İnternet Bankacılığı, bankacılık hizmetlerinin internet üzerinden sunulduğu bir alternatif dağıtım kanalıdır. Türkiye'de bugün internet bankacılığı, herhangi bir banka şubesinin size sağlayacağı hizmetlerin hemen hepsinden, dünyanın neresinde olursanız olun, zaman ve mekandan bağımsız olarak çabuk ve kolayca yararlanmanızı sağlamaktadır. İnternet bankacılığını 24 saat, internet erişimine sahip herhangi bir bilgisayar aracılığıyla dünyanın her yerinden kullanabilirsiniz. İnternet bankacılığının sağladığı faydalar şöyle özetlenebilir:

- Hızlı ve kesintisiz bankacılık işlemleri,
- Şubeye gitmeden, sıra beklemeden kolay bankacılık işlemleri,
- Görerek ve seçerek bankacılık işlemi yapabilmek,
- Detaylı rapor ve bilgi alabilmek,
- Çok çeşitli bankacılık ürünlerini görerek bu ürünlerden faydalanabilmek,
- Bankacılık işlemlerini çok daha ucuza yapabilmek,
- İşlemlerin banka personeli tarafından dahi görülememesi nedeniyle, gizli ve güvenli bankacılık.

İnternet bankacılığı ile yapılan işlemler siz müşterilerimize sağladığı kolaylık ve avantajların yanısıra bankalar için de verimlilik ve maliyet tasarrufu sağlamaktadır.

Türkiye Bankalar Birliği, bankalar ve müşteriler açısından oldukça önemli bir işleve sahip olan internet bankacılığı işlemlerinde, olası dolandırıcılık eylemlerine karşı bilgi işlem güvenliğine özel bir önem vermektedir. Bu çerçevede; müşterilerimizin bilgilendirilmesi açısından aşağıdaki açıklamaların yapılmasında fayda görülmektedir.

Güvenliğiniz için aşağıdaki hususlara dikkat edilmesi tavsiye edilmektedir:

- Kimlik ve kişisel finansal bilgilerinizi isteyen e-postalar konusunda dikkatli olun.
- Kişisel bilgilerinizin talep edildiği bu tür e-postaları kesinlikle doldurmayın.
- Bankalar tarafından size verilen müşteri numarası, parola ve şifre bilgilerini üçüncü şahıslarla kesinlikle paylaşmayın.
- Banka ve ticari kurumlardan gelmiş gibi gösterilen ve sizden şifre, kullanıcı adı, müşteri numarası, kredi kartı numarası, kimlik numarası gibi bilgileri talep eden e-postalara itibar etmeyin.
- Bankalar e-posta yoluyla hiç bir şekilde müşterilerin kişisel bilgilerini istememektedir.
- Bankalar, e-posta yoluyla hiç bir şekilde şifre işlemleri yaptırmamaktadır.
- E-postalarda bulunan linkler ile e-postalar içerisinde yönlendirildiğiniz linklere girmeyin.
- Kredi kartınızı kullandığınız ya da kişisel bilgilerinizi yazdığınız bilgisayarın güvenli olmasına dikkat edin (Kullandığınız web sitesi http:// yerine https:// olmalıdır).
- Phishing web sitesi sahtekarlıklarına karşı uyarılmak için bilgisayarınıza İnternet'ten uyarıcı bir web tarayıcısı yükleyebilirsiniz (http://www.earthlink.net/earthlinktoolbar İnternet'ten ücretsiz olarak yüklenebilen bir tarayıcıdır).
- Düzenli olarak çevrimiçi hesaplarınızı kontrol edin, aylık kontrolü beklemeyin.
- Her hesap numaranız için farklı bir şifre belirleyin.
- Hesap numaranızın ve kimlik numaranızın yazılı olduğu materyalleri saklamayın, yok edin.

- Banka hesabınızı, kredi kartlarınızı ve banka kartlarının ekstrelerini düzenli kontrol edin, şüpheli gördüğünüz durumlarda bankanız ile irtibata geçin.
- İnternet tarayıcınızın güncel olduğunu ve tüm güvenlik ayarlarının yüklendiğini kontrol edin. Microsoft Internet Explorer kullanıyorsanız, Microsoft Security ana sayfasından http://www.microsoft.com/security/'den konu ile ilgili özel güvenlik ayarlarını yükleyin.
- Bilgisayarınızda güncel bir virüs koruma programı olmasına dikkat edin.
- Güvenlik duvarı (firewall) kullanımı güvenliğinizi artıracaktır.
- İnternet bankacılık işlemlerinizi güvenliğinden emin olmadığınız bilgisayarlardan yapmayın. Bu amaçla internet kafe gibi umuma açık yerlerdeki bilgisayarların kullanılmaması tavsiye edilir.

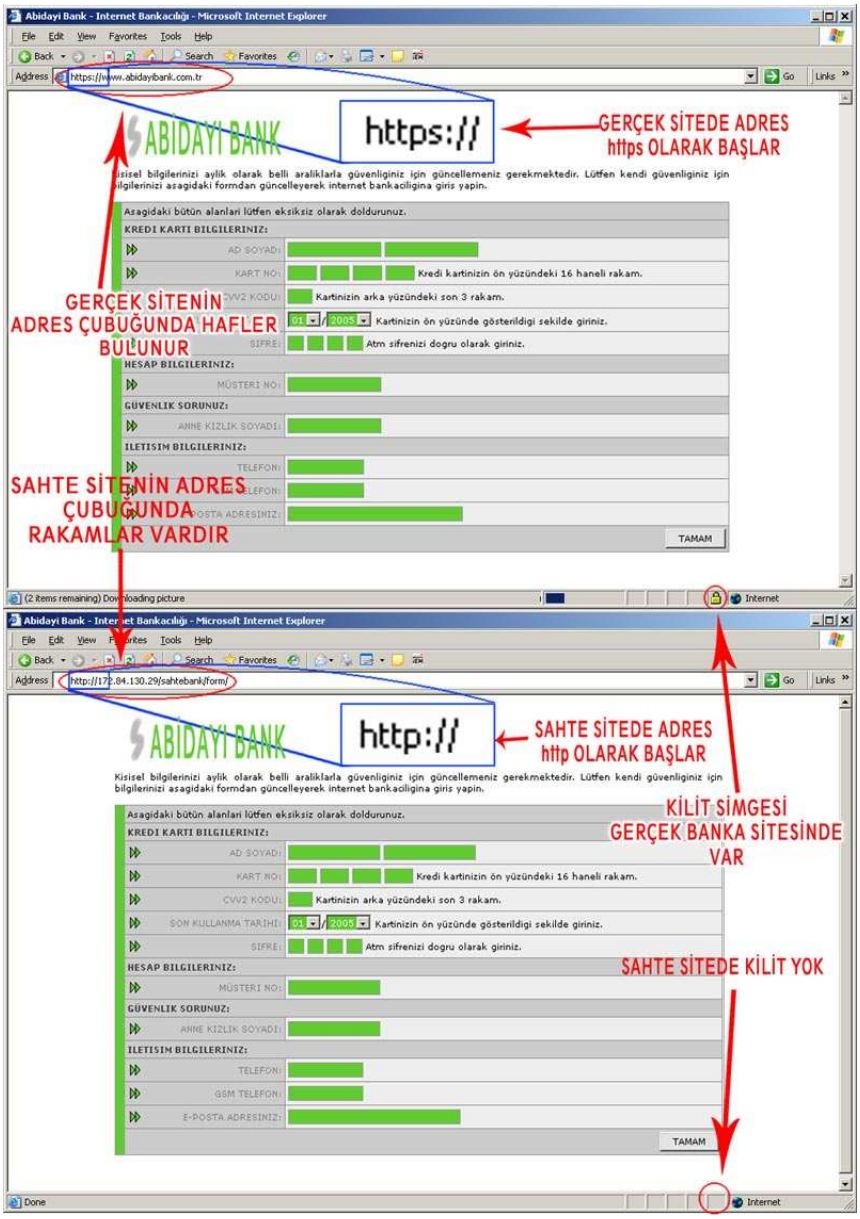
PHISHING (OLTA) SALDIRILARI

Son günlerde çeşitli banka ve finans kurumları tarafından gönderilmiş gibi görünen, acil ve çok önemli konular içeriyormuş gibi duran **sahte** e-postalar internette yayılmaktadır. Bu e-postalarda verilen linkler aracılığı ile banka müşterilerinden, **kart bilgileri, kart şifreleri, internet şubesi şifreleri ve kişisel bilgileri** istenmektedir. Bu eylem açık bir dolandırıcılık girişimidir. Kesinlikle bu tür e-postalara yanıt vermeyin veya istenen bilgileri girmeyin. Bankalar, e-posta yoluyla hiç bir şekilde şifre işlemleri yaptırmamaktadır, müşterilerin gizli kişisel bilgilerini istememektedir.

Bu dolandırıcılık saldırılarından korunmak için ayrıca şu noktalara dikkat edin:

- Size gönderilen e-posta'nın kimden geldiğinden ve doğruluğundan mutlaka emin olun.
- Tanımadığınız kişi ya da kurumlardan gönderilen e-postaların içerisinde bulunan linkleri tıklamayın, ekleri bilgisayarınıza yüklemeyin.
- Elektronik posta aracılığıyla veya başka bir ortamda sunulan web sayfa linklerini kullanmayın.
- Erişmek istediğiniz web sayfasının adresini tarayıcınızın adres satırına kendiniz yazın.
- Sadece sayılardan oluşan web adresi ile karşılaşırsanız **dikkatli olun**, çoğu kurum ya da kuruluş web adresi olarak isim kullanmaktadır.

Çoğu gerçek web sitesinin adres satırında sayılar yerine kurum ismi yer alır.



Phishing e-postalar konusunda birkaç örnek aşağıda verilmektedir.

Örnek Phishing Mail 1:

Sayın Abidayı Bank Müşterisi
Hesabınıza 24/şubat/2005 tarihinde Hüseyin Bey tarafından 270 YTL. havale edilmiştir.
Yapılan havale ile
ilgili ayrıntılar aşağıdadır.

Gönderen: Hüseyin Bey
Miktar: 270,00 YTL. (iki yüz yetmiş Yeni Türk lirası)
Şube: Mardin / Merkez
Açıklama: -
Havale onay ve/veya red işlemi için aşağıdaki linkden internet bankacılığı kullanabilirsiniz ve/veya hesabınızda gerekli incelemeleri yapabilirsiniz. Size havale gönderen kişinin bilgileri içinde aşağıdaki linki kullanabilirsiniz.

www.abidayibank.com.tr

Eğer yukarıdaki link çalışmıyorsa lütfen aşağıdaki linki kullanınız.

http://172.84.130.29/abidayibank/form/

Örnek Phishing Mail 2:

Sayın Abidayı Bank Müşterisi...

Son dönem içerisinde yaşanan internet yolu ile dolandırıcılık girişimlerini engellemek amacıyla sizler için abidayı sistemini Türkiye'de ilk defa kullanmaya başladık. Bu güvenlik sisteminin temelini tam olarak oturtmak amacıyla şimdi yaptığınız bütün işlemler ve anlık şifreniz cep telefonu numaranıza bildirilecektir. Bu yeni güvenlik sisteminin işleyişi şu şekildedir; Internet bankacılığına giriş yaptığınızda cep telefonu numaranıza anında bilgi mesajı SMS yolu ile ulaştırılır... Ve yaptığınız bütün Havale/Eft/Nakit Avans işlemleri seçiminize göre cep telefonunuza bildirilir... SMS Aktivasyonu işlemini bütün müşterilerimizin yapması sizlerin güvenliği için zorunlu hale getirilmiştir. Lütfen burayı tıklayarak web sitemiz üzerinden interaktif hesabınıza giriş yaparak uyarıların ulaşacağı cep telefonu numarasını müşteri bilgilerinize ekleyin...

İnternet Şubesine Ulaşmak İçin Burayı Tıklayın...
İnternet Bankacılığı Şifrenizi Almak İçin Burayı Tıklayın...

Bu link ile açılan sayfa birebir bankanızın internet sayfası görünümünde olabilir. Bu nedenle bu tür e-postalardaki linklerin açtığı sayfalarda kesinlikle şifrenizi ya da kişisel bilginizi girmeyiniz.

Phishing (Olta) saldırısından şüphelendiğiniz bir e-postaya cevap verdiyseniz derhal kart ve internet şubesi şifrelerinizi değiştiriniz. Bankanızın çağrı merkezini arayarak konu hakkında bilgi veriniz.

KEYLOGGER

Dolandırıcılar **phishing** yöntemiyle kullanıcının gizli bilgilerini elde etmenin yanı sıra bu bilgilere başka bir yöntem olan keylogger adı verilen klavye ve ekran görüntülerini kopyalayabilen programlar vasıtasıyla ulaşabilmektedirler. Keylogger yöntemi ve alınabilecek önlemler hakkında kısa bilgiler aşağıdadır.

İnternet kullanan banka müşterilerinin veya internet üzerinden ticaret yapan kullanıcıların online işlem şifrelerinin çalınması keylogger, yani klavye tuş girdilerini kayıt eden yazılımlar vasıtasıyla da yapılmaktadır. Kullanıcıların bilgisayarlarına yerleştirilen keylogger adlı yazılım, bilgisayarda yapılan her türlü işlemlerin bir kaydını tutar, bu kayıtlar klavyeden girilen bilgilerin yanı sıra ekran görüntüleri de olabilir. Bu kayıtlar ya sistemde bir txt (metin) dosyası olarak tutulur ya da klavye girdileri e-posta ile saldırgana (hacker) gönderilir.

Keylogger Türü Yazılımlar Sisteme Nasıl Giriyor ?

1) Kötü niyetli kişiler tarafından yazılan ve işletim sistemlerinin açıklarından yararlanılarak hedef bilgisayarın kısmen veya tamamen yönetici haklarını saldırgana teslim eden truva atı

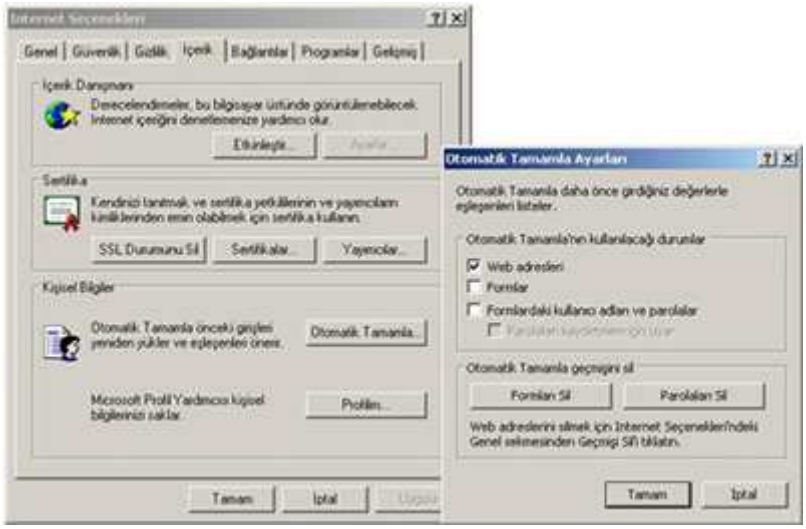
(trojan) adlı yazılımlar aracılığıyla keylogger yazılımları sisteme yüklenebilir.

2) Keylogger yazılımı bilgisayara kullanıcı tarafından yüklenebilir.

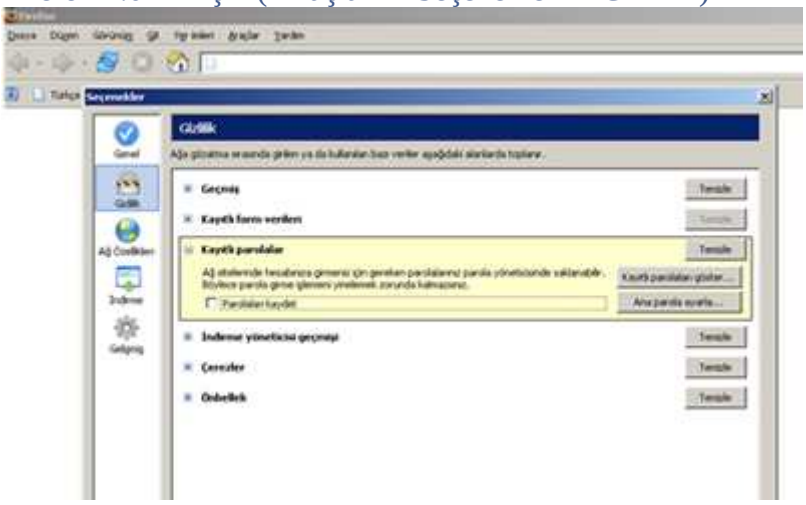
Keylogger ve benzeri programlardan etkilenmemek için:

• Mutlaka işletim sisteminizin güncelleştirmelerini yapın
• Bir güncel ve aktif antivirüs programını bilgisayarınızda bulundurun
• Bankacılık ve önemli işlemlerinizi güvenli olmayan bilgisayarlardan yapmayın
• Kullandığınız bilgisayarın web browserı (internet tarayıcısı)'nın otomatik tanımlama özelliğindeki "Formlarda kullanıcı adları ve parolalar" ile ilgili kısmın işaretsiz olmasına dikkat edin.
Yukarıda bahsedilen "Formlarda kullanıcı adları ve parolalar" bölümündeki düzenleme aşağıdaki şekilde yapılabilir.

İnternet Explorer 6.0 için (Araçlar->İnternet Seçenekleri->İçerik->Otomatik Tamamla)



Firefox 1.0 PR İçin (Araçlar -> Seçenekler -> Gizlilik)



İNTERNETTE GÜVENLİK

İnternette gezinti yapmak, bilgisayarınızın fiziksel olarak internet ortamı ile temasa geçmesi olarak açıklanabilir. Bu durumda her zaman bilgisayarınıza ve kayıtlı bilgilerinize dışarıdan ulaşılma olasılığı vardır. İnternette güvenlik, size gönderilen ve sizin dışarıya gönderdiğiniz bilgilerin güvenli bir şekilde aktarılabilmesidir.

Bir bilgisayara izinsiz erişim için 2 temel yol vardır:

1- En kolay yol bir dosyanın içine virüs programı saklamaktır. Siz bu dosyayı bilgisayarınıza kopyaladığınızda (veya e-posta ekinden açtığınızda) ve çalıştırdığınızda, virüs bilgisayarınıza bulaşmış olacaktır. Virüsler genellikle uygulama (.EXE) dosyalarında saklanabilmektedir. Ancak **macro** virüsü ofis programlarının içinde de saklanabilmektedir. (.DOC, .XLS and .PPT dosyaları). İki virüs tipi de sisteminize zarar verebilir veya bilgisayarınızdaki ya da ofis ağınızdaki gizli bilgilerinizin kopyalanmasına neden olabilir.

Bu tehlikeden korunmanın en iyi yolu yüzde yüz güvenmediğiniz sitelerden program indirmemek, bu programları kullanmamak ve tanımadığınız kişi veya kurumlardan gelen e-postalar da ekli olan dosyaları açmamaktır.

2- Bilgisayarınıza aktif web içeriği kullanarak ulaşmak mümkündür. ActiveX ve Java normalde interaktif içerik sağlamak için kullanılan teknolojiler olmakla birlikte zaman zaman kötü amaçlı olarak ta kullanılabilmektedirler. Tarayıcınızın ayarlarını yaparak bu içeriğin kişisel bilgisayarınıza veya bilgisayar ağınıza zarar verme ihtimalini ortadan kaldırabilirsiniz.

Güvenlik Alanları

Bilgisayarınızı zararlı içeriklerden korumanın anlamı, ziyaret ettiğiniz sitelerdeki zararlı içeriği etkisiz kılmak veya en azından bir tehdide karşı sizi uyarmaktır. Tarayıcınızda farklı güvenlik seviyeleri tanımlayabilirsiniz. Bu güvenlik alanları sayesinde aktif içerik kullanımı ve güvendiğiniz sitelerden dosya indirme konusunda problem yaşamazsınız ve kesintisiz olarak internette gezinebilirsiniz.

İlk programı kurduğunuzda mevcut ayarlarla internet üzerindeki bütün sayfaları görüntüleyebilirsiniz ancak siteleri **güvenilir** ve **kısıtlanmış** olarak ayırmanız gerekmektedir.

Bazı web siteleri siz buraları ziyaret ettiğinizde sizin hakkınızda bilgi toplar ve bu bilgileri bilgisayarınızda bir text dosyasında tutarlar. Bu dosyalara "Tanımlama Bilgisi" (Cookie) denir. Bu dosya, sizin hangi siteleri ziyaret ettiğiniz ve bu sitelerde doldurduğunuz formlardaki bilgilerden oluşur.

Cookie'ler virüs yaymak için kullanılamazlar. Ancak siz bu tür bilgilerin bilgisayarınızda tutulmasını istemiyor olabilirsiniz. Ziyaret ettiğiniz web sitelerinde var olan "Tanımlama Bilgisi" kullanımını güvenlik ayarları vasıtası ile kontrol edebilirsiniz. Güvenlik ayarlarınızı TOOLS (ARAÇLAR) altındaki INTERNET OPTIONS (INTERNET SEÇENEKLERİ) penceresinden PRIVACY (GİZLİLİK) adımı seçerek yapabilirsiniz.

Faydalı Linkler

İnternet kullanırken karşılaşabileceğiniz bazı güvenlik açıklarını kapatmak ve bilgisayarınıza gelebilecek saldırılara karşı sisteminizi koruyabilmek için bazı yardımcı programların sisteminizde kurulu olması gerekmektedir. "Internet Security, Personal Firewall, Anti Virus,

Anti Trojan" gibi isimlerle adlandırılan bu yardımcı programları indirebileceğiniz bazı web adresleri aşağıdadır.

Türkçe içerikli linkler:

- http://www.iem.gov.tr/iem/?idno=147
- Superonline program arşivi
- E-kolay.net program arşivi
- Microsoft Tükiye, Windows güvenlik yamaları ve güncellemeleri

İngilizce içerikli linkler:

- Tucows.com'un güvenlikle ilgili programları
- Download.com'un güvenlikle ilgili programları
- Norton güvenlik yazılımları