**T.C.**
**KADİR HAS ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**
**İŞLETME (MBA) BÖLÜMÜ**

# TÜRK BANKACILIK SİSTEMİNDE İNTERNET BANKACILIĞI İLE YAPILAN DOLANDIRICILIKLAR

# VE BİLİŞİM SUÇLARI HUKUKU

**Yüksek Lisans Tezi**

**SEHER ERGÜÇ**

**İstanbul, 2008**

**T.C.**
**KADİR HAS ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**
**İŞLETME (MBA) BÖLÜMÜ**

# TÜRK BANKACILIK SİSTEMİNDE İNTERNET BANKACILIĞI İLE YAPILAN DOLANDIRICILIKLAR VE BİLİŞİM SUÇLARI HUKUKU

**Yüksek Lisans Tezi**

**DANIŞMAN**

**DR. BİRGÜL ŞAKAR**

**HAZIRLAYAN**

**SEHER ERGÜÇ**
**2006.09.01.019**

**İstanbul, 2008**

# İÇİNDEKİLER

**Sayfa No.**

# TABLO LİSTESİ

# ŞEKİL LİSTESİ

# GRAFİK LİSTESİ

# KISALTMALAR

| | |
|---|---|
| age. | Adı geçen eser |
| s. | Sayfa |
| S | Sayı |
| TBB | Türkiye Bankalar Birliği |
| BDDK | Bankacılık Düzenleme ve Denetleme Kurulu |
| TCMB | Türkiye Cumhuriyet Merkez Bankası |
| YTL | Yeni Türk Lirası |
| ATM | Otomatik Para Çekme Makineleri |

# GİRİŞ

İletişim ve bilgisayar teknolojisindeki gelişmeler gün geçtikçe artmaktadır. Teknolojinin gelişmesiyle birlikte bankacılık işlemlerinde de değişimler yaşanmaktadır. İletişim imkânları bankacılık işlemlerini kolaylaştırmakla birlikte bankacılık sektörünün yapısını da değiştirmiştir. Ülkemizde faaliyet gösteren bütün bankalar faaliyetlerini internet ortamına taşıyarak müşterilerine internet üzerinden hizmet verme imkânına sahip olmuşlardır. Elektronik bankacılık, bankaların geleneksel mevduat alma ve kredi verme faaliyetleri için pazarlarını geliştirmesini sağlamıştır. Yeni ürünler, hizmetler sunmalarını ve mevcut ödeme hizmetlerini sunmada kendi rekabet pozisyonlarını güçlendirmiştir. Ayrıca elektronik bankacılık bankaların işletme maliyetlerini azaltmaktadır.

Elektronik bankacılık ve elektronik paranın devam eden gelişmesi, ulusal ve uluslararası çapta bankacılık ve ödeme sisteminin verimliliğini artırma ve bireysel işlemlerin maliyetini azaltmaya katkıda bulunmaktadır.

Elektronik bankacılıktaki gelişmeler ve kullanıcıların hızla artması dolandırıcılarında yeni bir suç devrimine başlamış olduğunu göstermektedir. Günümüzde bilgisayar kavramı sadece hayatımızı kolaylaştıran bir devrim olmaktan çıkmış suç kavramı ile birlikte anılan bir araç haline de gelmiştir.

Elektronik bankacılıkta gelişmelerin yaşandığı günümüzde ortaya çıkacak risk ve sorumluluklarda incelenmelidir. Elektronik bankacılık işlemlerini gerçekleştiren kimselerin maruz kalabilecekleri çok sayıda riskten kaynaklanan yükümlülük ve sorumlulukların, tarafların menfaatlerine aykırı düşmeden belirlenmesi ve paylaştırılması gerekmektedir.

## SUMMARY

There is rapid advancement at communication and computer technology every other day. As the technology advances, there are also changes in banking transactions. The communication possibilities have changed the banking sector structure and eased the banking transactions. All the banks in our country have carried their activities to internet and had the oppurtinity to serve their customers online. Electronic banking have helped the banks to improve their market for traditional fund raising and credit granting New products have reinforced their competitional positions in offering their services and current payment services. Also electronic banking have reduced banking operational costs.

Ongoing progress of electronic banking and electronic money have helped productivity of national/international banking and payment systems, also reduced the costs of personel transactions.

The advancement of electronic banking and the number of users show that there is a new crime revolution of fraud. In our modern days, the computer concept has become a crime concept as well as a revolution that eases our life.

Also, the risk and responsibilities should be explored in todays fast-changing world. The liability and responsibility should be clarified and shared between the parties without being unjust.

# 1. İNTERNET, DOLANDIRICILIK VE İNTERNET BANKACILIĞI TANIMLARI

İnternet dünya bilgisayarlarını birbirine bağlama aracı olup, tüm dünyadaki bilgisayarların birbirleriyle haberleşmesine imkân veren ortak bir elektronik dil ve kurallar dizisidir. İnternet yeni bir küresel haberleşme aracı ve küresel bilgi kaynağıdır. Mesafenin bu ortamda önemi yoktur.[1] İnternet tanımı dünya üzerindeki milyonlarca bilgisayarın birbirlerine bağlanmalarıyla oluşan bilgisayar ağları sistemi olara yapılmaktadır.[2]

İnternet, gerçekdışı bir evrendir. Eğitim ve ilerlemede internet ön plana çıkarılmaktadır. [3]

Yeni teknolojiler, bireyler ve toplumlar için yeni fırsatların yanında yeni problemlerde yaratmaktadır. Yeni teknolojiler olumlu ve olumsuz etkilere sahiptirler ve genellikle ikisi bir arada görülür. [4]

İnternet, sonsuz bir bilgi kaynağı olması ve mesafeleri ortadan kaldırması yanında dolandırıcılık gibi kötü amaçlar içinde kullanılmaya başlanmıştır.

Dolandırıcı kelimesi Türk Dil Kurumu Sözlüğünde "Birini aldatarak mal veya parasını alan kimse" olarak tanımlanmaktadır.[5] Dolandırıcılık eylemlerine hemen her ülkede ve her kültürde rastlamak mümkündür. Ancak, son yıllarda özellikle bilişim sektöründeki gelişmeler nedeniyle dolandırıcılık eylemleri teknolojik yöntemlerin kullanıldığı daha karmaşık bir yapı haline gelmiştir. Dolandırıcılık amacıyla kurulan çete ve şebekeler ise daha organize halde çalışmaktadır. Dolandırıcıların veya dolandırıcılık amacıyla kurulmuş olan çetelerin hedefinde "şahıslar" olduğu gibi kurumlar da yer almaktadır. Bankacılık, dolandırıcılık eylemlerine en çok hedef olan sektörlerin başında

---

1 Frances Cairncross , "The Death Of Distance, London: Orion Business Books", 1997, s.95.

2 Erkan Boğaç, Songür Mursat, "Açıklamalı Bilg ve İnt Terimleri Sözlüğü" , Ankara: Hacettepe-Taş Kitapçılık, 1999, s.282

3 Clifford Stoll, "Slicon Snake Oil: Second Thoughts on the ınformation Hıgway", London Pan Books, 1996, s.3-4

4 Emmanuel Mesthane, "Technology as a Social and Political Phenomenon" , (1976), www.icisleri.gov.tr/_Icisleri/WPX/tezler_internetsuclari.doc, (14 Eylül 2007)

5 Kenan Burçin Atakan, Ceren Sayar, Fisun Büyükgören ,Fatma Aydın, Ali Süha Ter, Emre Sargın, Türkiye Bankalar Birliği İnternet Bankacılığı Çalışma Grubu, "Bankacılıkta Dolandırıcılık Eylemleri Tespit Önleme Yöntemleri",Nisan 2007, www.tbb.org.tr/v12/doc/Kitapçık.pdf ,(14 Eylül 2007), s.5-6.

gelmektedir. Bankalar, teknolojik altyapılarının kurulmasında ve bankacılık işlemlerinin gerçekleştirilmesinde güvenliğe son derece önem vermektedirler. Dolandırıcılık girişimleri ortak noktası, ele geçirilmek istenen değerin nakit para olmasıdır. Eylem girişimi, internette müşterilerin bilgilerinin casus yazılımlarla ele geçirilmesi ve ele geçirilen tutarın banka şubeleri veya otomatik para ödeme makineleri (ATM) yoluyla banka dışına çıkartılmasıdır. Bu nedenle, dolandırıcının şubeye gelerek hesap açması veya otomatik para ödeme makinelerinde kullanabileceği bir kart alması gerekmektedir.

Hacker, İngilizce "Hack" kelimesinden gelmektedir. Hack "kesmek", "baltalamak" anlamında kullanıldığı gibi, "Kiraya verilen at" anlamına da gelmektedir. "Hacker" ise "korsan" anlamına gelmektedir. Hacker kültürü 1961 yılında MIT Tech Demiryolu Maket Kültürü Derneğinde oluştuğu genel olarak kabul görmektedir. İnternet öncesi ilk çevirim içi bağlantı olarak Kuzey Amerika kıtasında 1969 yılında başlatılan ARPANET hacker kültürünün filizlenmesi için uygun ortamı sağlamıştır. İlk zamanlarında elektronik ortam kültürü olarak kullanılan bu kelime zamanla kötü niyetli girişimleri anlatmaya başlamıştır.[6]

Türk Dil Kurumu' nun tanımına göre hacker: "Bilgisayar ve haberleşme teknolojileri konusunda bilgi sahibi olan, bilgisayar programlama alanında standardın üzerinde beceriye sahip bulunan ve böylece ileri düzeyde yazılımlar geliştiren kişi" olarak tanımlanır.[7]

Hacker, yetenekli ve zeki bir bilgisayar yazılım ve donanımlarında uzman kişidir. Gerçek yeteneği ve bilgisi, bilgisayar güvenliği ve mantıksal programlama üzerinedir. Tüm bilgilere giriş özgürlüğü olduğu inancıyla yüksek seviyede ihtisaslaşmış bilgiye sahip bir kişi olarak kabul edilmektedir.[8]

İş dünyası, kendi internet sitelerinde ticari markalarını ve fikri mülkiyetlerini korumak, müşteriler ve satıcılarla güvenli bir link kurmak amacı ile şifre teknolojisini

---

6 TBB, "Dolandırıcılık Eylemleri Tespit ve Önleme Yöntemleri", Mart 2007, www.tbb.org.tr/v12/doc/Sunum.ppt, (18 Eylül 2007), s.8.

7 http://www.tekstilteknik.com/sozluk/yabanci.asp?yabbas=H, (14 Eylül 2007)

8 David S. Wall, "Their Victims and Their Regulation" , 1999, s.110

kullanır. Bankalar mali transferlerin güvenilirlik ve dokunulmazlığını sağlamak için şifreleme kullanırlar. Hackerler bu şifreleri çözen kişilerdir.[9]

İnternet bankacılığı, çoğu defa "ev ya da ofis bankacılığı" (Home-Banking) olarak tanımlanan kullanımları ifade etmektedir. Ev ya da ofis bankacılığı, internet teknolojisinden önce telefon ya da kablolu televizyonlar aracılığı ile yapılabilmekteydi. İnternet bankacılığı, uzaktan erişimi sağlayan internetin kullanılması yoluyla bankacılık işlemlerinin yapılması olarak tanımlanabilir.[10]

### 1.1. GENEL BİLGİ VE TARİHÇE

Sosyal bir varlık olan insanlar toplu halde yaşamaktadırlar. Bunun sonucunda toplu halde yaşayan bu insanlar devlet olarak örgütlenmiş ve güvenliklerini, devletçe kurulan kolluk güçlerince sağlamışlardır. Devletler artık güvenliğin sağlanması için devlet tekelini kaldırıp, özel ve gönüllü güvenliğin çalışmasına da izin verme, hatta bu sistemleri teşvik etme yoluna gitmektedirler.[11]

Günümüzde şebeke (network) ağlarıyla birbiriyle temas eden bilgisayarların ağırlığının arttığı bir yaşam biçimi gelişmektedir. Güvenliğin yönü; kamu ya da özele ait mekân ve kişileri koruyarak iş hayatını, ticari sözleşmeleri, kişisel bilgileri ve internet güvenliğini içeren daha geniş bir alana doğru kaymaktadır. İnternetteki her uygulama için güvenlik ihtiyacının düşünülmesine ve tespit edilmesine gerek duyulmaktadır.

Risk, tehdit, güvenirlik, zayıflık, sorumluluk, bütünlük, kişisel gizlilik gibi kavramlar üzerinde yeniden düşünülmeye başlanılmış ve konu akademik ilgi alanı haline gelmiştir. Güvenlik kapsamındaki değişim, ticaret sürecine, teşebbüslerin yeniden yapılandırılmasına ve güvenlik mühendisliği kavramının ortaya çıkmasını sağlamıştır.

---

9 Dorothy E.Denning , "LawEnforcement, Security and Surveillance in the Information Age" ,London, 2000, s.129

10 Abdullah Çelik, "İnternet Bankacılığı: Uygulamalar ve Bankacılığın Geleceğindeki Muhtemel Etkileri", Active Dergisi, 2002, Sayı:27, s.1.

11 Ali Kuyaksil, Harun Köroğlu, "Türkiyede Meslekleşme Olgusu olarak Özel Güv. Hiz.", Polis ve Sosyal Bilimler Dergisi, Ekim 2005, Cilt:3, Sayı:2, s.83.

İnternet üzerinden iş ve bilgi iletişim süreçleri ilerledikçe güvenlik sistemlerine olan ihtiyaç giderek daha hayati bir öneme sahip olmaya başlamaktadır. E-ticaret, tedarik zinciri yönetimi, uzaktan erişim gibi internet olanaklarının iş süreçlerini kolaylaştır. Yüksek hızlı, ses veri görüntü taşıyan çoğul ortam uygulamalarının da haberleşme sistemlerine katılımıyla bu alanda yapılan yatırım maliyetleri artmış bunun gereği olarak güvenlik de bir parametre olarak en yüksek yatırım ve maliyet kalemlerinden biri olarak ortaya çıkmıştır.[13]

Türkiye'de faaliyet gösteren bankaların birçoğu müşterilerine internet üzerinden de hizmet vermektedir. Ülkemizde ilk internet bankacılık hizmeti 1997 tarihinde İş Bankası tarafından verilmeye başlanmıştır. Oldukça yeni olan bu dağıtım kanalında ilk yıllarda kayıtlı dolandırıcılık eylemi oldukça azdır. Son dönemde, bu konudaki yasal boşluklar internet bilgi hırsızları (hacker) tarafından fark edilmiş kötü niyetli girişimler ve saldırılar başlamıştır. İnternet bankacılığı dolandırıcılık eylemlerindeki ortak kurgu; müşterinin özel bilgilerinin, kullanıcı bilgisayarından çeşitli yöntemlerle çalınması ve bu bilgilerin kullanılarak müşteri adına internet üzerinde işlem yapılmasıdır. İnternet üzerinden gerçekleştirilen dolandırıcılık eylemlerindeki artış, bankaların eylemlerden zarar gören müşterileri ile sorunlar yaşamasına neden olmuştur. Bu dönemde, Türkiye Bankalar Birliği nezdinde üye bankaların etik ilkeler ve yasal mevzuatlara uygun olarak birlikte hareket etmesi için gerekli ortamın yaratılması, bankalar arası iletişimin artması ve Emniyet Genel Müdürlüğü ile koordineli hareket edilmesine gayret edilmiştir. Bu platforma üye bankaların güvenlik birimleri, internet mağduru olan müşteri şikâyetini ilgili bankalara bildirerek diğer bankaların da önlem almalarını sağlamaktadır. Bankaların Emniyet Genel Müdürlüğü bilgisi dâhilinde ortak hareket etmesi, dolandırıcılık girişimlerinin ve müşteri mağduriyetinin azaltılmasına katkıda bulunmuştur. Ayrıca internette bankacılık hizmeti veren bankaların almış oldukları ek güvenlik önlemleri saldırı adedinin düşürülmesine yardımcı olmuştur.[14]

13 Hakan Kaptan, "Bilişim Güvenliği", 2006, http://www.artifex.com.tr/Content_Articles/Default.asp?articleId=14, (30 Eylül 2007)
14 TBB, a.g.e, s.6.

2000'li yıllardan itibaren, internet bankacılığı müşterilerine hackerlar tarafından ciddi sayıda saldırı düzenlenmektedir. Sayısı hızla artan kötü niyetli yazılımlar internet bankacılığı müşterileri açısından önemli bir sorun haline gelmektedir.[15]

Teknoloji bir yandan hayatımıza yeni bir yaşam tarzı getirirken diğer yandan yeni suç şekilleri yaşamımıza girmeye başlamıştır. Bilgisayar suçları, dijital suçlar, internet suçları, siber suçlar, ileri teknoloji suçları, ağ suçları gibi yeni terimler kullanılmaya başlanmıştır.

Bilişim kelimesi bilgisayar, bilgisayar teknolojileri ve iletişim teknolojilerini kapsadığından bu ortamda gerçekleşen ve değişik şekillerde adlandırılan bu suç türleri ''Bilişim Suçları ''olarak adlandırılmaktadır.[16]

## 1.2. SERVİS SAĞLAYICILARI

### 1.2.1 İnternet Erişim Sağlayıcılar ( Internet Access Provider – IAP)

İnternet Erişim Sağlayıcı, kullanıcıların internet ağına erişmelerini sağlayan internet bağlantısıdır. Başkasına ait içeriklere ulaşılmasına yalnızca aracılık etmektedirler. Erişim sağlayıcı doğrudan internet bağlantısına sahiptir.[17]

### 1.2.2 İnternet Servis Sağlayıcılar ( Internet Service Provider- ISP)

İnternet Servis Sağlayıcılar, internete bağlanmak isteyen kişiler ile internet arasında köprü görevini yürüten kuruluşlardır. Kullanıcı, bir internet servis sağlayıcı kuruluşu ile internet ağına dâhil olmaktadır.

İnternet Servis Sağlayıcıları, kullanıcıların internete ulaşabilmeleri için kendi bilgisayarlarını bir giriş kapısı olarak kullanan internet kuruluşudur. Belirli bir alt yapı

15 TBB, a.g.e,s.5-6.
16 Murat Yılmaz, "Bilişim Suçları Hakkında", 2001, http://www.olympos.org/article/articleview/261/1/2, (1 Eylül 2007)
17 Sait Güran, Teoman Akünal, Köksal Bayraktar, Erdener Yurtcan, Abuzer Kendigelen, Önder Beller, Sezer Bülent , "İnternet ve Hukuk Temel Metni", 2002, http://www.sosyalbil.selcuk.edu.tr/sos_mak/makaleler ,(18 Eylül 2007), s.614.

kurarak sahip oldukları doğrudan internet bağlantısını bir ücret karşılığı kullanıma açarak internete erişim olanağı sağlamaktadırlar. [18]

### 1.2.3 İnternet İçerik Sağlayıcılar ( Internet Content Provider- ICP)

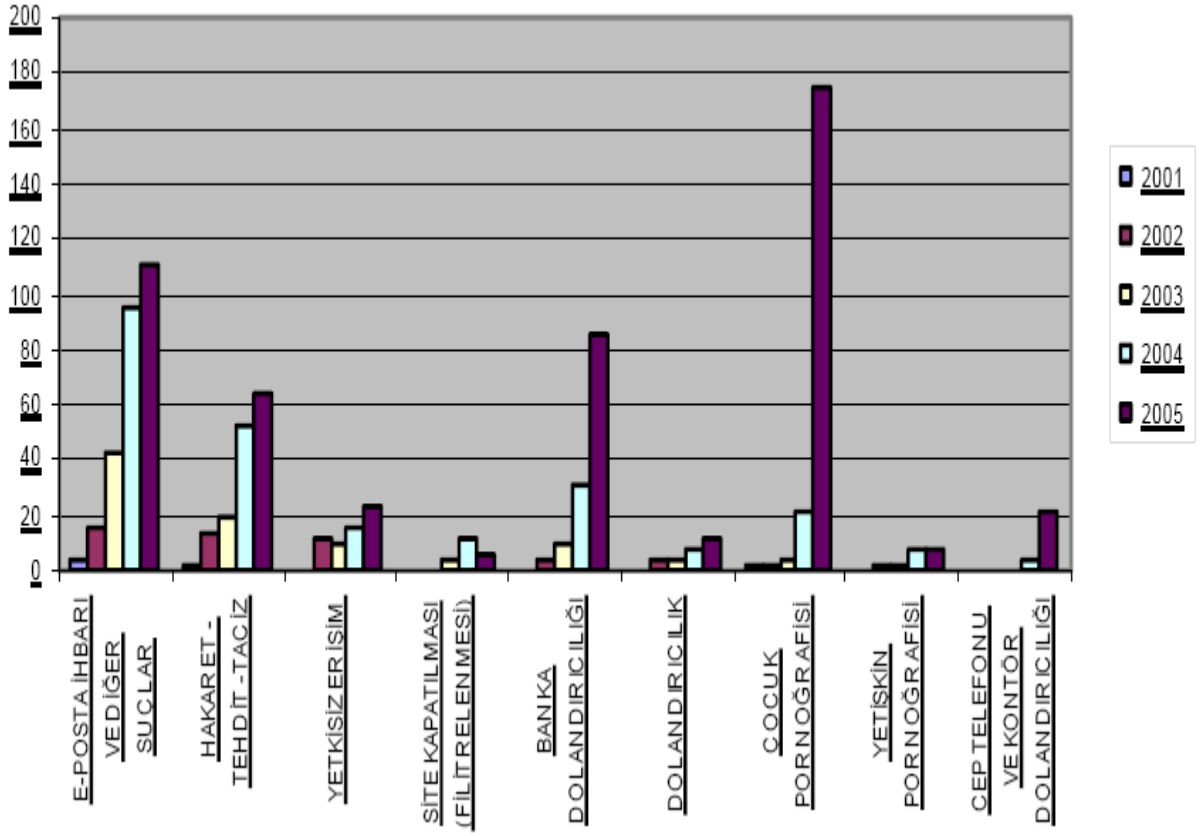
İnternet İçerik Sağlayıcı, bir bilgi ya da belgeyi internet ortamında yayınlanacak şekilde düzenleyen kişi ya da kuruluşlardır. Bilgiyi üreten konumundadır. Bir web sayfasının içeriğini hazırlayıp internete gönderme işlemini de servis sağlayıcı aracılığıyla gerçekleştiren, içerik sağlayıcıdır. Bir dosya ya da bilgiyi kullanıcıların kendi bilgisayarlarına yükleme hizmeti verirler. İçerik sağlayıcılar, forumlarda başkaları tarafından gönderilen mesajları yazma ve gerek gördüğünde kendisine ait mesajları silebilme imkanına sahip bulunmaktadırlar.[19]

### 1.2.4 Kullanıcılar

İnterneti etkin ve yararlı bir biçimde kullanmak suretiyle bilgi toplumunu oluşturacak bireylerin her birisi kullanıcıdır. Kullanıcılar gerçek veya tüzel kişiler olabilmektedirler. İnternette yayınlanmakta olan bilgi ve belgeleri izleyebilir, okuyabilir ve kendi bilgisayarlarına yükleyebilirler. Kullanıcılar, İnternet Ceza Hukukunun hem sanık hem de mağdurlarıdır. İnternet ortamında veya internet kullanılarak işlenen suçlar da internet suçu olarak adlandırılmaktadır.[20]

18 Hasan Sınar, "İnternet ve Ceza Hukuku", İstanbul: Beta Yayınları, 2001, s.42.
19 Önder Demir, " İnternet Servis Sağlayıcısının Cezai Sorumluluğu".İzmir Barosu Dergisi, 2000, Sayı:3, s.3
20 Demir, a.g.e, s.3.

**Ülkemizde 2001–2005 Tarihlerinde İşlenen Bilişim Suçları ve İstatistikleri(Adet)**




**Grafik 1.**Yıllara Göre Bilişim Suçları İstatistikleri

**Kaynak:** Mehmet Dalyan, **“** Siber Suçlar ve Acil Durum Yönetmeliği” , 01.07.2006, http://dalyanda.com/wp- content/uploads/2006/06/ MehmetDalyanda_SiberSuclar_ve_ AcilDurumYonetimi_Haziran2006.pdf, (1 Mayıs 2008)

İnternet şube kullanan müşterisi sayısı gün geçtikçe artmaktadır. Türkiye Bankalar Birliği' ne üye olan 46 bankanın 26'sından alınan verilere göre Nisan-Haziran 2007 döneminde internet bankacılığı hizmetleri için kayıtlı bireysel müşteri sayısı 18.066.542 olmuştur. Bu dönemde 3.156.279 bireysel müşteri tarafından en az bir kez internet bankacılığı işlemi yapılmıştır. Bu miktar, toplam kayıtlı bireysel müşteri sayısının yüzde 17'sini oluşturmaktadır. Nisan-Haziran 2007 döneminde, aktif bireysel müşteri sayısında bir önceki yılın aynı dönemine göre 677.756 adet, bir önceki üç aylık döneme göre ise 96.706 adet artış olmuştur. Aynı dönemde kayıtlı bireysel müşteri sayısında bir önceki yılın aynı dönemine göre 2.698.336 adet, bir önceki üç aylık döneme göre ise 681.179 adet artış olmuştur. Aktif müşteri sayısı arttıkça internet dolandırıcılarının saldırılarında hızla artış görünmektedir. İnternet şube kullanımı verileri aşağıdaki tabloda yer almaktadır. [21]

21 İnternet Bankacılığı İstatistikleri, 14.08.2007, //www.tbb.org.tr/net/dönemsel/, (14 Eylül 2007)

**Tablo 1**

**Nisan - Haziran 2007 Döneminde İnternet Bankacılığı Kullanan Müşteri Sayısı(Adet)**

| | Haziran 2006 | Mart 2007 | Haziran 2007 | Net Değişim Nisan-Haziran 2006 dönemine göre | Net Değişim Ocak-Mart 2007 dönemine göre |
|---|---|---|---|---|---|
| **Bireysel müşteri sayısı** | | | | | |
| Aktif | 2.478.523 | 3.059.573 | 3.156.279 | 677.756 | 96.706 |
| Kayıtlı | 15.368.206 | 17.385.363 | 18.066.542 | 2.698.336 | 681.179 |
| **Aktif / kayıtlı müşteri oranı (yüzde)** | **16** | **18** | **17** | | |
| **Kurumsal müşteri sayısı** | | | | | |
| Aktif | 355.700 | 404.350 | 421.734 | 66.034 | 17.384 |
| Kayıtlı | 752.797 | 852.838 | 926.945 | 174.148 | 74.107 |
| **Aktif / kayıtlı müşteri oranı (yüzde)** | **47** | **47** | **45** | | |
| **Toplam müşteri sayısı** | | | | | |
| Aktif | 2.834.223 | 3.463.923 | 3.578.013 | 743.790 | 114.090 |
| Kayıtlı | 16.1.003 | 18.238.201 | 18.993.487 | 2.872.484 | 755.286 |
| **Aktif / kayıtlı müşteri oranı (yüzde)** | **18** | **19** | **19** | | |

**Kaynak:** İnternet Bankacılığı İstatistikleri, 14.08.2007, //www.tbb.org.tr/net/dönemsel/, (14 Eylül 2007)

**Tablo 2**

**Ekim - Aralık 2007 İnternet Bankacılığını Kullanan Müşteri Sayısı (Adet)**

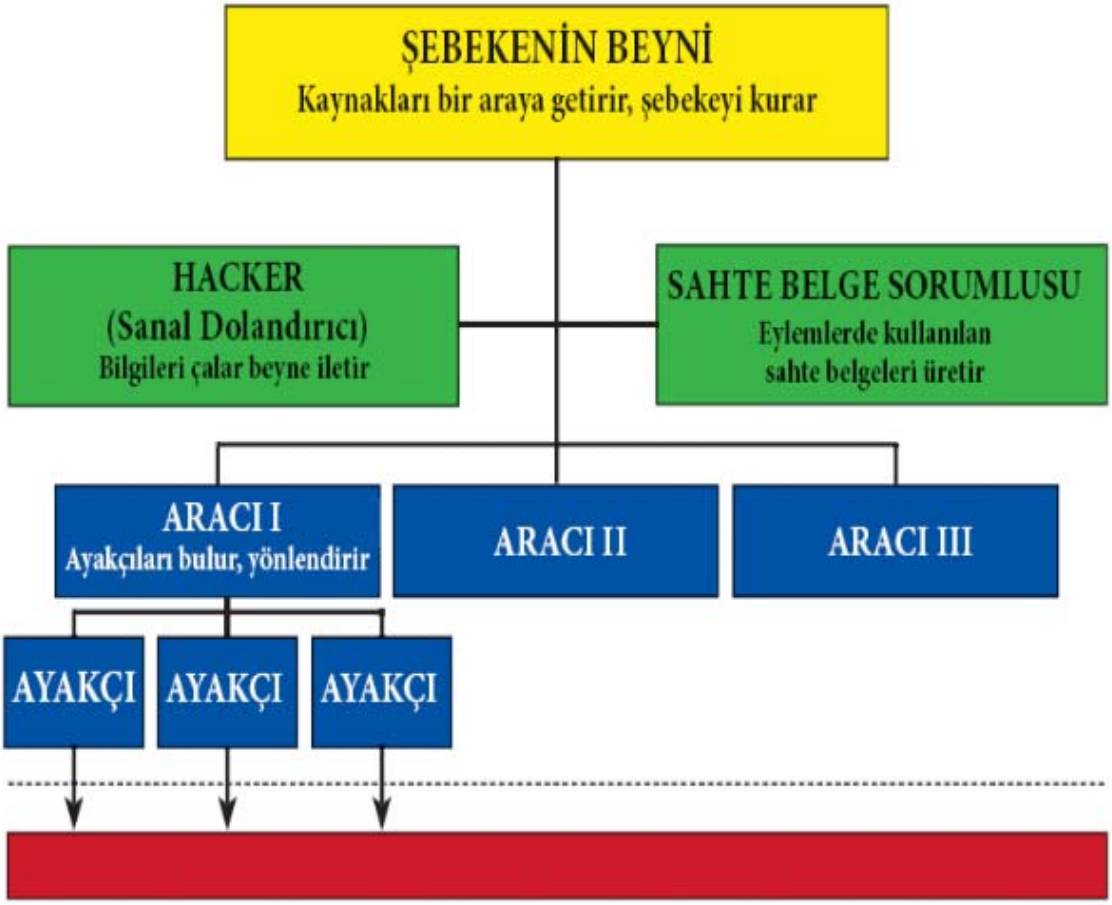
| | Aralık 2006 | Eylül 2007 | Aralık 2007 |
|---|---|---|---|
| **Bireysel müşteri sayısı** | | | |
| Aktif (A) *(son 3 ayda 1 kez login olmuş)* | 2.976.292 | 3.551.347 | 3.795.627 |
| Kayıtlı (B) *(en az 1 kez login olmuş) (*)* | - | 8.558.033 | 8.908.956 |
| Kayıtlı (C) *(son 1 yılda en az 1 kez login olmuş) (*)* | - | 5.426.713 | 4.920.907 |
| **Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)** | **-** | **41** | **43** |
| **Kurumsal müşteri sayısı** | | | |
| Aktif (A) *(son 3 ayda 1 kez login olmuş)* | 391.565 | 466.934 | 478.737 |
| Kayıtlı (B) *(en az 1 kez login olmuş) (*)* | - | 1.097.752 | 1.131.302 |
| Kayıtlı (C) *(son 1 yılda en az 1 kez login olmuş) (*)* | - | 661.803 | 588.211 |
| **Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)** | **-** | **43** | **42** |
| Toplam müşteri sayısı | | | |
| Aktif (A) *(son 3 ayda 1 kez login olmuş)* | 3.367.857 | 4.018.281 | 4.274.364 |
| Kayıtlı (B) *(en az 1 kez login olmuş) (*)* | - | 9.655.785 | 10.040.258 |
| Kayıtlı (C) *(son 1 yılda en az 1 kez login olmuş) (*)* | - | 6.088.516 | 5.509.118 |
| **Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)** | **-** | **42** | **43** |

**Kaynak:** İnternet Bankacılığı İstatistikleri, 25.01.2008, //www.tbb.org.tr/net/donemsel/, (01 Şubat 2008)

İnternet bankacılığı için kayıt yaptıran ve en az bir kez "login olmuş" toplam (bireysel ve kurumsal) müşterilerin yüzde 43'ü Ekim-Aralık 2007 döneminde en az bir kez internet bankacılığı işlemi yapmıştır. Ekim-Aralık 2007 döneminde, toplam aktif müşteri sayısında bir önceki yılın aynı dönemine göre 906.507 adet, bir önceki üç aylık döneme göre ise 256.083 adet artış olmuştur.

### 1.3. İNTERNET DOLANDIRICILIĞI ÇETE YAPISI

İnternet dolandırıcılığı için şubelere gelenler genellikle eğitim düzeyi düşük, işsiz ve daha önce sabıkası olmayan şahıslardır. Şubelere internet dolandırıcılığı vasıtasıyla gönderilen tutarları almaya gelen kişilere 'ayakçı' denir. 'Aracı' ayakçı adı veren kişileri bulan ve şubeye getiren kişilerdir.




**Şekil 1:** İnternet Dolandırıcılığıyla Amacıyla Kurulan Bir Şebekenin Organizasyon Yapısı
**Kaynak:** Türkiye Bankalar Birliği İnternet Bankacılığı Çalışma Grubu, Nisan 2007, s.7., www.tbb.org.tr/v/doc/Kitapçık.pdf , (28 Eylül 2007)

Ayakçılar, aracılar tarafından sadece bir, iki eylemde kullanılır. Banka şubesinde hesap açarak, açılan hesaba gelen parayı çekip aracıya veren ayakçılar, yapmış oldukları bu iş karşılığında ele geçirmiş oldukları tutarın oldukça önemsiz bir kısmını komisyon olarak almaktadır. Yakalanan şahıslardan alınan istihbarat doğrultusunda, şebeke içerisinde kanun dışı yollardan elde edilen paranın paylaşımı ortalama olarak aşağıdaki gibidir.

Ayakçı: 50 – 100 USD

Aracı : % 10 - %20

Sahte Belge Sorumlusu: 50 – 100 USD

Sanal Dolandırıcı (Hacker) : % 20 - %30

Beyin: : %50 - %70

# 2. KİŞİSEL BİLGİLERİN ÇALINMASI

İnternet bilgi hırsızları çeşitli yöntemlerle müşterilerin özel bilgilerini ele geçirmektedirler. Bu yöntemlerden en çok kullanılanlar; Truva Yazılımlar, Keylogger( Tuş Kaydedici) , Sahte Siteler ve Phishing (Olta Saldırıları)' dır.

## 2.1. TRUVA(TROJEN) YAZILIMLAR

"Truva yazılımları" isimlerini "Truva atından" almaktadırlar. Tecrübesiz ve bilgisi yeterli olmayan bir kullanıcıya faydalı ve ilginç gibi görünen, ancak bilgisayara yüklenip çalıştırıldığında zarar veren yazılımlardır. Sanal dolandırıcılar tarafından zararsız bir programın (oyunlar, anlık bilgi veren yazılımlar vb) içine ek olarak yerleştirilebilir veya korsan bir "Truva yazılımının" başka bir obje olarak görünmesi sağlanabilir. Örneğin; kullanıcı, hava durumu ile ilgili anlık bilgi veren bir program indirdiğini zannederken aslında bir "Truva yazılımını" indirmiş olabilir.

## 2.2. KEYLOGGER (TUŞ KAYDEDİCİ)

Bilgisayar kullanıcılarının internette dolaşırken, klavye kullanarak girdikleri bilgileri kaydeden ve bu bilgileri kötü niyetli kişilere gönderen yazılım türüne keylogger(tuş kaydedici) denir. Keylogger(Tuş Kaydedici) yazılımları; uzaktan erişime açık, yeterince korunmayan bilgisayarlara sanal dolandırıcılar tarafından yüklenebileceği gibi kullanıcı tarafından oyunlar, e-postalar vb. yollarla farkında olmadan da yüklenebilir. Keylogger(Tuş Kaydedici) yüklenmiş bir bilgisayardan internet şubesine giriş yapıldığında kullanılan tüm bilgiler sanal dolandırıcılar tarafından ele geçirilebilir.[22]

Keylogger(Tuş Kaydedici) internet üzerinde mevcut bazı resim veya programların içerisine saklanarak ya da internet üzerindeki web sitelerinin gezilmesi sırasında mağdur bilgisayarına mağdurun bilgisi dışında yüklenmesi sağlanır. Program, mağdur bilgisayarında aktif hale geldiği andan itibaren çalışmaya başlar. Klavye ile yazılan bütün bilgileri mouse ile tıklanan ya da mouse' un üzerinde uzun süre beklenen bölgelerin resimlerini kaydederek rapor haline getirir ve bu rapor zararlı yazılımı derleyen veya yazan kişilere internet aracılığı ile gönderilir. Bu sayede programı mağdur bilgisayarlarına bulaştırmak üzere yayan kişiler, mağdur bilgisayarından yapılan bütün e-posta, bankacılık ve finans, özel şifreleri ve diğer bütün şifreleri ele geçirebilmektedirler.[23]

### 2.2.1 Keylogger (Tuş Kaydedici) Türü Yazılımların Sisteme Girmesi

**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(tuş kaydedici) yazılımları sisteme yüklenirler.

---

22 TBB, a.g.e, s.8.

23 Kürşad Başoğlu, "Teknolojiye Boyun Eğmeyin( Bilişim Suçlarına Genel Bakış)",10.09.2007, www.bilisimsuclari.com/2007/09/10 , (17 Kasım 2007)

**2)** Keylogger(Tuş Kaydedici) yazılımı bilgisayara kullanıcı tarafından yüklenebilir:

Örneğin; güvenilmeyen bir bilgisayarda bilgisayar sahibi tarafından sisteme başkaları tarafından giriş yapılması halinde (login olunması) ne gibi işlemler yapıldığı bilgisayar sahibi tarafından bilinmek istenebilir. Bu durumda sisteme yüklenecek bir keylogger(tuş kaydedici) yazılımı ile bilgisayarda başka kullanıcıların yaptıkları bütün işlemler kaydedilmiş olur. Eğer bilgisayar pek çok kişiye açık bir ağda ise bilgisayarda yapılan bütün işlemler keyloggerı(tuş kaydedici) yükleyen kişi tarafından öğrenilebilir.

Ayrıca işletim sistemlerinde tespit edilen açıklarla sisteme rahatlıkla uzaktan müdahale edilebilmekte ve bu müdahalelerin başında sisteme dosya aktarma, aktarılan dosyayı çalıştırma gibi işlemlerle sonrasında kullanıcılar takip edilebilmektedir.

Keyloger(tuş kaydedici) ve benzeri programlardan etkilenmemek için aşağıdaki güvenlik önlemlerine uyulmalıdır:

— İşletim sisteminin güncelleştirmeleri yapılmalıdır,

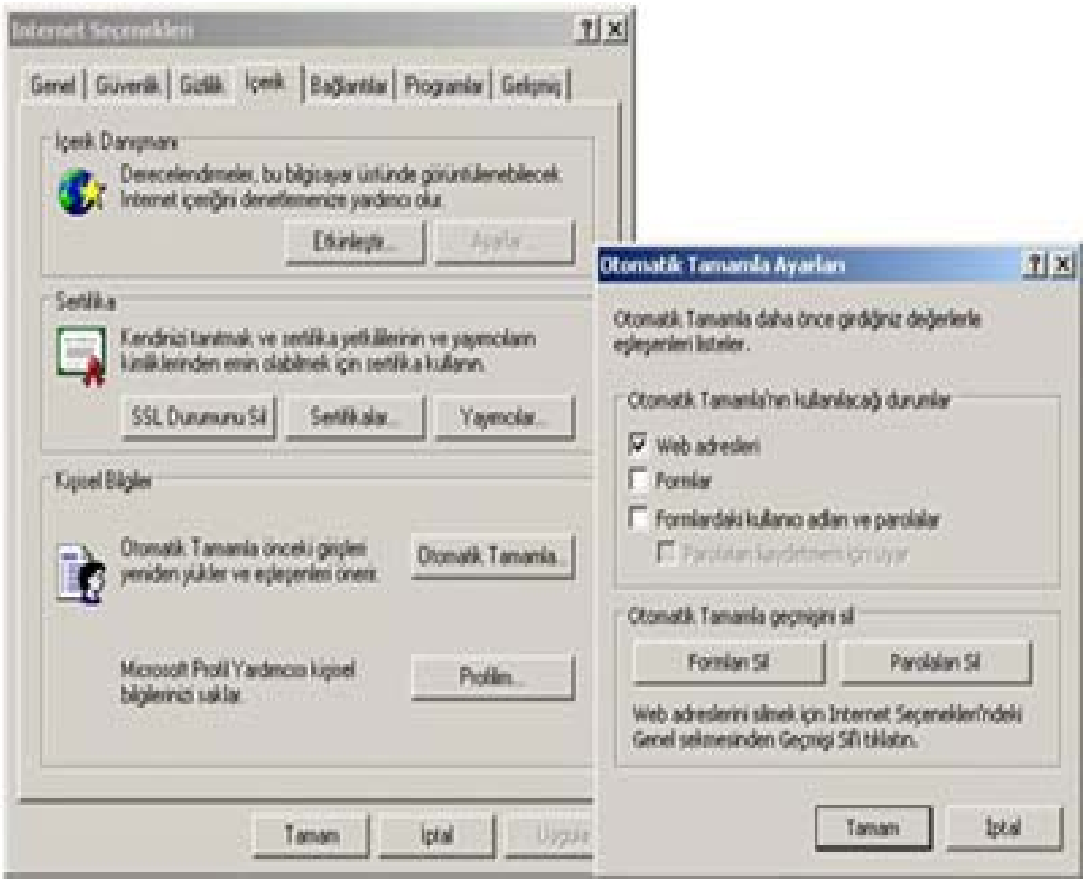
— Bilgisayarda güncel ve aktif anti virüs programı bulunmalıdır,

— Bankacılık ve önemli işlemler güvenli olmayan bilgisayarlardan yapılmamalıdır,

—Bilgisayarın web browserı(internet tarayıcısı)'nın otomatik tanımlama özelliğindeki "Formlarda kullanıcı adları ve parolalar" ile ilgili kısmın işaretsiz olmasına dikkat edilmelidir..

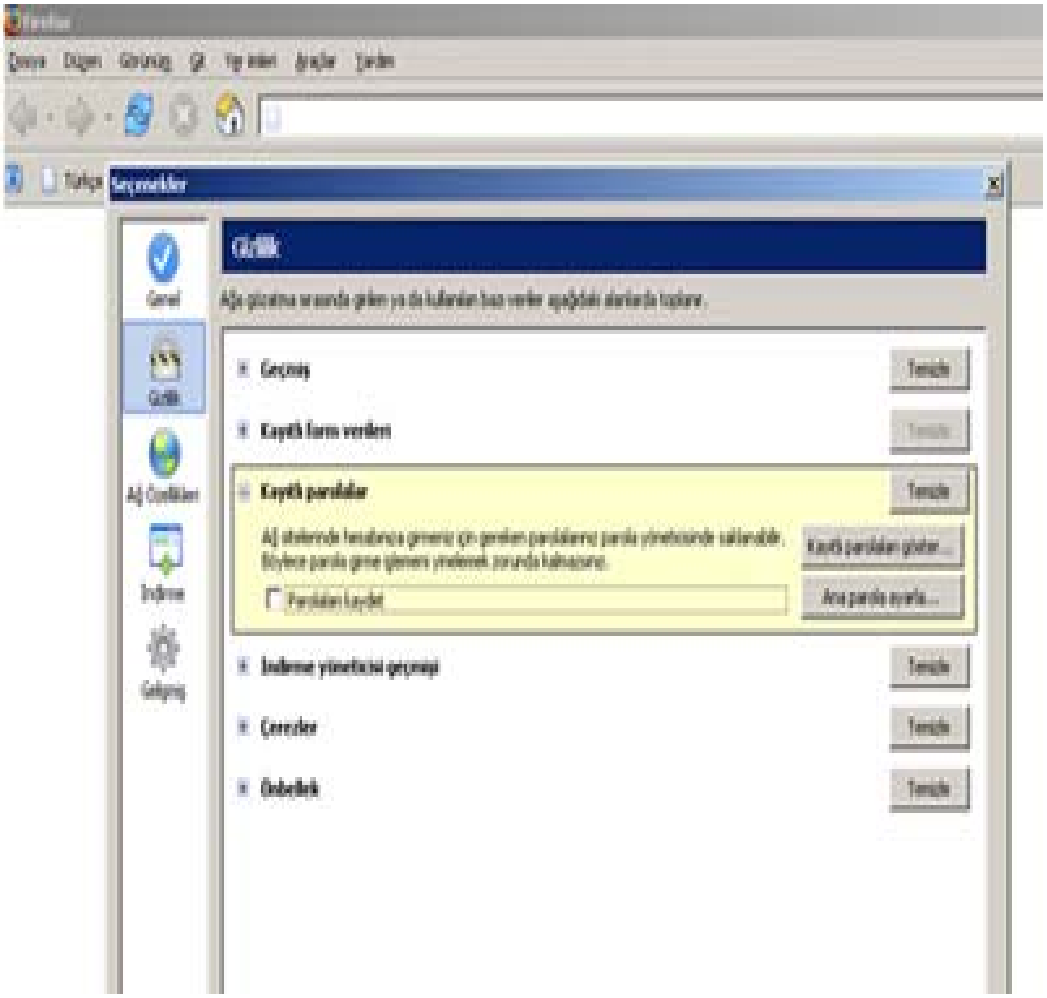
"Formlarda kullanıcı adları ve parolalar" bölümüne aşağıdaki şekilde giriş yapılmalıdır.[24]

24 Mustafa Sansar, "Sanal Dolandırıcılıkta Son Nokta Phıshıng" ,31.10.2007 , http://www.iem.gov.tr/iem/?menu_id=1&detay_id=68 ,(24 Kasım 2007)




**ŞEKİL 2:** İnternet Explorer 6.0 için ( Araçlar->İnternet Seçenekleri->İçerik->Otomatik Tamamla)

**Kaynak:** Mustafa Sansar, "Sanal Dolandırıcılıkta Son Nokta Phıshıng" ,31.10.2007 , http://www.iem.gov.tr/iem/?menu_id=1&detay_id=68, (24 Kasım 2007)



**ŞEKİL 3:** Firefox 1.0 PR İçin ( Araçlar -> Seçenekler -> Gizlilik)

**Kaynak:** Mustafa Sansar, "Sanal Dolandırıcılıkta Son Nokta Phıshıng" ,31.10.2007 , http://www.iem.gov.tr/iem/?menu_id=1&detay_id=68 , (24 Kasım 2007)

## 2.3. SCREENLOGGER (EKRAN KAYDEDİCİ)

Keylogger(Tuş Kaydedici) ile aynı prensipte çalışan ve klavye tuşları yerine ekran görüntülerini kaydeden yazılım türüne screenlogger denir.

Screenlogger(Ekran Kaydedici) programlar sanal klavyeden şifre girilirken kaydedilen ekran görüntülerini; yazılımı hazırlayan kişilere istediği anda, istediği oranda göndererek kullanıcının sanal klavyeyle ulaşabilme imkanı vermektedir.[25]

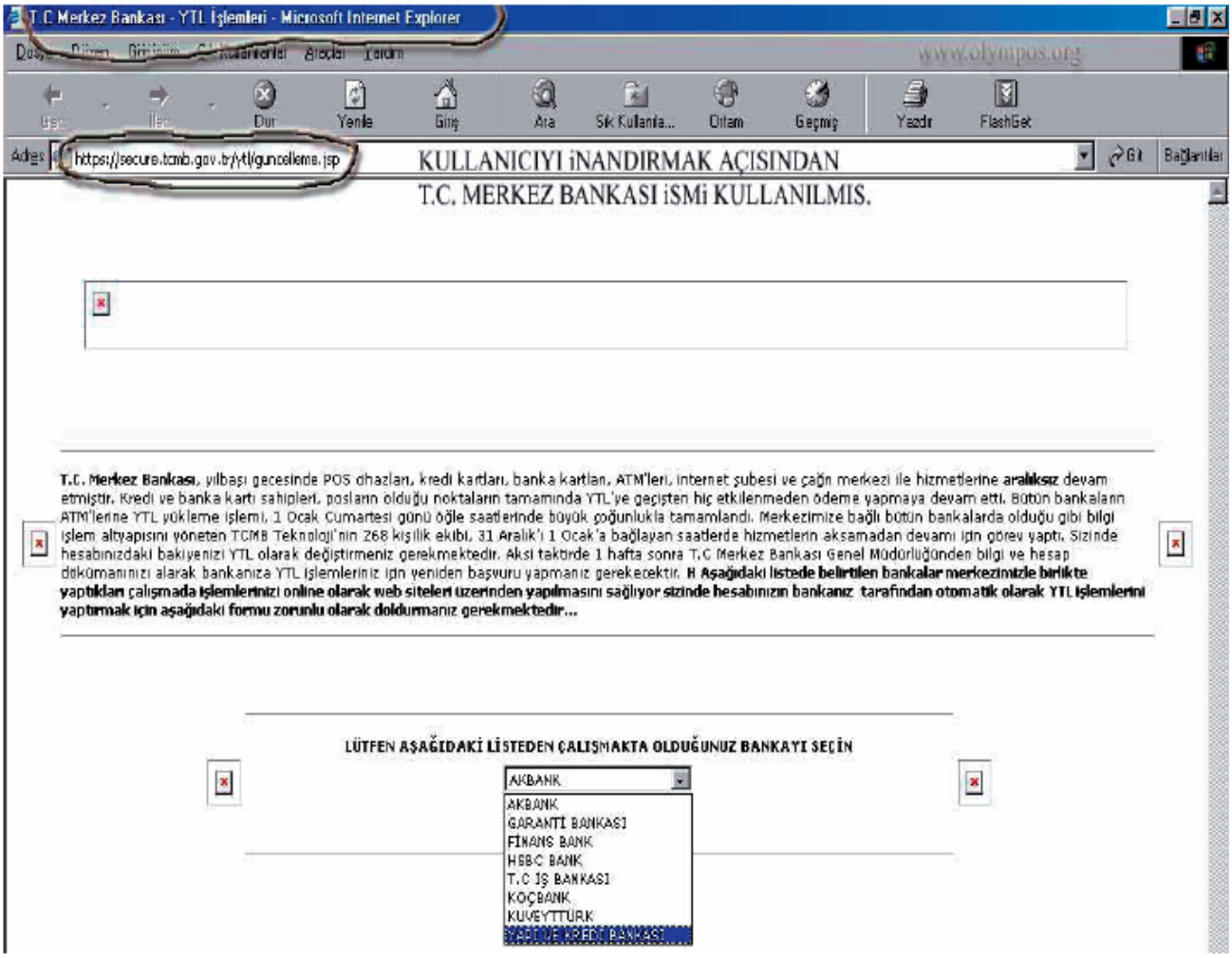
Kullanıcının Mouse ile tıkladığı her anın resmini çekerek kaydeden bu programlar sayesinde sanal dolandırıcılar sanal klavye kullanılarak girilen bilgileri de ele geçirebilirler. Ekran görüntülerini anlık resimler yerine film gibi hareketli görüntüler olarak kaydeden veya bilgisayarda kayıtlı tüm bilgilere erişim sağlayan "trojenler" de mevcuttur. Bu tarz yazılımların, özellikle "internet Kafe" gibi çok sayıda kişinin ortak kullandığı ve yeterli güvenlik önlemi alınmamış bilgisayarlarda bulunma olasılıkları çok yüksektir.

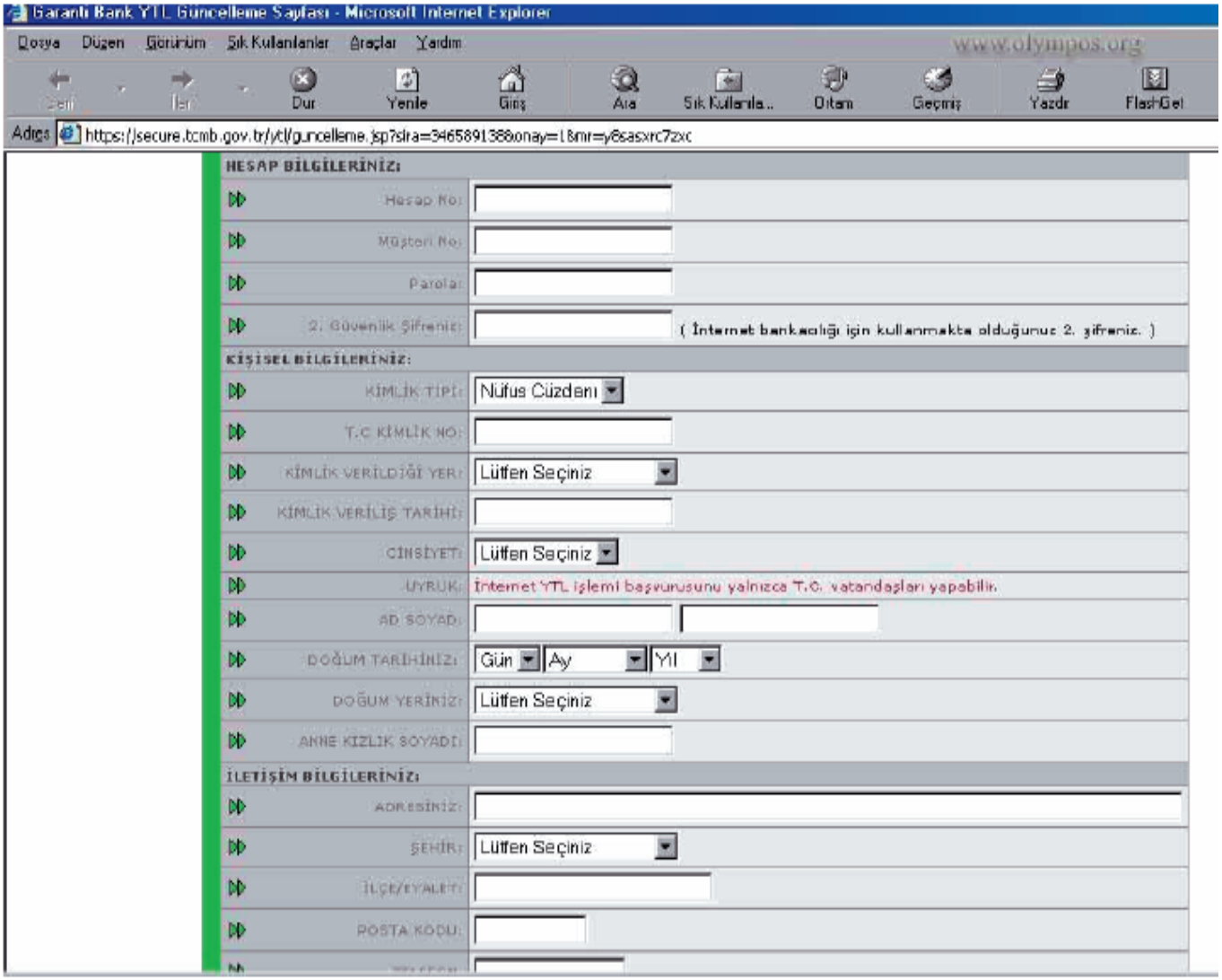
## 2.4. SAHTE SİTELER

Sanal dolandırıcılar tarafından hazırlanan özellikle banka ve finans kurumlarının sitelerinin görsel olarak benzerlerine sahte site denir. Hazırlanan bu sahte sitelere arama motorlarındaki reklâm destekleyici adreslerle ziyaretçi çekilebileceği gibi, gerçek sitenin adresinin çok benzeri bir adrese yerleştirilerek, kullanıcıların yanlışlıkla gelmeleri de beklenebilir. Ziyaretçileri sahte sitelere çekmek için en çok kullanılan"Phishing(Olta Saldırıları) yöntemidir".

Aşağıda yer alan örnekte TCMB sitesi gibi hazırlanmış sahte bir site yer almaktadır. Burada amaç müşterilerin kişisel bilgilerini ele geçirmektir.

25 R. Yılmaz Yazıcıoğlu, "Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi", Hukuk ve Adalet Eleştirel Hukuk Dergisi, İstanbul, Y:1, Sayı:1, Ocak-Mart 2004, s.172-185


T.C Merkez Bankası - YTL İşlemleri - Microsoft Internet Explorer
www.olympos.org
Dur
Yenile
Giriş
Ara
Sık Kullanıla...
Ortam
Geçmiş
Yazdır
FlashGet
Adres
https://secure.tcmb.gov.tr/ytl/guncelleme.jsp
Git
Bağlantılar
KULLANICIYI iNANDIRMAK AÇISINDAN
T.C. MERKEZ BANKASI iSMi KULLANILMIS.
T.C. Merkez Bankası, yılbaşı gecesinde POS cihazları, kredi kartları, banka kartları, ATM'leri, internet şubesi ve çağrı merkezi ile hizmetlerine aralıksız devam etmiştir. Kredi ve banka kartı sahipleri, posların olduğu noktaların tamamında YTL'ye geçişten hiç etkilenmeden ödeme yapmaya devam etti. Bütün bankaların ATM'lerine YTL yükleme işlemi, 1 Ocak Cumartesi günü öğle saatlerinde büyük çoğunlukla tamamlandı. Merkezimize bağlı bütün bankalarda olduğu gibi bilgi işlem altyapısını yöneten TCMB Teknoloji'nin 268 kişilik ekibi, 31 Aralık'ı 1 Ocak'a bağlayan saatlerde hizmetlerin aksamadan devamı için görev yaptı. Sizinde hesabınızdaki bakiyenizi YTL olarak değiştirmeniz gerekmektedir. Aksi taktirde 1 hafta sonra T.C Merkez Bankası Genel Müdürlüğünden bilgi ve hesap dökümanınızı alarak bankanıza YTL işlemleriniz için yeniden başvuru yapmanız gerekecektir. H Aşağıdaki listede belirtilen bankalar merkezimizle birlikte yaptıkları çalışmada işlemlerinizi online olarak web siteleri üzerinden yapılmasını sağlıyor sizinde hesabınızın bankanız tarafından otomatik olarak YTL işlemlerini yaptırmak için aşağıdaki formu zorunlu olarak doldurmanız gerekmektedir...
LÜTFEN AŞAĞIDAKİ LİSTEDEN ÇALIŞMAKTA OLDUĞUNUZ BANKAYI SEÇİN
AKBANK
AKBANK
GARANTİ BANKASI
FİNANS BANK
HSBC BANK
T.C İŞ BANKASI
KOÇBANK
KUVEYTTÜRK
YAPI VE KREDİ BANKASI




**Şekil 4:** TCMB Adı Kullanılarak Hazırlanmış Sahte Site

**Kaynak:** Türkiye Bankalar Birliği İnternet Bankacılığı Çalışma Grubu, Nisan 2007, s.10., www.tbb.org.tr/v/doc/Kitapçık.pdf , (28 Eylül 2007)

YTL para birimine geçişin sağlandığı dönemde, şekildeki sahte site, olta saldırısı amacıyla düzenlenmiş mailin içeriği çoğu bilgisayar kullanıcısını ikna edici özellikteydi. Olta saldırılarının tehlikesinden haberdar olmayan bir çok bilgisayar kullanıcısı online(çevrimiçi) bankacılık işlemlerindeki YTL değişikliğini yapabileceği düşüncesi ile; gönderen başlık kısmında "T.C. Merkez Bankası" yazan ve gönderen e-posta adresi olarak da " merkezbankasi@tcmb.gov.tr " e-posta adresli bu e-posta'nın tuzağına düşerek mağdur olmuşlardır.

E-Posta iletisinde; YTL para birimine yeni geçildiği belirtilmektedir ve herkesin kafasında birçok sorunun bulunduğu bir dönemde oldukça inandırıcı gözükmektedir. Sosyal mühendisliğin ikna ediciliği ve yanıltıcılığının iyi bir şekilde kullanıldığı bu e-postada açıkça görülmektedir. E-Posta iletisinde öncelikle iletiyi alana, iletide geçen bankaların YTL güncelleme işlemi olduğu vurgusu yapılmaktadır. Böylece insanların kafasında böyle bir güncellemenin varlığı konusunda karmaşıklık yaratılarak sosyal mühendisliğin ilk adımı başlatılmaktadır. Sosyal mühendislikte ilk önce sorun varmış gibi gösterip sonra çözüm yöntemi sunmak iyi ve her zaman tutarlılığı yüksek bir taktiktir. Sonrasında ise YTL güncelleme işlemlerinin ücretsiz olarak yapıldığı, bu işlemin iletide belirtilen internet adreslerinden veya Merkez Bankası Ankara şubesinden yapılabileceği vurgusu yapılmaktadır. Bu vurgu yine bir taktik olmakla birlikte, saldırgan çoğu insanın Merkez Bankası'nın Ankara Şubesi ile iletişim haline geçmesinin zor olacağını bilmekte ve bu yüzden de iletide geçen linkleri vurgulayarak insanların kafasında bir kolay yol olduğu kanaatini uyandırmaktadır. İstenilen formun doldurulması ile bilgiler kullanıcının bilgisayarından otomatik olarak kötü niyetli kişilerin bilgisayarlarına aktarılmış olacaktır.[26]

26 Ahmet Hakan Ekizer, "Oltaya Gelmeyin (Phishing Saldırıları)" 15.01.2007, http://www.ekizer.net/content/view/15/1/, (10 Ekim 2007)

## 2.5. PHİSHİNG (OLTA SALDIRILARI)

Sanal dolandırıcılar tarafından banka, kart şirketi veya resmi bir kurumdan geliyormuş gibi hazırlanan e-postaya phishing(olta saldırıları) denir. "Phishing saldırıları", internet suçları arasında en yaygın ve tehlikeli olanlarından biridir. Bu saldırıların amacı bireylerin veya kurumların finansal işlem yapmak için kullandıkları bilgileri çalmaktır. Hazırlanan e-postalar, elde edilen tüm e-posta adreslerine gönderir. E-postanın konusu, müşteri bilgilerinin güncellenmesi veya şifrelerin değiştirilmesi amacını içeren ifadelerden oluşur ve ilgili kurumun bire bir kopyası şeklinde görünen internet sayfalarına giden linklerden oluşur. Bazı müşteriler, tehlikenin farkında olmadan, adreslere tıklayarak istenilen bilgileri doldurur. Bunun sonucunda, müşterinin kişisel bilgileri ve şifreleri dolandırıcılar tarafından çalınmış olur.

Bankacılık hesaplarına yetkisiz giriş yaparak kar elde etmek isteyen 3. kişiler internet kullanıcılarına ilk bakışta herhangi bir bankadan gönderildiği düşünülen e-postalar göndererek enteraktif bankacılık hesaplarında güncelleme ve güvenlik ayarlarını yapmalarını istemekte ve e-posta gönderisinde bankanın internet adresine benzeyen fakat farklılıkları bulunan bir link vererek buradan sisteme giriş yapabilecekleri belirtilmektedir. Bu e-posta iletisini alan kullanıcılar istenilen güncellemeleri yapmak üzere belirtilen adrese tıklarlar ve karşılarına ilgili banka sayfasına çok benzeyen bir sayfa geldiğinden herhangi bir şüpheye düşmeden istenilen bütün bilgileri verirler ve bu bilgiler 3. şahıslara anında aktarılmış olur.[27]

— Phishing(Olta Saldırıları) metodu ile yapılan çevrimiçi(online) sahtekarlıklarda

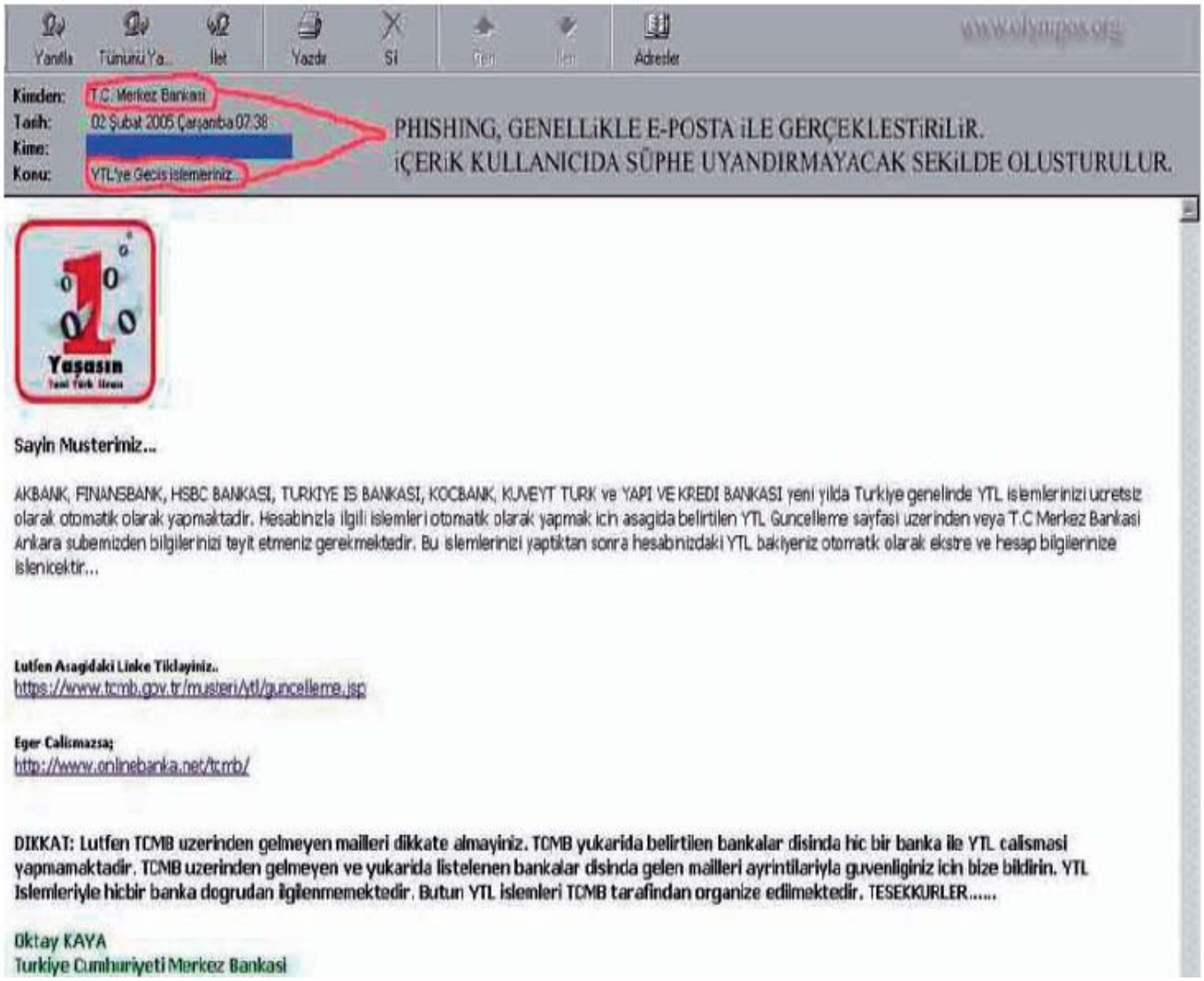
— Kredi, debit/ATM kart numaraları/CVV2

— Şifreler ve parolalar

— Hesap numaraları

27 Ahmet Pek, Emiyet Müdürü, "Şifre Operasyonu ve İnteraktif Dolandırıcılık", 25.5.2006, www.samsuntso.org.tr/Bilgi_Bankasi/interaktif_dolandiricilik.pdf, (24 Kasım 2007), s.1

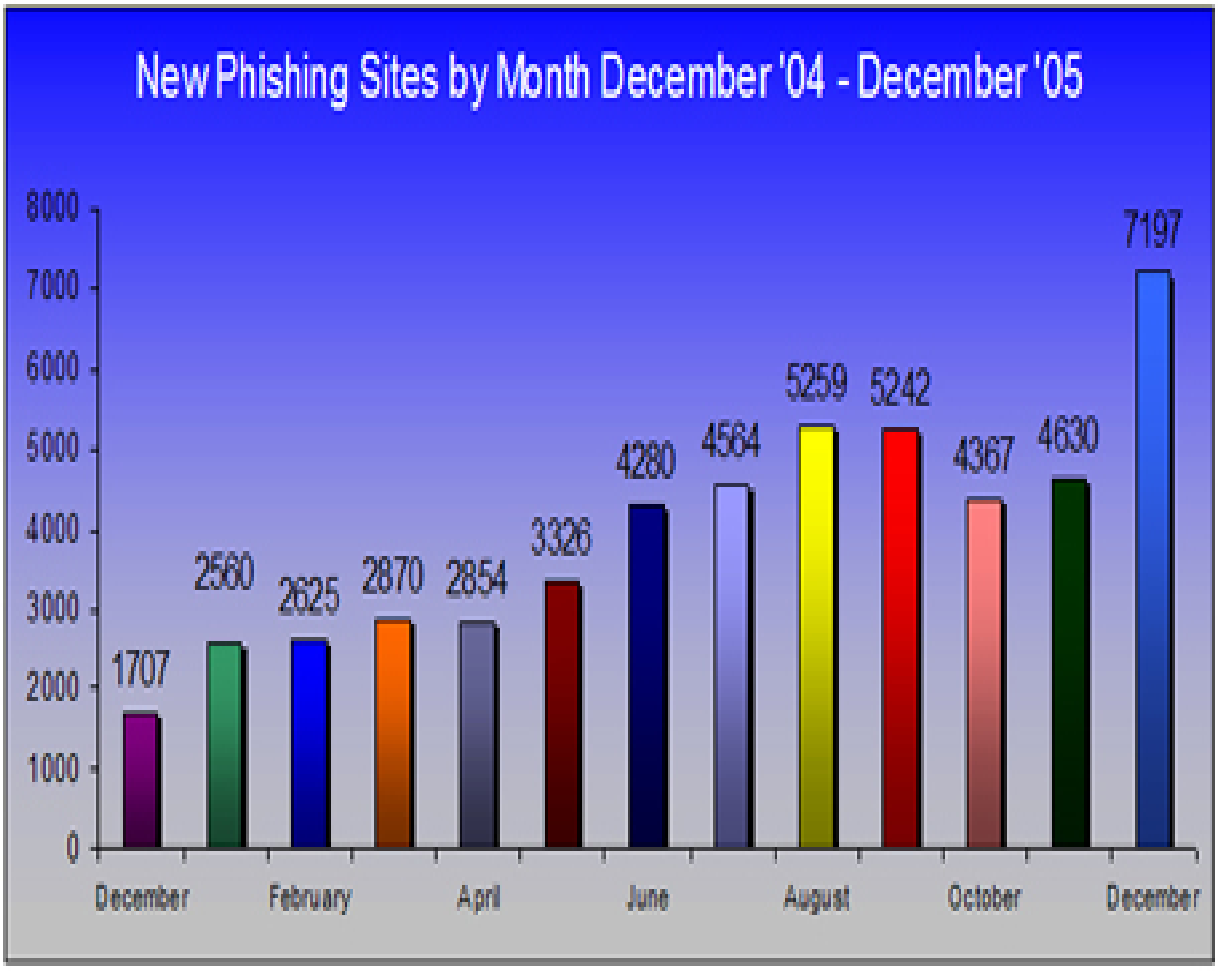
— İnternet bankacılığına girişte kullanılan kullanıcı kodu ve şifreleri gibi bilgiler ele geçirilir.



**Şekil 5:** PHİSİNG İçin Hazırlanmış Bir E-Posta Metni

**Kaynak:** Türkiye Bankalar Birliği İnternet Bankacılığı Çalışma Grubu, Nisan 2007, s.., www.tbb.org.tr/v/doc/Kitapçık.pdf , (28 Eylül 2007)

Uluslararası bir organizasyon olan Anti-Phishing Çalışma Grubunun(Sızdırma Dolandırıcılığı Karşıtı Çalışma Grubu) tarafından , Aralık 2004 – Aralık 2005 tarihleri arasındaki bir senelik olta saldırı adetleri araştırılmıştır. Anti-Phishing Working Group(Sızdırma Dolandırıcılığı Karşıtı Çalışma Grubu), phishing saldırılarının ve e-posta yoluyla gerçekleştirilen sahtekarlıkların, bilgi paylaşımı ve endüstride bu konuda geliştirilen çözümlerin tanınması ve uygulanması yoluyla ortadan kaldırılmasına yönelik faaliyet göstermektedir. Gruba, finansal kurumlar, hukuk ajansları, kamu politikalarını belirleyen gruplar ve çözüm sunucu firmalar üye olmaktadır. Şemaya bakıldığı zaman devamlı bir artış gözlenmektedir. Özelikle yeni yıl olan 2006 yılına geçilen ve 2005 yılının son ayı olan aralık ayında olta saldırıları sitelerinde büyük artışlar dikkati çekmektedir. Bunun sebebi ise saldırganların yeni bir finansal yılın devreye girmesini fırsat bilmesi ve gün geçtikçe olta saldırılarının bilgisayar korsanları tarafından popüler olarak kullanılmasıdır.




**Grafik 2.** Aylara Göre Phishing (Olta Saldırıları) Adetleri

**Kaynak:** Ahmet Hakan Ekizer, Hackerler, Yöntemleri ve Araçları,http://www.ekizer.net**,** (17 Kasım 2007), s.13

### 2.5.1 Phishing (Olta Saldırıları)n Dolandırıcılığının Aşamaları

Genel olarak bütün phishing(Olta Saldırıları) dolandırıcılıkları aynı aşamaları takip ederek işlerler. Bu aşamalar sırasıyla; "Planlama", "Hazırlık", "Yemleme", "Toplama", "Dolandırma" ve "Dolandırma Sonrası İşlemler" olarak 6 ana kısma ayrılır.

#### *2.5.1.1 Planlanma Aşaması*

Saldırının ilk aşaması olan planlama, hedef firmanın seçimi, kurban profilinin seçimi ve saldırı tipinin tercihi gibi kilit bazı kararların alındığı kısımdır. Saldırıyı gerçekleştirecek olan dolandırıcı işe ilk olarak popüler ve müşterisi fazla olan bir kurumu seçmek ile başlar. Bu kurumun internet sitesinde bulunan zaafların fazlalığı saldırganın işini kolaylaştırmanın yanında aynı zamanda saldırının başarısı açısında da önemlidir. Ayrıca saldırının konusunu oluşturacak firmanın hesaplarından yapılacak para transferlerinin izlenmemesi ya da firmanın bazı kilit işlemleri kayıt altına almıyor olması saldırganın saldırı esnasında ve sonrasında gizli, isimsiz kalmasında büyük fayda sağlamaktadır. Bu da hedef seçimini bu açıkları barındıran firmalara doğru kaydırır.

Hedef firma seçildikten sonra kurban seçimine geçilir. Bu aşamada hedef olarak seçilen firmanın genel müşteri profili izlenir ve bu profile uygun bir saldırı planlanır. Müşteri profili gençler olan bir firma hedef olarak seçilmişse, yapılacak yemleme esnasında kullanılacak e-posta listesinin gençlerin daha çok bulunduğu sitelerden elde edilmiş bir liste olması saldırının başarı şansını artıracaktır.

Kurban profili seçildikten sonra sıra hedef firma ve kurban profili göz önüne alınarak seçilecek olan saldırı türüdür. Saldırı türü seçiminde ana kıstas hedef firmanın sitesindeki bulunan zaaflar ve bu zaafların kullanımıdır. Genel olarak kabul görmüş üç farklı saldırı türü vardır. Bunlar; Taklit Saldırılar, Direkt e-posta Saldırılar ve Popup(açılan küçük pencere) Saldırıları'dır.

**— Taklit Saldırılar**

Hedef sitenin birebir aynısını ya da çok benzer bir taklidini yapmak olarak açıklanabilecek bu saldırı türünde hedef sitenin bütün bir kopyası bazı belirli programlar vasıtası ile alınır. Sonra bu kopyada girilen bilgileri toplayıp asıl çalışan sisteme geri döndürecek toplayıcı sistemi oluşturulur. Bu türün özelliği kullanıcılara kurulan kopya sitenin asıl sitenin bir uzantısı ya da kendisi gibi olduğu hissini vermektir. Yapılan bu kopya sitenin ve gönderilen e-postanın uyumu ve inandırıcılığı saldırının başarısını direkt olarak belirleyen faktörlerdir. Bu tip saldırı günümüzde en yaygın olarak kullanılmakta olan saldırı türüdür.

**— Direkt E-Posta Saldırılar**

Direkt e-posta saldırılarında sadece kurbanın girdiği bilgileri toplayacak bir toplayıcı sistemi bulunmaktadır. Veriler direkt olarak saldırı e-posta içerisinde sorulur. Verilerin girileceği kutucuklar ve gönderim butonu e-posta içerisinde yer alır. Gizli bilgilerini gösterilen kutucuklara giren kurbanın gönder butonuna basması ile birlikte veriler saldırganın toplayıcı sistemine ulaşır. Bu noktada eğer saldırgan verileri gerçekte çalışmakta olan sisteme doğru yönlendirirse kullanıcı gerçekte çalışan sisteme girdiğini sanır ki bu da aldatıldığını anlamasını oldukça güçleştirir. Bu tip saldırıları önlemek için her geçen gün gelişen e-posta istemcilerinin gönderim işlemlerinde kullanıcı uyarılmaktadır ve gönderim işlemlerine kısıtlamalar getirilmektedir.

**— Popup(Açılan Küçük Pencere) Saldırılar**

Bu tip saldırı artık günümüzde geçerliliğini yitirmekte olan bir saldırı türüdür. Bu saldırı türünde hedef sitenin mevcut açıklarından faydalanarak sitenin içeriğine müdahale ederek hedef sayfaya girildiğinde bir Popup(açılan küçük pencere) penceresinin çıkması ve bu pencere vasıtası ile kullanıcıdan bilgilerin istenmesi şeklinde gerçekleştirilir. Günümüzde bu tür saldırının engellenmesi için tüm bilgisayarlarda Popup(açılan küçük pencere) engelleyici özelliği bulunan internet görüntüleyici kullanılmaktadır ve sitelerde bulunan belirli açıkların yüksek oranda kapatılması sağlanmaktadır.

#### *2.5.1.2 Hazırlık Aşaması*

Saldırının hedef firması, hedef kullanıcı kitlesi ve saldırı tipi seçildikten sonra sıra saldırıda kullanılacak sistemi oluşturmaya gelir. Bu aşamaya hazırlık aşaması denilmektedir. Hazırlık aşaması genel olarak beş ana bölümde incelenmektedir. Bunlar; "Sitenin Kopyalanması", Tuzağın Oluşturulması, "Toplayıcı Sistemin Hazırlanması", "Yemleme Sisteminin Hazırlanması" ve "Sistemin Sunuculara Yerleştirilmesi" dir.

**— Sitenin Kopyalanması**

Hedef olarak seçilen firmanın web sitesi bazı programlar vasıtası ile birebir bilgisayar ortamına aktarıldıktan sonra içerisindeki bazı kısımların gerekli düzenlemeleri yapılır. Bu düzenlemeler esnasında saldırgan mevcut sitenin olabildiğince benzeyen bir kopyasına ulaşmayı amaçlar. Bunun için sitenin içeriğinde bulunan bazı bağlantılar ve resimler kurbanın siteye olan inancının artması için mevcut hedef siteye bağlanır. Bu adım taklit saldırı tipinde geçerli olan bir adımdır.

**— Tuzağın Hazırlanması**

Sitenin birebir kopyalanmasının ardından yapılacak olan kopyalanan site içerisinde hedef sitede bulunana benzer bir bilgi girişi kısmının konulmasıdır. Bu konulan tuzak, toplayıcı sistem ile birlikte çalışarak girilen bilgileri toplayacak ve saldırıyı amacına ulaştıracaktır. Bu aşamada saldırgan açısından önemli olan nokta bir önceki aşamada da olduğu gibi saldırganı olabildiğince inandırmaktır. Hazırlanan tuzak taklit bir saldırı yapılacaksa kopyalanan sitenin içerisine, direkt e-posta saldırısı ise gönderilecek e-postanın içine, popup(açılan küçük pencere) bir saldırı yapılacaksa hazırlanan popup(açılan küçük pencere) kutucuğunun içine yerleştirilir.

**— Toplayıcı Sistemin Hazırlanması**

Bu aşamada kurulan tuzaktan gelecek verilerin uygun şekillerde tutulmasını sağlayacak sistem oluşturulur. Saldırganın isteği doğrultusunda gelen veriyi bir veritabanında tutabilir, e-posta yöntemi ya da anında mesajlaşma yoluyla saldırgana

iletebilir. Bu seçim tamamıyla saldırganın istemi ve yeteneği ile ilgili bir durumdur. Bu işlem için saldırganın belirli bazı kodlama yeteneklerine sahip olması gereklidir.

**— Yemleme Sisteminin Hazırlanması**

Yemleme işlemi e-posta sistemi üzerinden yapılmaktadır. Yemleme esnasında yem olarak atılan e-postaların kopyalanarak oluşturulan sitede olduğu gibi inandırıcılık konusunda üzerinde çalışılmış olması gerekmektedir. merkezbanka.org alan adı üzerinden alınan alt alan adı olarak http://tcmb.gov.tr.teyit.merkezbanka.org adresi sayesinde kullanıcılar kandırılmaya çalışılmaktadır. Hâlbuki birçok kullanıcı TCMB'nin resmi internet sitesinin http://www.tcmb.gov.tr olduğunu bilir. Bu yüzden de verilen örnek inandırıcılıktan çok uzak bir saldırıya aittir.

Bazı yemleme örneklerinde gidilen internet adresleri farklı olarak gösterilmekte ve bu da kullanıcıları inandırma konusunda daha başarılı sonuçlar vermektedir.

**— Sistemin Sunuculara Yerleştirilmesi**

Önceki adımlar sıra ile gerçekleştirildikten sonra sıra sistemin sunuculara yerleştirilmesine gelmektedir. Bu aşamada saldırganlar en az iz bırakarak en inandırıcı olabilecek çözümü aramaktadırlar. Phishing(olta saldırılar) tekniğinin ilk ortaya çıktığı yıllarda ücretsiz web alanı sağlayan siteler kullanılmaktaydı ve bu sitelerin inandırıcılık konusunda büyük eksikleri vardı. Zaman içerisinde daha inandırıcı olması açısından daha masraflı olan ücretli web alanları kullanılmaya başlandı ve göz yanılgısı sağlayan alan adlarının kullanımı da yaygınlaştı. Örneğin 2005 yılı içerisinde yapılan bir saldırıda hedef alınan Garanti Bankası için kurbanları şaşırtmak amaçlı **www.bank-garanti.com** adresi kullanılmıştır. Bu tip başarılı örneklerin yanı sıra **merkezbanka.org** gibi başarısız örneklerde mevcuttur.

#### *2.5.1.3 Yemleme Aşaması*

Yemleme işlemi saldırının en önemli aşamasıdır. Yemleme esnasında yapılan hatalar sistemin inandırıcılığını yok ederek bütün bir saldırının başarısız olmasına neden olabilir.

Yemleme esnasında genel olarak e-posta kullanılır. İstem dışı gönderilen e-postalara phishing(olta saldırıları) postaları da örnek gösterilebilir. E-posta dışında anında mesajlaşma ile telefon aramaları, chat odaları yolu ile forumlar ve haber grupları yolu ile kurbanlara ulaşılabilmektedir. Bu durumda yemleme yöntemlerini iki ana kısımda incelenecektir. Bunlar; e-posta yolu ile yemleme ve diğer yöntemler ile yemlemedir.

**— E-Posta Yolu İle Yemleme**

SMTP protokolü (Simple Mail Transfer Protocol), bir e-posta göndermek için sunucu ile istemci arasındaki iletişim şeklini belirleyen protokoldür. Sadece e-posta yollamak için kullanılan bu protokolde, istemci bilgisayar SMTP sunucusuna bağlanarak gerekli kimlik bilgilerini gönderir, sunucunun onay vermesi halinde gerekli e-postayı sunucuya iletir ve bağlantıyı sonlandırır. İlk olarak 1982 yılında o zaman ki sınırlı kullanım alanı içerisinde oluşturulmuş bir protokoldür. Zaman içerisinde birkaç yenilemeden geçmiş olsa da çok ciddi güvenlik zaaflarını bünyesinde bulundurmaktadır. En son Nisan 2001 tarihinde değişikliğe uğrayan SMTP Protokolü RFC2821 referansı ile yayımlanan bu son değişiklik metninin 7. kısım 1. bölümünde açık olarak SMTP protokolünün her türlü saldırıya açık ve güvenlik zaafları bulunan bir protokol olduğu kabul edilmiştir. Sistemi geliştirenler tarafından bile kabul edilen bu zaaflar phishing(olta saldırılar) ve benzeri birçok farklı saldırının e-posta tabanlı olarak geliştirilmesine olanak sağlamaktadır. Bu konuda farklı çalışmalar yapılmaktaysa da henüz toplum tarafından kabul gören bir sonuca ulaşılamamıştır.

Phishing türü sayılan SPAM(Dolandırıcılık Maili) sisteminden yardım almakta ve onun bazı tekniklerini benimsemektedir. Bu tekniklerden en bilineni sayfa taraması yöntemidir. Bu yöntemde saldırgan piyasada bulunana sayfa filtreleme programları yardımıyla arama motorları ya da başka bazı yöntemler sayesinde ulaştığı sayfaları ve

bunlara bağlı sayfalardan e-posta adreslerini ayıklamakta ve kendisine bir gönderim listesi oluşturmaktadır. Bu konuda A.B.D. Ulusal Ticaret Komitesi tarafından yapılan bir araştırmaya göre internet sitelerinde verilen her 100 e-posta adresinden 86'sına, haber gruplarında verilen her 100 posta adresinden yine 86'sına SPAM(Dolandırıcılık Maili) olarak adlandırılan istem dışı postalar gelmektedir. Bu açıdan değerlendirildiğinde internet üzerinde farkında olmadan bırakılan e-posta adresleri büyük oranda saldırganlar tarafından ele geçirilmekte ve bu postalar phishing(olta saldırılar) ve başka saldırılara konu olmaktadır.

Çeşitli şekillerde toplanan e-posta adreslerinden sonra geriye kalan iş daha önceden hazırlanmış olan postaları listede bulunan adreslere göndermektir. SMTP protokolünde bulunan açıklardan faydalanan isimsiz posta gönderim araçları, gönderimi yapılan postayı istenilen bir posta adresinden geliyormuş gibi gösterebilmektedir. Bir postanın teyit@tcmb.gov.tr adresinden gelmesi durumunda inandırıcılık artacaktır. Bu noktada saldırgana çıkan engel SPAM(Dolandırıcılık Maili) postaları engellemesi için geliştirilmiş anti-SPAM (SPAM önleyici) filtre programlarıdır. Bu programlar belirli bazı SPAM(Dolandırıcılık Maili) tekniklerine göre geliştirilmiş programlardır ve SPAM(Dolandırıcılık Maili) postaların kullanıcılara ulaşmasını engellemek için oluşturulmuşlardır. Bu noktada anti-anti-SPAM olarak adlandırılan bir düşünce sistematiği ile SPAM(Dolandırıcılık Maili) olarak filtre tarafından yakalanması mümkün olan posta, filtre programının zaafları araştırılarak SPAM(Dolandırıcılık Maili) kategorisinden çıkartılmaya çalışılır. Örneğin bu tip filtreler mesajın içeriğinin boyutuna göre aynı boyutta ve çok sayıda yakın zamanlı gönderilmiş postaları SPAM(Dolandırıcılık Maili) olarak algılamaktadır. Bu engeli aşmak için saldırganlar postaların içine gözükmeyecek bir biçimde gelişi güzel karakterler yazdırmaktadırlar ki bu sayede filtre farklı boyutlarda olduğundan postaları SPAM(Dolandırıcılık Maili) olarak nitelendirmemektedir. Filtrelerin yeni bir gelişim göstermesinin ardından saldırganlar bu gelişimi aşmak için yeni bir teknik

geliştirirler. Bu da yine filtrelerin bu yeni geliştirilen tekniği fark edip ona uygun güncellemeleri yapması şeklinde devam eden bir süreçtir.[28]

### 2.5.2 Phising ( Olta Saldırıları) Saldırılarından Korunma Yöntemleri

Bilgisayarlarda bankacılık işlemleri yapılırken olumsuz durumlardan korunmak için pek çok önlem vardır. Bunlardan bazıları çok basit olmakla birlikte bazıları zaman ayırarak ya da bir uzmandan yardım alınarak gerçekleştirilebilecek işlemlerdir. Phising saldırılarının hedefi elektronik posta ile kullanıcıları yanıltmak ve kişisel bilgilerini ele geçirmektir.

Online(Çevrimiçi) dolandırıcılık, sahtekârlık ve virüslere karşı bu konuda bilinçli ve bilgili olmak gerekir. Phising saldırılarından korunmak için aşağıdaki uyarılara dikkat edilmelidir.

**1.** Tanınmayan adreslerden gelen mesajlar cevaplanmadan silinmelidir. "Aşağıdaki bağlantıyı tıklayın" gibi e-posta isteklerine cevap verilmemelidir.

**2.** İşlem yapılan web sayfasının güvenli olup olmadığı mutlaka kontrol edilmelidir. İnternet tarayıcısının üst kısmında adres bölümünde bulunan adresin "https://" olup olmadığı kontrol edilmelidir. "https://" in sonunda bulunan "s" harfi bu sayfanın güvenli ve çeşitli şifreleme metotları ile işlem yaptırdığını belirtir.

**3.** İnternet tarayıcısının sağ alt kısmında yer alan kapalı kilit işareti, güvenli ve şifrelenmiş bir sayfada işlem yapıldığını gösterir.

**4.** İnternette bankacılık işlemi ve alışveriş yapılmak isteniyorsa, ilgili sitenin yazılarak girilmesi en güvenli yoldur.

---

28 Şükrü Alataş, Murat Altan "İnternet Denizin Popüler Avlanma Yöntemi",10.11.2007, http://inettr.org.tr/inetconf12/bildiri/25.pdf, (12 Aralık 2007), s.3-8.

**5.** Sahte siteler genelde sayısal rakamlar içermektedir. Sayısal rakamlar içeren sayfalar mutlaka çalışılan kurumla irtibata geçilerek kontrol edilmelidir.

**6.** Çalışılan hiçbir kurum kişisel bilgileri isteyen e-posta göndermez. Bu şekilde bir e-postayla karşılaşıldığında mutlaka ilgili kuruma bilgi verilmelidir.

**7.** Kullanılan bilgisayar güvenli olsa bile network güvenli değilse parasal işlem yapılmamalıdır.

**8**. Bankalardan gelen hesap özeti ve kart ekstreleri düzenli olarak kontrol edilmelidir. Şüpheli bir işlemle karşılaşıldığında ilgili bankayla irtibata geçilmelidir.

**9.** Anti virüs programları devamlı olarak güncellenmelidir.

**10.** Çeşitli kurumlardaki hesaplar ve birden fazla e-posta için farklı şifreler belirlenmelidir. Çünkü bir şifrenin dolandırıcıları eline geçmesiyle diğer hesaplarda bu şifreyle denenecektir.

**11.** Belirlenen şifreler sık sık değiştirilmelidir.

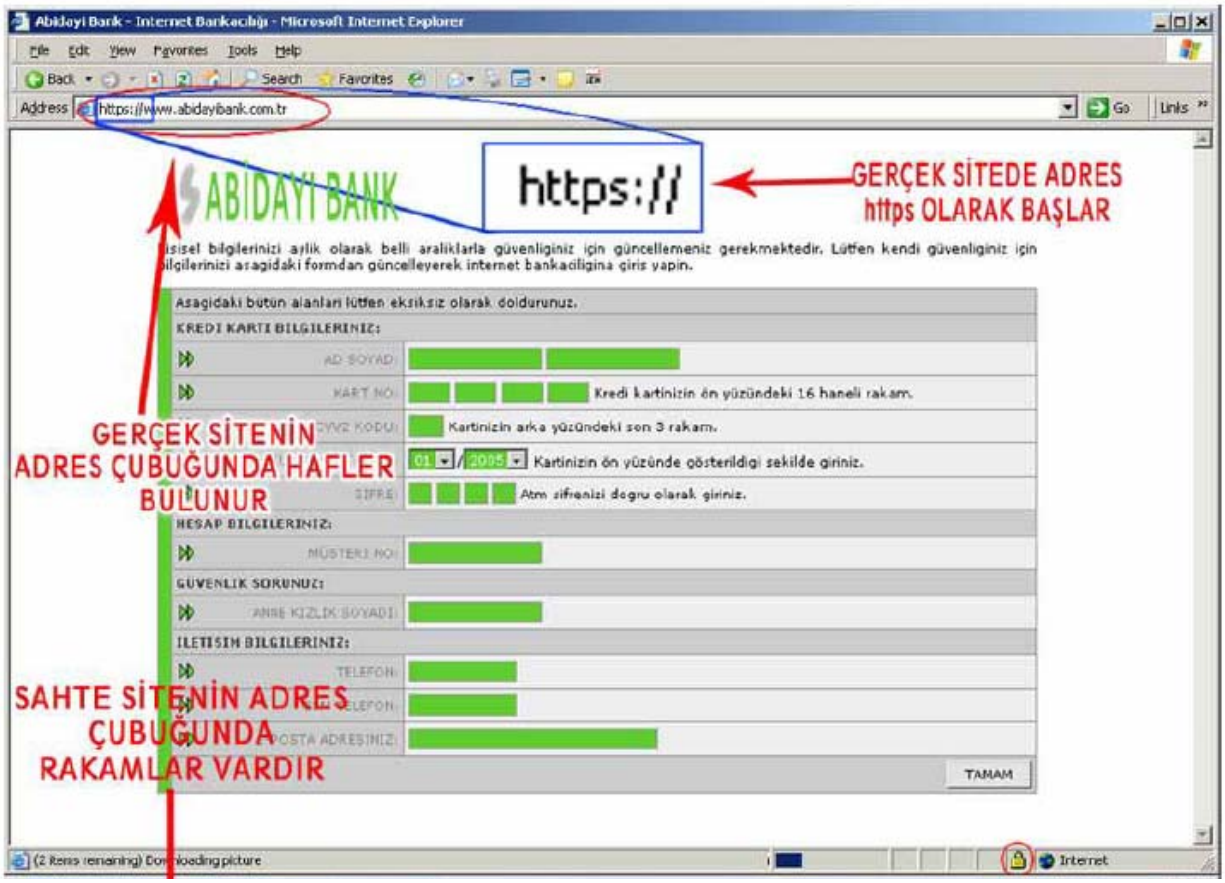
**12.** Dolandırıcı kişiler phising(olta) saldırı yöntemiyle müşterilerin hesaplarına ulaştıktan sonra buradaki tutarları kendi kimlikleri ortaya çıkmadan çekmek isterler. Bu işlem için kimsenin şüphelenmeyeceği aracı hesaplar bulmak amacıyla internetten ilan verirler.

Bu ilanlarda çaba harcanmadan kolayca para kazanılacağı bunun çok kolay bir iş olduğu yer alır. Bu ilanla işi kabul eden kişilerin hesapları belli bir komisyon karşılığında, uluslararası para transferleri yapan şirketler aracılığıyla transfer etmek amacıyla kullanılmaktadır. Böylece dolandırıcılığı gerçekleştiren kişiler kimliklerini gizlemiş olup, ilan aracılığı ile bu işe başvuran kişilere suçu atmış olacaktır.

Yapılan bu işlem kara para aklama işlemi olup, sonucu kanuni takibata varmaktadır. Böyle bir ilanla karşılaşıldığında e-posta kesinlikle silinmemeli ve yönlendirdiği web sitesiyle ilgili bilgiler toplanarak çalışılan kurumun bilgi işlem bölümüne haber verilmelidir. Bireysel kullanıcılar bir dilekçe ile savcılığa başvurmalı ve yazı polise götürülmelidir.[29]

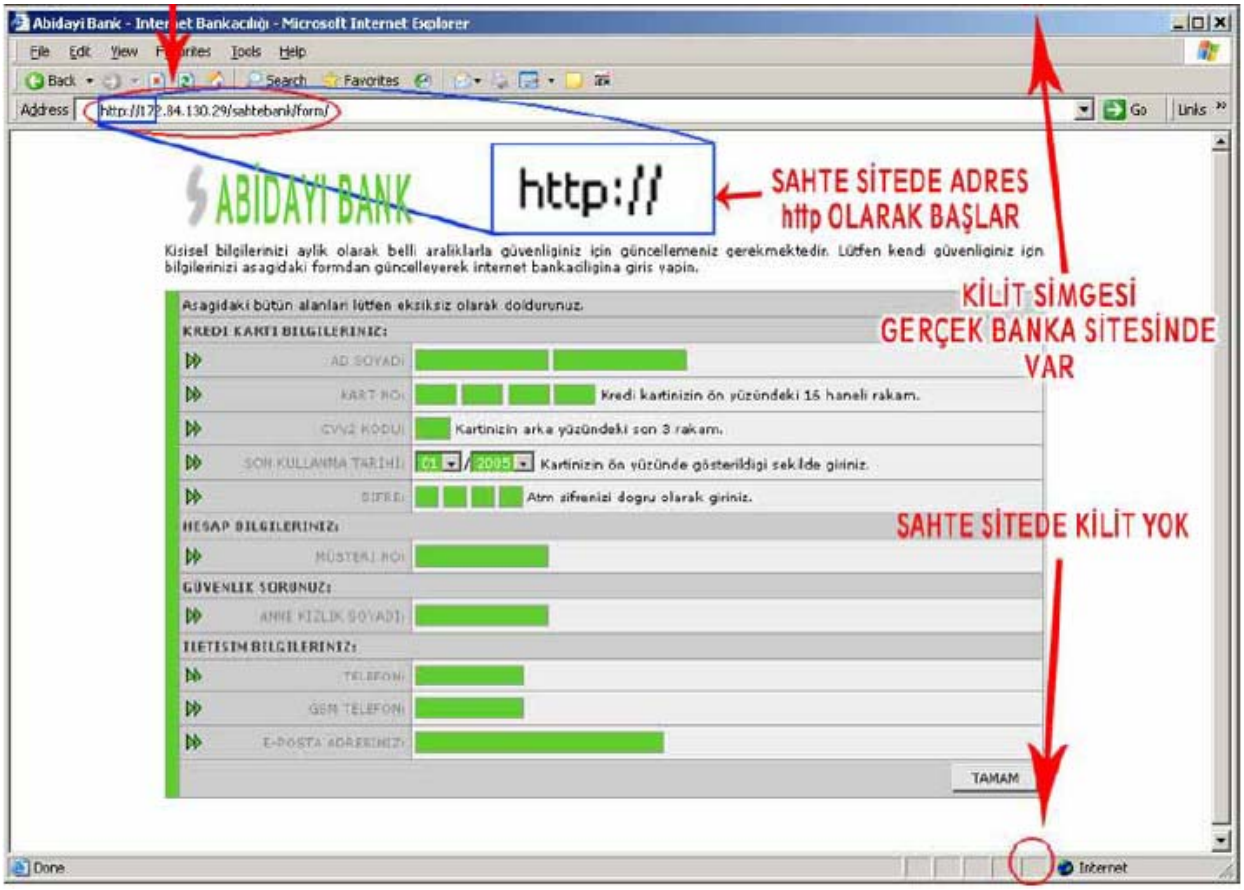
29 Pek, a.g.e, s.1.

**Genel olarak sahte site ile gerçeğini ayırt etmek için aşağıdaki şekli inceleyebiliriz.**



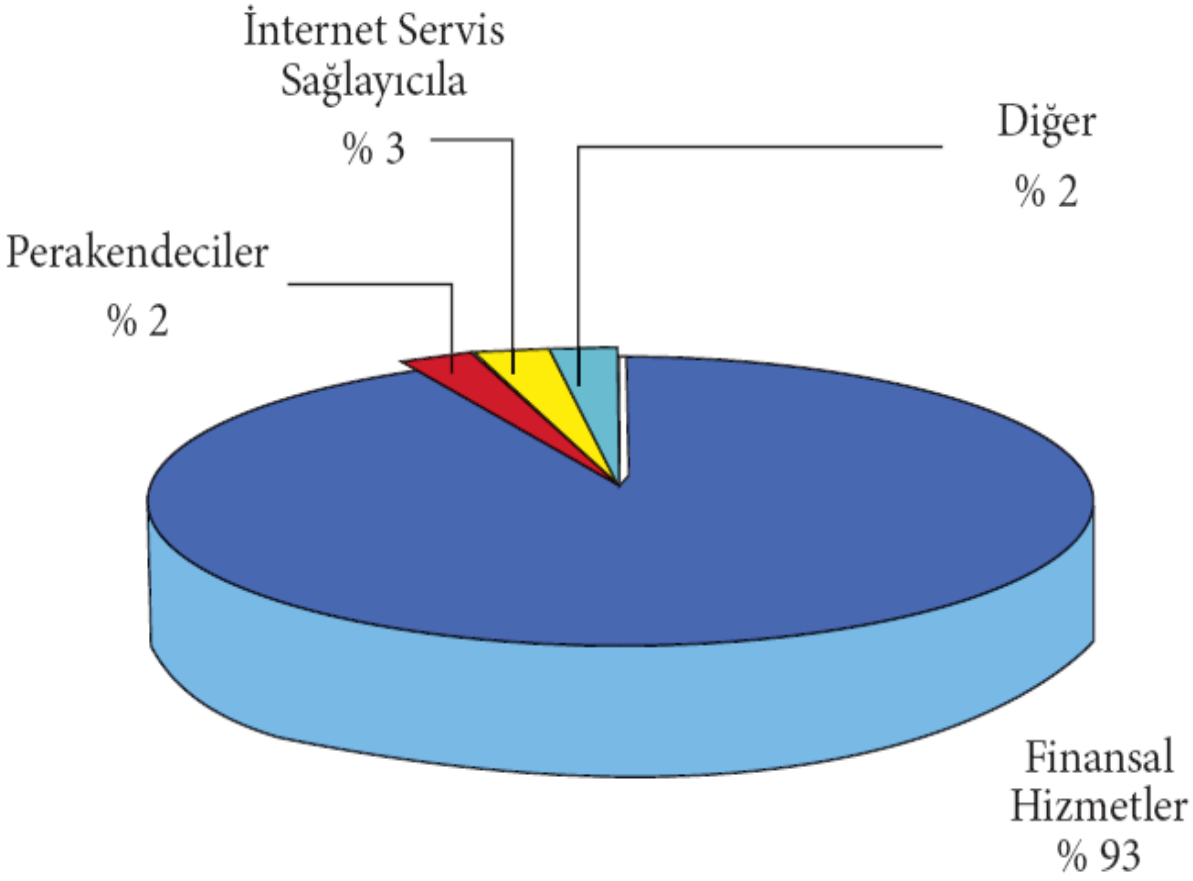

**Şekil 6:** Gerçek İnternet Sitesi

**Kaynak:** Mustafa Sansar, "Sanal Dolandırıcılıkta Son Nokta Phıshıng" ,31.10.2007, http://www.iem.gov.tr/iem/?menu_id=1&detay_id=68, (24 Kasım 2007)




**Şekil 7:** Sahte İnternet Sitesi

**Kaynak:** Mustafa Sansar, "Sanal Dolandırıcılıkta Son Nokta Phıshıng" ,31.10.2007 , http://www.iem.gov.tr/iem/?menu_id=1&detay_id=68, (24 Kasım 2007)




**Grafik 3:** Phishing ( Sahte Site ) Saldırılarında Hedef Alınan Sektörler

**Kaynak:** Türkiye Bankalar Birliği İnternet Bankacılığı Çalışma Grubu, Nisan 2007, s.40., www.tbb.org.tr/v/doc/Kitapçık.pdf , (28 Eylül 2007)

## 2.6. E-POSTA YÖNTEMİ:

E-posta yöntemini kullanan dolandırıcılar 3 şekilde aldatma yoluna gider;

**1)** E-postaya devamlı temas halinde olunan kuruluşlardan gönderiliyormuş izlenimi verilen sahte bir e-posta gönderilir. Bu e-postalarda kullanıcıya, kurumun web sitesine giderek şifresinin süresi dolduğu bilgisi verilir ve altta o sayfaya yönlendirileceği bir link(bağlantı yolu) verilir. Korsan daha önce hazırladığı ve kuruluşun sitesinin aynısı olan bu siteye kurbanını getirdikten sonra, ondan şifresini girmesini ister. Kullanıcı kendi şifresini yeni şifresiyle değiştirir. Böylece eski şifre hala geçerlidir ve dolandırıcı eski şifreyi öğrenmiştir. Dolandırıcı eski şifreyi kullanarak internet aracılığı ile para transferi işlemi yapabilir.

**2)** Bazı e-postalarda, bir yarışma düzenlendiği ve bu yarışmaya katılması teklif edilen kullanıcılara büyük bir ödül kazandıkları ancak gerekli kişisel bilgileri vermeleri gerektiği yer alır. Bilgiler verildiğinde ise korsan kullanıcıya ait kişisel bilgileri ele geçirmiş olacaktır.

**3)** Çalıştığı kurumdan geliyor gibi gözüken e-postalarda müşterilerden bilgilerini güncellemeleri istenir. Bunun kendileri açısından daha iyi hizmet verebilmek için gerekli olduğu belirtilir.

## 2.7. YAŞANMIŞ İNTERNET DOLANDIRICILIĞI OLAYLARI

İnternet bankacılığı ile kredi kartı borcunu ödemek isteyen Akbank müşterisi E.Aysan Altuğ, 11 Mayıs 2007 Cuma günü sisteme giriş yapmak istedi ancak ilgili bankanın 3 aylık sürelerle verdiği kullanıcı adı ve şifre süresinin dolduğu uyarısıyla karşılaşmıştır ve bilgilerini ilgili ekrana girerek şifre değişikliğini gerçekleştirmiştir. Bu

işlemden yarım saat sonra hesabındaki 9.500 Ytl tutar Fatih Çağlar ve Erol Köse isimli şahısların hesabına havale edilerek banka kartlarıyla harcama ve nakit çekim yapılarak kullanılmıştır.

E. Aysan Altuğ iddiasında şifre değişikliği yaptıktan sonra sisteme giriş yapamadığını için ilgili bankanın müşteri hizmetlerini aradığını ve banka çalışanı tarafından şifrelerinin istendiğini belirtmişir[30]

***Akbank tarafından gerekli incelemeler yapılarak olay hakkında aşağıdaki açıklamalar yapılmıştır;***

Yapılan incelemede ilgili şikâyete dair bankanın herhangi bir kusuru olmadığı tespit edilmiştir. Detaylar aşağıdaki gibidir;

— Müşterinin 11.05.2007 tarihinde saat 14:32:08'de müşteri temsilcisi ile yapmış olduğu görüşme dinlenerek kişisel bilgilerin alınmadığı tespit edilmiştir. Haberde yer alan "Telefondaki ses kendisinden şifre ve müşteri numarası gibi bilgileri aldı" ifadenin asılsız olduğu belirtilmiştir.

— Dolandırıcılık olayının gerçekleşmesinin ardından müşteri "Dolandırıcılık Acil Grubu" tarafından aranmıştır. Müşterinin "İnternet şubesine girerken hata aldım" demesi üzerine, internet şubesine giriş yaptığı ekran görüntüsü kendisinden talep edilmiştir. Gönderilen ekran görüntüsü incelendiğinde bankaya ait olması gereken site olmadığı, bireysel müşteri numarasının girileceği sahanın mevcut olmadığı ve PC de yer alan virüs nedeniyle "sahte Akbank sitesine yönlendirme olduğu" görülmüştür.

— Akbank ana sayfasında bu tür sahte sitelerden nasıl korunabileceğini anlatan güvenlik uyarılarının mevcut olduğu ve bankanın tüm müşterilerine bu konuda bilgilendirme yapıldığı belirtilmiştir.

30 Cumhur İlyasoğlu, "Müşteri Hizmetlerini Aradı, Hesapları Boşaltıldı",01.06.2007, http://www.pcguvenlik.com, (15 Aralık 2007)

— Gerçekleşen talihsiz olayın müşterinin PC güvenliğini sağlayamaması nedeniyle, internet şube bilgilerinin kötü amaçlı kişilerin eline geçmesinden kaynaklandığı ve çağrı merkeziyle yapılan görüşme ile bir ilgisi bulunmadığı tespit edilmiştir."[31]

Yapılan incelemede müşterinin Akbank internet sitesi yerine sahte siteye giriş yaparak şifrelerini kaptırdığı tespit edilmiştir.

## 2.8. İNTERNETNET ŞUBESİ GÜVENLİK ÖNLEMLERİ

Müşterilerin internet bankacılığı üyeliği esnasında güvenli kullanım konusunda bilgilendirilmesi önemlidir. Tüm banka sitelerinde aşağıdaki hususlar genel anlamda belirtilmiştir. Müşteriye bu hususlar kısaca anlatılmalı ve varsa bankanın ana sayfasında yer alan "güvenlik uyarılarının" okunarak uygulanması için yönlendirme yapılmalıdır.

— Kullanıcı bilgilerinin gizli kalmasına özen gösterilmelidir. Şifre, parola ve kullanıcı adı belirlenirken kolaylıkla tahmin edilebilecek (isim, doğum tarihi vb.) bilgilerden oluşmamasına dikkat edilmelidir.

— Kullanıcı bilgilerinin paylaşılmaması gerekmektedir. Şifre, parola, kullanıcı adı ve kişisel bilgiler paylaşılmamalı, bir yerde yazılı olarak tutulmamalıdır.

— Sık sık kullanıcı adı, şifre ve parola bilgileri değiştirilmeli, aynı bilgilerin farklı sitelerde kullanılmamasına özen gösterilmelidir. Her hesap için ayrı şifre belirlenmelidir.

— Sadece güvenliğinden emin olunan bilgisayarlardan işlem yapılmalıdır. Bilgisayar güvenliği olmayan ortamlarda (internet kafeler gibi yerlerde) internet bankacılığı

31 ANKA, "Akbank' tan Dolandırıcılık İzahı"02.06.2007, http://www.gercekgundem.com/?p=66958&com=all, (15 Aralık 2007)

kullanmamalıdır. Bu tür bilgisayarlara yüklenen programlar vasıtasıyla kolayca kullanıcı adı, şifre ve parola ele geçirilebilir.

— İşletim sistemi ve internet tarayıcının güncel tutulması gerekmektedir. Bilgisayarın korunması ve sorunsuz çalışmasını sağlamak için, yazılım üretici firmalar tarafından yayınlanan güncellemelerin takip edilerek, bilgisayarın sık sık güncellenmesi gerekmektedir.

— Lisansı olmayan yazılım kullanılmamalıdır. Lisansı olmayan yazılımlar kullanıldığında güvenlik açıkları olabilir. Bilgisayara lisansı ya da kaynağı belli olmayan programlar yüklenilmemelidir.

— Anti-virüs yazılımı kullanılmalıdır. Anti-virüs yazılımları bilgisayarı zararlı virüs, parazit, "truva atı" ve diğer tehlikelere karşı korur. Bilgisayarın güven içinde kullanılması için bir anti-virüs yazılımı kullanılması ve yazılımın güncel tutulması gerekmektedir.

— İnternet güvenlik duvarı (firewall) kullanılmalıdır. Güvenlik duvarı yazılımları, bilgisayarı ve orada tutulan bilgilere yetkisi olmayan kişilerin erişimini engeller. Bilgisayarın güvenle kullanılması için bir internet güvenlik duvarı yazılımı kullanılmalıdır.

— Tarayıcıda otomatik tanımlama fonksiyonu kullanılmamalıdır. Tarayıcıda otomatik tanımlama fonksiyonu kullanılıyorsa devre dışı bırakılmalıdır. Otomatik tanımlama fonksiyonu, daha önce girilen şifreler de dâhil olmak üzere tüm bilgileri saklar. Bu fonksiyonun devre dışı bırakılması güvenlik açısından uygun olacaktır.

# 3. SAHTE BELGE, BANKA KARTI SAHTECİLİĞİ VE DOLANDIRICILIĞIN TESPİTİ

## 3.1. SAHTE BELGE DÜZENLENLENMESİ VE SAHTE HESAP AÇILIŞI

Dolandırıcılık girişimlerinin ortak noktası, hemen hemen tüm dolandırıcılık girişimlerinde sahte belgenin kullanılmasıdır. Sahte belge kullanımı özellikle bankacılık sektörüne karşı işlenmiş suçlarda ön plana çıkmaktadır.

Şubeye başvurarak hesap açmak için gelen şahsın yapmış olduğu başvuru dikkatle incelenmelidir. Dolandırıcılık amacıyla açılan hesaplara gelen bir veya iki transfer sonrası para çekilişi yapılmakta ve dolandırıcılık olayı gerçekleştirildikten sonra bu müşteri bir daha şubeye uğramamaktadır.

Müşteri hesabının ilk hareketleri( ilk 5–10 hareketi) şüpheli kabul edilmeli ve bu hesap hareketleri için azami dikkat sarf edilmelidir. Şubeye hesap açılışından sonra ilk defa para çekmeye gelen müşteriye kimlik kontrolüyle birlikte ek güvenlik önlemleri uygulanmalıdır.

Hesap hareketleri mutlaka incelenmeli ve hesaba gelen bir havale veya EFT mevcut ise bu tutarın hangi kanaldan transfer edildiği kontrol edilmelidir. İnternet, ATM(otomatik para çekme makineleri) , çağrı merkezi ve diğer alternatif dağıtım kanalları (şube dışı bankacılık) kullanılarak yapılan transferlerin amirden veya amir bankadan teyit edilmesi önerilmektedir. Şubeyle yeni çalışmaya başlayan bir müşteriye, aynı şubeden veya aynı bankadan sürekli gelen havale ve EFT' ler hangi kanaldan yapılmış olurlarsa olsun şüpheli işlem olarak değerlendirilmelidir. Şüpheli hesap ve transferlerin kaynaklarının tespiti için banka bu konudan sorumlu "güvenlik bölümü" ile temasa geçilmesi gerekmektedir.

Hesap açılışlarında alınan belgeler çok ciddi bir şekilde incelenmeli ve gerekli araştırmalar yapılmalıdır. Hesap açılışı ve sonrasında yapılacak tüm bankacılık işlemlerinde müşterinin iki kimliği teyit edilerek işlem yapılmalıdır. Eğer şüpheli durum devam ediyorsa bankalar nüfus müdürlüğüyle irtibata geçerek kimliği teyit ettirebilir.

Sahte kimlik kullanılarak açılan hesaplar ve sahip olunan "banka kartı" ile 24 saat şube dışından para çekilmektedir. Müşterinin ne iş yaptığı, hangi bankalarla çalıştığı, bankayla hangi amaçla çalışacağı gibi müşteriyi tanıma ilkeleri içerisindedir ve uygulanması önemlidir. Sorgu yapılmadan, sadece müşterinin ibraz etmiş olduğu nüfus cüzdanı fotokopisine istinaden açılan mevduat hesabı; şubeye, bankaya veya başka bir kişinin zararına dönüşebilir. Bankaların internet şubesi müşterilerinin kullanıcı kodları ve şifreleri ele geçirilerek bu müşterilerin hesaplarından, paravan olarak açılan hesaplara EFT ve havaleler yapılmaktadır. Sadece kimlik ibrazı ile herhangi bir sorgu kriteri gerçekleştirilmeden açılan bu tür hesaplara yapılan transferler, genellikle aynı gün çekilerek müşteri zararına dönüşmektedir. Genellikle sahte kimliklerin kullanıldığı bu yöntemle, müşterilerin mevduat hesaplarındaki tutarlar dolandırıcıların eline geçmektedir. Yukarıda belirtilen yöntemle parasını çaldıran müşteri; Cumhuriyet Savcılığı' na suç duyurusunda bulunurken, kendi çalışmış olduğu banka ile birlikte parayı ödeyen ve müşterisini tanımadan, ibraz edilmiş olan sahte kimliğe istinaden hesap açmış olan banka şubesi aleyhine de dava açmaktadır. Bankalar aleyhine açılan bu davalar; görevde ihmal tespit edilirse kurum için zararla sonuçlanmaktadır.

## 3.2. KİMLİK TEYİT EDİLİRKEN DİKKAT EDİLMESİ GEREKEN HUSUSLAR

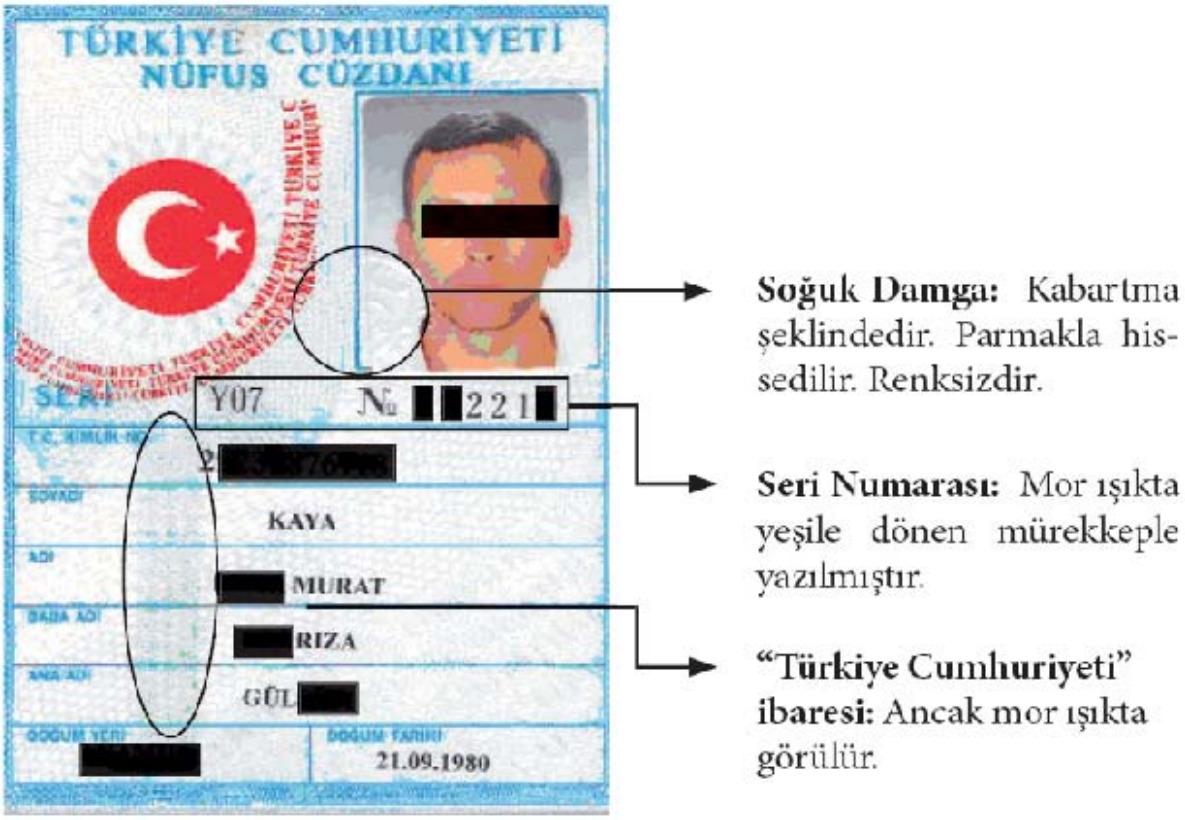
Bankacılık Sektöründe müşteri kimliğinin tespiti, 4208 sayılı Kara paranın Aklanmasının Önlenmesine Dair Kanun'da işaret edildiği üzere, nüfus cüzdanı, ehliyet ve pasaport ile yapılmaktadır. Bu belgeler sahtecilik olaylarında sıkça kullanılır. Kimlik belgeleri teyit edilirken aşağıdaki hususlara dikkat edilmelidir.

### 3.2.1 Nüfus Cüzdanını Teyit Ederken Dikkat Edilmesi Gereken Hususlar

**1.** Erkeklerin nüfus cüzdan seri numaraları tek (Örn: A01/A83vb.) kadınların nüfus cüzdanlarının seri numaraları ise çifttir.

**2.** Fotoğrafın sol alt köşesinde soğuk mühür bulunmalıdır. Mührün ortasında ay/yıldız, çeperinde ise verildiği nüfus müdürlüğünün adı yer almaktadır. Başparmakla yapılan muayenede soğuk mühür "kabartı" şeklinde hissedilmelidir.

**3.** Nüfus cüzdanının arka tarafında, nüfus müdürüne ait bir imza ve bir paraf yer almalıdır. İmza, nüfus müdürü tarafından, paraf ise belgeyi düzenleyen memur tarafından atılmaktadır. Aynı alanda ilgili nüfus idaresinin mührüde yer almalıdır. Mührün üzerinde ay yıldızın hemen altında nüfus müdürlüğünün ismi yer almalıdır. Şüphelenilen durumda ilgili nüfus idaresi telefonla aranarak nüfus cüzdanında ismi geçen personelin kurumda çalıştığı araştırılmalıdır. Hesap açılışlarında maksimum güvenlik uygulanmalıdır.




**Şekil:8** Sahte Nüfus Cüzdanı Örneği

**Kaynak:** Türkiye Bankalar Birliği İnternet Bankacılığı Çalışma Grubu, Nisan 2007, s.16., www.tbb.org.tr/v/doc/Kitapçık.pdf , (28 Eylül 2007)

### 3.2.2 Ehliyet Teyit Ederken Dikkat Edilmesi Gereken Hususlar

**1.** Sürücü belgesinde fotoğraf sahasının sağ alt köşesinde başparmakla yapılacak muayene sırasında fark edilecek soğuk mühür bulunmaktadır. Mührün ortasında bir ay yıldız, çeperinde ise TC İçişleri Bakanlığı, Emniyet Genel Müdürlüğü ibaresi yer almaktadır.

**2.** Sürücü Belgesinin sağ alt tarafında kabartma yazılarla 5 haneli bir numara bulunmaktadır.

**3.** Belgenin arka yüzünde ehliyet sahibinin imzası bulunmaktadır. Sahte ehliyetlerde imza, genelde belgeyi düzenleyen kişi tarafından atılmaktadır. Bu nedenle banka şubesine gelen kişiden kontrol için alınan ehliyet işlem sonuna kadar personelde kalmalı ve müşterinin imzası alınarak karşılaştırma yapılmalıdır.

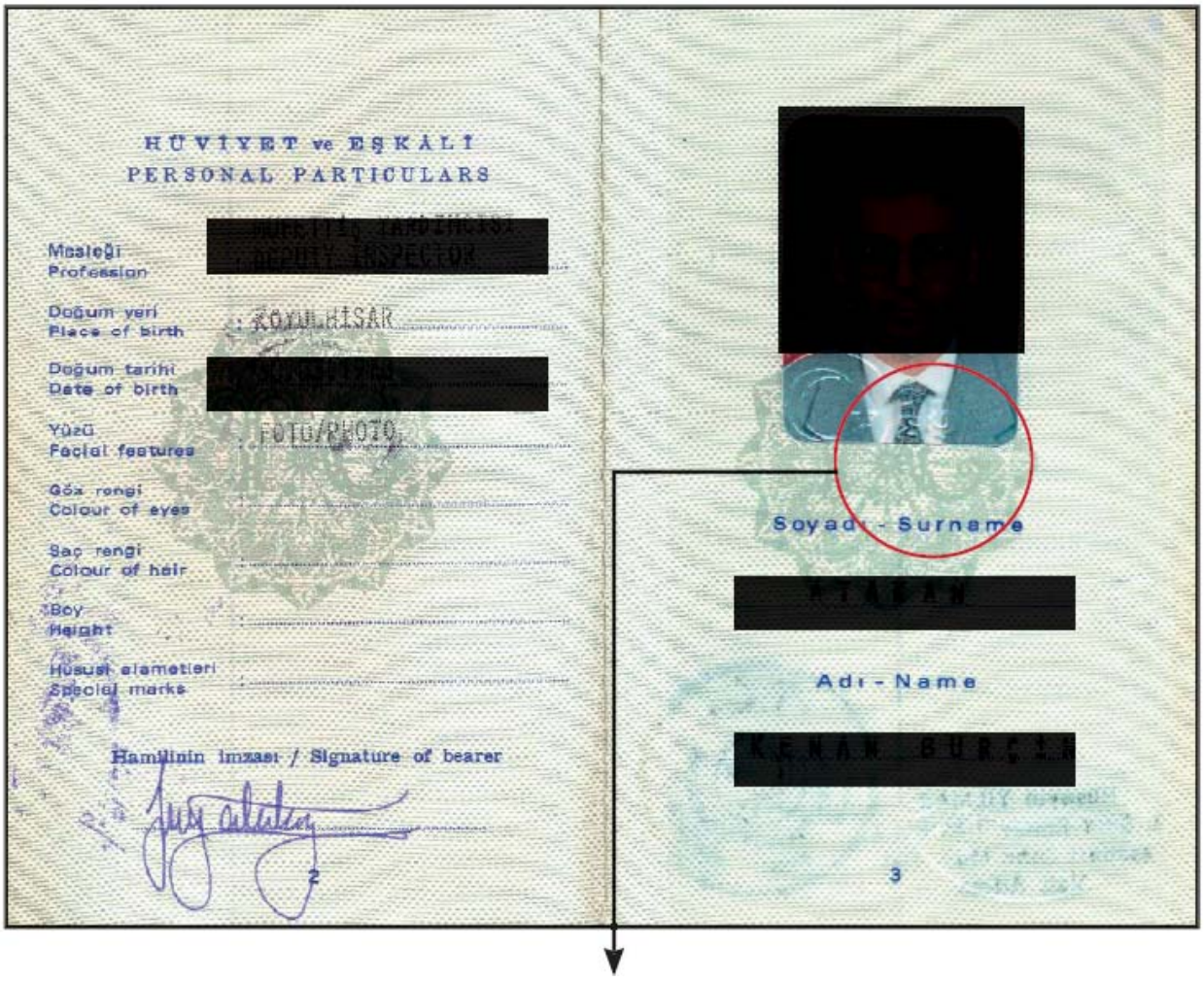
### 2.2.3 Pasaport Teyit Ederken Dikkat Edilmesi Gereken Hususlar

**1.** Yurt dışında yerleşik müşteriler genelde kimlik olarak pasaport kullanırlar. Kişinin beyan ettiği yurda giriş tarihi ile pasaport arkasında yer alan yurda giriş mührü karşılaştırılmalıdır.

**2.** Pasaport üzerinde yer alan soğuk mühür parmak teması ile hissedilmelidir.

**3.** Yurt dışında yaşayan Türkiye Cumhuriyeti vatandaşlarının yaşadıkları ülkelerdeki oturma izinleri kontrol edilmelidir.

**4.** Başka bir ülkede oturma izni olan bir kişinin, o ülkenin dilini konuşması ve o ülkenin temel özeliklerini bilmesi beklenir. Eğer, banka personeli ilgili ülkenin dilini konuşabiliyorsa şahsa bu dilde sorular sormalıdır.




**SOĞUK MÜHÜR**

**Şekil:9** Pasaportun Güvenlik Özellikleri


**Türkiye'ye Giriş-Çıkış Mühürleri** Müşterinizin anlatmış olduğu öyküyle tutarlı olmalıdır.


**Kaynak:** Türkiye Bankalar Birliği İnternet Bankacılığı Çalışma Grubu, Nisan 2007, , www.tbb.org.tr/v/doc/Kitapçık.pdf , (28 Eylül 2007), s.20.

## 3.3. KİMLİK TESPİTİNDE KULLANILACAK DİĞER BELGELER

Birçok banka, mevzuatında kimlik tespitinde kullanılacak belgelerini nüfus cüzdanı, sürücü belgesi ve pasaport olarak belirtmişse de, bunların dışında kimlik tespitinde birçok yardımcı belge kullanılabilir. Bunlar; askeri kimlikler, öğrenci kimlikleri, kurum kimlikleri ve tanıtım kartları, meslek odası kimlikleri, mesleki sertifikalar, diplomalar, "debit kart(banka kartı)" ve kredi kartları, isme düzenlenmiş faturalar, elektrik, su ve benzeri aboneliklerden kaynaklanan adrese gönderilmiş borç bildirim yazıları, telefon faturaları ve benzeri belgelerdir. Bu belgeler tek başına kimlik belgesi olarak kullanılmasa da, şüphelenilen durumlarda kişinin kimliğini tespit etmek için yardımcı belgeler olarak kullanılabilir.

Bir şube ile uzun süredir çalışan bir kişinin referansı kimlik tespitinde kullanılabilecek en önemli veridir. Bu kapsamda kimlik tespiti sırasında oluşacak şüpheleri gidermek için, müşteriye hizmet veren personelin veya bir şube çalışanının bu kişi hakkında referans vermesi veya şahsı makul bir süreden beri tanımış olması önemlidir.

## 3.4. BANKA KARTI SAHTECİLİĞİ

Banka kartları ile müşterilerin ATM(otomatik para çekme makineleri) ve POS(ödeme noktaları) aracılığıyla işlem yapması, 1980'li yılların ikinci yarısından sonra başlamış ve hızla yaygınlaşmıştır. Gelişen bu teknoloji sayesinde nakit ihtiyacı olan kişinin banka şubesine gitme zorunluluğu ortadan kalkarak, 24 saat boyunca nakit ihtiyacını karşılayacağı bir imkâna sahip olmuştur.

Dolandırıcı kişiler tarafından çeşitli yöntemlerle kart sahteciliği yapılmaya başlanmıştır. Bu yöntemlerden en sık kullanılanları kart sıkıştırma, kart kopyalama ve banka kartıyla alışveriş yöntemleridir.

### 3.4.1 ATM (Otomatik Para Çekme Makineleri) Kart Sıkıştırma

Dolandırıcılar; ATM(otomatik para çekme makineleri)'nin kart okuyucu bölmesine kâğıt, yapışkan maddeli kart ve benzeri yabancı maddeleri, bir kart vasıtası ile sıkıştırmaktadırlar. Bu işlemin uygulandığı bir ATM(otomatik para çekme makineleri)'de dışarıdan herhangi bir sorun görülmeyebilir. Ancak, ATM(otomatik para çekme makineleri) müşteri tarafından kullanılmaya çalışıldığında, kart sıkışacaktır. Dolandırıcı şahıs müşterinin arkasında bekler ve sıkışma sırasında müşteriye şifresini girmesi için yönlendirmede bulunur. Yardım eder gibi görünen kişinin aslında amacı mağdurun şifresini öğrenmektir. Bunun üzerine şifresini deneyen müşterinin parolası dolandırıcı şahıs tarafından görülecektir. Dolandırıcı şahıs ve müşteri işlem yapamayacaklarını anladıklarında ATM(otomatik para çekme makineleri)'nin başından beraberce ayrılıp başka bir ATM(otomatik para çekme makineleri) bulmaya giderler veya konu hakkında bankayı bilgilendirmeyi amaçlarlar. Ancak, dolandırıcı şahsın ortakları aynı anda ATM(otomatik para çekme makineleri)'nin kart okuyucu sisteminde sıkışmış olan kartı bir cımbız veya başka bir aparat kullanarak ele geçirir ve en yakın başka ATM(otomatik para çekme makineleri)'den müşterinin parasını çekerler. Hedef alınan müşteri kitlesinin genelde orta yaş ve üzeri emeklilerden oluşmaktadır. Emekli maaşlarının verildiği günlerde bu tip olaylara sıkça rastlanılmaktadır.

### 3.4.2 Kart Kopyalama

Müşterinin banka kartındaki bilgilerin ele geçirildiği ancak kart aslının müşteride kaldığı bir diğer yöntem de banka kartının manyetik alan bilgilerinin kopyalanmasıdır. Kart kopyalama iki yöntemle gerçekleştirmektedir. ATM(otomatik para çekme makineleri)'lere kurulan kopyalama kart okuyucu aparat, bir kamera ve bazı durumlarda sahte klavye yerleştirilmektedir. Kart okuyucu aparat, ATM(otomatik para çekme makineleri)'deki kart okuyucunun hemen önüne monte edilir. Müşteri kendi işlemini gerçekleştirirken klavyeye

girmiş olduğu tüm bilgiler aparata kayıt edilir. ATM(otomatik para çekme makineleri)'ye yerleştirilen kamera veya sahte klavye vasıtasıyla da müşterinin şifre bilgisi dolandırıcılar tarafından ele geçirilmektedir. Dolandırıcılık şebekeleri elde ettikleri kartların manyetik alan bilgilerini bilgisayardan kodlama yoluyla boş kartlara aktararak banka kartı özelliğine sahip kartlar oluştururlar. Kopyalama sırasında kart şifreleri temin edildiği için müşterilere ait hesaplarda kopya kartlarla istenilen ATM(otomatik para çekme makineleri)'den para çekilebilir ya da harcama yapılabilir. İkinci yöntem ise; kartın bir okuyucudan geçirilerek kopyalanmasıdır. Genellikle lokanta, dinlenme yerleri, alış veriş mağazalarında çalışan dolandırıcılık şebekesi üyeleri, ödeme yapılmak amacıyla verilen kartları pos cihazları dışında birde bu okuyucudan geçirirler ve kartın manyetik bilgileri bu okuyuculara aktarılmış olur. Daha sonra bu bilgiler bilgisayara aktarılarak yine kodlama yöntemiyle bilgisayardan kartlara yüklenir. Kopyalanmış kartlarla, sahte belgelerle açılmış olan üye işyerlerinden harcama yapılmış gibi gösterilir ya da sahte kimlik kullanılarak konudan habersiz üye işyerlerinde alışveriş yapılır. Bu yöntemde mağdurların herhangi bir yaş tercihi bulunmamaktadır. Kartın manyetik alanının kopyalanması özellikle yaz aylarında, turizm bölgelerinde veya büyük şehirlerde yaşanmaktadır.[32]

Bu durumda kart olduğu gibi imal edilmekte ve manyetik şerit bilgilerinin kopyalanmasıyla sahtecilik gerçekleştirilmektedir. Kopyalanan bilgiler gerçek kart hamiline ait bilgilerdir.[33]

### 3.4.3 Banka Kartı İle Yapılacak Dolandırıcılık Eylemlerinden Korunma

— Banka müşterileri para çekme makinelerinden işlem yaparken, kullanılan ekranın kimse tarafından görülmemesine dikkat etmelidir.

32 TBB, a.g.e, s.29.
33 Volkan Güner Güngör, "Bilişim Hukuku", Kadir has Üniv Yayınları, 2006, s.425.

— Banka kart cihaz içinde sıkıştığında, yakınlarda banka personeli varsa yardım istenmeli veya ilgili bankanın çağrı merkezi aranarak kartın kapatılması sağlanmalıdır. ATM (para çekme makinesi), kartın güvenliği sağlanmadan terk edilmemelidir.

— Müşterilerin kartları ile yapacakları alışveriş esnasında banka kartlarından yapılacak tahsilâtın, gözlerinin önünde olması gerektiği aksi takdirde kartın manyetik alanının kopyalanabileceği konusunda bilgilendirme yapılmalıdır.

Belirtilen güvenlik önlemleri için bilgilendirmeler banka personeli tarafından "banka kart" taleplerinin alınması sırasında veya e-posta, mobil telefonlarla kısa mesaj (SMS) bilgilendirmeleri şeklinde de gerçekleştirilebilir.

Bankaların sahip oldukları ATM(otomatik para çekme makineleri)'lere kamera sistemi takmaları, dolandırıcılar açısından caydırıcı olabilmektedir. Diğer yandan ATM(otomatik para çekme makineleri)'de oluşması muhtemel kalabalığa karşı ATM(otomatik para çekme makineleri) önüne bir çizgi çekilerek servis alan müşteri dışındaki şahısların çizginin gerisinde kalmaları sağlanmalıdır. ATM(otomatik para çekme makineleri) kart hareketleri güvenlik bölümleri tarafından yardımcı bazı yazılımlar kullanılarak incelenmeli, müşterinin şüpheli görünen nakit çekimleri veya alışverişleri mutlaka müşteriye sorulmalıdır.

Özellikle maaş ödeme günlerinde yoğunlaşan dolandırıcılık eylemlerini önleme amacıyla şubedeki güvenlik görevlisinin ATM(otomatik para çekme makineleri) önünü kontrol etmeleri ve müşterilere yardımcı olmaları gerekmektedir.

## 3.5. DOLANDIRICILIĞIN TESPİTİ VE İLGİLİ MERCİLERE BİLDİRİLMESİNİN ÖNEMİ

Bankaların, dolandırıcı şahısları eylem sırasında fark etmeleri ve en yakın jandarma veya emniyet birimlerine haber vermeleri müşteri, banka ve diğer bankalarında zarar görmemesi açısından önem arz eder. Dolandırıcı şahıslar tek başlarına hareket etmez.

Geniş bir çete yapısına sahiptir. Şubeye gelip para çekecek olan kişi veya mağdur müşterinin hesabından dolandırıcı şahsın hesabına aktarılan tutarı banka kartıyla çekecek olan kişi, sadece işlemin son aşamasını gerçekleştirecek kişidir. Bu eylemlerde bir kişinin bile yakalatılması diğer kişilere ulaşılmasını sağlayabilir. Ayrıca dolandırıcılık eyleminden sonra müşteriyi savcılığa suç duyurusunda bulunması için yönlendirmek bankaların birincil görevi olmalıdır. Savcılık suç duyurusuna istinaden soruşturma başlatır. Olay emniyete intikal eder ve emniyet birimleri olayın detayı hakkında araştırma yapmaya başlar. Burada yine bankaların üzerine önemli görevler düşer. Banka, emniyetin talep ettiği bilgileri eksiksiz ve detaylı bir şekilde emniyete vermekle yükümlüdür. Verilen her bilgi emniyeti dolandırıcı şahıslara bir adım daha yaklaştıracaktır. Ayrıca internetten yapılan tüm işlemlerde dolandırıcılığın gerçekleştiği IP (servis sağlayıcı) numarası bankaca tespit edilir ve emniyet tarafından talep edilir. Emniyet bu IP (servis sağlayıcı) numarasının hangi telefon ve adrese kayıtlı olduğunun bilgisini Türk Telekom' dan tespit eder. Bankaların dolandırıcılık eylemine ait tüm bilgileri detaylı olarak vermesi emniyet ve jandarmaya dolandırıcıların yakalatılması için ipucu vererek diğer dolandırıcılık olaylarıyla da bağlantı kurarak, başarılı operasyonlar yapılmasını sağlayacaktır. İnternet dolandırıcılığı farklı bankalarda farklı isimlerde gerçekleşse de sahte belgelerle aynı kişiler tarafından yapılıyor olması büyük bir olasılıktır. İnternet dolandırıcılığını yapan şahıslar birbirine bağlı örgütlerdir. Polis ve jandarma bankaların verdiği bilgilerden yola çıkarak ve verileri birleştirerek bu bilgi paylaşımını başarılı bir operasyona dönüştürebilir.

## 3.6. DOLANDIRICILIK OPERASYONU ÖRNEKLERİ

### 3.6.1 27 Haziran 2007 Jandarma' nın ' İnternet Fareleri' Operasyonu:

İstanbul' da, jandarma tarafından 26 ayrı adrese düzenlenen operasyonda, internet üzerinden banka hesap bilgilerini ele geçirdikleri kişilerin hesaplarını boşaltan 30 kişilik şebeke çökertilmiştir.

İstanbul İl Jandarma Komutanlığı ekipleri tarafından, bir şebekenin internet üzerinden dolandırıcılık yaptığının tespit edilmesi üzerine başlatılan istihbarat çalışmaları sonucunda, liderliğini Nedim K' nın yaptığı iddia edilen suç örgütünün, 1000 USD karşılığında satın alarak ya da sahte belge düzenleyerek bol miktarda kredi kartı temin ettiği belirlenmiştir.

Genişletilen incelemelerde, temin edilen kredi kartlarına ait hesap numaralarının, şebekenin "hacker" tabir edilen üyesi Eyüp İ' ye bildirilerek, daha önceden internet üzerinden şifreleri kırılmış mağdurlara ait hesaplardaki paraların suç örgütüne ait kredi kartlarına aktarıldığı anlaşılmıştır.

Bu tespitler üzerine delil elde etmek için bir süre araştırma yapan jandarma, adli makamlardan alınan arama ve el koyma kararı doğrultusunda şebeke üyelerini yakalamak amacıyla 26 ayrı adrese operasyon düzenleyerek, Nedim K. ile Eyüp İ' nin de aralarında bulunduğu 30 kişiyi göz altına almıştır.

Şüphelilerden, 5 adet tabanca, 160 adet tabanca fişeği, 9 adet bilgisayar, 1 hard disk, 141 adet farklı isim ve bankalara ait kredi kartı, 142 adet hesap cüzdanı, 190 adet CD, 21 adet pos cihazı, 8 adet şifre aleti, değişik kişiler adına düzenlenmiş çok sayıda kimlik kartı fotokopisi, çek, senet, banka dekontu ve para ile bir miktar uyuşturucu madde ele geçirilmiştir.

Operasyon sonrası, şebeke üyelerince internet üzerinden şifrelerinin elde edildiği belirlenen 15 kişinin durumunun jandarma görevlilerince bankalara bildirilmesi sayesinde, 22 kişinin hesabındaki 500 bin USD' nin bloke edilmesi sağlanarak vatandaşların zarar görmesinin engellendiği belirtilmiştir.

— ***Şebekenin Suç İşleme Yöntemi;***

Jandarma yetkilileri, şebekenin, "hacker" tabir edilen Eyüp İ. tarafından özellikle mağdurlara ait güvenliği alınmamış bilgisayarlara bulaştırılan casus yazılımlar vasıtasıyla internet banka hesap bilgileri ve şifreleri elde ettiğini, ardından vatandaşların hesaplarındaki paraların çeşitli yöntemlerle ele geçirilen kartlara gönderildiğini ifade

etmiştir.

Şebeke üyelerinin, hesaplardaki havale limitlerini artırabilmek ve SMS(kısa mesaj servisi) güvenliğini aşabilmek için mağdurlara ait cep telefonu SİM kartlarının kayıp olduğunu öne sürerek GSM bayilerine bildirdiklerini ve böylece sahte belgelerle yeni SİM kartı elde ettiklerini ifade eden yetkililer, daha sonra bu yöntem aracılığıyla çıkartılan bankamatik kartlarını kullandıklarını söyledi. Yetkililer, şebeke üyelerince şifresi ele geçirilen hesaptan havale yapılan bankamatik kartlarıyla şebeke üyesi iş yerinden alışveriş yapılmış gibi göstererek pos cihazından para çekimi yapıldığını dile getirerek, bu işlem sonucunda ele geçirilen paranın yüzde 25–35' inin iş yeri sahibine verildiğini, geri kalan kısmın ise şebeke üyelerince paylaşıldığını anlatmıştır.

Yetkililer, bankalarla koordineli olarak yapılan operasyonda**,** bazı vatandaşların ele geçirilmesi planlanan hesaplarındaki yaklaşık 500 bin YTL' nin kurtarıldığını dile getirerek, söz konusu dolandırıcılık suçunun mağdurları arasında emekli ikramiyesi çalınan bir öğretmen ile tedavisi için biriktirdiği parayı çaldıran bir kanser hastasının da yer aldığına dikkat çekmiştir.

Şebeke üyelerinin elde ettikleri paralarla lüks bir hayat yaşadıklarını da vurgulayan jandarma yetkilileri, bu kişilerin son model araçlar kullandıkları, İstanbul'un lüks restoranlarında yemek yedikleri, eğlence yerlerinde partiler düzenledikleri ve uyuşturucu âlemi yaptıklarının belirlendiğini kaydetti. Operasyonda gözaltına alınan 30 şüpheli, jandarmadaki işlemlerinin ardından "Büyükçekmece Adliyesi" ne gönderilmiştir.[34]

### 3.6.2 İzmir Emniyeti Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü Mali Büro Amirliği Sanal Banka Dolandırıcılığı Operasyonu:

34 Anadolu Ajansı, "İnternet Dolandırıcılarına Ağır Darbe", 27.06.2007, http://www.haber7.com/haber.php?haber_id=251716, (08 Aralık 2007)

İzmir' de, internet aracılığıyla Rus hackerlerden elde ettikleri yerli ve yabancı kişilere ait hesap bilgileriyle kredi kartı düzenleyip yurtiçi ve yurtdışında kullanarak haksız kazanç sağlayan uluslararası 13 kişilik şebeke, polisin operasyonuyla çökertilmiştir.

Anlaşmalı işyerlerine ve ATM cihazlarına manyetik cihazlar yerleştirip vatandaşların bilgilerini de elde eden zanlıların, çoğunun üniversite mezunu olduğu, 3'ünün 5 dil birden bildiği öğrenildi. Binlerce kişinin kredi kartıyla işlem yapan zanlıların evlerinde bulunan kartların çip bilgilerini okuyan 2 'smart card reader( akıllı kart okuyucu)' ve pos makinalarının bağlı olduğu telefon hatlarına bağlanıp işlemlerde kullanılan bütün kart numara ve bilgilerini kaydeden bir 'telephone call lagger' adlı cihazların Türkiye'de ilk kez ele geçirildiği bildirilmiştir.

İzmir Emniyeti Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü Mali Büro Amirliği ekipleri, vatandaşlardan gelen şikâyetler ve teknik takipleri doğrultusunda, Basmane Semti'ndeki bir otelde çalışan 37 yaşındaki Cumhur Ser'in elebaşılığını yaptığı bir şebekenin, internette MSN aracılığıyla irtibat kurduğu Rus hackerlardan yerli ve yabancı kişilere ait hesap bilgilerini edindiğini, bunlarla kredi kartı düzenleyip yurt içi ve yurt dışına kullanarak haksız kazanç sağladığını saptadı. 6 aydır sürdürülen soruşturmada, bilgileri ele geçirilen kişiler adına sahte kredi kartı ve kimlikler düzenlendiği, bu kartların, komisyon karşılığında anlaşılan çeşitli illerdeki turistik yerlerde kullanıldığı belirlendi. Ayrıca, internetteki bir kredi kartı sitesine de üye olan zanlıların, para karşılığı da hesap bilgilerine ulaştığı tespit edildi. Çeşitli ülkelerdeki kredi kartı kopyalama cihazlarını Türkiye'ye getirerek yeni yöntemler bulmaya çalışan zanlıların, bankaların ATM cihazlarına da manyetik cihazlar yerleştirip vatandaşların bilgilerini de elde ettiğinin saptanması üzerine harekete geçilmiştir. Eldeki bilgi ve delillerinin toplanmasının ardından İzmir, Uşak ve Kocaeli'nde gerçekleştirilen baskınlarda, elebaşı Cumhur Ser, Samuel Kemal Dinler (39), Alpnehir Barman (40), Mehmet Turgut (41), Ümit Kamil Aktaş (26), Osman Alaçam (28), Mesut Demirtaş (35), Mustafa Efe (28), Adalet Bozkurt (45), Çağtay Kaldemir (19), Erdoğan Lokman (41), Hakan Tekbastı (37) ve Bekir Özgür (28)

yakalanmıştır.

Zanlıların evlerinde ve bazı yerlerde yapılan aramalarda, sahte kartların kabartma ve rakamlarını basan embosser cihazı, manyetik alanlarını yazan encoder cihazı, kart bilgilerini kopyalayan papağan cihazı, ATM'lere takılan kart aparatları, 552 şeritli plastik kart, 6 değişik bankalara ait POS cihazı, sahte kimlikler, belgeler, bilgisayar, 3 boş pasaport, 2 ruhsatsız tabanca, 83 mermi ele geçirildi. Baskınlarda, ayrıca, kartların çip bilgilerini okuyan iki 'smart card reader' ve POS makinalarının bağlı olduğu telefon hatlarına bağlanıp işlemlerde kullanılan bütün kart numara ve bilgilerini kaydeden bir 'telephone call lagger' adlı cihazın Türkiye'de ilk kez ele geçirildiği bildirildi. Şu ana kadar yöntemleriyle binlerce insanı mağdur eden zanlıların, sorgulamasında, çoğunun üniversite mezunu olduğu ortaya çıktı. Zanlılardan Alaçam, Demirtaş ve Dinler'in 5 dil bildiği öğrenildi. Yabancı kişilerin kredi kartlarını genellikle Japonya, Tayland ve Kıbrıs'ta kullandığı da öğrenildi. Emniyet yetkilileri, zanlıların, çok profesyonel faaliyet gösterdiklerini, ne kadar kişinin mağdur edildiğinin tespit edilmeye çalışıldığını, firardaki 3 kişinin yakalanması için çalışmaların sürdüğünü bildirdi. Sorgularının ardından işlemleri tamamlanan 13 zanlı da adliyeye sevkedilmiştir.[35]

# 4. BİLİŞİM SUÇLARI VE HUKUKU

Bilişim kelimesi; insanların teknik, ekonomik ve toplumsal alanlardaki iletişimlerinde kullandıkları, bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akılcı biçimde işlenmesi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi demektir. Bu alanda tanımlanan suçlar; bilgisayar suçu, bilgisayarla

35 Burak Akdağ, "İnternet Dolandırıcılığı Şebekesi Çökertildi", 01.11.2007, http://www.polishaber.com/article_view.php?aid=15650 , (24 Kasım 2007)

ilgili suç, bilgisayar suçluluğu, elektronik suç, bilgisayar vasıtasıyla işlenen suçlar, bilişim suçları ya da suçluluğu, bilişim ihlali gibi terimlerle tanımlanmaktadır.[36]

Bilişim suçları ilk olarak, bilgisayarında geliştirildiği Amerika Birleşik Devletleri'nde ortaya çıktığı için bu yeni suç tipinin adlandırılması da bu ülke hukukçuları tarafından yapılmıştır. Amerikan öğretisi ve uygulamasında bu suç tiplerine genel olarak ' compiter crime' denilmektedir.[37]

Suç, insanlık tarihi kadar eski bir kavramdır. Her dönemde, dönemin şartlarına göre şekil alan suç ve suçlu kavramı da günümüzdeki dönüşüme paralel gelişmeler göstermektedir. Bilişim teknolojisinin gelişmesi ve bilginin eski devirlere göre daha çok önem kazanması, bilginin ekonomik, sosyal, siyasal değerinin artması, bu değerler üzerinde kolay yoldan hak sahibi olmak isteyen kişileri, bilişim teknolojisi marifetiyle suç işler hale getirmiştir. Ayrıca günümüze kadar suçlu grubunda yer almayan binlerce insan, artık bilişim teknolojisi marifetiyle suç işlemeye başlamıştır. Bunun temel sebeplerinden birisi, hayatı kolaylaştıran teknolojinin, suç işlemeyi de kolaylaştırmasıdır.[38]

Suçla mücadele kavramı modern toplumlarda sosyal düzenin sağlanması ve geliştirilmesinden sorumlu tutulan polis, günümüzde geleneksel suça müdahale edici yaklaşımını terk ederek, suç önlemeye yönelik çalışmalara odaklanmaktadır. Toplum destekli suç önlemeye dayalı polislik felsefesi; suçla mücadelenin polis ve devlete ait bir görev olmakla birlikte, toplumsal bir işbirliğiyle suçların oluşmadan önlenmesi ve suç sebeplerinin ortadan kaldırılmasıyla kamu güvenliğinin sağlanmasını amaçlayan faaliyetler bütünüdür.[39]

Gerçek ve köklü bir suçla mücadele yöntemi olan önleyici suç önleme süreci aşamaları aşağıdaki gibidir;

— Suç ve suçlularla ilgili tüm bilgilerin toplanması,

---

36 Cevat Özel, "Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", İstanbul Barosu Dergisi, İstanbul, Eylül 2001, Sayı:7-8-9, s.863.

37 Murat Volkan Dülger, "Bilişim Suçları", Ankara: Seçkin Yayıncılık, 2004, s.63.

38 Mehmet Özcan , "Türkiye'de İnternet Konferansları VII" İstanbul Harbiye Askeri Müzesi, Bilal Şen, "Bilişim Suçlarının Getirdikleri ve Üzeyir Garih Cinayeti", Polis Dergisi, Aralık 2002, Sayı: 29, s.13-24.

39 Hüseyin Şimşek, "Toplum Destekli Polislik", Yüksek Lisans Tezi, Kırıkkale, 2002, s.13-24

— Suç oluşumunu kolaylaştıran şartların tespiti ve analizi,

— Suça zemin hazırlayan şartların önünü alabilecek olası önleyici vasıta ve tedbirlerle ilgili çalışmaların yapılması,

— En isabetli, ekonomik ve uygulanabilir tedbirlerin seçimi ve uygulamaya konulması,

— Uygulama sonuçlarının takibi ve değerlendirilmesi aşamalarından oluşmaktadır.[40]

İnternet suçlarının artmasında ve daha önce adli suç işlememiş kişilerin internet aracılığıyla suç işler hale gelmesinde suç işlemenin kolaylaşmasının yanı sıra, kullanıcıların internet üzerinden gerçekleştirilen eylemlerin herhangi yasal bir yükümlülüğünün ve herhangi bir yasal düzenlemenin olmadığına dair yanlış bir yargının bulunmasıdır. Ayrıca bu suçları işleyenler arasında, yaptıklarının suç olup olmadığını bilmeyen veya düşünmeyen, sadece bilinmezin, ulaşılmazın büyüsüne kendini kaptırmış, ama eylemleri çok derin hasarlar bırakan, büyük bölümü çocuk yaşta binlerce insan vardır.[41]

İnterneti iletişim, bilgi edinme ve paylaşım gibi iyi amaçlarla kullanan kullanıcıların varlığına karşılık, teknolojinin yaramaz çocukları olarak adlandırılan geleneksel olarak bireyleri suç işlemeye götüren nedenlerle hareket eden, sistemlerin açıklarını bularak bu sistemlere atak yapan ve sisteme izinsiz girerek çeşitli hasarlar yaratan programcılar ve bilgisayar ile uğraşan hackerlar ortaya çıkmıştır.[42] Bilişim teknolojisinden faydalanarak internetteki yerini almak isteyen "terör örgütleri"nin faaliyetlerini bu ortama taşıması[43], "hırsızlık" ve "dolandırıcılık" gibi suçların bu ortamda işlenmeye başlanması, internet'te izinsiz yayınlanan film, müzik ve oyunların oluşturduğu "lisans hakları

40 Aytekin Geleri, Mustafa Soysal, Mustafa Kaygısız, Tamer Azem Arslan, "İnternet Suçlarıyla Mücadelede Suç Önleme Anlayışı ve Bilinçli Kullanıcı" 27.06.2007, http://www.bilisimsuclari.com, ( 01.12.2007)

41 Bilal Şen, "Bilişim Suçlarının Getirdikleri ve Üzeyir Garih Cinayeti", Polis Dergisi, Yıl 7, S. 29, Ekim-Kasım-Aralık 2002, 13–24.

42 R.Yılmaz Yazıcıoğlu, "Bilgisayar Suçları", İstanbul: Alfa Yayınevi, 1997, s.120–121.

43 M.Volkan Dülger: "Bilişim Suçu Olarak Pornografi", 09.09.2004, http://turk.internet.com/haber/yazigoster.php3?yaziid=10852 , (29Aralık 2007)

ihlalleri"[44] şeklindeki suçların genişlemesi, hakaret amaçlı sitelerin kurulması ve bilgisayar orijinli resimler yoluyla yasadışı yayınların giderek artması[45] internetin kötü amaçla kullanılabileceğini göstermektedir.

## 4.1. BİLİŞİM ALANINDA SUÇLAR BÖLÜMÜNDE DÜZENLENEN SUÇ TİPLERİ

### 4.1.1 Hukuka Aykırı Olarak Bilişim Sistemine Girme ve Sistemde Kalma Suçu(m.243)

Bu maddeyle yasa koyucu "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme ve orada kalmaya devam etme" eylemini suç tipi haline getirmiştir. Bilişim sistemine girişlerin cezalandırılması için verilerin ele geçirilmesi şartı kaldırılmakta ve veri ele geçirilsin ya da geçirilmesin bilişim sisteminin güvenliğinin ihlal edilmesi suç haline getirilmektedir.[46]

Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçuna karşılaştırılmalı hukukta birçok ülke hukukunda yer verilmektedir. Bu ülkelerde örnek olarak; Fransa CK. m.323–1, Alman CK. m.202a, Danimarka CK. m193 ve 263, İtalya CK. m.6–2 verilebilir. Bu suç tipi genellikle verilerin ele geçirilmesi suçuyla birlikte düzenlenmektedir.[47]

Bilişim sistemine hukuka aykırı erişimin engellenmesiyle, sistemden faydalanan kişilerin çok sayıdaki farklı türden çıkarları korunmaktadır. Bu kişilerin çıkarları verilerin

---

44 Mustafa Toplaoğlu: "İnternette Fikri Haklar Sorunları" 09.09.2004, http://turk.internet.com/haber/yazigoster.php3?yaziid=10852 , (29Aralık 2007),

45 David S. Wall, "İnternet Rejimi ve Düzenleme Sorunu", Çev: Hasan Sınar, Adalet Yüksek Okulu, 20.Yıl Armağanı, İstanbul, 2001, s.203.

46 Yılmaz Yazıcıoğlu, "Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirmesi", Hukuk ve Adalet: Eleştirel Hukuk Dergisi, İstanbul, Ocak-Mart 2004, Sayı:1, s.177., Berrin Akbulut, "Türk Ceza Kanununda Bilişim Suçları", Yayımlanmamış Doktora Tezi (Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Ceza ve ceza Usul Hukuku Bilim Dalı), Konya, 1999, s.78, Olgun Değirmenci, "Bilişim Suçları", Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2002, s.153.

47 Stein Schjolberg, "The Legal Fremework-Penal Legislation in 44 Countries", 08.02.2004, www.mosstingrett.no, (17 Aralık 2007)

gizliliğinin korunması, özel hayatın dokunulmazlığı ve kurumların ihtiyaç duyduğu güvenlik duygusu gibi farklı hukuksal değerleri kapsamaktadır.[48]

Bu suçla korunan hukuksal değer bilişim sisteminin güvenliğidir. Suça ait maddi unsuru, hangi yolla olursa olsun bilişim sitemine girmek ve orada kalmaya devam etmek oluşturmaktadır.[49]

### 4.1.2 Bilişim Sisteminin İşleyişinin Engellenmesi, Bozulması Verilerin Yok Edilmesi veya Değiştirilmesi Suçu (m.244/1-2)

Bu madde de bilişim sistemine ve verilere her ne yöntemle olursa olsun zarar verme eylemleri düzenlenmiştir.

Günümüzde modern yaşama düzeninin ana konularını oluşturan ekonomi, sağlık, eğitim, bilimsel, araştırmalar, idare ve savunma gibi pek çok yaşamsal alanda bilişim sistemleri vazgeçilmez araçlar olmuşlardır. Bu nedenle bilişim sistemlerine ve içerdiği verilere karşı yapılan saldırılar sonu bu sistemlerin zarar görmesi ya da geçici olarak çalışmaması çok büyük zararlara neden olabilmektedir. Yasa koyucu da bu büyük tehlikeyi öngörerek verilere ya da veri işlemeye zarar verme eylemlerini bu madde ile suç haline getirmiştir.[50]

### 4.1.3 Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu (m.244/4)

Hukuka aykırı yarar sağlamak, banka ve kredi kartlarını kötüye kullanmak, bilişim sistemleri aracılığıyla dolandırıcılık ve hırsızlık eylemleri farklı suç tipleri olarak düzenlenmiştir. Bunların nasıl gerçekleştirileceği suç tipinde açıkça belirtilmiştir.

---

48 Necati Meran, "Yeni Türk Ceza Kanununda Sahtecilik – Malvarlığı Bilişim suçları ile Ekonomi ve Ticaret Alanında Suçlar", Ankara: Seçkin Yayıncılık, 2005, s.363.

49 Levent Kurt, "Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanundaki Uygulanması", Ankara: Seçkin Yayıncılık, 2005, s.151. - Ali Karagülmez, "Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri", Ankara: Seçkin Yayıncılık, 2005, s.167

50 Av.Murat Volkan Dülger, "Bilişim Suçları, Ankara: Seçkin Yayıcılık, 2004, s.65

### 4.1.4 Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (m.245)

Bu maddeyle yasa koyucu sahte kredi veya banka kartlarının kötü amaçla kullanılması için üretilmesini durdurmak istemekte ve bu kartların üretilmesinden kullanılmasına kadar geçen dört aşamayı cezalandırmaktadır. Bu aşamalar; kartın sahte olarak üretilmesi, satılması veya devredilmesi, satın alınması ve devir alınması, son aşama da bunların haksız yarar elde etmek amacıyla kullanılmasıdır.

Bu suçun gerçekleştirilmesiyle kişilerin mal varlığı üzerinde büyük zararlar verilmektedir. Bu suçla korunan hukuksal değer kişinin mal varlığı olarak belirlenmektedir.[51]

## 4.2. BİLİŞİM SUÇLARINDA UYGULANICAK CEZALAR

Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır.

Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, ikinci fıkraya göre verilecek cezalar yarı oranında artırılır.

---

51 Murat Volkan Dülger, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu" , Güncel Hukuk Dergisi, İstanbul, Kasım 2005, Sayı 23, s.28–30.

Bir donanım ve programı, bu Kanunda tanımlanan suçları işlemek amacıyla üreten, uyarlayan, ithal eden, satan, sağlayan, dağıtan, tanıtan veya aynı amaçla bilişim sisteminin tamamına veya bir kısmına erişimi mümkün kılan parola, erişim kodu veya benzer veriyi sağlayan kişi, iki yıldan beş yıla kadar hapis ve ikibin güne kadar adlî para cezası ile cezalandırılır.

Bilişim sistemiyle kendisi veya başkası lehine haksız yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, iki yıldan beş yıla kadar hapis ve bin günden beşbin güne kadar adlî para cezası ile cezalandırılır.[52]

## 4.3. BİLİŞİM SUÇLARI KANUNU HAKKINDAKİ GÖRÜŞLER

Bilişim sistemlerinin organize suçlarda ve sanal terörizmimde kullanılması durumları düzenlenmeli ve bu konu açısından ilgili yasalarda düzenlemeler yapılmalıdır.[53]

İstenmeyen elektronik iletilere ilişkin diğer ülkelerde yapılan düzenlemeler dikkate alınarak bu soruna çözüm getirilmeli ve istenmeyen elektronik ileti gönderilmesi suç haline getirilmelidir.[54]

Ülkemizde yürürlülükteki mevzuatta kişilerin internetteki eylemlerinden kaynaklanan cezai sorumluluğunu belirten bir düzenleme bulunmamaktadır.[55]

Ayrı bir yasada internet servis sağlayıcıların, erişim sağlayıcılarının ve içerik sağlayıcılarının ceza hukuku açısından sorumlulukları ayrı ayrı düzenlenmelidir.[56]

Bilişim suçlarıyla mücadelede maddi ceza hukukunun ve ceza muhakemesi hukukunun birlikte ele alınmasıyla bir sonuç elde edilmesi mümkündür. Bilişim suçlarının özelliği dolayısıyla uluslararası nitelikte olması, suçun işlendiği yer bakımından sorunların

52 Prof. Dr. Eşref Adalı, "Bilişim Ağı Hizmetlerinin Düzenlenmesi Bilişim Suçları Hakkında Kanunu Tasarısı", http://160.75.26.41/, ( 18 Aralık 2007), s.8.
53 Yener Ünver, "Ceza Kanunun Değerlendirilmesi", Ankara: Seçkin Yayıncılık, 2006, s.106.
54 Emrehan İnal, "Reklâm Hukuku ve Aldatıcı Reklâmlar", İstanbul: Beta Yayıncılık, 2000, s.102.
55 Selman Dursun, "Bankacılık Düzenine Karşı İşlenen Suçlar", Ankara: Seçkin Yayıncılık, 2006, s.285.
56 Gökhan Ahi, "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler", 04.07.2005, http://hukukcu.com/modules/smartsection/item.php?itemid=74, (12 Kasım 2007)

çıkmasına buda suçun kovuşturmasının nerede yapılacağı sorununa yol açmaktadır. Bu sorunların aşılması ancak uluslararası işbirliğine işlerlik kazandırılmasıyla mümkün olacaktır. Avrupa Siber Suç Sözleşmesi' nde bu konuda ayrıntılı düzenlemeler bulunmaktadır. Bu sözleşmeye ülkemiz tarafından da taraf olunması ve 5237 sayılı TCK' nın suçun işlendiği yer konusunda ilişkin maddelerinde bu sözleşmeye paralel gerekli düzenlemelerin yapılmasıyla bu sorunun aşılması mümkün olabilecektir.[57]

Suçla mücadele için öncelikli olarak yapılması gereken bir adli bilişim biriminin kurulmasıdır. Bu adli tıp içinde de kurulabilir. İkinci olarak hâkim ve savcılarımıza yeterli eğitim verilmelidir. Üçüncü husus ise servis sağlayıcılara yasal yükümlülükler getirerek delillendirme de yaşanan problemlerin önüne geçilmelidir.

Delillendirme de en hayati nokta, gelen sahte elektronik postanın kağıt çıktısının 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 gerekir.

Böyle bir eyleme maruz kalan kişi bankasını bilgilendirmeli ve ardından savcılığa dilekçe ile başvurmalıdır. Burada hem mağdura hem savcıya hem de güvenlik güçlerine düşen görev hayati önemdeki birkaç delilin en kısa zamanda toplanmasını sağlamaktır.

Dünya, teknolojinin hızla gelişmesiyle ortaya çıkan bu eyleme hazırlıksız yakalanmıştır ve bu sebeple bu suçu açıkça düzenleyen bir yasa maddesi bulunmamaktadır. ABD' li hukukçuların "The Anti – Phising Act" olarak adlandırdıkları yasa tasarısı ile büyük finansal kayıplara neden olan bilişim suçları önlenmek istenmektedir.[58]

---

57 Hasan Sınar, "Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme" , İstanbul: Galatasaray Üniversitesi Yayınları, 2004, s.785.

58 Ali Osman Özdilek, Burak Çekiç, Muharrem Taç, "Sanal Dolandırıcılık (Phising)", 30.01.2006, http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=3&id=16, (12 Kasım 2007)

## 4.4. BİLİŞİM SUÇLARI ALANINDA YAPILAN ULUSLARARASI ÇALIŞMALAR

Kayıtlara geçen ilk bilişim suçu, 18 Ekim 1966 tarihli Minneapolis Tribüne gazetesinde yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" isimli makale ile kamuoyuna duyurulmuştur.[59] Bu olaydan bir süre önce, 1960'lı yılların başında Amerikan telefon santrallerini kullanan ve bedava uzun mesafeli telefon görüşmesi yapan "phreaker"lar; elektronik korsanlar olarak bir yer altı dünyası yaratarak faaliyetlerini sürdürmekteydiler.[60]

1970'li yılların ilk yarısından itibaren hükümetler ve uluslararası kuruluşlar bilişim suçlarıyla ilgilenmeye başlamış ve bu alanda düzenlemeler getirmiştir. Bilişim suçları ile ilgili ilk kapsamlı kanun teklifi 1977'de Senatör Ribikoff tarafından Amerikan Kongresi'ne sunulmuştur. Bu teklif Kongre tarafından kabul edilmemesine rağmen, bu suç grubunun dünya çapında tanınmasını sağlamıştır.[61]

13 Mayıs 1974'de Parlamentolar Arası Çalışma Birliği'nin Bonn'da yaptığı toplantıda bilişim suçları ele alınmıştır. Bu toplantı sırasında bilişim sistemlerinden istifade edenlerin, bilişim sistemlerinin kötüye kullanılmasından doğan tehlikeler ve bilişim sistem ihlalleri hakkında çok az bilgiye sahip oldukları, bilişim sistemlerinin kötüye kullanılması ve ihlallerinin önlenmesi için gerekli yüksek yatırım rakamlarından korktukları gibi gerçekler ortaya çıkmıştır. Toplantı esnasında kötüye kullanma ve ihlallerin önlenmesi için kanun zoru ile alınması gereken asgari tedbirler de tartışılmıştır ancak teklif, bilişim sistemleri üreticileri ve bilişim sistemleri kullanıcıları tarafından işletmenin iç organizasyonuna müdahale sayıldığı için reddedilmiştir.[62]

---

59 Emin Aydın, "Bilişim Suçları ve Hukukuna Giriş", Ankara: Doruk Yayınları, 1992, s.25

60 Mungo Paul, Clough Bryan, "Sıfıra Doğru Veri Suçları ve Bilgisayar Yer altı Dünyası", Çev.:Emel Kurma, İstanbul: İletişim Yayınevi, 1999, s.20.

61 Stein Schjolberg, "Unauthorized Access to Computer Systems",15.01.2003, www.mossbyrett.of.no/info/legal.html, (12 Kasım 2007)

62 Feridun Yenisey, "Bilgisayarla İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi", 1975 http://www.caginpolisi.com.tr/37/59-60-61-62-63-64.htm, (15 Aralık 2007), s. 331-332.

Avrupa Konseyi 1970'li yıllarda elektronik bilgi bankalarında işlenen veriler dolayısıyla, bireylerin özel hayatının korunması amacına yönelik çalışmalar başlatmıştır. 1973 ve 1974 yılında Avrupa Konseyi Bakanlar Komitesi, elektronik veri bankalarında uygulanacak ilkeleri kapsayan 2 tavsiye kararı kabul etmiştir. Bu tavsiye kararı uyarınca başta Almanya olmak üzere Avusturya, Fransa, Danimarka, Norveç gibi ülkeler 70'li yılların sonunda "Verilerin Korunması" konusunda özel yasaları hukuk mevzuatlarına dâhil etmişlerdir.[63]

Telekomünikasyon sistemlerinde meydana gelen gelişmeler ve veri iletişim hızlarının ülkeler arası çok yüksek hızlarda yapılması karşısında elektronik veri bankalarında saklanan, kişilerin özel hayatlarına ilişkin verileri koruma konusunda Avrupa Konseyi üyesi ülkelerin mevzuatlarının yetersiz kalmasından dolayı, konuyu uluslararası boyutta ele almak ve uluslararası bir sözleşme ile düzenlemek gereği doğmuştur. "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması"na ilişkin 108 sayılı sözleşme, 28 Ocak 1981 tarihinde imzaya açılmış ve aynı tarihte Avrupa Konseyi üyesi ülkelerle birlikte Türkiye tarafından da imzalanmıştır.[64]

Bilişim suçları alanında karşılaştırmalı olarak ceza yasalarının birbiri ile uyumlaştırma çalışmalarına ilk kez 1983 yılında OECD ülkelerinde başlanmıştır. Bu çalışmalar 1986 yılında sonuçlanmış ve "Bilgisayarla İlgili Suç: Hukuki Politikaların Analizi – Computer Related Crime: Analysis of Legal Policy" raporu ile üye ülkelere birtakım ihlalleri müeyyide ile karşılamak için gerekli düzenlemeleri yapmaları tavsiye edilmiştir. OECD tarafından hukuki düzenleme altına alınması tavsiye edilen ihlaller şunlardır;

— Bilgisayar yoluyla dolandırıcılık,

— Bilgisayar yoluyla sahtecilik,

— Bilgisayar program ve verilerinde değişiklik yapılması,

63 Veysel Bozkurt, "Elektronik Ticaret Hukuk Çalışma Grubu Raporu", İstanbul: Alfa Yayınları , 1998, s.266.
64 Olgun Değirmenci, "Bilişim Suçları", Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, İstanbul 2002, s.40.

— Bilgisayar programlarının telif haklarına aykırı olarak kopyalanması, çoğaltılması ve dağıtılması,

— Telekomünikasyon sistemlerinin, bilgisayarın diğer fonksiyonlarının ve iletişiminin değişikliğe uğratılması.[65]

Avrupa Konseyi'nin görevlendirdiği bir uzmanlar komitesi, 1986 yılında hazırladığı raporu esas alacak şekilde bir çalışma yapmıştır. Bu çalışma sonucunda rapor doğrultusunda bu raporda belirtilen ihlallerin üye ülkelerin ceza kanunlarına ithal edilmesi gerektiği fikrini benimsemiş ayrıca raporda yer almayan bir takım ihlallere de yer vermiştir. Konsey'in bu alandaki ikinci çalışması 1995 yılında yapılmıştır. 11 Eylül 1995 tarihinde Bakanlar Komitesi tarafından kabul edilen bir çalışmada, bilişim teknolojilerinin getirdiği yeniliklere göre ceza usul yasalarındaki soruşturma ve el koymaya ait hükümlerin değiştirilmesi, elektronik delil, şifreleme sistemlerinin kullanılması, uluslararası işbirliği başlıkları altında ceza usul yasalarında yapılacak değişikliklere dair kurallar konulmuştur.[66]

Washington DC.'de Aralık 1997'de toplanan G8 İç ve Dışişleri Bakanları "İleri Teknoloji Suçları"nı ele almışlardır. Bakanlar 10 prensip ve 10 noktada eylem planı üzerinde anlaşmaya varmışlardır. Buna göre;

— Telekomünikasyon ve bilgisayar sistemlerine yapılan ihlallerin cezai müeyyide ile karşılanması hususunda üye ülkelerin hukuk sistemlerinin gözden geçirilmesi ve ileri teknoloji suçlarının araştırılmasının geliştirilmesine yardımcı olunmasına,

— İleri teknoloji suçlarıyla artan hususların karşılıklı yardım anlaşmalarının ve düzenlemelerin yapılması sırasında göz önünde bulundurulmasına,

— Ülkesel bazda yerleri tespit edilmeyen verilerin bilgisayar yolu ile araştırılması ve sınırlar ötesi araştırma, karşılıklı yardım için yerine getirilmesi önerilen delillerin

65 Yasin Beceni, "Siber Suçlar", 01.01.2003, http://hukukcu.com/modules/smartsection/item.php?itemid=83, (18 Aralık 2007), s.26.
66 Değirmenci, a.g.e, s.41

muhafaza edilmesi hususlarında uygulanabilir çözümlerin geliştirilmesi ve incelenmesinin devam edilmesine karar verilmiştir.[67]

Ayrıca G8 bünyesinde (A.B.D., İngiltere, Fransa, Almanya, İtalya, Japonya, Kanada, Rusya ve Avrupa Birliği' ninde bünyesinde kurumsal olarak yer alan bir birliktir.) yapılan çeşitli toplantılarda konuya ilişkin öneriler ve tavsiye kararları da sunulmuştur.

Birleşmiş Milletler bünyesinde konu 7. ve 8. Suçtan Korunma ve Suçluların Rehabilitasyonu Kongrelerinde tartışılmıştır. Son olarak İtalya'da düzenlenen "Sınırlar Ötesi Organize Suçlarlarla Mücadele Sempozyumu"nda bilişim suçları ele alınmış ve çözüm önerileri getirilmeye çalışılmıştır.

Bilişim suçlarına ilişkin en kapsamlı düzenleme Avrupa Konseyi bünyesinde gerçekleştirilen "Avrupa Siber Suç Sözleşmesi"dir. Avrupa Konseyi Suç Sorunları Komitesi (European Committee on Crime Problems) Kasım 1996'da siber alanda işlenen suçlar üzerinde çalışmak üzere bir uzmanlar komitesi (The Committee of Experts on Crime in Cyber-Space) oluşturmuştur. Komite Nisan 1997'de başladığı çalışmaları sonucunda Siber Suçlar Sözleşme Taslağı ile açıklayıcı raporu Avrupa Suç Sorunları Komitesi'ne Haziran 2001'de sunmuştur. Taslak, 8 Kasım 2001'de Avrupa Konseyi Bakanlar Komitesinde kabul edilerek, 23 Kasım 2001'de Budapeşte'de düzenlenen Siber Suçlar Uluslararası Konferansında imzaya sunulmuştur. Sözleşmeye 26 Avrupa Konseyi üyesi ülke ile beraber ABD, Japonya, Kanada ve Güney Afrika imza koymuşlardır.[68] Siber Suç Sözleşmesi, sözleşmenin amacını, göz önünde bulundurulan çalışma ve ilkeleri açıklayan bir giriş bölümü ile beraber 4 bölüm ve 48 maddeden oluşmaktadır. "Ulusal Düzeyde Alınacak Önlemler" başlıklı II. Bölüm; maddi ceza hukuku, usul hukuku ve yargı yetkisine ilişkin düzenlemeleri içermektedir. Sözleşmede bilişim suçları "Maddi Ceza Hukuku"

67 Beceni, a.g.e, s.22.

68 Mehmet Özcan, "Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu", 19.04.2002, www.dikey8.com, (25 Aralık 2007)

başlığı altında 1. Kısımda düzenlenmiştir. Bu düzenlemeye göre bilişim suçları aşağıdaki şekilde tasnif edilmiştir.[69]

**1.** Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar;

— Hukuku aykırı erişim.

— Hukuka aykırı müdahale

— Verilere Müdahale (Verilere karşı nas-ı ızrar)

— Bilişim Sistemine Müdahale.

— Cihazların Kötüye Kullanımı

**2.** Bilgisayarlarla İlgili Suçlar;

— Bilgisayarla İlgili Sahtecilik Eylemleri.

— Bilgisayarla İlgili Dolandırıcılık Eylemleri.

**3.** İçerikle İlgili Suçlar.

— Çocuk Pornografisi ile İlgili Suçlar.

**4.** Telif Hakları ve Benzer Hakların İhlali ile İlgili Suçlar.

Sürekli olarak kendini yenileyen, yeni suç tipleri ve işlenme şekillerinin ortaya çıktığı bilişim suçları alanında, hukuka aykırı eylemlerin önlenmesine ilişkin çabalar artarak devam etmektedir.

69 Draft Convention on Cyber Crime and Explanatory Memorandum Related There To, wwwconventions.coe.int/treaty/EN/projects/cybercrime27.doc, (25 Ekim.2002)

# 5. TÜRK BANKACILIK SİSTEMİNDE ELEKTRONİK BANKACILIK RİSK YÖNETİM PRENSİPLERİ, TARAFLARIN SORUMLULUKLARININ DEĞERLENDİRİLMESİ VE YENİ ÖNERİLER

## 5.1. ELEKTRONİK BANKACILIKTA RİSKLER

Finansal kurumlar olan bankalar değer yöneten yapıları nedeniyle farklı riskleri taşımak durumundadırlar. Elektronik bankacılık ve özellikle internet uygulamalarının bankalar tarafından sunulmasından sonra kredi riski, faiz riski gibi risklere yeni riskler eklenmiştir. Bu risklerin çok farklı nedenleri olabilir. Değişim ve gelişimin bankalar arasında rekabeti de arttırmış birçok hizmet ve ürün birkaç ay gibi kısa sürede, yeterli testler yapılmadan üretimden uygulama ortamlarına aktarılmaktadır. Bu bankaların operasyonel risklerini arttıran bir durumdur.

Bankalar verecekleri hizmetlerin hazırlanması ve sunumunda birçok farklı şirketler ile çalışmaktadır. Bu teknolojiyi sağlayan şirketlerin geneli 1995 yılından sonra kurulmuştur için kurumsal bir yapıya sahip değildirler. Servis ve ürün sağlayan dış şirketlerin faaliyetlerini durdurması veya bu şirketlerden kaynaklanacak bir güvenlik ihlali bankayı önemli sorumluluk altında bırakabilmektedir.

İnternetin açık bir sistem olması dağıtım kanalı olarak bankalara önemli yararlar sağladığı gibi internetin bu yapısı sebebiyle, bankalar internet üzerinden ataklara maruz kalmaktadır. Bu yeni risklerin yönetilmesi için bankaların kendi operasyonel yapılarına ve kültürlerine uygun risk yöntemleri geliştirmeleri gerekmektedir. Finansal ürünlerin fazlalaşması, sermaye yeterlilik şartlarının yasa koyucular tarafından arttırılması ve risk teloransını fazla arttırmadan müşteriye hızlı servis sunma sebepleriylede risk yinetimi bankaların üzerine düşmeleri gereken bir nokta olmuştur. Basel komitesi Elektronik Bankacılık Grubunun (EBG) yaptığı çalışmada bankaların 3' lü bir yapı kurarak etkin bir

risk yönetimi oluşturabilecekleri belirtilmiştir. Bu yapıların parçaları aşağıdaki gibi ifade edilebilir.

— Yönetim Gözetimi
— Güvenlik Kontrolleri
— Yasal ve İtibari Risk Yönetimi

Bankalardaki elektronik bankacılık ürünlerinden oluşabilecek risklerin bu üç başlık altındaki farklı sorumluluklar dâhilinde yönetilebileceği düşünülmektedir. Yönetimden bankacılık ürünlerinin yönetim ve gözetimi, kapsamlı güvenlik ve kontrol mekanizmalarının kurulumundan, dış kaynak kullanımındaki ilişkilerin yönetiminde etkili olması beklenmektedir.

Elektronik kanallardan yapılan ve bankacılık ürün ve hizmetlerinin sağlanması yoluyla kullanılan bankacılıkta fiziki para yerine yaratılmış bir değer kullanılmaktadır. Bu elektronik değer karşılıklı iki cihaz arasındaki bilgi akışı sonucu para yerine değişimi yapılan varlıktır.

Bankaların elektronik dağıtım kanalları iki farklı yapıya sahiptir. Birinci yapı açık sistemlerdedir. Bu sistemlerde erişim için herhangi bir kısıt yoktur. Bankanın her müşterisi dağıtım kanalından yararlanabilir. Bir diğer yapı ise kapalı dağıtım yapısıdır. Müşteri belli üyelik koşullarını yerine getirerek kapalı dağıtım kanalının sunduğu servislerden yararlanabilir. İki dağıtım kanalında da farklı oranlarda riskler mevcuttur.[70] En önemli risk katogarileri; Operasyonel Risk, Ticari İtibar Riski[71] ve Yasal Risktir.

### 5.1.1 Operasyonel Risk

Operasyonel riskler sistemsel entegrasyonun uyumlu bir şekilde kurulamadığı ve sistemin mimarisinin güvenli bir şekilde oluşturulamadığı durumlarda ortaya çıkmaktadır.

70 Basel Bankacılık Denetim ve Gözetim Komitesi, "Elektronik Bankacılık ve Elektronik Para Faaliyetleri için Risk Yönetimi, TBB Yayınları, Mart 1998, s.6.
71 David Carse, "Regulatory framework of e-banking", 8 Ekim 1999, s.71.

Bankaların müşteri ile değişimini yaptığı bilgilerin güvenliği ve bu bilgilere erişimin kontrolünün sağlanamaması bankayı operasyonel riskler altında bırakır. İnternetin geniş bir erişime izin veren halka açık ağlar üzerinde kurulu olması nedeniyle kontrolü zordur. Bu nedenle yeterli kontrol mekanizmaları geliştirilerek dışarıdan ve içeriden maruz kalınacak taarruzlar nedeniyle operasyonel riskler engellenmelidir. Sahte elektronik para yaratımı bu tür güvenlik ihlallerinden biridir. Banka personellerinden biri müşteri bilgilerini kullanarak karşılığı olmayan elektronik para yaratabilir. Bu banka ve müşteriyi zora sokacak bir durumdur. Eğer banka müşteri bilgilerine erişecek personelinin banka kaynaklarına ulaşımını belli güvenlik seviyelerinde kontrol etmez ise bu operasyonel riskin sorumluluğu bankanın kendisinde olacaktır.

Operasyonel işlemlerde karşılaşılan bir diğer durum bankanın sistem tasarım, uygulama ya da bakımı sırasında çıkabilecek olumsuzluklar neticesinde karşı karşıya kalınabilecek operasyonel risklerdir.

Bankalar sistemlerinin kurulum ve yönetimi aşamalarının birçok basamağında bazı hizmetleri harici hizmet sağlayıcılarından almayı tercih etmektedirler. İhtisaslaşmanın verdiği verimlilikle başarılı sonuçlar alınsada harici hizmet sağlayıcılarından bu hizmetlerin alınması bazı risklere sebep olmaktadır. Bu sebepler aşağıdaki gibidir;

— Gerekli uzmanlığın yetersizliği
— Teknolojik adaptasyon hızlarının yavaşlığı
— Hizmet sağlayıcılarının mali yapılarından kaynaklanan iş görmezlik
— Hizmet sağlayıcılarının kendi sistemlerinin çökmesi

Yukarıda belirtilen sebepler nedeniyle oluşabilecek hatalar hizmet sunumunu yavaşlatabilir, durdurabilir veya dış ataklara banka bilgilerini korumasız bırakabilir. Başka bir operasyonel risk kaynağı da müşterilerin suistimalleridir. Müşteriler elektronik bankacılık yoluyla yaptıkları işlemleri inkâr edebilirler. Bu durumda müşterilerin

kimliklerinin ve yapılan işlemin kontrolünün uygun bir şekilde yapılmaması bankayı zarara sokabilir.

Müşteri kimliği ve işlemin yapılması için verdiği yetki ispat edilemez ise yasal risklerle beraber operasyonel riskte oluşmakta ve bankaya maliyet yükü getirilebilmektedir.

### 5.1.2 Ticari İtibar Riski

Banka hakkında kötü kamuoyu yaratılmasında etkili olabilen bu risk türü bankanın müşterilerinde birebir yaşadığı sorunlar neticesinde banka ürün işletmelerinde bir 3.şahısın müdahalesi sonucu yaşanabilir.

Bankanın ürün ve hizmetlerinden yararlanmak isteyen müşteriler yaşadıkları sorunlarla ilgili olarak bankadan gerekli ilgiyi göremiyorsa bu bankanın müşteri gözündeki itibarını zedeleyecektir. Müşteri sadakati üzerine türlü stratejiler düzenlendiği bir rekabet ortamında bu durum bankayı önemli ölçüde sarsabilir.

Yeterli güvenlik önlemleri alınmadığı için bankanın web sitesinin çökertilmesi veya müşteri bilgilerinin çalınması gibi durumlarda ise bankanın itibarının zedelenmesinin yanında tüm sektöründe güven kaybına uğramasına neden olabilir.[72]

### 5.1.3 Yasal Risk

Kanuni kural ve yükümlülüklerin ve öngörülen uygulamaların ihlali durumunda veya internetteki gelişim hızında gelişemeyen yasal düzenlemelerdeki belirsiz kalan konularda yaşanacak sorunlarda karşılaşılan risk çeşididir. Banka hizmet kanallarından yapılan işlemlerde yeterli güvenlik ve denetim kontrolleri yapılamadığı durumlarda kara

72 Basel Bankacılık Denetim ve Gözetim Komitesi, "Elektronik Bankacılık ve Elektronik Para Faaliyetleri için Risk Yönetimi, Ankara: TBB Yayınları, Mart 1998, s.8

para aklamakta dâhil kanunsuz uygulamalarda banka aracı olarak kullanılabilir ve bu tür nedenlerle bankalar yargıya intikal eden olaylarda taraf olabilir.

Müşteri bilgilerinin korunması ve gerektiği şekilde saklanması da bir değer önemli yasal risk kaynağıdır. Banka müşterisinin kişisel bilgilerinin izni olmaksızın kullanılması veya dağıtılması bankaların müşterileriyle olan ilişkilerinin bozulmasıyla karşılaşacağı itibar riskinin yanında yasal olarak ta bankaya zarar verebilecek bir sürecin başlamasına neden olabilir.

### 5.1.4 İnternet Bankacılığında Ana Risk Unsurları[73]

— Sisteme yetkisiz giriş (Hacker)
— Sisteme virüslerin gönderilmesi
— Verilerin kaybı, zarar görmesi veya değiştirilmesi
— Sistemin zarar görmesi
— Yetersiz müşteri güvenlik uygulamaları
— Personelin sisteme kötü niyetli erişim imkânın artması
— Müşterinin yaptığı işleme itirazı
— Yasal düzenlemelerin yetersiz kalması
— Müşterilerin yeterince bilgilendirilmemesi
— Uluslar arası ilişkiler de oluşabilecek mutabakatsızlıklar
— Müşterinin risk değerlendirmelerinde yetersizlikler
— Personelin yeterli bilgiye sahip olamaması

73 Sabih Arkan, "Bankacılıkta Kullanılan Yeni Elektronik Sistemlerle İlgili Hukuki Sorunlar, Ankara: TBB Yayınları, 1991, s.1.

## 5.2 İNTERNET ATAKLARINDAN KORUNMA

İnternet üzerinden yapılan saldırılara karşı en önemli unsur insandır. Güvenlik için en yeni teknoloji kullanılsa bile sistemi yöneten ve çalıştıran personel güvenliğin öneminin bilincinde değilse tehlike her zaman için vardır. Güvenliğin bilincine varmış bir ekip tarafından kullanılabilecek teknolojiler aşağıda yer almaktadır;

— Firewall( Ateş Duvarı)
— İletişim Güvenliği ve Kriptolama
— Güvenlik Yapısı
— SSL Güvenliği
— Erken Uyarı Sistemleri
— Unix ve Windows İşletim Sistemleri
— Güvenilir İşletim sistemleri
— Zararların Asgari Düzeye İndirilmesi
— Genel Önlemler

### 5.2.1 Firewall ( Ateş Duvarı)

Firewall (Ateş Duvarı) İki veya daha fazla bilgisayar ağı arasındaki ağ trafiğini yöneterek bir güvenlik politikası sağlayan donanım ve yazılım içeren çözümdür. Ağların bazıları kullanıcının kontrolü dışında olabilir. Bir firewall genel olarak bilgisayar sistemlerine, ağa ve kullanıcının gizli bilgilerine yapılabilecek saldırılara karşı ilk kalkanı oluşturur. Firewall tüm organizasyonu koruyacak şekilde kolayca kurulabilir.[74]

Firewaller genelde izin veren ve izin vermeyen olarak iki şekilde ayarlanabilir. İzin veren şemada sistemdeki bütün servisler ve bilgiler firewall tarafından internete

74 http://www.checkpoint.com/product/protect/images/firewall-1_index_lg.gif, 25.05.2002

kapatılır ve sadece kullanıcı tarafından birkaç tanesine izin verilir. İzin vermeyen şemada ise bütün servis ve bilgiler açıktır. Firewallın sadece bir kaçına izin vermediği durumdur.

Firewaller güvenlik aracı olarak bir güvenlik politikası belirlenmesine yardımcı olurlar. Ancak firewall üzerinden geçmeyen ağlar firewall tarafından korunmamaktadır.

### 5.2.2 İletişim Güvenliği ve Kriptolama(Kodlama)

İletişim güvenliği ile ilgili olarak; veri gizliliği, veri bütünlüğü, bağlanılırlık ve reddedilme sağlanması gerekmektedir.

Elektronik ortamda bilginin yetki dışı kullanımını önlemek için kullanılan araçlardan birisi kriptolama(kodlama) sistemleridir. Eletronik bilgiyi bir formdan farklı bir formata aktarırlar.

Kriptolama(kodlama) terim olarak iletilen verinin değiştirilmesidir. Değiştirilen veri ulaştığı noktada tekrar eski haline gelir. Bu şekilde aradaki verinin güvenilir şekilde iletilmesi sağlanır.[75] Bu işlem veri gizliliği, bütünlüğü ve etkin iletişim gibi faydalar sağlar.

İnternete olan ilginin artmasıyla birlikte kurumlar için kurumsal ağ güvenliği önemi artan bir konu haline gelmiştir. Kurumsal ağların güvenliğini tehdit eden yazılımların ve bilginin internette bol miktarda serbestçe dolaşması bu konunun önemini daha fazla arttırmıştır.

Kurumsal bir ağ internete bağlandığı zaman aslında ağ fiziksel olarak hakkında hiç bir bilgi olmayan bilgisayar ağına ve onların kullanıcılarına bağlanır. Bir internet bağlantısı kurumlara bilgi paylaşımı ve internet üzerindeki uygulamaların kullanımı yönünde birçok

75 http://www.signalguard.net/sifreleme/key.htm, 24.05.2002

fırsat tanımaktadır ancak bu yapılırken kurumun kendi ağı içerisindeki bilgiye, yetkisiz kişilerin ulaşması engellenmelidir.

Kripto(kodlama) sistemlerinin değiştirme işlemi bir kriptolama anahtarı tarafından kontrol edilir. Bu anahtar bir karakter dizisidir ve kriptolama sisteminin güvenirliliği bu anahtarın korunmasına bağlıdır.

Kriptolama(kodlama) sisteminin sağladığı servisler 4 ana başlıkta toplanabilir;

— Güvenlik: Bilginin yetkisiz kişilerden saklanmasını sağlar
— Yetki denetimi
— Bilgi bütünlüğü: Bilginin yetkisiz kişilerce değiştirilmemesi
—Bilgi kaynağı denetimi: Mesajların doğru kaynaktan gelip gelmediğinin denetlenmesi

Genel olarak kriptolama(kodlama) sistemleri öncelikle güvenlik sağlar. Bunun için kullanılan yöntem şifrelemedir. Şifreleme işlemi okunabilir haldeki elektronik bilginin okunamayan şifreli hale getirilmesidir. Bu değişim işlemi bir kripto(kodlama) anahtarı (k) tarafından kontrol edilir. Bu değişimin geri alınması ise bu kripto anahtarı ile ilişkili (l) anahtarı tarafından kontrol edilir.

### 5.2.3 Güvenlik Yapısı

İnternet üzerinden gerçekleşen finansal işlemlerin uygulanmasında güvenliğin temeli, pek çok bilgisayar uygulamasında olduğu gibi şifre güvenliğine dayanmaktadır. Kullanıcıların şifreleri uygulamaları sıkı bir şekilde korunmalıdır. Şifreler sistemde kimsenin çözemeyeceği tek yönlü fonksiyonlarla kriptolanmalıdır.

### 5.2.4 SSL Güvenliği

SSL (Secure Sockets Layer) protokolü bilginin bütünlüğü ve gizliliği için, internet üzerinde iki taraf arasında oluşan tarfiğin şifrelenerek, gizliliğin ve bütünlüğün korunmasını sağlayan kriptolamadır(kodlama)[76] SSL protokolü bütün yaygın web sunucuları tarafından desteklenen bir protokoldür. SSL gönderilen bilginin kesinlikle ve sadece doğru adreste deşifre edilebilmesini sağlamaktadır. Bilgi gönderilmeden önce otomatik olarak şifrelenir ve sadece doğru alıcı tarafından deşifre edilebilir. Her iki taraftada doğrulama yapılarak işlemin ve bilginin gizliliği korunur.

### 5.2.5 Erken Uyarı Sistemleri

Bir web sitesine karşı yürütülen yetkisiz erişim ve saldırıların zarar verici boyutlara ulaşmadan saptanmasını sağlayan çeşitli güvenlik teknolojilerinin kullanılmasıdır.

— Ağ tabanlı yetkisiz erişim ve saldırı saptama sistemlerinin kurulması,
— Sistem tabanlı yetkisiz erişim ve saldırı saptama sistemlerinin kurulması,
— Sistem bütünlüğü saptama sistemlerinin kurulumu,
— Tuzak ve yanıltıcı sistemlerin siteye eklenmesi,
— Bilgi güvenliği acil durum planı hazırlanması,
— Bilgi güvenliği acil durum ekibi oluşturulması işlemlerini kapsar.

Erken uyarı sistemleri atakları taramak veya atak hazırlıklarını belirlemekle, network trafiğini, uygulamaları ve işletim sistemlerini izleyerek güvenlik yöneticisini uyarırlar, otomatik olarak cevap verirler ve dış bağlantı yolunu keserler.

76 http://www.deltamenkul.com.tr/ssl.htm, 18.04.2008

Bu sistemler güvenlik yöneticisine atağın niteliği, etkilenen sistemleri ve güvenlik açıklarını kapama imkânı verir. Ayrıca bu bilgiler yasal başvurularda kanıt sağlamak açısından da önemlidir.[77]

### 5.2.6 Unix ve Windows İşletim Sistemi

İki sitemde kullanıcı, dosya ve dizinler bulunmaktadır.[78] Windows NT güvenlik modeli; yalnızca kimliği doğrulanmış kullanıcıların sistem kaynaklarına erişmesine izin verir. Güvenlik modeli nesnelere erişenleri, kişinin bir nesneyi kullanabildiği eylemleri ve denetlenen olayları yönetmek için bileşenler içerir.[79] Güvenlik sisteminin temel fonksiyonlarından birisi kullanıcı doğrulamadır. Bir çok sistemin kullanıcı temelleri kullanıcı adı ve password(giriş şifresi) üzerine kuruludur. Sistem bunları password database(giriş şifresi veri tabanı)' inde saklar. Unix sistemlerinde genellikle sistem kullanıcılarının başka kullanıcılarının password(giriş şifresi)' lerini görmeleri ve işlem yapmalarını engellemek için databasede(veri tabanı) gerçek şifreler saklanmaz. Şifrelerin kriptolanmış(kodlama) hali saklanır.[80]

### 5.2.7 Güvenilir İşletim Sistemleri

Bilgisayar teknolojisi ve internet kullanımının iş, devlet ve özel hayata yönelik kullanımının artması ile birlikte güvenliği arttırmaya yönelik olarak yeni güvenlik önlemleri alınmaktadır. Bu önlemlerden biride güvenilir işletim sistemleridir. Bu teknoloji hackerları bilgisayar sisteminin erişim ve kontrol ünitelerinden uzak tutmakta ve sistem yöneticisinin yanlışlıkla zarar verici değişikliler yapmasından korumaktadır.[81]

---

77 Stephen Kent, "On The Trail of İntrusions İnto İnformation Systems", 2000, s.52
78 John Viega and Jeffrey Voas, "IT Professional Technology Solutions for The Enterprise", 2000, s.40
79 http://www.microsoft.com/turkiye/windows2000pro/ozellikler.asp, 15.05.2002
80 John Viega and Jeffrey Voas, a.g.e, s.41.
81 Sandra Key Miller, "Computer İnnovative Technology for Computer Professionals, 2001, s.16

### 5.2.8 Zararların Asgari Düzeye İndirilmesi

Bir web sitesi başarılı bir yetkisiz erişim veya kırma çalışması ile karşı karşıya kaldığında, gerçekleşen saldırının boyutlarını saptama ve bu saldırının geride bıraktığı izleri toplamak büyük önem taşır. Bu izler hem saldırıdan olası en düşük zararla kurtulmamızı hem de saldırgana yasal yaptırımların uygulanabilmesi için gerekli bilgiyi sağlar. Gerekli alt yapı kurabilmek için gerekli araçlar;

— Ağ dinleyici yazılımlar; Ağ üzerinde belirli bir trafik deseni yakalandığında kayıta başlayan ve ağ trafiğini kaydeden araçlardır.
— Paket inceleme yazılımları; Kayıt edilen trafik bilgisinin içinde gerçekleşen trafiği yorumlamaya ve içeriğini tespit etmeye yarayan araçlardır.
— Delil toplama yazılımları; Kayıt edilen trafik içerisinde delil olarak kullanılabilecek paketleri ayıklamayı ve sunmayı amaçlayan yazılımlardır.

### 5.2.9 İnternet Bankacılığında Alınabilecek Genel Önlemler

— Ağ saldırılarına karşı güvenlik duvarları
— İşletim sisteminin gerekli güvenlik ayarlarının ve iyileştirmelerinin yapılması
— Tüm sistemin denetiminin yapılması
— Tespit edilen sistemdeki zayıflıkların düzeltilerek teste tabi tutulması
— Düzenli ve geniş kapsamlı teftişler yapmak
— Sistemin iç kontrol mekanizmalarının arttırılması
— Sistemin fiziksel güvenliğinin sağlanması
— Sisteme uygun Firewall' lar (Bazı verilere ulaşmayı engelleyen yazılımlar) koymak
— Gelişmiş şifreleme teknikleri kullanmak
— Gelişmiş kimlik kontrolü teknikleri kullanmak
— Son kullanıcıların doğru yetkilendirilmesini sağlamak
— İç sistemdeki güvenlik önlemlerinin sürekli izlenmesi

— Virüs taramasının düzenli ve güncel bir şekilde yapılması

— Sistem bilgilerinin sadece ilgili personelce bilinmesi ve gereken personel yedeğinin yapılması

— Dış denetimlerle sistemi sürekli geliştirmek

— Yapılan kritik işlemlerin loglanmasını sağlamak

— Yapılan işlemlerin niteliğine uygun limitler koymak

— Hizmet alınan firmalarla yapılan anlaşmaların özenli takibi

— Mevcut donanım ve yazılım kapasitelerinin düzenli olarak gözden geçirilmesi

— Sistemin devamı ve güncellenmesi için sorumluluk dağıtan bir mekanizma kurulması

—Sorumluluk dağıtan mekanizmanın sonraki işlemleri kontrol edecek şekilde yapılandırılması

— İşlemlerde bilgilerin korunmasının ne kadar önemli olduğunun müşterilere anlatılması

— İşlemlerin kontrol kopyasının oluşturulması

— Sözleşmelerin kanunlara ve uluslararası ilişkilere uygun olarak düzenlenmesini sağlamak

— Yasal belirsizliklere karşı alınacak risk toleransına karar vermek

— Kamuya yönelik ürün bilgisi geliştirmek ve yayınlamak

— Personelin yukarıdaki unsurlara uygun eğitimini sağlamak

— Kurumun internet ekibinin güvenlik teknolojilerini takip edebilmesi

—Web sitesi uygulamalarının incelenerek güvenlik risklerinin belirlenmesi ve değerlendirilmesinin yapılması

— Kurum içerisindeki sistemler için gerekli olacak ağ kurallarını ve kullanıcıların güvenlik açısından uymaları gereken kuralları belirleyen bir güvenlik politikası oluşturulması

— İnternet sunucu ve güvenlik uygulama sistemlerinin güvenlik açıklarının incelenerek, olası güvenlik açıkları için raporlar hazırlanması

— Güvenlik açıklarının engellenebilir olanlarının engellenebilmesi veya bu açıklardan oluşabilecek olası saldırılar için gereken önlemlerin alınması

— Sistem yöneticilerine kurulan güvenlik alt yapısının eğitiminin verilmesi

— Olası bir saldırı anında yapılacak işleri, alınacak önlemlerin belirlenmesi ve acil durum planı hazırlanması
— Acil durum planını uygulamaya sokmak için gerekli bilgi düzeyine sahip bir acil durum ekibi oluşturulması
— Kurum içi ve dışı ağlarda yetkisiz erişim ve saldırı testleri yapılması
— Personelin internet kullanımına ilişkin prosedür belirlenmesi ve taahhütname alınması
— İnternet kullanım yetkilerinin personelin görev tanımlarına uygun olarak yapılması
— Gelen ve giden elektronik posta mesajlarının içeriği, eklenen program ve dökümanların niteliği kontrol edilmelidir.

## 5.3. RİSK YÖNETİMİ

Elektronik bankacılık ve elektronik paranın daha fazla kullanımı bankacılık ve ödeme sisteminin verimin artırabilir, müşterilere ve tüccarlara fayda sağlayabilir. Elektronik bankacılık ve elektronik para faaliyetlerine girişen bankalar için riskler vardır. Riskler faydalarla dengelenmelidir; bankalar riskleri yönetebilmeli, kontrol edebilmeli ve gerekirse ilgili kayıpları karşılayabilmelidir. Elektronik bankacılık ve elektronik para faaliyetlerinden kaynaklanan riskler ayrıca bankaların karşılaştığı diğer riskler kapsamında değerlendirilmelidir.

Teknolojik yeniliğin, yüksek hızın, elektronik para ve elektronik bankacılıkta bankaların karşılaştığı risklerin mahiyeti ve kapsamını değiştirmesi muhtemeldir. Gözetmenler bankaların, banka yönetiminin mevcut risklere karşılık vermesini ve yeni risklere adapte olmasını sağlayacak süreçlere sahip olmasını beklerler. Risk değerlendirme, riske maruz kalmayı kontrol etme ve riskleri izlemenin üç temel unsurunu içeren bir risk yönetim süreci bankaların ve gözetmenlerin bu hedeflere ulaşmasına yardımcı olacaktır. Bankalar, yeni elektronik bankacılık ve elektronik para faaliyetlerine başlarken ve bu faaliyetlerle mevcut uğraşlarını değerlendirirken böyle bir süreci kullanabilirler.

Bankaların, yönetim kurulu ve üst yönetim tarafından uygun görülen kapsamlı bir risk yönetimi sürecine sahip olması zorunludur. Elektronik bankacılık ve elektronik para faaliyetlerinde yeni riskler teşhis edildikçe ve değerlendirildikçe, yönetim kurulu ve üst yönetim bu değişikliklerden haberdar edilmelidir. Yeni bir faaliyetin başlatılmasından önce, kapsamlı bir inceleme yapılmalıdır ki üst yönetim, risk yönetimi sürecinin önerilen yeni faaliyetten kaynaklanan riskleri değerlendirmek, kontrol etmek ve izlemek için yeterli olmasını temin edebilsin.

### 5.3.1 Risk değerlendirme

Risk değerlendirme daimi bir süreçtir. Üç adımı vardır. Birincisi, banka riskleri teşhis etmek ve mümkün olduğunda miktarlandırmak için titiz bir analitik sürece girişebilir. Banka yönetimi, hem banka üzerine olabilecek etkisi (maksimum potansiyel etki dahil) ve hem de böyle bir olayın meydana gelme ihtimali bakımından her riskin büyüklüğüne ilişkin makul ve savunulabilir bir yargı oluşturmalıdır.

Risk değerlendirmede ikinci adım, belirli bir sorunun olması durumunda bankanın uğramaya katlanabileceği kayıpların değerlendirmesine dayalı olarak, banka yönetim kurulu veya üst yönetiminin bankanın risk toleransını belirlemesidir. Son olarak, yönetim, riske maruz kalmanın tolerans limitleri içinde olup olmadığını belirlemek üzere, kendi risk toleransını riskin büyüklük değerlendirmesi ile karşılaştırabilir.

### 5.3.2 Riskleri yönetme ve kontrol etme

Riskleri ve risk toleransını değerlendirmiş olan banka yönetimi riskleri yönetmek ve kontrol etmek için önlemler almalıdır. Risk yönetimi sürecinin bu aşaması, güvenlik politikaları ve önlemleri uygulama, iç iletişimi koordine etme, ürün ve hizmetleri değerlendirme ve yükseltme, dışa yaptırma risklerini kontrol etme ve yönetmeyi sağlayacak önlemleri uygulama, açıklama ve müşteri eğitimi sağlama ve ihtimal planları geliştirme

gibi faaliyetleri içerir. Üst yönetim, risk limitlerini uygulamadan sorumlu personelin, elektronik bankacılık veya elektronik para faaliyetini yürüten iş ünitesinden bağımsız yetkiye sahip olmasını sağlamalıdır. Bankalar, politika ve prosedürler yazılı dökümanlarda belirlenir ve tüm ilgili personele sunulursa, her hangi bir faaliyette mevcut çeşitli riskleri kontrol etme ve yönetme yeteneklerini artırırlar.

#### 5.3.2.1 Güvenlik politikaları ve önlemleri

Güvenlik, veri ve işletim süreçlerinin özgünlük ve gizliliğini korumada kullanılan sistem, uygulama ve iç kontrollerin birleşimidir. Uygun güvenlik, banka içindeki süreçler ve banka ile harici şahıslar arasında iletişim için yeterli güvenlik politikaları ve güvenlik önlemlerinin geliştirilmesi ve uygulanmasına dayanır. Güvenlik politikaları ve önlemleri, elektronik bankacılık ve elektronik para sistemleri üzerine harici ve dâhili taarruz riski ve güvenlik ihlallerinden kaynaklanan itibar riskini de sınırlayabilir.

Bir güvenlik politikası, bilgi güvenliğini desteklemede yönetimin niyetlerini ifade eder ve bankanın güvenlik organizasyonunun açıklamasını sağlar. Ayrıca bankanın güvenlik riski toleransını tanımlayan kılavuzu oluşturur. Politika, bilgi güvenlik önlemlerini tasarımlama, gerçekleştirme ve uygulama sorumluluklarını tanımlayabilir ve politikaya uymayı değerlendirme, disiplin önlemlerini uygulama ve güvenlik ihlallerini rapor etme prosedürlerini oluşturur.

Güvenlik önlemleri, güvenli sistemler ve operasyon kurmaya katkıda bulunan donanım ve yazılım araçları ve personel yönetiminin birleşimidir. Üst yönetim, güvenliği, en zayıf halkası kadar kuvvetli olan kapsamlı bir süreç olarak görmelidir. Bankalar, harici ve dahili taarruzları,  ve elektronik bankacılık ve elektronik paranın suistimalini önlemek veya hafifletmek için bir dizi güvenlik önlemini seçebilir. Bu tür önlemler, örneğin şifreleme, parola, ateş duvarları, virüs kontrolleri ve çalışanları ayırmayı içerebilir.

Ateş duvarları gelen mesajları süzse de, İnternetten indirilen virüs bulaşmış programlara karşı koruma sağlamazlar. Sonuçta, yönetim özellikle uzaktan bankacılık için virüs taarruzu ve veri imhası ihtimalini azaltmak için önleme ve deteksiyon kontrolleri geliştirmelidir. Virüs bulaşması riskini azaltan programlar, ağ kontrolleri, kullanıcı politikaları, kullanıcı eğitimi ve virüs tespit yazılımını içerebilir.

Güvenlik tehditleri kurum içinden de yapılabilir. Elektronik bankacılık ve elektronik para sistemleri, mümkün olduğunca hâlihazır ve eski çalışanlar tarafından yapılacak yetkisiz faaliyetlere karşı da korunmalıdır. Mevcut bankacılık faaliyetlerinde olduğu gibi, yeni çalışanları geçici çalışanları danışmanlar için geçmiş kontrolleri yanı sıra dâhili kontroller ve görevlerin ayrılması da sistem güvenliğini korumak için önemli önlemlerdir.

#### 5.3.2.2 İç iletişim

Üst yönetim kilit personele elektronik bankacılık ve elektronik paranın bankanın tümel hedeflerinin nasıl destekleyeceğini iletirse, operasyonel, itibar, yasal ve diğer riskler yönetilebilir ve kontrol edilebilir. Aynı zamanda, teknik personel sistemlerin nasıl çalışmak üzere tasarımlandığını ve bunun yanı sistemlerin sıra güçlü ve zayıf taraflarını açık şekilde üst yönetime anlatmalıdır. Bu prosedürler, bir bankacılık organizasyonu içinde farklı sistemlerin uyumsuzluğu ve kötü sistem tasarımından doğan operasyonel riskleri, veri problemleri, sistemlerin beklendiği gibi çalışmamasından doğan müşteri memnuniyetsizliğiyle ilişkili itibar riski, kredi ve likidite riskini azaltabilir.

Yeterli iç iletişim sağlamak için tüm politikalar ve prosedürler yazılı olarak sağlanmalıdır. Ayrıca, üst yönetim, personel ve yönetim uzmanlığı eksikliğinden kaynaklanan operasyonel riskleri sınırlama için teknolojik yeniliklerin hızına paralel olarak sürekli bir eğitim, beceri ve bilgileri yükseltmeyi şirket politikası olarak benimsemelidir.

Eğitim, teknik kurs ve personele önemli piyasa gelişmelerini izlemek için zaman vermeyi içerebilir.

#### 5.3.2.3 Değerlendirme ve Yükseltme

Ürün ve hizmetleri geniş kapsamlı kullanıma başlatmadan önce değerlendirmek operasyonel ve itibar risklerini sınırlamada yardımcı olur. Test etme, teçhizat ve sistemlerin uygun şekilde çalıştığını ve istenen sonuçları doğurduğunu doğrular. Yeni uygulamaları geliştirmede pilot programlar yararlı olmaktadır. Sistem yavaşlama ve durma riski de mevcut donanım ve yazılımın yeteneklerinin düzenli olarak incelenmesiyle önlenebilir.

#### 5.3.2.4 Dışa yaptırma

Bankaların, esas yetkinlikler üzerinde stratejik olarak odaklanarak uzmanlık alanı dışındaki faaliyetlerde uzmanlaşan diğer kuruluşlara başvurmaları yaygınlaşmıştır. Bu düzenlemeler, maliyet azaltma ve sürümden kazanma gibi yararlar sağlamaktadır fakat operasyonlarını etkileyen riskleri kontrol etme sorumluluğu devam etmektedir. Bankalar, dıştan hizmet sağlayıcılarla çalışmaktan doğan riskleri sınırlayacak politikalar benimsemelidir. Banka yönetimi kendilerine hizmet sağlayanların operasyonel ve mali performansını izlemeli, taraflar arasındaki sözleşme ilişkisinin yanı sıra her bir tarafın beklentilerinin açıkça anlaşılmasını ve yükümlülüklerinin yazılı ve uygulatılabilir sözleşmelerde tanımlanmasını sağlamalı ve gerekirse hizmet sağlayıcıları derhal değiştirebilecek şekilde bir ihtimal düzenlemesi bulundurmalıdır.

Bankanın hassas bilgilerinin güvenliği kritik önemdedir. Dışa yaptırma düzenlemesi, bankanın hassas bilgileri hizmet sağlayıcı ile paylaşmasını gerektirebilir. Banka yönetimi, hizmet sağlayıcının hassas verileri korumayı hedefleyen politika ve prosedürlerini inceleyerek, hizmet sağlayıcının bu faaliyetler kurum içinde yapılmışçasına aynı güvenlik düzeyini koruma yeteneğini değerlendirmelidir. Gözetmenler gerekirse,

hizmet sağlayıcıların yetkinlik, operasyonel ve mali performansını bağımsız olarak değerlendirme hakkına sahip olmak isteyebilirler.

#### 5.3.2.5 Açıklamalar ve Müşteri Eğitimi

Açıklamalar ve müşteri eğitimi, bir bankanın yasal ve itibar riskini azaltmaktadır. Yeni ürün ve hizmetlerin nasıl kullanılacağını, hizmetler ve ürünler için alınan ücretleri ve problem ve hata çözme prosedürlerini gösteren açıklamalar ve müşteri eğitim programları, bankanın müşteri koruma ve özel yaşam kanun ve yönetmeliklerine uymasına yardımcı olmaktadır. Bağlanılan bir web sitesine bankanın hizmetleri hakkında açıklamalar, bağlanılan sitelerdeki hizmetler ve ürünlerle ilgili problemlerden kaynaklanan yasal riski azaltabilir.

#### 5.3.2.6 İhtimal Planlama

Bir banka, elektronik bankacılık ve elektronik para hizmetlerinin durması ihtimalini düşünerek bu ihtimalle karşılaştığında izleyeceği yolu önceden planlamalıdır. Plan, veri kurtarma, alternatif veri işleme yetenekleri, acil durum personeli ve müşteri hizmet desteği hususlarını içerir. Yedekleme sistemleri periyodik olarak test edilmelidir. Bankalar, ihtimal operasyonlarının normal üretim operasyonları gibi güvenli olmasını sağlamalıdır.

Elektronik bankacılık ve elektronik paranın önemli bir özelliği, donanım sağlayıcılar, yazılım sağlayıcılar, internet hizmet sağlayıcıları ve telekomünikasyon şirketleri dâhil harici kuruluşlara dayanmasıdır. Banka yönetimi bu tür hizmet sağlayıcıların yedekleme yeteneklerine sahip olmasını isteyebilir. Yönetim, hizmet sağlayıcıların arızalanması durumunda uygulayabileceği telafi edici eylemleri düşünmelidir. Bu planlar, diğer sağlayıcılar ile kısa vadeli sözleşmeler ve hizmet kesilmesiyle ilgili müşteri kaybını

nasıl çözeceğine ilişkin politikayı içermelidir. Gerektiği durumlarda hizmet sağlayıcıları derhal değiştirme hakkını saklı tutmalıdır.

İhtimal planlama, bankanın kendi eylemleriyle birlikte elektronik bankacılık veya elektronik ürün ve hizmeti sunan başka bir kurumun problemlerinden kaynaklanan itibar riskini sınırlamada yararlı olmaktadır.

### 5.3.3 Riskleri İzleme

Sürekli izleme, her risk yönetimi sürecinin önemli bir özelliğidir. Uygulamaların hızla değişmesi ve bazı ürünlerin internet gibi açık ağların kullanımına dayalı olması sebebiyle elektronik bankacılık ve elektronik para faaliyetleri için izleme önemlidir. İzlemenin iki önemli unsuru sistem test etme ve denetlemedir.

#### 5.3.3.1 Sistem Test Etme ve Tarama

Sistem operasyonunu test etme olağan dışı faaliyetleri tespit etmeye, önemli sistem problemleri, kesilmeleri ve sisteme yapılan saldırıları önlemeye yardımcı olmaktadır. Girme testi, normal prosedürler dışında sisteme girmek, güvenlik mekanizmasının tasarım ve uygulamasındaki hataların teşhis, izolasyon ve teyidi üzerine odaklanır. Tarama faaliyeti, izleme için yazılım ve denetlemenin kullanıldığı bir izleme şeklidir. Rutin operasyonları izlemek, anormallikleri araştırmak ve güvenlik politikalarına uymayı test etmek amacıyla güvenlik etkinliği bakımından sürekli kararlar verme üzerine odaklanır.

#### 5.3.3.2 Denetleme

Denetleme (dâhili ve harici) elektronik bankacılık ve elektronik para hizmetlerinin sağlanmasında eksiklikleri tespit etme ve riskleri asgariye indirgeme için önemli bir bağımsız kontrol mekanizması sağlamaktadır. Denetçinin rolü, uygun standart, politika ve

prosedürlerin geliştirildiğini ve bankanın sürekli olarak bunlara uyduğunu doğrulamaktır. Denetleme personeli, doğru bir inceleme yapmak için yeterince uzmanlığa sahip olmalıdır. Dâhili bir denetçi, risk yönetim kararları veren çalışanlardan ayrı ve bağımsız olmalıdır. Yönetim harici denetçileri, elektronik bankacılık veya elektronik para faaliyetinin bağımsız bir değerlendirmesini sağlamak için tercih edebilir.

### 5.3.4 Sınır Ötesi Risklerin Yönetimi

Sınır ötesi riskler, bankaların ülke içinde karşılaştığı risklerden daha karmaşık olabilir. Dolayısıyla bankalar ve gözetmenler, sınır ötesi elektronik bankacılık ve elektronik para faaliyetlerinden kaynaklanan operasyonel, itibar, yasal ve diğer riskleri değerlendirme, kontrol ve izleme için daha fazla dikkat göstermeye ihtiyaç duyabilirler.

Farklı ulusal pazarlardaki müşterilere hizmetler sunmayı seçen bankalar, farklı ulusal yasal gerekleri anlamalı ve müşteri beklentileri, ürün ve hizmet bilgilerinde ulusal farklılıkları kavrayabilmelidirler. Üst yönetim, kredi verme ve likidite yönetimi için mevcut sistemlerin sınır ötesi faaliyetlerden kaynaklanan muhtemel zorlukları dikkate almasını sağlamalıdır. Bir banka, ülke riskini değerlendirmeye ve yabancı ülkedeki ekonomik ve politik iklim problemleri nedeniyle hesap hizmeti kesintisini dikkate alan ihtimal planları geliştirmeye ihtiyaç duyabilir. Bir banka ayrıca, yabancı bir hizmet sağlayıcısının yükümlülüklerini yerine getirmesini sağlamada zorluklarla karşılaşabilir. Dış ülkede konuşlu hizmet sağlayıcılarına dayanan bankaların durumunda, ulusal gözetmenler sınır ötesi hizmet sağlayıcılardan bilgilere erişimi ve bunları faaliyetlerini her durum için ayrıca değerlendirme isteyebilirler.

Ulusal gözetmenler, yargı belirsizliklerini teşhis etme ve tartışmada önemli bir rol oynayabilirler. Ayrıca güvensiz ve yasadışı uygulamaları tespit edecek önlemler geliştirmeye devam edebilirler. Gözetmenler ürün ve hizmet yenilikleri ve endüstri

uygulamaları hakkında bilgiyi paylaşmak için işbirliği çabalarına devam edebilir, güçlendirebilir.[82]

## 5.4. TÜRK BANKACILIK SİSTEMİNDE ELEKTRONİK BANKACILIK RİSK YÖNETİM PRENSİPLERİNİN UYGULAMASINA İLİŞKİN TEBLİĞİ VE TEBLİĞ HÜKÜMLERİNİ GELİŞTİRMEYE YÖNELİK ÖNERİLER

Bankacılık faaliyetlerinde bilgi teknolojilerini kullanmasından kaynaklanan riskler oluşmaktadır. Bu risklerden biri müşterilere sunulan elektronik bankacılık hizmetidir. Bankalar bilgi sistemlerini kullanmaları sebebiyle oluşan riskleri ölçmek, izlemek, kontrol etmek ve önlemek üzere gerekli önlemleri almaktadır.

Bankacılık Düzenleme ve Denetleme Kurulu tarafından "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" hazırlanmış ve 14 Eylül 2007 tarihinde resmi gazetede yayımlanmıştır. Tebliğ' de bankalar tarafından bilgi sistemlerinin yönetiminde uygulanacak ilkelerin standart hale getirilmesi amaçlanmıştır. Tebliğ 01.01.2008 tarihinde yürürlülüğe girmiştir. Elektronik bankacılıkla ilgili risk yönetim prensipleri; "Kimlik Doğrulama", "Güvenlik Kontrol Sürecinin Tesis edilmesi ve Yönetilmesi", "İnkâr Edilemezlik ve Sorumluluk Atama", "Denetim İzlerinin Oluşturulması", "Müşterilerin Bilgilendirilmesi", "Servis Sürekliliği ve Kurtarma Planı", "Elektronik İmza" dır.[83] Bankalar, bu Tebliğ hükümleri ile ilgili mevcut faaliyet ve sistemlerini, yürürlük tarihinden itibaren azami iki yıl içerisinde Tebliğ hükümlerine uygun hale getirecektir.

Tebliğ maddeleri incelenmiş ve uygulama hakkındaki geliştirilmesi gereken konulara değinilmiştir.

82 Basel, a.g.e, s.12-15.

### 5.4.1 Kimlik Doğrulama

Elektronik ortamda gerçekleşen işlemler için uygun bir kimlik doğrulama mekanizması kurulmalıdır. Risk değerlendirmesi bankacılık işleminin niteliğine göre yapılmalıdır. Finansal işlemlerde, işlemin başlangıcından son aşamasına kadar kimlik doğrulamada maksimum güvenlik uygulanmalıdır.

— Cep tel kullanmayan müşteriler için şifre üreten cihazlarla kimlik doğrulama veya sabit numaradan aranarak kimlik doğrulama işlemi gerçekleştirilebilir.

— Günlük işlem limit belirlemesi müşteri inisiyatifinde olmalıdır. Müşterinin kendi hesapları dışındaki EFT ve havale işlemlerinde kimlik doğrulama işlemlerinde ek güvenlik uygulanabilir. Müşterinin ilk defa yaptığı veya şüpheli görünen güncel 1000 YTL ve üzeri işlemlerde müşteri aranarak kimlik teyit işlemi yapılmalıdır.

— Müşterinin belirleyeceği limit üzerindeki işlemlerde şifre mesajından sonra işlemi teyit eden 2. bir onay mesajı gönderilmelidir.

### 5.4.2 Güvenlik Kontrol Sürecinin Tesis Edilmesi ve Yönetilmesi

Güvenlik kontrollerinin yeterliliği yılda en bir kez test edilmelidir ve sızma testleri yapılmalıdır.

İnternet bankacılığında gerçekleşen şüpheli işlemlerin tespiti için takip mekanizması kurulmalıdır.

Müşterinin internet bankacılığına giriş aşamasındaki kimlik kontrollerinin en üst güvenlik seviyede yapılabilmesi için bankalar tarafından uygun yapının kurulması gereklidir. İnternete giriş aşamasında kullanılacak parola karmaşık ve tahmin edilmesi zor nitelikte olmalı ve sistem bunun için müşteriyi zorlamalıdır. Parolanın değişmesi en üst güvenlik seviyelerinde yapılmalıdır.

— Tebliğde bir yılda denmesine rağmen uygulamada bu sürenin çok uzun olduğu görülecektir. Uygulamaların hızla değişmesi ve virüslerin sürekli olarak yenilenmesi sebebiyle bu sürenin maksimum 3 ay olarak sınırlandırılması önerilmektedir.

— Bankaların güvenlik birimlerinde etkin bir izleme programı kullanılmalıdır. Müşterilerin alışkanlıkları dışında, şüpheli saatlerde ve ilk defa yapılacak işlemleri sistem tespit etmeli bu işlemleri onay aşamasında bekletmelidir. Gerekli güvenlik incelemeleri yapıldıktan sonra onay verilmelidir.

— Ülkemizde yabancı bankaların ortaklık ve satın alma yoluyla finansal sisteme girmesi ile bilgisayar yazılım ve denetim mekanizmalarının operasyonel maliyeti düşmekte ve uluslar arası piyasalarda kullanılan takip mekanizmasını güncel olarak bankalarda kullanılması sağlanmaktadır. %100 Türk sermayeli kalan bankaların bu sistemlere yatırım yapması gerekmektedir

### 5.4.3 İnkâr Edilemezlik ve Sorumluluk Atama

Banka tarafından sunulan internet bankacılığı servisi, müşterilerin yanlış işlem yapma ihtimalini azaltacak gerekli kontrolleri içerecek şekilde düzenlenmeli ve başlattıkları işlemlere ilişkin riskleri tamamen anlamalarını sağlamalıdır.

— Müşterilerin daha önceki olan sahtecilik işlemleri ile ilgili periyodik bilgiler verilmesi ve bu konularda uyarılması gereklidir. Müşterilerin bilgilerinin ne şekilde çalınacağı müşterilere açık ve anlaşılır şekilde anlatılmalıdır. Bu uyarıları internet işlemlerine giriş yapacağı sıralarda periyodik olarak verilmesi önerilmektedir.

— Bankalar tarafından internet şube kullanan müşterilerine belli periyodlarda otomatik olarak virüs tarayıcı programlar gönderilmelidir.

— Müşteriler internet şube başvuru aşamasında bilgilendirmeli ve daha sonrada güvenlik önlemlerini hatırlatıcı uygulamalarda bulunmalıdır. İnternet şube başvuru formlarında güvenlikle ilgili özet bilgiler yer almalıdır. Ayrıca bankanın internet sayfasında bu bilgiler müşteri finansal işleme başlamadan önce dikkat çekici yerlerde bulunmalıdır. Belli aralıklarla müşterilere sms, posta ve e-mail(e-posta) yoluyla güvenlik önlemleri hatırlatılmalıdır.

Bu uyarılar genel olarak aşağıdaki bilgileri içermelidir;

— E-maille(e-posta) gelen linklerden veya başka internet adreslerinde kesinlikle İnternet Şubeleri şifre bilgilerinizi girmeyiniz.

— E-maillerde(e-posta) şifre bilgileriniz istenirse veya şifre bilgileri isteyen sayfalara link verilirse kesinlikle girmeyiniz.

— Şifre ve Parola bilgilerinizi kimseyle paylaşmayınız, açık olarak yazmayınız, başka sitelerde kullanmayınız.

— Bilgisayarınızı en güncel Anti Virüs ve AntiSpyWare programlarıyla yetkisiz erişimlere karşı koruyunuz.

### 5.4.4 Denetim İzlerinin Oluşturulması

Banka, internet bankacılığı faaliyetlerine ilişkin işlem ve kayıt tutma süreçlerinin ve alt yapısının, delil üretecek ve bu delillerin bozulmasını önleyecek, yanıltıcı delilleri ayırt edebilecek ve taraflara sorumluluk yüklemede kullanılabilecek bilgileri sunacak şekilde yapılandırılmalıdır.

— Bu konuda sanal dolandırıcılara yetirince ceza uygulanmamaktadır. Bu kişilerin takip edilerek gözetim altında çalıştırılması ve iyi ücretlendirme uygulanarak topluma kazandırılması gerekmektedir. Böylece hackerları dolandırıcılık eylemlerinden uzak

tutarak, onların bilgi ve tecrübelerinden yararlanabilir ve daha etkin bir bilişim güvenliği sağlanabilir.

— 2007 Haziran ayında jandarma tarafından yapılan operasyonda yakalanan 31 kişilik çetede 2 kişi hacker olarak görev yapmaktaydı. Bu tip kişilerden yararlanılmalıdır.

### 5.4.5 Müşterilerin Bilgilendirilmesi

Banka, internet bankacılığı hizmetine ilişkin mevcut politika ve prosedürler ile dikkat edilmesi gereken hususlar konusunda müşterilerini bilgilendirmeli ve gerekli uyarılarda bulunmalıdır. Ayrıca banka, müşterinin talebi olmadan müşteri adına internet bankacılığını açamaz.

— Banka, internet bankacılığı hizmetine sadece maliyetlerin azaltılması yönüyle bakılmamalıdır. Müşterilere risklerle ilgili doğru ve açık bilgilendirme yapılması önerilmektedir. İnternet bankacılığı talebi ve kullanma imkânı olmayan bir müşteriye satış amaçlı internet bankacılığı hizmeti verilmesi için baskıda bulunulmamalıdır.

— Çağrı merkezlerinde müşterilere internet bankacılığı işlemlerinde her türlü soru ve sorunları için yardım alabilecekleri özel bir hat tesis edilmelidir.

### 5.4.6 Servis Sürekliliği ve Kurtarma Planı

Banka, internet bankacılığı servisi için beyan ettiği düzeyde servis sürekliliğini sağlar. Servis kesintisinin doğurabileceği hukuki sorumlulukları en aza indirmek üzere banka gerekli önlemleri alır.

— Vergi ödemeleri ve fatura ödemelerinde internet üzerinden yapılan ödemelerde son gün ve müşterilere sunulan ödeme saatlerinde kesinti yaşanırsa müşterinin ödeyemediği

fatura ve vergi borcu için bankanın sorumlu olmadığını anlatacak bilgilendirilme yapılmalıdır.

— Servis kesintisi ve süresi hakkında müşterilere sms bilgilendirilmesi yapılmalıdır.

### 5.4.7 Elektronik İmza

Bilişim suçlarını önlemek amacıyla 15.01.2007 tarihinde Meclisten geçen "Elektronik İmza Kanunu", 23.01.2007 tarihinde Resmi Gazetede yayınlanarak, 24.07.2004 tarihinde yürürlülüğe girmiştir.

Elektronik İmza: başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir.[84]

Kişinin el yazısı ile attığı imzanın sahip olduğu özellikleri elektronik ortamda gerçekleştirmeye yarayan matematiksel formüller veya şifreleme programlarıdır.[85]

Elle atılmış imzanın tarayıcıdan geçirilerek, elektronik ortama aktarılmış halidir.[86]

Elektronik imza, klasik imzaya tanınan işlevleri kapsayarak bireyin kimliğini tanıtır ve bireyin mesajın içeriğini onayladığını gösterir.[87]

Veriyi oluşturan ve gönderen kişiye ait olduğunu gösterir ve bu işlevini ancak elektronik olarak yerine getirebilir[88]

Teknolojinin kaydettiği hızlı gelişme ve internetin küresel nitelikte kullanımı elektronik yoldan aktarılan verilerin tasdikini sağlayacak hizmetlerin sağlanmasını ve buna

---

84 Prof Dr. Gürsel Öngören, "İnternet Hukuku", İstanbul: Öngören Hukuk Yayınları, 2006, s.88.
85 Leyla Keser Berber., "E-İmza Yasasına İlişkin Olarak Yapılması Gerekenler, II. Türkiye Bilişim Şurası Hukuk Çalışma Grubu, 27.02.2004, www.bilisimsurasi.org.tr/hukuk/docs/e-imza_taslak_raporu_20040227.doc, (03 Mart 2008)
86 Dr. Mine Erturgut, "Elektronik İmza Kanunu", Mayıs 2007, www.tbd.org.tr/resimler/ekler/cec07e9ba5f5bb2_ek.pdf, (05 Mart 2008)
87 Ayşe Saadet Arıkan, "Dünyada ve Türkiye' de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım", Ankara, TİGV-Bilten, 1999, s.151
88 Fikret Eren , "Borçlar Hukuku Genel Hükümler", İstanbul: Beta Yayınları, 2001, s.49.

bağlanacak hüküm ve sonuçlarının ispat edilebilirliğinin de sağlanmasını zorunlu kılmaktadır.[89]

Mahkeme bir vakanın gerçeğe uygun olup olmadığına ikame edilen delillere göre karar verir. Delilin hâkimin kanaatini etkileme kabiliyeti, delilin maddi ispat gücü olarak ifade edilebilir.[90]

Kanun bir yandan elektronik imzanın elle atılan imzayla aynı hukuki sonucu doğuracağını belirtmişken, diğer yandan konuya ilişkin düzenleme getirmiştir. Bu düzenlemeye göre elektronik imzayla oluşturulan veriler senet hükmündedir ve aksi ispat edilinceye kadar kesin delil sayılırlar.[91]

E-imza tarafları koruyan bir delil niteliğindedir ve internet banka kullanıcıları için 01.01.2007 tarihinden itibaren azami 2 yıl içerisinde kullanımı zorunla hale getirilecektir.

— Elektronik imza kullanımı ve yararları hakkında daha çok bilgilendirme yapılmalı ve müşterinin bu sistemi kullanımına teşvik edici faaliyetlerde bulunulmalıdır.

Belirtilen risk prensipleri tüm bankalarda standart hale getirilmelidir. Şuan ki uygulamada genel olarak tüm bankalarda internet şubesi kullanımında şifre sorumluluğu ve işlem yapılan bilgisayarın güvenirliliği müşteriye aittir. Bu kapsamda sorumluluğun müşteriye yüklenmesi için banka gerekli tüm güvenlik önlemlerini almış ve müşterisini güvenlik önlemleri alması konusunda bilgilendirmiş olmalıdır.

89 Doç Dr. Haluk Konuralp, "Medenî Usul Hukukunda İspat Kurallarının Zorlanan Sınırları," Ankara: Anadolu Üniv Hukuk Fakültesi Yayınları , 1999, s.15.
90 Mehmet Kamil Yıldırım, "Medeni Usul Hukukunda Delillerin Değerlendirilmesi", İstanbul; Kazancı Yayınları, 1990, s.35.
91 Mete Tevetoğlu, "Bilişim Hukuku", İstanbul: Kadir Has Üniversitesi Yayınları, 2006, s.49.

### 5.5. Türkiye' deki Bazı Bankaların İnternet Bankacılığı Güvenlik Uygulamaları

Kullanılan güvenlik uygulamalarına bakıldığında birçok bankada sms şifre, e-imza ve sanal klavyesi uygulaması görülmektedir. Bddk' nın düzenlemiş olduğu tebliğde yer alan hükümlerin bazıları bankalarda uygulanmaya başlanmıştır.

#### 5.5.1 Garanti Bankası İnternet Bankacılığı Güvenlik Uygulamaları;

— Şifrematik

Şifrematik'te üretilen bir şifre ile İnternet Şubesi'nde işlemler gerçekleştirdikten sonra, şifrematik kullanan bir başkası aynı şifreyi bir kez daha kullanamaz. İnternet Şubesi'nde yeniden bir işlem yapmak istenildiğinde Şifrematik' le yeni bir şifre oluşturur ve işlem tamamlanır.

— Cepşifrematik

Cep Şifrematik, Garanti Bankası İnternet ve Cep Şubesi kullanımında ekstra güvenlik sağlayan "Tek Kullanımlık Şifre" üreten bir uygulamadır. Cep Şifrematik'te üretilen bir şifre ile İnternet ve Cep Şubesi'nde işlemler gerçekleştirdikten sonra, kullanan kişi ve bir başkası aynı şifreyi bir kez daha kullanamaz.

İnternet ve Cep Şubesi'nde yeniden bir işlem yapmak istenildiğinde Cep Şifrematik' le yeni bir şifre oluşturur ve işlemi tamamlanır.

— Mobil İmza

Mobil İmza, elektronik ortamlarda kullanabilecek kimlik kartıdır.

— SMS ile Doğrulama

İnternet Şubesi üzerinden yapılan para transferleri, bilgi güncellemeleri ve bazı ödeme işlemlerinin gerçekleştirilmesi öncesinde kullanıcıdan sms yoluyla onay alma işlemidir.

— Mini Klavye (Sanal Klavye)

Mini Klavye, bilgisayarın klavyesindeki tuşları kullanmadan, fare kullanarak ekrandan İnternet Şubesi şifre girişinin yapmasına olanak sağlar.[92]

### 5.5.2 Yapı Kredi Bankası İnternet Bankacılığı Güvenlik Uygulamaları;

— Akıllı Sms

Bir alıcıya ilk defa yapılan para transferi için "Tek Kullanımlık Şifre" SMS'i gönderir.

— Akıllı Anahtar

İnternet bankacılığı kullanıcılarına iki kademeli güvenlik sağlayan bir üründür. Akıllı Anahtar her kullanımda “Tek Kullanımlık Şifre” üretir ve internet bankacılığı girişlerinde her zamanki şifreye ek olarak kullanılmaktadır.

— Akıllı Cep

Akıllı Cep, cep telefonunda çalışan "Tek Kullanımlık Şifre" üretim yazılımıdır. Akıllı Cep ile internet bankacılığına girişte iki kademeli güvenlik, cep telefonunun tarafından üretilen tek kullanımlık şifreler ile sağlanır.

1) Cep Telefonuna yüklenen Akıllı Cep uygulamasını kullanıcı tarafınızdan belirlenen açılış şifresini (PIN) girerek çalıştırılır,

2) Akıllı Cep çalıştığında, cep telefonunun ekranında 8 hanelik Tek Kullanımlık Şifresi belirecektir,

3) Telefonun ekranında beliren 8 haneli rakamı aktivasyon ekranındaki ilgili alana girilir ve "Tamam" tuşuna basılır.

Aktivasyon işleminden sonra Yapı Kredi İnternet Bankacılığı’na her giriş sırasında kullanıcı kodu ve statik şifreye ek olarak Akıllı Cep tarafından üretilecek Tek Kullanımlık Şifre ile sisteme girilmesi beklenecektir.

92 http://www.garanti.com.tr/subesiz/internet_bankaciligi/guvenlik/, 18.04.2008

— Mobil İmza

Elektronik ortamda ıslak imza atmış gibi işlem yapılabilmesini sağlayan bir servistir. 5070 sayılı Elektronik İmza Kanunu'na göre elle atılan imza ile eşdeğer sayılan elektronik imzanın cep telefonuyla atılması sağlanır.

— PC Klavye

PC Klavye, Yapı Kredi İnternet Bankacılığı şifre giriş ekranında kullanılan sanal klavyenin kişiselleştirilmiş halidir. Gerçek Yapı Kredi İnternet Bankacılığı sayfasında olduğunu göstererek bazı internet tehditlerinden korunmayı sağlar.[93]

### 5.5.3 Akbank İnternet Bankacılığı Güvenlik Uygulamaları;

— Cep şifre

Bireysel ve Kurumsal İnternet Şubeleri 'nden yapılan tüm para transferi işlemleri (Havale, EFT gibi) cep telefonunuza SMS ile gönderilen CepŞifre ile gerçekleştirilir.

Bireysel müşteriler için cep şifre zorunlu, Kurumsal müşteriler için isteğe bağlıdır. CepŞifre, İnternet Şubesi üzerinden yapılan para transferleri ve bazı ödeme işlemlerinin son ekranında SMS yoluyla onay alma işlemidir.

— Mobil İmza

— Parola

Bireysel İnternet Şubesi'nde CepŞifre kullanılmayan bazı işlemlerde, kullanıcı tarafından belirlenen parolanın 2 farklı karakteri sorularak işlem yapılır.

Kurumsal İnternet Şubesi' nde cep şifre kullnamayan müşteriler parola kullanmaktadır.

— Ip kısıtlama

93 http://www.ykb.com/tr-TR/sinirsiz_bankacilik/internet_bankaciligi, 18.04.2008

### 5.5.4 Finansbank İnternet Bankacılığı Güvenlik Uygulamaları;

— Mobil İmza

— SMS Şifresi

Tek Kullanımlık Yüksek Güvenlik SMS Şifresi", Finansbank İnternet Bankacılığı işlemleri için cep telefonuna gönderilecek onay şifresidir. İki tür SMS şifresi bulunmaktadır. Giriş SMS Şifresi : İnternet Bankacılığı'na giriş işlemi sırasında kullanılır. İşlem SMS Şifresi: İnternet Bankacılığı'nda yapılan para transferleri ve ödeme işlemlerinde kullanılır.

— Ip kısıtlama

İnternete bağlanılan ülkeyi, internet servis sağlayıcısı veya internete bağlanırken kullanılan bilgisayarın Ip numarası öğrenilerek bilgiler sisteme tanımlanabilir. Kullanıcının tanımladıkları dışındaki ülkelerden, internet servis sağlayıcılarından veya bilgisayarlardan İnternet Bankacılığı'na erişim engellenmetedir.[94]

### 5.5.6 İşbankası İnternet Bankacılığı Güvenlik Uygulamaları;

— İ-Anahtar

İ-anahtar, "Tek Kullanımlık Şifre" üreten bir cihazdır. İş Bankası internet şubesine girerken, her seferinde i-anahtar ile farklı bir şifre üreterek, giriş güvenlik seviyesi arttırabilir.

— Mobil Onay

Mobil Onay, belirli işlemlerin sistemde kayıtlı cep telefonuna gönderilen

94 http://www.finansbank.com.tr/bireysel/intbank.jsp, 19.04.2008

“Mobil Onay Kodu”nu girerek doğrulamasını sağlayan bir uygulamadır. Mobil onay kodu rakam veya harflerden oluşan 4 haneli bir koddur ve tek kullanımlıktır.

— Mobil İmza

— SMS ile uyarı

SMS ile uyarı sistemi'ni kullanmanız halinde Havale, EFT gibi transfer işlemlerini gerçekleştirdiğiniz anda sistemimiz, otomatik olarak işlem hakkında bilgi veren bir SMS gönderir.[95]

— Sanal Klavye

— Ip kısıtlama

### 5.5.7 Denizbank İnternet Bankacılığı Güvenlik Uygulamaları;

— ŞifreTek

— ŞifreTek Mobil, java destekli cep telefonlarına yüklenen ve bu telefonlar üzerinde çalışan Tek Kullanımlık Şifre üreten bir uygulamadır.

— Sms Doğrulama

Ek güvenlik isteyen kullanıcılar, internet şubeye girişlerde ve para transfer işlemlerinde, belirli saat ve belirli tutarlarda sms doğrulama opsiyonunu seçerek işlem yapabilirler.[96]

— Sanal Klavye ve Mobil İmza

95 ttp://www.isbank.com.tr/interaktif/i-interaktif-guven.html, 19.04.2008
96 http://www.denizbank.com/TR/Acikdeniz/guvenlik/, 19.04.2008

## 5.6. TARAFLARIN SORUMLULUKLARI

### 5.6.1 Banka Müşterisinin Sorumluluğu

Müşterinin şifre ve diğer bilgilerine dışarıdan müdahale edilmesi durumunda sorumluluğun nasıl paylaştırılacağı önemli bir konudur. Elektronik bankacılık hizmeti alan müşterinin sorumluluklarını belirlemeden önce bankanın elektronik bankacılığı kullanımı konusunda müşterilerine gereken güvenlik bilgilerini iletip iletmediği ve bu konudaki sorumluluğunu yerine getirip getirmediği tespit edilmelidir.

Bankaların müşterileri ile yaptıkları elektronik bankacılığı sözleşmelerinde ve müşterilere yaptıkları uyarılarda kendilerine verilen şifreleri iyi muhafaza etmeleri, bu şifreleri başka kişilere vermemeleri gerektiği belirtilmektedir. Bu uyarılar ve imzalanan elektronik bankacılığı sözleşmeleri, müşterilere özen yükümlülüğü getirmektedir. Yapılan bu uyarılara rağmen bunları dikkate almayarak özensiz davranan, şifre ve bilgisayar güvenliğini sağlayamayan müşterinin meydana gelen zararı kendi sorumluluğundadır.[97] Ancak müşterinin özen yükümlülüğünü yerine getirip getirmediğini tespit etmek zordur. Olta ve yanlış adrese yönlendirme yöntemleriyle dışarıdan yapılan müdahalelerde açılan internet sayfası, bankanın internet sayfasıyla aynı görünümdedir. Sahte sitelerde tek fark bir harf ya da adresin sayılar içermesidir. Kullanılan bilgisayarın, virüse karşı, güvenlik açıklarını kapatacak yazılımlar içermesi ve bu tür sitelere girişi engelleyecek özellikte olması gerekmektedir. Ancak müşterinin bu özellikte yazılımlar kullanması zorunluluğu henüz kesin bir karara bağlanmamıştır.

Alman Yüksek Mahkemesi "Dialar(otomatik ağ bağlantısı)" kararında ortalama bir internet kullanıcısının dialeri(otomatik ağ bağlantısı) engelleyici yazılımlar bulundurmak zorunda olmadığını ve bu kontrolün ondan beklenemeyeceği kararına ulaşmıştır. Bu karara göre internet kullanıcısına güvenli yazılımlar kullanma zorunluluğu getirilmez. Ancak

97 İrene Karper, " Kazancı Hukuk Otomasyon Programı" ,18.10.2007 http://www.karar.org/forum/hukuk/elektronik+bankacilikta+bankanin+yukumluluk+ve+sorumluluklari+3-t5803.0.html, (25 Ocak 2008)

mahkemenin bu görüşü eleştirilmektedir ve ilk derece mahkemelerinde bu konularda farklı içtihatlar ortaya konulmaktadır.[98]

Bankanın tam olarak aydınlatma yükümlülüğünü yerine getirdiği hallerde, müşterilerinde özen yükümlülüğünü yerine getirmesi gerekmektedir. Müşteri, ortalama bir internet kullanıcısından beklenen önlemleri almalıdır. Bankanın kendisine tavsiye ettiği yazılımları kurmak, gerekli ve yeterli güvenlik önlemlerini almak zorundadır.

### 5.6.2 Bankanın Sorumluluğu

Bankaların dışarıdan müdahaleye karşı kurum olarak önlemlerini almak ve ayrıca müşterilerini bu konuda uyarmak yükümlülükleri vardır. Bankanın asıl sorumluluğu, müşterilerine bu tür saldırılara karşıda etkin olabilecek standartta yazılımları hazırlayıp sunmasıdır. Bankaların web sayfalarının kolayca taklide elverişli olmaması için gerekli tedbirlerin de banka tarafından alınması gereklidir. Bazı bankalar müşterilerine özel sayfalar ve tasarımlar yapmaktadır.

Bankanın sorumluluğunun tayininde en önemli konu, bankanın kullandığı donanım ve yazılımın güvenli olduğunun ispatıdır. Bankaların ayrıca elektronik bankacılıkta belirli bir standarda sahip olmaları gerekir.[99] Bu konuyla ilgili standart oluşturma çabaları devam etmektedir.[100]

Bankanın yazılımlarının incelenmesi ve güvenlik testinden geçirilmesi ticari sır( banka sırrı) kapsamında değerlendirilmektedir.[101] Bankalar, kullandıkları yazılımlarının incelenmesini ticari sırlarının açığa çıkması endişesiyle engelleyebilirler. Güvenlik

98 Karper, a.g.e
99 Melih Gençtürk, "Elektronik Bankacılık ve Güvenlik", 30.10.2006, http://hukukcu.com/modules/smartsection/item.php?itemid=116, ( 30.Aralık 2007)
100 Abdülkadir Kırmızı, "Hacker Yöntemiyle Şubeyi Koruyorlar", Capital Mayıs 2003, http://www.capital.com.tr/haber.aspx?HBR_KOD=2602, (30 Aralık 2007)
101 Mehmet Emin Bilge, "Ticari Sırların Korunması", Ankara: Asil Yayınevi, 2005, s.5

standardının bulunmadığı hallerde ispat yükünün bankalarda olması gerekir. Bankalar bütün yazılımlarının, güvenlik sistemlerinin incelenmesini kabul etmiyorsa, mahkemeye tatmin edici açıklamalar yapmak zorundadır.

Tüketici birliklerinin bankaları, güvenliği yüksek olan standartlara zorlama eğilimi vardır. Almanya federal tüketici merkezinin yayınladığı raporda, bankaların artık güvenli sisteme geçmeleri gerekliliği anlaşılmıştır. Bu rapora göre; bankaların klasik şifre sistemlerinden vazgeçip elektronik bankacılıkta gerçekleştirilecek her işlem için bir defalık şifre üreten cihaz veya cep telefonu ile şifre verilmesi sistemine geçmelidir.[102]

102 Nicola D. Schmidt, "Verbraucherschutz im Internet - Wie viel Vertrauen ist gerechtfertigt?", 2005, s.25

## SONUÇ:

İnternet bankacılığı kullanımda banka ve kullanıcı aynı taraftadır, karşılarında ise organize suç çeteleri bulunmaktadır.

İnternet bankacılığı dolandırıcılık olaylarının engellenmesinde banka ve kullanıcıların birlikte hareket etmesi gerekmektedir. Her iki tarafın sorumlulukları farklıdır. Güvenlik konusunda sadece bir tarafın özenli hareketi yeterli değildir.

Bankalar en güvenli şekilde internet bankacılığını kullandırmakla yükümlüdür. Kullanıcılar ise, İnternet bankacılığı kullandıkları PC güvenliğini sağlamak ve güvenlik konusunda özenli davranmakla yükümlüdür.

Bankacılık işlemlerinin elektronik ortama taşınması nedeniyle yeni riskler ortaya çıkmıştır. Elektronik bankacılık işlemlerindeki gelişmeler arttıkça bu gelişmelere bağlı risklerde artmaktadır. Bankalar bu riskleri yönetmede daha etkin olmalıdır.

Teknolojinin sürekli değişmesi, kanunda bu konuda düzenlemeler yapılmasını zorlaştırmaktadır. Bilişim suçları hukuksal değerlere göre daha düzenli ve kapsamlı maddeler içermelidir.

Sistemden kaynaklanan eksiklik ve aksaklık sebebiyle oluşan zararlara banka katlanmalıdır. Kullanıcının hatasından kaynaklanan zararlara ise sistemi kullanan banka müşterisi katlanmalıdır. Bazı durumlarda ise iki tarafta suçlu bulunabilir. Bu tür durumlarda ise taraflar suç oranı kadar sorumluluğa katlanmalıdır.

# KAYNAKÇA


Adalı Eşref, "Bilişim Ağı Hizmetlerinin Düzenlenmesi Bilişim Suçları Hakkında Kanunu Tasarısı", http://160.75.26.41/, ( 18 Aralık 2007)

Ahi Gökhan, "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler", 04.07.2005, http://hukukcu.com/modules/smartsection/item.php?itemid=74, (12 Kasım 2007)

Akbulut Berrin, "Türk Ceza Kanununda Bilişim Suçları", Yayımlanmamış Doktora Tezi (Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Ceza ve ceza Usul Hukuku Bilim Dalı), Konya, 1999

Akdağ Burak, "İnternet Dolandırıcılığı Şebekesi Çökertildi", 01.11.2007, http://www.polishaber.com/article_view.php?aid=15650 , (24 Kasım 2007)

Alataş Şükrü, Altan Murat "İnternet Denizin Popüler Avlanma Yöntemi",10.11.2007, http://inettr.org.tr/inetconf12/bildiri/25.pdf, (12 Aralık 2007)

Anadolu Ajansı, "İnternet Dolandırıcılarına Ağır Darbe", 27.06.2007, http://www.haber7.com/haber.php?haber_id=251716, (08 Aralık 2007)

ANKA, "Akbank' tan Dolandırıcılık İzahı"02.06.2007, http://www.gercekgundem.com/?p=66958&com=all, (15 Aralık 2007)

Arıkan Ayşe Saadet, “Dünyada ve Türkiye' de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım”, Ankara, TİGV-Bilten, 1999, s.151

Arkan Sabih, “Bankacılıkta Kullanılan Yeni Elektronik Sistemlerle İlgili Hukuki Sorunlar, Ankara: TBB Yayınları, 1991

Atakan Kenan Burçin, Sayar Ceren, Büyükgören Fisun, Aydın Fatma, Ter Ali Süha, Sargın Emre, Türkiye Bankalar Birliği İnternet Bankacılığı Çalışma Grubu, “Bankacılıkta Dolandırıcılık Eylemleri Tespit Önleme Yöntemleri”,Nisan 2007, www.tbb.org.tr/v12/doc/Kitapçık.pdf ,(14 Eylül 2007)

Aydın Emin, “Bilişim Suçları ve Hukukuna Giriş”, Ankara: Doruk Yayınları, 1992

Basel Bankacılık Denetim ve Gözetim Komitesi, “Elektronik Bankacılık ve Elektronik Para Faaliyetleri için Risk Yönetimi, Ankara: TBB Yayınları, Mart 1998

Başoğlu Kürşad, “Teknolojiye Boyun Eğmeyin( Bilişim Suçlarına Genel Bakış)”,10.09.2007, www.bilisimsuclari.com/2007/09/10 , (17 Kasım 2007)

BDDK,“Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ”,14.09.2007 http://www.bddk.org.tr , (15 Mart 2008)

Beceni Yasin, “Siber Suçlar”, 01.01.2003, http://hukukcu.com/modules/smartsection/item.php?itemid=83, (18 Aralık 2007)

Berber Leyla Keser, "E-İmza Yasasına İlişkin Olarak Yapılması Gerekenler, II. Türkiye Bilişim Şurası Hukuk Çalışma Grubu, 27.02.2004

Bilge Mehmet Emin, "Ticari Sırların Korunması", Ankara: Asil Yayınevi, 2005

Boğaç Erkan, Mursat Songür, "Açıklamalı Bilg ve İnt Terimleri Sözlüğü" , Ankara: Hacettepe-Taş Kitapçılık, 1999

Bozkurt Veysel, "Elektronik Ticaret Hukuk Çalışma Grubu Raporu",İstanbul: Alfa Yayınları, 1998

Cairncross Frances, "The Death Of Distance, London: Orion Business Books", 1997

Carse David, "Regulatory framework of e-banking", 8 Ekim 1999

Çelik Abdullah, "İnternet Bankacılığı: Uygulamalar ve Bankacılığın Geleceğindeki Muhtemel Etkileri", Active Dergisi, 2002, Sayı:27

Dalyan Mehmet, " Siber Suçlar ve Acil Durum Yönetmeliği" , 01.07.2006, http://dalyanda.com/wp- content/uploads/2006/06/ MehmetDalyanda_SiberSuclar_ve_AcilDurumYonetimi_Haziran2006.pdf, (1 Mayıs 2008)

Değirmenci Olgun, "Bilişim Suçları", Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2002

Demir Önder, " İnternet Servis Sağlayıcısının Cezai Sorumluluğu".İzmir Barosu Dergisi, 2000, Sayı:3

Denning Dorothy E., "LawEnforcement, Security and Surveillance in the Information Age" ,London, 2000, s.129

Dokurer Semih, " Ülkemizde Bilişim Suçları Ve Mücadele Yöntemleri",1 Mayıs 2003, www.bilisimsurasi.org.tr/dosyalar/17.doc.,(14 Eylül 2007)

Draft Convention on Cyber Crime and Explanatory Memorandum Related There To, wwwconventions.coe.int/treaty/EN/projects/cybercrime27.doc, (25 Ekim 2002)

Dursun Selman, "Bankacılık Düzenine Karşı İşlenen Suçlar", Ankara: Seçkin Yayıncılık, 2006

Dülger Murat Volkan: "Bilişim Suçu Olarak Pornografi", 09.09.2004, http://turk.internet.com/haber/yazigoster.php3?yaziid=10852 , (29Aralık 2007)

Dülger Murat Volkan, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu" , Güncel Hukuk Dergisi, İstanbul, Kasım 2005, Sayı 23

Dülger Murat Volkan, "Bilişim Suçları, Ankara, Seçkin Yayıcılık, 2004

Ekizer Ahmet Hakan, “Oltaya Gelmeyin (Phishing Saldırıları)” 15.01.2007, http://www.ekizer.net/content/view/15/1/, (10 Ekim 2007)

Ekizer Ahmet Hakan, Hackerler, Yöntemleri ve Araçları,http://www.ekizer.net, (17 Kasım 2007)

Emmanuel Mesthane, “Technology as a Social and Political Phenomenon” , 1976, www.icisleri.gov.tr/_Icisleri/WPX/tezler_internetsuclari.doc, (14 Eylül 2007)

Eren Fikret, “Borçlar Hukuku Genel Hükümler”, İstanbul: Beta Yayınları, 2001

Erturgut Mine, “Elektronik İmza Kanunu”, Mayıs 2007, www.tbd.org.tr/resimler/ekler/cec07e9ba5f5bb2_ek.pdf, (05 Mart 2008)

Geleri Aytekin, Soysal Mustafa, Kaygısız Mustafa, Arslan Tamer Azem, ”İnternet Suçlarıyla Mücadelede Suç Önleme Anlayışı ve Bilinçli Kullanıcı” 27.06.2007 http://www.bilisimsuclari.com, ( 01.12.2007)

Gençtürk Melih, “Elektronik Bankacılık ve Güvenlik”, 30.10.2006, http://hukukcu.com/modules/smartsection/item.php?itemid=116, ( 30.Aralık 2007)

Güran Sait, Akünal Teoman, Bayraktar Köksal, Yurtcan Erdener, Kendigelen Abuzer, Beller Önder, Bülent Sezer, “İnternet ve Hukuk Temel Metni”, 2002, http://www.sosyalbil.selcuk.edu.tr/sos_mak/makaleler ,(18 Eylül 2007)

İlyasoğlu Cumhur, “Müşteri Hizmetlerini Aradı, Hesapları Boşaltıldı”,01.06.2007, http://www.pcguvenlik.com, (15 Aralık 2007

İnal Emrehan, “Reklâm Hukuku ve Aldatıcı Reklâmlar”, İstanbul, Beta Yayıncılık, 2000

Kaptan Hakan, “Bilişim Güvenliği”, 2006, http://www.artifex.com.tr/Content_Articles/Default.asp?articleId=14, (30 Eylül 2007)

Karper İrene, “ Kazancı Hukuk Otomasyon Programı” ,18.10.2007 http://www.karar.org/forum/hukuk/elektronik+bankacilikta+bankanin+yukumluluk+ve+sorumluluklari+3-t5803.0.html, (25 Ocak 2008)

Kent Stephen, “On The Trail of İntrusions İnto İnformation Systems”, 2000

Kırmızı Abdülkadir, “Hacker Yöntemiyle Şubeyi Koruyorlar”, Capital Mayıs 2003, http://www.capital.com.tr/haber.aspx?HBR_KOD=2602, (30 Aralık 2007)

Konuralp Haluk, “Medenî Usul Hukukunda İspat Kurallarının Zorlanan Sınırları,” Ankara: Anadolu Üniv Hukuk Fakültesi Yayınları , 1999

Kurt Levent, “Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanundaki Uygulanması”, Ankara, Seçkin Yayıncılık, 2005, s.151. - Ali Karagülmez, “Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri”, Ankara: Seçkin Yayıncılık, 2005

Kuyaksil Ali, Köroğlu Harun, "Türkiyede Meslekleşme Olgusu olarak Özel Güv. Hiz.", Polis ve Sosyal Bilimler Dergisi, Ekim 2005, Cilt:3, Sayı:2

Meran Necati, "Yeni Türk Ceza Kanununda Sahtecilik – Malvarlığı Bilişim suçları ile Ekonomi ve Ticaret Alanında Suçlar", Ankara: Seçkin Yayıncılık, 2005

Miller Sandra Key, "Computer İnnovative Technology for Computer Professionals, 2001

Öngören Gürsel, "İnternet Hukuku", İstanbul: Öngören Hukuk Yayınları, 2006

Özcan Mehmet, "Türkiye'de İnternet Konferansları VII" İstanbul Harbiye Askeri Müzesi, Bilal Şen, "Bilişim Suçlarının Getirdikleri ve Üzeyir Garih Cinayeti", Polis Dergisi, Aralık 2002, Sayı: 29

Özdilek Ali Osman, Burak Çekiç, Muharrem Taç, "Sanal Dolandırıcılık (Phising)", 30.01.2006, http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=3&id=16, (12 Kasım 2007)

Özel Cevat, "Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", İstanbul Barosu Dergisi, İstanbul, Eylül 2001, Sayı:7-8-9

Paul Mungo, Bryan Clough, "Sıfıra Doğru Veri Suçları ve Bilgisayar Yer altı Dünyası", Çev.: Kurma Emel, İstanbul: İletişim Yayınevi, 1999

Pek Ahmet, Emniyet Müdürü, "Şifre Operasyonu ve İnteraktif Dolandırıcılık", 25.5.2006, www.samsuntso.org.tr/Bilgi_Bankasi/interaktif_dolandiricilik.pdf, (24 Kasım 2007)

Sansar Mustafa, "Sanal Dolandırıcılıkta Son Nokta Phıshıng" ,31.10.2007 , http://www.iem.gov.tr/iem/?menu_id=1&detay_id=68 ,(24 Kasım 2007)

Schjolberg Stein, "The Legal Fremework-Penal Legislation in 44 Countries", 08.02.2004, www.mosstingrett.no, (17 Aralık 2007)

Schjolberg Stein, "Unauthorized Access to Computer Systems",15.01.2003, www.mossbyrett.of.no/info/legal.html, (12 Kasım 2007)

Schmidt Nicola D., "Verbraucherschutz im Internet - Wie viel Vertrauen ist gerechtfertigt?", 2005

Sınar Hasan, "Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme" , İstanbul: Galatasaray Üniversitesi Yayınları, 2004

Sınar Hasan, "İnternet ve Ceza Hukuku", İstanbul: Beta Yayınları, 2001

Stoll Clifford, "Slicon Snake Oil: Second Thoughts on the ınformation Hıgway", London Pan Books, 1996

Şen Bilal, "Bilişim Suçlarının Getirdikleri ve Üzeyir Garih Cinayeti", Polis Dergisi, Yıl 7, S. 29, Ekim-Kasım-Aralık 2002

Şimşek Hüseyin, “Toplum Destekli Polislik”, Yüksek Lisans Tezi, Kırıkkale, 2002

TBB, “Dolandırıcılık Eylemleri Tespit ve Önleme Yöntemleri”, Mart 2007, www.tbb.org.tr/v12/doc/Sunum.ppt, (18 Eylül 2007)

Tevetoğlu Mete, “Bilişim Hukuku”, Kadir Has Üniversitesi Yayınları, 2006

Toplaoğlu Mustafa, “İnternette Fikri Haklar Sorunları” 09.09.2004, http://turk.internet.com/haber/yazigoster.php3?yaziid=10852 , (29Aralık 2007)

Ünver Yener, “Ceza Kanunun Değerlendirilmesi”, Ankara: Seçkin Yayıncılık, 2006

Viega John and Voas Jeffrey, “IT Professional Technology Solutions for The Enterprise”, 2000

Wall David S., “İnternet Rejimi ve Düzenleme Sorunu”, Çev: Hasan Sınar, Adalet Yüksek Okulu, 20.Yıl Armağanı, İstanbul, 2001, s.203

Wall David S., “Their Victims and Their Regulation” , 1999

Yazıcıoğlu R.Yılmaz, “Bilgisayar Suçları”, İstanbul, Alfa Yayınevi, 1997

Yazıcıoğlu R. Yılmaz, “Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirmesi”, Hukuk ve Adalet: Eleştirel Hukuk Dergisi, İstanbul, Ocak-Mart 2004, Sayı:1

Yıldırım Mehmet Kamil, “Medeni Usul Hukukunda Delillerin Değerlendirilmesi”, İstanbul; Kazancı Yayınları, 1990

Yılmaz Murat, “Bilişim Suçları Hakkında”, 2001, http://www.olympos.org/article/articleview/261/1/2, (1 Eylül 2007)

http://www.checkpoint.com/product/protect/images/firewall-1_index_lg.gif, 25.05.2002

http://www.deltamenkul.com.tr/ssl.htm, 18.04.2008

http://www.denizbank.com/TR/Acikdeniz/guvenlik/, 19.04.2008

http://www.finansbank.com.tr/bireysel/intbank.jsp, 19.04.2008

http://www.garanti.com.tr/subesiz/internet_bankaciligi/guvenlik/, 18.04.2008

http://www.microsoft.com/turkiye/windows2000pro/ozellikler.asp, 15.05.2002

http://www.signalguard.net/sifreleme/key.htm, 24.05.2002

http://www.tekstilteknik.com/sozluk/yabanci.asp?yabbas=H, (14 Eylül 2007)

http://www.isbank.com.tr/interaktif/i-interaktif-guven.html, 19.04.2008

http://www.ykb.com/tr-TR/sinirsiz_bankacilik/internet_bankaciligi, 18.04.2008

www.bilisimsurasi.org.tr/hukuk/docs/e-imza_taslak_raporu_20040227.doc, (03 Mart 2008)

www.tbb.org.tr/net/dönemsel/, 14 Eylül 2007