T.C.
MİLLÎ EĞİTİM BAKANLIĞI

PAZARLAMA VE PERAKENDE

e-BANKACILIK HİZMETLERİ
343FBS017

Ankara, 2011

- Bu modül, mesleki ve teknik eğitim okul/kurumlarında uygulanan Çerçeve Öğretim Programlarında yer alan yeterlikleri kazandırmaya yönelik olarak öğrencilere rehberlik etmek amacıyla hazırlanmış bireysel öğrenme materyalidir.
- Millî Eğitim Bakanlığınca ücretsiz olarak verilmiştir.
- PARA İLE SATILMAZ.

İÇİNDEKİLER

AÇIKLAMALAR

KOD	**342**
ALAN	**Pazarlama ve Perakende**
DAL/MESLEK	**Sigortacılık**
MODÜLÜN ADI	**Elektronik Bankacılık**
MODÜLÜN TANIMI	Elektronik bankacılıkla ilgili genel kavramları öğreten, E-Bankacılık uygulamaları ve güvenlik kurallarını açıklayan, teknolojideki değişmeler ve yenilikler dikkate alınarak, açık ve anlaşılır olarak hazırlanmış öğrenim materyalidir.
SÜRE	40/24
ÖN KOŞUL	
YETERLİK	Üçüncü Şahıs Mali Sorumluluk Sigortası poliçesi satmak
MODÜLÜN AMACI	**Genel Amaç**: Gerekli ortam sağlandığında, E bankacılık uygulamalarını ve güvenlik kurallarını uygulayabileceksiniz. **Amaçlar**: ➢ E-Bankacılıkla ilgili kavramları ve tanımları açıklayabileceksiniz ➢ Güvenli E-Bankacılık kullanımını yapabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	Sınıf ortamı ve büro ortamında projeksiyon, Bilgisayar donanımı ve internet erişimi sağlanmalıdır.
ÖLÇME VE DEĞERLENDİRME	Modülün içinde yer alan her faaliyetten sonra, verilen ölçme araçlarıyla kazandığınız bilgi ve becerileri ölçerek kendi kendinizi değerlendireceksiniz.Öğretmen; modül sonunda sizin üzerinizde ölçme aracı uygulayacak, modül ile kazandığınız bilgi ve becerileri ölçerek, değerlendirecektir.

GİRİŞ

Sevgili Öğrenci,

Paranın bir değişim değeri olmasıyla, ticaret yeni bir çehre kazanmış, teknolojik gelişimler eşliğinde sanal para kavramının oluşmasıyla e-ticaret anlayışı doğmuştur. Zamanla, evde, internetin başında dünyanın her hangi bir yerinden alış veriş yapmak son derece kolaylaşmıştır.

Bankalar her geçen gün teknolojik gelişmelerle paralel olarak hizmet ve ürünlerini çeşitlendirmektedirler. En az maliyetle en çok kar elde edebilmenin yollarını aramaktadırlar. Bu da, her yere şube açarak genişlemekle olamaz. Yeni bir şube açmak bankalar için özellikle kısa vadede büyük maliyetlerin altına girmek anlamına gelmektedir ki, bu, sıcak paraya en çok ihtiyaç duyulan bir sektörde hizmet veren banka için son derece riskli bir durum oluşturmaktadır. O halde, daha kestirmeden sonuca gitmenin yollarını aramak bir gerekliliktir. Tam da bu nokta da e-bankacılık bu yaraya merhem olmaktadır.

Askeri amaçlarla 1960'ların ortasında hayata giren internet, büyük bir hızla diğer alanlara da sirayet etmiştir. Bankalar bu fırsattan iyi yararlanarak hızla internet şubeleri açmış ve kısa sürede olumlu karlar elde etmişlerdir. Ancak, sistemdeki açıklardan yararlanmayı meslek haline getirmiş olan bir takım insanlar yüzünden çok sayıda internet bankacılığı müşterisinin mağdur olması, internet bankacılığının daha hızlı yayılmasına engel olmuştur. Bankalar bu durumlarla sürekli mücadele etmek amacıyla güvenlik duvarlarını artırıcı önlemler almak zorunda kalmıştır.

İnternet bankacılığı ülkemiz için emekleme döneminden yeni çıkmıştır. 80'lerin sonunda tanıştığımız bu hizmet sayesinde banka şubelerindeki kuyruklar çok az da olsa azalmaya başlamıştır. İnternet kullanım oranının artmasına paralel olarak eğitimle beraber internet bankacılığının kullanımı da artış göstermektedir. Bazı olumsuzluklar olsa da internet bankacılığı her geçen gün gelişmektedir. Bankacılık sektörü bu gelişmeler paralelinde bilgisayar teknolojisini iyi kullanabilen elemanlara ihtiyaç duymaktadır. Bu modül ileriki meslek hayatın için sana yeni fikirler verecek ve yeni kapılar açacaktır. İlk adımı at ve teknolojik yeniliklere hazırlıklı ol.

ÖĞRENME FAALİYETİ–1

AMAÇ

Elektronik bankacılığın özelliklerini ve tarihsel gelişimini tanımlayabileceksiniz.

ARAŞTIRMA

Sevgili öğrenci, bu faaliyet öncesinde şu araştırmaları yapmalısınız:

- İnternetin insanlığa etkisini araştırınız?
- Elektronik bankacılık sistemini kullanan kişi ve kurumlarla görüş alışverişinde bulununuz.

Araştırmalarınız sonucu edindiğiniz bilgileri, sınıfta arkadaşlarınızla paylaşmanız ve onlarında düşüncelerini almanız gerekmektedir.

1.İNTERNET BANKACILIĞI

Bankacılık sektörü tüm hızıyla gelişmektedir. Günümüzde bankalar stratejik önem taşımaktadırlar. Elektronik bankacılığa karşı ilgi giderek artmaktadır. Teknolojik ürünler, genç, eğitimli, ekonomik ve sosyal statüsü yüksek müşteriler tarafından kullanılmaktadır

Resim 1.1: Bankanın kapısını açın

Bankacılık işlemleri, günümüzde teknolojinin gelişmesiyle daha kolaylaşmış, maliyet, zaman ve risklerin en aza indirilmesi, karlılığın maksimize edilmesi için yeni kanallar devreye girmiştir. Bu kanallardan en önemlisi, bankacılık için dönüm noktası olabilecek bir yenilik olan "internet bankacılığı"dır.

1.1. İnternet Bankacılığının Tanımı

Banka; halktan topladığı ya da kendi sahip olduğu paraları kredi olarak kullandıran ve para akışına aracılık eden iktisadi işletme ve bu işletmenin sahibi durumunda olan anonim şirketin adıdır. Bankacılık sektörü, elektronik ticaretin en yoğun uygulamalarına rastlanılan sektör konumundadır. Söz konusu teknolojik gelişmeler sonucu ortaya çıkan ve genel olarak "Şubesiz Bankacılık Uygulamaları" olarak adlandırılan şubesiz bankacılık faaliyetleri arasında, telefon bankacılığı, ev bankacılığı, internet şubeleri örnek gösterilebilmektedir.

İnternet bankacılığı; ev ve ofis bankacılığının yapılmasına olanak veren interaktif yazılımların yerini internetin alması ve güvenlik sorununa çeşitli çözümler üretilmesiyle gelişen ve web temelli olarak gerçekleştirilen bankacılık işlemidir.

Resim 1.2: Oturduğunuz yerde, rahat, hızlı, yorulmadan

Genel olarak bankacılıkta yeni teknolojilerin kullanılması, örgütsel yapıda değişikliklere, bankalardaki bilgi akış sisteminin standartlaşmasına, etkinliğin sağlanmasına olanak sağlamaktadır. Ayrıca, aynı işlemlerin tekrarının engellenmesine ve daha kısa zamanda daha fazla işlem yapılabilmesine, orta düzey yönetici istihdamının azalmasına, yönetimin sorumluluğunun dağıtılmasıyla her gruba farklı görev, yetki ve sorumluluk verilmesi mümkün olmaktadır.

Bankaların, gerçek anlamda elektronik bankacılığa geçişi, kişisel bankacılık hizmetlerinin 1980'lerin sonlarına doğru herkesin kendi bankacılık işlemlerini kendisinin yapması olanağı sağlayan para çekme makineleri (ATM) ile başlamıştır. ATM'lerde, banka müşterisine verilen bir elektronik banka kartı yardımıyla, bütün temel bankacılık işlemleri yapılmaktadır.

Resim 1.3: Dünyayı bilgisayarınıza taşıdık

Türk bankacılık sektörü son yıllardaki teknolojik gelişmelerden önemli ölçüde etkilenmiş ve yapılan büyük ölçekli teknolojik yatırımlar ile klasik bankacılık işlemlerinin yanı sıra teknolojinin gerektirdiği yeni bankacılık ürünlerini de kullanmaya başlamıştır. Ülke ekonomisinde önemli bir yer tutan bankacılık sektörü, son 15-20 yıllık dönemde önemli bir yapısal değişim ve gelişim süreci geçirmiştir. Bu hızlı değişimin en önemli kaynağı ise teknolojik ve elektronik alanda yaşanan gelişmelerdir. Bu değişime çabuk uyum sağlayan ve zamanında gerekli yatırımları yapan bankalar için teknoloji büyük bir rekabet gücü olmuştur.

Teknoloji kullanımının bankalar için önemli hale gelmesi ile birlikte, bankalar müşterilerine hizmet sunmak için geliştirdikleri yeni yöntemleri de kullanmaya başlamışlardır. Bu hizmetlerden bazılarına, Otomatik vezne makineleri (ATM), kredi kartları, telefon bankacılığı ve internet bankacılığı örnek olarak gösterilebilmektedir.

İnternet kullanımında meydana gelen artışla birlikte internet aracılığıyla yapılan bankacılık işlemleri gün geç tikçe artmaktadır. İnternet bankacılığı, bankacılık işlemlerinin internet ortamında bankaların web siteleri üzerinden istenildiği zaman dünyanın her yerinden ulaşılarak yapılmasını sağlamaktadır. İnternet bankacılığında, banka personeli ile bire bir ilişki içinde bulunulmamaktadır. Müşteri, bankacılık işlemlerini gerçekleştirirken kendi girdiği talimatlar doğrultusunda otomatik olarak gerçekleştirmektedir.

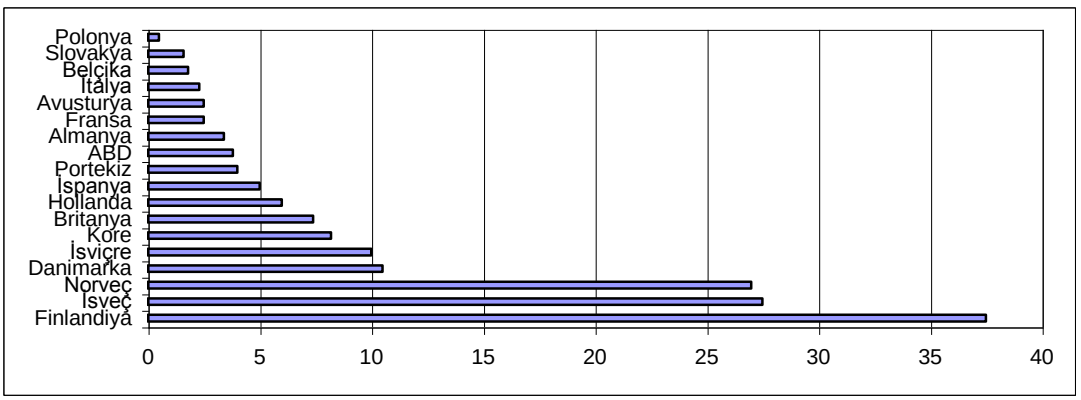
İnternet bankacılığında, internetin yüksek ve ucuz işlem kapasitesi sayesinde para yatırıp çekme dışında tüm bankacılık işlemlerinin en ucuz maliyetle yapılması mümkündür. İnternet bankacılığıyla banka müşterileri, para yatırıp çekme dışında kalan;

- Hesap ekstrelerinin alınması,
- Hesaplarındaki para miktarının ve hesap bilgilerinin öğrenilmesi,
- Para transfer işlemleri,
- Kredi kartı bilgi sorma ve borç ödeme işlemleri,
- Döviz işlemleri,
- Her türlü yatırım hesabı kıymet bilgileri alım satım talimatlarının verilmesi,
- Vergi, SSK gibi ödemelerinin gerçekleştirilmesi ve daha bir çok gerçek bankacılık işlemini yer ve zamana bağlı kalmaksızın internet üzerinden gerçekleştirebilmektedirler.

İnternet bankacılığıyla hemen hemen fiziksel şubelerden yapılmakta olan tüm işlemler yapılabilmektedir.

İnternet, yeni müşteriler elde etmeleri, müşteri ilişkilerini geliştirmeleri ve satışlarını artırmaları için bankalara büyük olanaklar sağlamaktadır. Günümüzde internet bankacılığı hizmeti sunmak bankalar için bir zorunluluk halini almıştır. Satış ve hizmet aşamasında internet teknolojileri ve insan ilişkilerini birleştiren kuruluşlar, gelişmede ve büyümede en ön sıralarda yer almaktadır. Büyük bankaların çoğu uzun zaman önce internet yapılarını oluşturmuşlar ve bugün ikinci ya da üçüncü jenerasyon sistemlere adım atmışlardır.

Bankacılık işlemlerini 1998 yılından bu yana internet üzerinden gerçekleştirmek isteyen insanların sayısında büyük artış gözlenmektedir. Amerika Genel Muhasebe Ofisi 2003 yılında ABD'de evlerinden bankacılık hizmeti gerçekleştiren insanların sayısını 2,5 milyon olarak tahmin ederken, 2004 yılı için 18 milyon kullanıcı tahmininde bulunmaktadır Şekil 1'de seçilmiş ülkelerin internet bankacılığı kullanım oranları yüzdesel olarak verilmiştir.



Şekil 1.1: Nüfusa göre internet bankacılığı kullanım oranları (yüzde)

Burada göze çarpan şey, tıpkı internet kullanım oranlarında olduğu gibi internet bankacılığı kullanım oranlarında da Kuzey Avrupa ülkelerinin diğer ülkelerden belirgin bir şekilde üstün olmasıdır. ABD'de ise internet kullanım oranı % 55 civarında iken internet bankacılığı kullanım oranı % 4'ler seviyesinde bulunmaktadır.

1.2. İnternet Bankacılığında Temel Öğeler

İnternet bankacılığını ev ve ofis bankacılığından ayıran özellik, internet bankacılığında bankanın günün her saatinde milyonlarca müşteriye hizmet verebilmesidir.

ABD'de başlayan internet bankacılığı fiziksel para çekimi hariç bütün hizmetleri müşterilere sunabilmektedir. Sanal cüzdanların 2000'li yıllarda (smart card- akıllı kartlar) kullanımının yaygınlaşması ile beraber para çekiminin de gerçekleştirilmesi planlanmaktadır.

IBM Danışma gurubuna göre, ABD ve AB'de gerçekleştirilen bankacılık işlemlerinin bugün için yaklaşık % 5'ini temsil etmesine rağmen, internetin 10 yıl içerisinde finansal hizmetlerin sunumunda en önemli dağıtım kanalı olması öngörülmektedir.

Bir ülkede internet bankacılığının uygulanması kişisel bilgisayar miktarı, telefon aboneliği ve internet bağlantısıyla doğrudan ilişkilidir. Tablo 1'de gelişmişlik düzeyi farklı ülkelerdeki bu veriler görülmektedir.

ÜLKE	Toplam Nüfusa Göre Kişisel Bilgisayar Kullanımı (%)	Toplam Nüfusa Göre Cep Telefonu Aboneliği (%)	Toplam Nüfusa Göre İnternet Bağlantısı (%)
Sanayileşmiş Ülkeler Ortalaması	32	44	3,46
Finlandiya	36	65	10,57
Almanya	30	29	1,61
İtalya	19	53	0,59
Japonya	29	45	1,33
Norveç	45	62	7,15
Portekiz	9	47	0,50
İsveç	45	58	4,88
ABD	52	31	11,23
Arjantin	5	12	0,18
Çin	1	3	0
Türkiye	3	13	0,05

Tablo 1.1: Seçilmiş Ülkelerdeki İnternet Bankacılığını Etkileyen Unsurlar.

Tablodan da anlaşılacağı gibi sosyal, kültürel ve demografik özelliklerden de etkilenmesine rağmen ülkedeki internet kullanımı kişisel bilgisayar miktarı ve telefon aboneliği ile doğrudan ilişkilidir. Dolayısıyla, internet bankacılığının yaygınlaşması kişisel bilgisayar kullanımı ve internet bağlantılarının artırılması ile mümkün olabilmektedir. Son yıllarda gözlemlenen teknolojik gelişmeler karşısında yapılan tahminlere göre Amerika Birleşik Devletlerinde banka müşterilerinin % 8 ile % 22 arasında bir oran internet bankacılığını tercih ederken bu oran İskandinav ülkelerinde yaklaşık % 30'dur.

Resim 1. 4: İşten bankaya gitmekbu kadar kolaymıydı!

İnternet bankacılığı kullanımının olumlu ve olumsuz yönleri bulunmaktadır. Bunlar:

- İnternet üzerinden yapılan işlem maliyeti şubeden yapılan işlem maliyetine göre oldukça ucuzdur. Şöyle ki, şube'de işlem başına hizmetin maliyeti yaklaşık 1.5 YTL iken, bu rakam internet bankacılığında 0.1 YTL' ye düşebilmektedir. Maliyetteki düşüş yanında bölgesel farklılık gözetmeden günün her saatinde her türlü hizmet verebilmede rahatlık ve uygunluk finansal hizmetlerin pazarlamasında önemli rekabet avantajı ortaya çıkarmıştır.
- İnternet bankacılığının en olumsuz yönü büyük miktarda yatırım gerektirmesidir. Yoğun rekabet koşullarında ise internet bankacılığı uygulamasına geçildikten sonra uzun bir süre bu işlemlerden kazanç sağlamaları mümkün olmamaktadır. Ancak, bu yatırım yapılmadığı takdirde bankaların sektördeki rekabet güçleri azalacaktır.

- Daha çok eğitim düzeyi yüksek ve teknoloji ile büyüyen gençler arasında daha yaygın olan internet bankacılığın başarısında, güvenlik, gizlilik ve toplumsal güvenin sağlanması önemli rol oynamaktadır.

- İnternet bankacılığında temel riskleri güvenlik, itibar, yasal, kredi, likidite, faiz oranı ve piyasa oluşturmaktadır. İnternet bankacılığının diğer bir olumsuz yönü ise şubelerde gerçekleşen bire bir müşteri ilişkilerindeki olumlu yönlerin ortadan kalkmasıdır.

1.3. İnternet Bankacılığının Adımları

İnternet bankacılığının gerçekleşme aşamalarını da inceleyecek olursak, internette bankacılık beş ana adımda gerçekleşmektedir.

- Adım: Stratejik sayfalar, bankanın kendisinin, hizmetlerinin ve ürünlerinin tanıtıldığı yani müşteri ilişkilerinin düzenlemede kullanıldığı ilk adımdır. İlk adımda aktivite azdır. Bu adımda bilgi sunulmaktadır. Bankanın ürünleri hakkında ayrıntılı bilgiler verilerek, banka müşterisinin donanımı artırılmaktadır.

- Adım: İnteraktif bir sayfa hazırlanmakta, ilgili programlar sayfadan indirilebilmekte, basit hesap fonksiyonları gerçekleştirilmektedir. Formlar doldurulmakta , adres değişimleri, hareket sorgulamaları yapılabilmektedir.

- Adım: Bu adımda gerçek bankacılık işlemlerine ilk giriş yapılmakta, hesap işlemleri internet üzerinden gerçekleşebilmektedir. Bu adımda fatura ödemeleri, havale, EFT (Elektronik Fon (para) Transferi) yapılabilmekte olduğu gibi yeni hesap açtırmak da mümkün olmaktadır.

- Adım: Bir önceki adıma ek olarak müşteri kendi portföyünü yönetebilmektedir. Gelecekteki yatırımları için tavsiyeler alabilmekte, kredi başvurusu yapabilmekte, kredi açtırabilmektedir.

- Adım: Elektronik para çekiminin yapılması bilgisayar, telefon veya televizyon yoluyla elektronik cüzdan doldurulduğunda fiziksel şubenin yaptığı tüm işlemlerin yapılmış olacağı düşünülmektedir.

1.4. İnternet Bankacılığının Durumu

İnternet bankacılığı en çok Kuzey Amerika, Yeni Zelanda, Norveç ve Finlandiya gibi Kuzey ülkelerinde daha yaygın olarak kullanılmaktadır. Dünya genelinde 36 milyona ulaşan online banka hesaplarının dağılımına baktığımızda % 45 oranına denk gelen 16 milyon hesabın Kuzey Amerika'da olduğu, bunu 13 milyon hesap ile Avrupa'nın takip ettiği, geri kalan 7 milyon hesabın Japonya, Asya Pasifik, Avustralya başta olmak üzere diğer ülkeler arasında dağıldığı görülmektedir.

1.4.1. ABD'de İnternet Bankacılığının Durumu

ABD'deki banka web sitelerinin şu üç alandaki fırsatları değerlendirmek için kullanıldığı görülmektedir:

- Bilgiyi pazarlamak,
- Banka ürün ve hizmetlerinin dağıtımını gerçekleştirmek,
- Müşteri ilişkilerini iyileştirmek

ABD'de 1997 yılında web sitesi sahibi şirketlerin %35'lik kısmının maliyetlerini düşürmek amacıyla web sitesi kurduklarının ortaya çıkmış olduğu görülmektedir. Yine bu şirketlerin % 13'lük kısmın pazarlama faaliyetleri, %18'lik kısmın satış yapmak ve % 2'lik kısmın müşterilere hizmet vermek amacıyla web sitesi sahibi oldukları görülmektedir. ABD'de toplam banka şube sayısının 2025 yılına kadar şu anki sayınını 2/3 oranında azaltılması planlanmaktadır.

Resim 1.5: Dünya çok küçüldü

1.4.2. Avrupa Ülkelerinde İnternet Bankacılığının Durumu

Avrupa birliği kriterlerine göre teknolojik gelişme ile iç pazarın birleştirilmesi, ekonomik ve mali bütünleşmenin sağlanması arasında yakın bir bağ bulunduğu vurgulanmaktadır. Bu nedenle, Birliğin mali ve parasal bütünleşmesi ve tek halklı bir Avrupa'nın genişlemesi, malların ve sermayenin serbest dolaşımı, ancak yeni ödeme araçlarının sağladığı teknolojik destekten yararlanıldığı takdirde,

bütünüyle etkili olabileceğinden Birlikte ödeme sistemlerini kullananların çıkarı açısından, bu sistemlerin birbiriyle uyumlu ve tamamlayıcı olmasını mümkün kılacak standartlar ile yasa, tüzük, yönetmelik ve uygulama kurallarının koordine ve uyumlaştırılması için işbirliği yapılması gerekliliği öngörülmektedir. Dolayısıyla, internet ve diğer yeni teknolojilerin Avrupa bankalarının işlem, ürün ve dağıtım kanallarına entegrasyonunda nihai hedef, rekabet avantajı kazanmaları, pazar payını artırmaları, etkinlik ve risk yönetim becerilerini geliştirmeleridir.

Resim 1.6: O banka benim bankam

1.4.3. Türkiye'de İnternet Bankacılığının Durumu

Türkiye'de bilişimin önde gelen destekçisi bankalar, internete girmekte ve bu ortamdan çok şey beklemektedirler. Türkiye'de genellikle teknolojik anlamda , özellikle de bilgisayar alanında gelişmelerin ana kaynağı bankalar olmaktadır. İlk etkin bilgisayar kullanımı, ilk network kurulumu, ilk parasal bilgi transferi doğru ve yaygın olarak bankalar tarafından yapılmıştır.

Bankalarımızın, şubelerinin kapısından içeri giren müşteriye güler yüz gösterip para kazanmak varken, internet bankacılığına soyunmalarındaki etkenler şöyle sıralanabilir.

- Gelişen teknolojiyi yakından takip etme isteği,
- Bankaların, şube kurma, yönetme, geliştirme ve personel giderlerini karşılama maliyetlerinden kaçınma isteği,
- Alternatif kanallar içerisinde internet bankacılığının, bilinen bütün gelişmelerden daha ucuza gelmesi (Örneğin; şu anda hemen tüm bankaların kullandığı telefonla müşterilere cevap verme sistemi internet bankacılığından çok daha pahalı bir sistemdir),
- Rutin işlerin internet şubesi aracılığıyla gerçekleşmesinin, şubelerin yükünü azaltacağı beklentisi,
- İnternete giren ve bankalarından yenilik bekleyen müşteri profili.

Resim 1.7: Dünden bugüne çok şey değişti

İlk internet şubesi 1998 yılında Türkiye İş Bankası tarafından devreye sokulmuştur. Ardından Garanti Bankası, Osmanlı Bankası ve Pamukbank da aynı yıl içerisinde internet üzerinden bankacılık hizmeti sunmaya başlamıştır. Günümüzde ise internet bankacılığı hizmeti sunan bankaların sayısı hızla artmıştır.

Hemen hemen bütün bankaların internet şubesi bulunmaktadır. Ancak Türkiye'de şube açan yabancı bankalar ile yabancı sermayeli kalkınma ve yatırım bankalarının Türkiye'de internet bankacılığı şubesi bulunmamaktadır.

Bu noktada, ülkemizdeki internet bankacılığı kullanımının son durumunu açıklamak gerekmektedir. İnternet bankacılığı hizmetleri için kayıtlı bireysel müşteri sayısı 2006 yılı Haziran sonu için 15 milyon 368 bin 206 olmuştur. Türkiye Bankalar Birliği (TBB)'nin yayınladığı rapora göre, 2006 yılının ilk yarısında 2 milyon 478 bin 523 bireysel müşteri tarafından en az bir kez internet bankacılığı işlemi yapılmıştır. Bu miktar, toplam kayıtlı müşteri sayısının % 16'sını oluşturmaktadır. Haziran 2006 döneminde, Mart 2006 dönemine hem aktif bireysel müşteri sayısında 128.062 adet, kayıtlı müşteri sayısında ise 626.645 adet artış gerçekleşmiştir.

1.5. İnternet Bankacılığının Gelişim Süreci

İnternet bankacılığının gelişim sürecini ifade etmeye öncelikle dünyadaki gelişim sürecini incelemekle başlamak doğru olacaktır.

1.5.1. Dünyada İnternet Bankacılığının Gelişimi

TCP/IP transfer protokolü ise 1980'leri ortalarında geliştirilmiştir. "World wide web (www) html dili" (standart kodlama sistemi) ise1989 yılında bulunmuştur. Bunlar bilgisayarların açık ağlarda, iyi bilinen adıyla "internet" üzerinde birbirleri ile iletişime geçmesini sağlamıştır. Tarama, sınıflandırma araçları, hızlı işlemciler, uydular, optik kablolar vb. gibi bilgisayar ve iletişim teknolojilerinde sağlanan diğer gelişmeler, söz konusu iletişimi önceden öngörülemeyen boyutlara taşımıştır. Bundan 15 yıl kadar önce 1 milyon olan host (sunucu) bilgisayar sayısı 1997 yılında 20 milyona ulaşmıştır. 2007 yılında ise bu sayının 500 milyona ulaşacağı tahmin edilmektedir. İnternet kullanıcı sayısının da günümüzde yarım milyar civarında olduğu düşünülmektedir.

İnternet bankacılığı kuşkusuz yenidir. Ancak geçerli olan esaslar ve ilkeler bakımından geleneksel bankacılık işlemleri ile paralellik göstermekte, zaman zaman klasik bankacılık işlemlerine de başvurmaktadır. İnternetin gelişimine bağlı olarak gelişen bir başka boyut da elektronik ticaret olmuştur. Bu yaklaşımla e-ticaret ve internet bankacılığının gelişimi paralellik arz etmektedir.

İnternet bankacılığının gelişim süreci, 1996 yılına dayanmaktadır. İnternet ortamında e-ticaret şirketler tarafından yoğun olarak 1996 yılından itibaren kullanılmaya başlamıştır. Şüphesiz bundan önceki yıllarda da, e-ticaret uygulamalarının varlığından bahsetmek mümkündür. Ancak, bu tür uygulamalar ya "intranet" olarak adlandırılan şirket içi ağlar, ya da "ekstranet" denilen ve şirketlerin kendi aralarında veya belirli müşterileri ile bilgi alışverişinde, ticari ilişkide bulundukları ve üçüncü taraflara kapalı olan uygulamalardır.

Resim 1.8: İnternette Dünya bankacılığı

E-ticaretin gelişim sürecinin, doğal olarak, internetin gelişimine bağlı olduğu gözlenmektedir. Çünkü, e-ticaret kavramı; herkese açık elektronik ağ üzerinden gerçekleştirilen ticari faaliyetleri ifade etmektedir. Toplam e-ticaret, 1997 yılında tahmin edilen 26 milyar USD'lık seviyesinden, 2001 yılında 330 milyar USD'a yükselmiştir. 2006 sonu itibariyle bu rakamın 1 trilyon USD olması beklenmektedir.

1.5.2. Türkiye'de İnternet Bankacılığının Gelişimi

Bankalar, gerçek anlamda elektronik bankacılığa geçtikten sonra, kişisel bankacılık hizmetlerine 1980'lerin sonlarına doğru (herkesin kendi bankacılık işlemlerini kendisi yapması) otomatik vezne makinesi (ATM- Automated Teller Machine) ile geçmiş bulunmaktadır. ATM'lerde, banka müşterisine verilen bir elektronik banka kartı yardımıyla, hemen hemen bütün temel bankacılık işlemleri yapılmaktadır. Bunun bir uzantısı olarak, kişisel bankacılık hizmetleri, 1995'lerde "telefon" bankacılığı ile tanışmıştır. Hesaplara "telefon" yardımıyla otomatik erişmek ve işlemler yapmak mümkün hale gelmiştir. Bunun sonraki aşamasında ise, özellikle 1998'lerden sonra, internet bankacılığı ortaya çıkmıştır.

Hesaplar arasında havale, EFT, kredi kartı ödemesi, otomatik ödeme talimatları, döviz alım satımı, hatta bazı bankaların "Yatırım" kanalları kullanılarak fon alım satımı, borsada hisse senedi alma/satma gibi birçok hizmetler günümüzde internet bankacılığı kavramın içinde yer almakta ve her gün artan sayıda kişi bu servislerden yararlanmaktadır. WAP protokolü kullanarak "cep telefonları" ile WAP Bankacılığı ise 2000'li yılların başından itibaren hayata geçmiştir. Bu sistemde, yukarıda tanımlanan tüm bankacılık hizmetlerine "WAP destekleyen cep telefonlarından" menüler yardımıyla erişmek mümkündür.

Günümüzde kişisel bilgisayarlar aracılığıyla daha hızlı ve daha kolay ulaşılan internet bankacılığı yapılmaktadır. Başlangıçta bir çok banka interneti, kendilerini ve sundukları bankacılık hizmetlerini tanıtmak amacıyla kullanmaya başlamıştır. Ancak gelişmekte olan bankacılık sektöründe, interaktif bankacılık devri başlamıştır. Türkiye'de de büyük bankalar hızla internet üzerinden bankacılık işlemlerinin yapılabilmesi için ardı arkasına internet şubeleri açmışlardır. Türkiye İş Bankası, Garanti Bankası gibi büyük bankalar 1998 yılında internet şubelerini açmışlardır. Başlangıçta çok az işlem internet üzerinden yapılabilmekteyken gelişen güvenlik ve altyapı teknolojileri ile pek çok işlem internet üzerinden yapılabilir hale gelmiştir. Örneğin, Garanti Bankası'nın hedefleri arasında bankacılık işlemlerinin yüzde 70'inin internet üzerinden yapılması yer almaktadır.

Günümüzün iletişim harikası olan internet, bankacılık sektörüne de damgasını vurmaktadır. Nakit çekme dışındaki her türlü bankacılık işlemleri sanal banka şubelerinde yapmak mümkün hale gelmiştir. Türkiye'de internette ilk şubeyi Türkiye İş Bankası açmış, bunu diğer bankalar izlemiştir.

İnternet bankacılığında bankada hesabı olan müşterilere istemeleri halinde internet şifresi verilmektedir. Şifreyi alan kişiler internet bağlantılarıyla nakit para çekme dışında her türlü yatırım, havale, fatura ödemesi ve tüketici kredisi başvurusu gibi işlemleri yapabilmektedir. Bu işlemler arasında hisse senedi ve yatırım fonu alım satımı, döviz alım satımı, mevduat hesabı açma ön plana çıkmaktadır.

Ayrıca bankaların internet şubelerinde sanal alışveriş yapılmaktadır. Sanal alış veriş merkezlerinde yer alan mağazalar internet üzerinden ısmarlanan ürünlerin (ülkemizde üç iş günü içinde müşterilerinin evine ya da iş adreslerine teslim etmektedir), ürün bedellerini kredi kartı ya da vadesiz YTL hesabından tahsil etmektedir.

1.6. Bankalar ve İnternet Bankacılığı

Bankaların internet bankacılığı uygulamasını tercih etmelerinin bir çok nedeni vardır. Genel olarak bankalar da bir ticari işletmedir ve amaçları kar maksimizasyonudur. Bunu sağlayacak olan bütün fırsatlar ve yenilikler değerlendirilmelidir. Bu yeniliklerden belki de en önemlisi elektronik bankacılıktır. İnternet bankacılığı da elektronik bankacılık hizmetlerinin en göz alıcısıdır. İnternetteki teknolojik gelişmeler ilerledikçe, hem banka şubelerinin sayısı hem de ATM ile ev ve ofis bankacılığının önemi azalacaktır. Nakit para yatırma ve çekme işlemleri dışındaki bankacılık işlemlerinin çoğu internet üzerinden yapılabilecektir.

Resim 1.9: İnternette buluşalım

İnternet kullanımının gelişimi beraberinde müşteri eğilimlerinde de bir değişiklik meydana getirmiştir. Müşterilerin artık bir çok kanaldan işlem yapmaya istekli oldukları görülmektedir. Bankalar da müşterilerini en çok ekonomik yönden avantaj sağlayacak kanala yönlendirmektedir. İnternet, bu kanalların en başında gelmektedir. Bunun nedeni müşteri tarafından bir online işleminin bankaya çok daha ucuza mal olmasıdır. Müşterilerin de kişisel ve kalitesi daha yüksek hizmet bekledikleri görülmektedir.

Bankacılar genel olarak elektronik ödemelere endişeyle bakarlar. Çünkü, kağıda dayalı gelirler risk altındadır. Ancak elektronik ödemelerin de hemen ortaya çıkmayacak olan bazı gelir fırsatları sunması olasıdır. ATM'ler ilk ortaya çıktıklarında masraf artırıcı olarak görülmüşlerdir, ancak yavaş yavaş erişim ve değişim ücretlerinden gelen gelirleri artırmaya başlamışlardır. Aynı şekilde, finansal kurumlar müşterilerine online finansal yönetim hizmetleri ve ödeme çeşitlilikleri veya tüccarlara sahtekarlıktan korunma hizmetleri sunarak yarar sağlayabilmektedirler.

İnternet bankacılığındaki artış bireysel bankacılık uygulamaları ve yeni ürünlere olan talebi de artırmaktadır. İnternet kullanıcıları internet üzerinden yaptıkları alışverişler ve reklamlarla internet bankacılığı ürünlerini yakından tanıyıp taleplerini artırmaktadır.

Bankaların sadece internet bankacılığı yatırımları yapmalarının yeterli olmayacağı kesindir. Hizmetlerin içeriğinde farklılık yarattıkları ve kendilerine en yüksek değeri katacak müşterilere ve onların ihtiyaçlarına odaklandıkları ölçüde internet bankacılığında başarılı olabilmeleri söz konusudur. Müşteriye özel üretilecek olan ürün ve hizmetlerle müşteri sadakatiyle karlılık artırılacaktır. Çünkü, finansal kuruluşların yeni müşteri elde etmesi var olan müşterilerle çalışmasına oranla on kat daha maliyetlidir. Sürekli müşteriler daha fazla ürün ve hizmet almakta, fiyatlara karşı daha az hassasiyet göstermekte ve yeni müşterileri de beraberinde getirmektedirler.

1.6.1. İnternet Hizmetlerinin Bankacılığa Sağlayabileceği Katkılar

İnternet hizmetlerinin bankacılığa sağladığı katkıları şu şekilde açıklamak mümkündür:

- Bire bir iletişim imkanı sağlamaktadır; Elektronik posta veya etkileşimli sayfalar kullanılarak banka müşterisi bireyler veya şirketler ile direkt iletişim imkanı elde edilir. Normal posta hizmetinden çok daha hızlı, hatasız, takibi kolay ve maliyeti düşüktür.

- Kişiselleştirme ile müşteriye önemli olduğu hissettirilebilmektedir; İnternet şubesi sayfalarında kişilere özel bankacılık bilgileri sunmak mümkündür. Bu, müşteri memnuniyetini önemli ölçüde etkilemektedir.

- Yeni bankacılık araçları imkanı sunmaktadır; İnternet bankacılığını, yalnızca kullanılan bankacılık enstrümanlarının internet ortamına taşınması olarak düşünmemek grekmektedir. Dünyada hızla artan internet kullanımı ve elektronik ticaretin önümüzdeki yıllarda ülkemizde de yoğun olarak kullanılacağı kesin gözükmektedir.

- Artan bireysel işlemlerin işlem masrafını azaltmaktadır; Bankacılık sisteminde bireysel bankacılığın önemi son yıllarda oldukça artmıştır ve önümüzdeki yıllarda daha da çeşitlenmesi ve hacminin artması beklenmektedir. Daha çeşitli ve çok sayıda işlem ise şubelerdeki masrafı artırabilecektir. Ancak, bireysel bankacılık çok önemli bir kâr kaynağıdır; dolayısı ile artan düşük miktarlı ve kişisel işlemleri iyi yönetebilmek ve düşük harcamalar ile gerçekleştirmek ihtiyacı bulunmaktadır.

- Müşteri veri tabanı oluşturma imkanı vermektedir; Çeşitli nedenlerle bankalar tarafından şubelerindeki müşteri kayıtları ihmal edilmiş olabilmektedir. Bugüne kadar kişisel bilgiler önemli olarak görülmemekle birlikte, günümüzde ticari firmalar için müşterilerinin yaşı, cinsiyeti, doğum tarihi, mesleği gibi bilgiler büyük önem taşımaktadır. Burada e-müşteri ilişkilerinden (e-crm) bahsetmek gerekmektedir. CRM, tüm süreçleri (üretim,finans,pazarlama,satış) kapsayan bir"yönetim felsefesi"ya da yaklaşımı olarak ifade edilmektedir. Buna bağlı olarak e-ticaret uygulamalarının temeline müşteri odaklı bu yönetim anlayışını yerleştirmişse buna da kısaca e-CRM denilmektedir.

- Bankanın imajını artırıcı bir unsur konumundadır; Gelişen teknolojinin dışında kalmamış olmak, bankaların hizmet boyutlarının genişlemesi, müşteri üzerinde olumlu bir etki yaratmaktadır. Klasik şube anlayışının yanında müşterilerin olası beklentilerine cevap vermeye hazır bir sanal şube, bankaların yenilikçi ve gelişmeye açık olduğunun göstergesi sayılabilmektedir.

- Şubeleri WEB tabanlı sistemlere terfi ettirebilmektedir.

Günümüzde çok sayıda bankada şube yapısında client/ server bilgisayar tabanlı uygulamalar kullanılmaktadır. Ancak bu tür sistemlerin işletme masrafları çok yüksektir. Bilgisayar ayarlarındaki kullanıcı sorunları, yeni versiyon yazılımların dağıtılması ve kullanıcıların müdahale imkanlarının kısıtlanması için bir çok pahalı tedbirin alınması zorunlu olmuştur. Buna rağmen bu tarz sistemlerin çalışır vaziyette tutulması için önemli personel kaynağı ayrılması gerekmektedir.

Resim 1. 10: Bu son gelişimiz

Genel olarak bankacılıkta yeni teknolojilerin kullanılması, örgütsel yapıda değişikliklere, bankalardaki bilgi akış sisteminin standartlaşmasına, etkinliğin sağlanmasına olanak sağlayacaktır.

Ayrıca, aynı işlemlerin tekrarının engellenmesine ve daha kısa zamanda daha fazla işlem yapılabilmesine, orta düzey yönetici istihdamının azalmasına, yönetimin sorumluluğunun dağıtılmasıyla her gruba farklı görev, yetki ve sorumluluk verilmesi mümkün olacaktır.

1.6.2. İnternet Bankacılığı Yapan Bankaların Web Ortamında Verdikleri Hizmetler

İnternet bankacılığı hizmeti veren bankaların web sayfaları aracılığıyla sundukları hizmetleri aşağıdaki gibi sıralamak mümkündür. Bunlar:

Hesap bakiyeleri, ekstre ve dekont görüntüleri (mevduat hesapları, kredi hesapları, yatırım portföyü görüntülenmesi), talimatlı ödemeler, para transferleri ve ödemeler (hesaplar arası transfer, hesaba havale, isme havale, EFT (diğer banka hesaplarına transfer), yurtdışına dövizli havale, mevduat hesabından yatırım hesabına transfer, yatırım hesabından mevduat hesabına transfer, senet ödeme, SSK ödeme, motorlu taşıtlar vergisi ödeme, vergi ödeme, fatura ödeme), tüm kredi kartı işlemleri (kredi kartı ekstre bilgileri ve dönem hareketleri, kredi kartı borç ödeme, başkasına ait kredi kartı borcunun ödenmesi, kredi kartından nakit avans çekme, kredi kartı ekstrelerinin e-mail yoluyla gönderilmesi), döviz alım- satımı, kurların takibi, yatırım gerçekleştirme (repo, otomatik repo, devlet tahvili- hazine bonosu alım-satımı, yatırım fonu alım-satımı, yabancı yatırım fonu işlemleri, fon alım-satım emir takibi), hisse senedi işlemleri (hisse senedi fiyatlarının görüntülenmesi, hisse senedi alım-satımı, hisse senedi emir bölme- iyileştirme, lot altı alım-satım, alım satım emir takibi, halka arz işlemleri için talep toplanması), hesap açma işlemleri (vadesiz döviz hesabı açma, vadeli hesap açma- kapama vadeli hesaptan para transferi yapma), ileri vadeli para transferleri (ileri vadeli EFT emri, ileri vadeli havale emri, ileri vadeli işlemler güncelleme- iptal), talimat verme işlemleri (fatura talimatı, SMS, e-mail, posta talimatı– döviz kurları, repo oranları), sık yapılan transfer bilgileri, isme havale hesabı ekleme, hesaba havale hesabı ekleme, EFT hesabı ekleme olarak sayılabilmektedir.

1.6.3. İnternet Bankacılığının Müşterilerine Sağladığı Olanaklar

İnternet bankacılığı, müşterilerine, internet erişimi olan herhangi bir bilgisayar üzerinden yılın 365 günü, günün 24 saati işlem yapabilme olanağı sağlamaktadır. Evden, işyerinden veya o an için bulunulan mekandan dışarı çıkmadan, bilgisayar başında, para çekme dışındaki tüm bankacılık işlemleri bu sistem sayesinde yapılabilmektedir. Şubeden yapılan işlemlerin ortalama maliyeti yüksekken, maliyetin yüksekliği bakımından telefon bankacılığı, ATM'den yapılan işlemler gelmekte ve bunu en düşük maliyet olarak internet bankacılığı izlemektedir. İnternet bankacılığı, bir banka müşterisinin mümkün olan en kısa sürede, en kolay şekilde ve en ekonomik işlem yapabilmesine imkan tanımaktadır. İnternet üzerinden yapılabilen, para çekme dışındaki tüm işlemlere göz atmakta fayda bulunmaktadır.

Bunlar :

- Hesap Açılışları (vadeli, vadesiz, yatırım, vb.)

- Para Transferleri (havale, eft, otomatik havale talimatları)
- Yatırım İşlemleri (repo, yatırım fonu, hisse senedi, döviz, hazine bonosu gibi menkul kıymetlerin alımı ve satımı)
- Ödeme İşlemleri (fatura, vergi, trafik, üniversite harç, vb. ödemeler)
- Kredi Kartı İşlemleri (her türlü kredi kartı borç ödemeleri)
- Başvuru İşlemleri (hesap açma, kredi kartı istemi, otomatik ödeme talimatı verme, vb.)
- Bilgi Hizmetleri (hesaplarınızla ilgili anlık ve geriye yönelik tüm bilgiler)

olarak sıralanabilmektedir.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ E- Bankacılığı kavrayınız.	➢ E-Bankacılığın tanımını yapınız. ➢ E- Ticareti araştırınız ➢ Diğer elektronik uygulamaları araştırınız
➢ Bankacılığın fonksiyonlarını sıralayınız.	➢ Bankaların görevleri hakkında bilgi toplayınız. ➢ Günlük hayatımızda bankaları niçin ne kadar kullandığını Araştırınız. ➢ Objektif değerlendirmeler yapınız.
➢ E-Bankacılığın olumlu ve olumsuz yönlerini sıralayınız.	➢ E-Bankacılıkta temel öğeleri araştırınız ➢ E- Bankacılığı kullanan kişi ve kurumlardan olumlu ve olumsuz geri bildirimler toplayınız. E-bankacılığa geçişle kişilerin yaşamları nasıl değişmiştir açıklayınız.
➢ Bankaların E-Bankacılığı kullanma nedenlerini tespit ediniz	➢ E-Bankacılık nasıl ortaya çıkmıştır araştırınız. ➢ Türkiye'deki E-bankacılık uygulamalarını diğer ülkelerle karşılaştırınız.
➢ WAP bankacılığını kavrayınız	➢ WAP bankacılığını kullanımını e- bankacılıkla karşılaştırınız. ➢ İnternetin Bankacılığa katkısını açıklayınız?

ÖLÇME VE DEĞERLENDİRME

A. OBJEKTİF TESTLER

1. Aşağıdakilerden hangisi e-bankacılığı açıklar?
   A) Sosyal bankacılık
   B) Bireysel Bankacılık
   C) Ticari bankacılık.
   D) İnterten bankacılığı

2. Aşağıdakilerden hangisi internet bankacılığı kullanımının olumsuz yönlerinden biridir.
   A) Büyük miktarda yatırım gerektirir
   B) İşlem maliyeti düşüktür
   C) İstenilen zamanda kullanılabilir
   D) Kolay ve rahattır.

3. E-Bankacılıkta müşteri kendi portföyünü kaçınca adımda yönetir
   A) 1. Adım
   B) 2. Adım
   C) 3. Adım
4. 4. Adım

5. E-Ticarette kullanılan şirket içi ağlara ne denir
   A) İntranet
   B) Ekstranet
   C) E-Bankacılık
   D) E-Ticaret

6. E-Bankacılık da daha kısa zamanda daha fazla işlem yapılır.
   Doğru ( ) Yanlış ( )
7. E-Bankacılığı sadece ülke sınırları içinde kullanabiliriz.
   Doğru ( ) Yanlış ( )
8. İlk etkin bilgisayar kullanımı, ilk network kurulumu, ilk parasal bilgi transferi doğru ve yaygın olarak bankalar tarafından yapılmıştır".
   Doğru ( ) Yanlış ( )

DEĞERLENDİRME

Cevaplarınızı modülün sonundaki cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete geri dönerek tekrar inceleyiniz

Tüm sorulara doğru cevap verdiyseniz diğer faaliyete geçiniz.

B. PERFORMANS TESTİ

Modül ile kazandığınız yeterliği aşağıdaki ölçütlere göre değerlendiriniz.

DEĞERLENDİRME ÖLÇÜTLERİ	Evet	Hayir
E-Bankacılığı açıklayabilir misiniz?		
E-Bankacılığa geçiş sürecini açıklayabilir misiniz?		
E-Bankacılık adımlarını açıklayabilir misiniz?		
ABD ve Avrupa Birliği'nde e-bankacılık sistemini genel hatlarıyla anlatabilir misiniz?		
E-Bankacılığın dünyada ki gelişimini açıklayabilir misiniz?		
Bankaların E-Bankacılığa geçiş dönemini açıklayabilir misiniz?		
E-Bankacılığın müşterilere sağladığı olanakları açıklayabilir misiniz?		

DEĞERLENDİRME

Yapılan değerlendirme sonunda hayır cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız öğrenme faaliyeti 1'i gözden geçiriniz. Cevaplarınızın tamamı evetse bir sonraki öğrenme faaliyetine geçiniz.

ÖĞRENME FAALİYETİ–2

AMAÇ

Güvenli Elektronik bankacılık kullanımını gerçekleştirebileceksiniz

ARAŞTIRMA

Sevgili öğrenci, bu faaliyet öncesinde yapmanız gereken öncelikli araştırmalar şunlar olmalıdır:

- Bir bankanın internet sitesini verdiği hizmetler açısından inceleyiniz?
- E-Bankacılıkla ilgili yaşanmış güvenlik problemlerini araştırınız?
- E-Bankacılığın güvenli kullanımı için alınması gereken önlemleri araştırınız

Yaptığınız araştırmaların sonuçlarını arkadaş gurubunuz ile paylaşınız.

2. İNTERNET BANKACILIĞI KULLANIMININ ETKİNLİĞİ VE GÜVENLİK

İnsanoğlunun daima hızlı bir değişim içinde bulunduğu, çağlar boyunca görülmüş ve kendi doğası içinde hep yeni şeyler arayışını doğurmuştur. İnsanoğlunun eski alışkanlıklarını bıraktığı ve hızla çağa ayak uydurmuş olduğu günümüzde, bunu en güzel yansıtan şey ise şüphesiz ki internettir.

2.1. İnternet Bankacılığı Kullanımının Etkinliği

İnternet bankacılığı, bankacılık hizmetlerinin internet üzerinden sunulduğu bir alternatif dağıtım kanalıdır. Türkiye'de bugün internet bankacılığı, herhangi bir banka şubesinin sağlayacağı hizmetlerin hemen hepsinden, dünyanın neresinde olunursa olunsun, zaman ve mekandan bağımsız olarak çabuk ve kolayca yararlanmayı sağlamaktadır. İnternet bankacılığı 24 saat, internet erişimine sahip herhangi bir bilgisayar aracılığıyla dünyanın her yerinden kullanılabilmektedir. İnternet bankacılığının sağladığı faydalar şöyle özetlenebilmektedir:

- Bankacılık işlemleri, hızlı ve kesintisiz yapılabilmektedir.
- Bankacılık işlemleri, şubeye gitmeden, sıra beklemeden kolayca yapılabilmektedir.
- Bankacılık işlemi, görerek ve seçerek yapılabilmektedir.
- Detaylı rapor ve bilgi alınabilmektedir.
- Çok çeşitli bankacılık ürünlerini görerek bu ürünlerden yararlanılabilmektedir.
- Bankacılık işlemleri çok daha ucuza yapılabilmektedir.
- İşlemlerin banka personeli tarafından dahi görülememesi nedeniyle, bankacılık işlemleri gizli ve güvenli olarak gerçekleşebilmektedir..

İnternet bankacılığı ile yapılan işlemlerin müşterilere sağladığı kolaylık ve avantajlar bankalar için de verimlilik ve maliyet tasarrufu sağlamaktadır.

Eskiden bir banka işlemi için saatlerce beklenirken artık bu gibi işlemler saniyelerle ifade edilebilen bir hıza ulaşmış durumda veya saatlerce dolaşılıp alınan bir hediye web sayfalarından anında alınabilmektedir. Bu ve benzeri güzelliklerini gördüğümüz internetin ne yazık ki kullanıcı tabanlı olarak kötü yanları da bulunmaktadır.

Resim 2.1: Bankanızdan güvenlik isteyiniz

Günümüzde internet kullanıcılarının % 80 gibi bir kısmının artık olmazsa olmazlarından olan e-posta, internet bankacılığı, e-alışveriş gibi birçok kullanım alanları kötü niyetli internet kullanıcıları tarafından istismar edilmektedir. Güvenlikle ilgili endişeler internet bankacılığının gelişmesini yavaşlatan temel nedenler arasında yer almaktadır. Güvenlik endişenin artması internet bankacılığı kullanımını azaltmaktadır.

İnternet bankacılığında güvenlik konusunu beş düzeyde incelemek mümkündür. Bunlar:

- Kullanıcı düzeyi: İnternet bankacılığının güvenliğini sağlayacak en önemli unsur kişilere özel olarak verilen kullanıcı adı ve şifrelerdir. İnternet bankacılığı kullanıcısı kesinlikle kullanıcı adı ve şifresinin bir başkası tarafından öğrenilmesi ve kullanılmasının önüne geçmelidir.

- Online bankacılık programı düzeyi: Bu programlar banka ile internet kullanıcısının bilgisayarı arasında gidip gelen bilgiyi korumaktadır. İnternet bankacılığı hizmeti veren bankalar, ana bilgisayar sistemlerini korumak için internet kullanıcılarının ana bilgisayara doğrudan erişimini engellemektedirler. Bunun yerine sadece bu iş için adanmış server adı verilen bilgisayarları kullanmaktadırlar. Bu bilgisayarlar aynı zamanda "firewall" adı verilen ve yalnızca güvenlik amacıyla kullanılan bilgisayarların görevlerini yerine getirmektedirler. Kullanıcıya ait olan tüm bilgiler dolaşıma çıkmadan önce SSL yöntemi ile şifrelenmektedir.
- Devlet düzeyi: Devlet, bankalarla ilgili olarak mali yapılarının güçlü olup olmadığı ve operasyonlarının güvenli bir şekilde yapılıp yapılmadığı hakkında denetlemeler ve düzenlemeler yapmaktadır. Devletin internet bankacılığı konusundaki tutumu gerek bankalar gerekse internet bankacılığı kullanıcıları açısından önem arz etmektedir. Finansal hizmetler ülkenin kritik altyapıları olarak görülmekte ve bu hizmetlerin ekonominin düzgün çalışmasını engelleyecek her türlü saldırıdan korunması gerektiği önemli bir gerçektir.
- Bankanın bilgisayar sistemleri ile ilgi tedbirler: Bankalar bilgisayar sistemlerini güven altına almak için yüksek tutarlarda harcamalar yapmakta ve sistemin güvenliğini sağlamak için güvenlik politikaları geliştirmektedirler. Bu politikalar banka bilgi ağının hangi şartlarda dış sistemlere açılıp açılmayacağını detaylı olarak düzenlemektedir. Bankaların bu noktada kullandıkları araçlardan en önemlisi "firewall"lardır. Firewall'lar kendilerini sistem güvenliğine adamış bilgisayarlardır. Bunların çalışma prensibini kısa bir örnekle anlatmakta yarar vardır.
- İnternet bankacılığı hizmetini kullanan bir kimse banka hesaplarının bakiyesini almak istediğinde bu bilgi öncelikle firewall adı verilen bilgisayara gelmektedir. Firewall kişinin şifrelerini kullanarak kim olduğunu belirledikten sonra ana bilgisayara bağlanarak yalnızca talep edilen bu bilgiyi almakta ve kişiye ulaştırılmasına aracılık etmektedir. Kişinin doğrudan ana bilgisayara bağlanması mümkün olmamaktadır. Oluşturulan bu güvenlik yapısına teknik olarak "proxy- based firewall" denilmektedir.
- Bilgisayar dışındaki temel banka güvenlik tedbirleri: Güvenlik, bankacılıkta diğer işletmelerden farklı olarak bankacılık kültürünün bir parçasıdır ve banka operasyonlarının her aşamasında gündeme gelmektedir. Bankanın bilgisayar sistemlerine saldırılar sürekli artmaktadır. Bankalar sistemlerinin dışında sistemlerin bulunduğu mekanları da kartlı giriş, video kamera gibi önlemlerle sürekli olarak korumaktadırlar.

Resim 2.2: Küçük ama sorumluluğu büyük

Bu aşamalardaki önlemlerin başarılı olması halinde internet bankacılığı güvenliğinin sağlanabileceği düşünülmektedir. Ortaya çıktığı ilk zamanlarda sadece temel seviyede dosya transferi ve web sayfaları yayınlama aracı olarak kullanılan internet artık birçok değişik uygulama için temel bir alan haline gelmiş durumdadır.

Bununla birlikte farklı araçlarla yürütülen birçok hizmet internet üzerine taşınarak daha zengin bir içeriğe kavuşturulmaktadır.

Şu anda üzerinde en çok tartışılan ve sürekli yenilenen internet hizmetlerinin başında e-ticaret ve e-devlet uygulamaları gelmektedir. İçinde bulunulan koşullarda ticaretin hemen her alanda "gelişme" ve "ilerleme" için temel dinamik olarak değerlendirildiği göz önüne alınırsa internet de yaşanılan "gerçek" dünyadan bağımsız olmadığı için bu ilerlemeden gerekli payı almaktadır.

İnternet, yapısı gereği farklı ortamlardaki bilgisayarların birbirleriyle serbestçe iletişim kurabilecekleri açık bir sistem olduğu için güvenlik kontrolleri özel bir anlam taşımaktadır. Teknolojinin gelişme hızına paralel olarak güvenlik önlemlerinin sürekli güncel tutulması gerekmektedir. İnternet bankacılığı hizmeti verilirken öncelikle kullanılan yazılım, donanım ve network altyapısının güvenliğinin sağlanması hedeflenmektedir. Bu doğrultuda bankaların internet bağlantıları dış saldırılara karşı güvenlik duvarlarıyla korunmaktadır. Standart önlemlere ek olarak, olası saldırıların tespit edilmesi ve engellenmesi için kurulan sistemler, güncel olarak izlenmektedir ve yeni saldırı tiplerine karşı sürekli geliştirilmektedir.

Eğer internet üzerinden yapılan ticari işlemlerde güvenlik açıkları çok sık yaşanırsa kullanıcıların internetten yaptıkları işlemleri iptal etme yolu ve bir daha da kolay kolay internette bu tür işlemler yapmayacakları kesindir. Konunun bu kadar önemli olmasından dolayı her sene çeşitli firmalar güvenlik üzerine araştırmalar hazırlayıp yayınlamaktadır. Ülkemizde diğerlerine göre daha yoğun bir şekilde kullanılan e-ticaret uygulamaları olan internet bankacılığı ve kredi kartları ile internet üzerinden gerçekleştirilen alışverişler güvenlik konusunda daha öncelikli bir konuma sahiptir.

Yayınlanan bir araştırmaya göre Türkiye'deki şirketlerin yüzde 27'sinin bilişim sistemlerinde çok yüksek seviyede güvenlik açıkları olduğu değerlendirilmesi yapılmıştır. Daha pratik bir ifadeyle "Şirketlerin yüzde 48'inin web sunucu bilgilerinin kolaylıkla çalınabileceği, ana sayfalarının değiştirilebileceği veya bir başka adrese yönlendirilebileceği tespit edilirken, şirketlerin yüzde 29'unda isim çözmek için kullanılan DNS (Domain Name System) sunucularındaki açıklar nedeniyle, şirket e-postalarının ele geçirilmesi ve çalışanların internet üzerinden erişmiş oldukları bankacılık gibi işlemlerde kullandıkları şifrelerin çalınması riski saptandı" denilmektedir. Özellikle son dönemlerde e-posta adreslerine gönderilen ve müşteriyi banka bilgilerini güncellemeye çağıran aldatıcı mesajların varlığı göz önüne alınırsa konunun önemi daha iyi anlaşılacaktır

2.2. İnternet Bankacılığında Karşılaşılan Sorunlar

Klasik şube bankacılığının maliyeti, işlem başına telefon bankacılığına göre daha yüksek maliyetli, telefon bankacılığı ise internet bankacılığına göre daha yüksek maliyetli olmakta ve dolayısıyla teknoloji yoğun bankalar, bankacılık işlemlerinin maliyetlerini azaltmak için alternatif bankacılık kanallarını cazip hale getirmeye özen göstermektedirler. Buna örnek olarak ülkemizde şubeye giderek EFT yapmak belirli bir maliyet getirirken, internet bankacılığı ile yapılan EFT işlemlerinden ücret alınmamaktadır.

Alternatif bankacılık kanalları deyince her ne kadar aklımıza en çok kullanılan iki kanal olan internet bankacılığı ve telefon bankacılığı gelse de, cep telefonu (WAP/GPRS) bankacılığı ve el bilgisayarı (Palm) bankacılığı da diğer alternatif bankacılık kanallarını oluşturmaktadır.

Resim 2.3: Sorunlarınızı az maliyetle kısa zamanda çözün

Bahsedilen tüm faydalarına rağmen alternatif kanalların kullanımının karşısında bazı engeller bulunmaktadır. Müşteriler çeşitli medya alanlarında, ayrıntılarını tam olarak bilemedikleri birçok internet yolsuzluğu, dolandırıcılığı ve hırsızlığı haberleri ile karşılaşmaktadırlar. Bunlara ilave olarak insanlarla yüz yüze işlem yapmaya alışmış kişiler, karşılarında makineler, bilgisayarlar olunca rahat hareket edememekte, hata yapmaktan korkmaktadırlar. Bu nedenle alternatif kanalları kullanmak konusunda biraz tereddütlü davranmaktadırlar.

Bankalar bu engelleri kaldırmak, alternatif bankacılığı özendirmek için her ne kadar ellerinden geleni yapsalar da, bazen varolan tedbirlerin yetersizliği, bazen de yanlış inanışlar, alternatif kanallardan beklenen kullanım artışının gerçekleşmesini engellemektedir.

Özellikle internet ve telefon bankacılığının karşı karşıya kaldığı sorunlar, engeller ve bunlara ilişkin alınabilecek tedbirlerden bahsetmek gerekirse, en temel engel güvenlik konularından kaynaklanan sorunlardır. Bu sorunları şu şekilde sıralamak mümkündür:

- Müşteri, karşısındaki web sitesinin gerçekten banka olup olmadığına emin olmayabilmektedir. Kendisini banka olarak ilan eden web sitesi, gerçekte o banka olmayıp banka ile ilgisi olmayan kişilerin oluşturduğu, bankanın web sitesine benzer bir şekilde tasarlanmış bir site olabilmektedir. Bu site, sadece kullanıcının ismi, şifresini kayıt eden ve sonra bir hata mesajı göstererek kullanıcıyı aldatan bir mekanizmadan ibaret olabilmektedir. Böylelikle bu sahte banka sitesi, kullanıcının giriş bilgilerine (kullanıcı ismi ve şifresine) sahip olabilmektedir.
- Banka, müşterisinin kimliğinin doğruluğu konusunda şüpheye düşebilmektedir. Bankaya kendisini banka müşterisi bay x olarak tanıtan kişi, aslında bir banka müşterisinin bilgilerini almış bir başka kişi olabilmektedir.

- Kullanıcılar yaptıkları bankacılık işlemlerini sonradan inkar edebilmekte, yapmadıklarını, bilmediklerini, başka birilerinin bu işlemleri kendilerinden habersiz yaptıklarını iddia edebilmektedirler. Örneğin internet üzerinden hisse senedi alım emri veren bir müşteri iki saat sonra aldığı hisse senedinin fiyatının düşmesi üzerine bankayı arayıp şifresinin çalındığını bildirebilmekte ve daha sonra, önceden yapılan işlemin kendisi tarafından gerçekleştirmediğini iddia edebilmektedir.
- Banka ile kullanıcı bilgisayarları arasında kurulan iletişim dinlenerek içeriğinde bulunan şifre, hesap no, kredi kartı bilgileri gibi hassas bilgiler başkaları tarafından elde edilebilmektedir.
- Kullanıcıların internet bankacılığı yaparken kullandıkları kişisel bilgisayarlar yeterince güvenli olmayabilmektedir. İnternet'ten gerek e-posta yoluyla, gerek indirilen programların bilgisayarlara yüklenmesiyle, virüs, truva atı gibi zararlı programlarla sürekli karşı karşıya kalınabilmektedir. Örneğin, kullanıcıların bilgisayarlarına yerleştirilebilecek (e-posta içine saklamak ya da bir oyun, ekran koruyucu içine gizlice yerleştirmek yoluyla) bir tuş kayıt edici program (keylogger) veya ekran kaydedici program (screenlogger) ile kullanıcılar iyi şifreler kullansalar dahi şifreleri kayıt edilebilmekte ve/veya sonradan öğrenilebilmektedir.

Sorunların ardından bu sorunların çözümü için bankaların aldıkları teknik önlemleri anlatmak gerekmektedir. Bu problemlerin tümünü, şifreleme ve hemen hemen 20 yıla yakın bir süredir bilinen açık anahtar altyapısı (Public Key Infrastructure-PKI) sayesinde çözmek mümkündür. Teknolojinin kullanımının pratik hale getirilememesi, bu çözümlerin bir kısmının günümüzde bile halen yaygınlaşmamasına sebep vermektedir. Fakat son yıllarda bu altyapının kullanımına imkan veren, hatta birkaç çözümü beraberinde barındıran uygulamalar piyasaya sürülmüş bulunmaktadır.

Resim 2.4: Tedbiri elden bırakmayın

Açık Anahtar Altyapısı (AAA) yüksek düzeyde güvenlik gerektiren uygulamaları koruyarak elektronik bankacılık ve ticaret, web tabanlı iş süreçlerinin otomasyonu, sayısal form imzalama gibi operasyonların gerçekleşmesini olanaklı kılar.

Açık anahtar altyapısı, açık anahtar şifreleme (public key cryptography) mimarisini kullanarak, kişi ve kurumların kimliğini tanımlayabilme, elektronik imza atabilme, yapılan işlerin inkar edilememesinin sağlanması, ve bilgilerin şifrelenerek saklanması, korunması gibi özellikleri kullanmaya imkan vermektedir. Açık anahtar şifreleme mimarisinde kişi ve kurumlar açık (public key) ve gizli (private key) olmak üzere iki anahtara sahiptirler. Açık anahtar tüm dünyaya ilan edilebilmekte ve dağıtılabilmekte iken, gizli anahtar çok dikkatli bir şekilde saklanmalıdır. Bu mimari basitçe şu şekilde çalışmaktadır: Herhangi bir bilgi, bilginin adresleneceği kişinin açık anahtarı ile bir grup matematik işlemden geçirilerek şifrelenmekte ve kişiye gönderilmektedir. Bu şifrelenmiş bilgiyi dünyada sadece kullanılan açık anahtarın diğer parçası olan gizli anahtar deşifre edebilmekte, dolayısıyla sadece gizli anahtara sahip olan kişi bu bilgiyi okuyabilmektedir.

AAA, asimetrik gizli şifreleme (kriptografi) özelliğini kullanan bir açık anahtar teknik altyapısıdır. Kripto anahtarları kullanan bu alt yapı; karmaşaya meydan vermeyecek kadar anlaması kolay, basit bir işleve sahiptir.

Kişilerin bankacılık sistemlerine ulaşmak için kullandıkları şifrelerin genellikle zayıf olma eğiliminde olduğunun üzerinde durmak gerekmektedir. Bahse konu şifreleri kuvvetli hale getiren teknolojilerin en başında tek kullanımlık şifre jeneratörü (OTP üreticisi- one-time-password generator) denilen, bir sefer kullanılabilen şifreler üreten cihazlar gelmektedir (Örneğin RSA SecureID, Encotone TeleID gibi). Bu kredi kartı büyüklüğündeki cihazlar hem kendilerinin bildikleri, hem de sunucu tarafından da bilinen bir algoritma sayesinde kullanıcının numarası, tarih ve zamanın bir fonksiyonu olan bir kerelik bir şifre üretmektedirler. Sunucu, bildiği sırrı kullanıcının sunduğu kullanıcı adı ve zaman sayesinde aynı şifreyi hesaplayabilmekte ve kullanıcının sunduğu şifrenin doğruluğu ile kişinin sisteme olan giriş iznine karar verebilmektedir.

OTP üretici cihazlar iki farklı tipte olmaktadır. Bunlardan donanım tipi olanlar, her türlü gerekli aparatı (tuş takımı, ekran gibi) üzerinde taşımakta ve bağımsız olarak çalışabilmektedirler. Örneğin internet bankacılığı hizmetini kullanacak müşteri, web sitesine gidecek kullanıcı adını girmekte ve OTP cihazını kullanarak o sefer kullanacağı şifreyi üretmekte, OTP'nin ekranında gördüğü bu şifreyi web sitesinin şifre bölümüne yazmakta ve bankacılık işlemlerini kullanmaya başlamaktadır. Bu şifreyi çalan bir kişi aynı şifreyi kullanmayı denediğinde ise sunucu, şifre bir seferlik olduğundan ve kullanıldığından dolayı onu reddetmektedir. Donanım tipi OTP cihazlarından başka diğer bir tip ise yazılım tipi olanlardır. Fakat yazılım tipi olanlar kullanıcının bilgisayarında çalışan bir bilgisayar kodu olduğundan bilgisayarın klavye ve görüntü imkanlarını kullanmaktadır ve beklenen güvenlik sağlanamaya bilinmektedir.

Kişilerin yaptıklarını inkar edebilmelerine karşı da alınabilecek önlemler bulunmaktadır. Yine açık anahtar mimarisinin sağladığı elektronik imza atabilme imkanı sayesinde, kişiler yaptıkları işlerin altına aynı gerçek imza atarmış gibi elektronik imza atabilmektedir. Böylece bankalar kişilerin verdiği bankacılık emirleri ile birlikte verdikleri emirlere ilişkin imzaları sistemde saklayabilmekte, kişilerin yaptıklarını inkar etmelerini önleyebilmektedirler.

Günümüzde artık internet bankacılığı problemlerini çözebilen hem elektronik imza atabilen, hem bir sefer kullanılabilecek şifre üretebilen, hem akustik hem görsel olarak çalışan ürünler ortaya çıkmaktadır.

Alternatif kanalları cazip hale getirmek bankalar açısından maliyetleri azaltmakta ve rekabet avantajının artırmaktadır. Kullanıcıların bir kısmında var olan hatalı inanışları ortadan kaldırmak, kişilerin sistemlere olan güvenlerini artırmak, kullanımı özendirmek için bankalar çeşitli etkin, kolay, basit çözümlere yatırım yapmalı, bunları kullanıcılarına sunmalı ve kullanıcıları bu konularda bilinçlendirerek eğitmelidir.

Bankalar son zamanlarda, sms şifreleme sistemi ile yeni bir güvenlik sistemi geliştirmişlerdir. Bu sistemde, siz işleminizi yapmadan hemen önce cep telefonunuza bir şifre gönderilmekte ve bunu girerek işleminizi bitirmeniz istenmektedir. Bu da önemli bir güvenlik arttırıcı sistem olarak görülebilir.

2.3. İnternet Bankacılığı Kullanımında Dikkat Edilecek Hususlar

İnternet bankacılığının sağladığı yararların yanında kullanımının beraberinde getirdiği bir takım riskler de söz konusudur. Önemli bir işleve sahip olan internet bankacılığı işlemlerinde, olası dolandırıcılık eylemlerine karşı bilgi işlem güvenliğine özel bir önem verilmektedir. Bu çerçevede; kullanıcıların bilgilendirilmesi açısından güvenlik için aşağıdaki hususlara dikkat edilmelidir:

Resim 15: Yalnız değilsiniz

- Kimlik ve kişisel finansal bilgilerinizi isteyen e-postalar konusunda dikkatli olunmalıdır.
- Kişisel bilgilerin talep edildiği bu tür e-postalar kesinlikle doldurulmamalıdır.
- Kişisel bilgiler, şifre, vesaire mutlaka ekran klavyesi kullanılarak girilmelidir.
- Bankalar tarafından verilen müşteri numarası, parola ve şifre bilgilerinin üçüncü şahıslarla kesinlikle paylaşılmaması gerekmektedir.
- Banka ve ticari kurumlardan gelmiş gibi gösterilen ve şifre, kullanıcı adı, müşteri numarası, kredi kartı numarası, kimlik numarası gibi bilgileri talep eden e-postalara itibar edilmemelidir.
- 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 yönlendirilen linklere girilmemelidir.
- Kredi kartının kullanıldığı ya da kişisel bilgilerin girildiği bilgisayarın güvenli olmasına dikkat edilmelidir (Kullanılan web sitesi http:// yerine https:// olmalıdır).
- Phishing web sitesi sahtekarlıklarına karşı uyarılmak için bilgisayara İnternet'ten uyarıcı bir web tarayıcısı yüklenebilmektedir. (http://www.earthlink.net/earthlinktoolbar İnternet'ten ücretsiz olarak yüklenebilen bir tarayıcıdır).
- Düzenli olarak çevrimiçi hesaplar kontrol edilmelidir.
- Her hesap numaranız için farklı bir şifre belirlenmelidir.
- Hesap numarasının ve kimlik numarasının yazılı olduğu materyalleri saklamamak gerekir. Bu materyaller derhal yok edilmelidir.
- Banka hesabı, kredi kartları ve banka kartlarının ekstreleri düzenli bir şekilde kontrol edilmelidir, şüpheli görülen durumlarda banka ile irtibata geçilmelidir.
- Kullanılan internet tarayıcısının güncel olmasına ve tüm güvenlik ayarlarının yüklenmesine dikkat edilmelidir. Microsoft Internet Explorer kullanılıyorsa, Microsoft Security ana sayfasından http://www.microsoft.com/security/'den konu ile ilgili özel güvenlik ayarları yüklenebilmektedir.
- Bilgisayarda güncel bir virüs koruma programı olmasına dikkat edilmelidir.
- Güvenlik duvarı (firewall) kullanımı güvenliği artıracaktır.
- İnternet bankacılık işlemleri güvenliğinden emin olunmayan bilgisayarlardan yapılmamalıdır. Bu amaçla internet cafe gibi umuma açık yerlerdeki bilgisayarların kullanılmaması tavsiye edilmektedir.

2.4. İnternet Ortamında Gerçekleştirilen Saldırıla

Günümüzde internet kullanıcılarının en büyük risklerinden bir tanesi sanal ortamda oluşan dolandırıcılıklar ve bu dolandırıcılıkların gerçekleştirilmesi için yapılan saldırılardır. Daha çok hacker adı verilen internet korsanları tardafından gerçekleştirilen bu saldırılar, önlem alınmadığı taktirde büyük sıkıntılara neden olabilmektedir. Bu saldırıların en önemlileri; olta saldırıları (phishing), e-posta yöntemi, tuş kaydedici (keylogger) ve ekran kaydedici (screenlogger) yöntemidir.

Uygulamada banka müşterileri, internet bankacılığını kullanırken risklerden korunmak için bilgisayarlarının güvenliklerini sağlamaları gerekmektedir. Güncel virüs programlarının kullanılması, güvenlik duvarı kullanımı, internet tarayıcısının güncelleştirilmesi ve güvenlik ayarlarının yüklenmesi, kullanıcı adı ve şifrenin düzenli aralıklarla değiştirilmesi, her bir hesap için farklı kullanıcı adı ve şifre kullanılması saldırılara karşı alınacak basit önlemleri oluşturmaktadır.

Resim 2.6: Saldırıların boyutu değişti

2.4.1.Olta (Phishing) Saldırıları

İnternet dünyasındaki kolaylıkların yanında dolandırıcıların da bulunduğunu unutmamak gerekir. Phishing de bu dolandırıcılık tiplerinden sadece bir tanesidir. "Phishing" terimi üç farklı kelimenin birleşmesinden ortaya çıkmaktadır. Password Harvesting'in (yani şifre toplama) baş harfleri ile fishing (balık tutma) kelimesinin birleşmesinden "phising" kelimesi ortaya çıkmaktadır.

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 verilmemelidir veya istenen bilgiler girilmemelidir. Bankalar, e-posta yoluyla hiç bir şekilde şifre işlemleri yaptırmamakta, müşterilerin gizli kişisel bilgilerini istememektedir. İşte özellikle ülkemizde şu günlerde bu şekil istismarların başında gelen olay ise: "phishing" yani kısaca hesabın bulunduğu bankanın, e-posta adresi veya bunun gibi bilgi girmeyi gerektiren bir kuruluşun web sayfasının bir kopyasını yapıp kullanıcının hesap bilgilerini çalmayı amaçlayan bir İnternet dolandırıcılığıdır. Olta atıldığında en azından bir balık yakalana bilineceği düşüncesinden esinlenerek oluşturulmuş ve uygulanmaktadır.

Örneğin kullanılan elektronik posta servisinin giriş ekranının bir kopyası elektronik posta olarak gelmekte ve bir şekilde kullanıcı adının ve şifrenin girilmesini istemektedir. Dikkatsiz bir şekilde bilgiler verildiğinde, sayfanın içine gizlenmiş bir kod parçası kullanıcı adını ve şifreyi dolandırıcılara göndermektedir.

Resim 2.7: Dikkat! Karşınızda biri var

Bu dolandırıcılık saldırılarından korunmak için ayrıca şu noktalara dikkat edilmelidir:

- Gönderilen e-posta'nın kimden geldiğinden ve doğruluğundan mutlaka emin olmak gerekmektedir.
- Bilinmeyen kişi ya da kurumlardan gönderilen e-postaların içerisinde bulunan linkleri tıklamamak, ekleri bilgisayara yüklememek gerekmektedir.
- Elektronik posta aracılığıyla veya başka bir ortamda sunulan web sayfa linklerini kullanmamak gerekmektedir.
- Erişmek istenilen web sayfasının adresini tarayıcının adres satırına bizzat yazmak gerekmektedir.
- Sadece sayılardan oluşan web adresi ile karşılaşılırsa dikkatli olmak gerekmektedir. Çoğu kurum ya da kuruluş web adresi olarak isim kullanmaktadır. Çoğu gerçek web sitesinin adres satırında sayılar yerine kurum ismi yer almaktadır.

2.4.1.1. Olta Saldırılarının İnternet Bankacılığı Kullanıcılarına Verdiği Zararlar

Phishing yöntemi kullanarak bilgisayar kullanıcılarını tuzaklarına düşüren dolandırıcılar özellikle aşağıda belirtilenleri çalmak suretiyle internet bankacılığı kullanıcılarına zarar vermektedir. Olta saldırılarını düzenleyenlerin çaldıklarını aşağıdaki gibi sıralamak mümkündür:

- Kredi, Debit/ATM Kart Numaraları/ CVV2
- Şifreler ve Parolalar
- Hesap Numaraları
- İnternet Bankacılığına Girişte Kullanılan Kullanıcı Kodu ve Şifreleri

2.4.1.2. Olta Saldırılarının İşleyişi

Phishing ile dolandırıcılar internet kullanıcılarını sahte e-posta yöntemi ile ağlarına düşürmeyi denemekte ve kullanıcıları bilgilerini almaktadırlar. Kullanıcı bilgileri, sisteme giriş için gereken her türlü şifre, kullanıcı adları ve parolaları kapsamaktadır.

2.4.1.3. Olta Saldırılarından Korunma Yolları

Unutulmaması gereken nokta her türlü online dolandırıcılık, sahtekarlık ve virüslere karşı en büyük korunma aracı, bu konuda bilinçli ve bilgili olmaktır. İnternette güvenli alışveriş yapmanın en önemli koşulu budur.

- E-posta adresine gelen mesajların doğruluğu ispatlanmalıdır. Bilinmeyen kimselerden gelen mesajlar silmek, asla cevap vermemek gerekmektedir. "Aşağıdaki bağlantıya tıklayın" gibi e-posta isteklerine asla cevap vermemek gerekmektedir.

➢ İşlemleri online yapılırken, işlem yapılan web sayfasının güvenli olup olmadığı mutlaka kontrol etmek gerekmektedir. İnternet tarayıcısının üst kısmında bulunan adres bölümünde bulunan adresin "https://" olup olmadığını kontrol etmek gerekmektedir. "https://"'in sonunda bulunan "s" harfi bu sayfanın güvenli ve çeşitli şifreleme metotları ile işlem yaptırdığını belirtmektedir. Ek olarak, internet tarayıcısının sağ alt kısmında yer alan kapalı kilit işareti, yine güvenli ve şifrelenmiş bir sayfada işlem yapıldığını göstermektedir.

Şekil 2.1. İnternet sayfasının güvenliğini gösteren kilit işareti

Bu işaret sayfanın SSL ile şifrelendiğini ve sitenin gerçekten çalışılankuruluşa ait olup olmadığını göstermektedir, üzerine iki kez tıklandığında ise; aşağıdaki örnekte görüldüğü gibi bir mesaj çıkacaktır.

ÖRNEK:

"Issued to: www.abidayibank.com.tr ve "Issued by: www.verisign.com/CPS Incorp.by Ref.LIABILITY LTD.(c)97 VeriSign" bilgileri kontrol etmek gerekmektedir.

➢ İnternet adresi olarak sayısal rakamlar içeren adresler ile karşılaşılırsa kullanmadan önce mutlaka kontrol etmek gerekmektedir.

➢ Ziyaret edilen web sitelerinde; adresler çoğunlukla adres kısmı, ardından firmanın ve şirketin ismine ek olarak, com, org, net gibi uzantılar ile bitmektedir. Örneğin; https://www.abidayibank.com.tr.

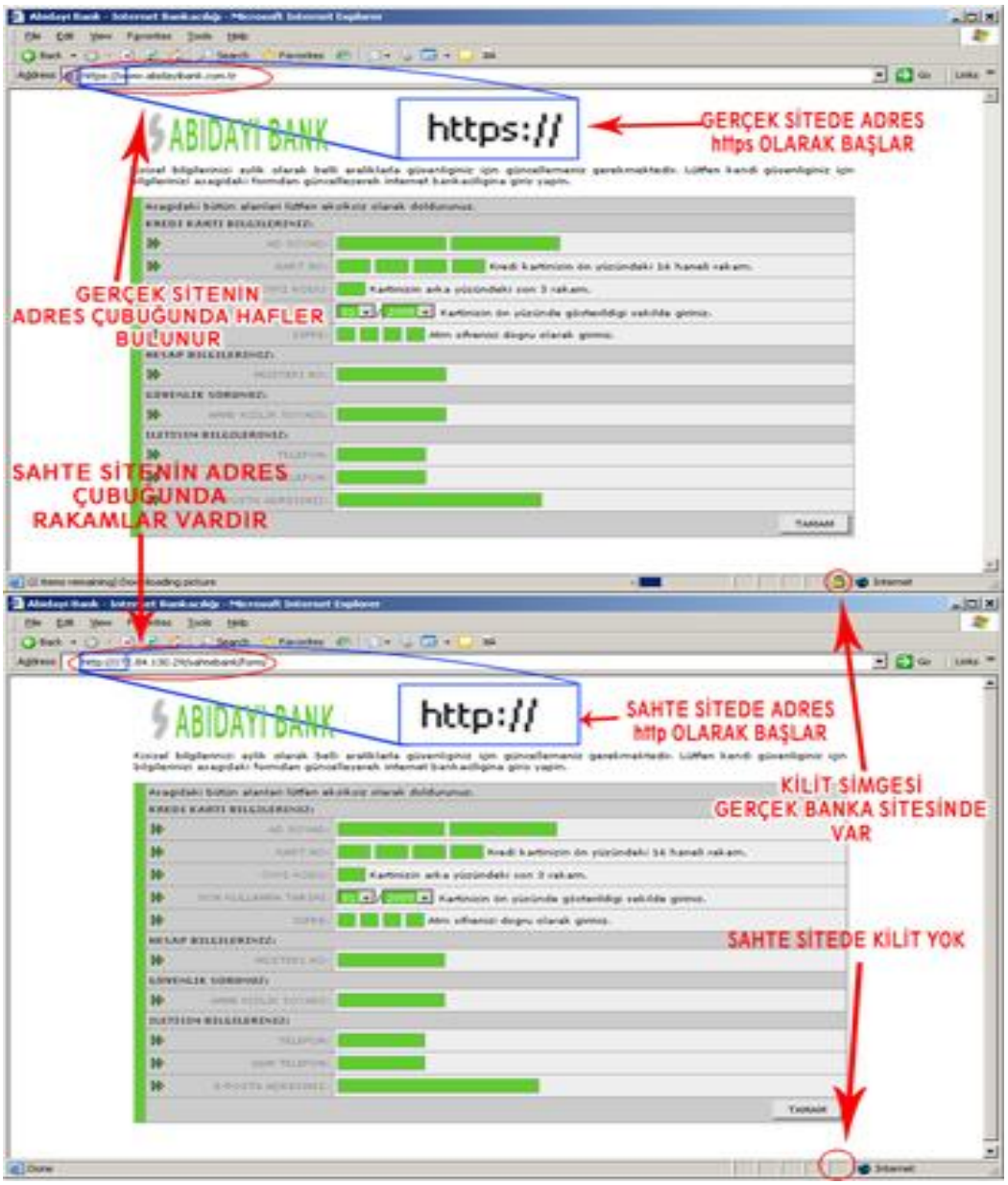
➢ Sahte sitelerde, çoğu zaman sayısal adresler kullanılmaktadır. Eğer bu tür bir durum ile karşılaşılırsa, direkt olarak çalışılan kuruluş ile irtibata geçmek gerekmektedir.

ÖRNEK:
Sahte siteler aşağıdaki gibi sayısal bir link verirler.

Şekil 2.2. Sayısal link örneği.

- Güvenilmeyen Network (Ağlarda) kesinlikle elektronik işlem yapmamak gerekmektedir. Kullanılan bilgisayar güvenilir olsa bile eğer networke (Ağa) güvenilmiyorsa elektronik işlem yapmamak gerekmektedir.
- Bankadan gelen kart ekstreleri ve hesabı düzenli olarak kontrol etmek gerekmektedir. Olası aksiliklerde kesinlikle banka ile irtibata geçmek gerekmektedir.
- Bilgisayar sistemini düzenli olarak kontrol etmek gerekmektedir. İşletim sisteminin güvenlik yamalarını yüklemek, antivirüs yazılımlarını devamlı olarak güncellemek gerekmektedir.
- Çeşitli kurumlardaki hesaplar veya eğer ki birden fazla e-posta adresi var ise kesinlikle her biri için farklı şifreler belirlemek gerekmektedir.
- Belirlenilen şifreleri belli aralıklarla mutlaka değiştirmek gerekmektedir.
- Eğer böyle bir eyleme maruz kalınırsa gelen e-postayı kesinlikle silmemek ve yönlendirdiği web sitesiyle ilgili bilgiler toplamak gerekmektedir.

Aşağıdaki şekil incelendiğinde sahte site ile gerçeğini ayırt etmek mümkün olmaktadır.



Şekil 2. 3. Gerçek site ile sahte site dizayn farkları.

2.4.2. E- Posta Yöntemi

E-posta yöntemini kullanan dolandırıcılar internet bankacılığı hizmeti kullanıcılarını aldatmak için çeşitli yollara başvurmaktadırlar.

Bunlar:

- E-posta adresine devamlı temas halinde olunan kuruluşlardan gönderiliyormuş izlenimi verilen sahte bir posta gönderilmektedir. Bu e-postalarda kullanıcıya kurumun web sitesine giderek şifresinin süresinin dolduğu söylenmekte ve altta o sayfaya yönlendirileceği bir link (bağlantı yolu) verilmektedir. E-posta adresi mutlaka iyi incelenmelidir, orijinal adres veya gönderilen kişi ile ilgili farkı bir karakter dikkatli bir bakışla anlaşılabilir.
- Bazı e-postalarda, bir yarışma düzenlendiği ve bu yarışmaya katılması teklif edilen kullanıcılara ödül olarak lüks bir otomobil verileceği söylenerek yarışmacılardan kişisel bilgileri istenmektedir. Bu gibi durumlarda bilgilerini veren kullanıcının tüm bilgileri dolandırıcının yani korsanın eline geçmektedir.
- Kullanılan bir başka teknikte ise; gelen e-postada müşteriye kişisel bilgilerini güncellemesi gerektiği tüm bilgileri tekrar girmesi bunun kendileri açısından daha iyi hizmet verilebilmesi için gerekli olduğu söylenmektedir.
- Son zamanlarda bazı bankaların başlatmış oldukları ve cep telefonları ile para transferine imkân veren sistem kullanılarak banka müşterilerine sanki kendi hesaplarına para gönderilmiş veya alınmış gibi gösterilip sahte banka sitesi linki (bağlantı yolu) verilerek bu paranın tahsil edilebilmesi için bilgi güncelleştirmesi istendiği belirtilmektedir.

Şekil 4'de dolandırıcılık amacıyla kullanılan bir e-posta görülmektedir. Yönlendirilen linke giren kullanıcı, kötü sonuçlarla karşı karşıya kalabilmektedir.

Sayın X Bank Müşterisi,

Hesabınıza 24 Şubat 2005 tarihinde Hüseyin GÜLOĞLU tarafından 270 YTL. havale edilmiştir. Yapılan havale ile ilgili ayrıntılar aşağıdadır.

Gönderen: Hüseyin GÜLOĞLU
Miktar: 270,00 YTL. (İki Yüz Yetmiş Yeni Türk Lirası)
Şube: Mardin / Merkez
Açıklama: -
Havale onay ve/veya red işlemi için aşağıdaki linkten internet bankacılığını kullanabilirsiniz ve/veya hesabınızda gerekli incelemeleri yapabilirsiniz. Size havale gönderen kişinin bilgileri için aşağıdaki linki kullanabilirsiniz…

www.xbank.com.tr
Eğer yukarıdaki link çalışmıyorsa lütfen aşağıdaki linki kullanınız.

http://172.84.130.29/xbank/form/

Şekil 2.4. E-posta yönteminde kullanılan örnek bir e-posta.

2.4.3. Tuş kaydedici (Keylogger) ve Ekran Kaydedici (Screenlogger) Yöntemi

Dolandırıcılar olta (phishing) yöntemiyle kullanıcının gizli bilgilerini elde etmenin yanı sıra bu bilgilere birde başka bir yöntem olan tuş kaydedici (keylogger) ve ekran kaydedici (screenlogger) adı verilen klavye ve ekran görüntülerini kopyalayabilen programlar aracılığıyla ulaşabilmektedirler.

Resim 2.8: Şifrenizi sık sık değiştirin

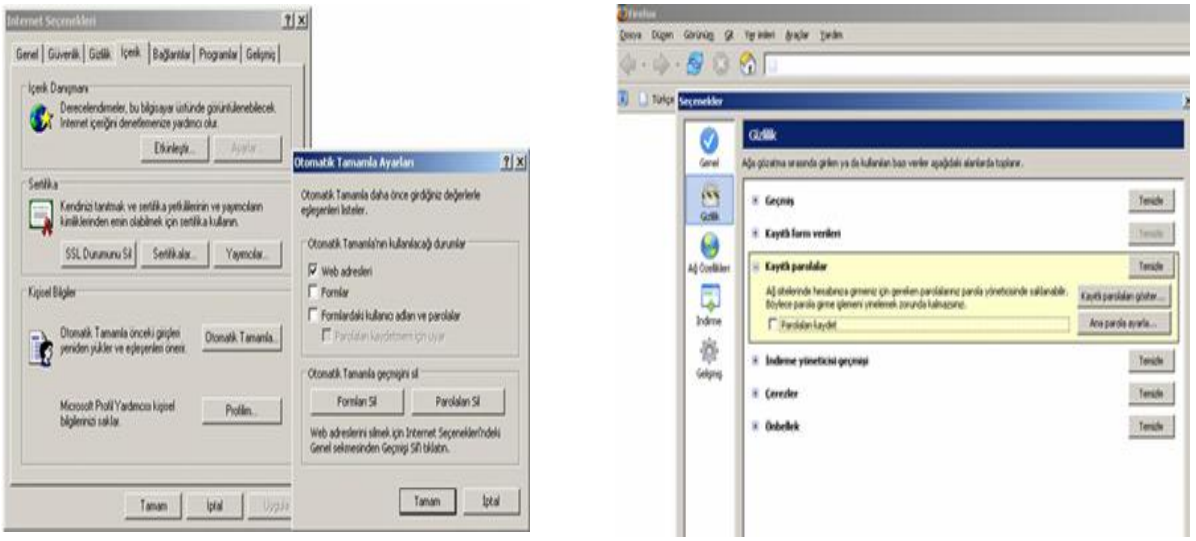
Kullanıcıların bilgisayarlarına yerleştirilen bu yazılımlar, bilgisayarda yapılan her türlü işlemin kaydını tutmaktadır. Bu kayıtlar ya sistemde bir txt (metin) dosyası olarak tutulmakta ya da klavye girdileri e-posta ile saldırgana (Hacker) gönderilmektedir.

Tuş kaydedici veya ekran kaydedici türü yazılımlar sisteme iki yoldan sızabilmektedir. Keylogger ve screenlogger yazılmları, ya işletim sistemlerinin açıklarından yararlanılarak hedef bilgisayarın yönetici haklarını kısmen veya tamamen saldırgana teslim etmekte olan truva atı (trojan) adlı yazılımlar aracılığıyla ya da kullanıcı tarafından bilinmeden bilgisayara yüklenebilmektedir.

Keylogger ve screenlogger benzeri programlardan etkilenmemek için :

- İşletim sisteminin güncelleştermelerini mutlaka yapmak gerekmektedir.
- Bir güncel ve aktif antivirüs programının bilgisayarda mutlaka bulunması gerekmektedir.
- Bankacılık ve diğer önemli işleri güvenli olmayan bilgisayardan yapmamak gerekmektedir.
- Kullanılan bilgisayarın web browserının (internet tarayıcısının) otomatik tanımlama özelliğindeki "Formlarda kullanıcı adları ve parolalar" ile ilgili kısmın işaretli olmamasına dikkat etmek gerekmektedir.

Şekil 5'de internet explorer ve mozilla firefox adlı browserlar için "Formlarda kullanıcı adları ve parolalar" ayarları gösterilmektedir. İnternet Explorer 6.0 için (Araçlar-> İnternet Seçenekleri-> İçerik-> Otomatik Tamamla) şeklinde bir yol izlemek gerekmektedir.



Şekil 2.5. İnternet Explorer 6.0 ve Mozilla Firefox için "Formlarda Kullanıcı Adları ve Parolalar" ayarı.

2.5. Kanunlarda İnternet Dolandırıcılığı Suçlarının Belirtildiği Maddeler

Bu sorunun cevabına aşağıdaki soru-cevaplarla ulaşmak mümkündür:

- Yeni ve eski TCK'ya göre internet dolandırıcılığı suçunun tanımı nedir?
- Bu suçun tanımı hem eski hem de yeni TCK'da tam olarak tanımlanmamıştır. Bu nedenle sonuca ulaşırken yorum yapmak zorunluluğu doğmaktadır. Bu suça bilişim suçu demek yorumdan dolayı zorlaşmaktadır. Ancak yeni TCK'da md:158/f bu suç için uygulanabilmektedir.
- Bunun gibi suçlarda korunan hukuki menfaat nedir?
- Sahte mailler ile işlenen bu suçlarda korunan hukukei menfaat kişinin mal varlığı haklarıdır.
- İnternet dolandırıcılığı suçunda mağdur kimdir ? (Banka mı yoksa müşteri mi?)
- Olayın gerçekleşmesiyle mağdur duruma düşen kimse banka değil müşteridir. Çünkü, mal varlığında azalma meydana gelen, hileye uğrayan kişi müşteridir.
- İnternet dolandırıcılığı suçunda olayın faili kimdir?
- Olayın faili herkes olabilmektedir. Yasa fail olabilmek için özel bir şart aramamaktadır.
- Suçla mücadelede hukuki olarak nasıl bir yöntem izlenmelidir?
- Suçla mücadele için öncelikli olarak bir adli bilişim biriminin kurulması gerekmektedir. İkinci olarak, hakim ve savcılarımıza yeterli eğitim vermek gerekmektedir. Üçüncü olarak ise servis sağlayıcılara yasal yükümlülükler getirerek bugün delillendirme de yaşanan problemlerin önüne geçmek gerekmektedir.

- Delillendirme nasıl yapılabilir?
- Delillendirme, gelen sahte elektronik postanın kağıt çıktısının mahkemeye sunulması değil, elektronik versiyonunun savcıya ya da mahkemeye sunularak üzerinde bilirkişi incelemesi yaptırılmasıdır. Ayrıca sahte postanın yönlendirdiği web sitesine ilişkin bilgilerin ve yine sahte elektronik postanın gönderildiği servis sağlayıcısından alınacak bilgilerin dosyaya konulması gerekmektedir.
- Mağdurun başvuru yolları nelerdir?
- Böyle bir eyleme maruz kalan kişinin derhal bankasını bilgilendirmesi ve ardından TCK'nun dolandırıcılık hükümlerine göre savcılığa dilekçe ile başvurması gerekmektedir. Burada hem mağdura hem savcıya hem de güvenlik güçlerine düşen görev hayati önemdeki bir kaç delilin en kısa zamanda toplanmasını sağlamaktır.
- Uluslararası hukukta internet dolandırıcılığı suçları ne boyuttadır? Uluslararası hukuk bunu nasıl karşılamaktadır?

Dünya bu eyleme hazırlıksız yakalanmıştır. Bu nedenle bunu açıkça suç olarak düzenleyen bir yasa maddesi bulunmamaktadır. Ancak, ABD'li hukukçuların "The Anti – Phishing Act" olarak adlandırdıkları ve Senatör Patrick Leahy tarafından sunulan yasa tasarısı ile ABD'de büyük finansal kayıplara yol açan sahte elektronik posta eylemleri ve bilişim suçları önlenmek istenmektedir. Diğer ülkelerin genel eğilimi ise ceza yasalarındaki bilişim suçlarını düzenleyen hükümlerden yararlanmak yönündedir <http://www.iem.gov.tr/iem/ > (2006, Mart 23).

2.6. İnternet Bankacılığında Güvenli İletişim, Bilgi Güvenliği ve Açık Anahtar Altyapısı

Son yıllarda internetin kullanımının yaygınlaşmasıyla beraber e-iş, çevrimiçi alışveriş, internet bankacılığı gibi yüksek güvenlik özelliği taşıyan hizmetler de günlük kullanımda yaygınlaşmaktadır. İnternet bankacılığının sağladığı kolaylıklar kaçınılmaz şekilde ağ ortamının bankacılık işlemlerinde de kullanımını yaygınlaştırmaktadır. Günümüzde internet, bankacılık işlemlerindeki baskın rolünü hem korumakta hem de büyük bir ivmeyle arttırmaktadır.

İnternet bankacılığının en önemli avantajları; işlemlerin daha düşük maliyetlerle gerçekleştirilebilmesi, kağıt tabanlı işlerde önemli oranda azalma sağlanabilmesi, bankacılık işlemlerinin herhangi bir yer veya hareket gerektirmeksizin istenilen her yerden günün her saati yapılabiliyor olmasıdır.

Bugün internet bankacılığının en yaygın kullanımı, elde edilmesi oldukça kolay ve gerçek anlamda bir güvenlik içermeyen doğrulama yöntemi olan müşteri numarası veya adı ve şifre kullanımı esasına dayanmaktadır. Bankaların kendi bünyelerinde bir takım güvenlik tanımlamalarına karşın tüm sektörde kabul görmüş genel bir standardın kullanımının eksikliği göze çarpmaktadır.

- Şifre ve Parolalar sözlük ataklarına, basılan tuşları kaydeden programlara ve dikkatsizlikten doğan hatalara açıktır.
- SSL iletişimin gizliliğini sağlamasına karşın gönderilen bilginin inkar edilememesi özelliğini taşımamaktadır. İletişimin gizliliği son kullanıcı tarafından üretilen bir oturum anahtarına dayanmaktadır.

- Anahtar yönetimi ve dağıtımı zordur. Tüm özel anahtarlar merkezi bir yerde durduğundan merkezde oluşacak bir hata bütün sistemi etkileyecektir.

- Uygulamaya özel geliştirilen yöntemler de esneklik ve standartlaşmadan yoksundurlar.

Resim 2.9: Birileri hata yapmanızı bekliyor

İnternet bankacılığında en yaygın olarak kullanılan güvenlik modelleri ve açıkları şunlardır;

Çok yaygın kullanım olmasına karşın internette bankacılık gibi önemli bilgilerin ağ üzerinde dolaştığı güvenli bir ortam tam anlamıyla oluşmamıştır. Genel senaryolar göz önüne alındığında internet bankacılığının tam anlamıyla güvenli hale gelebilmesi için dört temel gerekliliğin yerine getirilmesi gerekmektedir.

Bunlar:

- Ağ üzerinde kullanıcıların kendilerini güvenli bir şekilde tanımlamaları gerekmektedir.
- Yapılan işlemlerin ve iletilen verilen gizliliği gerekmektedir.
- İletilen verilen değiştirilmeden yerine ulaşması gerekmektedir.Yapılan ödeme veya gönderilen faturanın inkar edilmemes gerekmektedir.

Bilgi güvenliği için gerekli bir diğer işlemse kriptolamadır. Kriptolama, internet teknolojisi ile transferde bilgiyi koruyan temel mekanizmaya verilen isimdir. Verinin özel bir kod yada anahtar kullanılmadan diğerleri tarafından anlaşılmayacak şekle dönüştürülmesidir. Dekriptolama veriyi bir anahtar kullanarak orjinal şekline dönüştürme işlemidir.

Kriptolama bilgi sistemlerinde aşağıdaki fonksiyonları sağlamak için kullanılabilmektedir:

- kimlik tanılama (authentication)
- veri bütünlüğü (data integrity)
- gizlilik/mahremiyet (confidentiality/privacy)
- inkar edememe (non-repudation)

Çoğu sistemde kullanıcıların sisteme giriş yapmasına izin verilmeden önce doğru kullanıcı ismi ve şifre sağlamaları gerekmektedir. Kimliklerin doğrulanması işlemine kimlik tanılama/doğrulama (authentication) denir. Erişim kontrolü veya kimlik tanılama, bir kullanıcının sistemde kullanabileceği bilgi ve servisleri belirlemektedir. Bireylere yada gruplara kimlik tanılama seviyelerine göre erişim izni verilmektedir. Kriptolama teknikleri dijital imzalarla mesajların kaynağını doğrulamada kullanılabilmektedir. Bu imzalar mesajın yazarının kimliğini doğrulamakta ve alıcı, mesajın doğru kişiden geldiğine emin olmaktadır. Dijital imzalar şifrelerle birlikte yada şifrelerin
yerine kullanılabilmektedir

Resim 2.10: Virüs programıyla güvendesiniz

Kriptolama transfer edilen verinin bütünlüğünü garantilemektedir. Mesaj özetleri (digest) doküman ile birlikte dijital parmakizlerini yaratarak doküman ve dosyaların bütünlüğünü test etmektedir. Bu, dijital olarak imzalanmış mesaj özetleri verilerinin transfer edilirken değiştirilmediğini kontrol etmede kullanılabilmektedir. Kulak misafiri (eavesdropper) olarak tabir edilen kişiler internet üzerinde transfer edilen verileri yakalayan/dinleyen yetkisiz kişilerdir. Kriptolama veriyi karışık hale getirerek gizliliği kormaktadır.

Teyit servisleri bir mesajın yaratıcısını mesajın alınıp alınmadığı konusunda haberdar etmektedir. Ayrıca mesajın transfer sırasında değiştirilmediği konusunda da haberdar edebilmektedir. İnkar edememe, mesajı gönderen kişinin daha sonra mesajı gönderdiğini inkar edememesi veya alıcının mesajı aldığını inkar edememesidir. Bu teknikler genelde kaynağın inkar edilememesi (nonrepudiation of origin) ve teslimatın inkar edilememesi (nonrepudiation of delivery) olarak adlandırılmaktadır. Emin olmak için kriptografik alındı mesajları yayınlanabilmektedir

Yukarıda bahsedilen güvenlik uygulamalarının dışında kalan Açık Anahtar Altyapısı (AAA- Public Key Infrastructure (PKI)) ise, internet bankacılığı için en güvenli modeli ve en kapsamlı e-güvenlik çözümünü sunmaktadır. İnternet bankacılığı gibi bir ağ üzerinde kritik bilgilerin dolaştığı uygulamaları, bir bütün olarak güvenlik altına alan Açık Anahtar Altyapısı (AAA), diğer güvenlik modellerinden farklı olarak;

- Bir standarttır ve aynı altyapıya sahip tüm uygulamalara uyumludur,
- Daha güvenli bir çerçeveye sahiptir,
- Esnektir ve kolaylıkla ölçeklenebilir,
- Modülerdir.
- AAA internet bankacılığının tüm güvenlik gereksinimlerini eksiksiz karşılayan bir yapıya sahiptir;
- Kimlik Doğrulama – 3. parti bir sertifika otoritesinin dağıttığı sertifikaların kullanımıyla,
- Gizlilik – Gönderilen verilerin şifrelenmesiyle,
- Bütünlük – Hash yöntemiyle verinin "parmak izi"nin alınmasıyla,
- İnkar-Edememezlik – Gönderilen verinin sayısal imza ile imzalanmasıyla gerçekleştirilir.

İnternet bankacılığında sayısal imzaların ve sayısal sertifikaların kullanılması, internet gibi açık ağlar üzerinde yapılan bankacılık işlemleri için güvenli elektronik ortamı oluşturmaktadır. Günümüzde AAA küresel güven zinciri oluşturmada evrensel olarak kabul edilen bir standart haline gelmektedir. Bankacılık uygulamalarında akıllı kartların kullanımının yaygınlaşması, AAA'nı tamamlayan bir unsur olarak daha güvenli araçlar kullanılarak iletişim yapılmasını sağlayacaktır.

Ülkemizde Sayısal İmzanın (elektronik imza) yasallaşması ve yakın zamanda banka ve kredi kartlarında akıllı kartlara geçiliyor olması internet bankacılığı için çok daha güvenli ve geniş kapsamlı bir model oluşturulmasına önemli oranda destek olacaktır.

UYGULAMA FAALİYETİ

Işlem Basamaklari	Öneriler
➢ E-Bankacılığın sağladığı faydaları sıralayınız?	➢ Firewall kavramını araştırınız. ➢ Bankacılıkla ilgili araştırmaları ve anketleri takip ediniz. ➢ E-Bankacılığı kullanan kişi ve kurumlardan örneklar toplayınız.
➢ Alternatif bankacılık kanallarını tanımlayınız?	➢ Bankacılığın fonksiyonlarını araştırınız. ➢ Hangi şekillerden bankacılık faaliyetleri yapıldığını sıralayınız ➢ Alternatif bankacılık kanallarını maliyet ve zaman açısından karşılaştırınız
➢ E-Bankacılığı kullanırken alınacak güvenlik tedbirlerini kavrayınız.	➢ Açık anahtar altyapısı (Public Key Infrastructure-PKI) kavramını açıklayınız ➢ Tek kullanımlık şifre jeneratörü kavramını açıklayınız? ➢ Alınacak güvenlik tedbirlerini internet ortamında uygulayınız. ➢ Dikkatli olunuz ➢ İnternetten nasıl güvenli alışveriş yaparız? açıklayınız ➢ E-Posta ile dolandırıcılık nasıl yapılır? açıklayınız

ÖLÇME VE DEĞERLENDİRME

A. OBJEKTİF TESTLER

1. Aşağıdakilerden hangisi İnternet bankacılığının sağladığı faydalar dan biri değildir?
   A) Bankacılık işlemleri, hızlı ve kesintisiz yapılabilmektedir.
   B) Bankacılık işlemi, görerek ve seçerek yapılabilmektedir.
   C) Detaylı rapor ve bilgi alınabilmektedir.
   D) Bankacılık işlemleri daha pahalıya yapılmaktadır.

2. Aşağıdakilerden hangisi Olta saldırılarını düzenleyenlerin çaldıkları bilgilerden değildir.
   A) Yaşadığınız şehir
   B) Şifreler ve Parolalar
   C) Hesap Numaraları
   D) İnternet Bankacılığına Girişte Kullanılan Kullanıcı Kodu ve Şifreleri

3. İnternet güvenliği ile ilgili aşağıdakilerden hangisi yanlıştır?
   A) Sayısal rakam içeren adresler mutlaka kontrol edilmeli
   B) Farklı hesaplar için farklı şifreler kullanılmalı
   C) Belirlenen şifreler kesinlikle değiştirilmemeli
   D) Bankadan gelen ekstrelerle hesaplar düzenli kontrol edilmeli.

4. İnternet bankacılığı hizmetini kullanan bir kimse banka hesaplarının bakiyesini almak istediğinde bu bilgi öncelikle firewall adı verilen bilgisayara gelmektedir
   Doğru ( ) Yanlış( )

5. Bankalar e-posta yoluyla hiç bir şekilde müşterilerin kişisel bilgilerini istememektedir.
   Doğru ( ) Yanlış( )

6. Güvenlik duvarı (firewall) kullanımı güvenliği arttırır.
   Doğru ( ) Yanlış( )
7. Olta saldırılarından korunmak için erişmek istenilen web sayfasının adresini tarayıcının adres satırına bizzat yazmak gerekmektedir.
   Doğru ( ) Yanlış( )

DEĞERLENDİRME

Cevaplarınızı modülün sonundaki cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete geri dönerek tekrar inceleyiniz

B. PERFORMANS TESTİ

Modül ile kazandığınız yeterliği aşağıdaki ölçütlerine göre değerlendiriniz.

DEĞERLENDİRME ÖLÇÜTLERİ	Evet	Hayır
E-Bankacılığın faydalarını açıklayabilir misiniz?		
İnteret güvenliğinde kullanılan temel araçları açıklayabilir misiniz?		
E-Bankacılıkta karşılaşılan sorunları açıklayabilir misiniz?		
E-Bankacılık kullanımında dikkat edilecek hususları açıklayabilir misiniz?		
İnternet ortamında gerçekleşen saldırıları açıklayabilir misiniz?		
Olta saldırılarından korunma yollarını açıklayabilir misiniz.		
Tuş kaydedici ve ekran kaydedici yöntemiyle dolandırıcılık yöntemini açıklayabilir misiniz.		

MODÜL DEĞERLENDİRME

1. Aşağıdakilerden hangisi e- bankacılığın işlevlerinden biri değildir.
   A) Aynı işlemlerin tekrarının engellenmesi.
   B) İşlemler için daha az zaman harcanmasına
   C) Bilgi akış sisteminin standartlaşmasına.
   D) Orta düzey yönetici ihtiyacının artmasına

2. E- Bankacılığı kullanarak aşağıdakilerden hangisini yapamazsınız?
   A) Fatura ödeme
   B) Para aktarma
   C) Para çekme
   D) Hisse senedi alma

3. Aşağıdakilerden hangisi ilk internet bankacılığını kullanan bankadır.
   A) Garanti Bankası
   B) Osmanlı Bankası
   C) İş Bankası
   D) Akbank

4. Aşağıdakilerden hangisi alternatif bankacılık kanallarından biri değildir?
   A) Telefon bankacılığı
   B) İnternet bankacılığı
   C) Bireysel bankacılık
   D) Cep telefonu bankacılığı

5. E-Bankacılığa geçiş süreci para çekme makineleri (ATM) ile başlamıştır.
   Doğru ( ) Yanlış ( )

6. SSL network (ağ) üzerindeki veri transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla "Netscape" tarafından geliştirilmiş bir güvenlik protokolüdür.
   Doğru ( ) Yanlış ( )

7. Sigorta sözleşmesini hafifletici veya ağırlaştırıcı durumların en geç bir ay içinde sigortacıya bildirilmesi gerekmektedir.
Doğru ( ) Yanlış ( )

8. Telefon bankacılığı ise internet bankacılığına göre daha az maliyetlidir.
   Doğru ( ) Yanlış( )

9. Banka ile kullanıcı bilgisayarları arasında kurulan iletişim dinlenerek içeriğinde bulunan şifre, hesap no, kredi kartı bilgileri gibi hassas bilgiler başkaları tarafından elde edilebilmektedir.
   Doğru ( ) Yanlış( )

PERFORMANS TESTİ

Modül ile kazandığınız yeterliği aşağıdaki ölçütlerine göre değerlendiriniz.

DEĞERLENDİRME ÖLÇÜTLERİ	Evet	Hayır
Türkiye'de E- Bankacılığın gelişimini açıklayabilir misiniz ?		
E-Bankacılığın temel öğelerini açıklayabilir misiniz?		
Türkiye'de E-Bankacılığın Gelişimini açıklayabilir misiniz?		
E-Bankacılık yapan bankaların hizmetlerini açıklayabilir misiniz?		
İnternet hizmetlerinin bankacılığa sağlayacağı katkıları açıklayabilir misiniz?		
E-Bankacılığın ofis bankacılığından üstünlüklerini açıklayabilir misiniz?		
Türkiye'deki internet sitelerinin güvenliği konusnuda güncel verileri açıklayabilirmisiniz?		
E-Bankacılıkta karşılaşılan en temel güvenlik sorunlarını açıklayabilir misiniz?		
Olta saldırılarının E-Bankacılığa verdiği zararları açıklayabilir misiniz.		
İnternet sitesinin güvenli olup olmadığını anlayabilir misiniz?		
Kriptolama yöntemiyle korunma yöntemini açıklayabilir misiniz?		
E-Bankacılık kullanımında alınacak güvenlik tedbirlerini açıklayabilir misiniz?		
Güvenlikle ilgili püf noktaları açıklayabilir misiniz?		

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ 1 CEVAP ANAHTARI

1	D
2	A
3	D
4	A
5	DOĞRU
6	YANLIŞ
7	DOĞRU

ÖĞRENME FAALİYETİ 2 CEVAP ANAHTARI

1	D
2	A
3	C
4	DOĞRU
5	DOĞRU
6	DOĞRU
7	DOĞRU

MODÜL ÖLÇME SORULARI CEVAP ANAHTARI

1	D
2	C
3	C
4	C
5	DOĞRU
6	DOĞRU
7	DOĞRU
8	YANLIŞ
9	DOĞRU

ÖNERİLEN KAYNAKLAR

- http://www.bddk.org.tr

KAYNAKÇA

- TURAN Mehmet, **Elektronik Bankacılık,** C.I.S.A. Yayınları, İstanbul, 2003
- KURT Ertan, **İnternette Güvenlik: İnternet Bankacılığı,**. İnternet Akademi Derneği, Ocak, 2003
- http://www.tbb.org.tr
- http://www.wto.org
- http://www.iem.gov.tr
- http://www.foreigntrade.gov.tr
- http://www.tbb.org.tr