İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

ONLİNE BANKACILIK SUÇLARINA İLİŞKİN CEZA DAVA DOSYALARININ İNCELENMESİ

İsmet YİĞİTBAŞI
Enformatik Anabilim Dalı

Danışman
Doç. Dr. Mustafa AKSU

İkinci Danışman
Yrd. Doç. Dr. Fatih GÜRSUL

Mayıs, 2012

İSTANBUL

2601090401 Öğrenci numaralı İsmet Yiğitbaşı tarafından hazırlanan bu çalışma 26/07/2012 tarihinde aşağıdaki jüri tarafından Enformatik Anabilim Dalı Tezli Yüksek Lisans programında Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Jürisi

Doç. Dr. Mustafa AKSU(Danışman)
İstanbul Üniversitesi
Hukuk Fakültesi

Prof. Dr. Sevinç GÜLSEÇEN
İstanbul Üniversitesi
Enformatik Bölümü

Prof. Dr. Süleyman ÖZDEMİR
İstanbul Üniversitesi
İktisat Fakültesi

Prof. Dr. Mahmut KOCA
İst. Şehir Üniversitesi
Hukuk Fakültesi

Doç. Dr. Abdullah BAL
Yıldız Teknik Üniversitesi
Elektrik-Elektronik Fakültesi

ÖNSÖZ

Yüksek lisans tez çalışmamda ve yüksek lisans öğrenimimde desteğini ve ilgisini esirgemeyerek bana yol gösterici olan çok değerli danışman hocalarım Doç. Dr. Mustafa AKSU'ya ve Yrd. Doç. Dr. Fatih GÜRSUL'a en içten duygularımla teşekkür ederim. Ayrıca Bölüm Başkanı Prof. Dr. Sevinç GÜLSEÇEN başta olmak üzere çok değerli Enformatik Bölümü ailesine teşekkkür ederim.

Tez çalışmasının araştırma kısmında bana yardımcı olan Sultanahmet, Bakırköy, Kadıköy ve Pendik Adliyesi'ndeki çok değerli Cumhuriyet Savcıları, hakim ve kalem personeline ile İstanbul Emniyet Müdürlüğü Bilişim Suçları ve Sistemleri Müdürlüğü'ndeki başkomiser, komiser ve tüm emniyet çalışanlarına teşekkür ederim.

Çalışmamda beni sürekli yüreklendiren, destekleyen biricik aileme teşekkürlerimi sunuyorum. Ayrıca Mehmet Hanifi ŞEKER'e, Ahmet ZELKA'ya, Serhat YILMAZ'a ve Emrah KARABOĞA'ya yardımları için teşekkür ediyorum.

Mayıs, 2012 **İsmet YİĞİTBAŞI**

Sevgili Aileme …

İÇİNDEKİLER

ŞEKİL LİSTESİ

TABLO LİSTESİ

KISALTMALAR

TCK – Türk Ceza Kanunu

YY – Yüzyıl

ATM - Automatic Teller Machine, Otomatik Vezne Makinası

ABD – Amerika Birleşik Devletleri

vb. – Ve Benzeri

vd. – Ve Diğerleri

TDK – Türk Dil Kurumu

TBB - Türkiye Bankalar Birliği

EFT – Elektronik Fon Transferi- Electronic Fund Transfer

EPOS – Electronic Point of Sale-Elektronik Satış Noktası

PC – Personal Computer-Kişisel Bilgisayar

BDDK - Bankacılık Düzenleme ve Denetleme Kurulu

ETSI - Avrupa Telekomünikasyon Enstitüsü

SMS – Kısa Mesaj Servisi

CCV - Card Code Verification

GSM - Global System for Mobile Communications

SIM - Subscriber İdentity Module

ŞifreTek – Tek Kullanımlık Şifre

USB - Universal Serial Bus-Evrensel Seri Veriyolu

SSL - Secure Socket Layer, Güvenli Yuva Katmanı

HTTP - Hypertext Transfer Protocol-Hiper Metin Transferi Protokolü

IP -Internet Protocol- İnternet Protokol

SET - Güvenli Elektronik İşlemler, Secure Electronic Transactions

PIN - Kişisel Tanımlama Numarası, Personal Identify Number

ISS - İnternet Servis Sağlayıcıları

TEB – Türkiye Ekonomi Bankası

ÖZET

ONLİNE BANKACILIK SUÇLARINA İLİŞKİN DAVA DOSYALARININ İNCELENMESİ

Bu çalışmanın amacı; online bankacılık suçlarına ilişkin ceza dava dosyalarını inceleyerek literatüre katkı sağlamaktır. Çalışma iki ana kısımdan oluşmaktadır. Birinci kısımda; Türk Ceza Kanunun'daki (TCK) bilişim suçları maddeleri, online bankacılık, kişisel bilgi hırsızlığı yöntemleri, ilgili araştırmalar konu başlıkları altında bilgiler yer almaktadır.

İkinci kısım ise; bulgular, sonuçlar ve öneriler bölümlerinden oluşmaktadır. Araştırmanın örneklemini İstanbul ili sınırları içerisinde bulunan Bakırköy, Kadıköy, Sultanahmet ve Pendik Adliyeleri olmak üzere dört adliyedeki toplam yirmi bir ceza mahkemesi ile İstanbul Emniyet Müdürlüğü'nde faaliyet gösteren Bilişim Suçları ve Sistemleri Şube Müdürlüğü oluşturmaktadır. Veri toplama süreci, 2011 yılının Mayıs-Haziran ayları ile 2012 yılının Mart-Nisan ayları içerisinde gerçekleşmiştir. Elde edilen elli dört dosyadan "online bankacılık suçları ile ilişkili dava dosyalarını inceleme anketi"ne göre veriler toplanmıştır. Bu araştırma için nicel araştırma modeli uygulanmış ve ölçütlerin sıklıkları dikkate alınmıştır. Araştırma sonucunda elde edilen veriler, frekanslar ve yüzdeler hesaplanarak çözümlenmiştir. Bu hesaplamalar için Microsoft Excel 2010 paket programı kullanılmıştır.

Araştırma sonucunda 334 erkek, 24 kadın olmak üzere toplam 358 kişinin suça karıştığı tespit edilmiştir. Suça konu olan toplam para miktarın ise 3 milyon 700 bin TL olarak belirlenmiştir. Tüm dosyalar içinden Internet Protocol (IP) numarası tespit edilen 41 dosya bulunmuştur. IP numarası belirlenemeyen dosya sayısı 15'dir. Adliyelerde elde edilen dosyaların 27'sinde suç yöntemi belirlenememiştir. 20 dosyada ise dava hazırlık süresinin 24 ay ve 24 aydan fazla olduğu tespit edilmiştir. Elde edilen verilerde dijital delillerin ve bilişim uzmanı raporlarının az olduğu görülmüştür.

Bu sonuçlar ışığında; adli makamların bilişim suçlarına karşı özel olarak yapılanması, dijital delileri elde etmeye yönelik çalışmalarının artması gerektiği, sahte belgelere karşı kurumların ve şirketlerin gerekli önlemleri alması, bilişim uzmanlarının dava hazırlık aşamasında etkin olması, dava hazırlık süresinin kısaltılması adına kurumlar arası yazışmaların güvenli ağlar üzerinden gerçekleşmesi önerileri yapılabilir.

SUMMARY

INVESTIGATION OF CRIMINAL CASE FILES RELEVANT TO ONLINE BANKING CRIMES

The aim of this study is to contribute to the literature by investigating criminal case files related to online banking crimes. The study consists of two main parts. The first part includes the articles of computer crimes in Turkish criminal law, online banking, theft of personal information methods, and related researches.

The second part consists of material-method; findings, results, and suggestions. The sample of the research is derived from 21 criminal courts in 4 district judiciaries – included Bakırköy, Kadıköy, Sultanahmet, and Pendik Courthouses – and computer crimes - systems branch in İstanbul Police Department. The process of data acquisition is conducted in May-June 2011 and March-April 2012.

Data is gathered from 54 obtained files according to investigation criteria of case files related to online banking crimes. Quantitative research pattern is applied to this study and frequency of criteria is considered. The data obtained from this study is analyzed using frequencies and percentages. Microsoft Excel 2010 software package is used for these analysis. As a result of the research, it is confirmed that totally 358 people - 334 of them are male and 24 female – have been involved in crime. Of all files, IP (Internet Protocol) numbers of 41 files are determined and the number of files with unknown IP is 15. Crime methods of 27 files gathered from courthouses cannot be determined. It is confirmed that the case preparation of 20 files is 24 months and longer. It is seen that digital proofs and the reports of digital forensics specialists are inadequate.

In the light of these results, it can be suggested that judicial authorities should reorganize against computer crimes, the efforts on obtaining digital proofs should be increased, institutions and companies should take necessary precautions against false documents, digital forensics specialists should be effective during preparation stage of cases, and interinstitutional correspondences should be made on secure networks.

1. GİRİŞ

Suç kavramı, insanoğlunun varoluşundan beri hayatın içinde olan bir olgudur. Temelde toplumsal reaksiyonun bir ürünü olan suç hakkında birçok tanımlama yapılmaktadır. Bunlardan birinde suç, bir grubun reddettiği ve cezalandırdığı anti-sosyal davranış olarak ifade edilmektedir (Sharma, 1998). Başka bir tanım "kanuna karşı gelen ve cezalandırılan insan davranışı" şeklindedir (Rosa, 2003). Diğer bir tanımlama ise suçun ceza hukukuna göre yasaklanan, kovuşturma açılan ve cezalandırılan fiiller anlamına geldiğini belirtmektedir (Henry ve Lanier, 2001).

Tarih boyunca meydana gelen teknolojik gelişmelerin toplumsal hayata olumlu-olumsuz yansımaları olmuştur ve olmaya da devam etmektedir. Bu olumsuz durumlar arasında yeni nesil teknolojik sistemlerin ve aygıtların suç unsuru olmaya açık olması da bulunmaktadır. Failler, teknolojiyi kötü niyetlerini gerçekleştirmek için kullanmışlardır. Bu kişilerin kendi dönemlerinin teknolojileri olan okları, kılıçları, bıçakları, arabaları amaçlarına ulaşmak için birer araç olarak kullandıkları görülmüştür (Brown 1989, akt. Say 2006).

20. yy'da bilgisayar, internet ve cep telefonu teknolojilerinin iletişim, eğitim, bankacılık vb. alanlarda kullanılmasının insan yaşamına pozitif etkisi olmuştur. Uzaktan eğitim, mobil eğitim ile zaman ve mekân kavramı olmadan eğitim verilir hale gelmiştir. İnternet daha hızlı iletişim imkânı sağlamış ve bilgiye daha çabuk ulaşabilme platformu haline gelmiştir. Bununla birlikte insanlar mağazalara gitmeden internet ortamında kurulan sanal mağazalarda alışverişlerini yapar duruma gelmişlerdir.

Teknolojik çağa en çabuk adapte olan sektörlerden biri olan bankacılık, zamanın gelişmelerinden faydalanarak müşterilerine daha iyi hizmet sunmaya çalışmıştır. Bu doğrultuda bankalar, şube bankacılığının yanında telefon bankacılığı, ATM (Automatic Teller Machine), ev bankacılığı, online bankacılık vb. alternatif dağıtım kanallarını müşterilerine sunmuştur.

Çağımız teknolojilerinin kötüye kullanılması toplum güvenliğini tehdit edebilmekte ve yaşamın normal seyrini sekteye uğratabilmektedir. Bu gelişmeler, suç alanında çeşitlenmeleri meydana getirmiştir. Eski usul işlenen hırsızlık, dolandırıcılık, hakaret ve kişisel alana tecavüz suçları günümüzde bilgisayar ve/veya internet yoluyla gerçekleşebilmektedir. Bilgisayarın kullanımını engelleme, bilgiye müdahale, internet sayfalarını sabote, yetkisiz erişim ortaya çıkan yeni suç tiplerinden bazılarıdır (Etter, 2002).

Genel adı "bilişim suçu" olarak tanımlanacak suç için, "bilgisayar suçu", "bilişim ihlali", "bilişim suçluluğu", "bilgisayar vasıta kullanılarak işlenen suç", "bilgisayarın kötü niyetli kullanımı" şeklinde farklı tanımlamalar yapılmaktadır. Ayrıca internette yaşanan büyük gelişmeler nedeniyle bu alanda işlenen suçları ifade etmek için "İnternet suçu" veya "siber suç" kavramları da kullanılmaktadır (Durmaz, 2006).

Bu suçlar teknolojiyi kullanmakta olan bütün ülkelerin ortak sorunu haline gelmiştir. Başta Amerika Birleşik Devletleri (ABD) ve Avrupa ülkeleri olmak üzere ülkemizde adli, idari ve hukuki yapılanmaların düzenlenme ihtiyacı hissedilmiştir. Ülkeler bilişim suçlarını kendi şartlarına göre yorumlamış ve tanımlamıştır. Bilişim suçlarının ortak bir sınıflandırması 2001 yılındaki Avrupa Konseyi Siber Suç Sözleşmesi'nde yapılmıştır. Bu sözleşmede siber suçlar;

- Bilgisayar veri sistemlerinin ulaşılabilirliği, bütünlüğü ve gizliğine karşı işlenen suçlar
- Bilgisayar yoluyla suçlar
- İçerik bağlantılı suçlar
- Telif hakları ve bununla bağlantılı hakların ihlaline ilişkili suçlar

şeklinde kategorize edilmiştir.

Finans sektöründeki teknolojik ilerlemeler suça meyilli kişilerin dikkatini çekmiş ve bu kişiler finansal alanlardan haksız maddi kazanç elde etmeye çalışmışlardır. ABD'de bulunan bilgi güvenliği araştırmaları merkezi Ponemon Enstitüsü'nün 2011 yılının Ağustos ayında yayınladığı ve 50 işletme üzerinde gerçekleştirdiği çalışmada, siber suçun işletmelere maliyetinin yılda ortalama 6 milyon dolar olduğu tespit edilmiştir. Bu

değerin, yıla ve şirkete göre 1,5 milyon dolar ile 36 milyon dolar arasında değiştiği tespit edilmiştir. Ayrıca çalışmanın raporunda, söz konusu suçun maliyetinin geçen yıla göre % 56 arttığı bilgisi yer almaktadır.

Son yıllarda dünya çapında internet kullanıcılarının artmasına paralel olarak bankaların online bankacılık hizmetini kullanan müşterilerinin de sayısı artmıştır. Bu durum, kötü niyetli kişilerin ilgisini çekmiş ve onları online bankacılık sistemine karşı yasadışı eylemde bulunmaya ve bunlardan yarar sağlamaya itmiştir. Online bankacılık suçları, Avrupa Konseyi'nin siber suç sınıflandırmasında çoğunlukla bilgisayar yoluyla işlenen suçlar kapsamındaki kanun maddelerini ihlal etmektedir.

Literatürdeki çalışmalar genellikle online bankacılığın kullanımını etkileyen faktörleri tespit etmek için, online bankacılığı kullanan müşterilerin özelliklerini belirlemek için yapılmıştır. Online bankacılık suçlarının adli süreçteki durumunu inceleme amacıyla yapılan bir çalışma bulunmamaktadır. Bu araştırma, bu alandaki çalışmalara yön vermek ve katkı sağlamak amacıyla gerçekleştirilmiştir.

1.1. AMAÇ

Bu çalışmanın amacı, online bankacılık suçları ile ilgili dosyaları

- Suça konu olan Türk Ceza Kanunu (TCK) maddesi
- Suç Yöntemi
- Suç Unsurunda Kullanılan Sistemler
- Mağdur Tarafın Kullandığı Online Bankacılık Sistemi
- Mağdur Profili
- Suçlu Profili
- Suç Delilleri
- Suça Konu Olan Para Miktarı
- Dava Sonuçları
- Dava Süreleri
- Suçun Gerçekleşme Tarihi

maddeleri altında inceleyerek bu suç alanındaki araştırmalara katkı sağlamak ve yön vermektir.

1.2. ÖNEM

Bilişim teknolojilerinin ilerlemesi ve insan hayatına yerleşmesi ile bilişim suçları hem sayı olarak hem de çeşit olarak artmıştır. Literatürde bilişim suçlarından biri olan online bankacılık suçları ile ilgili çalışmaların eksikliği görülmektedir. Bu amaçla, ceza mahkemelerindeki online bankacılık suçlarına ilişkin dava dosyaları; suça konu olan TCK maddesi, mağdur tarafın kullandığı online bankacılık sistemi, mağdur profili, suç yöntemi, suçlu profili, suç delilleri, suça konu olan para miktarı, suçun gerçekleşme tarihi, dava süreleri ve dava sonuçları maddelerine göre incelenerek elde edilen bulgular, sonuçlar ve öneriler ile literatüre katkı sağlanacaktır.

1.3. SINIRLILIKLAR

Çalışma, İstanbul ili sınırlarındaki Bakırköy, Kadıköy, Sultanahmet, Pendik Adliyeleri olmak üzere 4 adliyedeki toplam 21 ceza mahkemesi ve İstanbul Emniyet Müdürlüğü'nde faaliyet gösteren Bilişim Suçları ve Sistemleri Şube Müdürlüğü ile sınırlıdır. Adliyelerde dava dosyaları araştırılırken Ulusal Yargı Sistemi (UYAP) üzerinden; bilişim, bilişim suçları anahtar kelimeleri kullanılarak tarama yapılmıştır. Dava dosyalarına ulaşmak için kimi zaman mahkeme kalemlerindeki suç kayıt defterleri incelenmiş kimi zaman da Bilişim Suçları Savcılığı'na ait arşivlerde inceleme yapılmıştır.

Diğer taraftan, Emniyet Müdürlüğü'ndeki elde edilen dosyalar dava aşamasına gelmedikleri için dava süreleri, dava sonuçları yönünden incelenememiştir. Bu çalışmanın neticesinde elde edilen sonuçlar, online bankacılık suç tipleri için genellenebilir.

2. GENEL KISIMLAR

2.1. TEMEL KAVRAMLAR

2.1.1. Bilişim, Bilişim Suçu, Siber Suç ve Hacker Kavramları

1900'lü yılların ikinci yarısında hayatımıza giren bilişim kelimesi, Fransızca kökenli "İnformatique" kelimesinin Türkçeye enformatik şekline çevrilmesi ile türetilen bir kavramdır (Yenidünya ve Değirmenci, 2003).

Türk Dil Kurumu (TDK) ise Bilişim Terimleri Sözlüğü'nde bilişim kelimesini

> *"İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalı. Disiplinlerarası özellik taşıyan bir öğretim ve hizmet kesimi olan bilişim bilgisayar da içeride olmak üzere, bilişim ve bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsar. Bundan başka her türlü endüstri üretiminin özdevimli olarak düzenlenmesine ilişkin teknikleri kapsayan özdevin alanına giren birçok konu da, geniş anlamda, bilişimin kapsamı içerisinde yer alır."*

şeklinde tanımlamaktadır (TDK, 2012).

Doktrinde bulunan bilişim suçu tanımlarından biri de;

> *"Elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların yasal olmayan şekilde değiştirilmesi, silinmesi veya bu tür kayıtlara girilmesi veya bilgi tecavüzü için hazırlık yapılması"* şeklindedir (Doğan, 1992).

Diğer bir tanım ise;

"Verilerle veya veri işlemle konu bağlantısı olan ve bilişim sistemleriyle ya da bilişim sistemine karşı işlenen suçlar" şeklindedir (Akbulut, 2000).

Bilişim suçları hakkında Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun 1983 yılının Mayıs ayında gerçekleştirdiği toplantıda, "Bilgileri otomatik olarak işleme tutabilen ya da verilerin transferine imkân tanıyan bir sistemde kanun dışı, ahlak dışı veya yetki dışı gerçekleştirilen her türlü davranış" tanımlaması genel bir kabul görmüştür (Özel, 2002).

Siber suç kavramı ise teknoloji, bilgisayar ve internet ile ilişkili olan suçlar olarak ifade edilmektedir (Schell ve Martin, 2004). Diğer bir siber suç tanımı; "internet ortamında ve elektronik ortamda işlenebilen hukuka aykırı eylemler" şeklindedir (Helvacıoğlu, 2004). Siber suç, kurban ve failin farklı şehirlerde ve ülkelerde bulunabileceği sınır tanımaz bir suç olarak da ifade edilmektedir. Ayrıca failin binlerce suçu, hızlı ve çaba sarf etmeden gerçekleştirmesinden dolayı bu suç tipini otomatik suç olarak da nitelendirenler bulunmaktadır (Brenner, 2010).

Klasik suçlarda, suçu gerçekleştiren kişi için kullanılan fail kelimesi bilişim suçları veya siber suçları işleyen kişiler için de kullanılmaktadır. Bu suçları gerçekleştiren kişileri diğer faillerden ayırmak için özel bir tanımlama olan hacker kavramı benimsenmiştir.

TDK; yabancı kökenli hacker kelimesini Türkçe'ye "bilgisayar korsanı" olarak çevirmekte ve bu kavramı

> *"Bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimse"*

şeklinde ifade etmektedir.
Diğer bir tanım; "Bilgisayara yetkisiz olarak giren kişi" şeklindedir (Brenner, 2010). Başka bir tanımda ise; "Bilgisayar konusunda yeteneğe sahip olan bilgisayar ağı hakkında her türlü bilgiyi öğrenmek için bilgisayar ağı güvenliğini kırarak giriş yapan kişi" olarak ifade edilmektedir (Gissel, 2005).

2.1.2. Siber Suçların Sınıflandırılması

Avrupa Konseyi'nin genel kabul gören siber suçları sınıflandırması; bilgisayar sistemlerine ve servislerine yetkisiz erişim, bu servislerin dinlenmesi, bilgisayar sabotajı, bilgisayar yoluyla sahtecilik, kanunla korunmuş bir yazılımın izinsiz kullanımı,

yasadışı yayınlar şeklindedir. Ayrıca ticari sırların çalınması, verilerin suistimali sahte kişilik oluşturma siber suçlar arasına girmektedir (Dokurer, 2011).

Bu çalışmada siber dünya diğer ifadesi ile internet üzerinde gerçekleştirilen suçlar hakkında bilgiler yer almaktadır. Siber suçlar; şiddet içeren ve şiddet içermeyen suçlar şeklinde kategorize edilmektedir.

2.1.2.1. Şiddet İçeren Siber Suçlar

Şiddet içeren siber suçlar; siber terörizm, tehdit yolu ile saldırı ve çocuk pornografisi şeklinde üçe ayrılmaktadır.

Siber terörizm; siber dünyada bilgisayar ağlarını kullanarak terörist faaliyetlerin planlanması veya koordine edilmesidir. Bu suçlarda e-postalar aracılığı ile iletişim kurulmaktadır. Terörist faaliyetlerin planlanması ve gruba yeni üye alımları, hazırlanan web siteleri üzerinden gerçekleşmektedir.

Teröristler, siber terörizmle;

- Kara ulaşımı trafik sistemini bozma
- Hava ulaşım sistemlerini bozma, uçakların çarpışmasına sebep olma
- Telefon sistemlerini felç etme
- Bilgisayar sistemlerini karmakarışık hale getirme
- Bankacılık ve finans sektörünü ait sistemleri çökertme
- Hastanelerin veri tabanlarında değişiklik yapma
- Devlet kurumlarının sistemlerini çökertme

fiillerini gerçekleştirmektedir (Shinder, 2002).

Tehdit yoluyla saldırı ise; bir kişiyi veya kişinin sevdiği insanları bilişim sistemlerini kullanarak tehdit etme faaliyetleridir. Bu suçlar e-posta, video ve telefon yoluyla işlenebilmektedir. Bu saldırılar, bir şirkete veya devlet kurumuna da düzenlenebilir (Roddel, 2008). Bu saldırılara paralel olarak internet üzerinden hakaret ve taciz fiilleri yapılmaktadır. Bu suçlar, günümüzde milyarlarca kullanıcıya sahip sosyal medya platformlarından Facebook ve Twitter'da sıkça görülmektedir.

Şiddet içeren suçlardan olan çocuk pornografisi; küçük çocukları kullanarak pornografik materyal oluşturan, bu materyallerin dağıtımını yapan ve bu materyalleri

izleyenleri kapsamaktadır. Bu faaliyetler, bilgisayar ve bilgisayar ağı kullanıldığı takdirde siber suç kapsamına girmektedir (Cross, 2008).

2.1.2.2. Şiddet İçermeyen Siber Suçlar

Şiddet içermeyen suçlar; Siber ihlal, siber dolandırıcılık ve siber hırsızlık şeklinde üç gruba ayrılmaktadır. Siber ihlal (Cyber Trespass); bilgisayara ve bilgisayar sistemine yapılan yetkisiz giriş saldırıları olarak tanımlanmaktadır. Fakat bu saldırılar verilerin zarar görmesi veya kötüye kullanılması amacıyla yapılmamaktadır. Genç bir bilgisayar korsanının kendisini kanıtlamak için bilgisayar ağlarına yetkisiz giriş yapması neticesinde kişisel e-postaları okuması veya bilgisayar sistemindeki hareketleri izlemesi bu suç tipine örnek olarak gösterilebilir (Shinder ve Tittel, 2002).

Siber dolandırıcılık (Cyber Fraud) ise son yıllarda internetin hızlı bir şekilde gelişmesi dolandırıcılık faaliyetlerinin online olarak gerçekleşmesine olanak tanımaktadır. Suçlular, internet teknolojilerine hızlı bir şekilde uyum sağlayarak geleneksel sahtekârlık yöntemlerini bu yollarla gerçekleştirmektedir (Miller ve Cross, 2012). Her geçen yıl da internet üzerinden yapılan dolandırıcılık faaliyetleri artmaktadır. Bu kategoride karşılaşılan suçlar; Açık Arttırma Dolandırıcılığı, Yatırım Dolandırıcılığı, Ön Ödeme Dolandırıcılığı (419 Dolandırıcılığı) ve Oltalama (Phishing)'dır.

Açık arttırma dolandırıcılığı; sık karşılaşılan internet dolandırıcılığı çeşitlerinden biridir ve E-Bay benzeri açık arttırma ile satış yapan web sitelerinde görülebilmektedir. Satıcı tarafından işlenen bu suç;

- Sahip olmadığı bir ürünü veya hizmetin satışını yapma
- Alıcıya geri ödemeyi zamanında yapmama
- Yanlış, eksik ürün veya hizmet satmaya çalışma

şeklinde olabilmektedir (Miller ve Cross, 2012).

Yatırım dolandırıcılığında; kötü amaçlı kişiler, sahte şirket web sitesi kurarak veya istenmeyen e-posta (spam) göndererek bilgisayar kullanıcılarına yatırım fırsatı sunmaktadır. Bu hileye aldanan kişiler yatırım için istenen parayı gönderdikten sonra dolandırılıcılar izlerini kaybettirerek ortadan kaybolmaktadır (Gerber ve Jensen, 2007).

The Silver Lake adlı yayınevinin editörleri (2006), Nijerya'da ortaya çıkan "ön ödeme dolandırıcılığı" diğer adı ile "419 dolandırıcılığı" isminin ülkenin ceza kanununda ilgili suç kodu numarasından geldiğini belirtmektedir. Bu dolandırıcılık yönteminde; kötü niyetli kimse kendini devlet görevlisi, doktor, avukat, din görevlisi, asker veya bu kişilerin çocukları olarak tanıtmakta böylece hedefteki kişilerin güvenini kazanmaya çalışmaktadır. Ayrıca bu kişiler, gönderdikleri e-postalarda resmi makam/kurum adresi kullanmakta ve e-postaya eklenen dokümanlarda sahte mühür, pul, logo kullanarak bilgisayar kullanıcılarını aldatmaya çalışmaktadır. E-posta içeriğinde ise hükümet sorunları, kişisel para ortaklığı gibi sahte senaryolardan yararlanılmaktadır. Bu durumda yapılacak tek şey; e-postalara geri dönüş yapmamaktadır.

Son yılların en yaygın siber dolandırıcılık yöntemi olan Oltalama (Phishing) kavramı, insanlardan kişisel ve finansal bilgilerini isteyen aldatıcı e-postaları tanımlamak için kullanılmaktadır. Söz konusu e-postaların; herhangi bir kurum, şirket veya bankadan geldiği süsü verilmektedir. Bu dolandırıcılıkta amaç; kişilerin kredi kartı bilgilerini, kullanıcı adını, şifrelerini, banka hesap bilgilerini ele geçirmektir (Ogunjobi, 2008). Bu dolandırıcılık tipi hakkında ayrıntılı bilgi, çalışmanın "Kişisel Bilgi Hırsızlığı Yöntemleri" bölümünde yer almaktadır.

Jentz ve Miller (2009), şiddet içermeyen suçların bir diğer çeşidi olan Siber Hırsızlığı (Cyber Theft); finansal ve kimlik hırsızlığı diye ikiye ayırmaktadır. Finansal hırsızlıkta; bilgisayar ağları şirket/kurum çalışanlarının büyük miktarda para kayıplarını kapsayan suçlar işlemesine imkân tanımaktadır. Bir şirketin muhasebe bölümünde çalışan birinin hesaplar arası para transferi yapması bu hırsızlığa örnek olarak gösterilebilir. Bilgisayar sistemleri üzerinden gerçekleştirilen işlemler firmaları; sabotaj, dolandırıcılık, zimmete geçirme, kişisel bilgilerin çalınması gibi durumlara karşı savunmasız bırakmıştır.

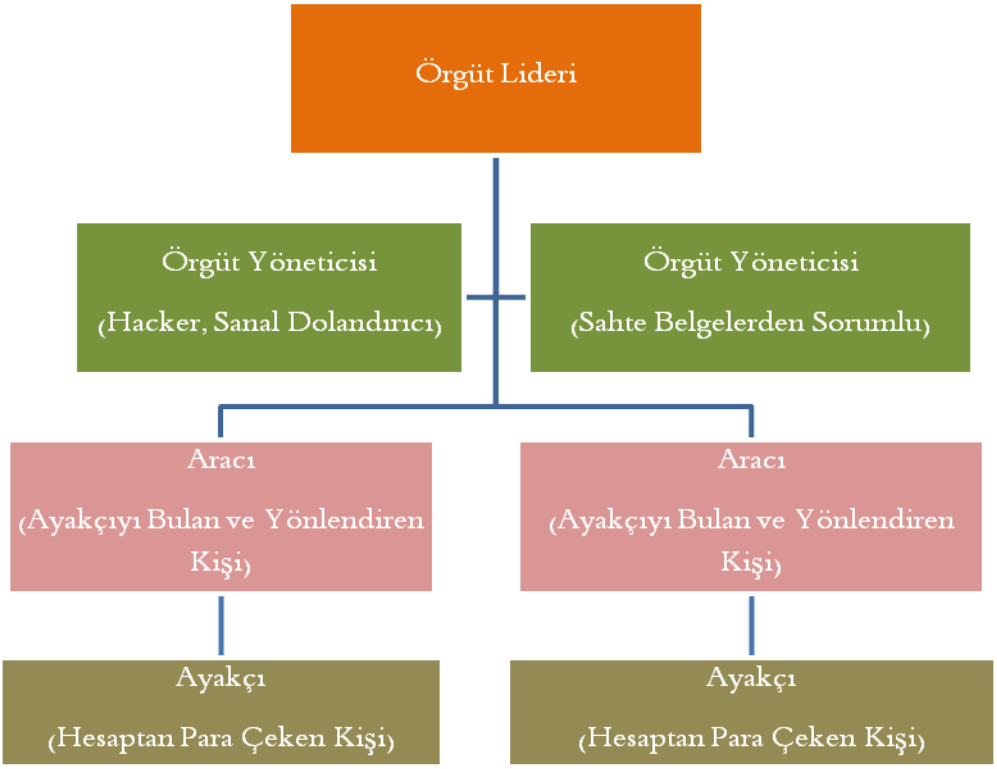
Kimlik hırsızlığında ise hırsızlar; hedefteki kişilerin finansal hesaplarına girmek için gerekli tüm bilgileri çalmaktadır. Bu suç, internetin yaygınlaşmasından önce de vardı. Hırsızlar, banka hesap numaralarını veya kredi kart numaralarını bulmak için kişileri izliyor veya onların çöp kutularını karıştırıyordu.

2.1.3. Online Bankacılık Suçları Çete Yapısı

İnternet üzerinden gerçekleşen, aralarında online bankacılık suçlarının da bulunduğu dolandırıcılık faaliyetlerini gerçekleştirmek için çeteler kurulmaktadır. Bu doğrultuda, Türkiye Bankalar Birliği (TBB) İnternet Bankacılığı Bilinçlendirme Çalışma Grubu'nun yaptığı araştırmanın Nisan 2007 tarihli raporunda internet üzerinden yapılan dolandırıcılık faaliyetleri hakkında bilgi verilmektedir. Çetede; Lider, Hacker (Yönetici), Sahte Belge Sorumlusu (Yönetici), Aracı (Üye) ve Ayakçı rolleri bulunmaktadır.

Ayakçı, banka şubelerine veya ATM'lere internet dolandırıcılığı vasıtası ile gönderilen miktarları almaya gelen kişilere denir. Çete yöneticileri, ayakçı vasfındaki kişiler için genellikle eğitim düzeyi düşük, işsiz ve sabıkası olmayan şahısları tercih etmektedir. Bu kişileri bulan ve banka şubesine veya ATM'lere getirenler ise "Aracı" olarak tanımlanmaktadır. Ayakçılar birkaç eylemde kullanılmaktadır. Sahte belge temininden sorumlu kişiler tarafından hazırlanan belgeler ile açılan banka hesaplarındaki parayı çeken ayakçılar söz konusu paranın cüzi bir kısmını almaktadır.

Elde edilen paranın dağılımı; örgüt lideri % 50 ila % 70 arası, hacker % 20 ila % 30 arası, sahte belge sorumlusu 50 – 100 TL, aracılar % 10 ila % 20 arası, ayakçılar 50 - 100 TL şeklindedir. Şekil 2.1'de online bankacılık suçları çete yapısının organizasyon şeması yer almaktadır.



Şekil 2.1: Online Bankacılık Suçları Çete Yapısı

2.2. TCK'DAKİ BİLİŞİM SUÇLARI MADDELERİ

Bilişim suçlarına, 26.09.2004 tarihinde kabul edilen ve 12.10.2004 tarihinde Resmi Gazete'de yayınlanan 5237 sayılı TCK'nın "Özel Hükümler" başlığı altındaki ikinci kitabının üçüncü kısmını teşkil eden "Topluma Karşı Suçlar"ın onuncu bölümünde "Bilişim Alanında Suçlar" kısmında yer verilmektedir.

Bu kısım; 243. madde "Bilişim sistemine girme", 244. madde "Sistemi engelleme, bozma, verileri yok etme veya değiştirme", 245. madde "Banka veya kredi kartlarının kötüye kullanılması" ve 246. madde "Tüzel kişiler hakkında güvenlik tedbiri uygulanması" konu başlıkları ile toplam 4 maddeden oluşmakta ve bu maddelerde bilişim suçları ile ilgili hükümler bulunmaktadır.

2.2.1. Bilişim Sistemine Girme Suçu

5237 TCK'nın 243. maddesi 3 fıkradan oluşmaktadır. Bu madde bilişim sistemine girme ve kalma suçuna ilişkin hükümleri içermektedir.

Maddenin birinci fıkrası;

> *"Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir"*

şeklindedir (Adalet Bakanlığı, 2012).

Söz konusu fıkranın en önemli hukuki faydası bilişim sistemlerinin güvenliğinin korunmasıdır. Ayrıca bu fıkranın verilerin gizliliğinin korunmasına, özel hayatın dokunulmazlığına, kişi ve kurumların güvenlik duygusuna yönelik yararları bulunmaktadır (Dülger, 2004).

Diğer taraftan yasa koyucu, yetkisiz erişim ile sistemde kalmaya devam etme fiillerinin beraber olma şartının bu maddenin hukuki yararlarını etkileyeceğine inanmamaktadır. Fakat *"Bilişim güvenliği korunmak istenseydi suç için gerekli olan kalmaya devam etme şartına yer verilmemesi gerekliliği"* düşüncesine sahiptir. Bu şartlarda temelde korunan hukuki yarar; bilişim sistemini kullanan bireylerin belli bir zamandan sonra rahatsız edilmemesidir (Karagülmez, 2009).

Bu maddenin ikinci fıkrası ise;

> *"Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir"* ve son fıkrası ise; *"Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur"*

şeklinde belirtilmiştir (Adalet Bakanlığı, 2012).

2.2.2. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu

TCK'nın 244. maddesi 4 fıkradan oluşmaktadır. Bu madde, bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçuna ilişkin hükümleri içermektedir.
Maddeye ilişkin fıkralar;

1. *"Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır*

2. *Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.*
3. *Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.*
4. *Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur"*

şeklinde ifade edilmiştir (Adalet Bakanlığı, 2012).

Birinci fıkradaki bilişim sistemlerinin işleyişini engelleme veya bozma suçuna yaptırım uygulanması, bilişim sistemlerinin çalışmasına yönelik hareketlerin engellenmesi amacını taşımaktadır. Ayrıca ilk iki fıkra, Avrupa Konseyi Siber Suç Sözleşmesi'nin 4. ve 5. maddesi ile paralellik göstermektedir. Bu sözleşmede yer alan 4. madde ile bilgisayar sistemindeki verilere veya programlara verilecek zararı engelleyerek bunların düzgün ve sağlıklı bir şekilde çalışmasına imkân tanınmaktadır. 5. maddede ise bilgisayar sistemlerinin verimli çalışması amacıyla sistem kullanıcılarının ve operatörlerinin kullanım hakları korunmaya çalışılmaktadır (Karagülmez, 2009).

Söz konusu maddenin üçüncü fıkrasında suçun ağırlaştırıcı nedeni düzenlenmiştir. Buna göre; bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçunun bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde verilecek ceza arttırılacaktır. Tüm kamu kurum veya kuruluşlarına ait bilişim sistemleri üç numaralı fıkra kapsamında değerlendirilebilecektir. Buna ek olarak, banka veya kredi kurumu niteliği olan özel kurum veya şirketler bu fıkra kapsamında değerlendirilecektir (Yılmaz, 2011).

Dördüncü fıkrada ise "bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu" düzenlenmiştir. Ayrıca bu suç tipinin düzenlenmesi, ilgili maddenin birinci ve ikinci fıkralarına atıf yapılarak gerçekleşmiştir. Bu fıkrada geçen söz konusu suçun "başka bir suç oluşturmaması halinde" söz öbeği kullanılarak aynı eylemlerin gerçekleştirilerek

hukuka aykırı yarar elde edilmesi ancak bunun bir başka suç tipinde düzenlenmiş olması halinde bu suç tipinin uygulanmayacağı belirtilmektedir. Bu kısmın iyi anlaşılması için yasa koyucu *"Bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması halinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir."* açıklamasını yasanın gerekçesinde belirtme ihtiyacı duymuştur (Dülger, 2011).

2.2.3. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu

TCK'nın 245. maddesi 5 fıkradan oluşmaktadır. Bu maddede banka veya kredi kartlarını kötüye kullanma suçuna ilişkin hükümler yer almaktadır.

Söz konusu maddede yer alan fıkralar;

1. *"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 adlî para cezası ile cezalandırılır.*
2. *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 adlî para cezası ile cezalandırılır.*
3. *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, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.*
4. *Birinci fıkrada yer alan suçun;*
   - *Haklarında ayrılık kararı verilmemiş eşlerden birinin,*
   - *Üstsoy veya altsoyunun veya bu derecede kayın (yakın olmasın) hısımlarından birinin veya evlat edinen veya evlâtlığın,*
   - *Aynı konutta beraber yaşayan kardeşlerden birinin,*

   Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

5. *(Ek fıkra: 06/12/2006 - 5560 S.K.11.md) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır"* şeklindedir (Adalet Bakanlığı, 2012).

245. madde ile söz konusu kartların haksız, hukuka aykırı olarak kullanılması yoluyla bankaların ve kart sahiplerinin zarara sokulması ve bu suretle hukuka aykırı yarar sağlanması önlenmek istenmektedir. Bu durum, maddenin gerekçesinde de açık bir şekilde ifade edilmektedir (Değirmenci, 2002; akt: Dülger 2004)

245. maddeye bir bütün olarak bakıldığında; üç farklı fiil cezalandırılmaktadır. Bu fiillerden ilki, birinci alt maddeye göre; başkasına ait banka veya kredi kartını bir şekilde ele geçiren ya da elinde bulunduran kişinin kart sahibinin rızası olmadan kullanması ya da üçüncü kişilere kullandırması ve bu yolla failin kendisine ya da üçüncü kişilere hukuka aykırı yarar sağlamasıdır. İkinci alt maddede; başkalarına ait banka hesaplarıyla ilişkilendirerek sahte banka veya kredi kartı türetilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi fiili düzenlenmektedir. Üçüncü alt maddesinde ise sahte olarak türetilen veya üzerinde işlem gerçekleştirilerek sahte hale getirilen bir banka kartı veya kredi kartının kullanılması ile kendisine veya üçüncü bir kişiye hukuka aykırı yarar elde etmesi fiili dikkate alınmaktadır (Güngör, 2007).

Fakat maddenin kapsayıcılığı hakkında Taşkın (2008); ilgili maddenin "banka veya kredi kartları" ifadesi ile teknolojik gelişmeler karşısında sınırlı ve yetersiz olduğu görüşünü savunmaktadır. Bu yüzden, doktrinde de yer yer belirtildiği gibi söz konusu maddenin başlığının "Nakit olmayan ödeme aracı" gibi daha kapsamlı kavrama göre yeniden düzenlenmesi gerektiği fikrine sahiptir.

2.2.4. Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması İle İlgili Madde

246. madde tek fıkradan oluşmaktadır. Bu maddede; 243. , 244. ve 245. maddelerde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlayan tüzel kişiler hakkında kendilerine özgü güvenlik tedbirlerine hükmolunacağı ifade edilmektedir (Adalet Bakanlığı, 2012).

2.2.5. TCK'da Yer Alan Bilişim Sistemleri Aracılığıyla İşlenen Suçlar İle İlişkili Maddeler

Bu başlık altında, 5237 sayılı TCK'nın "Özel Hükümler" başlığı altındaki ikinci kitabının ikinci kısmını teşkil eden "Kişilere Karşı Suçlar"ın onuncu bölümünde "Malvarlığına Karşı Suçlar" kısmında bulunan; 142/2-e maddedeki "Bilişim sistemlerinin kullanılması suretiyle hırsızlık" suçu ile 158/1-f maddedeki "Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık" suçu açıklanmaktadır.

2.2.5.1. Bilişim Sisteminin Kullanılması Suretiyle Hırsızlık Suçu

TCK'nın 141. maddesinde hırsızlık; "zilyedinin diğer ifadesi ile malı kullanmakta olan kimsenin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alma eylemi" olarak tanımlanmaktadır. Bu suçu işleyen kimseye ise bir yıldan üç yıla kadar hapis cezası verileceği belirtilmektedir. Buna ek olarak, hırsızlık suçunun nitelikli bir şekilde işlenme durumları 142. maddede açıklamaktadır. Bu suçun nitelikli hallerinden biri olan "Bilişim sistemlerinin kullanılması suretiyle hırsızlık" söz konusu maddenin 2. fıkrasının "e" bendinde yer almaktadır. 142/2-e'ye göre hırsızlık suçunun bilişim sistemleri kullanılması yoluyla gerçekleşmesi halinde eylemi gerçekleştiren kişiye üç yıldan yedi yıla kadar hapis cezasını verileceği ifade edilmektedir (Adalet Bakanlığı, 2012).

Bu maddede geçen bilişim sistemi ifadesi ile "verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler" kastedilmektedir. Örnek olarak; bir kimsenin başkasına ait mevduat hesabından kendi mevduat hesabına bilişim sistemlerini yoluyla para transferi yaptığı takdirde TCK'nın 142/2-e bendi uygulanacaktır (Ülkü, 2005).

2.2.5.2. Bilişim Sisteminin Kullanılması Yoluyla İşlenen Dolandırıcılık Suçu

TCK'nın 157. maddesinde dolandırıcılık; "hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlama eylemi" olarak tanımlanmaktadır. Bu suçu işleyen kimseye ise bir yıldan beş yıla kadar hapis ve beş bin güne kadar adlî para cezası verileceği belirtilmektedir.

TCK'nın 158. maddesinin 1. fıkrası dolandırıcılık eyleminin nitelikli bir şekilde gerçekleşme durumlarında verilecek hükümleri içermektedir. İlgili fıkranın f bendinde bahsi geçen nitelikli dolandırıcılık eyleminin "bilişim sistemlerini, banka veya kredi kurumlarını araç olarak kullanarak işlenmesi" belirtilmekte ve suçu bu şekilde gerçekleştiren kişi veya kişilerin iki yıldan yedi yıla kadar hapis ve beş bin güne kadar adlî para cezasına çarptırılacağı ifade edilmektedir (Adalet Bakanlığı, 2012).

157. maddede verilen ceza ile 158. maddede verilen ceza karşılaştırıldığında dolandırıcılık suçunun nitelikli bir yolla gerçekleştirilmesinde ceza artırımına gidildiği görülmektedir.

Dülger (2011), dolandırıcılığın bu nitelikli hali için bilişim sistemlerinin ve bilişim sistemi aracılığıyla gerçekleştirilen dolandırıcılık eylemlerinin kendine özgü yönleri dikkate alınmadan düzenlendiğine dikkat çekmektedir. Ayrıca, bu maddede "bilişim sistemleri üzerinde gerçekleştirilen hileli işlemler sonucu hukuka aykırı yarar sağlanması eylemleri"nin düzenlenmediğini, buna karşın dolandırıcılıkta bilişim sisteminin basit bir araç olarak öngörülmesinin düzenlendiğini belirtmektedir. Sonuç olarak Dülger (2011), bu suç tipi için buradan bağımsız bir düzenleme yapılması gerektiği düşüncesine sahiptir.

2.2.6. TCK'da Yer Alan ve Bilişim Sistemleri ile İşlenebilecek Diğer Suç Maddeleri

TCK'daki "Bilişim Alanında Suçlar" bölümündeki 243., 244., 245. ve 246. maddelerde suçların işlenmesinde bilişim sisteminin varlığı şartı aranmaktadır. Bilişim sistemi, bu tip suçların "olmazsa olmaz"ı konumundadır. Bu kısımda belirtilmekte olan suç tiplerinin ortak özelliği TCK'da düzenlenmiş olan geleneksel suç tiplerinin bilişim sistemleri yoluyla işlenmiş olmalarıdır. Bu suçların bilişim sistemlerinin "araç" olarak kullanılması ile işlenmesi neticesinde cezalar çoğu kez ağırlaştırılarak hükmolunmaktadır (Taşkın, 2008).

TCK'da bilişim anahtar kelimesi kullanılarak açıklanan suçlar ve hükümler haricinde bilişim sistemleri kullanılarak işlenebilecek suçlar bulunmaktadır.
Bu suçlar;

- 124. madde "Haberleşmenin Engellenmesi Suçu"

- 125. madde “Hakaret Suçu”
- 132. madde “Haberleşmenin Gizliliğini İhlal Suçu”
- 135. madde “Kişisel Verilerin Kaydedilmesi”
- 136. madde “Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu”
- 138. madde “Verileri Yok Etmeme Suçu”
- 226. madde “Müstehcenlik Suçu”
- 228. madde “Kumar Oynanması İçin Yer ve İmkân Sağlanması Suçu”

şeklindedir (Adalet Bakanlığı, 2012).

Bu tip suçlar arasına giren 142/2-e maddesindeki “Bilişim sistemlerinin kullanılması suretiyle hırsızlık” suçu ile 158/1-f maddesindeki “Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık” suçu online bankacılık suçlarında ihlal edilen suç maddeleri olduğu için ayrıntılı olarak açıklanmıştır.

2.3. ONLİNE BANKACILIK

Bu kısımda; online bankacılık kavramı, online bankacılıkta gerçekleştirilebilen işlemler, online bankacılığın tarihsel gelişimi, online bankacılıkta güvenlik önlemleri ve online bankacılıkta tarafların sorumlulukları başlıkları altında bilgiler yer almaktadır.

2.3.1. Online Bankacılık Kavramı

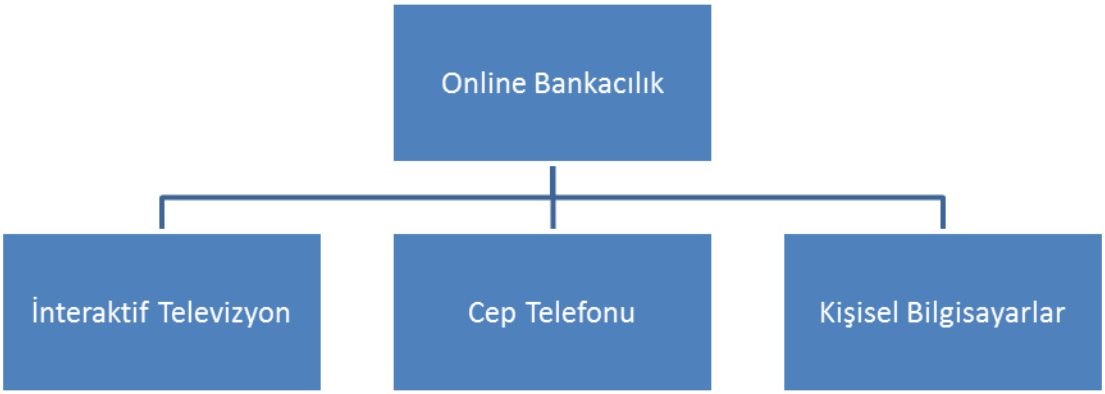
Teknolojinin bankacılık sektöründeki ilk uygulamaları sırasında, bankacılık işlemlerinin eş zamanlı gerçekleştirebilecek yollarının çoğu, online bankacılık kavramı altında tanımlanmaktaydı.

Bu doğrultudaki bir görüşe göre bankacılık işlemlerinin online olarak gerçekleşmesinin üç farklı yolu bulunmaktadır. Bu yollardan ilki olan internet tabanlı bankacılıkta; modem yolu ile internete bağlanıp “Internet Explorer” veya “Netscape Navigator” gibi web tarayıcıları üzerinden, bankanın resmi web sitesi vasıtası ile banka hesaplarına giriş yapılarak, işlemler gerçekleştirilmektedir. İkinci yol ise; bankaların, müşterilerinin kişisel bilgisayarlarına yüklenmesi yoluyla kullanılan yazılımlar sağlaması yoludur. Müşteriler, bu yazılım ile güvenli ağ üzerinden banka bilgisayarlarına

bağlanabilmektedir. Bankacılık işlemlerini online gerçekleştirmenin üçüncü yolu ise; kişisel finans yazılımı destekli yapılan bankacılıktır. Bu yöntemde, "Quiken" veya "Microsoft Money" gibi yazılımlar, finans bilgilerini banka ile değiştirmesine izin vermektedir. Yazılım, internet tabanlı kurulum yolu ile banka bilgisayarlarına bağlanmakta ve finans bilgilerini kişisel hesaptan indirmektedir. Çoğu banka sistemlerini bu duruma uyumlu hale getirmek için, birçok yazılım firması ile ortaklık yapmaktadır (SCN Education, 2001).

Bankacılık hizmetlerinde çok çeşitli ve ileri teknolojilerin kullanılması neticesinde, günümüzde çoğu zaman internet üzerinden yapılan bankacılık işlemleri için, internet bankacılığı ve online bankacılık terimleri kullanılmaktadır. Bu çalışma için "Online Bankacılık" terimi tercih edilmiştir.

Online bankacılık, kişisel bilgisayarla veya internete giriş yapılabilen diğer aygıtlarla interneti kullanarak elektronik bankacılık hizmetlerinin sağlanması olarak tanımlanmaktadır. Şekil 2.3'de, online bankacılık sistemlerine giriş için kullanılabilecek aygıtlar gösterilmektedir (Gkoutzinis, 2006).



Şekil 2.3: Online Bankacılık Sistemine Giriş İçin Kullanılabilecek Aygıtlar

Müşteriler, internet ortamındaki sanal bankalara, herhangi bir finansal yazılıma gerek olmaksızın bankalarının kendilerine verdikleri şifre veya şifreleri kullanıp sisteme giriş yaparak bankacılık işlemlerini gerçekleştirebilirler (Chou ve Chou, 2000).

Basel Bankacılık Heyeti (2005), online bankacılığı, elektronik kanallar aracılığıyla bireysel ve küçük değerdeki bankacılık ürün ve hizmetlerinin sağlanması olarak tanımlamaktadır. Bu ürün ve hizmetler; mevduat alma, borç verme, hesap yönetimi, finansal danışmanlık sağlanma, elektronik fatura ödeme ve elektronik para gibi, diğer elektronik ödeme ürünlerinin ve hizmetlerinin sağlanmasını içermektedir.

Jahankhani, Watson ve Me (2009), online bankacılığı, uygulamada; bilgilendirme, iletişim ve işlem amaçlı olmak üzere üçe ayırmaktadır.

- *Bilgilendirme Amaçlı Bankacılık:* Diğerlerine nispeten daha az risk içeren temel düzeyde bir online bankacılık seviyesidir. Bankanın amacı, sadece ürünlerini ve hizmetlerini pazarlamaktır. Bağımsız sunucuya sahip olan bu sistemlerde, sunucu ile bankanın yerel ağı arasında herhangi bir yol bulunmamaktadır.

- *İletişim Amaçlı Bankacılık:* Banka, müşterilerine bankanın sistemi ile etkileşime geçerek, posta yollama ve borç başvurusu gibi kısıtlı işlemleri gerçekleştirme izni vermektedir. İletişim amaçlı yapılan online bankacılık, bilgi amaçlı online bankacılık ile karşılaştırıldığında biraz daha fazla risk içermektedir. Bunun sebebi ise; sunucu ile bankanın yerel ağı arasında bir bağlantı olma ihtimalidir. Bu seviyedeki online bankacılıkta, dışarıdan gelebilecek virüs saldırılarına karşı verilerin güvenliğini sağlamak için, bilgisayar ağını izleme ve yetkisiz girişlerin kontrolü gibi işlemlerin yapılması gerekmektedir.

- *İşlem Amaçlı Bankacılık:* Modern bankacılık tipi olan işlemsel bankacılık, banka müşterilerine, finansal işlemlerini online gerçekleştirme imkanı sunmaktadır. Bu bankacılık tipi, sunucu ile banka yerel ağı arasındaki bağlantı nedeni ile yüksek güvenlik riski içermektedir. Müşteriler bakiye kontrolü, fatura ödemesi, hesaplar arası para transferi gibi farklı türden işlemleri bu yöntemle yapabilmektedirler.

2.3.2. Online Bankacılıkta Gerçekleştirilebilen İşlemler

Bankacılık işlemlerinin internet üzerinden yapılmasına dayalı olan online bankacılık, hem bankalara hem de müşterilere birçok avantaj sağlamaktadır. Bu hizmet sayesinde bankalar, müşterilerin şubeye gelmesine gerek kalmadan işlemlerini yapabilmelerine

olanak sağlamaktadır. Böylece bankalar, daha fazla müşteriye daha az maliyet ile hizmet verebilmektedir. Online bankacılık, zamandan bağımsız olduğu için, banka müşterileri günün her saatinde işlemlerini gerçekleştirmektedir. Diğer taraftan repo veya hisse senedi alım satımı, Elektronik Fon Transferi (Electronic Fund Transfer, EFT) vb. işlemlerde, belirli gün ve saat kısıtlaması bulunmaktadır.

Odabaşı (2006), işlem amaçlı online bankacılık kapsamına giren faaliyetleri;

- Vadeli hesap, vadesiz hesap, yatırım hesabı vb. hesap işlemleri,
- İsme veya hesaba havale, EFT gerçekleştirme, EFT ve havale talimatı verme, otomatik ödeme talimatı verme, vb. para transfer işlemleri,
- Repo, A ve B tip yatırım fonu; alım satımı ve alım satım talimatı verme, halka arz işlemleri, döviz alım satımı vb. yatırım işlemleri,
- Fatura ödemeleri, üniversite harç ödemeleri, motorlu taşıt vergisi ödemeleri, Trafik cezası ödemeleri vb. ödeme işlemleri,
- Kredi kartı borç ödemesi, kredi kartı hesap bilgilerini görüntüleme, sanal kart işlemleri vb. kredi kartı işlemleri ile bireysel kredi kartı başvuru işlemleri,
- Bakiye ve hesap hareketleri, hesaplarla ilgili tüm bilgiler, repo sorgulama, kredi kartı borcu ve ekstre bilgileri, çek-senet bilgileri vb. bilgi alınan işlemler,
- Günlük altın-döviz fiyatları, günlük repo ve faiz oranları, günlük yatırım fonu fiyatları vb. tüm genel bilgi işlemleri,
- Uçak, otobüs vb. bileti alma, kitap siparişi verme vb. işlemler,

şeklinde sıralamaktadır.

2.3.3. Online Bankacılığın Tarihsel Gelişimi

Bankalar, teknolojinin ve teknolojik devrimin ilk kullanıcıları olarak kabul edilmektedir. Bankaların bilgisayar çağındaki ilk uygulamaları, büyük bilgisayarlar ve mini bilgisayarlardır. Müşteri hesap bilgileri, banka dökümleri, kişisel kayıtlar ve hesap paketleri gibi veri girişleri, bilgisayar sisteminde elektronik tablolara dönüştürülmüştür. Bankacılık sektöründe teknolojinin kullanımı, işlerin daha hızlı ve rahat bir şekilde yapılmasını sağlamıştır. Teknolojik ilerlemeler ile birlikte, doğrudan müşteri hizmetleri fikri, bankalara cazip gelmeye başlamıştır (Kondabagil, 2007).

Gup (2003), bu fikrin yansıması olan elektronik bankacılık terimini; bankacılık hareketlerinin elektroniğin kullanımı yardımı ile gerçekleştirilmesi şeklinde tanımlamaktadır. Daniel (1999) ise elektronik bankacılığı, bankaların hizmetlerini, müşterilerine televizyon veya bilgisayar aracılığı ile sağlaması olarak belirtmektedir. Bu tanımlardan yola çıkarak elektronik bankacılığı; bankacılık hizmetlerinin elektronik aygıtlar vasıtası ile gerçekleştirilmesi şeklinde ifade edebiliriz.

1951 yılında, New York şehrindeki Franklin National Bank tarafından kullanılan ilk kredi kartı ve 1970' li yılların başında, City of National Bank of Colombus'un ATM'yi kullanması, elektronik bankacılığın gözle görülür ilk uygulamaları olarak kabul edilmektedir.

Elektronik Bankacılık, bilişim dünyasındaki gelişmelere adapte olarak gelişmiş ve doğrudan müşteri hizmetlerinin çeşitleri artış göstermiştir. Banka ve kredi kartlarının Elektronik Satış Noktası (Electronic Point of Sale, EPOS) cihazı ile ticari yerlerde kullanımı, bu gelişmenin ikinci yüzü olmuştur. Daha sonraları iletişim alanındaki ilerlemelerle birlikte, telefon bankacılığı, ev-ofis bankacılığı, son olarak da mobil bankacılık ve online bankacılık kavramları elektronik bankacılığa yön vermiştir (Kondabagil, 2007).

İnternet üzerinden bankacılık işlemlerinin gerçekleşmesi 1995 yılına dayanmaktadır. Online bankacılık için kurulan "Security First Network Bank", sadece internet üzerinden yapılacak bankacılığın maliyetini düşüreceği düşüncesi ile kurulmuş fakat hedeflenen olmamış ve bu çaba kısa sürmüştür. (Sarel ve Marmorstein, 2003).

Jenkins (2007), online bankacılığın, cep telefonu, internet vb. iletişim teknolojilerinin gelişimi ile birlikte, elektronik bankacılığın alternatiflerinden biri olarak, Amerika Birleşik Devletleri, Avrupa ülkeleri ve Avustralya gibi gelişmiş ülkelerde yaygınlaştığını belirtmektedir. Cartwright (2000)'a göre online bankacılık düşüncesi, 1980'lerdeki telefon bankacılığı ile başlamış ve internetin evlerde kullanılması ile yaygınlaşmıştır.

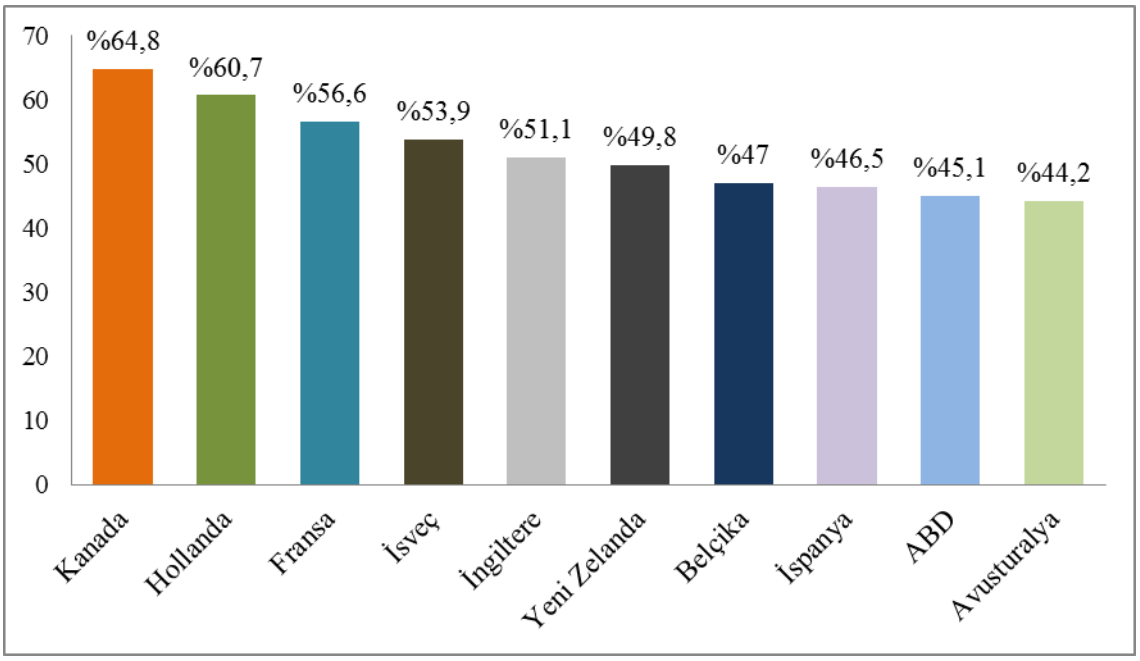
3.3.3.1. ABD'de ve Avrupa'da Online Bankacılık

Online bankacılık, bankacılık sektöründeki elektronik bankacılığa geçiş ve bilgi teknolojilerinin hızlı gelişimi ile ABD ve Avrupa ülkeleri gibi gelişmiş ülkelerde hızla benimsenmiş ve yayılmıştır. Bu gelişimin en önemli etkenlerinden biri internete ulaşma kolaylığıdır (Jenkins, 2007).

ABD'de sadece online bankacılık hizmetleri olarak kurulan banka, "Security First Network Bank" ve ilk defa şube bankacılığının yanında "NetBank" adında online bankacılığı kullanan banka ise 1996 yılında "Atlanta İnternet Bank" kuruluşudur. Citibank ve Wells Fargo gibi sektörün önde gelen bankaları, bu hizmeti 2001 yılında müşterilerin kullanıma sunmuştur (Gefen ve Straub, 2005).

Avrupa'da ise Heffernan (2005) çalışmasında, 2001 yılında özellikle Finlandiya ve İsveç olmak üzere İskandinavya ülkelerinin, elektronik bankacılıkta oldukça başarılı olduklarından bahsetmektedir. O zamanlar bu ülkelerde banka müşterilerinin % 30'u, internet kullanıcısı veya modem yoluyla PC (Personel Computer) bankacılığını kullanmaktaydı. Şekil 2.4'e göre, 2010 yılında İsveç'in, online bankacılık kullanımında dördüncü sırada bulunması, bu görüşü destekler niteliktedir.

Comscore Şirketi'nin yaptığı araştırmanın 2010 yılı verilerine göre; Kanada, online bankacılığı en az ayda bir kez kullananlar bakımından yaklaşık % 65 ile ön sırada bulunmaktadır. Kanada'yı % 61,4 ile Hollanda izlemektedir. Bunun yanında, ABD, Avusturalya ve bazı Avrupa ülkeleri, online bankacılık kullanımında ilk on sırada yer almaktadırlar.



Şekil 2.4: Online Bankacılık Kullanımının Ülkelere Göre Sıralaması

Comscore Araştırma Şirketi'nin Tablo 2.1'de belirtilen Haziran 2011 raporuna göre; 2011 yılının ilk çeyreğinde, Kanada'daki 13,3 milyon online bankacılığı kullanıcısının % 62'si fatura ödemelerini bu bankacılık yolu üzerinden gerçekleştirmiştir. Yine aynı zaman diliminde, ABD'de online bankacılık hizmetini kullanan 63,6 milyon kişinin % 68'i faturalarını online olarak ödemişlerdir.

Tablo 2.1 Fatura Ödeme İşlemini Yapan Kullanıcılar

Ülke	**Toplam Kullanıcı Sayısı**	**Fatura Ödeme İşlemini Yapan Kullanıcı (%)**
Kanada	13,3 milyon	% 62
ABD	63,6 milyon	% 68

3.3.3.2. Türkiye'de Online Bankacılık

Özkul (2005), Türkiye'de online bankacılık hizmetlerinin 1997'den itibaren uygulanmaya başlanmasının ve ilk uygulamalardan 2005 yılına kadar, 19 bankanın bu hizmeti sağlamasının Türkiye'nin online bankacılık hizmetlerinde ne kadar hızlı ilerleme kaydettiğinin göstergesi olduğunu ifade etmektedir.

Türkiye İş Bankası, 1997 yılında bankacılık işlemlerini internet ortamına taşıyarak Türkiye'nin ilk online bankacılık hizmetini başlatmıştır (Türkiye İş Bankası, 2012).

1997 yılından 2010 yılının Haziran ayına kadar, Türkiye İş Bankası üzerinden yapılan işlemlerin yaklaşık % 70'i online bankacılık, ATM, telefon bankacılığı gibi alternatif dağıtım kanallarından yapılmaktadır. Bu dağıtım kanalları arasında, online bankacılık % 34 ile ilk sırada yer almaktadır.

Garanti Bankası, bireysel online bankacılığa 1997 yılında geçmiştir. 2002 yılında kurumsal/tüzel internet şubesini müşterilerine sunmuştur. Güvenlik problemlerine önlem olarak; 2005 yılında şifrematik ve 2006 yılında cep şifrematik uygulamalarını hayata geçirmiştir. Bugünlerde Garanti Bankası'nın online bankacılık şubesinde; vadeli/vadesiz hesap açma, para transferi, fatura ödemeleri, kredi başvurusu, vergi ödemeleri gibi 300'den fazla işlem yapılabilmektedir. 2010 yılı verilerine göre Garanti Bankası'nın 1,6 milyon aktif internet şubesi kullanıcısı bulunmaktadır. Online bankacılık işlemlerinde EFT ve havale gibi para transferlerinde online bankacılık hizmetini kullanma payı yaklaşık % 75 civarındadır.

Online bankacılık hizmetlerini başlatan ilk bankalardan olan Yapı Kredi Bankası, güvenlik alanında getirdiği yenilikler ile bu alanda öne çıkmaktadır. Yapı Kredi Bankası; 2004 yılında tek kullanımlık taşınabilir akıllı cihaz ve 2005 yılında tek kullanımlık şifre üreten "Akıllı Cep Uygulaması" ile online bankacılık hizmetlerine yön vermiştir (Finans Kulüp, 2010).

TBB Aralık 2011 raporunda, TBB'ye kayıtlı 25 bankada, online bankacılık sistemine kayıtlı olan ve en az bir kez giriş işlemi yapmış olan bireysel müşteri sayısı son bir yılda 1,9 milyon kişi artarak 18,1 milyon olarak belirlenmiştir.

Tablo 2.2: Online Bankacılığı Kullanan Müşteri Sayısı

	Aralık 2010	**Eylül 2011**	**Aralık 2011**
Bireysel müşteri sayısı (bin kişi)			
Aktif (A) (son 3 ayda 1 kez login olmuş)	6.038	7.065	7.803
Kayıtlı (B) (en az 1 kez login olmuş)	15.609	17.242	18.106
Kayıtlı (C) (son 1 yılda en az 1 kez login olmuş)	7.975	9.323	10.389
Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)	39	41	43
Kurumsal müşteri sayısı (bin kişi)			
Aktif (A) (son 3 ayda 1 kez login olmuş)	655	763	803
Kayıtlı (B) (en az 1 kez login olmuş)	1.614	1.786	1.892
Kayıtlı (C) (son 1 yılda en az 1 kez login olmuş)	814	915	968
Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)	41	43	42
Toplam müşteri sayısı (bin kişi)			
Aktif (A) (son 3 ayda 1 kez login olmuş)	6.694	7.828	8.606
Kayıtlı (B) (en az 1 kez login olmuş)	17.223	19.028	19.998
Kayıtlı (C) (son 1 yılda en az 1 kez login olmuş)	8.789	10.238	11.358
Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)	39	41	43

Tablo 2.2'e göre; kurumsal bazda online bankacılık sisteminde kayıtlı olan ve en az bir kez giriş işlemi yapmış kişi sayısı 1,9 milyon civarındadır. Bireysel anlamda aktif müşteri sayısı yaklaşık olarak 8 milyon ve kurumsal müşteri sayısı yaklaşık olarak 900 bin civarındadır. Kurumsal ve bireysel olmak üzere toplam aktif müşteri sayısının 1 milyon 912 bin kişi artması, online bankacılığın ülkemizde hızla yaygınlaştığının bir göstergesidir (TBB, 2012).

Online bankacılık hizmetinden yapılan işlemler; yatırım ve finansal işlere göre ayrılmaktadır. TBB'nin istatistiklerine göre; EFT, havale ve döviz transfer işlemleri, finansal işlemlerin % 86'sını oluşturmaktadır. 2011 yılının son 3 ayında gerçekleştirilen yatırım işlemlerinde ilk sırayı döviz işlemleri almıştır. Bu işlemi, yatırım fonu işlemleri, gerçekleşen hisse senedi işlemleri ve vadeli hesap işlemleri takip etmiştir.

İl bazında hem % 38 kurumsal/tüzel müşteri oranı ile hem de % 33 bireysel müşteri oranıyla İstanbul birinci sıradadır. Her iki müşteri grubunda da bu ili Ankara ve İzmir takip etmektedir.

2.3.4. Online Bankacılıkta Güvenlik Önlemleri

2.3.4.1. Kullanıcı Adı ve Parola

Bankacılık Düzenleme ve Denetleme Kurulu'nun (BDDK) 2010 yılındaki tebliğinde, bankanın online bankacılıkta müşterilerine uygulanmasını zorunlu kılması gereken iki adet bileşenden bahsedilmektedir. Bu bileşenlerin ilkinin müşterinin "bildiği" bir unsur özelliği taşıması gerekmektedir.

Bu karar doğrultusunda bankalar, online bankacılık hizmetini müşterilerinin kullanımına açtığı zaman, müşterilerine kendilerini sisteme tanıtabileceği bir kullanıcı adı vermektedir. Genellikle müşteri numarası kullanıcı adı olarak atanmaktadır. Bunun yanında müşterinin online bankacılık sisteminde kendini ispat edebileceği bir parola da verilmektedir. Online bankacılık hizmetine giriş esnasında ilk adım olarak, müşterilerin sahip oldukları kullanıcı adı ve parolayı yazarak sisteme tanıtmaları gerekmektedir. Sistem, girilen bilgileri doğruladıktan sonra kullanıcı sisteme giriş yapabilmektedir (Ertürk, 2002). Günümüzde bankalar, kullanıcı adı ve parolanın yanında; tek kullanımlık şifre, sanal klavye, güvenlik resmi uygulamalarını da kullanıcılarına sunmaktadır.

2.3.4.1. Mobil İmza

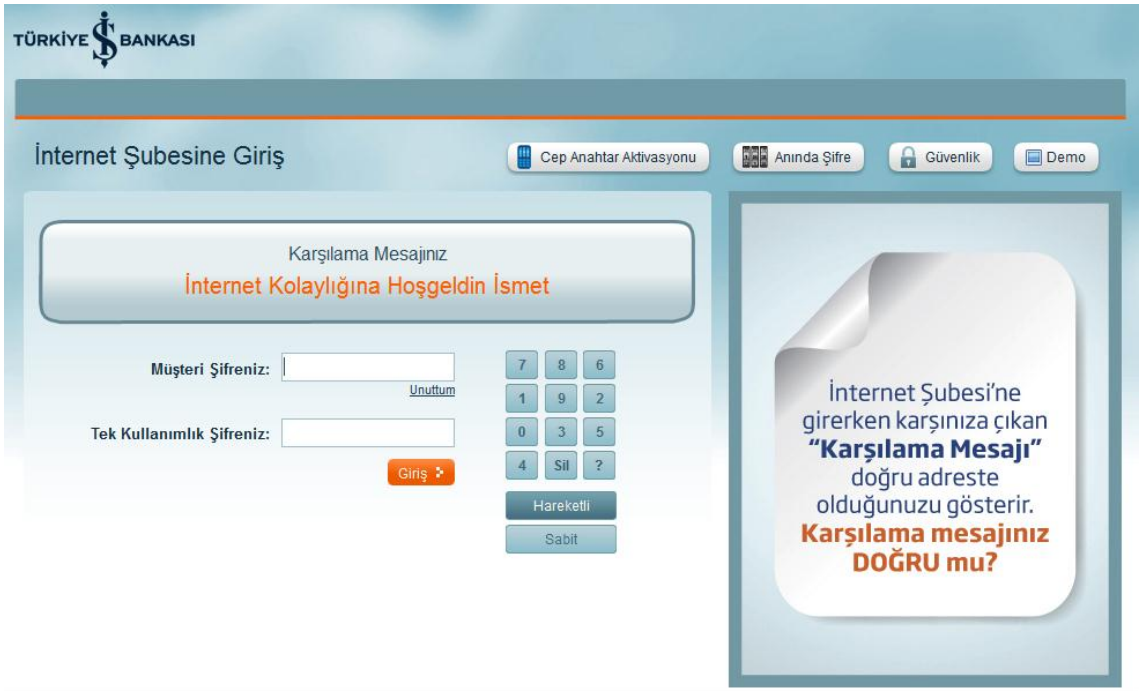
Avrupa Telekomünikasyon Enstitüsü (ETSI) mobil imzayı; herhangi bir vatandaşın mobil cihaz kullanarak işleme devam etme niyetini onaylamanın evrensel yolu şeklinde ifade etmektedir (ETSI, 2003).

Denizbank, resmi internet sitesinde müşterilerini mobil imza konusunda; 5070 sayılı Elektronik İmza Kanunu'nda tarif edilen ve ıslak imza ile eş değer Elektronik İmza'nın, cep telefonlarının SİM kartları kullanılarak atılmasını sağlayan bir servis şeklinde bilgilendirmektedir (Denizbank, 2011).

2.3.4.2. Sanal Klavye

Sanal klavye, ekranda klavyede bulunun tuşları gösteren ve mouse hareketleri ile tuşlara tıklanabilen bir uygulama olarak ifade edilebilir. Yeni olmayan bu fikrin temelinde, Windows İşletim Sistemleri'nde bulunan ve sırasıyla başlangıç, programlar, donatılar, erişebilirlik adımları takip edilerek ulaşılabilen ekran klavyesi bulunmaktadır. Fakat ekran klavyesi, keylogger gibi kötü amaçlı yazılımlara karşı korumasız durumda olduğundan bu program üzerinden girilen bilgiler kolaylıkla ele geçirilebilmektedir. Bu uygulama, aslında engelli bireylerin kullanımı için oluşturulmuştur. Keylogger tehditlerinden korunabilmek için, ekran klavyelerinin özel olarak tasarlanması gerekmektedir (Grebennikov, 2007).

Günümüzde bankaların müşterilerine sunduğu sanal klavye, fare yardımı ile şifrelerin girildiği online bir uygulama olarak tanımlanmaktadır. Ayrıca sanal klavyeler keylogger, spyware, truva atı benzeri zararlı yazılımlardan korunmak için tasarlanmıştır. Bu uygulamanın kullanılması ile kişisel bilgi hırsızlığı riskinin azalması beklenmektedir (Asim, 2011). Sanal klavye sayesinde, online bankacılık işlemlerinde ve elektronik alışverişlerde kullanıcı adı, şifre, parola, kredi kartı numarası, Kart Kodu Doğrulama (Card Code Verification, CCV) numarası gibi kişisel bilgiler, güvenli bir şekilde kullanılabilmektedir. Şekil 2.5'de Türkiye İş Bankası'nın online bankacılık sisteminde kullanılan sanal klavyenin de yer aldığı, internet şubesinin girişine ait ekran görüntüsüne yer verilmektedir.



Şekil 2.5: Sanal Klavye

2.3.4.3. Tek Kullanımlık Şifre

Tek kullanımlık şifre (One-Time Password) , kullanıcı adı veya şifre birleşimlerinin bir çeşididir. Sistem, her kullanımda yeni bir şifre üretmektedir. Dolayısıyla bir şifre iki kere kullanılmamaktadır (Lehtinen, Russell ve Gangemi, 2006).

Güvenlik adına online bankacılık hizmeti veren bankalar, tek kullanımlık şifreyi farklı şekillerde müşterilerine sağlayabilmektedirler. Bu uygulamalar şifre üreten cihazlar, Akıllı Cep, SMS Şifre, Cep Şifre, Mobil Onay, ŞifreTek şeklinde sıralanmaktadır.

Şifrematikler (Akıllı Anahtar), tek kullanımlık şifre üretme özelliğine sahiptir. Bu cihazlar hem yazılımsal hem de donanımsal olarak mevcuttur. Her şifrematiğin kendisi için tanımlanan bir kullanıcı adı vardır ve her cihazda birbirinden farklı şifre üretilmektedir. Aynı zamanda cihazlar, normal kullanıcı şifresi ve tek kullanımlık şifre olmak üzere iki aşamalı şifre sistemine sahiptir. İki şifreden birisi yanlış olursa kimlik doğrulama gerçekleşmemektedir. Böylece kullanıcı kimliklerinin çalınmasına karşı önlem alınmış olur. Tek kullanımlık şifreler, Evrensel Seri Veriyolu (Universal Serial Bus, USB) tipi cihaz, akıllı kartlar ve yazılım uygulamaları gibi farklı biçimlerde

kullanıcılara sunulmaktadır. Genellikle tek kullanımlık şifreler, kısa mesaj olarak hesap sahibinin cep telefonuna gönderilmektedir (Coleman ve Diğerleri, 2010).

2.3.4.4. Güvenli Yuva Katman (Secure Socket Layer, SSL) Güvenliği

Netscape Şirketi tarafından 1994 yıllında geliştirilen SSL, web tarayıcı ile web sunucu arasında, güvenli bilgi paylaşımını temin eden bir internet protokol çeşidi olarak tanımlanmaktadır. Bu katman, kimlik doğrulama ve gizlilik gibi iki temel güvenlik servisini barındırmaktadır. Sistemin temel mantığı, web tarayıcı ile web sunucusu arasında güvenli veri yolu tesis etmektir (Kahate, 2008).

SSL, gönderilen bilginin sadece doğru adreste deşifre edilebilmesini sağlamaktadır. Bilgi gönderilmeden önce otomatik olarak şifrelenir ve sadece doğru alıcı tarafından deşifre edilebilir. Her iki tarafta da doğrulama yapılarak işlemin ve bilginin gizliliği korunur (Ergüç, 2008).

Bu güvenli katmanda, kullanıcı ve sunucu arasında Hiper Metin Transferi Protokolü (Hypertext Transfer Protocol, HTTP) işlemlerini şifrelemede kullanılan simetrik anahtarını değiştirmek için, açık anahtarlı şifreleme kullanılmaktadır. Her işlem farklı bir anahtara sahiptir (Cole, 2011).

2.3.4.5. Güvenlik Resmi

Garanti Bankası'nın uyguladığı bu sistem, müşterilerin phishing saldırılarındaki sahte web sitelerinde işlem yapmalarını engellemeye yöneliktir. Online bankacılık şubesinin ilk kullanımı sırasında, sistemin sunduğu sekiz adet resimden biri güvenlik resmi olarak seçilmektedir. Bu güvenlik resmi, müşterilerin online bankacılık sistemine her girişlerinde parola ve şifre adımları arasında görünmektedir (Garanti Bankası, 2012).

2.3.4.6. İnternet Protokol (Internet Protocol, IP) Kısıtlaması

Online bankacılık hizmetlerinde alınabilecek güvenlik önlemlerinde birisi de IP kısıtlamasıdır. Bu hizmette müşteri sabit IP veya sabit IP aralığını belirleyerek kişisel online bankacılık hesabına farklı IP numaralarından giriş yapılmasını engelleyebilmektedir (Denizbank, 2012).

2.3.4.7. Tarih ve Saat Kısıtlaması

Bu kısıtlama IP kısıtlamasına benzer olarak, internet üzerinden müşterinin online bankacılık hesabına izinsiz girişleri engelleyebilmek için getirilen online bankacılık işlemlerinin belirli tarih ve saatte yapabilmesine imkan tanıyan bir önlemdir (INGBank, 2012).

2.3.4.8. Hesap Kısıtlaması

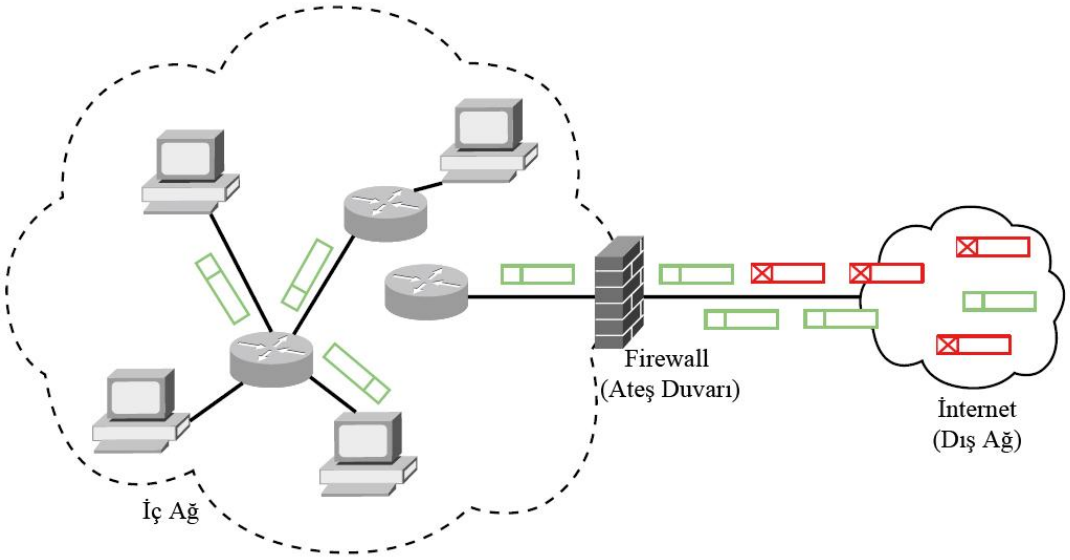
Türkiye'de bazı bankalar, müşterilerilerinin online bankacılık konusundaki güvenlik endişelerine yönelik hesap kısıtlaması uygulamaktadır. Bu önlemde müşteriler hesaplarını; online bankacılık sistemlerinde görüntülenebilen ancak finansal işlem yapılamayan veya online bankacılık sisteminde hiç görüntülenemeyen bir şekilde kısıtlayabilmektedir (INGBank, 2012).

2.3.4.9. Güvenlik Çemberi Uygulaması

Bu uygulama, Türkiye İş Bankası'nın müşterilerine online bankacılık hizmetleri için sunduğu güvenlik programıdır. Söz konusu uygulamanın amacı, müşterileri internet şubesine girişi sırasında olası truva atı, keylogger gibi kötü amaçlı yazılımların saldırılarına karşı korumaktadır (Türkiye İş Bankası, 2012).

2.3.4.10. Ateş Duvarı (Firewall)

Ateş Duvarı (Firewall), bir ağı korumak için yazılımsal veya donanımsal bir parça olarak tanımlanmaktadır. Firewall, kötü niyetli kişileri dışarıda tutan bir kara kutu gibidir (Osborne, 2006). Ateş duvarı için diğer bir tanımlama ise; ağ trafiğinin geçiş noktalarında bulunan ve ağlar arası geçişlerde veri paketlerinin güvenliğini kontrol eden bir sistem olduğu yönündedir. Ağ güvenliği için önemli olan bu sistem, genellikle kurum içi ağ ile internet arasındaki iletişimi kontrol için kullanılmaktadır. Bu iletişim Şekil 2.6'da resmedilmiştir. Bununla beraber; bu yapı, bir şirketin iş ortakları arasındaki veya ticari kuruluşların şubeleri arasındaki ağlarda güvenliği sağlamak için de kullanılabilmektedir (Brenton ve Hunt, 2002).



Şekil 2.6 : Ateş Duvarı (Firewall)

2.3.4.11. Güvenli Elektronik İşlemler (Secure Electronic Transactions, SET)

SET, VISA ve MasterCard tarafından 1996 yılında, internet gibi güvenli olmayan ortamlarda, kredi kartı ile yapılan işlemlerin güvenliğini sağlamak için geliştirilen bir protokoldür.

Bu protokol online işlemler sırasında;

- Yetkili sertifika ile yapılan kayıttaki ilk işlem sırasında, müşteri ve tüccarın kimliklerini doğrulamakta,
- Alışveriş sırasındaki tüketici, tüccar ve ödeme sertifikalarının değişiminde, ek kimlik doğrulaması gerçekleştirmekte,
- Hesap numarası, ödeme kartının son kullanma tarihi gibi hassas bilgilerin, müşteri ile banka arasında kalmasını sağlamakta,
- Alışveriş yapılan mağaza yetkililerinin, müşterinin kredi kartı bilgilerine ulaşamaması ve sadece ödeme yapıldığına dair onayı görebilmesine imkan tanımaktadır (Oram ve Viega, 2009).

Bu işlemlerde, taraflar arasında aktarılan bilgilerin gizliliğinde açık anahtar şifrelemesi ve dijital sertifikalar kullanılmaktadır. SET'in temel iki görevi bulunmaktadır; birincisi kredi kartı ve diğer ödeme bilgilerinin aktarılması için güvenli bir sistem altyapısı oluşturma, ikincisi ise müşteriden gelen bu bilgilerin onaylanmasını sağlamaktır (Keyes, 1999).

2.3.5. Online Bankacılıkta Tarafların Sorumlulukları

2.3.5.1. Bankanın Sorumluluğu

Bankanın, online bankacılık sistemine yönelik dışarıdan gelebilecek saldırılara karşı önlemleri alma ve müşterilerini bu saldırılar konusunda uyarma sorumlulukları bulunmaktadır. Bu önlemler doğrultusunda banka, online bankacılık sisteminin güvenliği için en üst seviyede bir altyapı sistemini kurmak zorundadır.

Nitekim bu doğrultuda BDDK, 14 Eylül 2007 tarihinde, "Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" i Resmi Gazete'de yayımlamıştır. Bu tebliğin üçüncü kısmının birinci bölümü, online bankacılık hakkında bazı kriterler içermektedir. Bu kriterler; güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi, kimlik doğrulama, inkâr edilemezlik ve sorumluluk atama, denetim izlerinin oluşturulması, servis sürekliliği ve kurtarma planı başlıkları altında açıklanmaktadır.

Tebliğin güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi adlı bölümünde; bilgi sistemlerinin güvenlik kontrolleri, yeterlilikleri yılda en az bir kez olmak kaydıyla düzenli olarak bağımsız ekiplerce test edilmesi, banka tarafından kurulan bilgi sisteminin şüpheli işlemleri tespit edici özelliğine sahip olması ile ilgili uyarılar yer almaktadır.

Kimlik Doğrulama kısmında ise; online bankacılık hizmetindeki kimlik doğrulama mekanizmalarında olması gereken bileşenler ve özellikler, sabit parola ve değişken parola özellikleri, ayrıntılı bir şekilde açıklanmaktadır.

Tebliğin diğer kısımlarında ise bankanın;

- online bankacılık faaliyetlerine ait işlemlerde inkar edilemez ve sorumluluk atama temelli kontrolleri sağlamak zorunda olduğu
- online bankacılık faaliyetleri için günümüz teknolojilerine uygun, verimli bir denetim izi tutma sistemi tesis etmesi gerektiği
- online bankacılık hizmetleri ile ilgili müşterilerini mevcut politika, prosedürler ve dikkat edilmesi gereken durumlar konusunda bilgilendirmek zorunda olduğu
- online bankacılık hizmetini sağlayan internet sitesinin bankaya ait olduğunu belli edecek teknikleri kullanması gerektiği

- online bankacılık servisi için beyan ettiği veya müşterilerine taahhüt ettiği seviyede servis sürekliliğini sağlamak zorunda olduğu,

belirtilmektedir (Resmi Gazete, 2012).

BDDK'nın 14 Eylül 2007 tarihinde yayınlanan tebliğin online bankacılık ile ilgili olan maddeleri EK-C kısmında yer almaktadır.

2.3.5.2. Müşterinin Sorumluluğu

Üçüncül kişilerin bireysel hesaba ilişkin işlem alanına giriş yaparak herhangi bir işlem gerçekleştirdiğini ispatlamak oldukça zordur. Söz konusu işlemi yapan kişi hesap sahibi olabileceği gibi, bu kişiye ait bilgileri ve şifreleri ele geçirmiş olan başka bir kişi de olabilmektedir. Bu nedenle hukuk dışı olduğu iddia edilen işlemin üçüncü kişi tarafından yapıldığı tespit edilmediği sürece, bu işlemin hesap sahibi tarafından gerçekleştirildiği kabul edilir ve sorumluluk hesap sahibine aittir (Ucar, 2009). Müşterinin online bankacılık gibi hizmetlerde kullandığı şifre ve parolalar, bankacılık sırrı kapsamında değerlendirilmektedir (İnceoğlu, 2006). Hatta anne kızlık soyadı gibi önemli bilgilerin de bu kapsamda sayılması gerektiği ifade edilmektedir. Online bankacılık hizmetinden yararlanan müşterilerin, banka tarafından kendilerine tahsis edilen kullanıcı adı, şifre, parola ve diğer kişisel bilgilerinin üçüncü kişilerin eline geçmemesi için gerekli önlemleri alma zorunluluğu bulunmaktadır (Ucar, 2009).

2.4. KİŞİSEL BİLGİ HIRSIZLIĞI YÖNTEMLERİ

Hackerlar online bankacılık suçlarını gerçekleştirirken kişisel bilgi elde etmek için bazı yöntemler kullanmaktadırlar. Bu kısımda hackerların kullandığı kişisel bilgi hırsızlığı yöntemleri açıklanmaktadır.

2.4.1. Sosyal Mühendislik Kavramı

Literatürde birçok sosyal mühendislik tanımlaması bulunmaktadır. Townsend (2010), sosyal mühendisliği belirli hedef davranışları değiştirmek için gerçekleştirilen psikolojik etkileme uygulamaları olarak tanımlamaktadır. Rothke (2005)'ye göre sosyal mühendislik, temel olarak insanların bilgi veya yardım için ikna edilmesi yoluyla hacklenmesi olarak tanımlanmaktadır.

Erbschloe (2004) ise hackerların bilgisayar sistemlerini ve ağlarını yasadışı saldırı veya kullanım için, bilgisayar kullanıcılarına yönelik sosyal maskeler, kültürel roller ve psikolojik hileler kullanmasını sosyal mühendislik olarak ifade etmektedir. Diğer bir tanımlama Kizza (2005) tarafından yapılmış ve kurum içinden veya dışından yetkili bir kişi maskesi kullanılarak gerçekleştirilen bir dizi hileler bütününü sosyal mühendislik şeklinde açıklamıştır.

Bu tanımlardan yola çıkarak sosyal mühendisliği; "hackerların kanundışı uygulamalar için insanların önemli bilgilerini kişisel alanlarına yetkisizce girip, aldatıcı, ikna edici ve psikolojik yöntemler kullanılarak elde etme çabası" şeklinde ifade edebiliriz.

Power ve Forte (2006) sosyal mühendisliği; insan tabanlı sosyal mühendislik saldırıları ve teknoloji tabanlı sosyal mühendislik saldırıları olmak üzere ikiye ayırmaktadır.

2.4.2. İnsan Tabanlı Sosyal Mühendislik Saldırıları

İnsan tabanlı sosyal mühendislik; mağdurun bilgisizliğinden ve insan doğasındaki yardım etme özelliğinden yararlanıp kişiyi aldatma demektir (Gulati, 2003). Thapar (2007) da, teknik olmayan bu saldırılarda insan davranışlarındaki zayıflıklardan yararlanmaya vurgu yapmaktadır. İnsan tabanlı sosyal mühendislik ile ilgili başka bir tanımlamayı Burlu (2011); saldırganların hedefledikleri bilgilere insani ilişkiler kurup ikna yöntemlerini kullanarak ulaşması şeklinde yapmaktadır.

Hackerlar istedikleri bilgileri elde etme adına birçok kimliğin arkasına saklanabilmektedirler. Bu doğrultuda kurban olarak bireyler veya kurumlar hedef alınabilmektedir. Seçilen kurban tipine göre kullanıcı-kullanıcı, kullanıcı-kurum, kurum-kurum arasındaki iletişimler takip edilmekte ve bu iletişimdeki zaaflar tespit edilmeye çalışılmaktadır. Bu süreçte insanların güvenme duygusu ve yardımcı olma istekleri hackerların işlerini kolaylaştırmaktadır. Bir şirketin özel bilgilerini veya şirketteki bir personelin bilgilerini elde etmek için,

- Yetkili Personel
- Kurum Personeli
- Müşteri Temsilcisi
- Hizmet Alan Kullanıcı

- Hizmet Sağlayıcı
- Teknik Personel
- Yardımsever Kullanıcı

kimlikleri kullanılabilmektedir (Elbahadır, 2011).

Hackerlar, hedeflerine ulaşmak için teknik temeli olmayan bazı yöntemler kullanmaktadır. Bu yöntemlerden biri olan Çöpleri Kurcalama (Dumpster Diving); önemli bilgileri elde etmek amacıyla çöp kutularının karıştırılması anlamına gelmektedir. Basit gözüken ama göz ardı edilen bu yöntem ile IP adresleri, kullanıcı adları ve şifreleri, e-posta adresleri, telefon numaraları bilgilerine rahatça ulaşılabilmektedir. Bu nedenle çöp kurcalama yöntemi hâlâ popülerliğini korumaktadır.

Bu güvenlik zafiyetine karşı hem bireysel hem de kurumsal olarak alınabilecek önlemler bulunmaktadır. Bunlardan bazıları; atık kutusu kullanımı, çöpler için kilit kullanımı, atıkları parçalama/yok etme politikası, kâğıt dokümanları parçalayan aygıtları kullanma zorunluluğu, çalışanlara yönelik farkındalık eğitimidir (Cross, 2008).

Teknoloji kullanımına dayalı olmayan diğer bir yöntem olan Omuz Üstünden Bakma (Shoulder Surfing); ATM şifreleri, kullanıcı adı ve şifreleri, kredi kartı numarası gibi kişisel bilgileri elde etmek için yapılan gözlem olarak ifade edilebilir. Hiçbir teknik temeli olmayan bu yöntemde dolandırıcı, sadece hedefteki kişinin dalgınlığından yararlanıp gözlem yaparak kişisel bilgileri ele geçirme çabasındadır (Allsopp, 2009).

Arata (2010) ise omuz üstünden bakma yönetimini; birinin ne yaptığını görmek için diğer bir kişinin arkasından bakma sanatı olarak tanımlamaktadır. Bu hırsızlık yönteminden korunma yolu olarak da; ATM'den para çekerken veya internet üzerinden kişisel bilgi gerektiren işlemler yaparken herhangi bir kimsenin bu işlemleri izleyip izlemediğinin kontrol edilmesi gerektiğini belirtmektedir.

Aslında, sosyal mühendislik saldırılarına karşı en iyi önlem farkındalıktır. Bu doğrultuda kurumlar, bu saldırılara karşı alınacak önlemler konusunda çalışanlarını eğitmelidir. Bunun yanı sıra alınabilecek önlemlerden birisi de kişinin şüpheci olmasıdır

(Long, 2008). Bu tip durumlarda; kişi normal, güvenilir, arkadaş canlısı insan profilinden uzaklaşarak biraz daha şüpheci karaktere bürünmelidir (Wiles, Gudaitis vd., 2011). Dünyanın ilk bilgisayar korsanlarından diğer adıyla hackerlarından olan Kevin David Mitnick "Teknoloji ve hizmetleriniz için servet harcayabilirsiniz fakat sistem ağınızın altyapısı hala eski moda olan sosyal mühendislik manipülasyonalarına karşı savunmasız kalabilir." demekte ve sosyal mühendisliğin ne kadar tehlikeli olabileceğine dikkat çekmektedir (Rothe, 2005).

2.4.3. Teknoloji Tabanlı Sosyal Mühendislik Saldırıları

Sosyal mühendislik saldırılarının amacı; farkettirmeden finansal bilgileri çalmaktır. Değişmeyen saldırı prensibi ise hedef kitlenin güvenini kazanmak için basit duyguları kullanarak uyarlanan bir senaryodur. Teknoloji tabanlı sosyal mühendisliğin en yaygın saldırı yöntemleri: Oltalama (Phishing), Kötü Amaçlı Yazılım (Malware), Tuş Kaydedici (Keylogger) ve Sahte Anti-Virüs Yazılımı (Roqueware)'dır (Townsend, 2010).

2.4.3.1. Oltalama (Phishing)

Phishing kelimesi, hackerların balık avlamanın İngilizcesi olan fishing kelimesindeki "f" harfini kendi ortak dillerinde "ph" harflerini kullanmalarıyla oluşmuştur (Jakobsson ve Myers, 2006). Hutchinson (2005) phishing teriminin; bilgisayar korsanlarının sanal dünyada kişilerin kredi kartı bilgilerini elde elmek için aldatıcı e-postaları tanımlarken kullandıkları "fish" yani balık avlamak kelimesinden devşirildiğini belirtmektedir. Bunun temelini de, hackerların 1960'lı yıllarda telefonu izinsiz kullanma anlamına gelen "phone phreaks" kelimelerindeki "ph" harflerini uyarlanmasına dayandırmaktadır.

Dunham (2008), 21. yüzyılın kimlik hırsızlığı olarak kabul edilen oltalamayı; sosyal mühendisliği ve teknik hileleri temel alarak kredi kartı bilgileri, sosyal sigorta numaraları, online giriş bilgileri gibi kişisel bilgileri çalma girişimleri olarak tanımlamaktadır.

Oltalama (Phishing) saldırıları alanında araştırmalar yapan uluslararası bir kuruluş olan Anti-Phishing Çalışma grubu oltalamayı; kişisel tüketici bilgilerini ve banka hesap bilgilerini çalmak için sosyal mühendisliği veya teknik aldatmacaları kullanılarak yapılan online bilgi hırsızlığının bir şekli olarak ifade etmektedir.

Lininger ve Vines (2005), oltalamayı kısa ve öz bir biçimde "otomatik kimlik hırsızlığı" olarak tanımlamaktadır. Günümüzde, Aldatıcı Oltalama (Deceptive Phishing), Kötü Amaçlı Yazılım Temelli Oltalama ve Açılır Pencere (Pop-Up) Temelli Oltalama sıkça karşılaşılan oltalama yöntemleri arasında yer almaktadır.

Aldatıcı oltalama yöntemi, ortaya çıktığı ilk yıllarda anlık mesaj gönderme temelli uygulanmaktaydı. Fakat son zamanlarda hackerlar aldatıcı oltalama yöntemi için e-postayı kullanmaktadır. Kullanıcıya gönderilen e-postada ilgi çekici içerikler yer almaktadır. Ayrıca e-posta, resmi bir kurumdan gelmiş havası taşımakta böylece hedefteki kişinin durumdan şüphelenmemesi sağlanmaktadır. Bu yöntemdeki e-postalar;

- "Müşterinin hesabı ile ilgili bir problem olduğu ve belirtilen linke tıklanarak sorunun çözülebileceği
- Müşteri hesabının risk altında olduğu ve sahtekârlığı önleyici programa üye olması gerektiği
- Müşterinin gerçekleştirmediği bir sipariş için gönderilen online faturadaki bağlantı linkine tıklanarak siparişi iptal edebileceği"

senaryolarını içerebilmektedir (Jakobsson ve Myers, 2006).

Birçok banka, müşterilerini son yıllarda artan aldatıcı oltalama saldırılarına karşı bilgilendirmektedir. Şekil 2.7.'de, Garanti Bankası'nın resmi internet sitesinde aldatıcı oltalama saldırılarında kullanılan e-posta örneği üzerinden müşterilerini bu tip saldırılara karşı uyarmaktadır.

Şekil 2.7 Sahte E-posta Örneği

Başka bir oltalama yöntemi olan kötü amaçlı yazılım temelli oltalamada ise hackerlar kullanıcının sistemine Malware (Kötü Amaçlı) türü yazılımlar ile saldırıyı gerçekleştirmektedir. Bu tip saldırılar sosyal mühendislik veya güvenlik zaafiyetleri yoluyla yayılmaktadır. Sosyal mühendislikte, bilgisayar kullanıcısının, hacker tarafından gönderilen e-posta ekindeki dosyayı indirmesi neticesinde zararlı yazılımlar bilgisayara yüklenmektedir. Solucan (Worms) ve virüsler ile güvenlik zaafiyetinden yararlanılması kötü amaçlı yazılım temelli oltalama saldırılarının diğer bir yoludur (EC-Council, 2009).

Açılır pencere (Pop-Up) temelli oltalama yöntemi ise diğer geleneksel oltalama tekniklerinden farklıdır. Londra Büyükşehir Polis Teşkilatı'nın Güvenlik Raporu'nda (2005), bu yöntemde açılan web sitesinin ilk olarak bankanın yasal web sitesi gibi gözüktüğü ve 5-10 saniye sonra müşterinin kişisel bilgilerini isteyen bir pop-up penceresi açıldığı belirtilmektedir. Bu pencereye girilen kişisel bilgiler de hackerların ortamına aktarılmaktadır.

Aslan (2012), bu saldırılara karşı alınabilecek güvenlik önlemlerini;

- Bilgisayarların işletim sistemi güncellemeleri ihmal edilmemeli
- Güncel ve kaliteli anti-virüs programı kullanılmalı
- Bilinmeyen kişi veya kurumlardan gelen e-postalar okunmadan silinmeli ve bu tür mesajlar dikkate alınmamalı
- E-posta yoluyla gelen her web site bağlantı linkine tıklanmamalı ve özellikle bankalar, sosyal paylaşım siteleri, alışveriş siteleri gibi bağlantılara erişileceği zaman klavye yardımı ile tarayıcıya adres yazılarak web sitesine giriş yapılmalı
- Güvenli olmayan internet bağlantılarından kesinlikle elektronik işlem gerçekleştirilmemeli
- Giriş yapılan web sitesinin sağ alt kısmında yer alan ve web sayfasının güvenli olduğunu gösteren kapalı kilit işareti olduğuna dikkat edilmeli
- Online bankacılık ve e-ticaret işlemlerinin HTTPS uzantılı web adresi üzerinden yapıldığına dikkat edilmeli

olarak ifade etmektedir.

Bu tip saldırılara karşı korunmanın en etkili yolu; bilinçli bilgisayar kullanıcısı olmaktır. Oltalama saldırısına maruz kalındığında öncelikle yetkili merciler bu konuda bilgilendirilmelidir. Böylelikle yetkililerin bu hususta önlem almasına ve saldırganların yakalanmasına yardım edilmiş olur.

2.4.3.2. Yemleme (Pharming)

Yemleme, sahte IP adresiyle Alan Adı Servisi'nde (Domain Name Server, DNS) yapılan değişiklik neticesinde kullanıcıları yasal web siteleri üzerinden sahte web sitelerine yönlendiren bir aldatma yöntemidir. Yemleme ve oltalama tekniklerinin ortak yönü sahte site üzerinden kişisel bilgileri çalmaktır. Fakat yemleme yöntemi daha karmaşık ve farkedilmesi zor bir yöntemdir (Parsons ve Oja, 2012). Çünkü oltalamada, sahte web site bağlantısı hedefteki kişiye gönderilmekte ve kişisel bilgiler girildiği takdirde bunlar saldırganlara ulaşmaktadır. Yemleme'de ise hacker, DNS sunucusuna giriş yaparak sunucu kayıtlarında bulunan yasal adres üzerinden sahte siteye yönlendirme yapmaktadır. Kullanıcı, yasal site olarak algıladığı sahte site üzerinden banka hesap numarası, şifre vb. kişisel bilgilerini girmektedir (Dilsiz, 2011).

2.4.3.3. Tuş Kaydedici (Keylogger)

Teknoloji dünyasında malware diye adlandırılan kötü amaçlı yazılımlar, sızmak istediği sistemin güvenlik kurallarını işlemez hale getirerek zararlı fonksiyonlar içeren programları sisteme entegre etmeyi amaçlamaktadır. Aslında kötü amaçlı yazılımlar virüslerin geniş bir sınıfıdır. Tuş Kaydedici (Keylogger), Truva Atı (Trojan Horse), Casus Yazılım (Spyware), Ekran Kaydedici (Screenlogger), Sahte Anti-Virüs Yazılımı (Rogueware) gibi saldırılar malware kategorisine giren zarar verme amacı taşıyan uygulamalardır (Bidgoli, 2004).

Ciampa (2011), tuş kaydedicilerin bilgisayar klavyesindeki her tuş hareketini yakalayabilme ve kaydedebilme özelliğine sahip olduğunu belirtmektedir. Kaydedilen bu bilgiler, saldırgan tarafından daha sonra alınabilmekte veya gizlice başka bir ortama aktarılabilmektedir.

Tuş kaydediciler, yazılımsal ve donanımsal olmak üzere ikiye ayrılmaktadır. Yazılımsal tuş kaydediciler; kötü amaçlı yazılım kategoresine giren truva atı davranışı gösteren ve

bilgisayara yüklenebilen bir programdır. Donanımsal tuş kaydediciler ise bilgisayar kasasının arka tarafına takılan 3 cm'den küçük olabilen bir parçadan oluşmaktadır (Simpson, Backman ve Corley, 2010).

Bu parça, klavye bağdaştırıcısı veya usb bağlantı portu ile klavye arasına yerleştirilmektedir. 64 Kilobayt (kb) hafızaya sahip bir donanımsal tuş kaydedici, 65 bin tuş darbesini hafızasına alabilmektedir (Ye, 2008). Bu cihaz, sıradan klavye bağlantısına benzediği ve bilgisayarın arka tarafında bulunduğu için farkedilmesi neredeyse imkânsızdır. Donanımsal tuş kaydedici, belli bir süre sonra bulunduğu yerden çıkarılarak kaydedilen veriler saldırgan tarafından anlamlı hale getirilmektedir. Donanımsal tuş kaydedicilerin bazı çeşitleri bilgisayara Şekil 2.8'deki gibi yerleştirilmektedir.

Şekil 2.8: Donanımsal Tuş Kaydedici

Yazılımsal tuş kaydedici ise kişisel bilgileri elde etmek için bilgisayara yüklenen programlardır. Bu tip tuş kaydediciler, fiziksel bir girişe ihtiyaç duymamakta fakat bir şekilde bilgisayara yüklenmesi gerekmektedir. Yazılımsal tuş kaydedicilerin bir diğer özelliği ise gerekli güvenlik taramaları yapılsa bile kolay kolay tespit edilememesidir (Ciampa, 2011). Bu yolla bilgileri alan hackerlar, ağ giriş yetkisine sahip olduğu sürece hedef bilgisayardaki herhangi bir dosya üzerinde işlem yapabilmektedir (Kim ve Solomon, 2010).

Bu tip tuş kaydedicileri önlemek için bilgisayara lisanslı bir anti-virüs programının yüklenmesi gerekmektedir. Bunun yanında, anti-keylogger olarak sınıflandırılan güvenlik araçlarını kullanmak faydalı olmaktadır. PrivacyKeyboard ve Advanced Anti Keylogger, piyasada bulununan birçok güvenlik araçlarından bazılarıdır. Bu araçlar klavyedeki tuş hareketlerini kaydeden zararlı yazılımlara karşı bilgisayarı korumaktadır (Ec-Council Press, 2010).

Diğer bir önlem olarak sanal klavye uygulaması gösterilmektedir. Bu uygulama ile kredi kartı bilgileri, şifre gibi kişisel bilgilerin bilgisayar ortamında yazılımsal tuş kaydedicilerden korunması mümkün olmaktadır. Buna ek olarak, bilgisayardaki ateş duvarı (firewall) uygulamasının aktif durumda olması gerekmektedir. Bu uygulama, tuş kaydedicilerin bilgisayara yüklenmesine karşı koyamamakta fakat bilgisayardan izinsiz veri transferini engellemektedir. Donanımsal tuş kaydedicilere karşı alınacak önlem ise bilgisayar donanımlarını sürekli kontrol etmektir (Bunker ve King, 2009).

2.4.3.4. Truva Atı (Trojan Horse)

Zararlı kodların özel bir çeşidi olan "Truva Atı" adını; Yunan Mitolojisi'ndeki Troy şehrine hediye olarak götürülen aslında içinde şehre saldırmak üzere olan askerlerin bulunduğu tahta truva atından almıştır (Colorik ve Janczewski, 2008). Bu program, mitolojideki truva atı gibi zararsız gözükmesine rağmen bilgisayar sistemine ve sistem kullanıcısına ciddi zararlar verebilmektedir. Truva atının eksik yanı, virüsler gibi kendi kendilerine çoğalamamasıdır (Dülger, 2004).

Kumar, Srivastava ve Lazarević (2005), truva atlarının devlet kurumlarına ait web sitelerine sabotajlarda, banka hesaplarına yönelik internet dolandırıcılığında ve iletişim, ısı, güç vb. alanlardaki sistemlere zarar vermede kullanılabileceğini belirtmektedir.

Sosyal mühendisliği temel alan bu saldırılarda zararlı dosya; resim, oyun, program veya normal dosya olarak gözükmekte, kullanıcının bunlara aldanıp truva atı yazılımını çalıştırması hedeflenmektedir. Hackerler bu saldırı için ön araştırma yaparak, hedef kullanıcının zaaflarını ve ilgi alanlarını tespit etmeye çalışmaktadır. Örnek olarak; oyun meraklısı bir kullanıcıya yönelik truva atına oyun paketi görüntüsü verebilmekte veya oyun görünümlü bir siteden saldırı gerçekleştirilebilmektedir. Bu truva atları, çalıştırıldığı anda içine entegre edilmiş olan zararlı kodlar aktif hale gelmektedir.

Truva atı, yapısal olarak kullanıcı (client) ve sunucu (server) olmak üzere iki kısımdan oluşmaktadır. İlk kısım olan "server.exe" formatındaki yazılım, bilgisayarın güvenlik duvarını aşmak ve içeri sızmak için tasarlanmaktadır. İkinci kısım olan "client.exe" ise güvenliği aşılmış sistemi kontrol etmeye yaramaktadır. Truva atları, internet üzerinden veya taşınabilir depolama aygıtları yoluyla bilgisayar sistemine bulaşmaktadır. Bu kötü amaçlı yazılımlar;

- Kullanıcı adı, şifre, banka hesap bilgilerini çalma
- Dosyaları kopyalama, değiştirme, silme ve yönetme
- Hedef sisteme uzaktan erişim sağlama
- Çalışan sistem uygulamalarına müdahale etme
- Sistem dosyalarına zarar verme
- Başka saldırılar için korunmasız duruma getirme
- Sabit disk, Ekran, CD-ROM gibi donanımsal araçlara müdahale etme

gibi zararlar verebilmektedir (Elbahadır, 2011).

Burlu (2011), truva atına karşı alınacak önlemleri;

- Şüpheli e-postalar açılmamalı ve bu postalarınn içindeki dosyalar da indirilmemeli
- Güvenli olmayan web sitelerinin açılır pencelerine tıklanmamalı ve ActiveX denetimleri etkinleştirilmemeli
- Zararlı kod ve casus yazılım olma olasılığı yüksek olan yasal olmayan sitelere giriş yapılmamalı
- Bilgisayardaki antivirüs yazılımları ve güvenlik duvarı uygulamaları sürekli güncel olarak sistemde yer almalı

şeklinde sıralamaktadır.

Elbahadır (2011) bu önlemlere ek olarak; "Drive By Download" temelli saldırılara karşı ActiveX kontrol ayarlarının yapılandırılmasının önemli olduğunu ve kontrollerin "sor modu"na ayarlanması gerektiğini belirtmektedir.

2.4.3.5. Casus Yazılım (Spyware)

Spyware terimi, casusluk anlamına gelen "spying" ve yazılım anlamına gelen "software" kelimelerinden oluşmaktadır. Türkçe adıyla Casus Yazılım, kötü amaçlı yazılım türüdür (Butler, 2010).

Bu yazılımların amacı, hedefin kişisel bilgisayarına veya bilgisayar ağına saklanarak önemli bilgileri toplamak ve bu bilgileri yazılımı geliştiren kişilere veya gruba göndermektir. Casus yazılımı geliştiren kişilerin öncelikli gayesi elde ettikleri bilgiler ile parasal kazanç sağlamaktır. Yazılımsal tuş kaydediciler ve truva atları bu tip yazılımların alt kategorisi olarak sayılmaktadır (Brown, 2010).

2.4.3.6. Ekran Kaydedici (Screenlogger)

Polimirova ve Nikolov (2010)'un yaptığı zararlı kodların sınıflandırılmasında bulunan altmış dört bilgi saldırısından biri de ekran kaydedicidir. Jakobsson ve Myers (2006) ekran kaydediciyi; alternatif güvenlik önlemlerini engellemek için kullanıcının sisteme girişlerini, hareketlerini ve ekranını izleyen yazılım olarak ifade etmektedir.

2.4.3.7. Salam Tekniği

Salam tekniği, hackerların çok sayıda banka hesabından önemsiz görünen küçük miktardaki paraları truva atı türü yazılım ile kullanıcının dikkatini çekmeden başka bir hesaba aktarma olarak tanımlanmaktadır. Bu tekniğin adı, çalınan paranın banka hesabından küçük dilimler halinde aktarılmasından gelmektedir (Krause ve Tipton, 1999).

2.4.3.8. Çöpe Dalma (Scavenging)

Çöpe dalma olarak ifade edilen yöntemde amaç; bilişim sisteminde gerçekleştirilen işlemler sonucunda kalan bilgileri toplamaktır. Hackerlar, elde ettikleri veriler ile kişisel bilgilere ulaşmaya çalışmaktadır. Bu bilgiler, bilgisayar sistemine ait çıktı birimlerince üretilen ve sonrasında çöpe atılan kâğıt, DVD/CD, mürekkep şeridi gibi malzemelerden elde edilmektedir. Ayrıca bilgisayar sisteminin belleğinde bulunan silinmiş bilgilere, gelişmiş yöntemler ve bazı programlar kullanılarak ulaşılmaktadır (Yazıcıoğlu, 1997).

Bilgisayar sisteminden bilgilerin geri getirilebilmesi için ileri düzeyde programlama bilgisine ve bilgisayar sistemine doğrudan veya ağ yoluyla ulaşılmasına ihtiyaç duyulmaktadır (Değirmenci, 2002). Çünkü kullanıcı dosyayı silerken, bilgiler tamamen

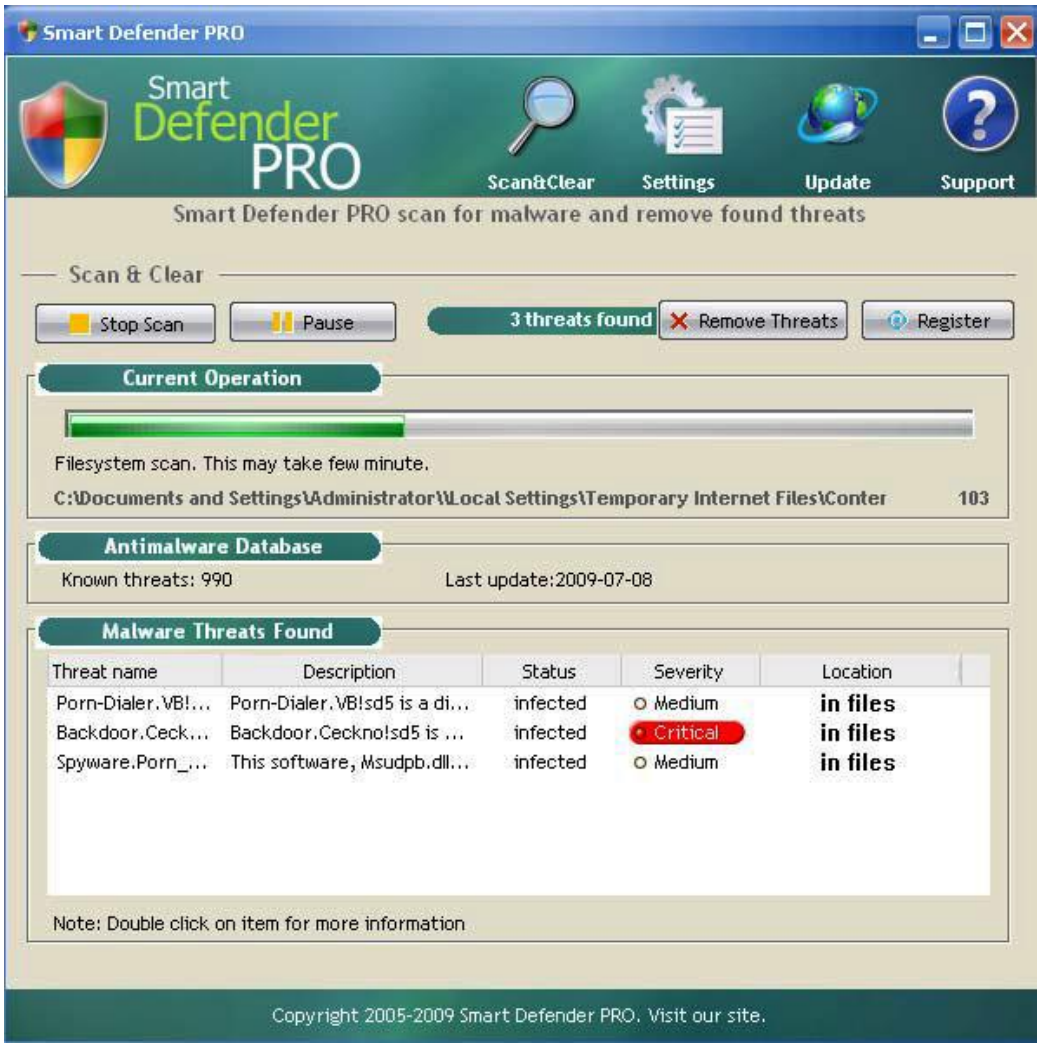
yok edilmemektedir. Onun yerine bilgisayarda tekrar kullanılabilecek alan oluşturulmakta ve silinen bilgiler geri getirilmektedir (Adomi, 2008).

Çöpe dalma yöntemine örnek olarak; 1981 yılında "Captain Zap" takma adıyla Pat Riddle adlı şahsın bilgi toplaması gösterilebilir. Captain Zap, telefon bilgilerini içeren kitapçıklardan ve şirket içi bilgi notlarından yararlanarak birçok telefon numarası elde etmiştir. Bu numaralar ile Amerikan Hava Kuvvetleri bilgisayarları başta olmak üzere, MIT (Massachusetts Institute of Technology), Pentagon ve Beyaz Saray'ın sistemlerine bağlanarak çok sayıda önemli veriye ulaşmıştır (Clough ve Mungo, 1999).

2.4.3.9. Sahte Anti-Virüs Yazılımı (Roqueware)

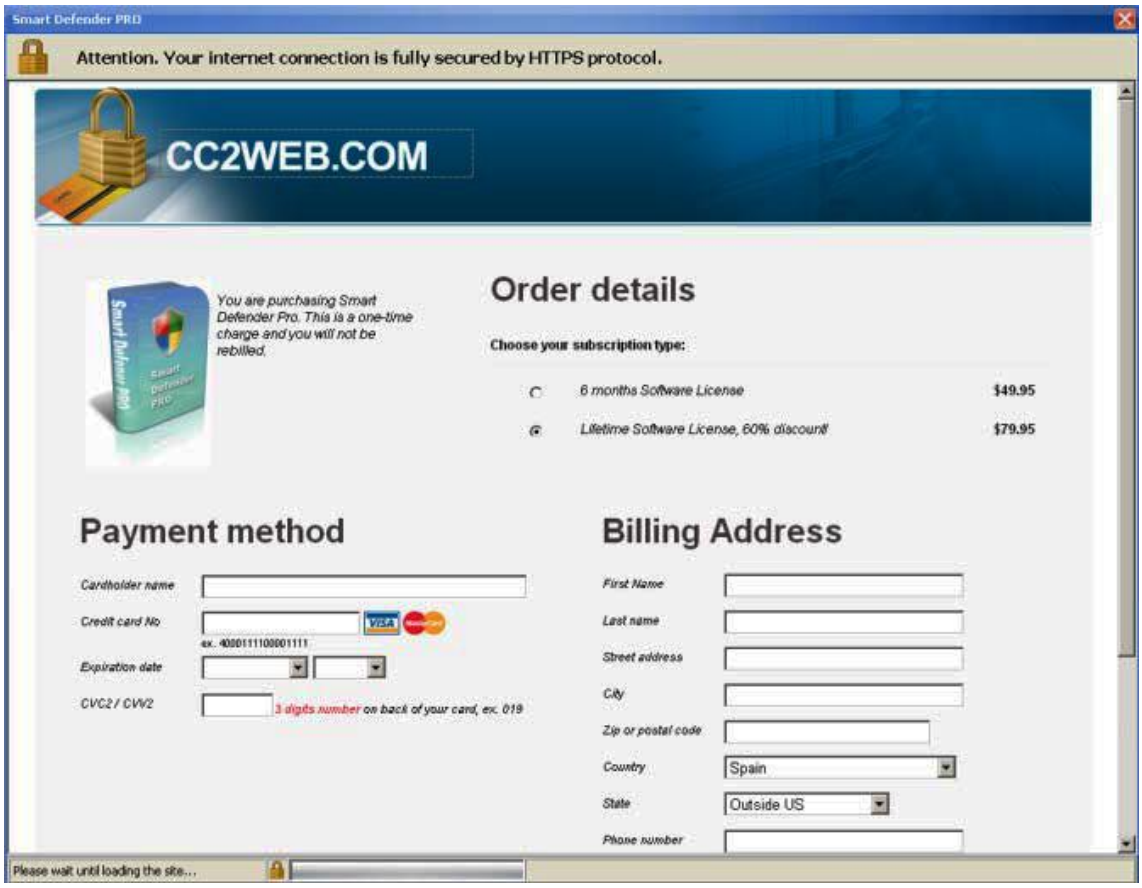
Kişisel bilgi hırsızlığı yöntemlerinin bir diğeri de son yıllarda ortaya çıkan Rogueware adlı sahte anti-virüs yazılımıdır. Rogueware, bilgisayar kullanıcılarını varolmayan tehditleri yoketmek için ödeme yapma tuzağı ile kullanıcıların paralarını çalma girişimlerini barındıran aldatıcı yazılım çözümleridir (Correl ve Corrons, 2009).

Gibson (2011)'un truva atı türü olarak belirttiği bu yazılım, orijinal anti-virüs programı gibi gözükerek virüs uyarısı vermekte ve kullanıcıyı virüsü yok etmesi için para ödemeye zorlamaktadır. Şekil 2.9'da, "Smart Defender Pro" güvenlik yazılımının sahte sürümünün ekran görüntüsü bulunmaktadır.



Şekil 2.9: Sahte Anti-Virüs Yazılımı Virüs Uyarısı

Sözde bazı virüslerin tespit edildiği ve kullanıcının "Remove Threats" butonuna tıklayarak tehlikeden korunması gerektiği belirtilmektedir. Kullanıcı, ilgili butona tıkladığında sahte yazılım kullanıcıya Şekil 2.10'daki ekran görüntüsünü çıkarmaktadır.



Şekil 2.10: Sahte Anti-Virüs Yazılımı Ödeme Ekranı

Bu görüntüde, kullanıcının virüslerden kurtulması için ödeme yapması gerektiği ifade edilmektedir. Yazılım, "Attention. Your Internet connection is fully secured by HTTPS protocol" Türkçe olarak "Dikkat. İnternet bağlantınız HTTPS protokolü ile tamamen güvenlidir" cümlesi ile kullanıcının güvenini kazanmaya çalışmakta ve ödeme ekranı ile kullanıcının alışveriş için gerekli tüm kredi kartı bilgilerini ele geçirmektedir.

Panda Güvenlik Laboratuvarı Raporu'na göre; 2009 yılında 1 milyona yakın Rogueware türü sahte güvenlik yazılımı tespit edilmiştir. Hackerlar, bu yazılımdan yılda 400 milyon dolar kazanç elde etmektedir. Aynı çalışmaya göre, 2009'un başından beri Facebook, MySpace, Twitter ve Digg gibi sosyal medya platformları sahte anti-virüs yazılımını yayan kişilerin hedefi konumundadır (Correl ve Corrons, 2009).

2.5. İLGİLİ ARAŞTIRMALAR

Bu kısımda literatürdeki online bankacılık ile ilgili çalışmalardan bahsedilmiştir. İnternet bankacılığı doktrindeki diğer ifadesiyle online bankacılık ile ilgili işletme, hukuk, işletme eğitimi, pazarlama v.b alanlardaki yüksek lisans, doktora ve akademik makale çalışmaları incelenmiştir.

Bu çalışmalar; banka müşterilerinin online bankacılık kullanımına ilişkin çalışmalar ile online bankacılık dolandırıcılığına ilişkin çalışmalar şeklinde şeklinde kategorize edilerek incelenmiştir. Aşağıda online bankacılık kullanan müşterilerin profili ve kullanım nedenleri hakkında yapılan çalışmalara yer verilmiştir.

Gaziler (2006) yüksek lisans tez çalışmasında, online bankacılığın kullanımı ve kullanım etkinliği-eğitim ilişkisini araştırmıştır. Çalışmanın örneklemini, Ankara ilinin Gölbaşı ilçesindeki Türkiye İş Bankası, Akbank, Yapı Kredi Bankası, Vakıfbank, T.C Ziraat Bankası ve Türkiye Halk Bankası müşterilerinden bankaya gelen 481 kişi oluşturmaktadır. Veri toplama aracı olarak kullanılan anket, çoktan seçmeli ve 5'li likert ölçekli (En Az, Az, Fikrim Yok, Çok, En Çok) toplam 15 soru olarak hazırlamış ve 20 kişilik ön çalışma ile son halini almıştır. Anket, yüz yüze görüşme yöntemi ile katılımcılara uygulanmıştır. Elde edilen veriler, SPSS (Statistical Programme for Social Sciences) programında yüzde analizi, Ki-Kare testi, F testi, serbestlik derecesi ve ANOVA testleri kullanılarak analiz edilmiştir.

Analiz sonucunda ortaya çıkan Ki-Kare testi verilerine göre online bankacılık kullanımı ile eğitim seviyesi arasında anlamlı bir ilişki olduğu tespit edilmiştir. Özellikle üniversite mezunlarının online bankacılık kullanım oranının yüksek seviyede olduğu belirlenmiştir. Bu grubu lise mezunları takip etmiştir. İlkokul ve ortaokul mezunlarının online bankacılık kullanım durumu ise dikkate alınmayacak derecede düşük çıkmıştır. Bunun nedeni olarak bilgisayar ve internet okur-yazarlığının yetersizliği vurgulanmıştır. Ortaya çıkan diğer bir sonuç, online bankacılık kullanımı ile yaş arasında anlamlı bir ilişki olduğu ve 26-35 yaş arasındaki katılımcıların yüksek oranda internet kullandığıdır. Online bankacılığı kullanan katılımcıların % 50'ye yakını bu bankacılık hizmetini güvenli bulmamaktadır. Bu hizmeti güvenli bulan katılımcıların oranı ise örneklemin % 27'lik kısmını oluşturmaktadır.

Pala (2010) çalışmasında, banka müşterilerinin online bankacılığa yönelik tercihlerini araştırmıştır. Araştırmanın örneklemini; zaman, maliyet, deneğe kolay ulaşılabilirlik ve gönüllülük ölçütlerine göre 196 kişilik bir çalışma grubu oluşturmaktadır. Bu araştırmada, veri toplama aracı olarak 5'li likert tipi ölçeğin yer aldığı bir anket uygulanmıştır. Anketin güvenirliği ve geçerliği için; bankacılık alanında üç uzmanın desteği ile 40 kişilik bir grup üzerinde pilot çalışma yapıldıktan sonra ankete son şekli verilerek örneklem üzerinde uygulanmıştır. Anket, katılımcılara e-posta yoluyla ulaştırılmış ve verilerin toplanması 10 gün sürmüştür. Elde edilen veriler; frekans, t-testi, varyans analizi (ANOVA), yüzde ve aritmetik ortalama teknikleri kullanılarak SPSS programı ile analiz edilmiştir.

Verilerin çözümlenmesi neticesinde; online bankacılığı kullanma sıklığının ATM ve telefon bankacılığı hizmetlerine göre daha fazla olduğu, kadınların erkeklere göre daha belirgin bir şekilde online bankacılığı yaşam tarzı olarak gördüğü, kişilerin online bankacılık tercihlerinde güvenlik, kolaylık, zaman tasarrufu ölçütlerinin dikkate alındığı belirlenmiştir. Ayrıca katılımcılar arasında Türkiye İş Bankası, Garanti Bankası ve Akbank online bankacılık hizmetlerinin kullanımının ilk üç sırayı paylaştığı fakat Türkiye İş Bankası müşterilerinin memnuniyet derecesinin daha fazla olduğu sonucu ortaya çıkmıştır.

Ekberg, Li ve Morina (2007), İsveç'in dört büyük bankasının müşterileri üzerinde gerçekleştirdiği çalışmanın neticesinde; müşterilerin online bankacılıkta kullanışlılığa verdiği önemin, güvenliğe verdiği önemden daha fazla olduğu sonucuna ulaşılmıştır.

Özcan (2007) Türkiye'de elektronik bankacılığın ilk örneklerini veren bankaların, yeni dağıtım kanallarından biri olan online bankacılığı kullanılmasının ve benimsenmesinin altında yatan sebepleri araştırmıştır. Çalışmanın örneklemi, Sakarya ilinde yaşayan kişilerden oluşturulmuş ve kolay örnekleme yöntemi ile 250 kişi seçilmiştir. Veri toplama aracı olarak kullanılan anket; çoktan seçmeli ve 5'li likert ölçekli (Tamamen Katılıyorum, Katılıyorum, Emin Değilim, Katılmıyorum, Tamamen Katılmıyorum) olmak üzere toplam 22 adet sorudan oluşmaktadır. Anketin katılımcılara ulaştırılması elden ve faks yoluyla gerçekleştirilmiştir. Anketlerin 210 tanesine geri dönüş yapılmış

ve bunların 10 tanesi bazı eksiklerden dolayı elenmiştir. Verilerin analizinde ise SPSS programı kullanılarak frekanslara, yüzdelere ulaşılmıştır. Değişkenler arası ilişkilerin ölçülmesinde Ki-Kare testinden yararlanılmıştır. Online bankacılığı kullanan katılımcıların, bu bankacılık hizmetini kullanmasında hangi faktörlerin etkili olduğunu belirlemek için faktör analizi yöntemi kullanılmıştır.

Söz konusu araştırma neticesinde;

- online bankacılığın kullanılma ve benimsenme sebebinin kullanım kolaylığı, uygunluk ve etkinlik gibi faktörlerin olduğu
- benimsenmenin temelinde; zamandan tasarruf, mekandan bağımsızlık, 7 gün 24 saat ulaşılabilir olmanın yatmakta olduğu
- online bankacılığı kullanmayan katılımcıların, online bankacılığı güvenli bulmadığı ve online bankacılık hakkında pek bilgiye sahip olmadıkları
- online bankacılık kullanımı ile demografik özelliklerin (yaş, cinsiyet, medeni durum v.b) arasında anlamlı bir ilişkinin olduğu

sonuçlarına ulaşılmıştır.

Özbal (2011), müşteri ilişkileri yönetimi felsefesi çerçevesinde kişinin online bankacılık kullanımında nelerden etkilendiğini araştırmıştır. Örneklemi, Ankara ilindeki 18 yaşından büyük lise ve üstü eğitime sahip 226 kişi oluşmaktadır. Bu kişiler bireyler rassal olarak seçilmiştir. Araştırmanın verileri, anketin 2010 yılının Nisan ayında yüzyüze görüşmeler yapılarak uygulanması sonucunda toplanmıştır. Toplanan veriler, SPSS programında Ki-Kare, yüzde dağımı, frekanstan yararlanılarak analiz edilmiştir. Anlamlılık değeri $p<0,05$ olarak belirlenmiştir. Verilerin analizi ile birlikte;

- online bankacılık kullanımı ile cinsiyet arasında anlamlı ilişki olduğu
- online bankacılık sitelerinin işlevselliği ve ürün çeşitliliğinden dolayı online bankacılığı kullananların % 65,1'inin bayan olduğu
- güvenlik önlemlerini alma ile eğitim durumu arasında anlamlı ilişkinin olmadığı
- eğitim seviyesi yüksek olan bireylerin online bankacılığı kullanmaya eğilimli oldukları
- online olarak verilen bankacılık hizmetlerinden yararlanma durumu ile yaş durumu arasında istatistiksel olarak anlamlı bir ilişki olduğu

sonuçları ortaya çıkmıştır.

Zhu'nun 2009 yılındaki çalışmasında online bankacılık güvenliğini; banka ve müşteri arasındaki mesajların yasallığından emin olma, banka hesaplarına üçüncül kişilerin ulaşamaması, online bankacılık işlemlerini müşterinin yapıp yapmadığının ispatı olmak üzere üç yönden incelemiştir. Araştırması neticesinde; online bankacılığın güvenli olmayan bir ortam olduğu ve güvenliğin sağlanması için cep telefonlarının daha geniş bir ekrana ve bilgisayar özelliklerine sahip olması gerektiği ifade edilmiştir.

Dağlı (2007), "banka müşterilerinin online bankacılığa karşı tutumlarının sınıfladırılmasına yönelik herhangi bir çalışma yoktur" ifadesi ile yola çıkarak, bu kitleyi online bankacılığa yönelik düşüncelerine göre anlamlı gruplar altında toplamaya ve oluşan grupları kendi içinde demografik ve sosyo-kültürel bakımdan tanımlamaya çalışmıştır. Örneklem olarak; İstanbul ili sınırlarındaki Avcılar, Şirinevler, Bakırköy ve Kadıköy bölgelerinde yaşayan, 18 yaş ve üstünde olup banka hesabı olan bireyler şeçilmiştir. Veri toplama aracı olarak, internet yolu ile 15 kişi üzerinden gerçekleştirilen pilot uygulama neticesindeki dönütler yardımıyla düzenlenen anket, yüz yüze görüşme yöntemi ile 232 kişiye uygulanmıştır. Bankacılık ve internet kullanım alışkanlıklarını belirlemek için ön anket yapılmıştır. Araştırma sonunda elde edilen bilgilerin analizi; SPSS programında frekans, K-Ortalamalar ve Ki-Kare testi kullanılarak gerçekleştirilmiştir. Bulguların çözümlenmesi sonucunda; online bankacılığı kullanan müşteriler, online bankacılığı kullanmaya yakın müşteriler ve online bankacılığa uzak müşteriler şeklinde üç grupta kümelenme meydana gelmiştir. Bu üç farklı kümenin, belirli demografik ve sosyo kültürel özelliklere göre farklılık gösterdigi belirlenmiştir. Müşterilerin kümelere ayrılmasında internet kullanımının, gelir düzeyinin, internet okuryazarlık ve eğitim seviyesinin etkili olduğu söylenebilir.

Birinci kümede yer alan online bankacılığı kullanan müşterilerin; eğitim seviyesi lisans ve lisansüstü, hergün interneti kullanan, gelir seviyesi orta ve yüksek düzeyde kişiler oldukları belirlenmiştir. İkinci küme; lise ve altı eğitim seviyesine sahip, internet ve online bankacılık kullanım bilgisi düşük kişilerden oluşmaktadır. Üçüncü kümedeki kişiler; online bankacılık hizmetini kullanmaya yakın fakat bu hizmeti pek kullanmayan kişilerdir.

Özdemir (2010), KOBİ'lerin online bankacılık hizmetlerini kullanma sıklığını ve yeterliliğini tespit etmeyi amaçlamıştır. Araştırmanın örneklemini; Aksaray, Niğde, Karaman ve Konya illerindeki 181 adet KOBİ oluşturmaktadır. 34 soruluk bir anket, veri toplama aracı olarak belirlenmiş ve yüz yüze görüşme yöntemiyle uygulanmıştır. Veriler, SPSS programında çok değişkenli varyans analizi (MANOVA), tek yönlü ANOVA, t-testi ve parametrik olmayan hipotez testleri yapılarak analiz edilmiştir. Bulgularda; işletmelerin % 83'e yakın bir kısmının online bankacılığın iş hayatındaki önemine inandığı ve işletmelerin yaklaşık olarak % 78'lik kısmının online bankacılığı kullandığı belirlenmiştir. Geriye kalan % 22'lik bir kesimin online bankacılığı kullanmama nedeni olarak; güvenlik problemi ve online bankacılık hakkında sahip oldukları bilgilerin yetersiz oluşu belirlenmiştir. Bunun yanında, online bankacılığı kullanan KOBİ'lerin bu hizmeti tercih nedeni; zamandan tasarruf ve düşük maliyet olarak tespit edilmiştir. Son olarak, işletmelerin online bankacılığı en çok EFT ve havale işlemleri için kullandıkları belirlenmiştir.

Mujwauzi (2009)'nın Çinli internet kullanıcılarına yönelik yaptığı araştırmada, örneklemi oluşturan kişilerin % 47'sinin online bankacılığı kullanmadıkları ve bu kişilerin % 68'inin online bankacılığın güvenli olmadığı görüşüne sahip oldukları sonucu ortaya çıkmıştır.

Umur (2006) çalışmasında online bankacılığı kullanan müşterilerin tutumlarını banka açısından değerlendirmiştir. Araştırmanın örneklemini, Türkiye'de faaliyet gösteren 6 banka oluşturmaktadır. Veri toplama aracı olarak 25 soruluk anket hazırlanmıştır.
24. ve 25. sorulara ait cevaplar mülakat yöntemi kullanılarak alınmıştır. Araştırma neticesinde, bankaların online bankacılığı kullanma nedenleri arasında maliyeti düşürmenin, hizmet kalitesini yükseltmenin, rekabet üstünlüğü elde etmenin, müşteri bağlılığını sağlamanın olduğu belirlenmiştir. Bunun yanında online bankacılığı kullanan müşterilerin büyük bir kısmını üniversite mezunu, orta ve yüksek gelir düzeyinde, yaşları 25-45 aralığında olan kişilerin oluşturduğu sonucuna varılmıştır.

Zerenler (2006), Atılgan (2006) ve Öztürk (2006) online bankacılık müşterilerine yönelik benzer çalışmalar yapmışlar ve yakın sonuçlara ulaşmışlardır.

Bu çalışmalar ışığında;

- Online bankacılık hizmetini çoğunlukla eğitim, bilgisayar-internet okuryazarlık ve gelir seviyesi yüksek kişiler tercih etmektedir. Cinsiyet bakımından kadın bireyler online bankacılığı daha çok benimsemektedir.
- Müşteriler online bankacılık hizmetlerini; kullanım kolaylığı, zaman tasarrufu, ulaşılabilirlik nedenlerinden dolayı kullanmaktadırlar.
- Müşterilerin banka tercihinde online bankacılık hizmeti veren bankaların web site işlevselliği ve güvenlik seviyeleri etkili olmaktadır.
- Diğer taraftan, güvenlik hakkında endişe taşıyan müşterilerin oranı değişkenlik göstermesine rağmen güvenlik endişesi online bankacılık kullanımını etkileyen bir ölçüt olarak devam etmektedir.

Aşağıdaki çalışmalar, online bankacılık ile ilgili olan dolandırıcılık vakaları ve bu vakaların müşterilerde oluşan güvenlik kaygısına etkisi hakkındadır.

Ergüç (2008)'ün Türk Bankacılık Sistemi'nde online bankacılık ile ilişkili dolandırıcılık suçları hakkında yüksek lisans çalışması mevcuttur. Bu çalışma beş bölümden oluşmaktadır. Birinci bölümde; internet ve dolandırıcılık kavramlarına yer verilmiştir. İkinci kısımda; kişisel bilgilerin çalınmasında kullanılan trojan, keylogger, screenlogger, sahte site v.b yöntemlerden bahsedilmiştir. Üçüncü kısımda; sahte belge, banka kartı sahteciliği ve dolandırıcılığının tespiti hakkında bilgiler bulunmaktadır. Bilişim Suçları Hukuku ana başlığı altında; kanundaki suç tipleri, uygulanacak cezalar, bilişim suçları kanunu hakkında önemli bilgiler ifade edilmiştir. Son bölüm olan beşinci bölümde ise; Türk Bankacılık Sistemi'nde elektronik bankacılık risk yönetim prensipleri ve tarafların sorumluluklarından bahsedilmiştir. Çalışmanın sonucunda, online bankacılık suçlarında organize suç çetelerinin olduğu ve aynı tarafta olan banka ve müşterilerin bu suçların engellenmesi için birlikte hareket etmesi gerektiği vurgulanmıştır. Taraflar bunları yaparken özellikle güvenlik konusunda bankanın güvenli online bankacılık hizmeti sunarak, müşterinin de bilgisayar güvenliği konusunda hassas davranıp kişisel bilgisayarının güvenliğini sağlayarak temel sorumluluklarını yerine getirmelerinin şart olduğu belirtilmektedir. Bununla beraber gelişen teknolojilerle artan bilişim suçlarının ilişkili kanunlarda kapsamlı ve ayrıntılı maddeler halinde yer alması gerektiği sonucuna ulaşılmıştır.

Adıgüzel (2009) çalışmasını, son yıllarda online bankacılığın yaygınlaşması neticesinde ortaya çıkan online bankacılık ile ilgili dolandırıcılık suçlarının artışından dolayı müşterilerde oluşan güvenlik kaygısının online bankacılığın kullanımına etkisi olup olmadığının araştırılması amacı ile gerçekleştirmiştir.

Araştırmanın örneklemini, araştırmanın evreni olarak seçilen Ankara ili Vakıflar Bankası Maltepe Şubesi'nin online bankacılık hizmetini kullanan 2698 müşterisi içerisinden "basit rastgele örnekleme" yönteminden yararlanılarak belirlenen 400 müşteri oluşturmaktadır. Örneklemdeki katılımcılara; cinsiyet, yaş, eğitim durumları, gelir düzeyi, gibi demografik özelliklerini belirlemek, ayrıca interneti kullanım sıklıkları, internete bağlandıkları mekanlar, online bankacılığı kullanıp kullanmadıkları, online bankacılık hakkındaki bilgi düzeyleri, online bankacılık sitelerindeki aranan özellikler, online bankacılığı kullanmıyorlarsa nedenleri, bilgisayar ve internet ile ilgili olarak aldıkları güvenlik önlemlerini tespit etmek amacıyla anket uygulanmıştır. Anketin güvenirliği ve geçerliği için yapılan pilot çalışmadan sonra ankete son şekli verilmiştir. Araştırma verileri; SPSS programında betimleyici istatistikler, mutlak ve nispi frekanslar, Ki-Kare Bağımsızlık Testi gibi çeşitli istatistiki çözümleme yolları kullanılarak yorumlanmıştır.

Araştırmadaki verilerin analizi neticesinde; online bankacılık kullanım oranının, yaş, eğitim düzeyi ve gelir düzeyine bağlı olarak değişiklik gösterdiği saptanmıştır. Diğer taraftan, online bankacılık ile ilgili yaşanan dolandırıcılık olaylarının online bankacılık kullanımını olumsuz etkilemediği yargısına ulaşılmıştır.

Bu çalışmalardan elde edilen sonuçlara göre, bankaların ve müşterilerin sorumluluklarını yerine getirmesi ve kanun koyucu tarafından bilişim suçları ile ilgili yeni kanunlar ve düzenlemeler yapılması gerektiği ortaya çıkmıştır. Bu sonuçlara ek olarak; günümüzde artan online bankacılık dolandırıcılıkları, müşterilerin güvenlik kaygısını etkilememektedir.

Tüm bu çalışmaların haricinde, Yılmaz (2007), doktora tez çalışmasında online bankacılığı hukuk temelli ele almıştır. Bu çalışmada Yılmaz (2007), internet üzerinden yapılan bankacılık işlemlerinin artması sonucu ve kullanıcıların karşılaştıkları; internet üzerinden hukuki işlemlerin kurulması, online bankacılık işlemlerinin belirlenmesi, online bankacılıkta ortaya çıkan güvenlik problemi sebebiyle kimlerin sorumlu tutulacağı, internet servis sağlayıcı kusurundan kaynaklanan problemler neticesinde neler yapılabileceği gibi özgün sorunlardan yola çıkarak, söz konusu bu problemleri ve bunlara ilişkin çözüm yollarını ortaya koymaya çalışmıştır.

Bu çalışma, literatür temelli ikincil kaynaklardan derlenen bilgiler ile oluşturulmuştur. Temel olarak beş bölüm bulunmaktadır. Birinci kısımda; online bankacılık ile ilgili dünya çapında ağ, internet, sunucu, bilgisayar, web sitesi, elektronik ticaret ve elektronik ticaret türleri v.b kavramlar hakkında bilgiler verilmektedir. İkinci kısımda; online bankacılığın tanımı, tarihsel gelişimi, işleyiş süreci ve online bankacılıkta müşterilerin korunması hususlarına değinilmiştir. Üçüncü kısımda; online bankacılık hizmet sözleşmesinden; tanım, hukuki nitelik, şekil, kurulum, sona erme çerçevesinde bahsedilmiştir. Dördüncü kısımda ise, online bankacılıkta güvenlik ve tarafların yükümlülükleri konusu incelenmiştir. İlgili çalışmanın son kısmını oluşturan beşinci kısımda, online bankacılıkta gerçekleştirilebilecek bankacılık hizmetleri yer almıştır.

Sonuç olarak; Avrupa Birliği uyum sürecinde tüketicinin korunması hakkındaki kanun düzenlenerek mesafeli sözleşme maddesi gelitirilmiş ve online bankacılık hizmet sözleşmesi mesafeli sözleşme sayılmıştır. Bu sözleşmenin banka ve müşterilere getirdiği bazı sorumluluklar bulunmaktadır. Banka, bilgi verme ve aydınlatma, online bankacılık hizmetinin yürütülebilmesi için tedbir alma ve sistem hatalarını giderme gibi sorumluluklarını yapmadığı takdirde Bankalar Kanunu'nun 96. maddesi vd. hükümlerine göre müşterinin uğradığı zararı karşılamak zorundadır.

Buna karşılık, müşteri kullanıcı adı ve şifrenin üçüncü kişilerin eline geçmemesi için gerekli önlemleri almak, bu bilgilerin kötü niyetli kişilere geçtiğini anladığında bankayı durumdan haberdar etmek, bilgisayarın güvenliğini sağlamak gibi sorumlulukları yerine getirmek zorundadır. Aksi takdirde, müşteri ortaya çıkacak zarara katlanmak zorunda kalacaktır.

Bunlara ek olarak; müşterinin internete bağlanamamasının internet sisteminden kaynaklanan problem olduğu durumda internet servis sağlayıcısının sorumlu olduğundan bahsedilmiştir. Kimi zaman da internet servis sağlama hizmetini bankanın verdiğinden dolayısıyla sorumluluğun bankada olduğu ve bankanın sorumluluğunun internet servis sağlama sözleşmesinden kaynaklandığı belirtilmiştir.

3. MALZEME VE YÖNTEM

Bu bölümde; araştırma modeli, araştırma örneklemi, veri toplama aracı, veri toplama süreci, verilerin analizi, araştırmanın geçerliği hakkında bilgiler yer almaktadır.

3.1. ARAŞTIRMA MODELİ

Bu yüksek lisans tez çalışmasında online bankacılık suçlarına ilişkin ceza dava dosyaları araştırılmıştır. Elde edilen dosyalar "Online Bankacılık Suçları İle İlişkili Dava Dosyalarını İnceleme Anketi" ne göre incelenmiştir. Bu araştırma için nicel araştırma modeli uygulanmış ve anketteki maddelerin sıklıkları dikkate alınmıştır.

3.2. ARAŞTIRMA ÖRNEKLEMİ

Bu çalışmanın örneklemini, İstanbul ili sınırları içerisinde bulunan Bakırköy, Kadıköy, Sultanahmet ve Pendik Adliyeleri olmak üzere 4 farklı yerdeki toplam 21 ceza mahkemesi ile İstanbul Emniyet Müdürlüğü'nde faaliyet gösteren Bilişim Suçları ve Sistemleri Şube Müdürlüğü oluşturmaktadır.

3.3. VERİ TOPLAMA ARACI

Bu çalışmada, online bankacılık suç dosyalarını incelemek için bilişim suçları ve hukuk alanında uzman 5 kişinin görüşü alınarak "Online Bankacılık Suçları ile İlişkili Dava Dosyalarını İnceleme Anketi" hazırlanmıştır. Bu anket; TCK'daki suç maddesi, suç yöntemi, suç unsurunda kullanılan sistemler, mağdur tarafın kullandığı online bankacılık sistemi, mağdur profili, sanık profili, suç delilleri, suça konu olan para miktarı, dava süresi, dava soruşturma süresi, dava sonucu olmak üzere 11 maddeden oluşmaktadır. Online Bankacılık Suçları ile İlişkili Dava Dosyalarını İnceleme Anketi, çalışmanın Ek-A kısmında verilmiştir.

3.4. VERİ TOPLAMA SÜRECİ

Veri toplama süreci iki kısımdan oluşmaktadır. Veri toplama sürecinin ilk kısmı; İstanbul ili sınırları içerisindeki Bakırköy, Kadıköy, Sultanahmet ve Pendik Adliyeleri'nden seçilen toplam 21 ceza mahkemesinde online bankacılık suçlarına ilişkin dava dosyalarının taranmasından oluşmaktadır. İkinci kısım ise İstanbul Emniyet Müdürlüğü'ndeki ilgili 11 online bankacılık suç dosyasının incelenmesinden oluşmaktadır.

3.4.1. Sultanahmet Adliyesi Veri Toplama Süreci

İstanbul Sultanahmet Adliyesi'ndeki araştırma 2011 yılı Mayıs ayının son haftasında yapılmıştır. Bu adliyede, 3. Ağır Ceza, 7. Ağır Ceza ve 13. Asliye Ceza olmak üzere üç farklı mahkemedeki online bankacılık suçlarına ilişkin davalara ulaşılmıştır.

3. Ağır Ceza Mahkemesi'nden 8 dava dosyası elde edilmiştir. Bu dava dosyalarının gerekçeli kararları incelediğinde bu dosyaların online bankacılık suçları ile ilgili olmadığı tespit edilmiştir.

13. Asliye Ceza Mahkemesi'nde 2007, 2008, 2009, 2010 ve 2011 yıllarına ait kayıt defterlerinde dava konularına bakılarak arama yapılmıştır. Bu defterlerde yaklaşık 1600 dava kaydının incelenmesi neticesinde 15 adet bilişim suçları ile ilişkili dava dosyası bulunmuştur. Bunlardan 12'sinin online bankacılık suçları ile ilişkili olduğu belirlenmiştir.

7. Ağır Ceza Mahkemesi'ndeki gerekçeli kararların incelemesi neticesinde online bankacılık ile ilgili olması muhtemel olan 4 dosya belirlenmiştir. Bu dosyalardan 2'sinin online bankacılık suçları ile ilgili olduğu tespit edilmiştir.

3.4.2. Pendik Adliyesi Veri Toplama Süreci

Pendik Adliyesi'nde 8 Haziran 2011 tarihinde yapılan araştırmada 4 dosya tespit edilmiş ve bu dosyalardan 2'sinin online bankacılık suçları ile ilgili olduğu belirlenmiştir.

15 Haziran 2011 tarihinde yapılan araştırmada ise 7 dava dosyası tespit edilmiştir. Bu dosyalarda 6'sının online bankacılık suçları ile ilişkili olduğu belirlenmiştir.

3.4.3. Kadıköy Adliyesi Veri Toplama Süreci

2011 Haziran ayının ilk haftasında 1. Ağır Ceza Mahkemesi'nde yapılan araştırmada online bankacılık suçlarıyla ilişkili dosya tespit edilememiştir.

Kadıköy Bilişim Suçları Bürosu savcılarından gerekli izinler alınarak Kadıköy Adliyesi arşivinde 2006, 2007, 2008 yıllarına ait iddianame klasörleri incelenmiştir. Bu klasörlerden, online bankacılık suçları ile ilişkili 8 dosyanın iddianame numarası alınmıştır. Daha sonra Bilişim Suçları Savcılık Bürosu Kalemi'nde dosyaların hangi mahkemelerde olduğu bilgisine ulaşılmıştır. Bu bilgiler doğrultusunda, Kadıköy 6. Asliye Ceza Mahkemesi'nde online bankacılık suçu ile ilgili dava dosyası gerekli izin alınarak incelenmiştir.

19-20 Nisan 2012 tarihlerinde yapılan araştırmada ise 1, 2, 3, 4, ve 7 Asliye Ceza Mahkemelerinde toplam 11 dosyadan 7'sinin online bankacılık suçu ile ilişkili olduğu belirlenmiştir.

3.4.4. Bakırköy Adliyesi Veri Toplama Süreci

Araştırmanın bu kısmı 3-13 Nisan 2012 tarihleri arasında 10 ceza mahkemesi ve bir sulh ceza mahkemesinde yapılan incelemelerle gerçekleştirilmiştir. Bu mahkemeler ve belirlenen dosya sayıları; 8. ve 10. Asliye Ceza Mahkemesi'nde 1'er dosya, 14. Asliye Ceza Mahkemesi'nde 3 dosya, 15. Asliye Ceza Mahkemesi'nde 3 dosya, 17. Asliye Ceza Mahkemesi'nde 1 dosya, 25. Asliye Ceza Mahkemesi'nde 5 dosya, 27. Asliye Ceza Mahkemesi'nde 5 dosya, 29. Asliye Ceza Mahkemesi'nde belirlenen 2 dosya, 31. Asliye Ceza Mahkemesi'nde 4 dosya ve 5. Sulh Ceza Mahkemesi'nde 1 dosya şeklindedir. Diğer taraftan 5. Asliye Ceza Mahkemesi'nde herhangi bir dosya tespiti yapılamamıştır.

3.4.5. İstanbul Emniyet Müdürlüğü Veri Toplama Süreci

İstanbul Emniyet Müdürlüğü'ne bağlı Bilişim Suçları ve Sistem Müdürlüğü'ndeki online bankacılık suçlarına ilişkin dosyaları incelemek için 29 Haziran 2011 tarihinde

dilekçe verilmiştir. İzin talep dilekçesi, çalışmanın Ek-B kısmında bulunmaktadır. Dilekçeye cevaben 5 Ekim 2011 tarihinde e-posta gönderilmiştir. Bilişim Suçları ve Sistem Müdürlüğü'ndeki iş yoğunluğundan ve araştırma konusu ile ilgili suçların tespitinin uzun sürmesinden dolayı dosyaların incelenmesi 2012 yılının Mart ayında yapılabilmiştir. Araştırmanın bu kısmında 11 dosya tespit edilmiştir.

3.5. VERİLERİN ANALİZİ

Araştırma sonucunda elde edilen veriler, frekanslar ve yüzdeler hesaplanarak çözümlenmiştir. Bu hesaplamalar için Microsoft Excel 2010 paket programı kullanılmıştır.

3.6. ARAŞTIRMANIN GEÇERLİĞİ

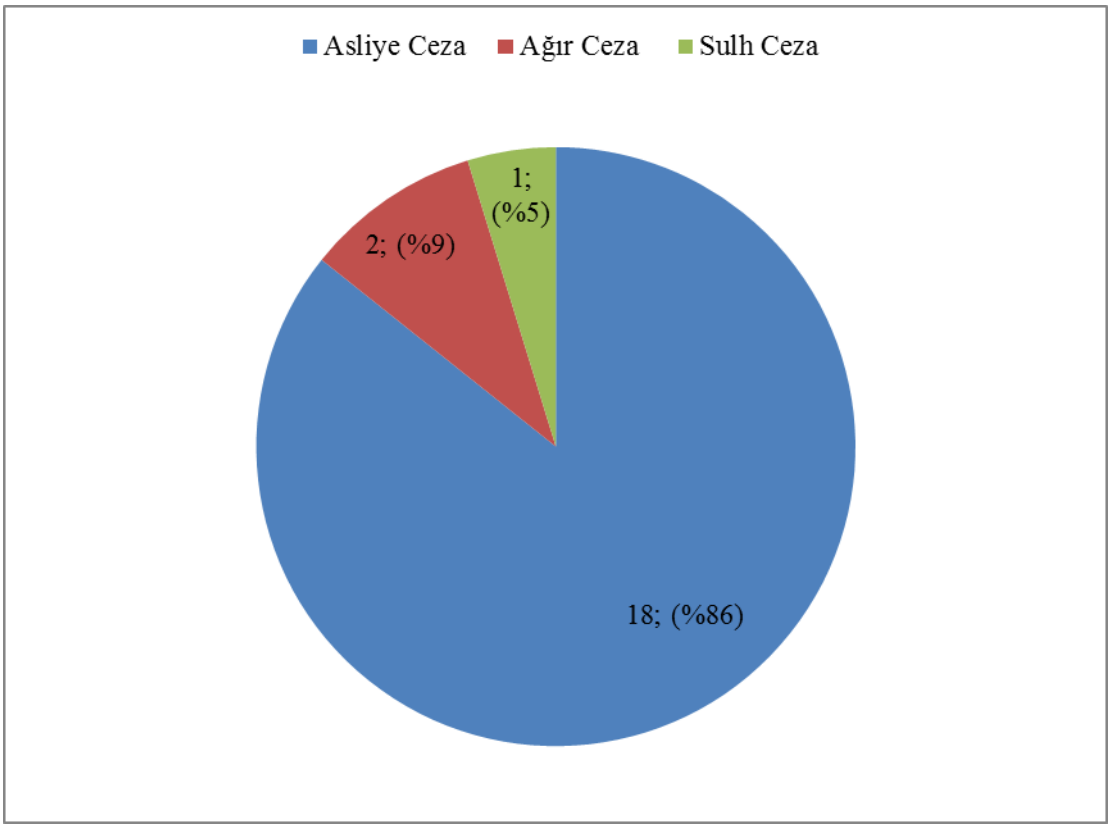
Hedeflenen verilere ulaşmak için bilişim suçları ve bilişim hukukunda uzman 5 kişinin görüşleri doğrultusunda hazırlanan "Online Bankacılık Suçları İle İlişkili Dava Dosyalarını İnceleme Anketi" kullanılmıştır.

Karasar (1999) ve Büyüköztürk (2007), örneklem içinde varılan bir sonucun gerçek dünyadaki genellenebilirlik seviyesini dış geçerlik olarak tanımlamakta ve dış gerçerliği araştırma desenlerinde karşılaşılan önemli bir sorun olarak ifade etmektedir. Bu araştırmadan elde edilen sonuçlar sınırlı bir genellemeye sahiptir. Sonuçlar, İstanbul ili ve aynı bilişim suç türü için genellenebilir.

4. BULGULAR

4.1. ARAŞTIRMA ÖRNEKLEMİNİ OLUŞTURAN MAHKEMELERİN TÜRLERİNE İLİŞKİN BULGULAR

Araştırma örnekleminin ilk kısmını İstanbul ili Bakırköy, Kadıköy, Sultanahmet ve Pendik olmak üzere 4 farklı adliyede bulunan toplam 21 mahkeme oluşturmaktadır. Araştırma örneklemini oluşturan mahkemelerin türlerine ilişkin bulgular Şekil 4.1'de verilmiştir. Bu bulgulara göre; araştırma yapılan mahkemelerin 18'i asliye ceza mahkemesi, 3'ü ağır ceza mahkemesi ve biri de sulh ceza mahkemesidir.

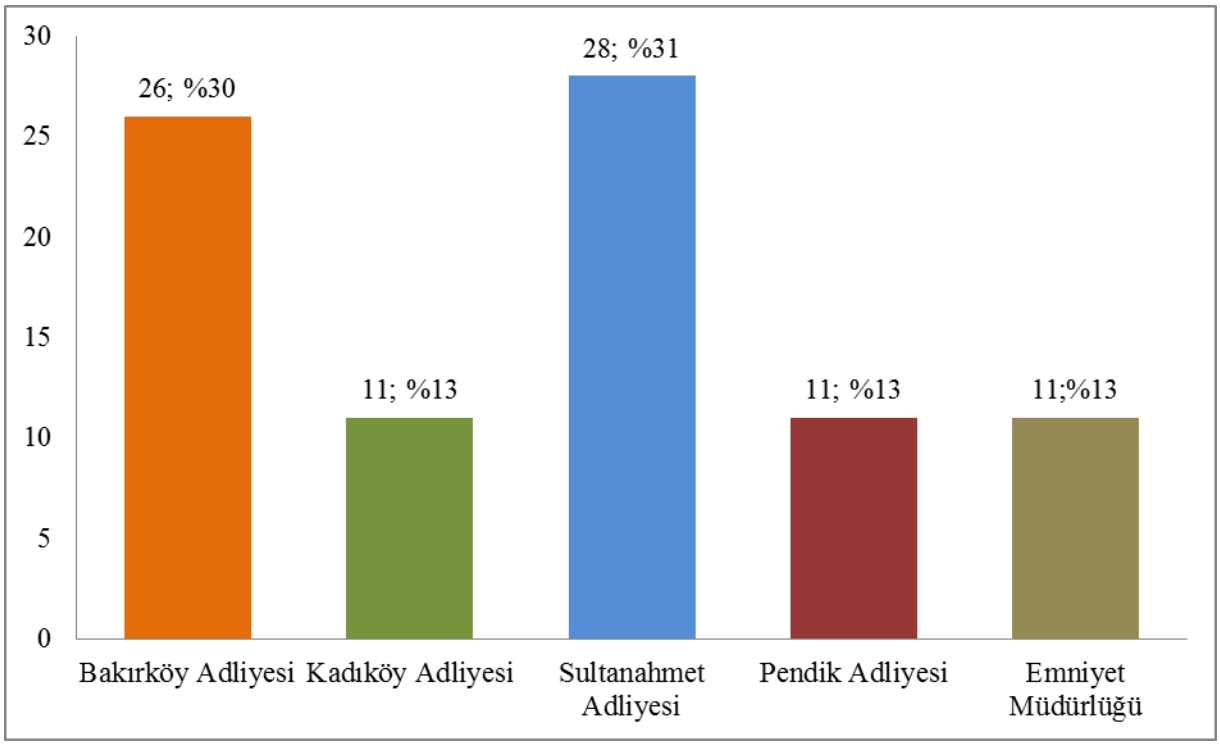


Şekil 4.1: Araştırma Örneklemini Oluşturan Mahkemelerin Türlerine İlişkin Bulgular

4.2. ERİŞİLEN SUÇ DOSYALARININ ERİŞİM YERLERİNE GÖRE DAĞILIMINA İLİŞKİN BULGULAR

Çalışma kapsamında elde edilen online bankacılık suç dosyalarının erişim yerlerine göre dağılımı Şekil 4.2'de verilmiştir. Bu dağılıma göre; erişilen toplam 87 dosyanın 28

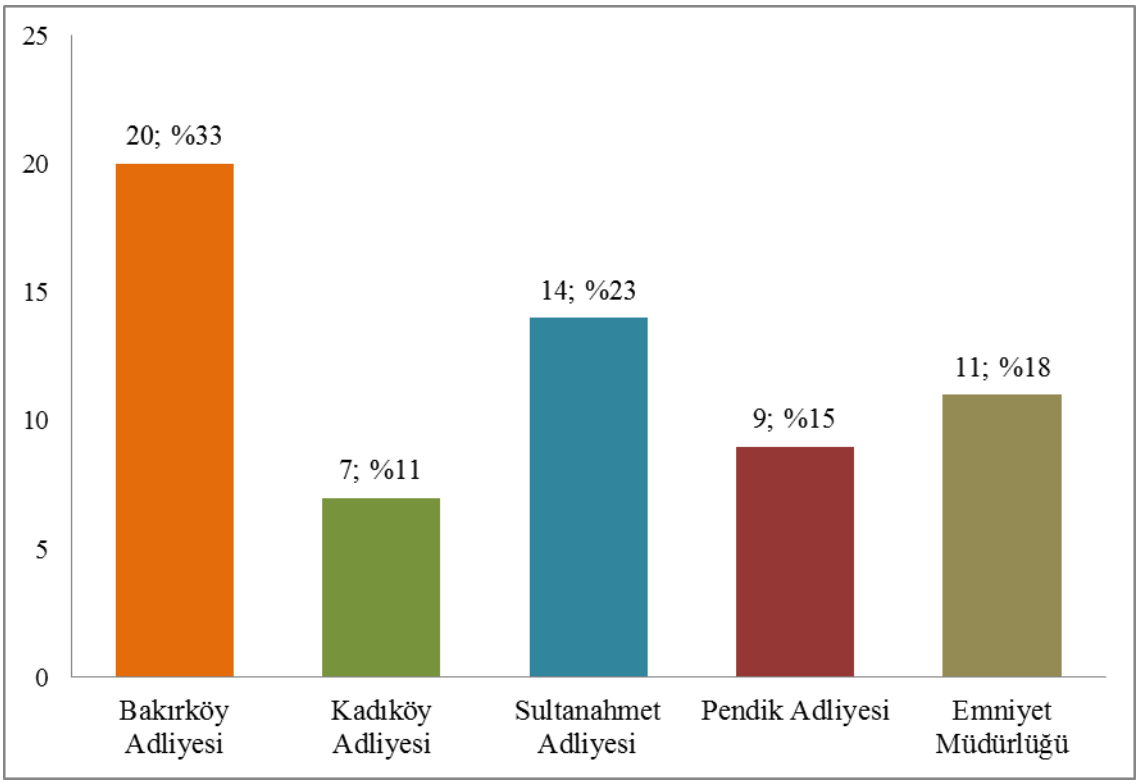
tanesi Sultanahmet Adliyesi'nde bulunmaktadır. Bakırköy Adliyesi'nde ise 26 dosyaya erişilmiştir. Kadıköy Adliyesi, Pendik Adliyesi ve Emniyet Müdürlüğü'nde 11'er dosyaya ulaşılmıştır.



Şekil 4.2: Erişilen Suç Dosyalarının Erişim Yerlerine Göre Dağılımı

Bu dosyalar arasında bulunan online bankacılık suç dosyalarının erişim yerlerine göre dağılımı ise Şekil 4.3'de verilmiştir. Bu dağılıma göre; erişilen toplam 87 dosyanın 61'i online bankacılık suçları ile ilişkilidir. Bakırköy Adliyesi'nde online bankacılık suçları ile ilgili 20 dosyaya erişilmiştir. Sultanahmet Adliyesi'nde 14 ve Emniyet Müdürlüğü'nde 11 online bankacılık suç dosyası bulunmuştur. Erişilen diğer online bankacılık suç dosyalarının dağılımı; Pendik Adliyesi'nde 9 ve Kadıköy Adliyesi'nde ise 7 olarak tespit edilmiştir.

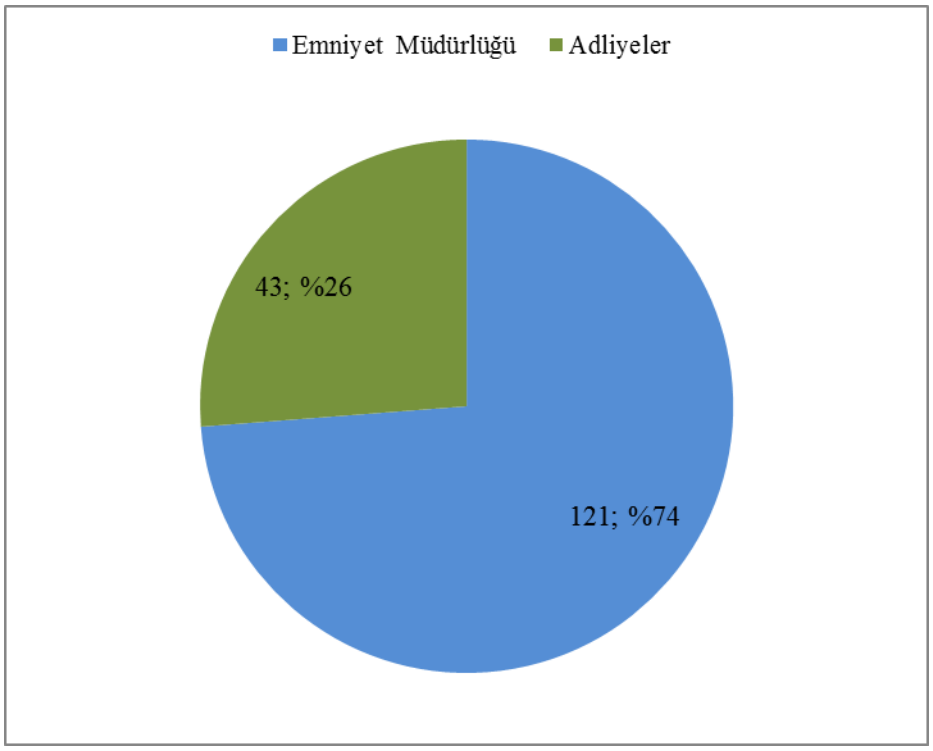
Öte yandan, elde edilen online bankacılık suç dosyalarının 7'sinin (Bakırköy Adliyesi'nde 4 dosya ve Pendik Adliyesi'ndeki 3 dosya) ilgili mahkeme kaleminde bulunmaması nedeniyle gerekli incelemeler yapılamamıştır.



Şekil 4.3: Erişilen Online Bankacılık Suç Dosyalarının Erişim Yerlerine Göre Dağılımı

4.3. İNCELENEN ONLİNE BANKACILIK SUÇ DOSYALARINDAKİ SUÇ SAYILARINA İLİŞKİN BULGULAR

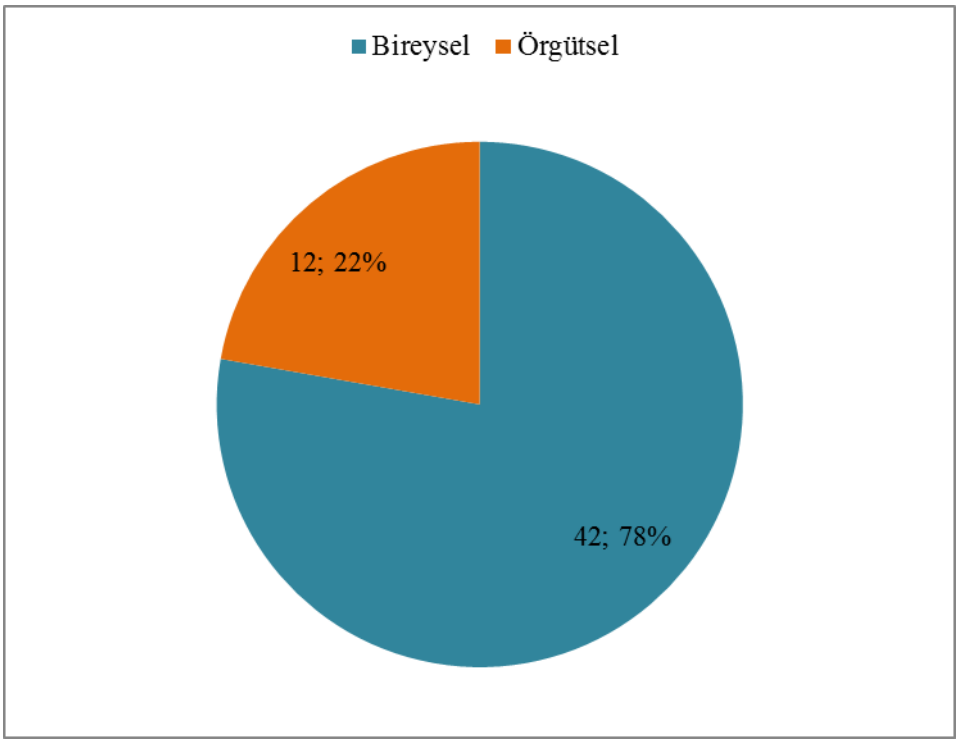
Çalışma kapsamında incelenen online bankacılık suç dosyalarındaki suç sayılarına ilişkin bulguların dağılımı Şekil 4.4'de verilmiştir. Bu dağılıma göre; örneklemdeki adliyelerde incelenen dosyalarda toplam 43 online bankacılık suçu tespit edilmiştir. Emniyet Müdürlüğü'ndeki dosyalarda birden fazla suç işlendiği dikkate alındığından toplam 121 online bankacılık suçu belirlenmiştir.



Şekil 4.4: İncelenen Online Bankacılık Suç Dosyalarındaki Suç Sayılarına İlişkin Bulgular

4.4. SUÇLARIN İŞLENME ŞEKLİNE İLİŞKİN BULGULAR

Çalışma kapsamında incelenen online bankacılık suç dosyalarındaki suçların işlenme şekline ilişkin bulguların dağılımı Şekil 4.5'de verilmiştir. Bu dağılıma göre; bireysel işlenen suç sayısı 42 olarak belirlenmiştir. Geriye kalan 12 dosyadaki suçların örgütlenmiş kişiler tarafından gerçekleştirildiği belirlenmiştir.



Şekil 4.5: Suçların İşlenme Şekline İlişkin Bulgular

4.5. İNCELENEN ONLİNE BANKACILIK SUÇ DAVALARININ DURUMUNA İLİŞKİN BULGULAR

Mahkemelerde erişilen 50 tane online bankacılık suç davaları dava durumuna göre Kararlı (sonuçlanmış), Derdest (devam eden), Yargıtay, Bilirkişi ve Zaman Aşımı başlığı altında gruplandırılmıştır. İncelenen online bankacılık suç davalarının durumuna ilişkin bulgular ve inceleme sonucu elde edilen veriler Tablo 4.1'de gösterilmiştir.

Bu verilere göre; Bakırköy Adliyesi'ndeki online bankacılık dosyaları 5'i kararlı, 12'si derdest, 1'i Yargıtay'da ve 1'i de bilirkişide olan dosyalardır.

Kadıköy Adliyesi'nde derdest dosya sayısı 7, kararlı dosya sayısı 2'dir. Sultanahmet Adliyesi'ndeki kararlı dosyalar 12 olup dosyaların büyük çoğunluğunu oluşturmaktadır. Bu adliyede, birer tane Yargıtay'da olan dosya ve zaman aşımına uğrayan dosya bulunmaktadır. Pendik Adliyesi'nde ise derdest dosya sayısı (7 tane) diğerlerine göre fazla sayıdadır. Bu adliyede, 1'er kararlı ve Yargıtay'da olan dosya tespit edilmiştir.

Tablo 4.1'deki dağılıma göre toplam 20 dosyanın kararlı olup sonuçlandığı, 24 dosyanın derdest olup devam ettiği, 3 dosyanın Yargıtay'a gönderildiği, 1 dosyanın bilirkişide olduğu ve 1 dosyanın da zaman aşımına uğrayarak kapatıldığı belirlenmiştir.

Tablo 4.1: İncelenen Online Bankacılık Suç Davalarının Durumuna İlişkin Bulgular

Dava durumu / Yer	Kararlı Dosya	Derdest	Yargıtay	Bilirkişi	Zaman Aşımı
Bakırköy Adliyesi	5	12	1	1	-
Kadıköy Adliyesi	2	5	-	-	-
Sultanahmet Adliyesi	12	-	1	-	1
Pendik Adliyesi	1	7	1	-	-
Toplam	**20 (%41)**	**24 (%49)**	**3 (%6)**	**1 (%2)**	**1 (%2)**

4.5.1. Kararlı Dava Dosyalarının Sonuçlarına İlişkin Bulguların Adliyelere Göre Dağılımı

Toplam 20 adet kararlı dava dosyasının sonuçlarına ilişkin bulguların adliyelere göre dağılımı Tablo 4.2'de verilmiştir. Bu dağılıma göre; Bakırköy Adliyesi'ndeki 5 kararlı dosyanın hepsi beraat ile sonuçlanmıştır. Kadıköy Adliyesi'nde de kararlı dosyalarda bulunan sanıklar hakkında beraat kararı verilmiştir. Pendik Adliyesi'ndeki karara bağlanan dosyada ise verilen ceza ertelenmiştir. Sultanahmet Adliyesi'ndeki 12 kararlı dosyanın 2'si mahkumiyet, 6'sı beraat, 3'ü mahkumiyet&beraat ve 1'i de cezanın ertelenmesi ile neticelenmiştir.

Tablo 4.2'deki verilere göre; 13 dosya beraatle, 2 dosya mahkumiyetle, 2 dosya cezanın ertelenmesiyle ve 3 dosya mahkumiyet&beraat ile sonuçlanmıştır.

Tablo 4.2: Kararlı Dosyalara İlişkin Bulguların Adliyelere Göre Dağılımı

Karar Tipi / Adliye	Mahkumiyet	Beraat	Erteleme	Mahkumiyet&Beraat
Bakırköy Adliyesi	-	5	-	-
Kadıköy Adliyesi	-	2	-	-
Sultanahmet Adliyesi	2	6	1	3
Pendik Adliyesi	-	-	1	-
Toplam	**2 (%10)**	**13 (%65)**	**2 (%10)**	**3 (%15)**

4.5.1.1. Kararlı Dava Dosyalarında Sanıklara Verilen Hapis Cezalarına İlişkin Bulguların Adliyelere Göre Dağılımı

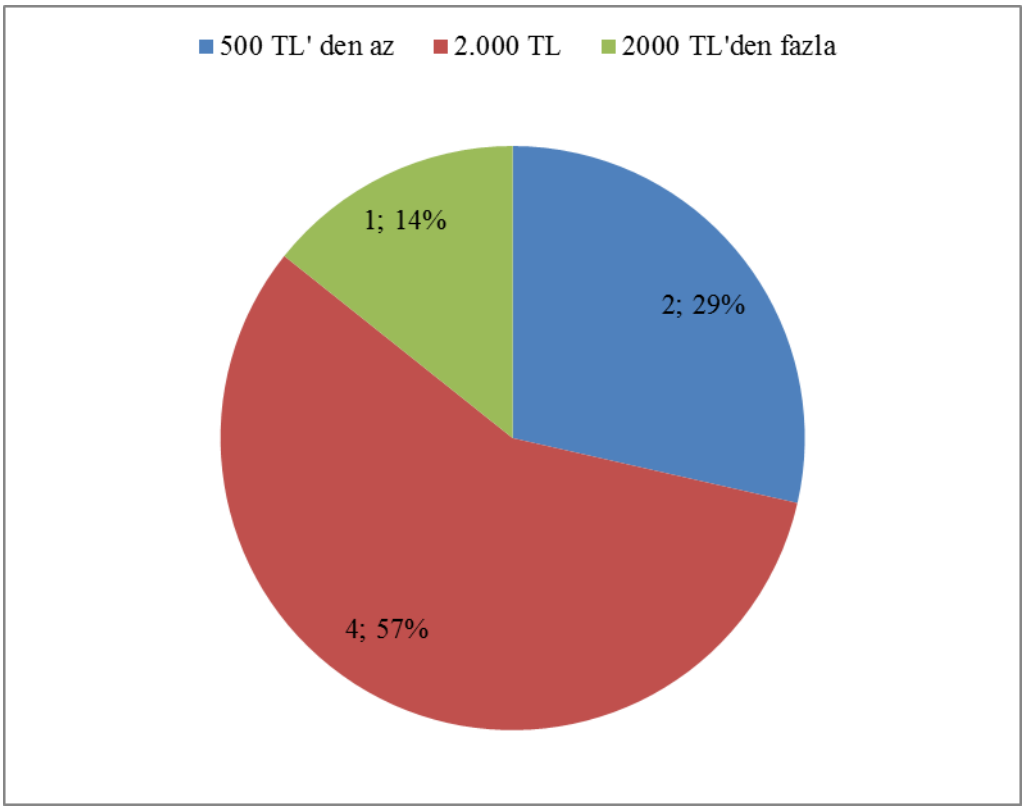
Çalışma kapsamında incelenen kararlı dava dosyalarında sanıklara verilen hapis cezalarına ilişkin bulguların adliyelere göre dağılımı Tablo 4.3'de verilmiştir. Bu dağılıma göre, hapis cezası ile sonuçlanan dosya sayısı 7 olarak tespit edilmiştir. Söz konusu dosyalarda toplam 8 sanığa hapis cezası verilmiştir. Dosyaların 5'inde 24 – 36 ay arası ve 2'sinde 36 aydan fazla hapis cezası verilmiştir. Bu davaların tamamının Sultanahmet Adliyesi'ndeki dosyalar arasında olduğu belirlenmiştir. Diğer taraftan, 24 aydan az hapis cezası verilen dosyanın Pendik Adliyesi'nde olduğu tespit edilmiştir.

Tablo 4.3: Kararlı Dava Dosyalarında Sanıklara Verilen Cezalara İlişkin Bulguların Adliyelere Göre Dağılımı

Ceza Süreleri (Ay) / **Yer**	**24 aydan az**	**24-36 ay arası**	**36 aydan fazla**
Sultanahmet Adliyesi	-	5	2
Pendik Adliyesi	1	-	-
Toplam	**1 (%12)**	**5 (%63)**	**2 (%25)**

4.5.1.2. Kararlı Dava Dosyalarında Sanıklara Verilen Adli Para Cezalarına İlişkin Bulgular

Çalışma kapsamında incelenen kararlı dava dosyalarında sanıklara verilen adli para cezalarına ilişkin bulgular Şekil 4.6'da verilmiştir. Bu verilere göre; toplam 7 kararlı dosyada adli para cezası verilmiştir. Verilen adli para cezası, 500 Türk Lirası'nın (TL) altında olan 2 dosya ve 2000 TL olan 4 dosya olduğu tespit edilmiştir. Bir dosyada ise 2000 TL'nin üstünde bir adli para cezası verilmiştir. Ayrıca adli para cezası verilen dava dosyalarının tamamının Sultanahmet Adliyesi'nde olduğu tespit edilmiştir.



Şekil 4.6: Kararlı Dava Dosyalarında Sanıklara Verilen Adli Para Cezalarına İlişkin Bulgular

4.5.2. Kararlı Dava Dosyalarında Dava Sürelerine İlişkin Bulguların Dava Durumuna Göre Dağılımı

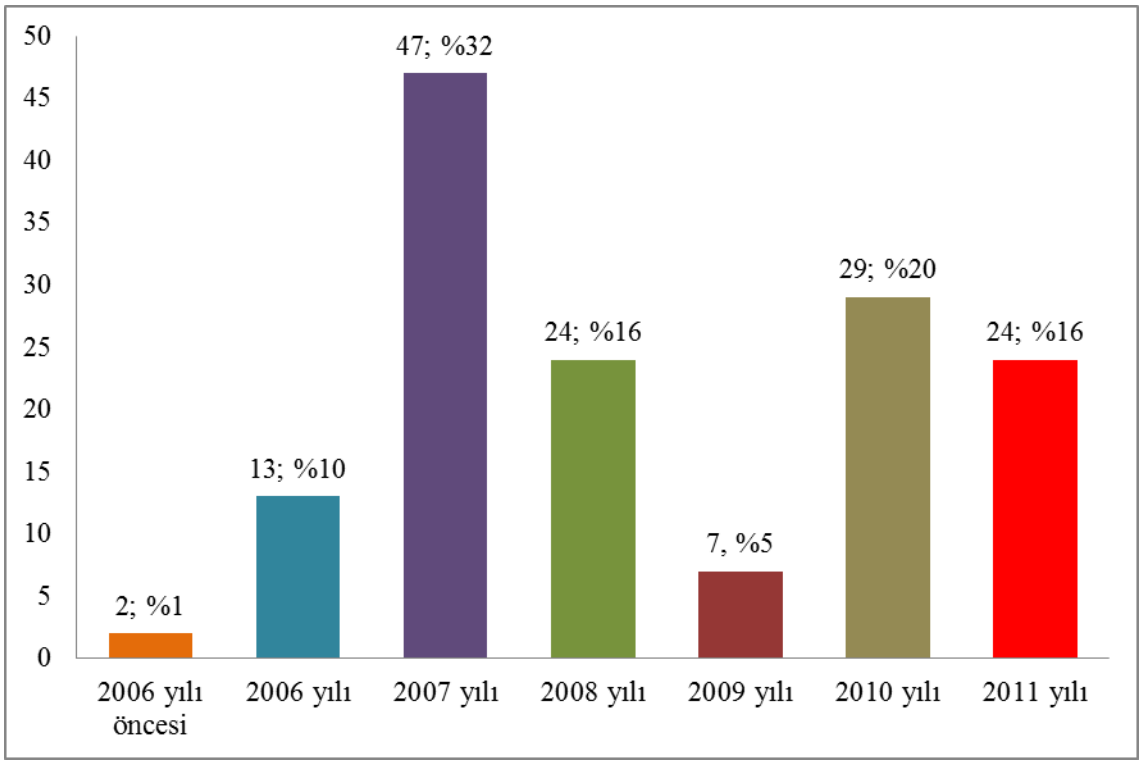
Kararlı dava dosyalarında dava sürelerine ilişkin bulguların dava durumuna göre dağılımı Tablo 4.4'de verilmiştir. Bu dağılıma göre; 7 davanın 7-12 ay arası bir sürede sonuçlandığı belirlenmiştir. Bu davaların 4'ü beraat, 1'i erteleme, 2'si de mahkumiyet&beraat ile sonuçlanarak karara bağlanmıştır. 13-18 ay ve 19-24 ay arası süren davalar 4'er tane olarak tespit edilmiş ve hepsinin beraat ile sonuçlandığı belirlenmiştir. Mahkumiyet, beraat, erteleme ve mahkumiyet&beraat ile sonuçlanan davalardan 1'er tane olmak üzere toplam 4 davanın 24 aydan fazla sürdüğü anlaşılmıştır.

Tablo 4.4: Kararlı Dava Dosyalarında Dava Sürelerine İlişkin Bulguların Dava Durumuna Göre Dağılımı

Dava Süresi (Ay) / Karar Tipi	0-6	7-12	13-18	19-24	24 aydan fazla
Mahkûmiyet	1	-	-	-	1
Beraat	-	4	4	4	1
Erteleme	-	1	-	-	1
Mahkûmiyet&Beraat	-	2	-	-	1
Toplam	**1 (%5)**	**7 (%35)**	**4 (%20)**	**4(%20)**	**4 (%20)**

4.6. İNCELENEN ONLİNE BANKACILIK SUÇLARINDAKİ SUÇ TARİHLERİNE İLİŞKİN BULGULARIN YILLARA GÖRE DAĞILIMI

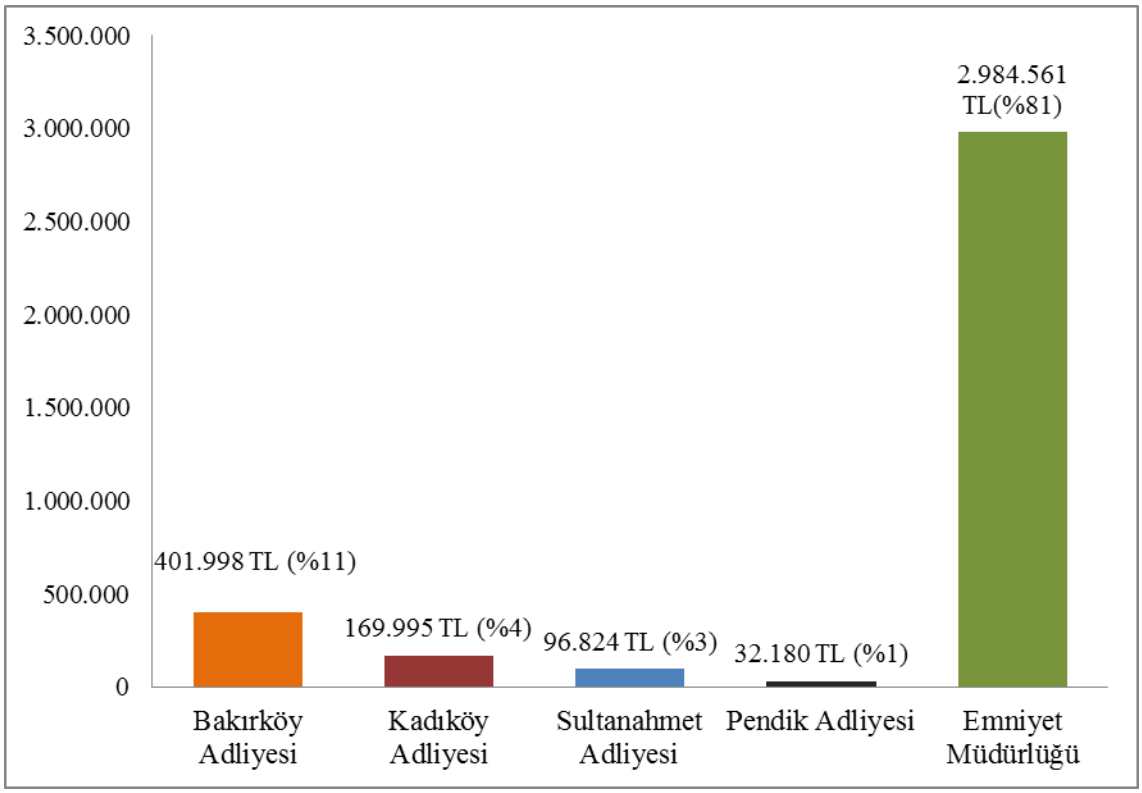
Çalışma kapsamında incelenen online bankacılık suçlarındaki suç tarihlerine ilişkin bulguların yıllara göre dağılımı Şekil 4.7'de verilmiştir. Bu dağılıma göre; suçların 2'si 2006 yılı öncesinde ve 13'ü 2006 yılında gerçekleşmiştir. Suçların 47 ise 2007 yılında gerçekleşmiştir. Bununla beraber, 2010 yılında işlenen suç sayısı 29 olarak tespit edilmiştir. Suçların 24'er tanesi 2008 ve 2011 yıllarında gerçekleşmiştir. Geriye kalan 7 suçun 2009 yılında gerçekleştiği tespit edilmiştir.



Şekil 4.7: İncelenen Online Bankacılık Suçlarındaki Suç Tarihlerine İlişkin Bulguların Yıllara Göre Dağılımı

4.7. SUÇA KONU OLAN PARANIN MİKTARINA İLİŞKİN BULGULAR

Suça konu olan para miktarı; dolandırıcıların başka hesaba aktardığı veya aktarmaya çalıştığı paranın değerini ifade etmek için kullanılmıştır. Çalışma kapsamında incelenen online bankacılık suçlarına konu olan para miktarlarına ilişkin bulgular Şekil 4.8'de verilmiştir. Bu bulgulara göre; suça konu olan toplam para miktarı 3 milyon 700 bin TL'dir. Bu miktarın büyük bir kısmını Emniyet Müdürlüğü'ndeki örgütsel suçlarda tespit edilen yaklaşık 3 milyon TL oluşturmuştur. Bakırköy Adliyesi'nde incelenen suçlara konu olan para miktarı yaklaşık 402 bin TL'dir. Kadıköy Adliyesi'ndeki 170 bin TL'ye yakın bir miktar paranın suça konu olduğu belirlenmiştir. Sultanahmet Adliyesi'nde 100 bin TL ve Pendik Adliyesi'nde 32 bin TL civarında bir rakam suçun konusu olmuştur.



Şekil 4.8: Suça Konu Olan Paranın Miktarına İlişkin Bulgular

Suça konu olan para miktarına ilişkin bulguların miktar aralığına göre dağılımı ise Tablo 4.5'de verilmiştir. Bu dağılıma göre para miktarı 1.000 ila 10.000 TL arasında bulunan; Bakırköy Adliyesi'nde 9, Kadıköy Adliyesi'nde 3, Sultanahmet Adliyesi'nde 9, Pendik Adliyesi'nde 4 ve Emniyet Müdürlüğü'nde 1 olmak üzere toplam 26 dosya belirlenmiştir. Bu kategoriyi, para miktarı 10.000 TL'den fazla olan 23 suç dosyası takip etmiştir. Bu miktar aralığının bulunduğu yere göre dağılımı; Bakırköy Adliyesi'nde 5, Kadıköy Adliyesi'nde 3, Sultanahmet Adliyesi'nde 3, Pendik Adliyesi'nde 2 ve Emniyet Müdürlüğü'nde 10 dosya şeklinde tespit edilmiştir.

Tablo 4.5: Suça Konu Olan Para Miktarına İlişkin Bulguların Miktar Aralığına Göre Dağılımı

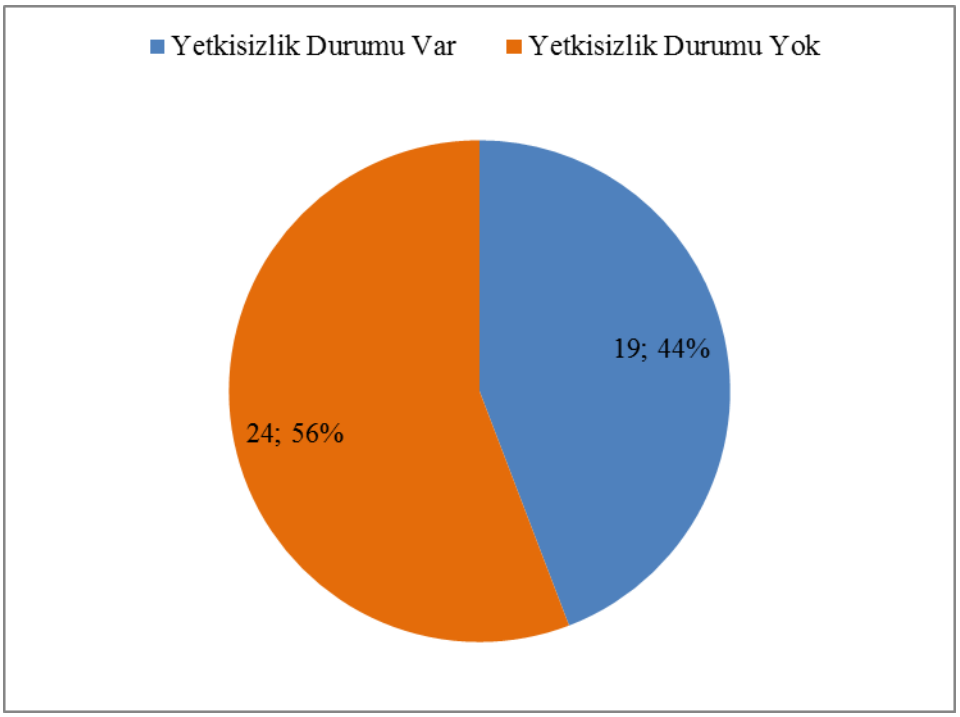
Para Miktarı (TL) / **Yer**	**1.000'den az**	**1.000 ile 10.000 arası**	**10.000'den fazla**
Bakırköy Adliyesi	1	9	5
Kadıköy Adliyesi	1	3	3
Sultanahmet Adliyesi	2	9	3
Pendik Adliyesi	1	4	2
Emniyet Müdürlüğü	-	1	10
Toplam	**5 (% 9)**	**26 (% 48)**	**23 (% 43)**

1.000 TL'den az bir parayı hedefleyen dolandırıcıların bulunduğu dosya sayısı ise 5 ile sınırlı kalmıştır. Bu dosyalar; Bakırköy, Kadıköy, Pendik Adliyelerinde 1'er dosya, Sultanahmet Adliyesi'nde 2 dosya şeklinde dağılım göstermiştir.

4.8. YETKİSİZLİK DURUMU OLUŞAN DAVALARIN SAYILARINA İLİŞKİN BULGULAR

Online bankacılık suçlarına ilişkin davalar, suçun işlediği yer konusundaki yetkisizlikten dolayı dava sürecinde bir Cumhuriyet Başsavcılığı'ndan başka bir Cumhuriyet Başsavcılığı'na gönderilebilmektedir.

Çalışma kapsamında yetkisizlik durumu oluşan davaların sayılarına ilişkin bulgular Şekil 4.9'da verilmiştir. Bu bulgulara göre; incelenen toplam 43 dosya içerisinde 19'unda yetkisizlik durumu oluşmuştur. Geriye kalan 24 dosyada yetkisizlik durumu tespit edilmemiştir.



Şekil 4.9: Yetkisizlik Durumu Oluşan Davaların Sayılarına İlişkin Bulgular

4.9. DAVALARIN HAZIRLIK SÜRELERİNE İLİŞKİN BULGULARIN ADLİYELERE GÖRE DAĞILIMI

Davaların hazırlık süresi; şikâyetçinin Cumhuriyet Başsavcılığı'na verdiği dilekçenin tarihi ile davanın başlangıç tarihleri arasında geçen süreyi ifade etmektedir. Çalışma kapsamında davaların hazırlık sürelerine ilişkin bulguların adliyelere göre dağılımı Tablo 4.6'da verilmiştir. Bu dağılıma göre; davaların 2'si 0-6 ay arası bir sürede hazırlanmıştır. Bu davalar Bakırköy ve Kadıköy Adliyesi'nde bulunmaktadır. 8 davanın hazırlık süresi 6-12 ay arasında sürmüştür. Bu davaların 4 tanesi Bakırköy Adliyesi'nde diğer 4 tanesi ise Sultanahmet Adliyesi'nde bulunmaktadır.

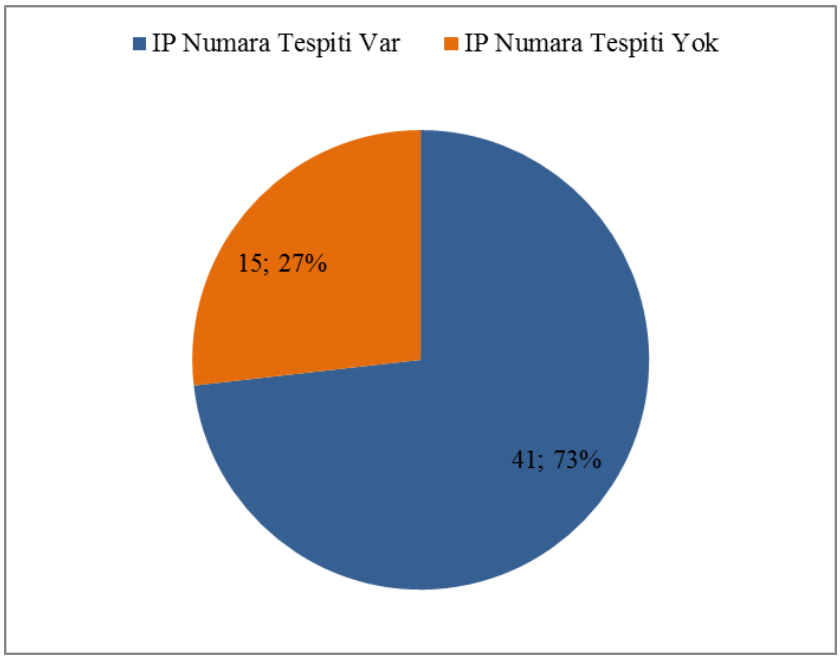
Hazırlık aşaması 24-36 ay arası süren dava sayısı; Bakırköy Adliyesi'nde 7, Kadıköy Adliyesi'nde 1, Sultanahmet Adliyesi'nde 3 ve Pendik Adliyesi'nde 1 olmak üzere 12 olarak tespit edilmiştir. Hazırlık aşaması 36 ay ve 36'dan fazla olan dava sayısı 8 olarak belirlemiştir. Bu davalar bulunduğu yer bakımından; Bakırköy Adliyesi 1, Kadıköy Adliyesi 4, Sultanahmet Adliyesi 1 ve Pendik Adliyesi 2 şeklinde bir dağılım göstermiştir.

Tablo 4.6: Davaların Hazırlık Sürelerine İlişkin Bulguların Adliyelere Göre Dağılımı

Süre (ay) / Yer	**0-6**	**6-12**	**12-24**	**24-36 arası**	**36 ve üzeri**
Bakırköy Adliyesi	1	4	4	7	1
Kadıköy Adliyesi	1	-	1	1	4
Sultanahmet Adliyesi	-	4	6	3	1
Pendik Adliyesi	-	-	3	1	2
Toplam	**2 (%5)**	**8 (%18)**	**14 (%32)**	**12 (%27)**	**8 (%18)**

4.10. IP NUMARALARININ TESPİTİNE İLİŞKİN BULGULAR

IP numarası, suça konu olan para başka hesaba aktarılırken kullanılan internet hattının kime ait olduğunu ve hattın bulunduğu yeri tespit etmek için gerekli bir bilgidir. Araştırmada elde edilen IP numaralarının tespitine ilişkin bulgular Şekil 4.10'da verilmiştir. Bu bulgulara göre; IP numarası tespit edilen 41 olay belirlenmiştir. 15 olayda ise IP numarası tespit edilememiştir. Bazı olaylarda parayı aktarmak için birden fazla internet bağlantısı kullanılmıştır. Bundan dolayı IP numaralarının tespit durumu ile ilgili bulgu sayısı toplamda 56 olarak belirlenmiştir.



Şekil 4.10: IP Numaralarının Tespitine İlişkin Bulgular

Tespiti yapılan IP numaralarının adreslerine ilişkin bulgular ise Tablo 4.7'de verilmiştir. Bu bulgulara göre; 27 IP numarasının adresinin ev olduğu tespit edilmiştir. IP numaralarının 4'ünün adresi internet kafe olarak belirlenmiştir. IP numaralarının 9'unun adresi belirlenememiştir. Geriye kalan IP numarasının adresi ise işyeri olarak belirlenmiştir.

Tablo 4.7: Tespiti Yapılan IP Numaralarının Adreslerine İlişkin Bulgular

		Frekans
Adres	Ev	27 (%66)
	İnternet Kafe	4 (%10)
	İşyeri	1 (%2)
	Belirsiz	9 (%22)
Konum	Yurtiçi	30
	Yurtdışı	2

Tablo 4.7'ye göre, adresi belirlenen IP numaralarının 30'u yurtiçinde bulunmaktadır. Bir adres ABD diğeri Hollanda olmak üzere 2 adresin konumu yurtdışı olarak tespit edilmiştir.

4.11. SUÇA MÜDAHİL OLAN KİŞİLERİN DEMOGRAFİK ÖZELLİKLERİNE İLİŞKİN BULGULARIN ERİŞİLEN YERLERE GÖRE DAĞILIMI

Çalışmada suça müdahil olan kişilerin demografik özelliklerine ilişkin bulguların erişilen yerlere göre dağılımı Tablo 4.8'de verilmiştir. Bu dağılıma göre; incelenen dosyalarda Bakırköy Adliyesi 40 kişi, Kadıköy Adliyesi 15 kişi, Sultanahmet Adliyesi 30, Pendik Adliyesi 6 ve Emniyet Müdürlüğü 142 kişi olmak üzere toplam 334 erkek birey suça karışmıştır. Suça müdahil olan kadın sayısı 24 olarak tespit edilmiştir. Bu sayıların dosyaların bulunduğu yere göre dağılımı ise; Bakırköy Adliyesi 4 kişi, Kadıköy Adliyesi 1 kişi, Sultanahmet Adliyesi 4 kişi, Pendik Adliyesi 2 kişi ve Emniyet Müdürlüğü 13 kişi şeklinde belirlenmiştir. Emniyet Müdürlüğü'nde suça müdahil olan kişi sayısının fazla olmasının sebebi örgütsel suçlardan kaynaklanmıştır.

Tablo 4.8: Suça Müdahil Olan Kişilerin Demografik Özelliklerine İlişkin Bulguların Erişilen Yerlere Göre Dağılımı

Cinsiyet / Yer	Erkek	Kadın	Toplam
Bakırköy Adliyesi	41	4	**45* (%13)**
Kadıköy Adliyesi	15	1	**16* (%4)**
Sultanahmet Adliyesi	30	4	**34* (%10)**
Pendik Adliyesi	6	2	**8* (%2)**
Emniyet Müdürlüğü	242	13	**255** (%71)**
Toplam	**334 (%93)**	**24 (%7)**	**358**

*İncelenen dava dosyalarındaki suça müdahil olan kişiler sanık olarak tanımlanmaktadır.

**Emniyet Müdürlüğündeki dosyalarda suça müdahil olan kişiler şüpheli olarak nitelendirilmektedir.

4.11.1. Suça Müdahil Olan Kişilerin Yaş Aralıklarının Cinsiyete Göre Dağılımı

Çalışma kapsamında suça müdahil olan kişilerin yaş aralıklarının cinsiyete göre dağılımı Tablo 4.9'da verilmiştir. Bu dağılıma göre; suça karışan yaşı 26'dan küçük bireylerin 24'ü erkek 3'ü ise kadın olarak tespit edilmiştir. Yaş aralığı 26-35 olan bireylerin 142'si erkek, 5'i kadın olduğu belirlenmiştir. Suça müdahil olan 118 erkeğin ve 11 kadının 36-45 yaş aralığında bulunduğu tespit edilmiştir. 46-60 yaş aralığında ise 38 erkek ve 5 kadın bulunmuştur. Suça müdahil olan ve yaşı 61'den büyük olan 7 erkek birey olduğu anlaşılmıştır. Öte yandan suça müdahil olan ve yaşı hakkında bilgi sahibi olunamayan 5 birey tespit edilmiştir.

Tablo 4.9: Suça Müdahil Olan Kişilerin Yaş Aralıklarının Cinsiyete Göre Dağılımı

Yaş Aralığı / Cinsiyet	26'dan küçük	26-35	36-45	46-60	61'den büyük	Belirsiz	Toplam
Erkek	24	142	118	38	7	5	**334**
Kadın	3	5	11	5	-	-	**24**
Toplam	**27 (%8)**	**147 (%41)**	**129 (%36)**	**43 (%12)**	**7 (%2)**	**5 (%1)**	**358**

4.11.2. Emniyet Müdürlüğü'ndeki Dosyalarda Suça Müdahil Olan Kişilerin Sabıka Durumlarının Cinsiyete Göre Dağılımı

Araştırmada Emniyet Müdürlüğü'ndeki dosyalarda suça müdahil olan kişilerin sabıka durumlarının cinsiyete göre dağılımı Tablo 4.10'da verilmiştir. Bu dağılıma göre; suça müdahil olan erkek bireylerin 91'inin sabıkalı, 69'unun sabıkasız, 82'sinin ise sabıka durumunun belirsiz olduğu tespit edilmiştir. Bununla birlikte suça müdahil olan kadın bireyin; 1'inin sabıkalı, 6'sının sabıkasız olduğu anlaşılmıştır. Diğer 6 kadın bireyin sabıka durumu hakkında ise herhangi bir bilgi bulunmamaktadır.

Tablo 4.10: Emniyet Müdürlüğü'ndeki Dosyalarda Suça Müdahil Olan Kişilerin Sabıka Durumlarının Cinsiyete Göre Dağılımı

Sabıka Durumu / Cinsiyet	Sabıkalı	Sabıkasız	Belirsiz
Erkek	91 (%38)	69 (%28)	82 (%36)
Kadın	1 (%8)	6 (%46)	6 (%46)

4.11.3. Emniyet Müdürlüğü'ndeki Dosyalarda Suça Müdahil Olan Kişilerin Soruşturma Sürecindeki Durumlarının Cinsiyete Göre Dağılımı

Araştırmada Emniyet Müdürlüğü'ndeki dosyalarda suça müdahil olan kişilerin soruşturma sürecindeki durumlarının cinsiyete göre dağılımı Tablo 4.11'de verilmiştir. Bu dağılıma göre; suça müdahil olan erkek bireylerin 103'ünün yakalandığı, 71'inin kaçak durumda olduğu, 18'inin ifadesinin alınıp serbest bırakıldığı ve bir erkek bireyin yakalanması için emir verildiği tespit edilmiştir. Ayrıca 41 erkek bireyin soruşturma sürecindeki durumu ile ilgili bilgi edinilememiştir.

Suça müdahil olan kadın bireylerin soruşturma sürecindeki durumu hakkında 7'sinin yakalandığı, 1'inin tutuklu olduğu bilgileri mevcuttur. Fakat 5 kadın bireyin durumu hakkında herhangi bir bilgiye ulaşılamamıştır.

Tablo 4.11: Emniyet Müdürlüğü'ndeki Dosyalarda Suça Müdahil Olan Kişilerin Soruşturma Sürecindeki Durumlarının Cinsiyete Göre Dağılımı

Durum / Cinsiyet	Yakalama Emri	Yakalandı	Firar	Tutuklu	Bırakıldı	Belirsiz
Erkek	1 (%1)	103 (%43)	71 (%29)	18 (%8)	8 (%3)	41 (%16)
Kadın	-	7 (%54)	-	1 (%8)	-	5 (%38)

4.12. MAĞDURLARIN DEMOGRAFİK ÖZELLİKLERİNE İLİŞKİN BULGULARIN ERİŞİLEN YERLERE GÖRE DAĞILIMI

Çalışmada tespit edilen mağdurların demografik özelliklerine ilişkin bulguların erişilen yerlere göre dağılımı Tablo 4.12'de verilmiştir. Bu dağılıma göre; Bakırköy Adliyesi'nde 9, Kadıköy Adliyesi'nde 4, Sultanahmet Adliyesi'nde 13, Pendik Adliyesi'nde 3 ve Emniyet Müdürlüğü'nde 74 kişi olmak üzere toplam 103 erkek bireyin mağdur durumda olduğu tespit edilmiştir.

Mağdur olan kadın sayısı ise 26 olarak belirlenmiştir. Bu sayının dosyaların bulunduğu yerlere göre dağılımı ise; Bakırköy Adliyesi 2, Kadıköy Adliyesi 2, Pendik Adliyesi 2 ve Emniyet Müdürlüğü 20 kişi şeklindedir. Bunun yanında, dolandırıcıların hedeflerinde şirket, banka gibi tüzel kişilerin de olduğu tespit edilmiştir. Dolandırıcıların, Bakırköy Adliyesi'nde 7, Kadıköy Adliyesi'nde 1, Sultanahmet Adliyesi'nde 1, Pendik Adliyesi'nde 2 ve Emniyet Müdürlüğü'nde 38 olmak üzere toplam 49 tüzel kişiliği hedef aldıkları belirlenmiştir.

Tablo 4.12: Mağdurların Demografik Özelliklerine İlişkin Bulguların Erişilen Yerlere Göre Dağılımı

Nitelik / Yer	Birey		Tüzel Kişilik	Toplam
	Erkek	Kadın		
Bakırköy Adliyesi	9	2	7	18
Kadıköy Adliyesi	4	2	1	7
Sultanahmet Adliyesi	13	-	1	14
Pendik Adliyesi	3	2	2	7
Emniyet Müdürlüğü	74	20	38	132
Toplam	**103 (%58)**	**26 (%15)**	**49 (%27)**	**178**

Çalışmada tespit edilen mağdur kişilerin yaş aralıklarının cinsiyete göre dağılımı ise Tablo 4.13'de verilmiştir. Bu dağılıma göre; mağdur durumdaki erkek bireylerin 6'sının 26-35, 13'ünün 36-45, 11'inin 45-60 yaş aralığında olduğu belirlenmiştir. 60 yaş üstünde ise sadece bir erkek bireyin olduğu belirlenmiştir. Kadın mağdurların yaş aralık dağılımı ise; 26-35 arası 2, 36-45 arası 1, 45-60 arası 1 şeklindedir. Mağdur durumda olan 22 kadın ve 72 erkek bireyin yaşları hakkında ise bilgi elde edinilememiştir.

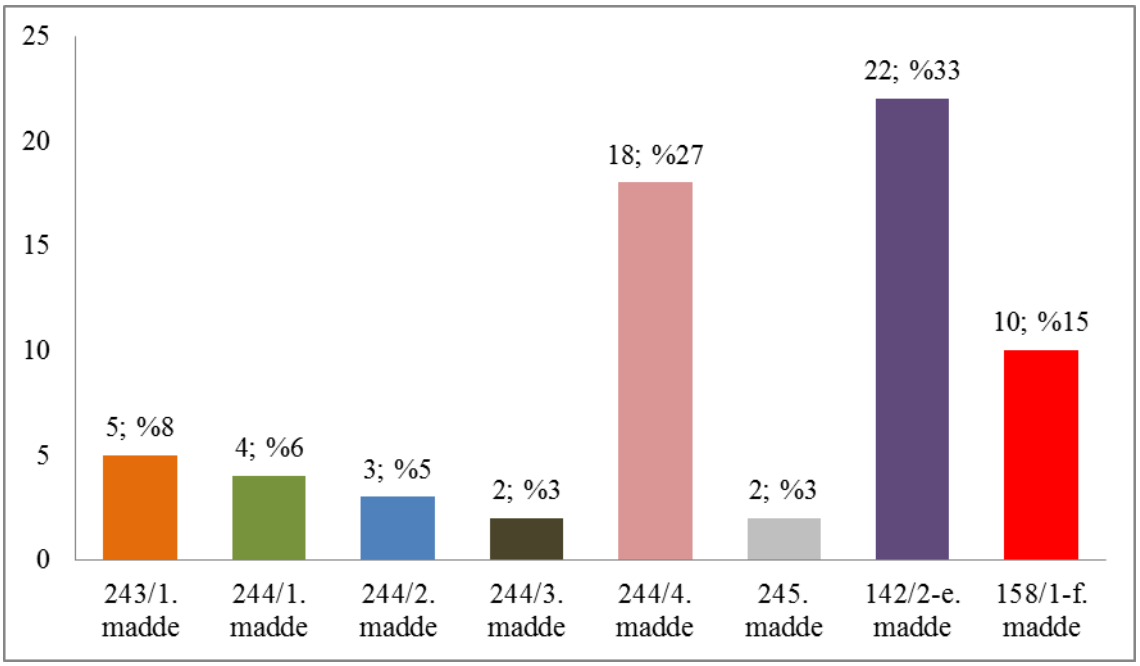
Tablo 4.13: Mağdur Kişilerin Yaş Aralıklarının Cinsiyete Göre Dağılımı

Yaş Aralığı / Cinsiyet	26-35	36-45	45-60	60'dan büyük	Belirsiz
Erkek	6	13	11	1	72
Kadın	2	1	1	-	22
Toplam	**8 (%6)**	**14 (%11)**	**12 (%9)**	**1 (%1)**	**94 (%73)**

4.13. SUÇA KONU OLAN TCK'DAKİ BİLİŞİM SUÇLARI MADDELERİNE İLİŞKİN BULGULAR

Çalışmada incelenen online bankacılık suçlarına ilişkin dosyalarda suça konu olan TCK'daki bilişim suçları maddelerine ilişkin bulgular Şekil 4.11'de verilmiştir. Bu bulgulara göre; bilişim sistemlerini kullanmak suretiyle yapılan hırsızlık eylemi hakkında olan TCK'nın 142/2-e maddesinin, 22 kez suça konu olduğu tespit edilmiştir. Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçuna ait cezanın açıklandığı TCK'nın 244/4 fıkrasının 18, bilişim sistemleri yoluyla nitelikli dolandırıcılık maddesi olan 158/1-f maddesinin 10, bilişim sistemine girme suçunu belirten 243/1 maddesinin ise 5 kez suça konu olduğu belirlenmiştir.

Bunların dışında; bilişim sisteminin işleyişini engelleyen veya bozan kişi hakkındaki cezayı açıklayan TCK'nın 244/1 maddesi 4 kez, bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi hakkındaki cezayı açıklayan 244/2 maddesi 3 kez, 244/1-2 fıkrasındaki fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde verilecek cezayı açıklayan 244/3 maddesi 2 kez suça konu olmuştur. 245. maddenin ise 2 kez suça konu olduğu belirlenmiştir.

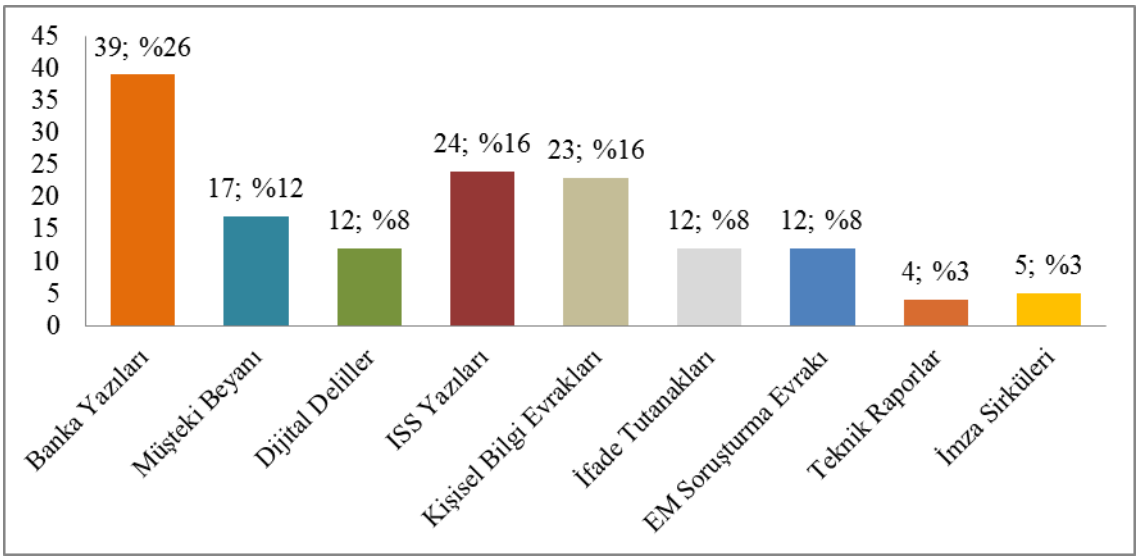


Şekil 4.11: Suça Konu Olan TCK'daki Bilişim Suçları Maddelerine İlişkin Bulgular

4.14. DAVA DOSYALARINDA BEYAN EDİLEN SUÇ DELİLLERİNE İLİŞKİN BULGULAR

Çalışmada dava dosyalarında beyan edilen suç delillerine ilişkin bulgular Şekil 4.12'de verilmiştir. Bu bulgulara göre; dosyalarda bankalardan gelen yazıların 39 kez delil olarak kullanıldığı tespit edilmiştir.

Dava dosyalarındaki deliller kısmında, ISS (İnternet Servis Sağlayıcıları)'den gelen internet abonesinin adres bilgilerini içeren 24 adet yazıyla karşılaşılmıştır. Dosyalardaki taraflar hakkındaki kişisel bilgi yazılarının ise 23 kez delil olarak kullanıldığı belirlenmiştir. 17 dava dosyasında müşteki ifadesi ile şikayetçi beyanları delil olarak kabul edilmiştir. Dava dosyalarının deliller kısmında; sanıkların ifade tutanaklarının, Emniyet Müdürlüğü (EM)'nden gelen soruşturma evraklarının ve dijital delillerin 12'şer kez yer aldığı görülmüştür. Dosyaların 4'ünde suç hakkında teknik uzmanlar tarafından rapor yazıldığı belirlenmiş, 5 dosya da ise delil olarak imza sirküleri kullanılmıştır.



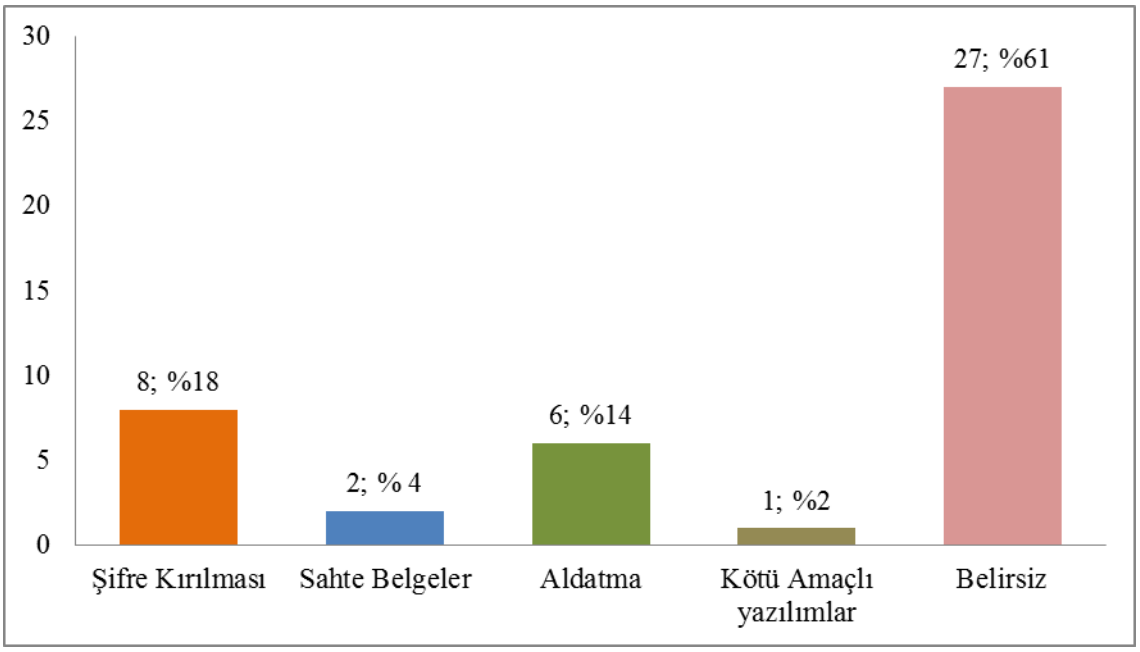
Şekil 4.12: Dava Dosyalarında Beyan Edilen Suç Delillerine İlişkin Bulgular

4.15. DOSYALARDA TESPİT EDİLEN SUÇ YÖNTEMLERİNE İLİŞKİN BULGULAR

Bu kısım, Adliyelerdeki ve Emniyet Müdürlüğü'ndeki dosyalarda tespit edilen suç yöntemlerine ilişkin bulgular şeklinde iki ayrılmıştır.

4.15.1. Adliyelerdeki Dosyalarda Tespit Edilen Suç Yöntemlerine İlişkin Bulgular

Çalışmada adliyelerdeki dosyalarda tespit edilen suç yöntemlerine ilişkin bulgular Şekil 4.13'de verilmiştir. Bu bulgulara göre; 8 olayda online bankacılık sistemine giriş için şifrelerin kırıldığı, 6 olayda online bankacılık ile aktarılan parayı çekmek için kişiler aldatılarak, bankamatik veya kredi kartlarının alındığı, 2 olayda ise sahte belgeler kullanıldığı belirlenmiştir. Buna ek olarak, bir olayda uzman bilirkişi mağdurun bilgisayarında kötü amaçlı yazılımlar tespit etmiştir. Bu bulgular dışında kalan 27 olayda suç yöntemi belirlenememiştir.



Şekil 4.13: Adliyelerdeki Dosyalarda Tespit Edilen Suç Yöntemlerine İlişkin Bulgular

4.15.2. Emniyet Müdürlüğü'ndeki Dosyalarda Tespit Edilen Suç Yöntemlerine İlişkin Bulgular

Emniyet Müdürlüğü'ndeki dosyaların incelenmesi sırasında 11 dosyanın 10'unda örgütsel bazlı suçlar işlendiği belirlenmiştir. Bu suçlarda; kişisel bilgilerin ele geçirilmesi, tek kullanımlık şifre güvenliğini aşma, sahte belge ile paranın çekilmesi, IP numaralarının manipülasyonu gibi yöntemler kullanıldığı tespit edilmiştir. Bu suç yöntemleri ile bilgiler aşağıda açıklanmaktadır.

Kişisel Bilgilerin Ele Geçirilmesi: Örgüt üyeleri, bu bilgileri elde etmek için birçok yol kullanmışlardır. Bu yolların ilki; banka görevlileri ile işbirliği yapıp müşteri bilgilerini elde etmektir. İkincisi ise; hackerların kişisel bilgileri siber suç yöntemleri ile elde etmesidir. Hackerlar, bu işlemler için Hollanda, Rusya vb. ülkelerde bulunan kiralık sunucuları kullanmaktadır. Zeus vb. yazılım ile elde edilen hesap ve şifre bilgileri bu sunuculara yüklenebilmekte ve hacker herhangi bir zamanda herhangi bir bilgisayardan bu sunucuya erişerek istediği bilgileri ulaşabilmektedir.

Tek kullanımlık Şifre Güvenliğini Aşma: Bu işten sorumlu örgüt üyeleri, ilk yol olarak elde edilen kişisel bilgiler doğrultusunda sahte belgeler ile SİM kart çıkartmaktadır. Böylelikle banka tarafından gönderilen tek kullanımlık mesajların bu SİM karta gelmesi sağlanmaktadır.

İkinci yol olarak ise bilgileri alınan kişilerin cep telefonu numarasına mesaj gönderilmektedir. Bu mesajın içeriğinde kişinin cihazına virüs bulaştıracak bir internet bağlantı adresi bulunmaktadır. Kişi bağlantıya tıkladığı zaman, virüs otomatik olarak telefona bulaşmakta ve cep telefonuna gelen tüm mesajlar hat sahibinin bilgisi dışında başka bir telefon numarasına yönlendirilmektedir. Böylece, tek kullanımlık şifrelerin ele geçirilmektedir.

Sahte Belge ile Paranın Çekilmesi: Bu yöntemde, örgüt yöneticileri sabıkasız kişileri kullanıp, onların hesapları üzerinden paralar çekilmektedir. Diğer bir yol ise sahte belgeler ile banka hesabı açılıp, paraların bu hesap üzerinden çekilmesidir.

IP Numaralarının Manipülasyonu: Bu yöntemde; örgüt üyesi olan hackerlar, Proxy ve Open Proxy gibi uygulamalarla masum kişilerin IP numaraları üzerinden suçları işleyebilmektedir.

5. TARTIŞMA VE SONUÇ

Bu bölümde; araştırmanın bulgularına dayalı olarak ulaşılan sonuçlara, araştırma sonuçlarına dayalı ve benzer araştırmalara yönelik önerilere yer verilmektedir.

5.1. SONUÇLAR

1. Araştırma sonucunda; 61'i online bankacılık suçları ile ilişkili olan toplam 87 dosyaya erişilmiştir. Erişilen online bankacılık suçları ile ilişkili dosyaların 43'ü incelenmiştir.
2. Bu inceleme neticesinde; 43 dosyada toplam 154 suçun tespiti yapılmıştır.
3. Suçun bireysel olarak işlendiği belirlenen dosya sayısı 42 olarak tespit edilmiştir. 12 dosyada ise suçların örgütsel olarak işlendiği belirlenmiştir. Bu dosyaların 10'u Emniyet Müdürlüğü'nde tespit edilmiştir.
4. Adliyelerde incelenen online bankacılık suçları ile ilişkili dava dosyalarının 20'sinde karara varılmış, 24'ü devam etmekte, 3'ü Yargıtay'a gönderilmiş, 1'i bilirkişide bulunmakta, 1'i ise zaman aşımına uğramıştır.
5. Kararlı dosyaların 2'si mahkûmiyet, 13'ü beraat, 2'si hükmün geriye bırakılması ile erteleme ve 3'ü de mahkûmiyet&beraat kararı ile sonuçlanmıştır.
6. Ceza kararlı dava dosyalarında; 5 kere 24-36 ay arası, 2 kere 36 aydan fazla ve 1 kere ise 24 aydan az hapis cezası verildiği tespit edilmiştir.
7. Adli para cezası verilen davaların tümümün Sultanahmet Adliyesi'nde olduğu belirlenmiştir. Bu dosyalardaki verilere göre sanıklara 1 kez 2000 TL'den fazla, 2 kez 500 TL'den az, 4 kez ise 2000 TL para cezası verilmiştir.
8. Kararlı davaların dava süreleri incelendiğinde; 7 dava 7-12 ay arası, 1 dava da 0-6 ay arası sürmüştür. Ayrıca, 13-18 ay, 19-24 ay ve 24 aydan fazla süren dava sayılarının 4 olduğu anlaşılmıştır.
9. Suçların işlenme tarihlerinin yıllara göre dağılımı; 2006 yılı öncesi 2, 2006 yılında 13, 2007 yılında 47, 2008 yılında 24, 2009 yılında 7, 2010 yılında 29, 2011 yılında 24 olarak tespit edilmiştir.
10. Suça konu olan toplam para miktarı 3 milyon 700 bin TL olarak belirlenmiştir. Bu paranın miktar aralığı olarak dağılımı ise 1.000 TL'den az 5 tane, 1.000 TL-10.000 TL arası 26 tane, 10.000 TL'den fazla 23 tane şeklindedir.

11. İncelenen 43 dosyanın 19'unda suçun işlenme yeri hakkında "yer durumundan yetkisizlik" oluşmuştur. Geriye kalan 24 dosyada ise böyle bir durum oluşmamıştır.
12. İnceleme neticesinde davaların hazırlık sürelerinin; 14 dosyanın 12-24 ay arası, 12 dosyanın 24-36 ay arası, 8 dosyanın 36 aydan fazla, 8 dosyanın 6-12 ay arası, 2 dosyanın ise 0-6 ay arası olduğu belirlenmiştir.
13. Dosyaların 41'inde IP numarası tespit edilmiştir. 15 dosyada ise IP numarası belirlenememiştir.
14. 32 IP numarasının adresi belirlenmiştir. Bu adreslerin 30'unun yurtiçi, 2'sinin de yurtdışında bulunduğu anlaşılmıştır. Adresi belli IP numaraları mesken olarak; 27'si ev, 4'ü internet kafe, 1'i de işyeridir. Adresi belirlenemeyen 9 IP numarası bulunmuştur.
15. Araştırma sonucunda 334 erkek, 24 kadın olmak üzere toplam 358 kişinin suça karıştığı tespit edilmiştir.
16. Suça karışan 27 bireyin 26 yaşından küçük, 147 bireyin 26-35 yaş aralığında, 129 bireyin 36-45 yaş aralığında, 43 bireyin 46-60 yaş aralığında bulunduğu belirlenmiştir. 61 yaşından büyük birey sayısının 7 ve yaşı belirlenemeyen birey sayısının ise 5 olduğu tespit edilmiştir.
17. Emniyet Müdürlüğü'ndeki dosyalarda suça karışan 91'i erkek, 1'i kadın olmak üzere toplam 92 bireyin sabıkalı olduğu belirlenmiştir. Sabıkasız birey sayısının 69'u erkek ve 6'sı bayan olmak üzere 75 olduğu tespit edilmiştir. Sabıka durumu tespit edilemeyen toplam 88 bireyin olduğu belirlenmiştir.
18. Suça müdahil olan bireylerin soruşturma süresindeki durumları hakkında; 110'unun yakalandığı, 71'nin firari olduğu, 19'unun tutuklu olduğu, 8'inin serbest bırakıldığı, 1'i hakkında yakalama emri olduğu bilgilerine ulaşılmıştır. Ayrıca suça karışanların 46'sının soruşturma durumu tespit edilememiştir.
19. Online bankacılık suçlarında 129 kişinin ve 49 tüzel kişiliğin mağdur olduğu belirlenmiştir. Mağdur durumdaki 129 bireyin 103'ü erkek, 26'sı kadındır.
20. Mağdur bireylerin; 8'inin 26-35 yaş aralığında, 14'ünün 36-45 yaş aralığında, 12'sinin 45-60 yaş aralığında ve 1'inin 60 yaşından büyük olduğu tespit edilmiştir.

21. Dosyalardaki inceleme neticesinde; TCK'nın bilişim suçları ile ilişkili 142/2-e maddesi 22 kez, 244/4 maddesi 18 kez, 152/2-f maddesi 10 kez, 243/1 maddesi 5 kez, 244/1 maddesi 4 kez, 244/2 maddesi 3 kez, 244/3 maddesi 2 kez ve 245. maddesi ise 2 kez suça konu olmuştur.
22. Araştırma neticesinde; 39 kez banka yazılarının, 24 kez internet servis sağlayıcısı yazılarının, 23 kez kişisel bilgi evraklarının, 17 kez müşteki beyanının, 12 kez dijital delillerin, 12 kez ifade tutanaklarının, 12 Emniyet Müdürlüğü soruşturma evrakının, 4 kez teknik raporların, 5 kez imza sirkülerinin suç delili olarak kullanıldığı tespit edilmiştir.
23. Adliyelerdeki incelemede, 27 dosyada suç yöntemi tespit edilememiştir. Suç yöntemi tespit edilen 17 dosyanın; 8'inde şifrelerin kırılması, 6'sında aldatma, 2'sinde dosyada sahte belge kullanımı ve 1'inde kötü amaçlı yazılım yöntemi kullanılmıştır.

5.2. ÖNERİLER

5.2.1. Araştırma Sonuçlarına Dayalı Öneriler

1. Bankaya ait her ATM'de kamera olmalı ve kameralar işlem yapan kişinin yüzünü rahat bir şekilde görüntülenecek pozisyonda bulunmalıdır.
2. Bankalarda dijital delillerin saklanmasına yönelik banka şubelerindeki ve ATM'lerdeki kamera görüntüleri uzun bir süre kayıt altında tutulmalıdır.
3. İnternet kafe ve müşterilerine ücretsiz kablosuz internet sağlayan işletmelerde güvenlik kamerası bulunmalıdır. Söz konusu işletmelerde kayıt altına alınan bu görüntüler uzun bir süre muhafaza edilmelidir.
4. Bankalar olağandışı durum tespit ettikleri zaman, olayın gerçekleştiği yer ile ilgili güvenlik kamera görüntüleri muhafaza altına alınmalıdır. Bankaların güvenlik birimleri aktif rol oynamalıdır. Banka bu tip özel durumlardan sorumlu olan ayrı bir birim oluşturabilir.
5. İnternet Servis Sağlayıcıları, internet abonelerine ait tüm kişisel bilgileri uzun süre saklamalıdır.
6. Kablosuz internet kullanan kişiler, mutlaka şifre kullanmalı ve şifre güvenliğinin yüksek olması için şifrelerde rakam, büyük-küçük harf, noktalama işaretleri bulunmalıdır.

7. Kişiler her ne sebeple olursa olsun; kredi veya bankamatik kartlarını başka kimselere vermemeli ve bu kartların şifrelerini söylememelidir.
8. Kablosuz internetlerin kullanımında şifrelerin kırılıp üçüncü kişilerin interneti kullanmasını engellemek için modemde kullanıcı kısıtlaması veya bilgisayar tanımlaması gibi güvenlik önlemleri alarak yetkisiz kullanımlar engellenmelidir.
9. GSM şirketleri, bankadan gelen şifre kısa mesajlarını eğer hat yönlendirmesi varsa engellemelidir.
10. Bireyler, online bankacılığa giriş yaptığı cihazın güvenli olduğundan emin olmalıdır.
11. Bireyler, sosyal mühendislik temelli aldatmalara karşı bilinçli olmalıdır.
12. Birey, online bankacılık işlemleri dahil özel bilgiler gerektiren online alışveriş, e-devlet işlemlerini internet kafeler veya diğer halkın kullanımına açık olan restoran, kafe vb. yerlerde yapmamalıdır.
13. Kurumların ve kişilerin yeni geliştirilen suç yöntemlerine karşı farkındalıkları arttırılmalıdır.
14. Banka çalışanları ve GSM satış bayii çalışanları sahte belgelere karşı eğitilmelidir. Dahası, bu yerlerde sahte belge tespit eden cihazlar kullanılmalıdır.
15. Davaların hazırlık aşamasında yer alan kurumların aralarındaki yazışma süreleri kısaltılmalıdır. Hatta bu yazışmalar internet veya özel ağ üzerinden e-belgeler aracılığı ile olmalıdır.
16. Adli makamlar, online bankacılık suçlarında ve diğer bilişim suçlarında daha fazla dijital delil elde etmeye çalışmalı ve dijital kayıtların saklanması için yeni çözümler üretmelidir.
17. Suçun işlendiği yer durumundan dolayı oluşan yetkisizliklerdeki zaman kayıplarının önlenmesine yönelik çalışmalar yapılmalıdır.
18. Bilişim suçlarındaki adli süreçte etkin rol oynabilecek, hem hukuk hem de bilişim alanında yetkin vasıflara sahip olan uzmanlar yetiştirilmelidir. Bu bağlamda; üniversiteler, lisans ve lisansüstü düzeyde adli bilişim uzmanlarını yetiştiren programlar açmalıdır.
19. Adli makamların bünyesinde adli bilişim uzmanlarının bulunduğu özel birimler oluşturulmalıdır. Bu birimlerde bulunan uzmanlar, davaların hem hazırlık aşamasında hem de kovuşturma aşamasında görev almalıdır.

20. Adli makamlarda bilişim suçları ile ilgilenen mahkemeler açılmalıdır. Bilişim Hukuku alanında uzmanlaşan hâkim ve savcılar yetiştirilmelidir. Bilişim Suçları Hâkimi, Bilişim Suçları Savcısı uzmanlık alanları oluşturulmalı ve yaygınlaştırılmalıdır.
21. Adli süreçte yer alan tüm kurumlar, online bankacılık suçları ve diğer bilişim suçlarına yönelik ortak terminoloji kullanmalıdır.
22. Bilişim suçları ile ilişkili kanun maddelerinde bilişim suçları spesifik olarak tanımlanmalı ve açıklanmalıdır.
23. Mahkeme kalemlerindeki iş yoğunluğunun azaltılmasına yönelik çalışmalar yapılmalıdır.
24. Adliyelerdeki kayıt altına alınan dava dosyaları daha basit ve ayrıştırılabilir şekilde tanzim edilmelidir.
25. Dava dosyalarında taraflara ait ayrıntılı demografik bulgular bulunmalıdır.

5.2.2. Benzer Araştırmalara Yönelik Öneriler

- Bu çalışma, İstanbul ili sınırlarında 4 ilçe adliyesindeki 21 ceza mahkemesi ve İstanbul Emniyet Müdürlüğü'nde gerçekleştirilmiştir. Çalışmanın farklı ilde, daha fazla mahkeme örneklemi ile gerçekleşmesi araştırmanın sınırlılığını azaltabilir.
- Örneklem olarak sadece Emniyet Müdürlüğü bazlı bir araştırma yapılabilir.
- Online bankacılık suçları veya bilişim suçları adli süreçlerinde bilişim uzmanlarının rolü üzerine bir çalışma gerçekleştirilebilir.
- Online bankacılık, online dolandırıcılık ve bilişim suçlarına banka örneklemi üzerinden bakış açısı getirebilecek çalışmalar yapılabilir.
- Adli ve idari mercilerde gerçekleştirelecek benzer çalışmalarda veri toplama süresi ve süreci iyi planlanmalıdır.

KAYNAKLAR

AARON, G. ve RASMUSSEN, R. , 2011, *Global Phishing Survey:Trends and Domain Name Use in 2H2010*, ABD, http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf [Ziyaret Tarihi: 01.01.2012].

ADALET BAKANLIĞI, 2012, *Türk Ceza Kanunu*, http://www.ceza-bb.adalet.gov.tr/mevzuat/5237.htm [Ziyaret Tarihi: 01.01.2012].

ADIGÜZEL, C. G., 2009, *Güvenlik Endişesinin İnternet Bankacılığı Kullanımına Etkisi ve Vakıfbank Müşterilerine Yönelik Bir Araştırma*, Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü.

ADOMI, E. E., 2008 , *Security and Software for Cybercafes*, Idea Group Inc (IGI), Amerika Birleşik Devletleri, ISBN 978-1-59904-905-2.

AKBULUT, B., 2000, *Bilişim Suçları*, SÜFHD, Sayı 1-2, Cilt.8

ALLSOPP W., 2009, *Unauthorised Access: Physical Penetration Testing For IT Security Teams*, John Wiley & Sons, Amerika Birleşik Devletleri, ISBN 978-0-470-74761-2.

ANTI-PHISHING ÇALIŞMA GRUBU, 2011, *Phishing*, http://www.antiphishing.org/reports/apwg_trends_report_h1_2011.pdf [Ziyaret Tarihi: 15.01.2012].

ARATA M. J., 2010, *Identity Theft For Dummies*, John Wiley & Sons, Indianapolis, ISBN 978-0-470-56521-6.

ASİM, M., 2011, *Multi-Layer Logon Verification Sytem: A case study of Indian Banks*, Trends in Computer Science, Engineering and Information Technology: First International Conference, Proceedings, Springer, Berlin, ISBN 978-3-642-24043-0.

ASLAN, M., 2012, *Phishing Saldırıları ve Sahte Sistemler*, http://www.bilgiguvenligi.gov.tr/son-kullanici-kategorisi/phishing-saldirilari-ve-sahte-sistemler.html [Ziyaret Tarihi: 01.01.2012].

AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ, 2012, *2001 yılı Siber Suç Sözleşmesi*, http://conventions.coe.int/Treaty/en/Treaties/html/185.htm [Ziyaret Tarihi: 24.03.2012].

AVRUPA TELEKOMÜNİKASYON STANDART ENSTİTÜSÜ (ETSI) , 2003, *Teknik Rapor*, http://docbox.etsi.org/EC_Files/EC_Files/tr_102203v010101p.pdf [Ziyaret Tarihi:27.03.2012].

BIDGOLI, H., 2004, *The Internet Encyclopedia 2. Cilt*, John Wiley and Sons, ABD, ISBN 0-471-22204-6.

BRENTON,C. ve HUNT,C., 2002, *Network Security*, John Wiley & Sons, San Fransisco, ISBN 0-7821-4142-2.

BROWN, B. C., 2010, *How To Stop E-Mail Spam, Spyware, Malware, Computer Viruses, And Hackers From Ruining Your Computer Or Network: The Complete Guide For Your Home and Work, Atlantic Publishing Company*, Florida, ISBN 978-1-601-38-303-7.

BUNKER G., KING G. F., 2009, *Data Leaks For Dummies*, John Wiley & Sons, New Jersey, ISBN 978-0-470-38843-3.

BURLU, K., 2011, *Bilişimin Karanlık Yüzü*, Nirvana Yayınları, İstanbul, ISBN 9758878628.

BUTLER T., 2010, *The Complete Guide to Your Personal Finances Online: Step-by-Step Instructions to Take Control of Your Financial Future Using the Internet*, Atlantic Publishing Company, Florida, ISBN 978-1-60138-297-9.

BÜYÜKÖZTÜRK Ş., 2007, *Deneysel Desenler*, Pegem Yayıncılık, 2. Baskı, Ankara, ISBN 975-6802-43-X.

CARTWRİGHT, I, R, 2000, *Mastering customer relations*, McMillan Master Series, London.

CHOU, D.C. VE CHOU, A.Y., 2000, *A Guide to the Internet Revolution in Banking. Information System Management*, Vol 17 No: 2, pp.51-57.

CIAMPA, M., 2011, *Security + Guide to Network Security Fundamentals*, 4. Baskı, Cengage Learning, Boston, ISBN 978-1-111-64012-5.

CLOUGH, B. ve MUNGO P., 1999, *Approaching Zero Data Crime and the Computer Underworld*, Çeviri: Kurma, Emel (1999), "Sıfıra Doğru Veri Suçları ve Bilgisayar Yeraltı Dünyası", İstanbul, ISBN 9789754704969.

COLARIK, A. ve JANCZEWSKI, J., 2008, *Cyber Warfare and Cyber Terrorism*, IGI Global,Londra, ISBN 978-1-59140-992-2.

COLE, E., 2011, *Network Security Bible*, John Wiley & Sons, Indianapolis, ISBN 978-0-470-50249-5.

COMSCORE DATA MİNE, 2010, *Top 10 Countries By Online Banking Penetration*, http://www.comscoredatamine.com/2010/10/top-10-countries-by-online-banking-penetration/ [Ziyaret Tarihi: 16.12.2011].

CORELL, S.,P. ve CORRONS, L., 2009, *The Business of Rogueware Analysis of the New Style of Online Fraud*, http://www.pandasecurity.com/img/enc/The%20Business%20of%20Rogueware.pdf [Ziyaret Tarihi: 11.01.2012].

CROSS, M., 2008, *Scene of the Cybercrime*, Syngress Yayınevi, 2. Baskı, ABD, ISBN 978-1-59749-276-8.

DAĞLI, R. M., 2007, *Banka Müşterilerinin İnternet Bankacılığına İlişkin Kanaatlerinin İncelenmesi ve Konu ile İlgili Pilot Bir Araştırma*, Yüksek Lisans, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

DANIEL, E., (1999), *Provision of electronic banking in the UK and Repulic of Ireland*, International Journal of Bank Marketing, Vol 17. No. 2, Sayfa Numarası 72-82.

DAVID D., COLEMAN, D. D., WESTCOTT D. A., HARKINS B. E., JACKMAN S. M., 2010, *CWSP Certified Wireless Security Professional Official Study Guide: Exam Pw0-204*, John Wiley & Sons, Indianapolis, ISBN 978-0-470- 43891-6.

DEĞİRMENCİ, O., 2002, *Bilisim Suçları*, Marmara Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

DENİZBANK,2012, *IP Kısıtlaması*, http://www.denizbank.com/acikdeniz/guvenlik/guvenlik-ayarlari.aspx [Ziyaret Tarihi: 13.03.2012].

DİLSİZ, R., 2011, İzmir, *İnternet'te Bireysel Güvenliği Nasıl Sağlarız?*, http://inet-tr.org.tr/inetconf16/bildiri/64.pdf [Ziyaret Tarihi: 19.03.2012].

DOĞAN, A. E. , 1992, *Bilişim Suçları ve Hukukuna Giriş*, Doruk Yayınları, Ankara, syf 27.

DOKURER S., *Bilişim Suçları*, http://www.dokurer.net/files/documents/Bilisim_Suclari_Bursa.pdf [Ziyaret Tarihi: 12.03.2012].

DUNHAM, K., 2008, *Mobile Malware Attacks and Defense*, Syngress Publication, Amerika Birleşik Devletleri, ISBN 978-1-59749-298-0, Sayfa Numarası 125-196.

DURMAZ, Ş., 2006 , *Bilişim Suçlarının Sosyolojik Analizi*, Gazi Üniversitesi Yayınlanmamış Yüksek Lisans Tezi, Ankara.

DÜLGER, M. V., 2004, *Bilişim Suçları*, Seçkin Yayıncılık, Ankara.

DÜLGER, M. V., 2011, *Bilişim Suçları ve Yeni Türk Ceza Kanunu*, http://www.dulger.av.tr/assets/pdf/bilisimsuclariveyctk.pdf [Ziyaret Tarihi: 21.11.2011].

EC-COUNCIL PRESS, 2009, *Ethical Hacking and Countermeasures: Threats and Defense Mechanisms*, Cengage Learning, Kanada, ISBN 978-14354-8361-3.

ECCOUNCIL PRESS., 2010, *Ethical Hacking and Countermeasures: Attack Phases*, Cengage Learning, Newyork, ISBN 978-1-4354-8360-6.

EKBERG, P.,Lİ, S., MORİNA, G. , 2007,*Online Banking Access System Principles Behind Choices And Further Development, Seen From A Managerial Perspective*, Jönköping Üniversitesi.

ELBAHADIR, H., 2011, *Hacking Interface*, 3. Baskı, Kodlab Yayınları, İstanbul, ISBN 978-6054205-27-1.

ERBSCHLOE M., 2005, *Trojans, worms, and spyware: a computer securityprofessional's guide to malicious code*, Elsevier Butterworth-Heinemann, ABD, ISBN 0-7506-7848-8.

ERGÜÇ, S., 2008, *Türk Bankacılık Sisteminde İnternet Bankacılığı ile Yapılan Dolandırıcılıklar ve Bilişim Suçları Hukuku*, Yüksek Lisans Tezi, Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü.

ERTÜRK, M. E., 2002, *İnternet Bankacılığı'nın Güvenliği ve Türkiye Uygulamasına İlişkin Bir İnceleme*, (Yayımlanmamış Yüksek Lisans Tezi), İstanbul, syf:69-70.

ETTER,B.,2002, *Leadership in the Hi-Tech Crime Environment*, Avustralya Centre For Plicing Research To 2/2002 Pelp At The Aipm Sydney.

FİNANS KULÜP DERGİSİ, 2010, *İnternet Bankacılığı*, Sayı 10, https://groups.google.com/forum/?fromgroups=#!topic/finanskulup/YnoiecDhW9c [Ziyaret Tarihi: 24.06.2011].

GAMMACK, J., HOBBS, V., PIGOTT D., 2011, *The Book of Informatics Revised Edition*, Cengage Learning, Avustralya, ISBN: 9780170130448.

GARANTİ BANKASI, 2012, *E-posta saldırı örneği*, http://assets.garanti.com.tr/assets/img/etc/sahte_eposta_ornegi.jpg, [Ziyaret Tarihi:12.12.2011].

GAZİLER, V., 2006, *İnternet Bankacılığı ve Kullanımının Etkinliği; Kullanım Etkinliği-Eğitim İlişkisini Ortaya Koymaya Yönelik Bir Araştırma*, Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Enstitüsü.

GERBER, J., JENSEN, E. L., 2007, *Encyclopedia of White-Collar Crime*, Greenwood Publishing Group, ABD, ISBN 0-313-33524-9.

GIBSON, D., 2011, *Microsoft Windows Security Essentials*, John Wiley and Sons, ABD, ISBN 978-1-118-11454-4.

GİSSEL, R., 2005, *The Development and Evaluation of a Computer Crime Investigative Distance-learning Program for the National Cybercrime Training Partnership*, MacroTech Press, ABD, syf 11.

GKOUTZINIS A. A., 2006, *Internet Banking And the Law in Europe: Regulation, Financial Integration And Electronic Commerce*, Cambridge University Press, İngiltere, ISBN 9780521860710.

GREBENNIKOV, N., 2007, *Keyloggers: How they work and how to detect them (Part 1)*, http://www.securelist.com/en/analysis/204791931/Keyloggers_How_they_work_and_how_to_detect_them_Part_1#prot [Ziyaret Tarihi: 29.03.2012].

GULATİ, R., 2003, *The Threat of Social Engineering and Your Defense Against It*, SANS Institute, http://123seminarsonly.com/Seminar-Reports/021/55172071-The-Threat-of-Social-Engineering-and-Your-Defense-Against-It.pdf [Ziyaret Tarihi: 01.02.2012].

GUP B. E., 2003, *The Future Of Banking*, Greenwood Publishing Group, ABD, ISBN 1-56720-467-8.

GÜNGÖR, N.M., 2007, *Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları*, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

HEFFERNAN S., 2005, *Modern Banking*, , John Wiley & Sons, İngiltere, ISBN 0-470-09500-8.

HENRY, S. ve LANIER, M. M., 2001, *What Is Crime?: Controversies Over the Nature of Crime and What to Do About It*, Rowman & Littlefield, ABD, ISBN 9780847698073.

HUTCHINSON, B., 2005, *Proceedings of the 5th European Conference on i-Warfare and Security*, Academic Conferences Limited, İngiltere, ISBN 1-905305-02-8.

INGBank, 2012, http://www.ingbank.com.tr/724-internetbankaciligi.asp, [Ziyaret Tarihi:29.03.2012].

JAHANKHANI H., WATSON D. L., ME G., 2010, *Handbook of Electronic Security and Digital Forensics*, World Scientific, Singapur, ISBN 978-981-283-703-5.

JAMES, L., 2005, *Phishing Exposed*, Syngress Yayınevi, ABD, ISBN 978-15974-90306.

JENKINS, H., 2007, *Adopting internet banking services in a small island state: assurance of bank service quality*. Managing Service Quality, 17 (5), Sayfa Numarası 523-537.

KAHATE A., 2008, *Cryptography and Network Security*, Tata McGraw-Hill Education, Yeni Delhi, ISBN 978-0-07-064823-4, syf 272-273.

KARAGÜLMEZ, A., 2009, *Bilişim Suçları Ve Soruşturma - Kovuşturma Evreleri*, Seçkin Yayıncılık, Ankara, ISBN 9789750214233.

KARASAR, N. ,1999, *Bilimsel Araştırma Yöntemi*, Ankara, Nobel Yayın Dağıtım.

KEYES, J., 1999, Banking Technology Handbook, ABD, CRC Press, ISBN 13: 9780849399923.

KIZZA J. M., 2005, *Computer Network Security*, Springer, Amerika Birleşik Devletleri,, ISBN 978-03872-0473-4.

KONDABAGIL J., 2007, *Risk Management in Electronic Banking: Concepts anad Best Practice*, John Wiley and Sons, Amerika Birleşik Devletleri, *ISBN* 978-0-470-82243-2.

KRAUSE, M. ve TIPTON, H. F., 1999, *Handbook of Information Security Management*, CRC Press LLC, ABD, ISBN 0849399475.

KUMAR V., SRIVASTAVA J. VE LAZAREVIĆ A., 2005, *Managing Cyber Threats: Issues, Approaches, and Challenges*, Springer, Newyork, ISBN 0-387-24226-0.

LEHTINEN, R., RUSSELL, D., GANGEMİ, G. T., 2006, *Computer Security Basics, O'Reilly Media*, ABD, 2. Baskı, ISBN 978-0-596-00669-3.

LININGER, R. ve VINES, R. D., 2005, *Phishing: Cutting the Identity Theft Line*, John Wiley & Sons, Indianapolis, ISBN 978-07645-8498-5.

LONDRA BÜYÜKŞEHİR POLİS TEŞKİLATI GÜVENLİK RAPORU, 2005, http://www.met.police.uk/fraudalert/docs/internet_bank_fraud.pdf [Ziyaret Tarihi: 15.01.2012].

LONG, J., 2008, *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*, Syngress Publishing, Burlington, ISBN 978-1-59749-215-7.

MİLLER R. L., CROSS F. B., 2012, *The Legal Environment Today: Business in Its Ethical, Regulatory, E-Commerce, and Global Setting*, Cengage Learning Yayınevi, 7. Baskı, ABD, ISBN 9781111530617.

MİLLER,R. L. ve JENTZ,G. A., 2009, *Fundamentals of Business Law: Excerpted Cases*, Cengage Learning, ISBN 978-0-324-59572-7.

MOORE, T. ve CLAYTON, R., 2007, *An Empirical Analysis of the Current State of Phishing Attack and Defence*, Birleşik Krallık, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.6098&rep=rep1&type=pdf [Ziyaret Tarihi: 20.01.2012].

MUHWAUZİ, T., 2009, *Internet Banking Comparison Between China And Sweden And A Reflection On Chinese İnternet Banking*.

ODABAŞI, Y., 2006, *Banka ve Sigorta Pazarlaması*, Anadolu Üniversitesi Yayınları, Eskişehir, ISBN 975-06-0406-7.

ORAM, A. VE VIEGA, J., 2009, *Beautiful Security*, O'Reilly Media, ABD, ISBN 978-0-596-52748-8.

OSBORNE,M., 2006, *How to Cheat at Managing Information Security*, Syngress Publishing, ABD, eISBN: 9780080508283.

ÖZBAL,T., 2011, *Bankacılık Sektöründe Müşteri İlişkileri Yönetimi ve İnternet Bankacılığında Müşterilerin Seçimlerine Etki Eden Faktörler*, Yüksek Lisans, Ufuk Üniversitesi Sosyal Bilimler Enstitüsü.

ÖZCAN, Z. Ö., *Türkiye'de Elektronik Bankacılık: İnternet Bankacılığı Üzerine Bir Çalışma,* Yüksek Lisans Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü.

ÖZDEMİR, R., 2010, *KOBİ'lerin İnternet Bankacılığına Adaptasyonu: Ortadoğu Anadolu Bölgesi'nde Anket Uygulaması*, Yüksek Lisans Tezi, Zonguldak Karaelmas Üniversitesi Sosyal Bilimler Enstitüsü.

ÖZEL, C., 2002, *Bilişim- İnternet Suçları*, http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm [Ziyaret Tarihi: 10.01.2012].

ÖZKUL, E., 2005, *Büro Teknolojileri, Anadolu Üniversitesi Yayınları*, Eskişehir, ISBN 975-06-0348-6.

PALA, E., 2010*, Alternatif Dağıtım Kanallarından İnternet Bankacılığına Yönelik Müşteri Tercihlerinin İncelenmesi,* Yüksek Lisans, Celal Bayar Üniversitesi Sosyal Bilimler Enstitüsü.

PANDA SECURİTY, *Rogueware Ekran Görüntüsü*, http://www.pandasecurity.com/img/enc/The%20Business%20of%20Rogueware.pdf [Ziyaret Tarihi:12.12.2011].

PARSONS, J. J. ve OJA D., 2012, *New Perspectives on Computer Concepts 2013: Comprehensive*, Cengage Learning, Boston, ISBN 9978-1-133-19056-1.

PERRY G. A., 2006, *Quicken All-In-One Desk Reference for Dummies*, Wiley Publishing, Indianapolis, ISBN 978-0-471-75466-4.

POLIMIROVA D. ve NICKOLOV E., 2010, Real-Time System for Assing The Information Security of Computer Networks, *Open Research Problems in Network Security: IFIP WG 11. 4 International Workshop INetSec 2010*, Springer, Sofya, Sayfa Numarası 125-126.

PONEMON ENSTİTÜSÜ, 2012, *Siber Suç Çalışma Yıllık Maliyet Raporu*, ABD Şirketler Benchmark Çalışması, http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf [Ziyaret Tarihi: 16.01.2012].

RESMİ GAZETE, 2012, *Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ*, http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2007/09/20070914.htm&main=http://www.resmigazete.gov.tr/eskiler/2007/09/20070914.htm Ziyaret Tarihi [12.02.2012].

RICHARD, P., DARIO F., 2006, *Social Engineering: Attacks Have Evolved, But Countermeasures Have Not*, *Computer Fraud & Security*, Volume 2006, Issue 10, Sayfa Numarası 17-20.

RODDEL V., 2008, *The Ultimate Guide to Internet Safety*, Lulu.com Yayıncılık, ABD, ISBN: 9781435711594.

ROSA, A. J. M. F., 2003, *Marinete, the Story of a Convicted Woman*, iUniverse, ABD, ISBN 0-595-25874-3.

ROTHKE, B., 2005, *Computer security: 20 things every employee should know*, McGraw Hill Professional, Wisconsin, ISBN 0-07-226282-6.

SAREL, D. ve MARMORSTEIN, H., 2003, *Marketing online banking services: The voice of the customer*, Journal of Financial Services Marketing, Vol. 8 No. 2, Sayfa Numarası 106-118.

SAY, K., 2006, *Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi*, Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü.

SCN EDUCATION B.V., 2001, *Electronic banking: the ultimate guide to business and technology of online banking*., Birkhäuser, Wiesbaden, ISBN 3-528-05754-8.

SHARMA, R. K., 1998, *Social Problems And Welfare*, Atlantic Publishers & Dist, Yeni Delhi.

SHELL, H. S., MARTIN, C., 2004, *Cybercrime: A Reference Handbook*, ABC-CLIO, Amerika Birleşik Devletleri, ISBN 1-85109-688-4.

SHİNDER D. L. ve TİTTEL E., 2002, *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Yayınevi, ABD, ISBN: 978-1931836654.

SHİNDER, D. L., 2002, *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress, ABD, ISBN: 1-931836-65-5.

SIMPSON, M, T., BACKMAN K. ve CORLEY J.,2010, *Hands-On Ethical Hacking and Network Defense*, Cengage Learning, Boston, ISBN 978-1-4354-8609-6.

SOLOMONI, M. ve KIM, D., 2010, *Fundamentals of Information Systems Security*, Jones & Bartlett Learning, İngiltere, ISBN:978-0-7637-9025-7.

STAPKO, T., 2007, *Practical Embedded Security, Newnes*, abd, ISBN 10: 0 7506-8215-9 ISBN 13: 978-0-7506-8215-2.

TAŞKIN, Ş.C., 2008, *Bilişim Suçları*, Beta Yayınları, İstanbul, ISBN 978-975-295-970-5.

TAŞKIN, Ş.C., 2008, *Karsılastırmalı Hukukta ve Hukukumuzda Bilişim Suçları*, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

THAPAR, A., 2007, Social Engineering: an attack vector most intricate to tackle, http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf [Ziyaret Tarihi: 09.01.2012].

THE SILVER LAKE, 2006, *Scams and Swindles*, Silver Lake Yayınevi, Los Angeles, ABD, ISBN 1-56343-834-8.

TOWNSEND, K., July–August 2010, The art of social engineering, *InfoSecurity*, Volume 7, Issue 4, Sayfa Numarası 32–35.

TÜRK BANKALAR BİRLİĞİ (TBB), 2012, Mart 2012 - İnternet ve Mobil Bankacılık İstatistikleri http://www.tbb.org.tr/tr/Banka_ve_Sektor_Bilgileri/Istatistiki_Raporlar.aspx [Ziyaret Tarihi: 31.03.2012].

TÜRK DİL KURUMU (TDK), 2012, *Bilişim Kavramı*, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.4fb131d34f0e37.60848210 [Ziyaret Tarihi: 12.01.2012].

TÜRK DİL KURUMU, Hacker Tanımı, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&kelime=bilgisayar%20korsan%C4%B1&guid=TDK.GTS.505594b5e699c8.43728482 [Ziyaret Tarihi: 10.05.2012].

TÜRKİYE BANKALAR BİRLİĞİ (TBB), 2007, Bankacılıkta Dolandırıcılık Eylemleri Tespit / Önleme Yöntemleri, İstanbul, https://esube1.ziraatbank.com.tr/esubestatic/html/tr_TR/tbbbilgi/Kitapk.htm [Ziyaret Tarihi: 16.10.2011].
TÜRKİYE İŞ BANKASI, *Güvenlik Çemberi Uygulaması*, http://www.isbank.com.tr/content/TR/Guvenlik/Guvenlik_Cemberi-297-292.aspx [Ziyaret Tarihi: 03.03.2012].

UCAR, A., *Bankacılık Sektöründe Bilişim Sistemlerinin Kötüye Kullanılmasına İlişkin Hukuki ve Cezai Sorumluluk*, books.google.

UMUR, K., 2006, *Bankaların İnternet Bankacılığını Kullanan Müşterilerin Tutumlarına İlişkin Değerlendirmeleri ve Bir Uygulama*, Yüksek Lisans, Marmara Üniversitesi Sosyal Bilimler Enstitüsü.

ÜLKÜ, M.M., 2005, *5237 Sayılı TCK 141-147. Maddelerinde Yer Alan Hırsızlık Suçları* , Çorum, http://www.ceza-bb.adalet.gov.tr/makale/151.pdf, [Ziyaret Tarihi: 21.02.2012].

VACA, J. R., 2009, *Computer and Information Security Handbook*, Morgan Kaufmann Yayınevi, Amerika Birleşik Devletleri, ISBN: 978-0-12-374354-1.

VACCA, J. R., 2005, *Computer Forensics: Computer Crime Scene Investigation*, 1. Cilt, Cengage Learning Yayınevi, ABD, ISBN 1-58450-389-0.

WILES J.,GUDAITIS T., JABBUSCH J., ROGERS R., LOWTHER S., 2011, *Low Tech Hacking:Street Smarts for Security Professionals.*, Elsevier, Massachusetts, ISBN 978-159749-665-0.

YAZICIOĞLU, R. Y., 1997, *Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile*, Alfa Yayınevi, İstanbul, ISBN 9753160410.

YE, N., 2008, *Secure Computer and Network Systems: Modeling, Analysis and Design*, John Wiley and Sons Yayınevi, ABD, ISBN 978-0-470-02324-2.

YENİDÜNYA, C. ve DEĞİRMENCİ, O., 2003, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, Legal Yayıncılık, İstanbul.

YILMAZ, S., 2007, *Hukuki Açıdan İnternet Bankacılığı*, Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

YILMAZ, S., 2011, *5237 Sayılı Tck'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar,* http://portal.ubap.org.tr/App_Themes/Dergi/2011-92-669.pdf [Ziyaret Tarihi: 21.01.2012].

ZHU, F., 2009, *Smart Card Based Solutions For Secure Internet Banking With A Primitive Reader Or Mobile Phone*, Lisans Tezi.

EKLER

EK A- ONLİNE BANKACILIK SUÇLARI İLE İLİŞKİLİ DAVA DOSYALARINI İNCELEME ANKETİ

TCK'daki Kanun Maddesi:

Suç Yöntemi:

Suç Unsurunda Kullanılan Sistemler:

Mağdur tarafın kullandığı Online Bankacılık Sistemi:

Suçlu Profili:

Mağdur Profili:

Suç Delilleri:

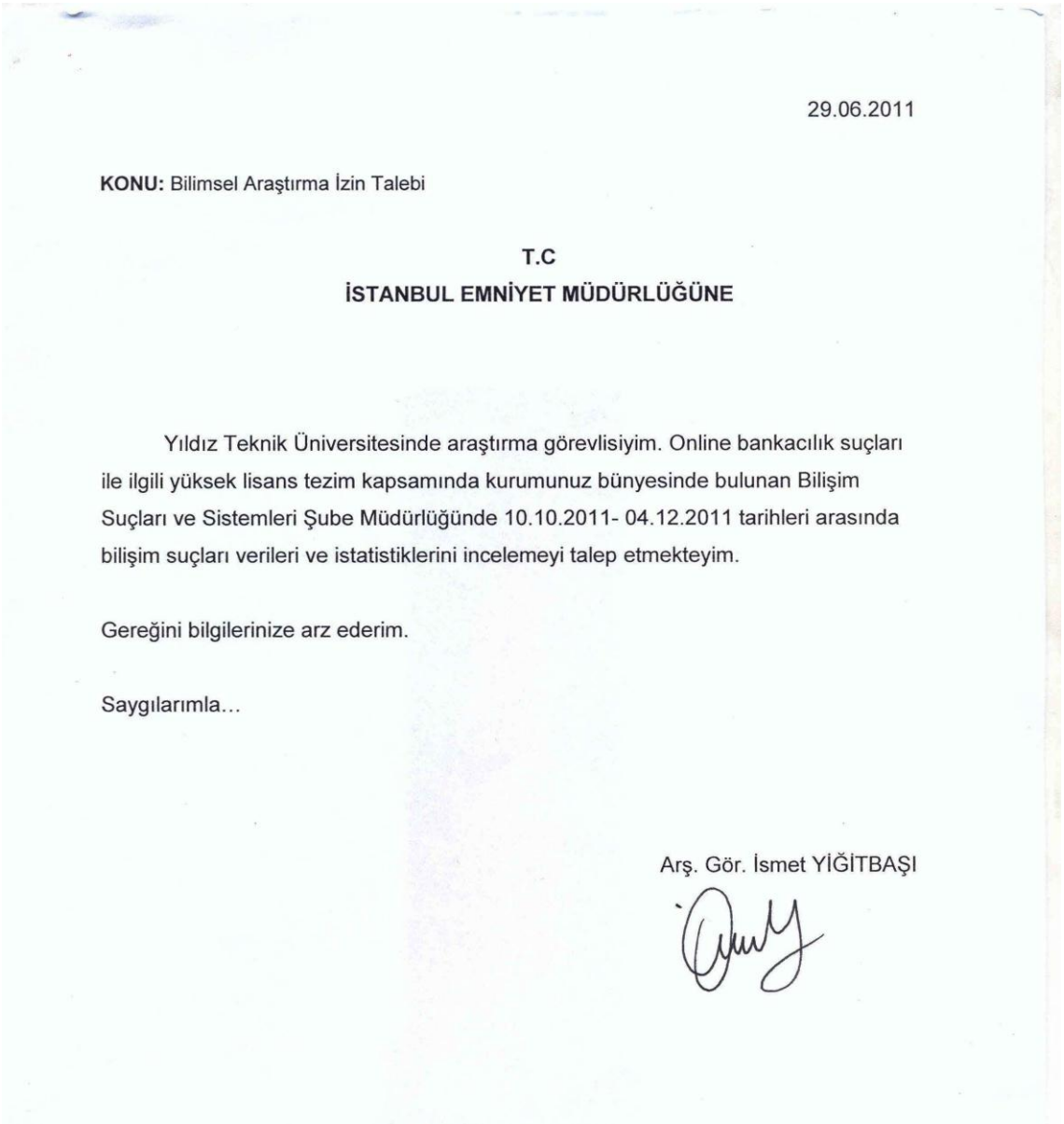
Suça Konu Olan Para:

Dava süresi:

Dava Sonucu:

Suçun Gerçekleşme Tarihi:

EK B- EMNİYET MÜDÜRLÜĞÜ ARAŞTIRMA İZİN DİLEKÇESİ



29.06.2011

KONU: Bilimsel Araştırma İzin Talebi

T.C
İSTANBUL EMNİYET MÜDÜRLÜĞÜNE

Yıldız Teknik Üniversitesinde araştırma görevlisiyim. Online bankacılık suçları ile ilgili yüksek lisans tezim kapsamında kurumunuz bünyesinde bulunan Bilişim Suçları ve Sistemleri Şube Müdürlüğünde 10.10.2011- 04.12.2011 tarihleri arasında bilişim suçları verileri ve istatistiklerini incelemeyi talep etmekteyim.

Gereğini bilgilerinize arz ederim.

Saygılarımla...

Arş. Gör. İsmet YİĞİTBAŞI

Şekil Ek.1 Bilimsel Araştırma İzin Talep Dilekçesi

EK C- BANKALARDA BİLGİ SİSTEMLERİ YÖNETİMİNDE ESAS ALINACAK İLKELERE İLİŞKİN TEBLİĞ İLGİLİ KISMI

İnternet bankacılığında uygulanacak hükümler

MADDE 24 – (1) Bu bölümde yer alan hükümler müşteriye ait finansal veya kişisel bilgilerin görülmesine, değiştirilmesine veya finansal sorumluluk yaratacak işlemlerin gerçekleştirilmesine imkân tanıyacak internet bankacılığı hizmetleri için geçerlidir. İnternet bankacılığına ilişkin her türlü altyapı bankanın bilgi sistemlerinin bir parçası olarak değerlendirilir. Bu bakımdan Tebliğin diğer bölümlerinde yer alan hükümler internet bankacılığı kapsamında yapılan çalışmalar için de geçerlidir. Bu bölüm altında yer alan maddelerin içerdiği hükümler, Tebliğin İkinci Kısım Birinci Bölümü altında yer alan aynı başlıklı maddelerin içerdiği hükümlere ilave olacak şekilde değerlendirilir.

Yönetim gözetimi

MADDE 25 – (1) İnternet bankacılığı faaliyetleri kapsamında sunulan bankacılık hizmetlerinin, internetin doğasından kaynaklanan güvenliği sağlayamama, kimliği doğru belirleyememe, inkâr edebilme ve sorumluluk atayamama gibi konularda bir takım ek risklere maruz kalacağı da göz önünde bulundurulur ve ilgili hizmetlere ilişkin süreçler üzerinde bu Tebliğin 26 ila 31 inci maddeleri arasında yer alan hükümler doğrultusunda ilave kontroller tesis edilir.

Güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi

MADDE 26 – (1) Güvenlik kontrollerinin yeterliliğini test etmek üzere bağımsız ekiplere, en az yılda bir kez olmak üzere, internet bankacılığı faaliyetleri kapsamındaki sistemler için sızma testleri yaptırılır.

(2) Banka, internet bankacılığı faaliyetleri kapsamında gerçekleşen sıra dışı ve şüpheli işlemleri tespit etmek için takip mekanizmaları kurar.

Kimlik doğrulama

MADDE 27 – (1) Banka, sunmakta olduğu internet bankacılığı hizmetleri için, bu hizmetlerin arz ettiği risk seviyelerine uygun ve güvenilir bir kimlik doğrulama mekanizması tesis eder. Müşterilerin, kurulan kimlik doğrulama mekanizmasından geçmeden hizmetlerden yararlanmasına müsaade etmeyecek bir yapı banka tarafından kurulur.

(2) Hizmetler için risk seviyelerinin tespiti yapılırken asgari olarak;

a) Müşteri tipi,

b) Müşteriye sunulan işlemsel olanaklar,

c) Banka ile müşteri arasında paylaşılan bilgilerin hassasiyeti,

ç) Kullanılan iletişim alt yapısı ve

d) İşlem hacmi

hususları dikkate alınır.

(3) İnternet bankacılığı için kimlik doğrulama işlemi, gerçekleştirilecek işleme taraf banka, müşteri ve varsa destek hizmeti kuruluşu gibi diğer müdahil tüm taraflar için yapılır.

(4) Müşterilere uygulanan kimlik doğrulama mekanizması birbirinden bağımsız en az iki bileşenden oluşur. Bu iki bileşen; müşterinin "bildiği", müşterinin "sahip olduğu" veya müşterinin "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Müşterinin "bildiği" unsur olarak parola/değişken parola bilgisi gibi bileşenler, "sahip olduğu" unsur olarak tek kullanımlık parola üretim cihazı, kısa mesaj servisi ile sağlanan tek kullanımlık parola gibi bileşenler kullanılabilir. Bileşenler tamamen müşterinin şahsına özgü olmalı ve bunlar sunulmadan kimlik doğrulama gerçekleştirilememeli, hizmetlere erişim sağlanamamalıdır.

(5) Kimlik doğrulamada elektronik imza kullanılması durumunda, yalnızca 15/01/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununun 4 üncü maddesinde düzenlenen güvenli elektronik imza kullanıldığı takdirde bu maddenin dördüncü fıkrasındaki hükümler yerine getirilmiş sayılır. Elektronik imza vasıtasıyla kimlik doğrulama gerçekleştirmede yabancı elektronik sertifikaların kullanılması halinde, bu fıkrada anılan Kanunun "Yabancı elektronik sertifikalar" başlıklı 14 üncü maddesinde ve ilgili alt düzenlemelerde yer alan hükümler geçerlidir.

(6) Müşterilere uygulanan kimlik doğrulamada kullanılacak parolaların ve değişken parolaların yönetilmesi için politika belirlenmeli, bu politika asgari olarak aşağıdaki hususları içermelidir;

a) Parolaların ve değişken parolaların tahmin edilmesi ve kırılması zor bir karmaşıklıkta ve uzunlukta olması, müşterilerin parolalarını ve değişken parolalarını belirlerken bu karmaşıklığı sağlayacak biçimde sistemsel olarak zorlanması,

b) Değişken parolaların, belirli bir süre için kullanılması, bu süre sonunda kullanım dışı kalması, müşterinin yeni bir değişken parola belirlemeye zorlanması; yeni değişken parolanın, son kullanılan belirli sayıdaki değişken paroladan farklı olmadığı sürece sistemin yeni değişken parolayı kabul etmemesi,

c) Parolaların ve değişken parolaların sıfırlanması işlemlerinin yeterli güvenlik kontrollerini içermesi,

ç) Müşterilerin, uygun parola ve değişken parola belirleme ve bunların gizliliğinin sağlanmasının önemi konusunda bilgilendirilmesi.

(7) Kimlik doğrulamada kullanılacak şifreleme teknikleri, güncel durum itibariyle literatürde kabul görmüş ve güvenilirliğini yitirmemiş algoritmaları baz

almalıdır. Kullanılacak şifreleme anahtarları, ilgili algoritmalar için anahtarın geçerli olacağı ve kullanılabileceği zaman zarfında kırılamayacak şekilde uzun seçilmelidir. Geçerliliğini yitirmiş, çalınmış veya kırılmış şifreleme anahtarlarının kullanılabilirliği engellenmelidir.

(8) Kimlik doğrulamada kullanılacak şifreleme anahtarları; bu anahtarların ele geçirilme ihtimallerini en aza indiren, gizliliğini sağlayan, değiştirilmesini ve bozulmasını önleyecek yöntemler barındıracak şekilde müşteri kullanımına sunulur. Şifreleme anahtarları kimlik doğrulama için kullanılmak istendiklerinde parola, PIN (Kişisel Tanımlama Numarası) veya biyometrik bir bileşen bilgisi ile erişilebilir olmalıdır.

(9) İnternet bankacılığı faaliyetleri kapsamındaki işlemlerin gerçekleştirilmesi için müşteriye işlem doğrulama kodu sorulması durumunda, kullanılacak doğrulama kodları tahmin edilmesi zor olacak şekilde yeterli uzunlukta alfabetik ve/veya rakamsal karakterden oluşmalı, rastgele yaratılmalı ve müşteriye internet kanalı haricinde bir iletim ortamı üzerinden ulaştırılmalıdır. İşlem doğrulama kodları, geçerli bir kodun tahmin edilmesine imkân vermeyecek şekilde değişken ve eşsiz olarak üretilmelidir.

(10) Tek kullanımlık parola sunan cihazlardaki bu bilgi belirli bir süre sonra siliniyor olmalı ve/veya bir temizleme olanağı ile cihazdan silinebilmeli, bu cihazların ürettiği parolalar, bilinen parola tahmin yöntemleriyle belirlenmesi imkânsız, değişken ve eşsiz olmalıdır.

(11) Müşterilere uygulanacak kimlik doğrulama mekanizmasında kullanılacak parola, değişken parola, tek kullanımlık parola cihazı, şifreleme gizli anahtarı, akıllı kart ve işlem doğrulama kodu gibi bileşenlerin üretim aşamalarından başlayarak müşteriye ulaştırılmasına kadar geçen sürecin tamamı boyunca güvenliği sağlanır ve müşteri kullanımına sunulduğu anda güvenilirliğinin bozulmadığından bankaca emin olunur.

(12) Banka tarafından internet bankacılığı faaliyetleri kapsamındaki işlemlerde kullanılmak üzere müşterilerine sunulan her türlü yazılımın kaynağının, ilgili banka olduğunun doğrulanabiliyor olması sağlanır ve bu yazılımların kullanıcı güvenliğini tehlikeye sokacak herhangi bir kod içermediğinin belirlenmesini sağlayacak kontroller banka tarafından yapılır.

(13) Banka tarafından oluşturulacak kimlik doğrulama mekanizmasının;

a) Başarısız kimlik doğrulama teşebbüsleri hakkında, ilgili müşterinin sisteme ilk girdiği anda bilgi vermesi, başarısız teşebbüslerin belirli bir sayıyı aşması halinde ise ilgili müşterinin internet bankacılığına erişimini bloke etmesi,

b) Başarısız kimlik doğrulama teşebbüsleri sonrasında, bu teşebbüsü gerçekleştiren kişiye, yanlış girilen kullanıcı bilgisi veya parolası/değişken parolası ile ilgili, örneğin böyle bir kullanıcının sistemde olmadığı veya parolanın/değişken parolanın yanlış girildiği gibi, gereksiz bilgi vermemesi

gerekir.

(14) Banka, tesis edeceği sistemler ve geliştireceği uygulamalarda müşterilerine ve personeline ait kimlik doğrulama bilgilerini ele geçirmeye yönelik bilinen saldırılara karşı gerekli sistemsel ve yazılımsal önlemleri alır.

(15) Olası tehditleri önceden belirleyebilmek ve gerekli önlemleri alabilmek adına, internet bankacılığı hesaplarına erişim için başarılı ve başarısız erişim teşebbüsleri düzenli olarak banka tarafından takip edilir, oransal bir anormallik görüldüğünde incelemeye alınır.

İnkâr edilemezlik ve sorumluluk atama

MADDE 28 – (1) Banka, sunmakta olduğu internet bankacılığı faaliyetleri kapsamında gerçekleştirilen işlemler için inkâr edilemezliği ve sorumluluk atamayı mümkün kılacak teknikleri kullanır ve kontrolleri tesis eder. Kullanılacak teknikler ve tesis edilecek kontroller, gerek banka için gerekse müşteri için, finansal sonuç doğuran her türlü işlemde, hem işlemi başlatan hem de işlemi sonuçlandıran tarafın gerçekleştirdiği işlemleri inkâr edememesini sağlamalıdır. Kullanılan tekniğin veya tesis edilen kontrollerin oluşturduğu denetim izleri delil teşkil edecek ve sorumluluk atayacak nitelikte olmalıdır.

(2) Kullanılacak teknikler kimlik doğrulama mekanizmasına dayalı ve onunla bütünleşik olabileceği gibi, tamamen inkâr edilemezliği ve sorumluluk atamayı sağlamaya yönelik de olabilir.

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

Denetim izlerinin oluşturulması

MADDE 29 – (1) Banka, tüm internet bankacılığı faaliyetleri için yeterli ve etkin bir denetim izi tutma mekanizması tesis eder. Banka asgari olarak;

a) Hesap açılışı, kapanışı ve hesapta değişiklik faaliyetlerine,

b) Finansal sonuç doğuran işlemlere,

c) Müşteri için verilen limit aşım onaylarına,

ç) İnternet bankacılığı sistemine erişimi düzenleyen hak, ayrıcalık ve kısıtlamalarda yapılan her türlü değişikliğe

ilişkin denetim izlerini tutar. Denetim izlerinin, gerçekleşen işlemlerin başlangıcından sonuna kadar akışını ve kaynağını gösterecek detayda bilgi içermesi gerekir.

(2) 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 yapılanmasını temin eder.

(3) Bu maddede bilgi ve belge tutulmasına ilişkin yer alan hükümler, diğer mevzuatın bilgi ve belge saklama ile ilgili hükümleri aynen saklı kalmak koşuluyla uygulanır.

Müşterilerin bilgilendirilmesi

MADDE 30 – (1) Banka, internet bankacılığı hizmetine ilişkin mevcut politika ve prosedürler ile dikkat edilmesi gereken hususlar konusunda müşterilerini bilgilendirir, gerekli uyarılarda bulunur.

(2) Banka, müşteri talebi olmadan internet bankacılığı hizmetini ilgili müşteri için kullanıma açamaz. Müşteri, internet bankacılığı hizmetine erişimi kapatmışsa veya kapattırmışsa, müşterinin yeni bir talebi olmadan internet bankacılığı hizmeti kullanıma açılamaz.

(3) Banka, internet bankacılığı hizmetinin verildiği internet sitesinde, erişilen sitenin bankaya ait olduğunu gösterecek teknikleri kullanır.

(4) Banka, internet bankacılığı hizmetini sunduğu internet sitesi üzerinden, kimliği ve kanuni statüsü ile ilgili bilgiler sunar. Bu kapsamda asgari olarak aşağıdaki bilgileri verir:

a) Bankanın ticari unvanı, genel müdürlük adresi,

b) Bankanın denetiminden sorumlu olan Bankacılık Düzenleme ve Denetleme Kurumuna ilişkin iletişim bilgileri,

c) Mevduatların sigortalanma koşul ve kapsamına ilişkin bilgiler.

(5) Banka;

a) İnternet bankacılığı servislerinin kullanımının taşıdığı riskler ve sağladığı faydalar ile internet bankacılığı servislerinden yararlanacak müşterilerin sorumluluk ve hakları hususunda müşterilerine açık ve anlaşılır bilgiler sunmakla,

b) Müşterilerin kişisel bilgilerinin gizliliğini sağlamaya ilişkin politika ve prosedürleri, banka güvenliğini zafiyete uğratmama hususunu gözeterek, müşteri dikkatine sunmakla,

c) İnternet bankacılığı servisi kapsamında hangi hizmetlerin verildiği ve bu hizmetlere erişim şartları ile güvenlik gereklilikleri konularında müşterilerini bilgilendirmekle,

ç) Müşterilerinde farkındalık yaratmayı amaçlayan yönlendirici güvenlik kılavuzları yayınlamakla ve banka güvenliğini zafiyete uğratmama hususunu gözeterek bu konudaki politika ve prosedürlerini müşterilerin dikkatine sunmakla,

d) İnternet bankacılığı sisteminde veya internet bankacılığı hizmetinin sunulduğu internet sitesinde yapılan erişilebilirliği etkileyebilecek değişiklikler hakkında müşterilerin bilgilendirilmesini sağlamakla

yükümlüdür.

(6) Banka ayrıca aşağıdaki hususlarda müşterilerini bilgilendirir;

a) İnternet bankacılığı hizmeti kapsamında sunulan servislerin nasıl kullanılacağı,

b) İnternet bankacılığı kanalı üzerinden bankacılık işlemlerinin güvenli bir şekilde gerçekleştirilebilmesi için müşteriler tarafından nelerin yapılması gerektiği, parola veya değişken parola seçiminde nelere dikkat edilmesi gerektiği, bunların güvenliğini sağlamaya ilişkin müşteri sorumlulukları,

c) Herhangi bir problemle karşılaşılması durumunda nelerin yapılması gerektiği,

ç) Sunulan ve alınan her bir hizmete ilişkin koşullar; tarafların açık ve tereddüde yer bırakmayacak şekilde sorumluluklarının ve görevlerinin tanımı.

(7) Bu madde kapsamında tanımlanmış olan müşteri bilgilendirmesine yönelik her türlü açıklama, bankanın internet bankacılığı hizmetini sunduğu internet sitesi üzerinden müşteri erişimine daima açık tutulur. Tüm açıklamalar mümkün olduğunca kısa ve anlaşılır olmalıdır. Açıklamalar internet bankacılığı hizmetinin verildiği sitede dikkat çekici bir yere yerleştirilir, müşterilerin en az bir kere okumasını garanti edecek şekilde yönlendirmeler ve sistemsel kısıtlamalar uygulanır.

(8) Banka, yaptığı pazarlama faaliyetleri, reklâmlar veya yayınlar vasıtasıyla müşterilerine internet bankacılığı sistemlerinin mutlak surette güvenli olduğu veya internet bankacılığı servislerinde hiçbir güvenlik riskinin bulunmadığı izlenimini ve bilgisini verecek ifadelerden kaçınır. Müşteriler internet bankacılığı risklerine ve tehditlerine karşı uyarılır ve bu hususlarda müşteri farkındalığı oluşturulması için azami özen gösterilir.

(9) Mobil iletişim cihazları üzerinden gerçekleştirilen internet bankacılığı işlemleri için de bu madde altında bahsedilen bilgilendirme zorunlulukları geçerlidir. Bu cihazların ilgili bilgilendirmeyi sağlama konusunda yetersiz kalması durumunda müşterinin söz konusu bilgilere farklı kanallar üzerinden ulaşması için gerekli yönlendirme yapılır.

Servis sürekliliği ve kurtarma planı

MADDE 31 – (1) Banka, internet bankacılığı servisi için beyan ettiği veya müşterilerine taahhüt ettiği düzeyde servis sürekliliğini sağlar. Servis kesintisinin doğurabileceği hukuki sorumlulukları en aza indirmek üzere banka gerekli önlemleri alır.

(2) Banka mücbir sebepler dışında müşterilerine önceden duyurmaksızın servis kesintilerine gidemez, internet bankacılığı servislerinde oluşacak kesintileri müşterilerine mümkün olduğunca önceden duyurur ve bu kesintilere ilişkin gerekçeleri de içerecek şekilde müşterilerini bilgilendirir.

(3) Servis süreklilik ve kurtarma planları geliştirilirken servis dışı bırakma atakları da göz önünde bulundurulur, bunlara karşı gerekli önlemler alınır.

EK D- ARAŞTIRMAYA DAİR FOTOĞRAFLAR

Şekil Ek.2 Bakırköy Adliyesi 27. Asliye Ceza Mahkemesi

Şekil Ek.3 Bakırköy Adliyesi 15. Asliye Ceza Mahkemesi

Şekil Ek.4 Bakırköy Adliyesi 8. Asliye Ceza Mahkemesi

Şekil Ek.5 Bakırköy Adliyesi 14. Asliye Ceza Mahkemesi

Şekil Ek.6 Kadıköy Adliyesi D Blok

Şekil Ek.7 Kadıköy Adliyesi 6. Asliye Ceza Mahkemesi

Şekil Ek.8 Pendik Adliyesi

Şekil Ek.9 Pendik Adliyesi 3. Asliye Ceza Mahkeme Kalemi

Şekil Ek.10 Pendik Adliyesi 3. Asliye Ceza Mahkemesi Duruşma Salonu

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı: İsmet YİĞİTBAŞI

Doğum Tarihi: 16.10.1985

Doğum Yeri: Hatay/Antakya

Medeni Hali: Bekar

Çalıştığı Kurum: Yıldız Teknik Üniversitesi

Görevi: Araştırma Görevlisi

Eğitim Durumu

Lisans: Yıldız Teknik Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Öğretmenliği (2004-2009)

Lise: Hatay Osman Ötken Anadolu Lisesi (1996-2003)

Yabancı Dil: İngilizce