılıklardan Korunma Yöntemleri

Müşteriler öncelikle ticari yazışmalarda ve bankada talimatlı işlemlerde kullandıkları e-posta adresinin güvenliğini sağlamalıdır. E-posta adresine erişebilen kullanıcılar sınırlı olmalı, erişim şifresi düzenli olarak değiştirilmelidir.

Sahte Talimatla İle Yapılan Dolandırıcılığa Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler

Müşteri kendisi adına sahte talimatla işlem yapıldığını öğrendikten sonra işlemin kendisi tarafından yapılmadığını yönünde itirazını Bankasına iletmeli ve Savcılığa Suç Duyurusunda bulunmalıdır.

Talimatlı işlemlerde kullandığı e-posta adresinin şifresi değiştirilerek güvenliği sağlanmalıdır.

Senaryo 1

Kiraz hanım özel bir şirketin finans müdürü olarak çalışmaktadır. Şirketinin ticari faaliyetleri sonucu yapılması gereken ödemeler ile ilgili bankasına kayıtlı e-posta adresi üzerinden para transferi talimatlarını iletmektedir. Şirkette yoğun günlerinden bir tanesinde talimat vermekte kullandığı şirket e-posta adresine bankasının ismine benzer bir başlık altında bilgilendirme e-postası gelir.

Bu e-posta içerisinde yer alan ve detaylı bilgi için girilmesi istenen linke giriş yaptığında boş bir sayfa açılır. Bu durumu çok fazla dikkate almayan Kiraz Hanım işine döner oysaki şirket e-posta adresi kötü niyetli kişilerce ele geçirilmiştir.

Ele geçirilmiş e-posta üzerinden geçmiş yazışmaları kontrol eden dolandırıcı, Kiraz hanımın daha önce şubeye ilettiği talimat üzerindeki alıcı bilgilerini değiştirerek şubeye 80.000 USD'lik bir sahte talimat göndermiştir. Gelen talimatı ve hangi e-posta adresinden geldiğini kontrol eden şube personeli işlemi gerçekleştirmeden önce müşteriyi sistemde kayıtlı telefonundan aramış ve işleme dair bilgileri teyit amaçlı paylaşması neticesinde talimatı Kiraz hanımın göndermediği ve e-posta adresinin ele geçirilerek bu işlemin yapılmak istendiği anlaşılmıştır.

Bunun üzerine ilgili talimat işleme alınmayarak, müşteri adına dolandırıcılık girişimi olduğu bilgisi Banka Güvenlik Birimi'ne iletilmiştir. Ayrıca müşteriye e-posta adresinin ele geçirildiği, şifresini değiştirmesi gerektiği iletilmiş ve Savcılığa suç duyurusunda bulunması için yönlendirilmiştir.

D) Şirket e-Postasının Ele Geçirilmesi İle Yapılan Dolandırıcılıklar

Banka müşterilerinin, ticari faaliyet içerisinde olduğu şahıs veya firmaların e-posta adresi ele geçirilebilmekte ya da taklit edilebilmektedir. Ele geçirilen/taklit edilen e-posta adresi üzerinden dolandırıcıya ait yeni bir hesap/IBAN numarası gönderilerek para transferlerinin artık bu hesaba yapılması istenmektedir. Banka müşterisi ise ticari faaliyette bulunduğu şahıs veya firmanın bu iletisine istinaden Bankaya vermiş olduğu talimalatlardaki alıcı IBAN numarasını değiştirerek para transflerini gerçekleştirir. Asıl alıcıya yapılması gereken ödemeler yapılmadığı için bir süre sonra dolandırıcılık vakası fark edilir. Bu tip dolandırıcılık vakalarının tespit ve önlenmesinde firmaların kendilerine ait yazışmalarda kullandığı e-posta adresinin güvenliğini sağlaması çok önem arz etmektedir.

Şirket e-Postasının Ele Geçirilmesi İle Yapılan Dolandırıcılıklardan Korunma Yöntemi

E-Posta Adres Güvenliği

Müşteriler öncelikle ticari yazışmalarda ve bankada talimatlı işlemlerde kullandıkları e-posta adresinin güvenliğini sağlamalıdır. E-posta adresine erişebilen kullanıcılar sınırlı olmalı, erişim şifresi düzenli değiştirilmelidir.

Şirket e-Postasının Ele Geçirilmesi İle Yapılan Dolandırıcılığa Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler

Müşteri para transferi yaptığı hesabın manipüle edildiğini öğrendikten sonra dolandırıcılığa maruz kaldığını bankasına iletmeli ve savcılığa suç duyurusunda bulunmalıdır.

Senaryo 1

Kurumsal bir firmada ödemelerden sorumlu olan Rüzgar Beye, İsveç'te ticari faaliyette bulunduğu firmadan bir mail gelmiştir. Banka hesaplarını İngiltere'ye taşıdıklarını ve son gönderilecek olan ürünlerin ödemesini bu yeni hesaba yapmaları belirtilmiştir.

Karşı tarafından kayıtlı e-posta adresinden bu bilgi iletildiği için Rüzgar Bey doğruluğunu sorgulayıp teyit etmeden, iletilen yeni hesap bilgilerini alarak 95.000 EUR'luk talimatı oluşturur ve şubesine iletir.

Bir hafta sonra İsveç firmasından gelen e-postada ödemenin henüz yapılmadığı bilgisini alan Rüzgar Bey, işlemin akıbetini sorgulamak için Şubesi ile görüşür. Şubeden talimattaki IBAN'a para transferinin yapıldığının bilgisini alan Rüzgar Bey, firma ile irtibata geçerek kendisine yeni gönderilen IBAN numarasına para tranferinin yaptığını söyler. Firmadan böyle bir hesap değişikliği talebi olmadığı bilgisini alır. Alıcı hesap bilgisi değişikliğini teyit etmeden para transferi talimatını onayladığı için firması zarara uğramıştır. Rüzgar Bey bankası ile iletişime geçerek dolandırıcılığa maruz kaldığını bildirir. Bankası, savcılığa suç duyurusunda bulunması için kendisini yönlendirir.

E) Şirketin Üst Düzey Yöneticisinin e-Postasının Ele Geçirilmesi İle Yapılan Dolandırıcılıklar

Firma üst düzey yöneticisinin (CEO/CFO vb.) e-postalarının ele geçirilmesi veya taklit edilmesi ile firmanın finans/muhasebe çalışanına e-posta ile sahte talimat gönderilerek, çalışanın kendisine gelen bu bilgilerle para transferi yapmasını istemesidir. Bu dolandırıcılık yönteminde, firma CEO/CFO vb. gibi davranılarak telefon ve diğer iletişim kanalları (anlık mesajlaşma uygulamaları vb.) üzerinden bankadan bilgi edinilmeye çalışıldığı ve hatta para transferi yapılmaya çalışıldığı da bilinmektedir.

Şirketin Üst Düzey Yöneticisinin e-Postasının Ele Geçirilmesi İle Yapılan Dolandırıcılıklardan Korunma Yöntemleri

Bu tür dolandırcılık girişimlerinde şirket çalışanlarının dikkat etmesi gereken önemli noktalar bulunmaktadır.

YÖNETİCİDEN TEYİT

Şirket çalışanı, talimat firma üst düzey yöneticisinden gelse dahi doğruluğunu teyit etmeden işleme almamalıdır.

Şirketin Üst Düzey Yöneticisinin e-Postasının Ele Geçirilmesi İle Yapılan Dolandırıcılığa Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler

Müşteri bu tür dolandırıcılığa maruz kaldığını bankasına iletmeli ve savcılığa suç duyurusunda bulunmalıdır.

Senaryo 1

Kurumsal bir firmada ödemelerden sorumlu olan Hakan Beye, aynı firmada üst düzey yönetici olan Arif Beyden bir mail gelmiştir. Arif Bey, gün içerisinde acilen yapılmasını istediği 32.000 USD'lik gecikmiş ödemeleri olduğunu ve gerçekleştirildikten sonra da kendisine bilgi verilmesini iletmiştir.

Ödemelerden sorumlu olan Hakan Bey, üst düzey yöneticisinden gelen bu e-postadaki bilgiler ile hızlıca bir talimat oluşturulması için kendisine bağlı çalışanlara bilgi vermiştir. Pararlelde Arif Beyi arayarak "acil olarak ilettiğiniz 32.000 USD'lik transfer talimatını işleme aldırdım, başka bir isteğiniz var mıdır" demesi üzerine, Arif Bey böyle bir istekte bulunmadığını belirtmiştir. Bunun üzerine Hakan Bey hızlıca çalışanlarına talimatın işleme alınmamasını söylemiştir.

Ayrıca şirketin teknik personeli ile iletişime geçerek Arif Beyin e-posta adresinin kontrol edilmesi istenmiştir. İnceleme sonucunda Arif Beyin e-posta adresinin ele geçirildiği anlaşılmıştır. Hakan Beyin işlemin teyidi için geri bildirim yapması sayesinde şirket önemli bir zarardan kurtulmuştur.

F) Sahte Vekaletname ile Yapılan Dolandırıcılıklar

Vekaletname; müşterilerin kendisi ile ilgili işlemleri, yürütmesi, takip etmesi amacıyla tayin ettiği vekilin yetki sınırlarını gösteren ve Noter aracılığı ile düzenlenen belgedir. Bu belge aracılığı ile para çekme, para transferi dahil olmak üzere birçok bankacılık işlemi yapılabilmektedir. Bu nedenle, kimlik belgesinde yapılan sahtecilik girişimlerine benzer şekilde;

- Bütünüyle sahte bir vekâletname belgesi düzenlenerek herhangi bir noterden onaylanmış gibi işlem yapılmaya çalışılabilir,
- Sahte kimlik ve belgelerle banka müşterisi gibi görünerek gerçek bir notere gerçek bir vekâletname hazırlatılabilir.

Sahte Vekaletname ile Yapılan Dolandırıcılığa Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler

Müşteri kendi adına sahte vekaletname ile işlem yapıldığını öğrendikten sonra işlemle ilgili itirazını bankasına iletmeli ve savcılığa suç duyurusunda bulunmalıdır.

Senaryo 1

Şadi Bey 1965 doğumlu eski askeri personel ve aynı zamanda XXBANK'ın özel bankacılık müşterisidir.

Şadi Bey evinde kahvaltısını yaparken sosyal medya üzerinden arkadaşı Yılmaz'dan bir mesaj alır. Yılmaz önce hal hatırını sorup neler yaptığını sorar sonrada kimsesiz çocuklara yardım için bir çalışmasının olduğunu bunun için de tüm arkadaşlarından destek istediğini iletir. Şadi Bey memnuniyetle kendisine destek olacağını iletir. Bunun üzerine Yılmaz, Şadi Beye katılımı için bir link göndereceğini bu link üzerinden kendisinden istenilen alanları doldurmasını ister. Arkadaşına yardımcı olmak isteyen Şadi Bey gönderilen link üzerinden kimlik görseli dâhil birçok bilgisini girer. Sonrasında telefonunu masaya koyarak bahçeye hava almaya çıkar.

Öğleden sonra saat 14:00 te XXBANK şubesine gelen Umut elindeki vekâletname ile şube personeli Şenay'a Şadi Bey'in damadı olduğunu kendisinin rahatsızlığından dolayı şubeye gelemediğini bir ev almak için hesabından 475.000 TL çekilmesini ve kendisine teslim edilmesini ister. Vekâletnameyi kontrol eden Şenay herhangi bir sıkıntı göremez ve parayı hazırlamak için biraz zaman ister. Umut paranın hazırlanması için bekler.

Bu sırada Şenay parayı hazırlarken yanındaki arkadaşı Hakan'a da durumu anlatır. Şadi Bey ev alıyormuş, en son geldiğinde işlemini sen yapmıştın bu konuda sana bir şey söyledi mi? Hakan bana bir şey demedi kendisi mi geldi diye sorar. Şenay Damadına vekâletname vermiş ödemeyi damadına yapacağım der. Hakan vekâletnameyi Türkiye Noterler Birliği sistemi üzerinden kontrol ettin mi diye sorar. Şenay vekâletnameye dikkatlice baktığını herhangi bir sorun görünmediğini ancak sistemden kontrol etmediğini söyler. Arkadaşının tavsiyesi ile sistemden kontrol etmeye karar veren Şenay, Türkiye Noterler Birliği sistemi üzerinden baktığında bu şekilde bir vekâletname olmadığını görür. Birazda tedirgin olan Şenay Hakan'a vekâletnameyi sistemden teyit edemediğini söyler.

Sakin olmasını söyleyen Hakan belki de sisteme düşmemiştir Şadi Bey'i arayıp teyit edelim der. Şadi Bey'i aradıklarında bu şekilde bir talebinin olmadığını ve kesinlikle bir ödeme yapılmamasını iletir. Durumu şube müdürüne ileten Şenay, müdürün talebi ile polisi arar. Bir süre sona şubeye gelen polis ekipleri Umut'u alarak emniyete götürür. Umut'un alınan ifadesinde Şadi Bey'i uzun zamandır sosyal medya üzerinden fake bir hesaptan takip ettiği, Şadi Bey'in arkadaşı Yılmaz Bey'in hesabını ele geçirerek Yılmaz Bey gibi mesaj attığı ve kişisel bilgilerini bu şekilde elde ettiği ortaya çıkar.

BÖLÜM 4

Uzaktan Kimlik Tespiti & Müşteri Edinimi

IV. Uzaktan Kimlik Tespiti ve Müşteri Edinimi

Uzaktan kimlik tespiti, müşteri temsilcisi ile kişinin; fiziksel olarak aynı ortamda bulunmasına gerek olmadan, çevrim içi olarak görüntülü görüşmesi ve birbiriyle iletişim kurmasıdır. Uzaktan kimlik tespiti için mutlaka yeni T.C. Kimlik Kartına ve akıllı telefona sahip olunması gerekmektedir.

Uzaktan müşteri olmak istenildiğinde, bankaların mobil bankacılık uygulamaları veya web sitesi aracılığı ile başvuru formu doldurarak başvuruda bulunulması gerekmektedir. T.C. Kimlik Kartı ve güvenlik doğrulamalarıyla daha hızlı bir şekilde şube ve evrağa bağlı kalmadan banka müşterisi olunabilmektedir.

Uzaktan müşteri ediniminde, çipli kimliklerdeki bilgilerin temassız olarak okunması, yüz doğrulama gibi adımlar sürecin daha güvenli olmasını sağlamaktadır.

Uzaktan Müşteri Edinim sürecinin yasal dayanağının ve güvenlik standartlarının oluşturulması amacıyla BDDK tarafından çalışmalar sonucu, Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine Ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik 1 Mayıs 2021 tarihinde yürürlüğe girmiştir.

Uzaktan Kimlik Tespiti ve Müşteri Ediniminde Yapılan Dolandırıcılıklardan Korunma Yöntemleri

Şubeden yüz yüze yapılan işlemlerdekine benzer şekilde sahte kimlikle yapılan uzaktan müşteri edinim işlemleri için müşteri olarak dikkat edilmesi gereken önemli noktalar vardır.

- Kimlik belgesi ve üzerindeki bilgilerin güvenliğini azami ölçüde sağlamalı,
- Kimliğin kaybolması, çalınması durumunda zaman kaybetmeden yenisini çıkarmalı ve müşterisi olduğu bankalara bilgi vermelidir.
- Doğrulama işlemi için; hesap açmak istediğiniz banka başka bankadaki hesabınızdan, kendi adınıza çok düşük tutarda para transferi yapmanızı talep edebilir.

Uzaktan Müşteri Ediniminde Yapılan Dolandırıcılıklara Maruz Kalınması Durumunda Müşterinin Yapması Gerekenler

Müşteri kendisi adına müşteri edinimi ve başvurular yapıldığını öğrendikten sonra işlemlerin kendisi tarafından yapılmadığını yönünde itirazını ilgili Bankaya iletmeli ve Savcılığa suç duyurusunda bulunmalıdır.

Senaryo 1

Televizyonda sıkça yayınlanan bankanın uzaktan müşteri edinimi ile ilgili reklamlarını gören Ahmet Bey, mobil bankacılık uygulaması üzerinden müşteri olmak için banka uygulamasını indirerek müşteri olma sürecini başlatır. Mobil uygulama üzerinden gerekli başvuru bilgilerini girip, kimlik kartının çipini okuttuktan sonra görüntülü görüşme asistanına bağlanır.

Bankanın görüntülü görüşme asistanı olan Beste Hanım'ın yönlendirmeleri ile kimlik doğrulama sürecine devam eder. Bu görüşmeler sırasında çok nazik bir şekilde, Beste Hanım'ın tüm direktiflerini uygulayan Ahmet Bey'in giriş yaptığı telefon bilgisinin, müşterinin diğer bankalardaki telefonu ile uyuşmadığına dair uyarı mesajı ekranda çıkar. Bunun yanı sıra, kimlik üzerindeki fotoğraf ve kimliğin yongası üzerinden gelen fotoğraf ile karşısındaki kişiyi karşılaştırdığında birebir benzemediğini tespit eder. Bu verilere göre görüşmedeki kişiden şüphelenen Beste hanım, müşterinin durumdan şüphelenmemesini sağlayarak görüşmeyi sonlandırır ve işlemi şüpheli olarak sonuçlandırarak görüşmenin incelenmesi amacıyla Banka Güvenlik Birimi'ne yönlendirir.

Güvenlik Birimi tarafından yapılan inceleme sonrasında Ahmet Bey'in akrabası olan Salih isimli kişinin, Ahmet Bey'in kimliği ile banka müşterisi olmak istediği tespit edilir. Salih'in bankalardan kredi alamayacak kadar kötü kayıtları olması sebebi ile dolandırıcılık girişiminde bulunduğu anlaşılır. Ahmet ve Salih aynı evde yaşadıkları için Ahmet farkında olmadan kimliği kolayca ele geçirilmiş ve işlem sonrası tekrar yerine konduğu için farkına varmamıştır. Beste Hanım'ın dikkati sonucu Ahmet Bey adına müşteri edinimi yapılması ve olası kredi kullanımlarının önüne geçilmiştir.

BÖLÜM 5

Dolandırıcılıktan Korunma Yöntemleri

V. Dolandırıcılıktan Korunma Yöntemleri

Dolandırıcılıkla mücadele konusunda alınacak önlemlerde hem kurumlara hem de kişilere önemli sorumluluklar düşmektedir. Zaman içinde dolandırıcılar kendilerini geliştirdikçe onlara karşı alınacak önlemler de gelişecektir. Günümüz itibariyle bankalar ve müşteri tarafından dolandırıcılıkla mücadele konusunda alınabilecek önlemlere aşağıda detaylı bir şekilde değinilmiştir.

A. Bankalar Tarafından Kullanılan Güvenlik Unsurları

Bankalar tarafından kullanılan güvenlik unsurları müşterilerin işlem güvenliklerini ve finansal değerlerini korumaya yöneliktir. Bunun için bankalar tarafından sunulan internet bankacılığı, mobil bankacılık, telefon bankacılığı, ATM gibi kanallar ve uzaktan müşteri edinim uygulamaları için yaratılmış en üst düzey güvenlik önlemlerinin alındığı ortamlardır.

Kullanıcı Adı / Müşteri Numarası: Banka tarafından müşteriye özel tanımlanan kişiye özel bir koddur.

Parola / Şifre: Kimlik doğrulamada kullanılan, belirli periyodlarla değiştirilmesi zorunlu olan gizli alfabetik ve/veya rakamsal karakterler dizisidir.

SMS OTP: Elektronik haberleşme işletmecilerinin sunduğu kısa mesaj servisi aracılığıyla iletilen tek kullanımlık paroladır.

Tek kullanımlık parola: Kimlik doğrulamada sadece bir kez kullanılmak üzere rastgele oluşturulan harf ve/veya rakamlar dizisidir.

Hassas veri: Kimlik doğrulamada kullanılan veriler başta olmak üzere; müşteriye ait olan, çeşitli sebeplerle bankaca muhafaza edilen ve üçüncü kişilerce ele geçirilmesi halinde, bu kişilerin müşteri olan kişilerle ayırt edilebilme mekanizmalarının zarar göreceği ve dolandırıcılık ya da müşteriler adına sahte işlem yapılmasına imkân verebilecek nitelikteki verilerdir.

Güvenlik Resmî: Bankalar tarafından internet bankacılığına girişte gösterilen ve daha önce müşteri tarafından seçilmiş olan resim/koddur. Bu sayede müşterinin giriş yaptığı sitenin müşterinin bankasına ait olduğu teyit edilmektedir.

Elektronik İmza: 15.01.2004 tarihli ve 5070 sayılı Elektronik İmza Kanununda tanımlanan kişiye özel elektronik imza sertifikasıdır.

Müşteri Bilgilendirmeleri: Bankaların internet sitelerinde veya e-posta/SMS yolu ile müşterilerine güvenlik ile ilgili yapmış oldukları bildirimlerdir.

Mobil Cihaz Onayı: Aktifleştirilimiş mobil cihazlar üzerinden alınan onaylardır.

Biyometrik kimlik doğrulama: Kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla kullanılan bir kişiye özgü ölçülebilir biyolojik veya davranışsal karakteristiğidir.

Yakın Alan İletişimi (NFC): Elektronik cihazların güvenilir, temassız işlem yapabilmesini ve sayısal içeriğe ve/veya elektronik cihazlara erişimini mümkün kılan, veri okuma ve yazmakta kullanılan kısa menzilli kablosuz teknolojidir.

B. Müşteriler Tarafından Alınması Gereken Önlemler

Bankalar tarafından alınan güvenlik önlemleri tek başına yeterli olmamaktadır. Alınan bu önlemlere ek olarak banka müşterilerinin de öncelikli olarak alması gereken bazı önlemler ve uyması gereken kurallar mevcuttur.

Bildirimlerle Gelen Linkler:

Kaynağından emin olmadığınız kısa mesaj (SMS), sosyal medya reklamları, anlık haberleşme uygulamalarından gelen mesajları ve e-posta iletilerini açmayınız ve içerisindeki linklere tıklamayınız.

Mobil Uygulamalar:

Bilinen yaygın uygulamalar haricinde, güvenliğinden emin olmadığınız uygulamaları yüklemeyiniz. Resmî uygulama mağazaları dışındaki ortamlardan uygulama indirmeyiniz.

Kimlik Bilgilerinin Gizliliği:

Banka işlemlerinde kullanılan kimliklerin güvenliği son derece önem arz ettiğinden; kimliklerin taranmış görüntüleri bilgisayarlarda saklanmamalı, fotokopileri rastgele yerlerde bulundurulmamalıdır.

Kart Bilgilerinin Güvenliği:

Kart bilgileri kişiye özeldir ve bu bilgilerin gizliliğini (kart numarası, son kullanma tarihi, güvenlik kodu/CVV2 kodu) koruyunuz. Güvenliğinden emin olmadığınız web siteleri, uygulamalarda kullanmayınız, üçüncü kişilerle paylaşmayınız. Kredi kartı ile sanal ortamlarda yapılan alışverişlerde sanal kart tercih ediniz.

Şifre/Parola Bilgilerinin Gizliliği:

Bankacılık işlemlerinde kullanılan şifre/parola (kart şifresi, tek kullanımlık şifre dahil olmak üzere) kişiye özeldir ve gizliliğinin sağlanması müşteri sorumluluğundadır. Şifre/parola bilgisinin kolay tahmin edilemeyecek şekilde (doğum tarihi vb.) oluşturulması önemlidir.

Görsel 34: *Şifre gizliliği Kaynak: TBB – Çalışma Grubu*

Ortak kullanıma tahsis edilmiş ve güvenliğinden emin olunmayan cihazlardan bankacılık uygulamalarına/kanallarına giriş yapılmaması önerilir. Ayrıca ortak kullanıma (kamuya) açık kablosuz internet bağlantıları üzerinden bankacılık işlemlerinin yapılmaması tercih edilmelidir. ATM ve POS gibi kamuya açık alanda yapılan bankacılık işlemlerinde kullanılan şifrelerin, başkaları tarafından görülmeyecek şekilde girişinin yapılması önemlidir.

Bankalardan Gelen Bildirimler:

Ürünlerin güvenliği ile ilgili hususlar hakkında bankalar tarafından verilen bilgilerin/açıklamaların okunması ve belirlenen talimatlara uygun olarak işlem yapılması güvelik açısından büyük önem arz etmektedir.

Güvenlikle ilgili herhangi bir tereddüt oluşması durumunda mutlaka bankaya başvurulmalı ve bilgi verilmelidir. Unutulmamalıdır ki, bankalar kişisel bilgileri müşterilerinden e-posta yoluyla asla talep etmezler.

Kişisel bilgileri soran e-posta ve/veya e-posta içerisinde yer alan linkler üzerinden bilgi paylaşılmamalı, cevap verilmemeli ve bu tür bir durumla karşılaşıldığında ilgili bankaya bilgi verilmelidir.

Bankalarca yapılan güvenlik duyuruları takip edilmeli ve bu duyurularda iletilen uyarılara dikkat edilmelidir.

Bankacılık İşlemi Yapılan Cihazların Güvenliği:

Bankacılık işlemi yapılan cihazların işletim sistemi ve internet tarayıcısı güncel tutulmalı, bu cihazlarda lisanslı "anti-virüs" yazılımları kullanılmalı ve bu yazılımlar periyodik olarak güncellenmelidir. Bankacılık işlemlerinde kullanılan cep telefonu dahil olmak üzere tüm cihazların güvenliği müşteri sorumluluğunda olup, bu cihazların üçüncü kişilerin kullanımına izin verilmemelidir.

İletişim Bilgilerinin Güncelliği:

Bankanın müşteri adına yapılan işlemlerle ilgili bilgilendirme yaptığı ve şüpheli işlem bildiriminde ulaşmak için kullandığı iletişim adreslerinin (cep telefonu numarası, e-posta bilgisi, ev/iş adresi vb.) banka kayıtlarında daima güncel tutulması önemlidir. Bu adreslerde yapılan değişiklikler müşteri tarafından bankaya zamanında bildirilmelidir.

C. Bilgi Güvenliği

Bilgi güvenliği, bir varlık olarak bilginin izinsiz ve yetkisiz kullanımının, üçüncü kişilerce ele geçirilmesinin, yok edilmesinin, değiştirilmesinin ve bilgilere hasar verilmesinin önlenmesi amacıyla kurumlar nezdinde alınan önlemler, bu amaçla kurulan sistemler ve işletilen politikalar olarak ifade edilebilir.

Veri sızıntısı ise kurum ve müşterilere ait verilerin bilinçli veya bilinçsiz şekilde izin alınmadan kurum dışına taşınarak belirlenmiş bilgi güvenliği politikalarının ihlalidir.

Veri Sızıntısına Sebep Olan Yöntemler

Kurumda bilgiler sunucu, kişisel ve dizüstü bilgisayarlar, tabletler, akıllı telefonlar, veri tabanı, elektronik posta, taşınabilir diskler, CD/DVD ROM, kâğıt, gibi ortamlarda yer alabilmektedir. O nedenle veri sızıntısı vakalarında, bu ortamlara yönelik atak yapılmakta ve elde edilen bilgiler hızlıca kurum dışına çıkarılmaya çalışılmaktadır. Veri sızıntısına yol açan ihlaller aşağıdaki yöntemlerle gerçekleşebilmektedir.

Giden E-posta:

E-posta iletileri, sistemde bulunan her türlü veriyi sızdırmak için kullanılabilir. Bu veriler, bir e-posta veya metin mesajı ya da bir dosya eki olarak üçüncü taraflara aktarılabilir.

Güvenli Olmayan Cihazlara İndirilen Dosyalar:

Kurum tarafından kullanıcıya tahsis edilmemiş cihazlar (kişisel kullanımda olan cep telefonu, bilgisayar, usb, tablet, CD/DVD rom, kamera vb.) ile herhangi bir kurum verisinin indirilmesi, kopyalanması suretiyle veriler kurum dışına çıkarılabilir. Güvenli olmaması ve kurum tarafından izlenememesi nedeniyle verilerin bu cihazlarda tutulması çok risklidir.

Fiziki Belgeler ve Çıktılar:

Fiziki belgeler üzerinde yer alan veriler ve dijital ortamdan alınan fiziki çıktılar en az dijital ortamda saklanan veriler kadar önemlidir. Bu ortamlarda yer alan verilerin kontrolü ve takibi zor olduğu için veri sızıntısında kullanılan önemli yöntemlerdir. Ayrıca, bireylerin ve şirketlerin değersiz olarak nitelendirdikleri, üzerinde bilgi bulunan her türlü materyallerin çöplüklere atılabildiği ve bu atıkların kötü niyetli kişiler tarafından bilgiye erişmek amacıyla toplandıkları görülmüştür. Bir çöp konteynerindeki atıklarda, kurumun iş yaptığı kişilere ait telefon bilgileri, organizasyon çalışanlarının adı, soyadı, unvanları, toplantı konu ve tarihleri, günü geçmiş DVD, CD, hesap ekstreleri, dekontlar gibi kaynaklar bulunabilmektedir.

Veri Sızıntısından Korunma Yöntemleri

Bilgi güvenliği prensiplerinin uygulanmasından kurumun kendisi kadar çalışanları da sorumludur. Kurum, veri sızıntısının önüne geçmek için gerekli teknik altyapıyı kurmalıdır ve bu sistemleri düzenli olarak güncellemelidir. Çalışanlar ise, gerek kurum tarafından tahsis edilen cihazların güvenliğini sağlamakla ve uygulamalarda kullanılan kimlik doğrulama unsurlarını korumakla yükümlüdür. Veri sızıntısının önüne geçmek için dikkat edilmesi gerekenler aşağıda özetlenmiştir:

Parola Güvenliği

Farklı Parola:

Her hesap için farklı bir parola kullanın; kurum içinde kullandığınız parolaları farklı bir yerde kullanmayın.

Kamuya Açık Bilgisayarlar:

Güvenliğinden emin olmadığınız veya yönetimi sizde olmayan kamuya açık bilgisayarlarda ya da ağlarda parolanızı kullanmayın.

İki Aşamalı Doğrulama:

Kullanabildiğiniz her yerde iki aşamalı kimlik doğrulama kullanın.

Şifre Gizliliği:

Parolanızı asla kimseyle paylaşmayın.

Parola Değişikliği:

Kimlik bilgilerinizi ve size ait bilinen bilgileri parolanızda kullanmayın, parolanızı düzenli olarak değiştirin,

Güçlü Şifre/Parola:

Parolalarınızı, karışık karakter ve rakamlar kullanarak tahmin edilmesi zor bir şekilde oluşturun.

Cihaz Güvenliği

Güncelleme:

Kurum tarafından tahsis edilmiş cihazların güvenlik ayarlarını değiştirmeyin, güncellemelerini zamanında yapın.

İşyerinde Kişisel Donanım:

Kurum cihazlarına kişisel donanım bağlamayın, iş dışında bir amaçla kullanmayın.

Alarm Durumu:

Cihazınızda herhangi bir anormal durumla karşılaşmanız durumunda (ekranın/uygulamaların kendiliğinden açılıp kapanması, antivirüs uygulamasının alert üretmesi gibi) herhangi bir işlem yapmadan hızlıca teknik birime bilgi verin.

E-Posta Güvenliği

Kurum E-Postaları:

Kurum tarafından çalışanlarına tahsis edilen e-posta adresleri iş dışında farklı bir amaçla kullanmayın.

Kişisel E-Postalar:

Kişisel e-posta adreslerini iş amaçlı kullanmayın.

Hassas Bilgi Paylaşımları:

Gizli ve hassas veri sınıfında yer alan bilgileri e-posta ile kurum dışına göndermeyin.

Abonelik İstekleri:

İşle ilgili olmayan web sayfalarına üye olurken kurum e-posta adresi kullanmayın.

Parola/Şifre Gizliliği:

Parola bilgilerini e-posta ortamında paylaşmayın.

Şüpheli E-Posta:

Kaynağından emin olunmayan, şüpheli e-posta bildirimlerini açmayın, içerisindeki linklere tıklamayın.

Genel Güvenlik İpuçları

Modem Güncelleme:

Evde kullandığımız modemlerimizi her zaman en güncel sürümde tutun.

Modem Şifresi:

Kullanılan modemlerin default username/password bilgilerini değiştirin ve yazılımlarını güncel tutun.

Cihaz Güncellemeleri:

Telefon, bilgisayar, tablet gibi cihazlarımızı en güncel sürümlerinde kullanın.

Güçlü Parola:

Basit parolalar kullanmayın, mutlaka 2li doğrulama ayarlarını yapın.

Güvensiz Linkler:

Güvenliğinden emin olmadığınız kaynaklardan gönderilen linklere tıklamayın.

Web Adresi Doğruluğu:

Girmek istediğiniz web sitesinin adresinin doğruluğundan emin olun.

Kurum İçi Eğilimler:

Kurumun bilgi güvenliğine yönelik paylaşımlarını dikkatle takip edin ve eğitimlerini zamanında tamamlayın.

Terminoloji

TÜRKÇE	İNGİLİZCE	AÇIKLAMA
Açılır Kapanır Pencere	**Pop-Up**	Bir siteye girildiği zaman onunla birlikte açılan reklam pencerelerine pop-up denilmektedir.
Alternatif Dağıtım Kanalları (ADK)	**Alternative Distribution Channels (ADC)**	Müşteri ile yüz yüze gelinmeden gerçekleştirilen bankacılık işlemlerini sağlayan araç veya ortamlardır. (Ör. İnternet Bankacılığı, Çağrı Merkezi, ATM vb.)
Anonim	**Anonymous**	Kimlik belirtilmeyen durum ve ortamlardır.
Arama Motoru	**Search Engine**	İnternet üzerinde bulunan içeriği aramak için kullanılan bir mekanizmadır. (Ör. Google, Yandex, Yahoo, vb.)
Atak, Saldırı	**Attack**	Bir bilgisayar sistemine izinsizce girme, bir web sayfasını kirletme, Truva atı sokma veya bir kodu kırma, vb. girişimlerdir.
Bağlantı	**Link**	İnternette bir sayfa içinde bağlantı sağlanarak başka bir sayfaya yönlendirme sağlayan fonksiyondur. Bağlantılar genellikle altı çizgili ya da farklı renklerde görülür. Üzerine geldiğinizde mouse el işaretine dönüşür.
Bilgisayar Korsanı	**Hacker**	Şahsî bilgisayarlara veya çeşitli kurum ve kuruluşlara ait bilgisayarlara ve ağlara izinsiz olarak giriş yapan kişilere denir.
Biyometri	**Biometer**	Kullanıcının fiziksel ve davranışsal özelliklerini tanıyarak kimlik saptamak üzere geliştirilmiş bilgisayar kontrollü, otomatik sistemler için kullanılan genel bir terimdir.
Çağrı Merkezi Ses imzası		Kullanıcıların kimliklerini sesleri aracılığıyla doğrulayan metin bağımlı bir diyalogsal ses biyometrisi çözümüdür.
Çevirim İçi	**On-line**	Bilgisayar sisteminde sunucuya bağlı ve çalışır durumda olma halidir.
Dijital imza	**Digital signature**	Kayıtlı bir işlemdeki bir belgeyle söz konusu belgeyi imzalayanı güvenli bir şekilde ilişkilendiren, elektronik ortamdaki kimlik doğrulama yöntemidir.
Doğrulama	**Authentication**	Elektronik bankacılıkta, kimlik denetimi, yetki denetimi; aslına uygunluğu kanıtlama, kimlik, yetki ve sayışım denetim protokolleridir.
Dolandırıcılık	**Fraud**	Türk Ceza Kanunu'nda "hileli davranışlarla bir kimseyi aldatıp onun veya başkasının zararına olarak, kişinin kendisine veya başkasına yarar sağlaması" olarak tanımlanmıştır. Bankacılık sisteminde dolandırıcılık, sahtekârlık, hırsızlık, çıkar amaçlı yapılan kötü niyetli girişimleri ifade eder.
Ekran Kaydedici	**Screen-Logger**	Ekran görüntüsü alan casus yazılımlardır.

Terminoloji

E-Posta ve Telefon ile Sipariş	**Mail Order/ Telephone Order (MO/TO)**	Kart bilgilerinin telefonda ya da e-posta aracılığı ile kart sahibinden edinilerek tamamlanan kartlı ödeme işlemleridir.
Erişim	**Access**	Elektronik bankacılıkta bilgisayar öz kaynaklarını kullanma olanağını elde etme olarak sıkça kullanılmaktadır. Bir sisteme erişim hakkını, kullanma hakkını elde etmek olarak da bilinir.
Etkinleştirme	**Activation**	Elektronik bankacılıkta sunulan bir ürünün kimlik doğrulama koşuluna bağlı olarak kullanıma açılması süreci olarak kullanılmaktadır.
Giyoş	**Guilloche**	Dairesel bir dizaynı tekrarlamak üzere karmaşık bir kombinasyon halinde karıştırılmış birbirine girmiş eğri çizgiden oluşan kümedir.
Gizli Veri	**Confidential information**	Gizli veriler, kanun, mevzuat, yönetmelik ve politikalar çerçevesinde korunan bilgidir.
Gökkuşağı Baskı	**Rainbow Print**	İki rengin karıştırılmasına olanak sağlayarak ofset baskı esnasında kimliğe uygulanmaktadır. Kimlik kartının ön yüzünde ana gövdede yatay, üst kulakçıkta yatay ve yan kulakçıkta dikey uygulamadır.
Görüntülü Görüşme Asistanı	**Video Call Assistant**	Uzaktan kimlik tespitinin müşteri temsilcisi aracılığı ile görüntülü olarak yapılmasıdır.
Hassas Veri	**Sensitive Information**	İşlenmelerinin ayrımcılık riskini doğurduğu kabul edilen bazı veriler hassas veri olarak tanımlanmaktadır. Hassas Veri'ler veya başka bir ifadeyle, Özel Nitelikli Kişisel Veriler, Kişisel Verileri Koruma Kanunu'nun 6. Maddesinde tanımlanmıştır.
Hiper-Metin Transfer Protokolü	**Hypertext Transfer Protocol (HTTP)**	İnternet ağında data transfer protokolüdür.
Hologram	**Hologram**	Yansıtmalı optik değişken görüntü cihazı (DOVID–Diffractive Optical Veriable Image Device) ile mikro yapılarda iki veya üç boyutlu kinematik ve efekt değiştiren renk tasarımları elde edilmektedir. Kimlik kartının sağ ön yüzünde fotoğrafın altında yer almaktadır. Dikkatli incelendiğinde Türkiye haritasının ortasında iki adet renkli hilal ve TC ibaresi bulunmaktadır.
İndirme	**Download**	Elektronik bir ortamdan dosya çekme işlemi.
İnternet Protokol Adresi	**Internet Protocol Address (IP)**	İnternet adresleme sistemidir. (Ör. http//www.ornek.comm adresi aslında 195.175.68.4 rakamlarına karşılık gelir.)
Kablosuz Erişim	**Wireles Fidelity (Wi-Fi)**	Kablosuz erişim noktaları aracılığı ile yerel alan ağına bağlanmayı ifade eder.

Terminoloji

Karekod	**QR Code**	Tarama usulü ile ödeme işlemlerinde kullanılmak üzere oluşturulan; alfa numerik verileri, karakterleri ve simgeleri depolayan, bakana göre sol alt köşede, sol üst köşede ve sağ üst köşede üç kare desen işaretleyiciden oluşan ve kare siyah-beyaz noktalar ya da pikseller şeklinde siyah ve beyaz modüllere sahip olan iki boyutlu kodudur.
Kimlik Doğrulama	**Authentication**	Kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla kullanılan, bir kişiye özgü ölçülebilir biyolojik veya davranışsal karakteristiğidir.
Kötü Amaçlı Yazılım	**Malware**	Bilgisayar ve mobil cihazlarda yer alan bilgileri ele geçirmek, sistemlerine erişim sağlamak, işlevlerini bozmak amacı ile kullanılan zararlı yazılımlardır.
Kullanıcı	**User**	Bir sistemi, uygulamayı kullanan olarak tanımlanan kişidir.
Mikro Yazı	**Micro Post**	Küçük (0.25 mm) harflerden oluşan cümledir, çıplak gözle okunamaz. Kimlik katının arka yüzünde üst bölge ile MRZ bölgesi arasına uygulanmıştır. Yedi tepe oluşturur.
Oltalama	**Phishing**	Dolandırıcıların rastgele kullanıcı hesaplarına gönderdikleri, kullanıcının özel bilgilerini (şifre, parola, müşteri numarası, kullanıcı adı, kredi kart numarası vb.) elektronik ortamlarda ele geçirilmesini amaçlayan saldırı türüdür.
Omuz Sörfü	**Shoulder Surfing**	Akıllı bir gözlemci kullanıcının girdiği şifreyi görene kadar takip eder ve şifreyi ele geçirir. Bunun için fiziki yakınlık, dürbün ve kamera kullanılmaktadır.
Optik Değişken Mürekkep	**Optically Variable Ink**	Bakış açısına bağlı olarak şeklin farklı renklerde (gül renginden yeşile kadar)görünmesini sağlayan mürekkeptir. Kimlik kartının arka yüzünde sağ alt köşede uygulanmıştır.
Otomatik Para Çekme Makineleri	**Automatic Teller Machine (ATM)**	Özellikle para çekme/yatırma için kullanılan ve bunu yanı sıra hesap hareketleri, havale, eft, fatura ödeme gibi işlemler için kullanılan insansız çalışan uçbirim aygıtıdır.
Reklam E-Postası (İstenmeyen)	**SPAM E-mail**	Kullanıcı tercihinden bağımsız olarak yapılan her türlü elektronik posta gönderimidir.
Sahte Alan Adı	**Fake Domain**	Kullanıcıların bilgilerini ele geçirmek amacıyla kurum ve markalarının internet sitelerine benzer şekilde oluşturulan web sitelerinin alan adlarına verilen isimdir. Ör. www.sahtealanadi.comm
Sanal Kart	**Online Card**	Bankalardan edinebileceğiniz, fiziki kartta olduğu gibi kart numarası, kullanma tarihi, CVC kodu gibi bilgilerinin bulunduğu ve sadece internet ortamında var olan ve kullanılan kart türü.

Terminoloji

Sanal POS	**Online POS**	Müşteri kredi kartına fiziksel olarak erişiminiz olmayan online, mobil, çağrı merkezi vb. kanallarda veya fiziksel POS bulundurmanızın zor olduğu saha satış, teslimat ekipleri vb. hizmet noktalarınızda, müşteri banka kartı veya kredi kartı bilgilerini güvenli şekilde alarak, bankaya online bir teknik entegrasyon üzerinden ödeme ve kart bilgilerini iletmenize ve işlemin sonucunu aynı yolla almanıza imkan veren altyapıdır.
Satış Noktası	**Point Of Sales Terminal (POS)**	Kredi kartlarının işlem yapabilmesi için kullanılan cihazdır.
Sosyal Ağ	**Social Network**	Sanal ortamlarda sosyal iletişim kurmaya yarayan sosyal medya mecralarıdır. (Ör: Facebook, Twitter, Instagram, vb.)
Sunucu	**Server**	Diğer bilgisayarlara veri sunan çok daha kapasiteli bilgisayara verilen addır.
Tarayıcı	**Browser**	"www." üzerinde dokümanların transfer edilip görüntülenmesini sağlayan programlara "browser (tarayıcı)" adı verilir. (Ör. İnternet Explorer, Google Chrome, Firefox, vb.)
Tek Kullanımlık Şifre	**One Time Password (OTP)**	Online bankacılıkta işlem onayları veya login ekranlarında kullanılan ek güvenlik sağlayan tek kullanımlık şifredir.
Truva Atı	**Trojan Horse**	Bir bilgisayar programına bağlanarak gizlenen, tahribatını yaparken programın olağan çalışmasına izin veriyormuş gibi gözüken virüslerdir.
Tuş Kaydedici	**Key-Logger**	Klavyeden basılan her tuşun loglarını tutan casus yazılımlardır.
Uyarı	**Alarm**	Dolandırıcılık ve suiistimal takip ekiplerinin olağandışı bir duruma almış oldukları her türlü ikazdır.
Varolmayan Kart	**Card not Present (CNP)**	Kartın fiziki olarak kullanılmadığı, üzerindeki bilgilerle tamamlanan e-ticaret ödeme işlemlerine verilen isimdir.
Vekaletname	**Proxy**	Bir kimsenin başka bir kimseyi belirli durumlarda kendi adına hareket edebilmesi için yazılı olarak yetkilendirdiğine ait yazılı bir belgedir
Veri	**Data**	Bir araştırmada, bir tartışmada, bir akıl yürütmede sonuca ulaşabilmek için gereken ilk bilgi.
Virüs Önler	**Anti-Virus**	Bilgisayar güvenliğini sağlayabilmek için bazı virüsleri temizlemeye yönelik programlardır.
VOIP (Voice Over IP) Arama	**VOIP (Voice Over IP)**	İnternet alt yapısı üzerinden yapılan aramaları ifade eder. Dolandırıcılar tarafından müşteri ya da Banka numaralarının taklit edilmesi amacıyla kullanılmaktadır.

TÜRKİYE BANKALAR BİRLİĞİ

Adres: Nispetiye Cad. Akmerkez, B3 Blok,
Kat 13, 34340 Etiler/İstanbul

Telefon: 0212 282 09 73 **Faks:** 0212 282 09 46
e-Posta: tbb@tbb.org.tr **KEP:** tbb@hs05.kep.tr