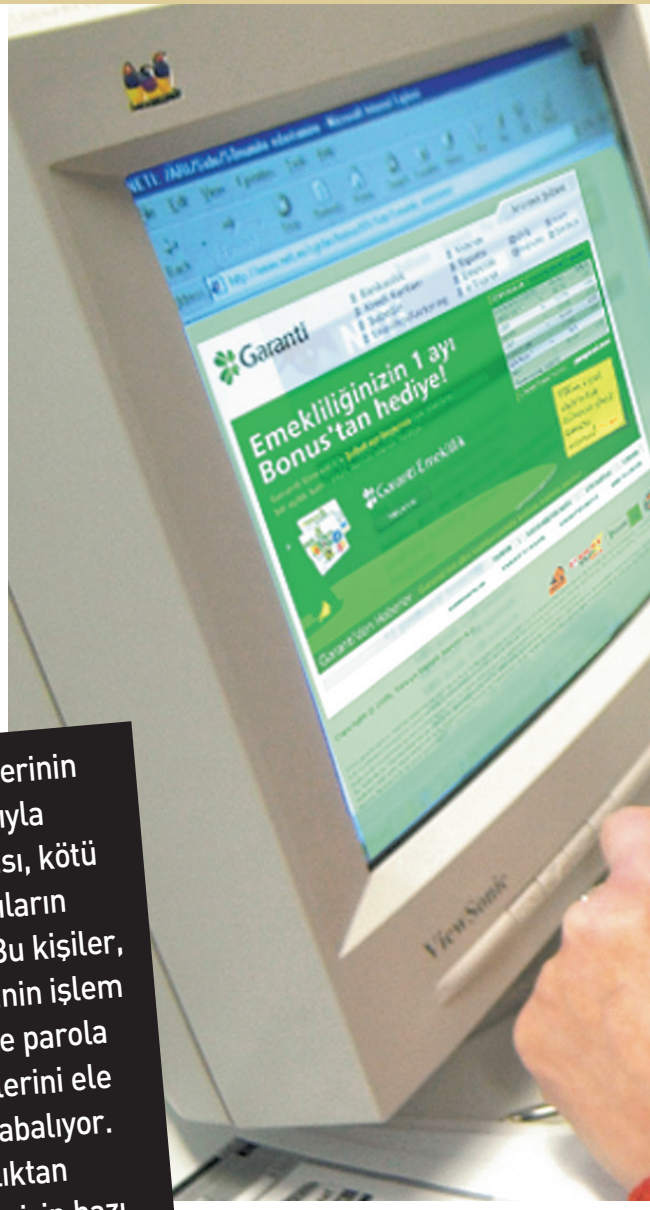
Dolandırıcıların hedefi internet bankacılığı



İnternet, pek çok açıdan hayatımızı kolaylaştırdığı gibi bazı konulara dikkat edilmediği takdirde sorunlara da yol açabiliyor. Özellikle bankacılık işlemlerinin internet kanalıyla yapılabiliyor olması, kötü niyetli kullanıcıların (hacker) dikkatini çekiyor, banka müşterilerinin işlem yaparken kullandıkları şifre ve parola gibi kişisel bilgileri ele geçirmek için çaba sarf etmelerine sebep oluyor. Sanal dünyada dolandırıcıların kullandıkları yöntemler şunlar:

Bankacılık işlemlerinin internet kanalıyla yapılabiliyor olması, kötü niyetli kullanıcıların dikkatini çekiyor. Bu kişiler, banka müşterilerinin işlem yaparken şifre ve parola gibi kişisel bilgilerini ele geçirmek için çabalıyor. Dolandırıcılıktan etkilenmemeniz için bazı kurallara uymanız ve dikkatli olmanız gerekiyor

SAHTE SİTELER

Dolandırıcılar, hedefledikleri web sitesini kopya ederek, bu sitenin adresine yakın bir adres üzerinden yayına başlarlar. Burada temel amaç, yanlışlıkla bu adrese gelen ya da e-posta, sahte ilanlar gibi yollar ile bu adrese "çağırılan" müşterileri yanıltarak, kendi hazırladıkları sahte siteye girmelerini sağlamak ve böylelikle müşteriler hakkında bilgi toplamaktır. Dolandırıcılar, bu bilgileri banka hesaplarınıza erişmek için kullanacaktır. Bu sahte sitelere yapılan girişleri artırmak için dolandırıcılar, çeşitli yollardan elde ettikleri e-posta adreslerine oldukça cazip avantajlar vaat eden ya da kullanıcıyı paniğe sürükleyecek içerikteki e-postalar göndermekte, arama motorlarına ücretli ilanlar vermektedir. Bu e-postalar ya da ilanlar, görünürde gerçek siteye bir bağlantı (link) içeriyormuş gibi durmakla birlikte, link tıklandığında banka müşterileri farkında olmadan sahte siteye yönlendirilmektedir.

Bankalar, hiçbir şekilde internet şubesine direkt bağlantı (link) içeren ya da sizden şifre veya herhangi bir kişisel bilgi isteyen e-postalar göndermemektedir. Dolayısıyla, bu şekilde bir e-posta almanız ya da abartılı bir ilanı tıklamanız halinde sizden kişisel bilgilerinizi girmeniz istenen bir alana yönlendirilirseniz, bankayı arayarak durumu bildiriniz. Böyle bir bağlantı kullanarak siteye giriş yapmak yerine, tarayıcı programınızın adres bölümüne bankanın internet adresini yazmak suretiyle giriş yapınız veya şubeyi "sık kullanılanlar"a eklediyseniz, sadece bu alandan seçerek giriniz.

YÜKSEK KAZANÇ VAAT EDEN E-POSTALAR

Birkaç bin dolardan birkaç yüz milyon dolara kadar çeşitli tutarların mantıklı gibi görünebilecek bir gerekçe ile bir hesaba aktarılması için e-posta alıcısına aracılık teklif edilen bu e-postalarda esas hedef, banka ve kimlik bilgilerinin temin edilmesidir. Bu arada yapılan bu aracılık işlemine karşılık ödül ya da komisyon olarak teklif edilen tutarın hesabınıza aktarılması için sizden belli miktarda bir avans da istenebilir. Bu avans tutarının gönderilmesi halinde dolandırıcılar, hem hesap numaranızın ve hesap bilgilerinizin doğruluğundan emin olurlar hem de bu bilgileri başka dolandırıcılık eylemleri için kullanmak üzere depolarlar. Bazı uluslararası örneklerde bu kişilerin, sizleri ikna etmek için sahte web sitelerine sizleri alıp transfere hazırmış gibi görünen (ama gerçekte asla varolmayan) milyonlarca doları gösterdikleri de görülmüştür.

Bu türe bir başka örnek de, lotarya ya da çeşitli piyangolardan genellikle birkaç yüz bin dolar ikramiye kazanıldığı yönünde gönderilen e-postalardır. Bu e-postalarda ikramiyeyi almanız için ilk şart olarak mesajı yanıtlamanız istenir. Sonrasında ise genellikle sizin gerçekten adı geçen kişi olduğunuzu anlamak için kimlik, ehliyet ya da pasaportunuzun kopyalarını (fotokopi ya da tarayıcı kullanarak) göndermeniz istenecektir. Ayrıca paranın hesabınıza aktarılması sırasındaki masraf ve komisyonlar için bir miktar ödeme yapmanız da



Türkiye Bankalar Birliği'nden virüs uyarısı

Türkiye Bankalar Birliği (TBB), internet bankacılığı kullanıcılarını, kişisel bilgileri elde etmeye yönelik son derece tehlikeli bir virüs konusunda uyardı. TBB duyurusunda, son dönemde internet bankacılığı kullanıcılarının, kullanıcı kodu, şifre, parola, güvenlik sorusu gibi gizli bilgilerini elde etmeye yönelik son derece tehlikeli bir virüs (torpig türevi) belirlendiği kaydedildi.
Banka müşterilerinin internet bankacılığına giriş için kullandıkları bilgisayarlara yerleştirilen söz konusu virüsle, müşterilere ait bilgilerin ele geçirildiği belirtilen duyuruda, müşterilerin bu tip virüslerden etkilenmemeleri için dikkat edilmesi gereken hususlar şöyle sıralandı:

- **Online işlemler gerçekleştirirken, işlem yapılan sayfada, daha önceki bağlantılardan farklı bir görünüm veya ifade varsa, hiçbir işlem yapılmadan ilgili banka ile irtibata geçilmeli.**
- **Güvenli olmayan internet sitelerine giriş yapılmamalı ve bu tür sitelerden dosya indirilmemeli.**
- **Bilinmeyen adreslerden gelen e-postalar açılmadan silinmeli, mümkünse bu tür e-postaları engelleyici tedbirler alınmalı.**
- **Bilgisayarlarda kullanılan yazılımlara ait güvenlik güncellemeleri mutlaka yüklenmeli. Antivirüs yazılımları kullanılmalı ve düzenli olarak güncellenmeli. Kişisel güvenlik duvarları (firewall) kullanılmalı.**
- **Kişisel bilgileri ele geçirmek üzere bilgisayara sızan casus yazılımlara karşı "anti-spyware" yazılımları kullanılmalı.**

Duyuruda, internet bankacılığı kullanıcısı olarak, şifre ve bilgisayarın güvenliğini sağlamak için bankanın internet sitesindeki güvenlik açıklamalarının dikkatle okunması önerildi.

istenebilecektir. Bu aşamada yapılan ödemeler kaybedileceği gibi, kimlik bilgileriniz de uluslararası şebekeler tarafından başka dolandırıcılık eylemlerinde kullanılacaktır. Lütfen bu gibi bilgileri üçüncü şahıslara göndermeyiniz.

TROJAN, KEY-LOGGER, SCREEN LOGGER GİBİ PROGRAMLAR

Trojan olarak bilinen ve dilimize "Truva Atı" olarak giren virüsler, bilgisayarınızı uzaktan kumanda etme amacına hizmet ederler. Genel olarak iki ayrı modülden oluştukları söylenebilir. İlk modül, kötü niyetli kullanıcıların bilgisayarınıza uzaktan erişimine ve kontrol sağlamasına izin verirken ikinci modül, hacker ile sizin bilgisayarınız arasında bağlantı sağlayacak bir "açık kapı" oluşturur. Trojan tarzı programlar, siz izin vermedikçe bilgisayarınıza yüklenmez. İnternet ortamında gelen .ini ya da .exe uzantılı dosyalar, bu küçük trojan yazılımlarını barındırıyor olabilir. Bilgisayarınıza özellikle ücretsiz yazılımları kurmadan önce güncel bir tarayıcı programla kontrol etmeyi ihmal etmemelisiniz. Anti virüs yazılımınızı sürekli olarak resmi sitesinden güncellemeli ve bir firewall programı ile bilgisayarınızı koruma altına almalısınız.

Key-logger, temel olarak, gerçek sahibinin bilgisi dışında düzenli olarak internet üzerinden bir başkasına veri transferi yapan küçük boyutlu bir program olarak tanımlanabilir. Kötü niyetli kişiler, bilinen key-logger programlarından birini kullanarak ya da kendileri küçük bir key-logger oluşturarak bu programcıkları çeşitli şekillerde uzak bilgisayarlara gönderirler. Key logger, uzak bilgisayara kendi kurulumunu gerçekleştirdikten sonra genellikle kendini hiç belli etmeden çalışmaya başlar ve kaydettiği verileri programlandığı zaman aralıklarında hacker'a iletir. Genellikle tüm klavye hareketlerini ara hafızasına alır ve transfer eder. Screen logger da key logger ile aynı temel mantığa dayanır. Ancak screen logger programlar ile taşınabilen data yalnız klavyenizde yaptığınız tüm vuruşlarla sınırlı olmayıp, ekran görüntülerinizi de içerir. Fare ile ekranda bir noktaya tıklamanız ile beraber aynı anda screen logger, adeta ekranın tamamının ya da küçük bir bölümünün (genellikle fare merkezli olarak küçük bir dörtgenin) o anki resmini çekerek bunları internet ortamında sabit bir adrese iletir. Bu gibi yazılımlar, genellikle kötü niyetli kullanıcılar tarafından kişisel bilgilerinizi ele geçirmek için kısaca yukarıdaki mantık ile işlevlerini sürdürmektedir".

Güvenli internet bankacılığı için yapmanız gerekenler

Güvenli internet bankacılığı yapabilmek için kullanıcıların olması gereken birtakım önlemler var. Bankanın internet şubesine girişte aşağıdaki noktalara dikkat edilmelidir:

➤ Tarayıcıyı ikna etmek için sahte web siteli programınızın adres çubuğuna bankanın internet adresini yazın ve "İnternet Şubesi Giriş" butonunu kullanın.

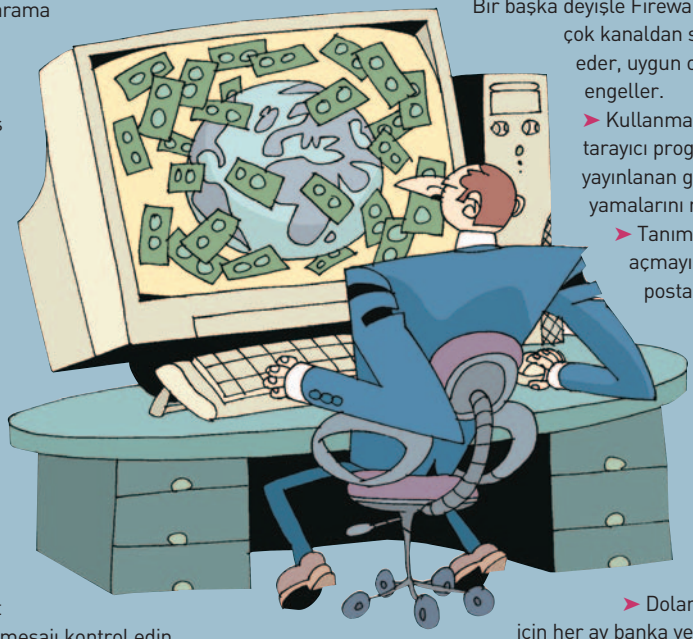
➤ Bankanın internet adresini sık kullanılanlar listenize ekleyin (Add To Favorites) ve siteye her girişinizde bu listedeki linki kullanın.

➤ E-postalarla gelen veya arama motorları dahil başka sitelerdeki linkleri kullanmayın.

➤ Bilgisayarınızda Windows işletim sistemi üzerinde Internet Explorer tarayıcı programını kullanıyorsanız, Güvenlik Çemberi'ni yükleyin. Güvenlik Çemberi, şifre ve parola girişi yaptığınız alanları koruma altına alır.

➤ Internet şubesine giriş güvenliğinizi daha da artırmak istiyorsanız, bir i-anahtar edinebilirsiniz.

➤ Doğru yerde olduğunuzdan emin olmak için mutlaka bir karşılama mesajı belirleyin ve internet şubesine her girişinizde bu mesajı kontrol edin.



➤ Bankanız sizlerden e-posta gibi kanallarla şifre ve kişisel bilgilerinizi göndermenizi ya da e-posta ile gönderilen bir linkle bu girişleri yapmanızı istememektedir. Bu gibi bir durumla karşılaşmanız halinde lütfen hiçbir bilgi girişi yapmadan tarayıcı programınızın penceresini kapatın.

➤ Şifre ve parolalarınızı belirli periyotlarla değiştirin. Şifre ya da parola oluştururken doğum tarihi, evlilik yıldönümü, aynı sayıların tekrarı (111111) ya da ardışık sayı dizisi (123456) gibi kolay tahmin edilebilecek bir kombinasyon kullanmayın.

➤ Her banka ya da site için başka bir şifre kullanın. Parolalarınızı, sadece harflerden ya da sadece rakamlardan değil, harf ve rakam karmasından oluşturun (PUZZ13 gibi). Şifrenizi ve parolanızı hiçbir yere kaydetmeyin.

➤ Banka personeli dahil hiç kimseye şifrelerinizi hiçbir zaman söylemeyin, kişisel bilgilerinizi üçüncü şahıslarla paylaşmayın.

➤ Güvenlik ayarlarınızı kişisel tercihleriniz doğrultusunda yeniden belirleyin. Bilgisayarınızın yeterince güvenli olmadığını düşünüyorsanız, şifrenizi girmek için kendi klavyeniz yerine sanal klavyeyi de kullanabilirsiniz.

➤ Bilgisayarınızı virüslere karşı sürekli olarak en güncel anti-virüs yazılımları ile tarayın.

➤ Hiçbir zaman bilgisayarınızın hackerlar için "gerekli olmayacağını" düşünmeyin. Bazı "küçük" yazılımlar ile saldırganlar bilgisayarınızın kontrolünü ele geçirerek dilledikleri zaman daha büyük saldırılarda cihazınızı kullanabilirler. Key-logger gibi çeşitli casus programlardan korunmak için anti-spy yazılımlar edinin. Bu yazılımları sürekli güncelleyerek bilgisayarınızı periyodik olarak kontrol edin.

➤ Bilgisayarınızı risklerden korumanın en önemli yollarından birisi de bir Firewall yazılımı edinmektir. Firewall (ateş duvarı) sayesinde bilgisayarınız ile art niyetli kullanıcılar arasına bir set çekilmiş olur. Temelde, hem şüpheli haberleşmeyi kısmen engellemek hem de şüphesiz haberleşmelere izin vermek gibi bir fonksiyonu yerine getirir. Bir başka deyişle Firewall, e-posta da dahil olmak üzere pek çok kanaldan size ulaşan bilgi ve belgeleri kontrol eder, uygun olmayan ya da şüpheli bilgi girişini engeller.

➤ Kullanmakta olduğunuz işletim sisteminiz ve tarayıcı programınız için üretici firma tarafından yayınlanan güvenlik güncelleştirmeleri ve yamalarını mutlaka kullanın.

➤ Tanımadığınız kimselerden gelen e-postaları açmayın; her ne sebeple olursa olsun IRC, e-posta gibi kanallar ile size ulaşan .ini ve .exe uzantılı dosyaları ve linkleri açmamaya özen gösterin.

➤ Internet'ten herhangi bir program indirirken sözleşmeyi dikkatle okumadan kurulumu kabul etmeyin. Ücretsiz yazılımlar, genellikle küçük casus programlar da taşırlar. Program ya da dosyayı indirdikten sonra kurulumu başlatmadan önce mutlaka virüs taramasından geçirin.

➤ Dolandırma amaçlı satın almaları önlemek için her ay banka ve kredi kartı dökümlerinizi düzenli olarak inceleyin, meblağ çok küçük dahi olsa size ait olmayan harcamaları tespit ederek bankamıza bildirin. Bu incelemeyi internet şubesini kullanarak kolayca yapabilirsiniz.

➤ Özellikle dosya paylaşım programları kullanıyorsanız, kişisel bilgilerinizin olduğu belgeleri paylaşıma kapalı alanda ve koruma altında tutun.

➤ Şüphe uyandıran bir durumla karşılaşmanız halinde hemen bankayı durumdan haberdar edin. Banka, hemen kişisel güvenliğiniz için önlemler alacak ve gerekli takibatı başlatacaktır. Hesaplarınızda bir sorun olup olmadığını tespit edebilmek için, hesaplarınızın ve kredi kartlarınızın hareketlerini internet şubesinden inceleyin. Yasal süreci başlatmak için polis tutanağı tutulmasını sağlayın.

➤ Özellikle internet kafe gibi çoklu kullanımın söz konusu olduğu yerleri bankacılık işlemleriniz için kullanmamaya çalışın.

➤ Hemen hemen tüm tarayıcı programlar, kullanıcılarına kolaylık göstermesi açısından profil bilgilerinizi saklayabilir. Otomatik tamamlama (Auto-Complete) olarak tanımlanan bu yapı, özellikle aynı bilgisayarda farklı kullanıcıların olması gibi durumlarda kullanıcılar açısından risk teşkil eder. Özellikle okul, ofis gibi çok kullanıcılı yerlerde kullanılan bilgisayarlarda tarayıcı programınızın otomatik tamamlama fonksiyonunu kapatın.

➤ Bilgisayarınızda, sadece tanınmış firmaların ürettiği lisanslı yazılımları kullanın. Bilmediğiniz bir firmanın ürünlerini ücretsiz dahi olsalar tercih etmeyin; key-logger gibi bilgilerinizi transfer edecek casus programlar içerebilecek bu gibi yazılımlara şüphe ile bakın.

➤ Internet şubesinde ya da kimlik doğrulaması yaparak giriş yaptığınız tüm sitelerde işlemlerinizi sona erdirdikten sonra mutlaka "Güvenli Çıkış" butonunu kullanın.