İnternet Bankacılığı & Çevrimiçi Alışveriş

Teknolojinin gelişmesiyle devreye giren alternatif dağıtım kanallarının en önemlilerinden biri "internet bankacılığı"dır. İnternet bankacılığıyla fiziksel şubelerden yapılmakta olan hemen hemen çoğu işlem yapılabilmektedir. Diğer bir önemli işlem çevrimiçi alışveriş ile artık internet kullanıcıları birçok ürün ve hizmete internet üzerinden verdikleri siparişlerle rahatlıkla ulaşabilmektedir. Tüm bu rahat ve kolay bir şekilde yapma imkânı tanıyan internet doğal olarak bu platformu suiistimal etmek isteyenlerin de durak noktası olmaya başlamıştır.

Bankalar üzerinden yapılan para transferi, kredi kullanma, kredi kartı işlemleri gibi çeşitli parasal işlemler ve çevrimiçi alışverişler, günümüzde internet bankacılığı ile bilgisayarlar veya mobil telefonlar üzerinden kolaylıkla yapılabilmektedir.

İnternet kullanımının giderek artması ile kullanımı yaygınlaşan internet bankacılığı, beraberinde teknolojik dolandırıcılık vakalarına da neden olmaktadır. Bu durum, kişisel verilerin güvenliğini ve güvenli bankacılık hizmetini her zamankinden daha önemli hale getirmiş, parasal işlem hizmeti veren kurum ve kuruluşların sistemlerinde güvenlik önlemleri almalarını ve internet bankacılığı kullanan kullanıcıların bilinçlendirilmesini zorunlu kılmıştır.
Siber suçluların kullandıkları ve her geçen gün geliştirdikleri malware, botnet, spam, phishing, kimlik hırsızlığı, sosyal mühendislik gibi yöntemler ile internet kullanıcılarını dolandırmaya çalışmaları nedeniyle, internet bankacığı kullanımında her zaman riskler olmaktadır. Ancak kullanıcılar, hizmeti veren kurum ve kuruluşların teknik olarak önlem almaları ve kendilerinin bilinçli kullanımı ile bu riski minimize edebilirler.

Siber Suçluların Bilgileri Çalmak İçin En Sık Kullandığı Yöntemler

Kötü Amaçlı Yazılımlar

Kötü amaçlı yazılımlar (casus yazılımlar), şifreler, numaralar ve hesap adları gibi bilgisayar veya telefondaki her şeyi kayıt altına alabilirler. Casus yazılımlar topladığı bu bilgileri bilgisayar korsanına yönlendirirler.

Kopya Sunucular

İnternet bankacılığı hizmetlerini kullanırken, tarayıcı veya mobil uygulama, iletişim kurduğu kurumun kimliğini doğrulamak için resmi banka sunucusu ile iletişim kuracaktır. Bilgisayar korsanları bazen bir banka olarak görünürler ve kullandığınız uygulamalara sahte banka sunucu sertifikası göndermeyi denerler. Böylece hesaplarınıza erişmeleri mümkün olur.

Kimlik Avı Dolandırıcılığı

Siber suçlular, e-posta, telefon ya da sosyal medya aracılığı ile iletişim kurarlar ve kendilerini güvenilir bir kurum olarak göstererek, banka bilgilerini almaya çalışırlar. Ayrıca; genellikle kurbanlarını banka sitelerine benzeyen kopya sitelere yönlendirerek şifre gibi hesap detaylarının girilmesini isterler.

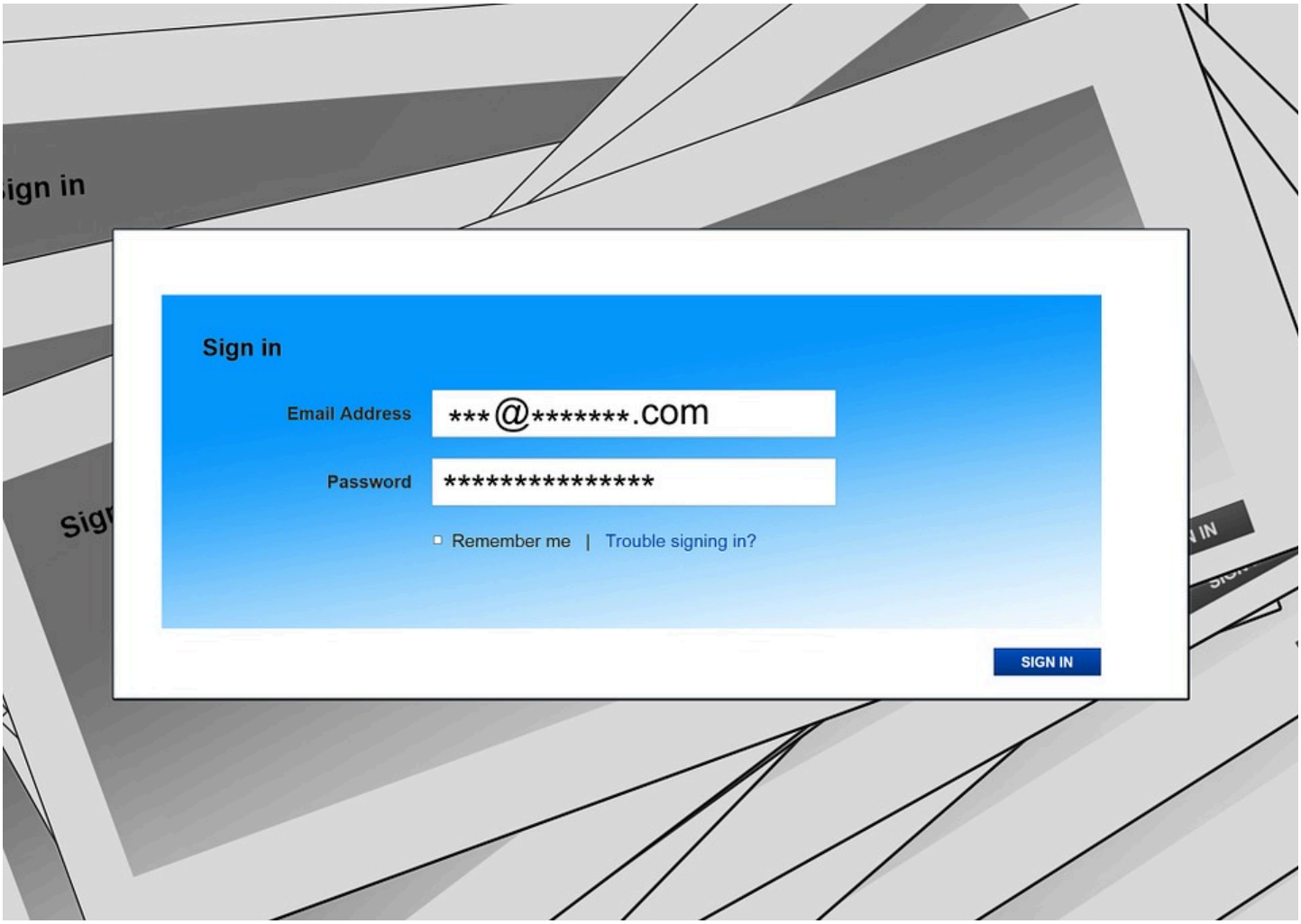
İnternet Bankacılığı ve Çevrimiçi Alışveriş'te Dikkat Edilmesi Gerekenler

- Kullanılan bilgisayar ve telefonun virüslere ve kötücül yazımlara karşı korunması için anti virüs programı kullanılmalıdır.
- Kullanılan tarayıcının ve işletim sisteminin güncel olmasına dikkat edilmelidir. (Bilgisayar ve akıllı telefonlarda kullanılan uygulamalar belirli zamanlarda güncellenmektedir. Bu güncellemeler genellikle yeni özellikler eklemek için yapılır. Ancak, çoğu zaman güvenlik açıklarını kapatmak için yapılır. Bu nedenle uygulamaların güncel tutulduğundan mutlaka emin olunmalıdır.)
- Bankaların sunduğu tek kullanımlık şifre hizmeti kullanılmalıdır. 3D Secure olarak adlandırılan bu sistemde; bankacılık işlemleri veya çevrimiçi alışveriş işlemi gerçekleşirken, banka tarafından kart sahibine sms ile bir şifre oluşturulmakta ve kart sahibinin kimliği doğrulanmaktadır.
- Mobil bankacılık işlemleri için mutlaka SMS doğrulama kullanılmalıdır.
- Bilgisayarda güvenlik duvarı kullanılmalıdır.
- Kurumsal bankacılık işlemlerinde elektronik imza kullanılmalıdır.
- İnternet Bankacılığı için sisteme giriş yaparken istenilen şifre bilgileri, bilgisayar klavyesi yerine bankaların oluşturduğu sanal klavyeler üzerinden girilmelidir.
- Nerden geldiği bilinmeyen elektronik postalar açılırken dikkat edilmeli, linkler tıklanmamalıdır. Hackerler genelde e-posta yolu ile kişilerin bilgisayarına virüs gönderme yolunu seçmektedirler.
- Güvenilmeyen sitelerden program indirmemeli ve bu programlar kullanılmamalıdır. Lisanslı programlar kullanılmalıdır.
- Mobil uygulama olarak kullanabilecek çok sayıda üçüncü taraf uygulaması bulunmaktadır. Kullanılan uygulamalar, App Store ve Google Play Store gibi uygulama mağazalarından indirilmelidir. Bu uygulamaların kötü amaçlı yazılım içerme olasılığı çok daha düşüktür ve bu resmi mağazalara eklenen uygulamalar sürekli bir şekilde incelenmektedir.
- Banka hesapları ve kredi kartı ekstreleri düzenli bir şekilde kontrol edilmelidir. Hatta ekstre bilgileri beklenmeden aralıklarla harcama kontrolleri yapılmalıdır. Herhangi bir gariplik fark edilirse zaman geçirmeden ilgili bankaya müracaat edilmelidir.
- İnternet bankacılığı ve E-ticaret sitelerinde alışveriş yaparken ödeme ekranında http:// yerine https:// yazmasına ve alışveriş yapılan sitenin SSL sertifikası olmasına mutlaka dikkat edilmelidir. Bu sertifika, kredi kartı bilgilerinin şifrelenmesini ve başkaları tarafından

kopyalanmasını engellemektedir.

(Https, SSL/TLS Protokolü ile HTTP protokolünün bir kombinasyonu olup, bir kaynaktan diğerine tüm bilgileri şifreli olarak gönderen bir güvenlik sistemidir.
Örneğin şifreli işlem yapılan tüm sayfalarda, sosyal ağ ve bankacılık sitelerinde bu protokol mevcuttur. Eğer bağlantıda https yazmıyorsa ve şifreli bağlantı yapılıyorsa çok dikkatli olunmalıdır. Benzer şekilde alışveriş yapılan sitenin ödeme bölümüne gelindiğinde adres çubuğunda https:// yazıp yazmadığına mutlaka dikkat edilmelidir. Eğer sadece http:// yazıyorsa o sayfadan ödeme yapmak riskli olacaktır.
İnternet bankacılığı işlemlerini yapmak için girilen sitenin bağlantısının gizli olup olmadığı veya diğer bir deyişle gerçekten bankaya ait site olup olmadığı, adres çubuğunun solunda yer alan "yeşil" renkli kilitli logodan kontrol edilebilir.)

- İnternet bankacılığı işlemlerinde internet sayfası veya mobil uygulama uzun süre yanıt vermiyorsa işlem yapmakta ısrar edilmemelidir.
- • Çevrim içi alışverişlerde, harcama limiti yüksek olan kredi kartı kullanmak yerine sanal kart kullanımı tercih edilmelidir. Bu şekilde sanal kartın limiti kullanıcı tarafından belirlendiği için risk de azaltılmış olacaktır. (Sanal kart, ilgili bankanın internet bankacılığı hizmeti üzerinden kolaylıkla tanımlanabilmektedir.)
- Güvenliğinden emin olunmayan siteler ve kurumlar ile kişisel bilgiler paylaşılmamalıdır. Banka işlemlerinde kullanılan şifre, parola vb. önemli bilgiler üçüncü şahıslarla kesinlikle paylaşılmamalıdır. Bankadan arıyorum diyen veya bunu belirten e-postalara itibar edilmemelidir. Unutulmamalıdır ki hiçbir banka veya görevlisi kullanıcı şifresini öğrenmek istemez.
- Kullanılan İnternet tarayıcı adres çubuğunda yazan site adına dikkat edilmelidir. Eğer site adında herhangi bir farklılık varsa, gerçeğinin birebir aynısı olan bir siteye yönlendirme yapılmış olabilir. Örneğin doğru bir siteye spam veya phishing yöntemleri kullanılarak ve sadece bir harfi değiştirilerek yönlendirme yapılmış olabilir. Bu yüzden e-posta linklerini tıklayarak hiçbir sayfadan işlem yapılmamalıdır. Mümkünse internette alışveriş yapılan siteleri ve bankacılık sayfaları adresleri sık kullanılanlar listesine eklenmelidir.
  Şifreler kolay tahmin edilebilecek şekilde oluşturulmamalı ve düzenli olarak değiştirilmelidir. (Klavyede arda arda gelen sayılar (123456 gibi) ve harflerden (asdf, abcd, qwe) oluşan şifreler kullanılmamalıdır. Bu tür şifreler, bu ortamı dolandırıcılık amaçlı kullananların çok kolayca tahmin edebileceği şifrelerdir. Şifrelerin, “sayı + harf + karakter” den oluşan ve tahmin edilmesi zor en az 8 karakterli bir şifre olmasına dikkat edilmelidir.)



- Ortak kullanılan bilgisayarlardan, ortak wi-fi alanlarından ve internet kafelerden alışveriş ve bankacılık işlemi yapılmamalıdır. Bu bilgisayarlara kredi kartı numarası ve diğer kişisel bilgiler yazılmamalıdır.
- İnternet bankacılığı kullanıldıktan sonra oturum kapatılmalıdır. Türkiye'de faaliyet gösteren çoğu bankanın mobil bankacılık uygulaması belirli bir süre işlem yapılmadığı takdirde otomatik olarak kapanmaktadır. Ancak bunun olmasını beklemeden işlem bittiğinde uygulamadaki oturum kapatılmalıdır.
- Tarayıcıdan yapılan internet bankacılığı için, tarayıcının şifreleri ya da kullanıcı adlarını kaydetmediğinden emin olunmalıdır.
- Güvenlik amacıyla bankaların ilettiği güvenlik kurallarına uyulmalıdır.

İnternet ortamından yapılan bankacılık işlemlerinde kullanıcı mağduriyetinin önüne geçilmesi için Bankalar, müşterilerini etkin bir şekilde bilgilendirmektedirler.
Bazı bankaların, güvenli internet bankacılığı işlemleri için kullanıcılarına vermiş olduğu bilgilere aşağıdaki linklerinden erişilebilir.

- https://www.ziraatbank.com.tr/tr/dijital-bankacilik/guvenlik
- https://www.garanti.com.tr/tr/bireysel/subesiz/internet_bankaciligi/guvenlik.page
- https://www.vakifbank.com.tr/guvenlik.aspx?pageID=361
- https://www.yapikredi.com.tr/sinirsiz-bankacilik/internet-subesi/guvenlik/guvenlik-icin-10-altin-ipucu
- https://www.denizbank.com/internet-bankaciligi/
- https://www.isbank.com.tr/TR/guvenlik/Sayfalar/guvenlik.aspx
- https://www.qnbfinansbank.com/sss/internet-subesi/guvenlik
- https://www.akbank.com/tr-tr/hizmetler/Sayfalar/guvenli-alisveris.aspx
  İnternet bankacılığı ve çevrimiçi alışverişteki tehlikelerle ilgili aşağıdaki videolar izlenebilir.
- https://www.youtube.com/watch?v=Mlnsbfg1oXs
- https://www.youtube.com/watch?v=Q18-MVGWYrM

ETİKETLER

#İnternetBanckacılığı #ÇevrimiçiAlışveriş

KAYNAKÇA

- [1] https://www.bankaciyim.net/haber/7022/internet-bankaciligi-guvenli-mi.html
- [2] https://www.sgkrehberi.com/haber/174159/internet-ve-mobil-bankacilik-islemlerinde-nelere-dikkat-etmeli.html
- [3] https://konupara.com/bankalar/mobil-bankacilik-guvenlik-16307/