BİLİŞİM YOLUYLA DOLANDIRICILIK VE KORUNMA YÖNTEMLERİ

YÜKSEK LİSANS TEZİ

Emin GÜRSOY

DANIŞMAN
Doç. Dr. Fehmi AKIN

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ

Haziran, 2015

AFYON KOCATEPE ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

BİLİŞİM YOLUYLA DOLANDIRICILIK VE KORUNMA YÖNTEMLERİ

Emin GÜRSOY

DANIŞMAN

Doç. Dr. Fehmi AKIN

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ

Haziran, 2015

TEZ ONAY SAYFASI

Emin GÜRSOY tarafından hazırlanan "**Bilişim yoluyla dolandırıcılık ve korunma yöntemleri**" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 17/06/2015 tarihinde aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü İnternet ve Bilişim Teknolojileri Yönetimi **Anabilim Dalı'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Doç. Dr. Fehmi AKIN

Başkan : Doç. Dr. Sinan YÖRÜK İmza
AKÜ Eğitim Fakültesi,

Üye : Doç. Dr. İbrahim Halil ÇANKAYA İmza
Uşak Üniversitesi Eğitim Fakültesi,

Üye : Doç. Dr. Fehmi AKIN İmza
AKÜ İktisadi ve İdari Bilimler Fakültesi,

Afyon Kocatepe Üniversitesi

Fen Bilimleri EnstitüsüYönetim Kurulu'nun

...../...../..... tarih ve

……. sayılı kararıyla onaylanmıştır.

…….

Prof. Dr. İbrahim EROL

Enstitü Müdürü

BİLİMSEL ETİK BİLDİRİM SAYFASI

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

17/06/2015

Emin GÜRSOY

ÖZET

Yüksek Lisans Tezi

BİLİŞİM YOLUYLA DOLANDIRICILIK VE KORUNMA YÖNTEMLERİ

Emin GÜRSOY

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü

İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı

Danışman: Doç. Dr. Fehmi AKIN

Bu araştırmada, bankacılık ve on-line ödeme işlemlerinin güvenli bir şekilde gerçekleştirilebilmesi için bu alanda karşılaşılabilecek dolandırıcılık yöntemlerinin tanınması ve alınabilecek önlemler noktasında farkındalık oluşturmak amaçlanmıştır.

Bilişim teknolojileri hayatımızın her alanına girerek kolaylıkları da beraberinde getirmiştir. Başta zaman tasarrufu sağlamasının yanı sıra ürün ve hizmetlerin de çeşitlenmesini sağlamıştır. Bu sayede eskiden evden çıkarak yapmak zorunda olduğumuz bankacılık ve alışveriş işlemlerini, bugün bilgisayarlarımızdan ve akıllı telefonlarımızdan yapabilmekteyiz. Teknoloji, bankacılık ve on-line alışveriş sektöründe de hız, zaman, maliyet, konfor ve güvenlik gibi birçok kalemde hizmet kalitesinin ve bağlantılı olarak kullanıcı memnuniyetinin artmasını sağlamıştır. Yine gelişen bu teknoloji kötü niyetli kişilerin eline geçtiğinde çok tehlikeli bir silah olarak insanların ekonomik ve sosyal yaşamını tehdit eder hale gelebilmektedir.

Klasik manada dolandırıcılık dediğimizde, dolandırıcı ile mağdur aynı mekânda bulunurken, işin içine bilişim teknolojisi girdiğinde farklı mekânlardan hatta farklı ülkelerden bile dolandırıcılık gerçekleştirilebilmektedir. Bu bağlamda teknoloji adeta suç işlemeyi kolaylaştırmıştır. Bankacılıkta, kısa zaman aralığında yüklü miktarda

paranın el değiştirebilmesi kolaylığından faydalanan dolandırıcılar, bu alanda yeni dolandırıcılık yöntemleri geliştirerek kullanmaktadırlar. Bu nedenle, alınabilecek küçük bir güvenlik önleminin alınmaması büyük maddi kayıplara sebep olabilmektedir. Bilişim yoluyla işlenen dolandırıcılık olaylarına baktığımızda, sade bir vatandaştan tutunda üst düzey bir kamu görevlisine ya da akademik kariyeri olan bir hocaya kadar geniş bir yelpazede mağdur kitlesi karşımıza çıkmaktadır. Bu mağduriyetlerden yola çıkılarak hazırlanan tezde, maddi kayıpları en aza indirebilecek çözüm önerilerinde bulunulmuştur.

Çalışmada betimsel tarama modeli kullanılmış ve araştırma verileri literatür taraması yapılarak elde edilmiştir. Tezin temelini oluşturan bilişim kavramı, bankacılık ve on-line ödeme işlemleri olarak sınırlandırılmıştır. Sonuç olarak, bilişim yoluyla karşılaşılabilecek dolandırıcılık olaylarını en aza indirebilmek ve güvenlik seviyesini en üst düzeye çıkarabilmek için bankacılıkta güvenlik parametresi olarak kullanılan kart ve şifre bilgisinin dışında farklı güvenlik çözümleri önerilmiştir.

2015, xiii+ 138 sayfa

Anahtar Kelimeler: Bilişim suçları, Kredi kartı dolandırıcılığı, İnternet dolandırıcılığı, Dolandırıcılıktan korunma yöntemleri

ABSTRACT
M.Sc. Thesis

CYBER FRAUD AND PROTECTION METHODS

Emin GÜRSOY
Afyon Kocatepe University
Graduate School of Natural and Applied Sciences
Department of Internet and Information Technologies Management
Supervisor: Assoc. Prof. Dr. Fehmi AKIN

In this research, it is intended that the banking and on-line payment transaction can be carried out safely by recognition methods and precautions to be taken from the fraud encountered in this area to create awareness.

By entering to every aspect of our lives, information technology has brought many conveniences. In addition to time saving, it has also increased the variety of products and services. Thus, while we had to get out of the house for shopping and banking, now we are able to do those through computers and smartphones. Technology has increased the service quality for banking and online shopping in terms of speed, time, cost, comfort and security, and so increased user satisfaction. However this technology, when fell into hands of malicious people, can become a very dangerous weapon and threaten the economic and social life of people.

While in the classical sense of the term fraud, the victim and the conman are located in the same place, but when information technology is involved, fraud can be carried out from different locations even from different countries. In this respect, technology has facilitated crime committing. Conmen, taking advantage of the easiness of transferring large amounts of money in short time, has developed new methods of fraud. That is why missing a small safety precaution can lead to big financial losses. When we look at IT

fraud, we can see that a wide range of victims, from a normal citizen to a high level public servant, or a professor with an academic career, is involved. This thesis is prepared, the solutions were made for minimizing the financial losses, by departing from these victimizations.

In this study, descriptive survey model have been used and research data have been obtained by literature scannning. Cyber concept, that the fundemantel of the thesis, is limited forms, as banking and on-line payment transactions. Eventually, for the purpose of minimizing incidents encountered by cyber fraud and maximizing the security to the highest level, (by) different security solutions have been recommended except of the card and password information used as the security parameters in banking.

2015, xiii + 138 pages

Key Words: Cyber crime, Credit card fraud, Internet fraud, Fraud protection methods

TEŞEKKÜR

Bu tez çalışması sırasında, bilgi ve tecrübesiyle bana her zaman destek olan danışman hocam Sayın Doç. Dr. Fehmi AKIN'a, her konuda öneri ve eleştirileriyle yardımlarını gördüğüm başta Sayın Doç. Dr. Sinan YÖRÜK hocam olmak üzere tüm hocalarıma, araştırma ve yazım süresince yardımlarını esirgemeyen tüm arkadaşlarıma teşekkür ederim.

Tez çalışmamı hazırlarken çoğu zaman ihmal ettiğim eşime ve çocuklarıma maddi ve manevi desteklerinden dolayı teşekkür ederim.

Emin GÜRSOY

AFYONKARAHİSAR, 2015

İÇİNDEKİLER DİZİNİ

Sayfa

KISALTMALAR DİZİNİ

Kısaltmalar

3G	Third Generation (Üçüncü Nesil)
ABD	Amerika Birleşik Devletler
AÖF	Açık Öğretim Fakültesi
ARPANET	Advanced Research Projects Agency Network (Gelişmiş Araştırma Projeleri Dairesi Ağı)
ATM	Automatic Teller Machine (Otomatik Vezne Makinesi)
BKM	Bankalar Arası Kart Merkezi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CD	Ceza Dairesi
CERN	Conseil Européen pour la Recherche Nucléaire (Avrupa Nükleer Araştırma Merkezi)
CGK	Ceza Genel Kurulu
DNS	Domain Name Server (Alan Adı Sunucusu)
DPT	Devlet Planlama Teşkilatı
FTP	File Transfer Protocol (Dosya Transfer Protokolü)
GPRS	General Packet Radio Service (Paket Anahtarlamalı Radyo Hizmetleri)
HTML	Hypertext Markup Language (Hiper Metin İşaretleme Dili)
HTTP	Hyper Text Transfer Protocol (Hiper Metin Transfer Protokolü)
IP	Internet Protocol (İnternet Protokolü)
İTÜ	İstanbul Teknik Üniversitesi.
NCP	Network Control Program (Ağ Kontrol Programı)
ODTÜ	Orta Doğu Teknik Üniversitesi
ÖSYM	Ölçme, Seçme ve Yerleştirme Merkezi
POS	Point of Sale (Satış Noktası)
PTT	Posta ve Telgraf Teşkilatı
SMTP	Simple Mail Transfer Protocol (Basit Posta Aktarım Protokolü)
SK	Sayılı Kanun
TCK	Türk Ceza Kanunu
TCP/IP	Transmission Control Protocol/Internet Protocol (Aktarım Kontrol Protokolü/İnternet Protokolü)
TDK	Türk Dil Kurumu
TİB	Telekomünikasyon İletişim Başkanlığı
TÜİK	Türkiye İstatistik Kurumu
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
ULAKNET	Ulusal Akademik Network
WİFİ	Wireless Fidelity (Kablosuz Bağlantı)

ŞEKİLLER DİZİNİ

Sayfa

RESİMLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

1.GİRİŞ

1.1 Araştırmanın Amacı

Teknolojik gelişmelere paralel olarak her geçen gün ortaya yeni ürünler çıkmaktadır. Bu yeni ürünlerin, ülkemizin refah seviyesinin artmasıyla birlikte herkes tarafından kullanılabilirliği de artmaktadır. Bu bağlamda yeni model bilgisayarlar, tabletler, akıllı telefonlar hayatımızın her alanına girmiş bulunmaktadır. Yine bilgisayarların, tabletlerin ve günümüz akıllı telefonlarının vazgeçilmezi olan internet, teknik alt yapının geliştirilmesiyle birlikte her geçen gün kullanımını ve hızını artırmaktadır. Gündelik hayatımızın her alanında etkin bir şekilde kullanmış olduğumuz interneti, akıllı telefonların yaygınlaşmasıyla birlikte cebimizde taşıyabilmekteyiz. Bu teknolojik gelişmeler doğrultusunda, eskiden evden çıkarak yapmak zorunda olduğumuz çoğu işimizi akıllı telefonlarımızla istediğimiz her yerden yapabilmekteyiz. Başta bankacılık ve alışveriş işlemleri olmak üzere çoğu alana kolaylıklar getiren bilişim teknolojileri bir taraftan da suç işlemeyi kolaylaştırmıştır. Bu manada teknolojinin güvenli kullanımının yaygınlaşmaması, kullanıcılarla bilgisayar korsanlarını baş başa bırakmaktadır. Bu karşılaşma genelde kullanıcıların maddi ve manevi olarak mağdur olması ile sonuçlanmaktadır. Çalışmada, bankacılık ve on-line ödeme işlemlerinin güvenli bir şekilde gerçekleştirilebilmesi için kullanıcılarda farkındalık oluşturmak amaçlanmıştır.

1.2 Araştırmanın Önemi

Bankalararası Kart Merkezinin internet sitesinde yayınlanan 2015 yılı Nisan ayı dönemsel istatistiki verilerine göre, yurt içi ve yurt dışında ülkemize ait banka kartlarıyla 166,7 milyon adet, kredi kartlarıyla 250,3 milyon adet alışveriş ve nakit çekim işlemi, yine internet üzerinden sanal poslar vasıtasıyla 26,1 milyon adet kartlı ödeme işlem gerçekleştirilmiştir. Bankacılıkta gerçekleşen bu kadar büyük işlem hacminin büyüklüğü kadar işlem güvenliğide büyük önem arz etmektedir. Çalışmada, bankacılık ve on-line ödeme işlemleri esnasında karşılaşılabilecek dolandırıcılık yöntemleri incelenmiş, alınabilecek önlemler belirtilmiştir. Tez, bu alanda yapılan az sayıda çalışma arasında yer alması nedeniyle ayrıca önem arz etmektedir.

1.3 Araştırma Modeli ve Aşamaları

Çalışmada betimsel tarama modeli kullanılmış ve araştırma verileri literatür taraması yapılarak elde edilmiştir. Çalışmanın ilk kısmı giriş kısmıdır. İkinci kısmında, tez içeriğinin daha iyi anlaşılabilmesi için öncelikle bilişimle ilgili temel kavramlar üzerinde literatür taraması yapılarak kavramlar irdelenmiştir. Yine bir biri ile ilişkili kavramlar olmasına rağmen farklı anlamlar ifade eden bilişim suçları ve bilişim yoluyla işlenen suçlar kavramı ayrıntılı bir şekilde açıklanarak bu suçlar ayrı ayrı incelenmiş ve aralarındaki ayrım netleştirilmeye çalışılmıştır.

Üçüncü kısımda, öncelikli olarak çalışmanın konusunu oluşturan dolandırıcılık suçu ile ilgili literatür taraması yapılarak tarihsel gelişimi araştırılmıştır. Sonrasında dolandırıcılık suçunun hukuki ve cezai boyutuyla, suçun unsurları ve nitelikli halleri ayrı ayrı belirtilerek, tezimizle direkt bağlantılı olan dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi (5237 sayılı TCK Md. 158/1-f) ayrıca geniş bir şekilde açıklanmıştır.

Dördüncü kısımda, ülkemizde kullanılan ödeme sistemleri incelenmiştir. Ekonomik değer taşımaları ve bu nedenle dolandırıcılık konularında başta hedef alınmaları nedeniyle kartlı ödeme sistemleri, mobil ödeme sistemleri ve dijital cüzdanlar ayrı ayrı incelenerek açıklanmıştır. Yine ülkemizde kullanılan ödeme sistemlerinin koordinasyonunu sağlayan Bankalararası Kart Merkezi ve bankacılık sektörüyle yakinen ilgili olan Kredi Kayıt Bürosu ile ilgili açıklama yapılmıştır.

Beşinci kısımda, çalışmanın en çok önem arz eden kısmını oluşturan bilişim yoluyla gerçekleştirilen dolandırıcılık yöntemleri dört ayrı başlık altında ayrıntılı bir şekilde incelenmiştir. Bu kısımda aktarılan bilgiler gündelik hayatta karşılaşılabilecek bilişim yoluyla dolandırıcılık olaylarının tanınması açısından büyük önem arz etmektedir. Teorik bilgilerin dışında, örneklerle ve resimlerle aktarılan bilgiler sayesinde farkındalık oluşturmak ve bu sayede mağduriyetleri en aza indirmek hedeflenmiştir.

Son kısımda bilişim yoluyla gerçekleştirilen dolandırıcılık olaylarında maddi kayıpların önüne geçebilmek adına alınabilecek önlemler, genel olarak, bankalar ve

kullanıcılar/müşteriler boyutuyla ayrı ayrı maddeler halinde sıralanmıştır. Bilişim teknolojilerini kullananların bildiği, bilmediği ya da bildiği halde bu güne kadar uygulamadığı güvenlik önlemleri, teorik bilgiler dışında karşılaşılabilecek durumlar örnekleriyle birlikte açıklanarak en yüksek düzeyde farkındalık oluşturulmaya çalışılmıştır.

1.4 Sınırlılıklar

Çalışmada işlenen bilişim kavramı, bankacılık ve on-line ödeme işlemleri olarak sınırlandırılmıştır.

2. BİLİŞİMLE İLGİLİ TEMEL KAVRAMLAR, BİLİŞİM SUÇLARI VE BİLİŞİM YOLUYLA İŞLENEN SUÇLAR

2.1 Bilişimle İlgili Temel Kavramlar

2.1.1 Bilişim Kavramı

Bilişim denildiğinde akla ilk olarak bilgisayar, internet ve teknoloji gibi kavramlar gelmektedir. Bilişim tanımları incelendiğinde, bazı tanımlarda bilişimin bir bilim dalı olarak değerlendirildiği, yine bilişimin bilgisayarı da içine alan üst bir kavram olduğu, bilgisayarın ise bilişimin bir ürünü olarak ortaya çıktığı görülmektedir (Akbulut 2000, Alaca 2008, Gürçam 2008).

Bilişim kelimesi dilimize 1967 yılında Fransız akademisi tarafından ortaya çıkan yeni bilim dalını tanımlamak için kabul edilen Fransızca "informatique" kelimesinden çevrilmiş olup Fransızca "information" ve "automatique" kelimelerinin birleşiminden türetilmiştir. Bu kelimeler dilimizde "enformasyon" ve "otomatik" kelimelerine karşılık gelmekte olup genel tabiriyle enformasyonun otomatik makineler aracılığıyla işlenmesi anlamındadır (Avşar ve Öngören 2010).

Enformatik olarak da kullanılan bilişim, verilerin işlenmesini ve iletilmesini ifade etmektedir. Verilerin işlenebilmesi için bilgisayar ve bilgisayar özelliği gösteren cihazların kullanılması gerekmektedir, bu nedenle bilişim ile bilgisayar iç içe geçmiş kavramlardır (Topaloğlu 2005).

Türk Dil Kurumu'nun web sitesinde yeralan bilim ve sanat terimleri ana sözlüğünde bilişim geniş bir şekilde tanımlanmıştır. Bu tanıma göre bilişim, "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. Disiplinler arası 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 (İnt. Kyn. 1).”

Aydın (1992)’a göre bilişim, “Bilginin iletişim yapısı ve özellikleri; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler ve öte yandan da; bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi, sibernetik, otomasyon ile insanın çalışma çevrelerindeki yerinde ve zamanında kullanılan teknolojileri temel alan bilgi sistemleri, şebekeleri, işlevleri, süreçleri ve etkinlikleridir.”

Akbulut (2000) bilişimi, “İnsanların teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin temeli olan bilginin elektronik araçlarla özellikle bilgisayarlar aracılığıyla işlenip, ses, görüntü ve veri taşıyan iletişim hatları aracılığıyla aktarılması bilimi” olarak tanımlamıştır.

Yine bilişimin bir bilim dalı olarak değerlendirildiği benzer bir tanımı Alaca (2008) “Teknik, ekonomik, sosyal, hukuki alandaki verinin, otomatik olarak işlenmesi, saklanması, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bilim dalı” olarak yapmıştır.

Literatürde yapılan bilişim tanımları incelendiğinde, bilginin işlenmesi, depolanması ve iletilmesi süreçlerinin temel alınarak tanımların yapıldığı görülmektedir.

Hukukumuzda bilişim kavramının ise 2005 yılı itibarıyla yürürlükte bulunan 5237 sayılı Türk Ceza Kanunu’nda Bilişim Sistemine Girme suçunun tanımlandığı 243. maddenin gerekçesinde, “Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir.” şeklinde belirtildiği görülmektedir. Tanımda verilerin toplanıp işlenmesi (veri işlem) belirtilmişken verilerin iletilmesi (veri iletişim) hususunun belirtilmediği, yukarıda

açıklanan tanımlar göz önünde bulundurulduğunda ise tanımın eksik olduğu görülmektedir (Erdağ 2010).

Bilişim kavramıyla ilgili başka bir eleştiri noktası da yasanın gerekçesinde belirtilen, verilerin otomatik işleme tabi tutulması hususunda olmaktadır. Otomatik işlem yapabilme kabiliyeti mekanik araçlara has bir özellik iken bilgisayarlar ve bilgisayar özelliği gösteren makineler işlemleri belli bir mantık ve düzen içerisinde elektronik olarak yapmaktadırlar (Dülger 2013).

Görüldüğü üzere zamanla yasalardaki tanımlar da eskimektedir. Bu bağlamda adalet duygusunun tam olarak tesis edilebilmesi adına teknolojik gelişmelere paralel olarak yasalarında revize edilerek güncellenmesi, yaşanılan zamanın ruhuna uygun, yeni çıkan teknolojileri de kapsayacak şekilde yeni suç tanımlarının yapılması ve uygulanması gerekmektedir. Bu şekilde yasa uygulayıcı birimlerin çalışma alanı etkinliği artırılarak en basiti bilişim, bilişim sistemi, bilişim alanı, bilişim suçu ve siber suç gibi kavramların tam olarak açıklığa kavuşturularak uygulamada birliğin sağlanması gerekmektedir.

2.1.2 Veri Kavramı

Veri, işlenmemiş ham bilgi topluluğu olarak tanımlanmaktadır. Sayısal, mantıksal, sembol ve işaret olarak değer alabilir. Veri, herhangi bir sınıflamaya, tasnife ve düzenlemeye tabi tutulmadığından, bilginin bu ham halinden yeterince faydalanmak mümkün değildir (Yurdanur 2009).

Literatürde, veri kavramının akademik çalışma alanına göre farklı tanımlamalarının olduğu görülmektedir. Dülger (2013)'e göre veri, "Bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği, sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgi olarak açıklanabilir."

Avrupa Konseyi Siber Suç Sözleşmesinin 1. maddesinde Bilgisayar Verisi, "Bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programıda kapsayan, olguları, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsilini ifade eder " şeklinde tanımlanmıştır (6533 SK 2014).

Ülkemizde bilişim kanunu olarak da bilinen 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun tanımlar başlıklı 2. maddesinin k bendinde veri, "Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer " olarak tanımlanmıştır.

Yapılan tanımlardan verinin, bilişim sisteminin çalışmasını sağlayan temel unsur olduğu görülmektedir. Veri, uygulamada kullanım alanına göre sayısal, mantıksal, işitsel ve görsel olarak farklı formatlarda değer almaktadır.

Bilgisayarın icadı ve ilk kullanılmaya başlandığı dönemde veriler bilgisayara insanlar aracılığıyla girilmekteyken, günümüz teknolojik gelişmeleri doğrultusunda insanların yanı sıra mikrofon, kamera, tarayıcı ve kullanım alanına göre çeşitli donanımlar vasıtasıyla bilgisayara veri girişi yapılabilmektedir. Plaka tanıma, parmak izi okuma, retina tarama ve sese duyarlı çalışan sistemler bilgisayara veri girişinde kullanılan sistemlere örnek olarak verilebilir.

Görüldüğü üzere bilişim biliminin temelini bilgisayar ve veri kavramı oluşturmaktadır. Bilgisayar olmadan veri, veri olmadan da bilgisayar düşünülemez. Bilgisayarlar sayesinde veriler yazılımlar aracılığıyla hızlı bir şekilde işlenerek, kullanıcısının değerlendirme yapacağı formlarda çıktı alınabilmektedir. Bilişim sürecinde veri; sayısal, mantıksal, işitsel ve görsel formlarda işlenerek bir noktadan diğer bir noktaya taşıyıcı sistemler vasıtasıyla aktarılabilmektedir.

Teorik olarak yapılan bilişim ve veri tanımlarının gündelik yaşamda karşımıza çıkan uygulamalarına baktığımızda;
Verinin işlenebilmesi için bilgisayar ve bilgisayar özelliği gösteren günümüzde revaçta kullanılan başta akıllı telefon, tablet ve pda gibi elektronik cihazlar,

Yine bu cihazların çalışabilmesi için üzerlerinde kurulu bulunan başta dünyaca ünlü Windows, Apple firmasının cihazlarında kullandığı Mac Os, akıllı telefonların vazgeçilmezi Android, Symbian yine açık kaynak kodlu Linux gibi işletim sistemleri,
Verinin işlenilerek istenilen formatta çıktı alınabilmesi için değişik dillerde yazılmış Microsoft Office, Photoshop ve Encase benzeri uygulama programları,
Verinin daha sonra tekrar işlenmesi ya da saklanması için manyetik (harddisk), elektronik (flash bellek) veya bulut bilişim benzeri hafıza birimleri,
Verinin istenilen noktaya iletiminin sağlanabilmesi için birden çok bilgisayarın bir birleri arasında gerek kablo (telefon, fiber optik vb.) gerekse de radyo frekansı ile belli protokoller (TCP-IP, NCP vb.) aracılığıyla bağlantı kurduğu görülmektedir.

2.1.3 Bilişim Sistemi

Bilişim sistemi; bilişim ve veri kavramlarını bünyesinde barındıran, veri-işlem ile veri-iletişim unsurlarını beraberce taşıyan araçlar bütünü olarak tanımlanmaktadır (Erdağ 2010).

Bilişim Ağı Hizmetlerinin Düzenlenmesi Ve Bilişim Suçları Hakkında Kanun Tasarısının tanımlar başlıklı 2. maddesinin 1. fıkrasının d bendinde bilişim sistemi, "Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem" olarak tanımlanmıştır.

Bilişimin çok geniş manada tanımlanarak geniş bakış açısıyla olgulara yaklaşması nedeniyle her bilgisayarın bir bilişim sistemi olduğu ancak herhangi bir bilişim sisteminin zorunlu olarak bir bilgisayar olmadığı kabul edilmektedir. Teknolojik gelişmelerle bilgisayarın çözemediği problemleri çözebilen bilişim sistemlerinin tasarlandığı bilinmektedir (Dülger 2013).

Bir bilim dalı olarak tanımlanan bilişimin, teknik manada sistemleşerek kullanılabilir hale gelmesiyle bilişim sistemi ortaya çıkmaktadır. Bilişim sistemi tabirine kulaklarımız oldukça aşinadır, öyle ki bu sistemler hayatımızda büyük boşlukları doldurmakta, yaşayışımızı kolaylaştırmakla birlikte yaşam kalitemizin de yükselmesinde büyük roller oynamaktadır.

Çalışmamızla bağlantılı olarak cep telefonu, tablet, ATM ve POS cihazlarını bilişim sistemi yönüyle incelediğimizde;
Cep telefonları ve tabletler, üzerlerinde bulunan mikro işlemcileri sayesinde veri işleme, hafıza birimleri sayesinde veri depolama ve wi-fi modülleri ya da gsm hattı (Gprs, 3G vb.) üzerinden internete bağlantı sağlayarak verinin iletişimini sağlamaktadırlar. Bu özellikler bir arada değerlendirildiğinde telefonların ve tabletlerin bilişim sistemi olduğu görülmektedir.

İlk çıktığı zamanlarda bankaların kapalı olduğu ya da hafta sonları da para çekebilmek için kullanılan ATM cihazlarından günümüzde birçok bankacılık işlemi yapılabilmektedir. Üzerlerinde kurulu bulunan işletim sistemi sayesinde verinin işlenmesini, sistemin ayrıca ağa bağlı olması nedeniyle bankanın veritabanına bağlantı sağlayarak limit ve benzeri kısıtlamaları sorgulayabilmesi yönüyle de verinin iletimini sağlamaktadırlar. Bu özellikleri nedeniyle ATM'lerin bilişim sistemi olduğu görülmektedir. ATM cihazlarının bilişim sistemi olduğu yönünde Yargıtay Ceza Genel Kurulunun 10.04.2001 tarih ve E. 2001/6-30, K. 2001/57 sayılı kararı bulunmaktadır.

Alışverişlerde nakit paranın yerine banka ve kredi kartları yaygın olarak kullanılmaktadır. Banka ve kredi kartları POS (Point of sale/Satış noktası) adı verilen elektronik cihaza okutularak veri işleme süreci başlamakta, yine kart bilgileri veri iletişim sürecinde POS cihazı ile banka arasında kurulan bağlantı/iletişim sayesinde ilgili bankadan sorgulamalar yapılarak limit ve benzeri sınırlamaların olup olmadığı kontrol edilmekte, olumlu sonuç dönmesi durumunda işlem onaylanmakta ya da sonlandırılmaktadır. Bu özellikleri nedeniyle POS cihazlarının bilişim sistemi olduğu görülmektedir.

2.1.4 Bilgisayar Nedir, Tarihçesi

Türk Dil Kurumu'nun web sitesinde yeralan güncel Türkçe sözlükte bilgisayar, "Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin" olarak tanımlanmıştır (İnt. Kyn. 2).

Bilgisayar, giriş birimleri vasıtasıyla dış dünyadan aldığı veriler üzerinde aritmetiksel ve mantıksal işlemler yaparak işleyen ve bu işlenmiş bilgileri çıkış birimleri ile kullanıcısına ileten, donanım (hardware) ve yazılım (software)'dan oluşan elektronik makinedir (Eralp 2007).

Erdağ (2010)'a göre "Bilgisayar, bir bilişim sistemidir. Hatta verilerin saklanması, işlenmesi ve iletilmesi bakımından en yaygın bilişim sistemi kuşkusuz bilgisayardır. Ancak bazen öğretide ve uygulamada aynı anlamda kullanıldıkları görülse de bilişim ve bilgisayar aynı şey demek değildir. Bilişim bilgisayara oranla daha geniş kapsamlıdır, bilgisayarı da kapsar."

Bilgisayar yazılım ve donanım olmak üzere iki kısımdan oluşmaktadır. Donanım bilgisayarın üzerine bulunan gözle görülüp elle tutulabilen tüm fiziksel parçalarını, yazılım ise bu fiziksel parçaların kendi aralarında uyumlu bir şekilde çalışmasını sağlayan soyut kod yapılarını ifade etmektedir.

Bilgisayar gündelik kullanımda ve literatürde; PC (personel computer), computer, kompütür, elektronik beyin, otomatik bilgi işlem makinesi gibi isimlerle isimlendirilmektedir. Yine bilgisayarın birçok tanımı bulunmaktadır. Bilgisayarın tüm bileşen ve özelliklerini kapsayan tanımının yapılması halinde gelişen teknoloji karşısında bu tanım yetersiz kalacak, zamanla yeni tanımlara ihtiyaç duyulacaktır.

Her bilgisayar elektronik bir cihazdır ancak her elektronik cihazı bilgisayar olarak nitelendirmek doğru olmayacaktır. Bilgisayarı kendisine benzeyen diğer cihazlardan ayırt eden fonksiyonunun ne olduğu konusu tam olarak açık değildir. Bilgisayarın, işlemlerini 4-5 temel işleme dayanarak yapması, programlanabilir ya da elektronik olması ayırt edici bir özellik değildir. Gelişmiş elektronik hesap makineleri, günümüzde kullanılan çamaşır makineleri ve fırınlar da bu özelliklere sahiptir (Alaca 2008).

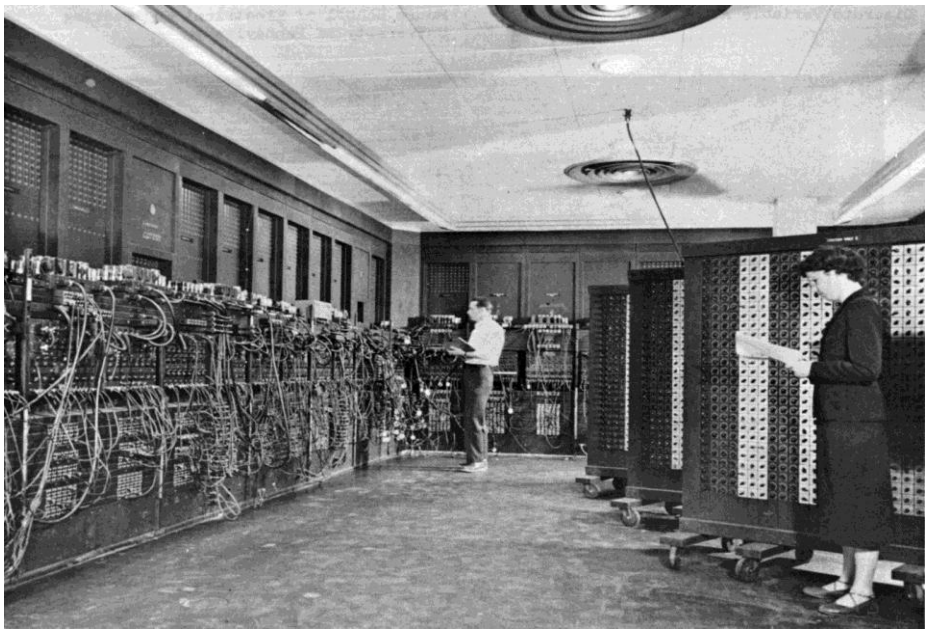
Alaca (2008)'nın aktardığı Yazıcıoğlu (1997) kaynağına göre bilgisayarı, elektronik hesap makineleri ve evde kullandığımız programlanabilir makinelerden ayırt eden en önemli özelliğinin "genel amaçlı" kullanılması olduğu belirtilmektedir.

Dülger (2013) bilgisayarları benzer makinelerden ayırt eden iki öğeden bahsetmiştir. Birinci öğede, bilgisayarın işletim yazılımının ya da uygulama yazılımının silinerek üzerine yeni yazılımların yüklenebilmesi ya da kullanıcının ihtiyaçlarına göre yüklü bulunan yazılımların yanına yeni yazılımların eklenebilmesiyle yeni özelliklerin kazandırılması. İkinci öğede, bilgisayarın yüklenebilirlik özelliğinin genel amaçlı olması ve bilgisayarın fiziki sınırları içerisinde her türlü işlemi yapabilmesi yani salt bir konuya özgülenmemiş genel amaçlı kullanılabilen bir makine olmasından bahsetmiştir.

Bu öğeler ışığında hesap makinesi, çamaşır makinesi, navigasyon aleti, araç yol bilgisayarının bilgisayar olmadığı anlaşılacaktır. Bu makineler daha önce belli işlemleri yerine getirebilmek için programlanmışlardır ve bu işlemler dışında herhangi bir işlem yerine getiremezler. Kısacası özel amaçlara yönelik kullanılmaktadırlar. Oysa ki bilgisayar, programcısının yazılım hüneri ve operatörünün kullanım alanına göre bir birinden bağımsız bir çok işi bir arada yerine getirebilmektedir. Buradan yola çıkarak smart phone, tablet pc ve pda'ları bilgisayar ya da bilgisayar özelliği gösteren cihaz olarak tanımlayabiliriz.

Hayatımızı kolaylaştırarak eğlenceli bir halde katan bilgisayarlar görünüşte çok kompleks yapılar olarak görünseler de temelde ikili sayı sisteminin 1 ve 0'larının kombinasyonlarından oluşmakta, elektronik olarak da devrenin açık ve kapalı olması prensibine göre çalışmaktadırlar (Karagülmez 2011).

Bilgisayarın tarihsel gelişimine baktığımızda ilk işlevsel bilgisayar 1943 yılında Pennsylvania Üniversitesinden J. P. Erkert tarafından bulunan ENIAC (Electronic Numerical Integrator And Calculator) olarak bilinmektedir. İlk bilgisayar olarak bilinen ENIAC, 30 ton ağırlığında ve 9x15 metrekarelik bir odayı doldurmaktaydı. Saniyede 5.000 işlem yapabilen ENIAC da yalnızca 80 karaktere eş veri hafızası bulunuyordu (Pala 2008). Resim 2.1'de ENIAC'a ait görüntü verilmiştir.



Resim 2.1 İlk bilgisayar ENIAC'a ait görüntü (İnt. Kyn. 3).

2.1.5 İnternet Nedir, Tarihçesi

İnternet, bilgiye ulaşmada hayatı kolaylaştırmada en çok kullanılan, yaşanılan zamana eğlence de katan son zamanların en büyük buluşudur. Bu yönleriyle internet hayatımızın vazgeçilmezleri arasında yerini almıştır. Öyle ki evden çıkmadan dünyanın diğer ucunda bulunan bir okula kayıt yaptırıp, internet üzerinden dersleri takip ederek mezun olunabilmekte, yine dokunup görmediğimiz ürünleri, bilgisayar ekranından seçerek ülke sınırları dışından evimize kadar getirtebilmekteyiz.

İnternet, İNTERnational ve NETwork kelimelerinin birleşiminden türetilmiş ve uluslararası ağ anlamına gelmektedir (Alaca 2008). Dünya üzerinde bulunan bilgisayarların ya da bilgisayar özelliği gösteren cihazların belli kurallar çerçevesinde birbirlerine bağlanmasıyla oluşan en büyük iletişim ağıdır.

Yurdanur (2009)'a göre internet, "Dünya çapında birçok bilgisayar ağının ortak bir protokol çerçevesinde haberleşmesini sağlayan ve bilgi kaynaklarının belirli izinler çerçevesinde paylaşımına imkân veren, sürekli yeni ağların katılımıyla gittikçe büyüyen en büyük ve en geniş ağdır."

Yalçın (2012)'a göre internet, "Birçok bilgisayar sisteminin birbirine bağlı olduğu, dünya çapında yaygın olan ve sürekli büyüyen bir iletişim ağıdır."

İnternet, dünya üzerinde üretilen bilgiye hızlı bir şekilde erişim ve paylaşma imkânı sunmaktadır. Gelişen teknolojilerle birlikte makul fiyatla ve güvenli bir şekilde herkes tarafından kullanılabilmektedir.

Yayla (2010)'nın aktardığı Buckland (1992) kaynağına göre "İnternetin geçmişi, 1800'lü yıllardan yayımlanmış olan bilimsel makalelerde teorik olarak bahsedildiği döneme kadar uzanmaktadır. Ancak internetin en önemli araçlarından birisi olan WWW uygulamasının teorik olarak bahsedildiği çalışma Vannevar Bush'un 1945 yılında yayınlamış olduğu "As We May Think" adlı makaledir. Bu makalede "Memex" (Memory Extension - Bellek Genişlemesi) adını verdiği teorik bir uygulamadan bahsetmektedir. Bu çalışma mikro filmler aracılığıyla bilgi ve görüntülerin uzun süreli saklanabileceği özel bir depolama yöntemini önermiştir."

İnternet ilk kez askeri amaçlı bir proje olarak ABD'de ortaya çıkmıştır. İkinci dünya savaşı sonrası soğuk savaş dönemindeki nükleer çatışma tehditleri nedeniyle 1960'lı yıllarda savunma amaçlı projelere büyük yatırımlar yapılmıştır (Baş 2013).

Bu projelerden biri de günümüzde kullanmış olduğumuz internetin atası olarak bilinen ARPANET'dir. ARPANET (Advanced Research Projects Agency Net) ABD Savunma Bakanlığı'nın araştırma konularında parasal destek sağlamak ile ilgili birimi olan ileri araştırma projeleri dairesi tarafından geliştirilmiştir. Daha sonra bu kurumun adı, başına Defense (savunma) sözcüğü getirilerek DARPA olmuştur. Bu daire 1957 yılının Ekim ayında ABD başkanı David Dwight Eisenhover tarafından kurulmuştur (Gönenç 2003).

Bilgisayarların birbirine bağlanması fikri ilk olarak 1962'de, ABD'de Masachusettes Teknoloji Enstitüsü'nden J.C.R. Licklider tarafından ortaya atılmıştır (Yayla 2010).

Licklider'in önermiş olduğu yapı, ARPA tarafından daha da geliştirilerek olası bir nüklüer savaş sonrası geleneksel haberleşme kanallarının zarar görmesi durumunda

iletişimin durmadan devamını sağlayabilmek için alternatif iletişim ağı oluşturmak fikriyle ARPANET (Advanced Research Projects Agency Net) olarak isimlendirilecek proje üzerinde çalışmaya başlamıştır. Zamanla bu proje büyük başarı göstermiş, ABD'de bulunan bütün üniversiteler ARPANET'e bağlanmıştır. Ağın büyümesi neticesinde kontrol güçlükleri oluştuğundan ARPANET ikiye ayrılarak Askeri siteler MILNET, askeri siteler dışında kalan siteler ve yeni siteler ARPANET'in parçası olmuşlardır (Gönenç 2003).

Bilgisayarların birbirlerine bağlanması birbirleri arasında iletişim kurması belli protokollere yani kurallar dahilin de olmaktadır. ARPANET'te bu protokol NCP (Network Control Protocol) olarak belirlenerek kullanılmıştır.

ARPANET'de ilk olarak kullanılan NCP protokolü ARPANET ağında bulunan bilgisayarların farklı türde ve yapıda olmaları nedeniyle iletişim sorunları ortaya çıkarmıştır. Bunun üzerine 1973 yılında ağ içinde kullanılmak üzere yeni bir protokol geliştirmek fikriyle Stanford University, University College London ve BBN (Bolt Beranek ve Newman)'in içinde bulunduğu bir internetworking projesi başlatılmıştır. 1978 yılına kadar İletim Kontrol Protokolü (TCP - Transmission Control Protocol)'nün dört uyarlaması geliştirilmiş ve denenmiştir. 1980 yılında bu küme sabitleşmiş ve ARPANET'e bağlı bilgisayarlar arasındaki iletişimi kolaylaştırmıştır. 1983'te tüm ARPANET kullanıcıları TCP/IP protokolü olarak bilinen yeni protokole geçiş yapmış ve standart olarak kullanılmaya başlanmıştır (İnt. Kyn. 4).

Günümüzde de halen kullanılmaya devam eden TCP (Transmission Control Protocol) / IP (İnternet Protocol) protokolü TCP ve IP olarak iki bölümden oluşmaktadır. Protokolün basit bir şekilde çalışma prensibine bakacak olursak; TCP, veri paketlerini çıkış noktasında küçük parçalara bölerek iletilmesini, varış noktasında da küçük paketlerin bir araya getirilerek birleştirilmesini böylelikle verinin taşınmasını sağlamaktadır. IP ise iletişim kuran makinelerin adres bilgilerini temsil etmektedir. Böylece veriler kaybolmadan çıktığı bilgisayardan istenilen bilgisayara ulaşmaktadır.
En eski ve en çok kullanılan TCP/IP protokolünün yanı sıra günümüzde bilgisayarlar arası dosya alma/gönderme protokolü olan FTP (file transfer protocol), elektronik posta

iletişim protokolü olan SMTP (simple mail transfer protocol) ve web ortamında birbirine bağlanmış farklı türden nesnelerin iletilmesi bir başka deyişle internet sayfalarının kullanıcılarına gösterimini sağlayan HTTP (hyper text transfer protokol) protokolü yaygın olarak kullanılmaktadır (Eralp 2012).

İnternet denince akla ilk olarak web siteleri gelmektedir. Oysaki internet ve web farklı kavramlar olup web siteleri internetin bir parçasıdır. Tarihsel gelişimde bu durumu göstermektedir. Bilgisayarlar arası iletişim kurularak noktadan noktaya bilgi paylaşımı sağlanarak kullanılmakta iken bizim bildiğimiz internet yani web sitelerinin keşfi 1989 yılında CERN laboratuarlarında Tim Berners-Lee tarafından HTML (hyper text markup language) işaretleme dilinin geliştirilmesi ve dünya çapında ağ (www) olarak da tanımlanan bilgi paylaşım sisteminin kurulmasıyla son halini almıştır (İnt. Kyn. 5).

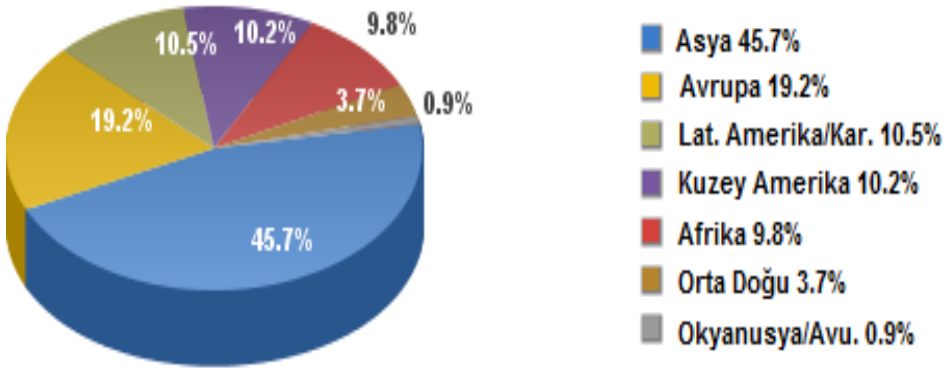
World wide web teknolojisinin 1989 yılında bulunmasına müteakip 1990 yılında bu teknolojinin dayandığı temel dosya transfer protokolü olan http protokolünün geliştirilmesi ile ARPANET tamamen ortadan kalkmıştır. Bütün ağ omurgalarının 1994 yılında birleşmesi ve bireysel kullanıma açılmasıyla bir zamanlar askeri bir güvenlik projesi olarak ortaya çıkan internet herkesin kullanımına açılarak bilgiye ulaşma ve paylaşma noktasında gündelik yaşamda yerini almıştır (Dülger 2013).

Kısaca ilk fikri ABD'de Licklider, Kleinrock ve arkadaşları tarafından ortaya atılan internet 1965-1970 yılları arası laboratuar testleri, 1970-1983 yılları arası saha testleri sonrasında 1983-1993 yılları arası üniversite, hükümet ve araştırma kurumları tarafından kullanılmaya başlanmıştır. 1993 yılında Mosaic (grafik arayüzlü web tarayıcı) programının ücretsiz olarak dağıtılması ile internet tüm iş dünyası ve ev kullanıcılarına ulaşarak bir anda yaygınlaşmıştır (Gürçam 2008).

2.1.6 Dünyada İnternet Kullanımı

İnternetin ilk olarak ABD'de bulunarak kullanılmaya başlanmasıyla birlikte, özellikle 1990'lı yıllar ve sonrasında internet teknolojisindeki hızlı gelişmelere paralel olarak dünyadaki internet kullanıcı sayısında da hızlı bir artış meydana gelmiştir. Bu artış, hem kullanıcı sayısında hem de alan adı sayısında hızlı bir artış olduğunu göstermektedir (Yalçın 2012).

Dünya üzerindeki internet kullanıcılarının coğrafik bölgelere göre dağılım oranlarına baktığımızda şekil 2.1'e göre küresel internet kullanıcılarının % 45,7 si Asya ülkelerinde bulunurken bunu % 19,2 ile Avrupa ve % 10,5 ile Latin Amerika/Karayipler takip etmektedir (İnt. Kyn. 6).



Şekil 2.1 İnternet kullanıcılarının dünyada coğrafik bölgelere göre dağılımı oranı-2014 (İnt. Kyn. 6).

Dünya üzerindeki internet kullanıcılarının sayısal dağılımlarına baktığımızda şekil 2.2'ye göre dünyada 2000 yılı Aralık ayı sonu itibarıyla 361 milyona yakın olan internet kullanıcı sayısının, 2014 yılı Haziran ayı itibarıyla aradan geçen 14 yılda 3 milyarı aşan internet kullanıcı sayısına eriştiği görülmektedir. Dünyanın % 42,3'ünü içerisine alan bu kullanıcı sayısı, internetin yayılımının hızlanarak devam ettiğini göstermektedir (İnt. Kyn. 6).

Çizelge 2.1 Dünya üzerindeki internet kullanıcılarının sayısal dağılımı-2014(İnt. Kyn.6).

DÜNYADA İNTERNET KULLANIMI VE NÜFUS İSTATİSTİKLERİ

(30 Haziran 2014 tarihi itibarıyla)

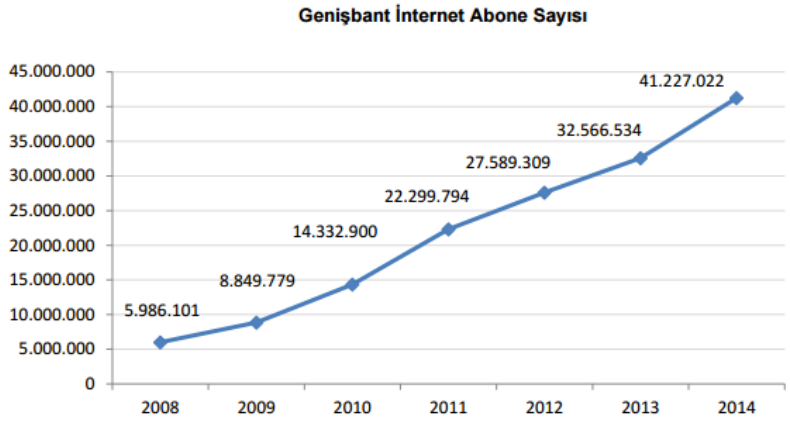
Dünya Bölgeleri	Nüfus (2014 Tahmini)	İnternet Kullanıcıları (31.12.2000)	İnternet Kullanıcıları Son Veriler	İnternete Erişim (% Nüfus)	Büyüme 2000-2014	Kullanıcılar % Tablo
Asya	3 996 408 007	114 304 000	1 386 188 112	34,7%	1,112.7%	45,7%
Afrika	1 125 721 038	4 514 400	297 885 898	26,5%	6,498.6%	9,8%
Avrupa	825 824 883	105 096 093	582 441 059	70,5%	454,2%	19,2%
Latin Amerika / Karayipler	612 279 181	1 068 919	320 312 562	52,3%	1,672.7%	10,5%
Kuzey Amerika	353 860 227	108 096 800	310 322 257	87,7%	187,1%	10,2%
Orta Doğu	231 588 580	3 284 800	111 809 510	48,3%	3,303.8%	3,7%
Okyanusya / Avustralya	36 724 649	7 620 480	26 789 942	72,9%	251,6%	0,9%
DÜNYA TOPLAMI	7 182 406 565	360 985 492	3 035 749 340	42,3%	741,0%	100,0%

2.1.7 Ülkemizde İnternet Kullanımı

Dünya üzerinde kısa sürede kendine yer edinen internet, ülkemizde de kitle iletişim araçları arasında yerini almış olup popülaritesini gün geçtikçe artırmaktadır. Ülkemizde ilk internet bağlantısı 1993 yılının Nisan ayında TÜBİTAK- ODTÜ (TR-NET) işbirliği ile bir DPT projesi çerçevesinde sağlanmıştır. 64 kbit/san hızındaki bu hat ODTÜ'den global internet ağına uzun bir süre ülkenin tek çıkış noktası olmuştur. Bu ilk bağlantıya müteakip olarak Ege Üniversitesi (1994), Bilkent (1995), Boğaziçi (1995) ve İTÜ (1996) bağlantıları gerçekleştirilmiştir (Çakır ve Topçu 2005).

İlk olarak akademik alanda kullanılmaya başlanılan internet, devamında gerekli teknik alt yapı çalışmaları neticesinde ticari olarak da kullanılmaya başlanmıştır. "1996 yılı Ağustos ayında da TURNET çalışmaya başlamıştır. 1997 yılına gelindiğinde, akademik kuruluşların internet bağlantısını sağlayan ULAKNET çalışmaya başlamış ve üniversiteler nispeten hızlı bir omurga yapısıyla birbirlerine bağlanmış ve internet kullanır hale gelmişlerdir. 1999 yılı içerisinde, ticari ağ altyapısında büyük değişiklikler olmuş ve TURNET'in yerini TTNET adında yeni bir oluşum almıştır (Bilek 2012)."

Geçen zaman zarfında, ülkemizde kablo internet alt yapısı genişleyerek güçlenmiş, bunun yanında teknolojik gelişmelerle birlikte kablosuz internet teknolojileri (Uydu, Gprs, 3G vb.) yaygınlaşmıştır. Şekil 2.3'de görüldüğü üzere 2008 yılı itibarıyla 6 milyona yakın olan genişbant internet abone sayısı 2014 yılı sonunda 41 milyonu geçmiştir (BTK 2015).



Şekil 2.2 Türkiye'de bağlantı çeşidine(*Sabit, mobil, kablo, fiber vb. tüm genişbant internet erişim yöntemleri dahil olup, çevirmeli (dial up) internet hariçtir*.) göre internet abone sayısı ile çeyrek ve yıllık bazda artış oranları (BTK 2015).

Tüik'in 2014 yılı Hanehalkı Bilişim Teknolojileri Kullanım Araştırması sonuçlarına göre;

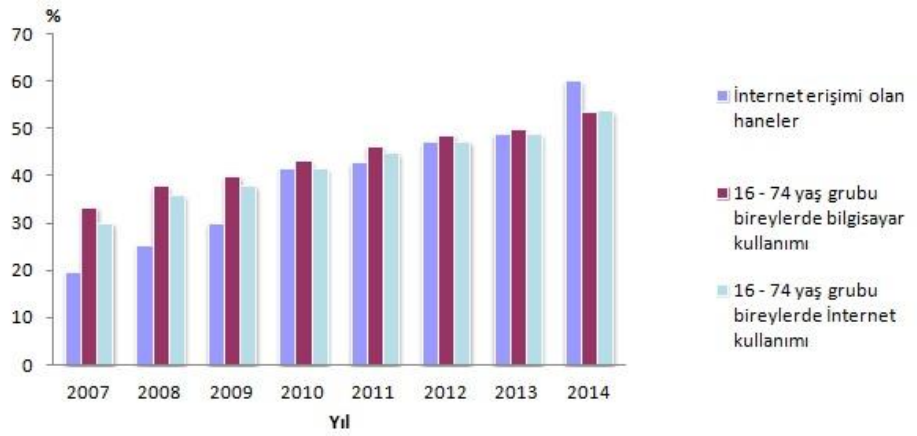
2014 yılı Nisan ayı itibarıyla Türkiye genelinde internet erişim imkanına sahip hanelerin oranı % 60,2 olmuştur. Şekil 2.4'ü incelendiğimizde 2007 yılında hane bazında internete erişim oranı % 20 civarındayken 2014 yılında bu oran % 60'ları bulmuştur. Ülkemizde internete erişim sağlayan hanelerin sayısında sürekli bir artış olduğu görülmektedir.

İnternete bağlantı çeşitliliğine baktığımızda; genişbant internet erişim imkânına sahip hanelerin oranı % 57,2 olmuştur. Buna göre hanelerin % 37,9'u sabit genişbant bağlantı (ADSL, kablo tv altyapısı üzerinden kablolu internet, fiber vb.) ile % 37'si mobil genişbant bağlantı ile ve % 6'sı da darbant bağlantı ile internete erişim sağlamıştır.

Hane halkının internet kullanım amaçlarına baktığımızda, 2014 yılının ilk üç ayında internet kullanan bireylerin % 78,8'i sosyal paylaşım sitelerine erişim sağlarken, bunu

% 74,2 ile on-line haber, gazete ya da dergi okuma, % 67,2 ile mal ve hizmetler hakkında bilgi arama, % 58,7 ile oyun, müzik, film, görüntü indirme veya oynatma, %53,9 ile e-posta gönderme-alma ve % 30,8 kişisel kullanım amacıyla mal veya hizmet siparişi verme ya da satın alma takip etmiştir (TÜİK 2014).

Temel Göstergeler 2007-2014



Şekil 2.3 Tüik hanehalkı bilişim teknolojileri kullanım araştırması (TÜİK 2014).

2.2 Bilişim Suçları

2.2.1 Bilişim Suçu Kavramı

Bilim insanlarının çalışmaları neticesinde 1940'lı yıllarda icat edilen bilgisayar ve 1960'lı yıllarda bilgisayarların birbirine bağlanması fikriyle ortaya çıkan internet insanoğlunun yaşamında yeni bir dünyanın kapılarını aralamıştır. Bu yeni dünyada bilişim ve internet teknolojileri hızla gelişerek insanoğlunun yaşamının her evresinde yerini almıştır. Bir taraftan bu teknolojik yenilikler yaşamı kolaylaştırırken, diğer taraftan da kötü niyetli insanlar ve organize çeteler için yeni suç işleme alanı ve yöntemleri ortaya çıkmıştır.

Bilgisayarların bilinilirliğinin artmasıyla birlikte bilgisayarın yaşamımızda bir parantez açacağı, on kadar bilgisayarın bütün bilgi işlem ile ilgili sorunları çözeceği düşünülmekteydi. Ancak bilgisayarların herkes tarafından kullanımının yaygınlaşması ile birlikte bütün tahminler altüst oldu. Bu gelişme 1960'lı yılların sonunda toplumda

yeni bir olgu olan bilişim suçu olgusunu ortaya çıkardı ve tarihte bilinen ilk bilişim suçu 18 Ekim 1966 tarihli Minneapolis Tribune de yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı makale ile kamuoyuna duyurulmuştur (Aydın 1992a).

Dünyada bilgisayarın ilk olarak Amerika Birleşik Devletlerinde ortaya çıkması ve kullanılması nedeniyle bu alanda işlenen suçların isimlendirilmesi Amerikan hukukçuları tarafından yapılmıştır. Bu bağlamda computer related crime (bilgisayar bağlantılı suç), computer assisted crime (bilgisayarla işlenen suç), crimes against computer (bilgisayara karşı işlenen suç) ve yaygın olarak da computer crime (bilgisayar suçu) kavramı kullanılmaktadır. Amerikan Hukuku'nda bilişim suçu kavramı, "bilgisayar verilerinin çalınması ya da sabote edilmesi veya herhangi bir suçun işlenmesi için bilgisayarın kullanılması gibi bilgisayar teknolojisini gerektiren suç çeşidi" olarak tanımlanmıştır (Dülger 2013).

Kale (2014) bilişim suçlarının tanımlanmasında herkes tarafından kabul gören bir tanımın olmadığını belirterek en geniş kabul gören tarifin, o zamanki adıyla Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun 1983 yılı Mayıs ayında Paris'te yapmış olduğu toplantısında bilişim suçlarının "bilgileri otomatik işleme tabi tutulan veya verilerin nakline yarayan bir sistemle gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış" olarak tanımlandığını, yine hukuki ve teknik terminolojinin dışında genel anlamda yapılacak bilişim suçları tanımının "teknolojinin yardımı ile genellikle sanal bir ortamda kişi veya kurumlara maddi veya manevi zarar vermek" olarak yapılabileceğini belirtmiştir.

Eker (2006) literatürde herkes tarafından kabul gören tanımın yapılamamasının nedenini, olgunun yeni olmasının yanı sıra bilişim teknolojilerinin sürekli devinim ve gelişme içerisinde bulunması ve dolayısıyla her geçen gün bir yeniliğin ortaya çıkması ve var olan teknolojilerin farklı biçimlerinin gündeme gelmesi gibi sebeplerden kaynaklandığını belirterek, bu alanda ana hatlarıyla kapsayıcı ve karma bir tanımı "bilişim araçlarına/sistemlerine karşı veya bilişim araçları/sistemleri vasıtasıyla işlenen,

verilerle, veri-işlem ile veri-aktarımlarıyla ilgili olan suç şekilleri" şeklinde yapmaktadır.
En anlaşılır şekliyle, bilgisayarlara/bilişim sistemlerine karşı ya da bilgisayarlar/bilişim sistemleri aracılığıyla yapılan hukuk ihlallerinin bilişim suçu olarak kabul edilerek bu yönde cezai yaptırımların düzenlendiği anlaşılmaktadır.

Ülkemizde, internet ve bilişim teknolojileri kullanılarak işlenen suç tipi tanımlanırken bilişim suçları kavramının yanı sıra siber suçlar, sanal suçlar, bilgisayar suçları, internet suçları, dijital suçlar ve ileri teknoloji suçları gibi kavramların kullanıldığı görülmektedir.

Taşkın (2008)'a göre bilişim sistemleri aracılığıyla işlenen suçlara "internet suçları" denerek kavram daraltıldığında suçun, internetin daha küçük kapsamlı hali olan belirli bir kuruluş içerisinde bilgisayarların birbirlerine bağlanarak oluşturulduğu intranet yapısı içerisinde işlenmesi durumunda bu kavramın yetersiz kalacağı ve bu durumda da bu alanda yapılan eylemlerin yaptırımsız kalabileceği belirtilmektedir.

Diğer bir kavram darlığı da bu alanda işlenen suçları "bilgisayar suçları" olarak tanımlamak olacaktır. Öyle ki teknolojik gelişmelerle birlikte akıllı telefonların, televizyonların ve çoğu elektronik cihazın içerisinde bilişim sistemi özellikleri barındırdığı görülmekte ve bu cihazlar üzerinden de suç işlenebildiği bilinmektedir. Bu yönüyle bu kavramın yetersiz kaldığı aşikârdır. Buna karşın öğretide kabul gören ve en çok kullanılan bilişim suçu/suçları kavramının teknolojik gelişmeler karşısında en kapsayıcı ve isabetli tabir olduğu anlaşılmaktadır.

Literatürde bilişim suçlarının tasnifinde de bir birlikteliğin olmadığı, farklı şekillerde tasniflerin yapıldığı görülmektedir. Aydın (1992b) bu tasnifi, bilişim sistemlerine karşı işlenen suçlar ve bilişim sistemleri ile işlenen suçlar şeklinde yapmıştır.

Ersoy (1994) bu tasnifi, bilişim araçlarına karşı suçlar, bilişim sistemleri ile işlenen suçlar ve bilişim sistemlerine karşı suçlar şeklinde yapmaktadır.

Diğer bir tasnifi Yazıcıoğlu (2004) bilgisayar marifetiyle işlenen klasik suçlar ve bilişim teknolojilerinin özelliğinden kaynaklanan yeni suç türleri şeklinde yapmaktadır.
Farklı bir tasnifi Eker (2006) bilişim sistemleri aracılığıyla işlenen suçlar (md.142/2-e, md. 158/1-f) ve bilişim sistemlerine karşı suçlar (md.243, md.244, md.245, md.246) şeklinde yapmaktadır.

Mahmutoğlu (2013) bu tasnifi, sadece bilişim sisteminin kullanılmasıyla işlenebilen suçlar (doğrudan ya da dar anlamda ve yahut gerçek bilişim suçları), bilişim sisteminin kullanılması zorunlu olmamakla birlikte, bazı suçların nitelikli hali olan suçlar ve kanunda bu sistemin kullanılması zorunlu olmamakla birlikte, söz konusu sistemin suçta vasıta olarak kullanıldığı suçlar, şeklinde ayrımlara tabi tutmuştur.

Tasnifler incelendiğinde teknolojik gelişmelerle birlikte farklı nitelendirmelerin ortaya çıktığı, ancak bilişim sistemlerine karşı ve bilişim sistemleri aracılığıyla işlenen suçlar şeklinde iki ayrımın yapılarak ortak paydada buluşulabileceği görülmektedir.

2.2.2 Hukukumuzda Bilişim Suçları

Teknolojik yeniliklerin toplumun her kesimine yayılması ve kullanılabilirliğinin artması zaman almaktadır. Bilişim toplumunun nispeten yeni bir kavram olması nedeniyle doğal olarak bilişim hukuku da yeni bir hukuk dalı olarak ortaya çıkmaktadır. Hukuk yavaş değişen ve toplumu daima geriden takip eden bir bilim dalıdır. Bunun nedeni hukuk kurallarının toplumun ihtiyacına ve beklentilerine göre şekillenmesidir. Bilişim toplumuna dönüşüm henüz yeni olduğundan bilişim hukuku da yeni yeni şekillenmektedir. Gelişmiş ülkelerde özellikle ABD ve Avrupa ülkelerinde bilgisayar kullanımının yaygınlaşması ile birlikte ortaya çıkan hukuksal sorunların çözülmesi adına yeni yasal düzenlemelerin yapılması, ülkemizde de bilişim suçları alanında düzenleme yapılmasına yol açmıştır.

Bilişim suçu kavramı ve cezai müeyyidesi ülkemiz hukukuna ilk olarak Fransız Hukuku'nun bu konudaki düzenlemelerinden esinlenilerek yürürlükte bulunan 765 sayılı ETCK'ya 14.06.1991 tarih ve 3756 sayılı yasanın 20. maddesi ile 525. maddeden sonra gelmek üzere "Bilişim Alanında Suçlar" başlığı altında 11. babı eklenerek giriş

yapmıştır. Kanunda 525 a, b, c ve d olarak sıralanan maddelerin ilk üçünde suç tipi olarak belirlenen eylemler ve sonuncusunda ise fer'i cezalar düzenlenmiştir (Karagülmez 2011).

Dülger (2013)'e göre, bu düzenlemenin 5237 sayılı TCK'nın genel düzenleme mantığı olan "suçla korunan hukuksal değer " kavramının dışında bilgisayar ortak kavramı temel alınarak yapıldığı ve bu düzenlemede, Verilerin ele geçirilmesi suçu (md.525 a/1), Başkasına zarar vermek için verilerin kullanılması, nakledilmesi veya çoğaltılması suçu (md. 525 a/2), Verilere veya veri işleme zarar verilmesi suçu (md. 525 b/1), Bilgisayar aracılığıyla hukuka aykırı yarar sağlaması suçu(md. 525 b/2) ve Verilerde sahtekarlık yapılması suçu (md. 525 c) olmak üzere beş farklı suç tipinin düzenlendiği belirtilmektedir.

Özel kanunlarda düzenlenen bilişim suçlarına baktığımızda; 5846 sayılı Fikir Ve Sanat Eserleri Kanunu'nda 07.06.1995 tarih ve 4110 sayılı yasa ile yapılan değişiklik neticesinde bilgisayar programları da sanat eseri sayılarak bilgisayar programlarına karşı gerçekleştirilen eylemler de yaptırım altına alınmıştır (Taşkın 2008).

1991 yılında ilk kez hukukumuza giren bilişim suçları, 01.06.2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu ile tekrar düzenlenerek, kanunun özel hükümleri düzenleyen ikinci kitabının "Topluma Karşı Suçlar" başlıklı üçüncü kısmının onuncu bölümünde "Bilişim Alanında Suçlar" başlığıyla yer almıştır. Bu bölümde, Bilişim sistemine girme (md.243), Sistemi engelleme, bozma, verileri yok etme veya değiştirme (md.244), Banka veya kredi kartlarının kötüye kullanılması (md.245) ve Tüzel kişiler hakkında güvenlik tedbiri uygulanması (md.246) suçları yer almaktadır.

Uluslar arası düzeyde bilişim suçları ile ilgili en kapsamlı düzenleme ise Avrupa Konseyi bünyesinde gerçekleştirilen Siber Suç Sözleşmesi (CONVENTION ON CYBER CRIME)'dir. Hazırlık süreci 4 yıl kadar süren sözleşme, 23 Kasım 2001'de konsey üyesi olmayan ülkeler de dahil olmak üzere Budapeşte'de imzaya açılmıştır. Siber Suç Sözleşmesi Türkiye Cumhuriyeti tarafından 10 Kasım 2010 tarihinde çekinceler belirtilerek imzalanmış ve bu sözleşme çekinceler ve beyanlar ile birlikte

TBMM'de "Sanal Ortamda İşlenen Suçlar Sözleşmesi" ismiyle onaylanarak, 02 Mayıs 2014 tarihi itibarıyla yürürlüğe girmiştir.

Bilişim suçlarını diğer klasik suçlardan ayıran birçok özellikten birisi de mağdur ile failin aynı ortamda bulunmamalarıdır. Hatta mağdur ile fail aynı şehirlerde olmamalarının yanı sıra farklı ülkelerde bile olabilmektedirler. Dünyayı çevreleyen bilişim ağları vasıtasıyla herhangi bir ülkeden herhangi bir bilgisayar kullanıcısına karşı suç işlenebilmektedir. Bu yönüyle bu suç türünün sınır aşan suçlar kapsamında olduğu ve suç soruşturma süreçlerinde ülkeler arası karşılıklı adli yardımlaşma mekanizmasının etkin bir şekilde kullanılarak suçun en hızlı şekilde aydınlatılması hedeflenmelidir. Ülkemizin de taraf olduğu Avrupa Konseyi Siber Suç Sözleşmesinin bilişim alanında soruşturma yürüten kolluk birimlerinin soruşturma kabiliyetini güçlendireceği değerlendirilmektedir.

2.2.3 Türk Ceza Kanununda Yer Alan Bilişim Suçu Türleri

Tez konumuz olan bilişim yoluyla dolandırıcılık suçlarına genelde 5237 sayılı TCK'da ayrı bir başlık olarak belirtilen bilişim suçları işlenerek geçiş yapıldığından, bu suçlara genel olarak değinilme ihtiyacı duyulmuştur. Bu bölümde incelenecek olan suç türleri aktarılırken maddenin tek tek unsurları açıklanmadan maddenin genel hatları irdelenerek bilgi aktarımı yapılacaktır.

2.2.3.1 Bilişim Sistemine Girme Suçu (TCK Md. 243)

5237 sayılı Türk Ceza Kanununun bilişim alanında suçlar başlıklı bilişim alanında işlenebilen suç tiplerinin tanımlandığı ilk maddesinde;

"Madde 243- (1) 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.
(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.
(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla

kadar hapis cezasına hükmolunur.” şeklinde düzenleme yapılmıştır.

Bu maddenin birinci fıkrasında suçun temel işleniş şeklini, ikinci fıkrasında ceza yönünden daha az cezayı gerektiren hali ve üçüncü fıkrasında ise neticesi sebebiyle ağırlaşmış hali düzenlenmiştir (Erdağ 2010).

Bu suç tipiyle, Avrupa Siber Suç Sözleşmesinin 2. maddesinde yeralan Yasadışı Erişim başlıklı düzenlemesine paralellik sağlanmaya çalışıldığı görülmektedir (Dülger 2013). 2. madde, “Taraflardan her biri, bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman, kendi iç hukuku kapsamında cezai bir suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir ” şeklinde düzenlenmiştir (6533 SK 2014).

Erdoğan (2012)’a göre bilişim sistemine girme ve kalma suçuyla korunmak istenen değerin karma nitelikte olduğu belirtilerek bu maddeyle, toplum düzeni, özel hayatın gizliliği, haberleşmenin gizliliği, kullanıcı ve sistem sahibinin menfaatleri, olası başka suçların işlenmesinin önlenmesi ve bilişim sisteminin güvenliği koruma altına alınmıştır.

Bu kanun maddesini toplum içinde yaşayan bireyler yönüyle ele aldığımızda, şahsımıza ait kişisel bilgisayarı bilgimiz ve iznimiz dışında yabancı bir kişinin açarak kullanmasını hoş karşılamayız, hatta kişisel bilgilerimize erişildiğini ve özel hayatımızın gizliliğinin ihlal edildiği düşünürüz. Yasa koyucu da buradan yola çıkarak bilgisayarımıza ya da veri tabanımıza ağlar vasıtasıyla uzaktan bağlantı sağlanarak bu bilgilere erişilmesini suç saymış, kişisel bilgileri ve özel hayatın gizliliğini koruma altına almıştır. Bu maddenin koruduğu değerler bağlamında toplum, özel sektör ve kamu yönüyle örnekler artırılabilir.

Madde metninde geçen “kimse” kelimesiyle, herkesin suçun faili ya da mağduru olabileceği yine fail ya da mağdurun taşıdığı sıfatı ya da görevi bakımından suçun faili ya da mağduru olmak konusunda herhangi bir öneminin olmadığı anlaşılmaktadır. Bundan 15-20 yıl öncesinde bilişim sistemlerine yetkisiz erişim, internet tabiriyle

hackleme konularında failin teknik bilgi, birikim ve tecrübesinin olması gerekirdi. Günümüzde bu alanda internet ortamında çok sayıda yazılı ve görsel bilginin bulunması ve bu bilgilere arama motorları sayesinde kolaylıkla ulaşılabilmesi ile sıradan insanların da bu bilgileri kullanarak bilişim sistemlerine yetkisiz erişim sağlayabildikleri görülmektedir.

Maddenin birinci fıkrasında, yalnızca bilişim sistemine girmiş olmakla failin cezalandırılamayacağı ayrıca failin sistemde bir süre kalma şartının tamamlayıcı unsur olarak arandığı görülmektedir. Ancak sistemde ne kadar süre kalmanın suç olarak nitelendirileceği, gerek kanun metninde gerekse de madde gerekçesinde açıklanmamıştır.

Gürocak, internet makalesinde bu süreyi, "failin sisteme girdiği andan itibaren sistemde yer alan verileri öğrenme, bu verileri kopyalama, değiştirme ve yok etme tehlikesinin oluşması için yeterli olacak kadar bir süre sistemde kalınması yeterli sayılmalıdır." şeklinde belirtmiştir (İnt. Kyn. 7).

Erdoğan (2012)'a göre, "failin bilişim sistemine eriştiğini öğrendiği anda sistemden hemen çıkmamış olması suçun tamamlanması için yeterlidir."

Süre konusunun somut olaya göre değişkenlik göstereceği aşikardır, bu nedenle süre hususunun mahkeme aşamasında değerlendirilmesi uygun olacaktır.

Bir de madde metninde geçen bedeli karşılığı yararlanılabilen sistem kavramından neyin kastedildiği açık değildir. Yine yasanın metninde ve gerekçesinde bu kavram hakkında açıklama yapılmamıştır. Bedel deyiminden yalnızca para anlaşılmamalıdır, bedelin herhangi bir karşılık olabileceği de değerlendirilmelidir. Ayrıca bu kavramdan karşılıksız yararlanma suçunun konusunu oluşturan "otomatlar" kastedilmemektedir. Otomatlar vasıtasıyla sunulan ve bedeli ödendiği takdirde hizmetten yararlanılması gereken durumlarda bedel ödenmeden fayda sağlanması eylemi 5237 sayılı TCK 163. maddede ayrı bir suç tipi olarak düzenlenmiştir (Taşkın 2008).

Dülger (2013)'e göre, bedeli karşılığı yararlanılabilen sistem kavramından, internet üzerinden ücret karşılığı hizmet veren web siteleri, internet kafe gibi yerlerde olduğu üzere belirli bir bedel karşılığı bilişim sisteminin kiralanması, bir kuruluş tarafından belli bir sistemin bedel karşılığı sunulması ve belli bir zaman ya da dönem sınırlamasıyla internet bağlantı servisinin sağlanması anlaşılmalıdır. Bugün için en çok bilinen ve karşılaşılan kavramların bunlar olduğu belirtilmektedir.

Literatürde, bedeli karşılığı yararlanılabilen sistemler kavramı hakkında birden çok görüş bulunmaktadır ve bu kavram halen tartışmalı bir durumdadır. Basit haliyle bedeli karşılığı yararlanılabilen sistemlerin kamuya açık olma niteliği taşımaları ve bedeli mukabilinde herkes tarafından kullanılabilir olması sebebiyle ve sonuç olarak sistemin tamamıyla kapalı bir sistem olmadığından hareketle, yasa koyucu tarafından ceza indirimine gidildiği düşünülmektedir.

2.2.3.2 Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK Md. 244)

"Madde 244- (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 halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur." şeklinde düzenleme yapılmıştır.

Yapılan bu düzenleme ile birlikte maddenin birinci fıkrasında bilişim sisteminin işleyişini engelleme veya bozmayı, ikinci fıkrasında bilişim sistemindeki verileri bozmayı, yok etmeyi, değiştirmeyi veya erişilmez kılmayı, sisteme veri yerleştirmeyi, var olan verileri başka bir yere göndermeyi, üçüncü fıkrasında birinci ve ikinci fıkrada

düzenlenen suçun ağırlaştırılmış halini ve dördüncü fıkrasında ise birinci ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması suç olarak tanımlamıştır.

Bu suç tipiyle, Avrupa Siber Suç Sözleşmesinin 4. maddesinde yeralan Verilere Müdahale ve 5. maddesinde yeralan Sisteme Müdahale başlıklı düzenlemelerine paralellik sağlanmaya çalışıldığı görülmektedir (Karagülmez 2011). Sözleşmenin 4. maddesi, "Taraflardan her biri bilgisayar verilerine haksız yere zarar verilmesi, verilerin silinmesi, tahrip edilmesi, değiştirilmesi veya engellenmesinin, kasten gerçekleştiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan her biri, 1. Paragrafta tanımlanan fiillerin ciddi zararla sonuçlanması gerektiğini şart koşma hakkını saklı tutabilir." 5. maddesi, "Taraflardan her biri, bilgisayar sistemlerine veri girişi yaparak, bu verileri ileterek, bilgisayar verilerine zarar vererek, bunları silerek, tahrip ederek, değiştirerek veya engelleyerek bir bilgisayar sisteminin işleyişinin haksız yere engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir." şeklinde düzenlenmiştir (6533 SK 2014).

Bu maddede düzenlenen suç tipiyle bilişim sisteminin veri ve yazılımlardan oluşan soyut unsurları ile birlikte bilişim sisteminin somut unsuru olan donanım kısmı da güvence altına alınmıştır. Bu yönüyle korunan hukuksal değer karma bir nitelik göstermektedir (Dülger 2013).

Madde gerekçesinde belirtildiği üzere bu düzenleme ile sistemlere yöneltilen zarar verme fiilleri özel bir suç hâline getirilmiştir. Bu bağlamda bilişim sisteminin, bu sistemin içerisinde yeralan verilerin veya diğer unsurların zarar görmemesi amaçlanmaktadır (Karagülmez 2011).

Failin suç işleme kastına göre sistemin işleyişinin engellenmesi veya bozulması durumunun düzenlendiği TCK 244. maddesinin ya da mala zarar verme suçunun düzenlendiği TCK 151. maddesinin uygulanıp uygulanmayacağına karar verilmektedir.

Sadece kişinin malvarlığına zarar verme kastıyla bilgisayara zarar vermesi durumunda TCK 151. maddesi, sistemi engelleme bozma kastıyla bilgisayara zarar vermesi durumunda ise TCK 244. maddesi hükümleri uygulanacaktır (Taşkın 2008). Görüldüğü üzere her iki durumda da bilgisayarın zarar görmesi nedeniyle sistemin işleyişi duracaktır. Ancak ceza tatbiki failin suç işleme kastına göre değişecektir.

"Sistemin engellenmesi teriminden, gereği gibi çalışmasının önlenmesi, faaliyet ve kapasitesinin sınırlandırılması, sistemin işleyişinin yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesi anlaşılmalıdır. Bozulma kavramından ise sistemin engellenmesi halinin en üst noktası olan durma noktasından daha da ileri olarak sistemin çökertilmesi, zarara uğratılması, işlemez hale getirilmesi, hatta fiziki olarak dahi zarar verilmesi anlaşılmalıdır (Avşar ve Öngören 2010)." Sistemin elektriğinin kesilmesi, çok önemli bir donanımının çıkarılması bu kapsamda değerlendirilebilir.

Sistemin engellenmesi ve bozulmasına en somut örnek DOS (Daniel of Service) saldırılarıdır. Hizmet aksatma olarak da bilinen bu saldırı türünde virüs bulaştırılarak zombi bilgisayar haline getirilen çok sayıda bilgisayar ile (bilgisayar ordusu) bir sunucu bilgisayara eş zamanlı ve çok sayıda istek gönderilmesi neticesinde, sunucunun kapasitesinin aşılması sonucunda da hizmet veremez hale getirilmesi amaçlanmaktadır. Bu saldırı türünün bilinen bir engelleme metoduda yoktur.

Güncel olarak da gerek ÖSYM'nin gerekse de AÖF'nin sınav sonuçlarını açıkladığı günlerde birçok kullanıcının sonuçları öğrenmek amacıyla siteye bağlanarak sorgu yapmaları neticesinde sunucuların eş zamanlı ve çok sayıda yapılan isteğe cevap veremeyerek siteye erişimin durduğuna ya da sistemin yavaş çalıştığına hepimiz şahit olmuşuzdur. Ancak burada saldırı yani suç işleme kastı yoktur. Tüm öğrencilerin merakla bir an evvel sonuçları öğrenme gayesiyle hareket etmeleri neticesinde bu durum ortaya çıkmaktadır.

İncelemiş olduğumuz maddenin birinci ve ikinci fıkrasında düzenlenen suç 5237 sayılı TCK'ya göre seçimlik hareketli bir suçtur. Birinci fıkrasında geçen, sisteminin işleyişini engellemek veya bozmak ve ikinci fıkrasında geçen sistemdeki verileri bozmak, yok

etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek eylemlerinden herhangi birinin ya da birkaçının birlikte işlenmesiyle suç işlenmiş sayılacak ve faile tek eylemden dolayı ceza verilecektir (Taşkın 2008).

İkinci fıkrada geçen kavramları kısaca açıklayacak olursak; bozmak, "verilerden elde edilmek istenen faydanın, değiştirme, tamamen veya kısmen tahrip etme gibi hareketlerle, elde edilememesini sağlamaktır." Virüs olarak adlandırılan zararlı yazılımlar aracılığıyla veri bütünlüğünün bozulması bozmaya örnek olarak verilebilir. Yok etmek, "verilerin ortadan kaldırılması anlamına gelmektedir." Verilerin bulunduğu sistem üzerinden silinmesi ya da bu sistemin formatlanarak biçimlendirilmesi ve yahut da verilerin bulunduğu taşınabilir belleğin, optik disk (cd, dvd, blue ray vb.)'in kırılması yok etmeye yönelik hareketler olduğu söylenebilir (Mahmutoğlu 2013).

Değiştirmek deyimiyle, "bir veri ya da veri grubu yerine başka verilerin konulması kastedilmektedir." Sistem yöneticisinin koymuş olduğu şifrenin yerine farklı bir şifrenin konulması örnek olarak verilebilir. Erişilmez kılmak**, "**Verilerin malikinin ya da ilgilisinin istediği zaman ve istediği verilere ulaşmasının engellenmesi anlamına gelmektedir." Örneğin hard diskimizde bulunan her dosyanın bir path (dosya yolu) yapısı vardır. Bu yapının silinmesi ya da değiştirilmesi durumunda dosyaya erişimimiz kalmayacaktır. Bu durum dosyanın silindiği anlamına gelmez. Farklı bir örnek de ise Yargıtay 11. CD (E:2010/9658 K:2012/ 21340)'nin vermiş olduğu karara göre Msn şifresinin kırılarak hesap sahibinin sisteme erişiminin engellenmesi bu kapsamda değerlendirilmiştir (Dülger 2013).

Sisteme veri yerleştirmek, "Bilişim sistemini kullanmakla yetkili olan kimsenin veya malikin izni olmaksızın sisteme dışarıdan herhangi bir verinin yerleştirilmesidir." İnternet ya da fiziksel/optik diskler aracılığıyla yapılan kaydetme, ekleme ve yükleme hareketleri bu kapsamda değerlendirilebilir. Var olan verileri başka yere göndermek ise, verilerin bulunduğu bilişim sisteminden başka bir bilişim sistemine yollayarak ya da kopyalamaya yarayan araçla kopyasının çıkarılarak aktarılmasını belirtmektedir. Verinin internet üzerinden e-posta yoluyla başka bir bilişim sistemine gönderilmesi ya

da fiziksel/optik diskler aracılıyla verinin kaydedilerek, kopyalanarak taşınması örnek olarak verilebilir (Taşkın 2008).

Maddenin üçüncü fıkrasında, birinci ve ikinci fıkradaki suçların ağırlaştırıcı hali düzenlenmiştir. Bu ağırlaştırıcı halin kabul edilmesinin nedeni, banka ve kredi kurumlarının herkes tarafından kabul gören güven kurumu olmaları ve bilişim suçlarında mali çıkar sağlamak amacıyla en çok hedef alınan kesimi oluşturması, kamu kurum ve kuruluşlarına ait bilişim sistemlerine yönelik suçların kişisel bir bilişim sistemine yönelik suça nazaran daha vahim sonuçlara hatta ülke güvenliğini tehdit edecek boyutta zararlara neden olabilmesidir (Boğa 2011).

Avşar ve Öngören (2010)'in madde kapsamında hukuka uygunluk sebebi ile ilgili görüşlerinde; web siteleri içerisinde bulunan bilgiler kamuya açık bilgiler olup herkes tarafından görülebilmesi nedeniyle önem arz etmektedir. Kişilerin, kendileri hakkında hakaret içeren ya da suçlayıcı beyanlar da bulunan web sitelerine karşı harekete geçerek kendileri hakkındaki bu verileri bozmaları veya değiştirmeleri halinde suç işlemiş olmayacaklarını, bu durumun meşru müdafaa hali kapsamında hukuka uygunluk sebebi olduğunu, bu maddede sayılan eylemlerin ancak hukuka aykırı olması durumunda cezalandırılacağını belirtmişlerdir.

2.2.3.3 Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK Md. 245)

"Madde 245 – (Değişik: 29/6/2005 – 5377/27 md.)
(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;
a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,
b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,
c) Aynı konutta beraber yaşayan kardeşlerden birinin,
Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.
(5) (Ek: 6/12/2006 – 5560/11 md.) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır." şeklinde düzenleme yapılmıştır.

Bu madde ile birlikte 5237 sayılı Türk Ceza Kanunu'nda ilk defa kredi kartları ile ilgili bir düzenleme farklı bir suç tipi olarak bilişim alanında suçlar başlığı altında kredi kartlarının kötüye kullanılması adıyla düzenleme yapılmıştır. Böylelikle 765 sayılı ETCK 525/b2 maddesinde düzenlenen "bilişim sistemi aracılığıyla hukuka aykırı yarar elde edilmesi suçunun" bankamatik ve kredi kartlarını kapsayıp kapsamadığı konusundaki tartışmalarda sonlandırılmıştır.

Kanunu koyucu, banka veya kredi kartları ile ilgili yapmış olduğu bu düzenlemesinde üç farklı suç tipine değinmiştir. Birinci fıkrada başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kişinin, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlamasını, ikinci fıkrasında başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmeyi, satmayı, devretmeyi, satın almayı veya kabul etmeyi ve üçüncü fıkrasında ise sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle yarar sağlamayı yaptırım altına almıştır (Erdağ 2010).

Suçun konusunu oluşturan banka veya kredi kartları 5464 sayılı Banka Kartları Ve Kredi Kartları Kanunu'nda düzenlenmiştir. Buna göre, **"**Banka kartı: Mevduat hesabı veya özel carî hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı

sağlayan kartı," ifade etmektedir. Kartla birlikte bankadan alınan şifre yardımıyla ATM üzerinden 7/24 hesapla ilgili tüm işlemler yapılabilmektedir. Ayrıca hesapta para bulunması şartıyla POS cihazları aracılığıyla mal ve hizmet alımı imkânı sunmaktadır.
"Kredi kartı: Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fizikî varlığı bulunmayan kart numarasını," ifade etmektedir. Banka ile yapılan sözleşme karşılığında belirlenen limit dahilinde gerek fiziksel gerekse de internet üzerinden sanal POS'lar yardımıyla mal ve hizmet satın alabilme, bunun yanı sıra nakit çekim imkanı sunmaktadır.
"Kart hamili: Banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek veya tüzel kişiyi," ifade etmektedir.

Birinci fıkrada geçen banka veya kredi kartının ele geçirilmesi ile ilgili olarak her ne suretle olursa olsun denilerek ele geçiriliş biçiminin önemli olmadığı vurgulanmıştır. Buradan kart sahibinin rızası ya da hile ile elde edilebileceği gibi çalınarak, bulunarak, zorla ya da hata ile de ele geçirilmiş olabilir. Belli bir kullanım imkânı tanınarak verilen banka veya kredi kartının yetki sınırları dışında kullanılması ile de bu suç oluşacaktır (Taşdemir 2009).

Banka veya kredi kartının ele geçirilmesi; sahibinin bilgisi olmadan, habersizce veya bularak kartın elde edilmesini belirtmektedir. Elinde bulundurma deyimi ise; ele geçirmeden sonraki süreçte yetkili ya da yetkisiz olarak kartın elde bulundurma durumunu ifade etmekte olup daha çok yasaya aykırı olmayan şekilde kartın elde bulundurulması halini anlatmaktadır. Kart sahibi; bankayla yapılan sözleşme gereği adına kart düzenlenen kişiyi, kartın kendisine verilmesi gereken kişi ise bankaca kart üretildikten sonra henüz teslim edilmediği aşamada banka görevlileri ya da teslimle görevli kişiler karşısında adına kart çıkarılan kişiyi ifade etmektedir. Kullanmak fiilinden kartı haksız yere kullananın fiili, kullandırtma fiilinden ise haksız bir kartı elinde bulunduranın başkasına bu kartı kullandırtma fiili anlatılmaktadır (Karagülmez 2011).

Başkasına ait banka veya kredi kartıyla hukuka aykırı olarak yarar sağlama biçimleri çeşitli şekillerde karşımıza çıkmaktadır. Görüleceği üzere madde metninde herhangi bir

sınırlamada yapılmamıştır. Buna göre günümüz teknolojisinde en yaygın, kartın otomatik para çekme makinesinde kullanılmasıyla, alışveriş maksatlı POS cihazlarında kullanılarak ya da veri iletim ağlarında kullanılmasıyla suç işlenebilmektedir (Dülger 2013).

Haksız yarar sağlama bağlamında en sık karşılaşılan yöntemlerden birisi de otomatik para çekme makinelerine kart sıkıştırma yöntemidir. Daha önceden kartın takılacağı hazne, kartı sıkıştıracak şekilde hazırlanmakta ve ATM'ye gelen mağdurun kartını hazneye takması ile birlikte kart hazneye sıkışmaktadır. Sonrasında fail müşteri gibi insancıl bir şekilde mağdura yaklaşmakta ve yardım etme bahanesiyle kart şifresini öğrenmektedir. Kartını çıkaramayan mağdur ATM'den ayrılınca, şifreyi öğrenen fail kartı cımbız yardımıyla hazneden çıkarmakta ve mağdurun parasını çekmektedir. Bu durum her ne kadar dolandırıcılık suçuymuş gibi görünse de, Karagülmez (2011)'e göre TCK 245/1. maddesinin uygulanması gerektiği belirtilmektedir. Yine bu yönde 11. CD'nin E:2010/7414 K:2012/9184 sayılı ve 17.05.2012 tarihli kararı bulunmaktadır.

Maddenin ikinci fıkrasında yer alan eylemin oluşabilmesi için tamamen sahte üretilen kartların veya gerçek olarak üretilmesine rağmen üzerinde değişiklik yapılarak sahteleştirilen kartların olması gerekmektedir. Teknik olarak birçok yolla sahte banka veya kredi kartının üretilmesi mümkündür (Eralp 2012).

Madde metninde geçen, "satma, sahte üretilen kartın üçüncü bir kişiye bedeli karşılığında verilmesini; devretme**,** bedel alıp almamaya bağlı olmaksızın elde bulundurulan sahte kartın üçüncü kişiye verilmesini; satın alma; sahte kartın bedel karşılığında alınmasını; kabul etme ise sahte kartın bir bedel olmaksızın alınmasını ifade etmektedir (Dülger 2013)." Böylelikle uygulamada karşılaşılabilecek her türlü hareket yaptırıma bağlanmış olmaktadır.

Dördüncü fıkrada fail bakımından ceza verilmeyecek hal düzenlenmiştir. Buna göre suçun sınırlı sayıda belirtilen akrabaya karşı işlenmesi halinde faile ceza verilmeyecektir. Bu durum ancak birinci fıkradaki suçları kapsamakta olup diğer fıkraları kapsamamaktadır (Karagülmez 2011).

Maddeye 2006 yılında eklenen beşinci fıkra ile birlikte, birinci fıkrada sayılan fiillerle ilgili olarak kanunun malvarlığına karşı suçlara ilişkin TCK'nın 168. maddesinde düzenlenen etkin pişmanlık hükümlerinin uygulanacağı düzenlenmiştir.

2.2.3.4 Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması (TCK Md. 246)

"Madde 246- (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur." şeklinde düzenleme yapılmıştır.

Bilişim suçu işleyen failin tüzel kişilik olması durumunda TCK 20. maddeye göre tüzel kişiler hakkında ceza yaptırımı uygulanamayacak ancak suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlara hükmolunacaktır (Taşkın 2008).

Tüzel kişiler hakkında uygulanabilecek güvenlik tedbirleri ise TCK 60. maddede "faaliyet izninin iptali" ve "müsadere" olmak üzere iki çeşit olarak düzenlenmiştir (Karagülmez 2011).

2.3 Bilişim Yoluyla İşlenen Suçlar

2.3.1 Bilişim Yoluyla İşlenen Suçlar Kavramı

Teknolojik gelişmeler toplumun dönüşümüne iyi yönde katkıda bulunduğu gibi suç işlemeye meyilli kötü niyetli kişiler için ise yeni suç işleme alanlarının kapılarını aralamıştır. Bu gelişme, kişilere, topluma ve hatta devletlere zarar verebilecek yeni bilişim suçu türlerini ortaya çıkarmıştır. Bunun yanı sıra klasik suç tipleri olarak tabir ettiğimiz daha önce yaşamış toplumlarda da var olan hırsızlık, dolandırıcılık, hakaret ve tehdit gibi suç türleri, fail ve mağdurun aynı mekânda etkileşim içinde olduğu suç işleniş metodundan farklı olarak mekân, zaman, sınır kısıtlaması olmaksızın bilişim sistemleri üzerinden işlenilebilir hale gelmiştir.

Akarslan (2011)'a göre, "bilişim yoluyla işlenen suçlar klasik (geleneksel) suçların bilişim yoluyla işlenmesidir." Bu suç türü, suçun işlenmesinde bilişim teknolojilerinin

araç olarak kullanılması neticesinde meydana gelmektedir.

Bilişim sistemleri üzerinden işlenebilen yukarıda saymış olduğumuz geleneksel suç türlerinin yanına zamanla yenilerinin eklenmesi muhtemeldir. Öyle ki hasta teşhis tedavi kayıtlarının bulunduğu sisteme yetkisiz erişim sağlanarak teşhis ve tedavi kayıtlarının değiştirilmesi durumunda hastanın ölümüne sebebiyet vermekle, bilişim yoluyla adam öldürme suçunun ortaya çıkması mümkün olabilmektedir (Dülger 2011).

Yukarıda saymış olduğumuz suçlar geneli mala karşı ya da şerefe karşı suçlardan olup suçun işlenmesinde bilişim teknolojilerinin kullanılması suça nitelikli hal kazandırmıştır. Sonuç olarak, bu saymış olduğumuz suçlar temelde bilişim suçu olmayıp, suçun işlenmesinde bilişim teknolojisinin araç olarak kullanılması söz konusudur. Böylelikle, bilişim suçu ve bilişim yoluyla işlenen suç ayrımının da belirginleştiği görülmektedir.

2.3.2 Türk Ceza Kanununda Düzenlenen Bilişim Yoluyla İşlenen Suçlar

2.3.2.1 Bilişim Sistemlerinin Kullanılması Suretiyle Hırsızlık (TCK Md. 142/2-e)

"Madde 142-(2)Suçun
e) Bilişim sistemlerinin kullanılması suretiyle," hırsızlık suçu düzenlenmiştir.

Hırsızlık suçu 5237 sayılı TCK 141. maddesinde, "Zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alan" kimsenin yapmış olduğu eylem olarak tanımlanmıştır.
Hırsızlık suçu malvarlığına karşı işlenen suçların en başta geleni ve en eski olanıdır. Bu eylemle mağdurun malvarlığında eksilme olurken, fail kendisine veya başkası lehine haksız zenginleşme sağlamaktadır (Eralp 2012).

TCK'nın 142. maddesinde hırsızlık suçunun nitelikli halleri düzenlenmiş olup birinci ve ikinci fıkra olmak üzere ikiye ayrılmıştır. Madde gerekçesinde, "Maddenin ikinci fıkrasında, hırsızlık suçunun birinci fıkraya nazaran daha ağır cezayı gerektiren nitelikli

şekilleri düzenlenmiştir." Buna göre bilişim yoluyla hırsızlık suçu daha ağır cezayı gerektiren nitelikli hal olarak ikinci fıkranın e bendinde yer almaktadır.

Taşkın (2008)'ın aktardığı Tezcan vd.(2007) kaynağına göre, öğretide basit hırsızlık suçunun düzenlendiği TCK 141. maddesinde somut nesnelerin çalınmasının yaptırıma bağlandığı belirtilerek bilişim yoluyla hırsızlık suçunda çalınan somut nesneler bulunmadığından TCK 142/2-e maddesinin uygulamasının zor olduğu görüşü bulunmaktadır. Ancak Taşkın (2008) bu görüşe katılmamaktadır.

Her ne kadar uygulama alanının zor olduğu belirtilmiş olsa da uygulamada bilişim sistemleri kullanılarak taşınır malların çalınmasının mümkün olduğu da görülmektedir. Akarslan (2011)'ın aktardığı Sayar (2008) kaynağına göre, bir binanın güvenlik sisteminin bilişim sistemine bağlı olduğu durumlarda, bu bilişim sistemine yetkisiz olarak erişim yapılarak güvenlik sisteminin devre dışı bırakılmasından yararlanarak, binadan taşınır malların çalınması durumunda TCK 142/2-e maddesinin uygulamasının mümkün olacağı belirtilmektedir .

Öğretide yapılan bir diğer tartışmada, mağdurun internet bankacılığı hesabına girilerek failin ya da başka kişilerin hesabına para havale edilmesi durumunda, hesaptaki paranın veri olarak değerlendirilip TCK 244/4. maddesinde düzenlenen "var olan verilerin başka bir yere gönderilmesi yoluyla haksız çıkar sağlama" suçunun oluştuğu görüşüyle çıkmaktadır.

Bu görüşte olan Taşdemir'e göre, hırsızlık suçunun taşınır mal üzerinde işlenmesi nedeniyle, suçun hukuki konusunu taşınabilir malın oluşturduğunu bu nedenle de verinin mal olarak kabul edilmesinin olanaklı olmadığını belirterek, bilişim sisteminin kullanıldığı durumlarda icra hareketinin gerçekleştiği her şeyin veri olması nedeniyle TCK 142/2-e maddesinin değil TCK 244. maddesinin oluşacağını savunmaktadır (Taşdemir 2009).

Taşkın, bu görüşe katılmayarak başkasına ait banka hesabına yetkisiz erişim sağlanarak paraları kendi hesabına aktaran failin aslında mağdurun parasını çaldığını, mal varlığına

zarar verdiğini, somut olarak para ele geçirilmemiş olsa bile başkasına ait malvarlığının elde edildiğini belirtmektedir. Kısaca bankadan para çekip çantasına koyan mağdurun bu parasını çalmakla, kişinin banka hesabına erişim yapılarak paranın başka hesaba aktarılması arasında bir fark olmadığı görüşüyle, bilişim sisteminin hırsızlık suçunda araç olarak kullanılabileceğini savunmaktadır (Taşkın 2008).

Taşkın (2008) ile benzer görüşte olan Dülger (2013) tarihsel ve teknolojik değişimler doğrultusunda, ilk zamanlar da taş üzerine basılı olan paranın zamanla form değiştirerek kağıt ve günümüzde banka hesaplarında veri halinde bulunduğu ve bu veri formundaki para ile borç ödeme, mal alımı gibi işlemler yapılarak Borçlar Hukuku ve Ticaret Hukuku'nda geçerli sayıldığını belirterek veri formundaki bu paranın, para olarak suça konu olacağının ve hesaptaki parayı temsil eden bu verilerin kağıt para gibi kabul edilmesi gerektiğini belirterek bu suçun TCK 142/2-e maddesine giren suçu oluşturduğunu savunmaktadır. Bu yönde ve tartışmalara son veren Yargıtay Ceza Genel Kurulunun 17.11.2009 tarihli E:2009/11-193, K:2009/268 sayılı kararı bulunmaktadır.

2.3.2.2 Bilişim Sistemlerinin, Banka veya Kredi Kurumlarının Araç Olarak Kullanılması Suretiyle Dolandırıcılık (TCK Md. 158/1-f),

"Madde 158(1) Dolandırıcılık suçunun;
f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle," dolandırıcılık suçu düzenlenmiştir.

Bu suç türü ile ilgili detaylı inceleme Dolandırıcılık bölümünde ayrıca yapılacaktır.

2.3.2.3 Haberleşmenin Gizliliğini İhlal (TCK Md. 132)

"Madde 132- (1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.(1)
(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.(1)

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. (Ek cümle: 2/7/2012-6352/79 md.) İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.(1)
(4) (Mülga: 2/7/2012-6352/79 md.).” şeklinde düzenleme yapılmıştır.

Madde gerekçesinde, “Söz konusu suç, belirli kişiler arasındaki haberleşmenin içeriğinin öğrenilmesiyle işlenmektedir. Kişiler arasındaki haberleşmenin ne suretle yapıldığının suçun oluşumu açısından önemi yoktur. Bu haberleşme, örneğin mektupla, telefonla, telgrafla, elektronik posta yoluyla yapılabilir. Bu suç açısından önemli olan, haberleşmenin belirli kişiler arasında yapılmasıdır. Söz konusu suçu, bu haberleşmenin tarafı olmayan kişi işleyebilir.”

Kayda almaktan kasıt kişiler arasındaki haberleşmenin sesli, bunun yanı sıra görüntülü olarak, bu imkânı sağlayan teyp, kamera, dijital kayıt cihazı hatta günümüzde bu özellikleri gösteren cep telefonu ve tabletler ile bir kopyasının elde edilmesidir (Karagülmez 2011).

Eskiden ulaşması günler alan mektup ya da konuşma yapabilmek için sıra beklenen telefon ile yapılan haberleşme, günümüzde teknolojik gelişmeler ile birlikte anlık hale gelmiştir. İnternet alt yapısı kullanılarak e-posta, elektronik sohbet(chat), anlık mesajlaşma(whatsapp, facebook vb.), internet üzerinden telefon görüşmesi ya da tele konferans gibi çeşitli yöntemler ile haberleşme yapılabilmektedir.

Kişiler arasındaki haberleşmenin üçüncü bir kişi tarafından açıklanması eylemi maddenin ikinci fıkrasında, kişinin kendisi ile yapılan haberleşmenin, haberleşmeyi yapan diğer tarafın izni olmaksızın açıklanması yine açıklanan bu verilerin basın ve yayın yoluyla yayımlanması eylemi üçüncü fıkrada suç haline getirilmiştir (Dülger 2013).

2.3.2.4 Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması (TCK Md. 133)

"Madde 133- (1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.(2)
(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.(2)
(3) (Değişik: 2/7/2012-6352/80 md.) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dört bin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur." şeklinde düzenleme yapılmıştır.

Madde gerekçesinde, kişiler arasındaki aleni olmayan konuşmaların dinlenmesi ve kayda alınması suç olarak tanımlanmaktadır. Konuşmaların özel gayret gösterilerek duyulması durumunda aleni olmayan görüşme söz konusu olmaktadır. Konuşmanın aleni olmayan konuşma kabul edilebilmesi için konuşmanın yapıldığı yerin önemi yoktur. Açık bir alan olabileceği gibi kapalı bir ev ortamı da olabilmektedir.

Aleni olmayan konuşmaların dinlenmesi ve kayda alınması eylemi denilince akla ilk olarak ortam dinlemesi gelmektedir. Ortam dinlemesi belli bir ortamdaki konuşmaların dinlenmesi ve hatta kayda alınmasıdır. Bu eylemi gerçekleştirebilmek için spesifik üretilmiş kayıt cihazları kullanılabileceği gibi yaygın olarak kullanılan bilgisayarlar ve cep telefonlarına yüklenen casus programlar vasıtasıyla da ortam dinlemesi yapılabilmektedir (Akarslan 2011).

Konuşma için iki kişi yeterliyken, söyleşiden bahsedebilmek için en az üç kişinin bulunması gerekmektedir. Birinci fıkrada fail konuşmacıların dışında birisiyken, ikinci fıkrada söyleşiye katılanlardan birisidir (Karagülmez 2011).

Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verilerin hukuka aykırı olarak açıklanması yine bu eylemin basın ve yayın yolu ile yapılması maddenin üçüncü fıkrasında suç olarak tanımlanmıştır. TCK 6. maddesinin 1. fıkrasının g bendinde, "Basın ve yayın yolu ile deyiminden; her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim aracıyla yapılan yayınlar," anlaşılacağı belirtilmiştir. Günümüzde en yaygın kullanılan kitle iletişim aracı internettir ve veriler en kısa zamanda çok sayıda kişiye ulaşabilmektedir.

2.3.2.5 Özel Hayatın Gizliliğini İhlal (TCK Md. 134)

"Madde 134- (1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.(1)
(2) (Değişik: 2/7/2012-6352/81 md.) Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur." şeklinde düzenleme yapılmıştır.

Bu düzenleme ile özel hayatın gizliliğinin ihlâli suç olarak tanımlanmıştır. Gerekçede, başkalarına ait yaşam alanına girilerek ya da başka suretle başkaları tarafından görülmesi mümkün olmayan özel bir yaşam olayının saptanması ve kaydedilmesinin cezalandırılacağı belirtilmektedir.

Özel hayat deyimi, "bir kimsenin kamuya mal olmuş hayatının yanında, maddi ve manevi varlığını geliştirebilmesi, kamusal hayatında hedef olarak kabul ettiği noktalara ulaşabilmesi ve kendisi için uygun gördüğü yaşam tarzını sürdürebilmesi için başkalarının denetiminden ve gözetiminde uzak, kendi düşünce ve kanılarıyla süsleyip şekillendirdiği bir yaşam alanıdır (Taşkın 2008)."

Özel hayatın gizliliği Anayasanın 20. maddesiyle teminat altına alınmıştır. Yine Medeni Kanunun 24. maddesinde, Avrupa İnsan Hakları Sözleşmesinin 8. maddesinde ve çeşitli özel kanunlarda özel hayat koruma altına alınmıştır.

Özel hayatın gizliliğinin ihlali eylemi herhangi bir biçimde olabilmektedir. Kişinin evinden, işyerinden; bilgi, belge, resim alma, buralarda veya kamusal alanlarda konuşmalarının dinlemesi şeklinde ihlaller gerçekleştirilebilmektedir (Avşar ve Öngören 2010).

İnternet aracılığıyla özel hayatın gizliliğinin ihlali elektronik posta yolu ile bilgisayar korsanlığı faaliyetleri ile web sitesindeki yayın ile kişisel verilerin toplanması ve rıza dışında kullanımı ile karşımıza çıkmaktadır (Kahraman 2009).

Özel hayata ilişkin ses ve özellikle de görüntülerin internet aracılığıyla ifşa edilmesinde, yaygın olarak sosyal paylaşım platformları kullanılmaktadır. Kitle iletişim aracı olarak çok sayıda insanın bu platformlara dahil olması sebebiyle kısa zamanda yayılım özelliği göstererek büyük mağduriyetler yaşanmasına sebep olmaktadır.

2.3.2.6 Kişisel Verilerin Kaydedilmesi (TCK Md. 135)

"Madde 135- (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.(2)
(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır." şeklinde düzenleme yapılmıştır.

Düzenleme ile kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınması suç olarak tanımlanmıştır. Gerekçede, suçun konusunu kişisel veriler oluşturmaktadır. Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmektedir. Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında herhangi bir ayrım yapılmamıştır.

Günümüzde çoğu kamu ve özel kuruluş kişisel verileri kaydederek işlemekte elde ettiği sonuçlara göre strateji belirlemektedir. Devletler, kişisel verilerin mahremiyetinin

sağlanması adına bu verilerin toplanma şekli ve yapısı ile ilgili kurallar koymuş hem de bu kuralların ihlal edilmesi durumunda uygulanacak cezai yaptırımlar belirlemiştir.

Kişiyle ilgili olan ve o kişiyi diğer kişilerden ayıran ve o kişiyi belirlenebilir kılan her türlü veri kişisel veri kapsamındadır. Kişinin adı-soyadı, özgeçmişi, telefon numarası, parmak izi, iris izi, dna örneği bu verilere örnek olarak verilebilir (Taşkın 2008).

Madde metninde hukuka aykırılık ön şart olarak belirlenmiştir. Mağdurun rızası, kanun gereği ya da suçların önlenmesi adına emniyet ve istihbarat emriyle bu bilgilerin kaydedilmesi durumunda suç oluşmayacaktır (Avşar ve Öngören 2010).

İnternet üzerinde web sayfalarına ya da sosyal paylaşım platformlarına kişinin kendisi ile ilgili bilgileri koyması ve bu bilgilerin başkalarınca kaydedilmesi durumunda öğretide iki farklı görüş bulunmaktadır. Karagülmez (2011)'e göre bu durum suç oluşturmayacaktır. Çünkü kişisel verilerini internet üzerinde paylaşan kişi bu bilgilerin başkaları tarafından kaydedilmesine rıza göstermiş olmaktadır. Dülger (2013)'e göre kişisel verilerin internet ortamında paylaşılmış olması bu verilerin herkes tarafından kullanılabileceği anlamına gelmeyeceği, veriyi yayınlayan kişinin açık rızası olmaksızın verilerin kaydedilmesi durumunda sosyal paylaşım platformu dahi olsa suç oluşacağı belirtilmektedir.

2.3.2.7 Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme (TCK Md. 136)

"Madde 136- (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır." şeklinde düzenleme yapılmıştır.

Madde gerekçesinde, "Bu madde hükmü ile hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır."

Düzenlemede, kişisel verilerin başkasına verilmesi, yayılması veya ele geçirilmesi

olarak üç farklı seçimlik hareket belirlenmiştir. Kişisel verilerin başkasına verilmesi yazılı verilerin elden ya da posta yoluyla veya sanal ortamda bulunan verilerin harici harddisk, flash bellek ya da cd/dvd rom'a kaydedilerek ya da internet üzerinden e-posta yoluyla gönderilmesi şeklinde olabilmektedir. Yayılması, kişisel verilerin mektupla birden çok kişiye gönderilmesi, web sitesi vasıtasıyla herkesin göreceği şekilde erişime açılması, forum odalarında ya da sosyal paylaşım platformlarında yayınlanması bunun yanı sıra toplu olarak e-mail ya da sms gönderme şeklinde gerçekleşebilmektedir. Ele geçirilmesi, kişisel verilerin bulunduğu yerden alınması, verinin kayıtlı bulunduğu bilişim sistemine girilerek verinin başka bir taşınabilir ya da sabit hafıza birimine kaydedilmesi yine sanal ağlar üzerinden kötü niyetli yazılımlar vasıtasıyla kişisel verilerin elde edilmesi mümkün olmaktadır (Dülger 2013).

Alışveriş yaptığımız, ürün ya da hizmet aldığımız firmalar bir şekilde kişisel bilgilerimizi, en çokta isim-soyisim, telefon, e-mail bilgilerimizi istemekte bizde müşteri olarak rızaen vermekteyiz. Ancak kötü niyetli ya da ticari maksatlı olarak kişisel verilerimiz satılmakta veya bir şekilde el değiştirmektedir. Bunun sonucu olarak hiç bağlantımız olmayan firmalardan ilgisiz ürünler için reklam mesajları ya da e-mailleri almaktayız. Hatta bu reklam mesajları/e-mailleri rahatsız edecek seviyeye ulaşabilmektedir. Kişisel verilerimizin güvenli bir şekilde muhafazası adına en kısa zamanda Kişisel Verilerin Korunması ile ilgili yasanın çıkarılması ve ihlaller karşısında caydırıcı cezaların verilesi gerekmektedir.

2.3.2.8 Verileri Yok Etmeme (TCK Md. 138)

"Madde 138- (1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.(4)
(2) (Ek: 21/2/2014-6526/5 md.) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır." şeklinde düzenleme yapılmıştır.

Bu düzenleme ile hukuka uygun olarak kaydedilmiş olan kişisel verilerin, belirlenen

süreler içerisinde yok etmeyen görevliler hakkında cezai yaptırım tanımlanmıştır.

Bu suç tipiyle iki ayrı hukuki değer korunmaktadır. İlki hem kişisel veriler hem de kişisel veriler açısından istenilen güvenlik, ikincisi ise kamu idaresinin güvenilirliği ve işleyişidir (Dülger 2013).

Konumuza bakan yönüyle bilişim yolu ile işlenen suçların tespitinde yer sağlayıcılar ve erişim sağlayıcıların tutmuş olduğu log kayıtları hayati önem taşımaktadır. Hangi kullanıcının, hangi zaman aralığında hangi IP numarası ile işlem gerçekleştirdiği, bu zaman aralığında IP numarasının hangi kullanıcıya tahsis edildiği gibi bilgiler log kayıtlarında yer almaktadır. Bu log kayıtlarının kişisel veri barındırdığı aşikardır. Bu bağlamda log kayıtlarının ne kadar süre saklanacağı 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve yönetmeliğinde log kayıtlarının en az altı ay tutulma zorunluluğu getirilmişken en fazla da iki yıl süre saklanabileceği belirlenmiştir. Yasa gereği sistemde iki yıldan fazla log kaydının bulunmaması, iki yılı aşan kayıtların düzenli olarak imha edilmesi gerekmektedir.

Maddenin ikinci fıkrasında 5271 sayılı Ceza Muhakemesi Kanunu'nda yer alan ve yok edilmesi belli sürelere bağlanan verilerle ile ilgili olarak düzenleme yapıldığı anlaşılmaktadır. Düzenlemeyle, özel hayatla ilgili çok sayıda kişisel veri içeren dinleme ve izleme kayıtları ile ilgili yasada belirtilen imha sürelerinin geçirilmesi durumunda cezanın bir kat artırılacağı hükme bağlanmıştır.

2.3.2.9 Türk Ceza Kanununda Düzenlenen Diğer Bilişim Yoluyla İşlenen Suç Türleri

5237 sayılı Türk Ceza Kanunu'nda yer alan ve yukarıda ele almış olduğumuz suçların yanı sıra Tehdit (Md. 106), Şantaj (Md. 107), Hakaret (Md. 125), Haberleşmenin engellenmesi (Md. 124), Müstehcenlik (Md. 226), Fuhuş (Md. 227) gibi suçların bilişim yoluyla işlenmesi mümkündür. Klasik suç türlerinin işlenişinde bilişimin vasıta olarak

kullanılamayacağı suç türü yok denecek kadar azdır. Madde metninin imkân verdiği ölçüde suçun bilişim yoluyla işlenmesinde olanak bulunmaktadır (Karagülmez 2011).

2.3.3 Özel Kanunlarda Düzenlenen Bilişim Yoluyla İşlenen Suç Türleri

2.3.3.1 Fikir ve Sanat Eserleri Kanununda Düzenlenen Bilişim Yoluyla İşlenen Suçlar

5846 sayılı Fikir ve Sanat Eserleri Kanunda 07.06.1995 tarihinde 4110 sayılı yasa ile yapılan değişiklik neticesinde bilişim sistemlerinin temelini oluşturan bilgisayar programları koruma altına alınmıştır (Taşkın 2008).

Kanunun 71. maddesinde tanımlanan "Manevi, Mali veya Bağlantılı Haklara Tecavüz", 72. maddesinde tanımlanan "Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri" başlıklı suç türleri konumuzla bağlantılı olduğu için başlık olarak değinilmiştir.

2.3.3.2 Elektronik İmza Kanununda Düzenlenen Bilişim Yoluyla İşlenen Suçlar

Elektronik İmza, 5070 sayılı Elektronik İmza Kanunun 3. maddesine göre, "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi" ifade etmektedir. Islak imzayla aynı hukuki geçerliliğe sahiptir.

Elektronik imza, "bir belgeyi imzalama niyetinde olan bir kişi tarafından sahiplenilmiş ya da icra edilmiş bir belgeyle/kayıtla mantıksal bir şekilde ilişkilendirilmiş veya eklenmiş bir süreç, elektronik bir ses veya sembol anlamına gelir (Sevim 2006)."

Kanunun 16. maddesinde tanımlanan "İmza Oluşturma Verilerinin İzinsiz Kullanımı" ve 17. maddesinde tanımlanan "Elektronik Sertifikalarda Sahtekârlık" başlıklı suç türleri konumuzla bağlantılı olduğu için başlık olarak değinilmiştir.

3. DOLANDIRICILIK

3.1 Dolandırıcılık Suçunun Genel Olarak Tarihsel Gelişimi

İlkel ve tarih öncesi toplumlarda malvarlığına karşı suçların dolayısıyla dolandırıcılık suçunun bilinmediği birçok yazar tarafından belirtilmiştir (Acar 2010). Dolandırıcılık suçu eski dönemlerde, inancı kötüye kullanma suçu ile birlikte hırsızlık suçunun bir türü olarak düşünülmüş ve cezalandırılmıştır. İnancı kötüye kullanma ve dolandırıcılık suçunun hırsızlık suçundan ayrılarak bağımsızlık kazanması ve malvarlığına karşı suçlar sistemi içerisinde yer alması için yüzyıllarca beklenmesi gerekmiştir (Selçuk 1982).

Eski toplumların ilk yasalarında, Yunanlılarda, Hititlerde, Sümerlerde, Hint'te, Asurlarda, İran'da, Mısır'da, Oniki Levha Kanunlarında hırsızlık ve mala zarar verme suçları ayrıntı bir şekilde düzenlenerek, çalınan ya da zarar verilen malın değerine göre ya da dinsel niteliği gözetilerek ölüm cezasına kadar varan yaptırımlar öngörülmüşken, bu toplumlarda dolandırıcılık suçlarına rastlanılmamışdır (Selçuk 1982).

Roma Hukuku'nda, bugünkü bilinen dolandırıcılık suçuna karşılık gelen bir suç türüne rastlanılmamaktadır. Ancak Roma Hukuku'nda hırsızlık olarak geçen "furtum" kavramının mülkiyetin gelişimini izleyerek, hırsızlık yanında dolandırıcılık suçunu da kapsadığı ileri sürülmüştür (Yırtımcı 2010).

Üçüncü asır hukukçularından olan Julius Paulus, furtum suçunu; "bir malın veya kullanılmasının veya zilyetliğinin hileli bir şekilde veya kazanç gayesiyle elde edilmesi" şeklinde tanımlamıştır (Bilen 2012). Bu tanıma göre "furtum" suçunun günümüz ceza hukukunda yer alan hırsızlık suçu ile birlikte dolandırıcılık ve güveni kötüye kullanma suçunu kapsadığı anlaşılmaktadır (Rado 1952).

Dolandırıcılık sözcüğü 1694 yılında Fransız diline girmesine rağmen yasal ve bağımsız olarak pozitif hukuka 19-22 Temmuz 1791 yılında çıkarılan yasayla yansımış ve resmileşmiştir. Daha önceki hukukta şu ya da bu şekilde evlere ya da topluma açık yerlere sızarak yapılan hırsızlıklara dolandırıcılık denilmesine karşın, bu yeni kanunla

birlikte cezaların kanuniliği ilkesinin de etkisiyle dolandırıcılık bağımsız bir suç türü olarak düzenlenmiştir (Selçuk 1982).

Dolandırıcılık suçu Türk Hukuku'na 1810 tarihli Fransız ceza yasasının çevirisi olan 1858 tarihli Ceza Kanunnamesinin 8. bölümünde iflas ve dolandırıcılık suçlarının hükme bağlanmasıyla girmiştir. Dolandırıcılık tanımlanırken Fransız yasasından oldukça ayrı ve daha genel bir biçimde tanım yapılmıştır. Bu suçla ilgili çağdaş anlamda bir düzenleme ise ancak 1926 tarihli yasa ile yapılabilmiştir (Selçuk 1982).

3.2 Dolandırıcılık Suçunun Hukuki ve Cezai Boyutu

Dolandırıcılık suçu, 5237 sayılı TCK'nın "Özel Hükümler" başlıklı ikinci kitabının "Kişilere Karşı Suçlar" başlıklı ikinci kısmının "Malvarlığına Karşı Suçlar" başlıklı Onuncu Bölümünde "Dolandırıcılık" başlıklı 157. maddesinde düzenlenmiştir. Maddede, hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişinin dolandırıcılık suçundan cezalandırılacağı hükme bağlanmıştır. Dolandırıcılık suçunun temel şekli 157. maddede düzenlenmiştir. Suçun cezasının artırılmasını gerektiren nitelikli haller 158. maddede ve cezanın azaltılmasını gerektiren hal ise 159. maddede düzenlenmiştir. Diğer yandan, 167. maddede dolandırıcılık suçunda şahsi cezasızlık sebepleri ile cezada indirim yapılmasını gerektiren şahsi sebepler, 168. maddede ise etkin pişmanlık hükümlerine yer verilmiştir.

Madde gerekçesinde, "Dolandırıcılık, hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kişinin kendisine veya başkasına yarar sağlamasıdır. Bu bakımdan dolandırıcılık suçu, kişilerin malvarlığına karşı işlenen bir suçtur. Söz konusu suç tanımı ile kişilerin sahip bulunduğu malvarlığı hakkının korunması amaçlanmıştır. Ayrıca, bu suçun işlenişi sırasında hileli davranışlar ile kişiler aldatılmaktadır. Aldatıcı nitelik taşıyan hareketlerle, kişiler arasındaki ilişkilerde var olması gereken iyi niyet ve güven ihlâl edilmektedir. Bu suretle kişinin irade serbestisi etkilenmekte ve irade özgürlüğü ihlâl edilmektedir."

Dolandırıcılık suçunun oluşabilmesi için birden fazla fiilin gerçekleşmesi gerekmektedir. Birincisi hile, ikincisi ise hilenin etkisi ile hileye maruz kalan kişinin veya bir üçüncü kişinin zararına olarak, fail veya bir başkasının menfaat sağlamasıdır (Karagülmez 2011).

Madde gerekçesinde, "Hile, icraî bir davranışla gerçekleştirilebileceği gibi; karşı tarafın içine düştüğü hatadan, bir konuda yanlış bilgi sahibi olmasından yararlanarak da, yani ihmalî davranışla da, gerçekleştirilebilir. Ancak, bu durumda kişinin, hataya düşen karşı tarafı bilgilendirmek konusunda yükümlülüğünün olması gerekir. Hataya düşen kişi ile hukukî ilişkide bulunulan durumlarda, böyle bir yükümlülük vardır. Ayrıca, muhatabın belli bir hususdaki hatası karşısında kişinin ihmalî davranışının, örneğin susmasının, bir beyan, açıklama değerini taşıması gerekir."

Elde edilen menfaat; para, taşınır ve taşınmaz mal olabileceği gibi hukuksal sonuç doğuran bir belge de olabilmektedir (Eralp 2012).

3.2.1 Dolandırıcılık Suçunun Unsurları

3.2.1.1 Maddi Unsurlar

Fail

Dolandırıcılık suçunun faili herkes olabilir. Fail yönünden bir özellik belirtilmemiştir. Bu suçu işleyen failin kendisine çıkar sağlaması şart değildir. Bu husus madde metninde "kendisine veya başkasına yarar sağlamak" şeklinde belirtilmiştir. Hileli davranışları yapan ile haksız yararı sağlayan farklı kişiler işbirliği içinde bu suçu işlemiş olabilirler. Bu durumda her iki kişi de ortak faildir (Taşdemir 2009).

Dolandırıcılık suçunun tüzel kişiler tarafından işlenmesi mümkün olmamaktadır. Dolandırıcılık suçunun işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında TCK 169. maddesi gereğince, bunlara özgü güvenlik tedbirlerine hükmolunacağı belirtilmektedir (Artuç 2007).

Mağdur

Malvarlığı zarara uğrayan gerçek kişiler dolandırıcılık suçunun mağdurudur. Belirtmekte fayda var ki hileli hareketlerle ancak insan aldatılabileceğinden tüzel kişiler bir suçtan ancak zarar gören konumundadırlar. Suçtan zarar gören ve mağdur kavramları karşılaştırıldığında, suçtan zarar gören kavramının mağdura göre daha geniş bir anlam ifade ettiği görülmektedir (Gökçen ve Balcı 2008).

Şirket ya da kamu kuruluşunda çalışan bir çalışanın işiyle alakalı hileli hareketlerle dolandırılması durumunda, çalışan mağdur konumundayken şirket ya da kamu kurumu malvarlığında azalma olduğundan dolayı suçtan zarar gören konumundadır.

Suçun Konusu

Dolandırıcılık suçunun eylem kısmını hileli davranışlarda bulunulması oluşturmaktadır. Kanun koyucu hileli hareketlerin ne olduğu hususunda bir açıklama yapmamıştır. Bu nedenle dolandırıcılık serbest hareketli bir suç tipidir. Hileli hareketler, icrai olabileceği gibi hataya düşen karşı tarafı bilgilendirmek konusunda yükümlülüğünün bulunması şartıyla, ihmali de olabilmektedir (Gökçen ve Balcı 2008).

İhmali davranışın, karşı tarafın içine düştüğü bir hatadan veya bir konuda yanlış bilgi sahibi olmasından yararlanarak gerçekleştirilebileceği ifade edilebilir. Bu durumda hataya düşen mağduru bilgilendirmek yükümlülüğü altında olanın susması da bazı durumlarda hile olarak sayılabilir. Bu yükümlülük yasadan, sözleşmeden veya güven ilişkisinden kaynaklanabilir (Taşdemir 2009). "Bu durumda, madde gerekçesindeki anlatım göz önüne alındığında; parası olmadığını bilerek taksiye binen kişinin hayatın olağan akışına uygun olarak, kendisinde taksi parasının bulunduğunu farz eden taksicinin bu yanlış kanısını düzeltme yükümlülüğü bulunmaktadır ve dolayısıyla fail bu şekildeki ihmali davranışı ile dolandırıcılık suçunu işlemiş olur (Yırtımcı 2010)."

Acar (2010) hileli davranışların üç şekilde gerçekleşebileceğini belirtmiştir. "-Gerçekte mevcut olmayan bir hususu olmuş, gerçekleşmiş gibi göstermek, - Gerçekleşmiş bir

vakıanın oluşum şekline başka unsurlar ilave etmek, - Gerçekleşmiş bir vakıayı bütün olarak veya belirli unsurları itibarıyla gerçekleşmemiş göstermek. Belirtilen bu hareketlerle kişinin dış dünyadaki gerçeklere ilişkin algısı fail tarafından bozulmakta, gerçekler gizlenmekte, gerçek hakkında yanlış bir tasavvura sahip olması sağlanmaktadır."

Hileli davranışın bilişim sistemlerinin araç olarak kullanılması suretiyle gerçekleştirilmesi mümkün olabilmektedir. Örneğin, failin başkasına ait sosyal paylaşım hesabını ele geçirerek arkadaş listesinde bulunan kişilere kendisini gerçek hesap sahibi gibi tanıtarak ikna etmesi ve mağdurlara verdiği telefon numarasına kontör göndermesini sağlaması halinde hileli davranış, bilişim sistemi aracılığıyla yapılmış olmaktadır (Yırtımcı 2010).

Selçuk (1982)'a göre hile, "Öznel ve nesnel koşulları sömürerek ve iknaya özgü söz ve jestlerle gerçeği peçeleyerek, edilgen öznenin yargılama gücünü etkileyen ve onda yanlış kanı uyandıran diyalektik ve entelektüel bir aldatma hareketidir."

Dönmezer (2004)'e göre hile, "Olaylara ilişkin yalan açıklamaların ve sarfedilen sözlerin doğruluğunu kuvvetlendirecek ve böylece muhatabın inceleme eğilimini etkileyebilecek yoğunluk ve güçte olması ve bu bakımdan gerektiğinde bir takım dış hareketler ekleyerek veya böylece var olan halden ve koşullardan yararlanarak, almayacağı bir kararı bir kimseye verdirtmek suretiyle onu aldatması, bu suretle başkasının zihin, fikir ve eylemlerinde bir hata meydana getirmesidir. Böylece dolandırıcının iradesi fesada uğratılmakta, sakatlanmaktadır."

Maddi olmayan yollarla karşısındakini aldatarak yanılgıya düşüren her türlü (oyun, entrika, dolap vb.) eylem hile olarak tanımlanmıştır. Bu eylemler bir gösteriş biçiminde olabileceği gibi gizli davranışlar olarak da ortaya çıkabilmektedir. Fail gösterişte kendi sahip olmadığı olanak ve sıfatları varmış gibi göstermekte, gizlilikte ise fail kendi durum ve sıfatını saklamaktadır. Hile; kaba, çıplak ve bir çırpıda anlaşılabilecek basitlikte yalanlarla gerçekleştirilemez. Bunun için yalanın belli yoğunluk ve ağırlık

taşıyan nitelikte yalan olması ve bu nitelikli yalan ile mağdurun aldatılması gerekmektedir (Taşdemir 2009).

Bu yönde Yargıtay 11. Ceza Dairesinin 22.04.2004 gün ve 16147/3528 sayılı kararında; "…Hile nitelikli bir yalandır. Yalan belli oranda ağır, yoğun ve ustaca olmalı, sergileniş açısından mağdurun denetleme olanağını ortadan kaldırmalıdır. Desise ise maddi nitelikte fiil ve hareketlerle mağduru hataya düşürmek için kullanılan aldatıcı vasıtalardır. Kullanılan hile ve desiseler ile mağdur yanılgıya düşürülmeli ve bu yanıltma sonucu kandırıcı davranışlarla yalanlara inanan mağdur tarafından sanık veya bir başkasına haksız çıkar sağlanmalıdır (Taşdemir 2009)."

765 sayılı ETCK'da dolandırıcılık fiilinin tanımında yer alan hile ve desise kavramı 5237 sayılı TCK'da yerini suçun maddi unsurunu oluşturan hareket olarak "hileli davranışlar" kavramına bıraktığı görülmektedir.

Ülkemizde öğretide hile ile ilgili olarak görüş birliği bulunduğu söylenemez. Bir görüşe göre; hukuki ve cezai hile arasında mahiyet ve maddiyet ayrımı bulunmamaktadır. Yalan aldatmışsa hiledir. İkinci görüşe göre; soyut yalanın dolandırıcılığı oluşturmayacağı bunun dış olaylarla desteklenmesi ve muhatabın inceleme eğilimini kaldıracak nitelikte bulunması gerektiği belirtilmektedir (Selçuk 1982).

Düzenlemede sadece hileli davranışlarda bulunulması yeterli görülmemiş, bununla birlikte mağdurun aldatılması da şart olarak belirlenmiştir. Aldanma, tamamen zihinsel bir durum olup kişinin normalde düşündüğü ile gerçekte karşılaştığının birbiriyle uyumlu olmamasını ifade etmektedir. Suçun gerçekleşebilmesi için soyut olarak mağduru kandırabilecek nitelikte bulunan hileli hareketlerin onu aldatması da gerekmektedir. Mağdur, failin kullandığı hileli davranışlar neticesinde hataya düşmeli, yani malvarlığı bakımından kendisini zarara sokan tasarrufu iradi ve rızai bir hareketle yapmış olmalıdır (Gökçen ve Balcı 2008).

Madde metninde geçen yarar deyimiyle; para, mal (taşınır, taşınmaz), hukuki sonuç doğuran herhangi bir belge ifade edilmektedir (Eralp 2012). Dolandırıcılık mala karşı

işlenebilen bir suç olduğu için elde edilen yararda malvarlığı ile alakalı olmalıdır. Suçun oluşabilmesi için mağdurun malvarlığında azalma, failin malvarlığında ise artış olmalıdır. Hileli davranışlar neticesinde manevi bir yarar elde edilmişse dolandırıcılık suçu oluşmayacaktır (Taşdemir 2009).

Korunan Hukuki Değer

Anayasamızda ve ülkemizin taraf olduğu uluslararası sözleşmelerde mülkiyet hakkı koruma altına alınmıştır. Bu bağlamda mülkiyet hakkına yönelen her türlü ihlal de Ceza Kanunumuzda suç sayılmıştır. Dolandırıcılık suçu da kişinin sahip olduğu malvarlığı değerleri aleyhine işlenen bir suç türüdür. Çünkü bu suç tipinde failin malvarlığında artma, mağdurun malvarlığında ise azalma meydana gelmektedir. Bu düzenleme ile malvarlığının yanı sıra irade özgürlüğü de koruma altına alınmıştır. Bu yönde Yargıtay CGK'nun 24.12.2002 tarih ve Esas:2002/6-306, Karar:2002/441 sayılı kararında; "...dolandırıcılık suçu, hile ve desiseler yaparak bir kişiyi hataya düşürüp onun veya başkasının zararına, kendisine veya bir başkasına haksız çıkar sağlamaktır. Bu suç iki konulu bir cürüm olup, mal varlığı yanında kişinin irade serbestîsi ve rıza özgürlüğü de korunmaktadır. Çünkü, dolandırıcılık suçunda malın teslimi mağdurun rızası ile gerçekleşmekte, fakat bu teslim hile ve desise kullanılarak sakatlanmış, özgür olmayan bir iradeye dayanmaktadır (Gökçen ve Balcı 2008)."

3.2.1.2 Manevi Unsurlar

Kast ve Taksir

Dolandırıcılık suçundan bahsedebilmek için failin hileli hareketlerde bulunması ve bu şekilde mağduru aldatması yeterli değildir. Failin sorumluluğu açısından haksızlık teşkil eden fiil ile fail arasında nedensellik bağlantısının bulunması gerekmektedir. Bu bağ suçun manevi unsurunu oluşturmaktadır (Bilen 2012).

Suçun manevi unsuru kast ve taksirden oluşmaktadır. TCK 21/1. ve 22/1. maddesi hükümleri gereğince kural olarak kast, istisnai olarak ise taksir manevi unsurun temel iki şeklini oluşturmaktadır. Dolandırıcılık suçunun düzenlendiği TCK 157. maddesinde

dolandırıcılığın taksirle işlenebileceği belirtilmediğinden dolandırıcılık kasten işlenebilen bir suçtur (Acar 2010). "Dolandırıcılık suçunda kastın hileli hareketlerle mağdurun hataya düşürülerek haksız yarar sağlamaya yönelik olması gerekir. Bu nedenle suçun taksirle işlenmesi olanaklı değildir. Failin başlangıçtan beri dış dünyaya yansıyan hareketleri de gözetilerek niyetinin ne olduğu araştırılıp kastı belirlenmelidir. Yargıtay birçok kararında başlangıçta dolandırma kastının (eylem öncesi kast) bulunup bulunmadığını aramıştır (Taşdemir 2009)."

Kast, TCK 21/1. maddeye göre suçun kanuni tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesidir. Taksir ise TCK 22/2. maddeye göre dikkat ve özen yükümlülüğüne aykırılık dolayısıyla bir davranışın suçun kanuni tanımında belirtilen neticesi öngörülmeyerek gerçekleştirilmesidir. Bununla birlikte TCK'da olası kast ve bilinçli taksir şeklinde kusurluluk çeşitleri de tanımlanmıştır. Buna göre olası kast, TCK 21/2. maddeye göre kişinin suçun kanuni tanımındaki unsurların gerçekleşebileceğini öngörmesine rağmen fiili işlemesi halidir. Bilinçli taksir ise TCK 22/3. maddeye göre kişinin öngördüğü neticeyi istememesine karşın, neticenin meydana gelmesidir.

Selçuk (1982)'a göre dolandırıcılık kasten işlenebilen bir suç türüdür ve kast için üç farklı zorunlu öğenin bulunması gerektiğini belirtmiştir. Birincisi, fail başkasını kandırmak ve yanılgıya düşürmek için hileli hareketler yaptığının bilincinde olmalıdır. İkincisi, fail haksız çıkar sağlama bilinç ve iradesinde olmalıdır. Sonuncusu, fail elde edeceği haksız çıkarın başkasının zararı karşılığında sağlandığının bilinç ve iradesinde olmalıdır. Bu üç öğe ile birlikte dolandırıcılık kastı ortaya çıkmaktadır.

Dolandırıcılık suçunun düzenlendiği TCK 157. maddenin gerekçesinde dolandırıcılık suçunun manevi unsuru açık bir şekilde ifade edilmiştir. Gerekçede, "Dolandırıcılık suçu, kasten işlenebilen bir suçtur. Burada söz konusu olan kast, dolandırıcılık suçunun maddî unsurlarının hepsinin fail tarafından bilinmesini ifade etmektedir. Bir başka ifadeyle, fail gerçekleştirdiği davranışların hile teşkil ettiğini, başka birini aldatıcı nitelikte olduğunu bilmelidir. Ayrıca, fail, bu hileli davranışlar sonucunda bunların etkisiyle, hileye maruz kalan kişinin veya başkasının malvarlığında bir eksilme meydana geldiğini, zarar gördüğünü ve buna karşılık, kendisinin veya sair bir kişinin

malvarlığında bir artma meydana geldiğini bilmelidir. Bu itibarla, fail, mağdurun malvarlığındaki eksilmenin, mağdurun gördüğü zararın kendi hileli davranışları sonucunda meydana geldiğini bilmelidir; hile ile zarar arasındaki illiyet bağının varlığının bilincinde olmalıdır. Belirtilen hususlara ilişkin kast, doğrudan kast olabileceği gibi, olası kast da olabilir."

3.2.1.3 Suçun Özel Görünüş Şekilleri

Teşebbüs

765 sayılı ETCK'da yer alan eksik teşebbüs ve tam teşebbüs ayrımı 5237 sayılı TCK'da "suça teşebbüs" başlığıyla tek maddede düzenlenmiştir. Suça teşebbüs TCK 35/1. maddesinde, "Kişi, işlemeyi kastettiği bir suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamaz ise teşebbüsten dolayı sorumlu tutulur." şeklinde tanımlanmıştır.

Dolandırıcılık suçunun hazırlık hareketleri, failin kendisine veya bir başkasına yarar elde etmek için mağdurun aldatılmasına yönelik hileli davranışları gerçekleştirmesiyle başlamaktadır (Selçuk 1982). Dolandırıcılıkta haksız yararın sağlanmasıyla birlikte hareket öğesi ve suç tamamlanmaktadır. Failin çıkar sağladığı ve mağdurun zarar gördüğü an suçun oluştuğu andır. Failin kandıracak nitelikteki hileli davranışlarına karşın buna kanmayan mağdurun bir zararı meydana gelmemiş ise örneğin kandırıldığını anlayıp istenen parayı ya da malı teslim etmemiş veya sonuç dışarıdan gelen başkaca bir engel nedeniyle elde edilememiş ise dolandırıcılığın teşebbüs aşamasında kaldığından hareketle teşebbüs hükümleri uygulanabilecektir (Eralp 2012).

İştirak

Bir kişi tarafından işlenebilecek bir suçun birden fazla kişi tarafından aralarındaki anlaşma ve işbirliği sonucunda işlenmesi suça iştirak olarak nitelendirilmektedir. İştirakle ilgili hükümler TCK'nın 37 ile 41. maddeleri arasında düzenlenmiştir. TCK iştirake ilişkin olarak faillik, azmettirme ve yardım etme olarak üç sorumluluk türü

belirlemiştir. Dolandırıcılık suçu bir kişi tarafından işlenebilecek bir suç türü olmakla beraber, birden fazla kişi tarafından birlikte de işlenebilmektedir. Dolandırıcılığın diğer suçlardan herhangi bir farklılığı bulunmadığından, iştirake ilişkin TCK'nın 37 ile 41. maddeleri arasında yer alan genel hükümlere göre değerlendirilir. Buna göre, fiilin işlenmesi üzerinde kurduğu hâkimiyet ölçü alınarak kişinin fail, azmettiren veya yardım eden olarak sorumluluğu doğacaktır (Bilen 2012).

Birden fazla fail tarafından gerçekleştirilen dolandırıcılık olayında failler arasında iştirak iradesinin de bulunması gerekmektedir. "Dolandırıcılık suçunda iştirak iradesi, hileli davranışların gerçekleştirilmesine katkıda bulunan kişinin bu tür davranışların hileli olduğu ve bunun neticesinde mağdurun aldatılarak zarara neden olunacağı bilinç ve iradesine sahip olmasını gerektirir. Hileli davranışların gerçekleştirilmesine katkıda bulunan kişinin iştirak iradesinin bulunmaması halinde, bu kişi suçun işlenmesinden sorumlu olmaz (Yırtımcı 2010)."

İçtima

Adalet Komisyonu raporunda Ceza Hukukunun temel kurallarından birisi de "Kaç tane fiil varsa o kadar suç, kaç tane suç varsa o kadar ceza vardır" şeklinde ifade edilmiştir. Bu çerçevede kural, cezaların içtimaı yani gerçek içtimadır. Suçların içtimaı ise istisna olarak kabul edilmiştir. Bu istisnalar dışında kalan haller için işlenen her bir suçtan dolayı ayrı ayrı cezaya hükmedilecek ve verilen her bir ceza bağımsızlığını koruyacaktır (Noyan 2007).

TCK'da suçların içtimaı, bileşik suç (Md.42), zincirleme suç (Md.43) ve fikri içtima (Md.44) başlıklarıyla ayrı ayrı düzenlenmiştir. Bu bağlamda dolandırıcılık suçunun bu ayrım gözetilerek ele alınması gerekmektedir.

"Dolandırıcılık suçunun bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı birden fazla işlenmesi durumunda TCK'nın 43/1. maddesi gereğince zincirleme suç hükümleri uygulanacaktır. Tek hareketle birden çok kişinin dolandırılması halinde (yurt dışına işçi olarak götürüleceğinden bahisle gazeteye ilan

verilerek, ilanda belirtilen hesaba para yatırtmak suretiyle kişilerin dolandırılması) ise TCK'nın 43/2. maddesinde düzenlenen aynı neviden fikri içtima söz konusu olacaktır. Ancak, birden fazla mağdura karşı ayrı fiillerle suçun işlenmesi durumunda, mağdur sayısınca suçun oluştuğunun kabulü gerekir (Gökçen ve Balcı 2008)."

TCK'da cezaların içtimaı ile ilgili olarak hüküm konulmamıştır. Bu durum Adalet Komisyonu raporunda hükmolunan birden fazla aynı veya farklı nitelikteki cezanın ne suretle infaz edileceği sorusunun infaz kanununda düzenlenmesi gerektiği düşüncesi olarak ortaya koyulmuştur (Noyan 2007).

"Öte yandan, dolandırıcılık suçunun 5237 sayılı TCK. md. 158/1-f bendinde düzenlenen "bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması" suretiyle işlenmesi halinde tek fiille, hem 158/1-f hükmünün, hem de bilişim alanında suçlar kapsamında yer alan sistemi engelleme, bozma verileri yok etme veya değiştirme yoluyla haksız çıkar sağlama suçu (md. 244/4) ile sahte veya üzerinde sahtecilik yapılan banka veya kredi kartını kullanarak yarar sağlama suçu (md. 245/3) söz konusu olabilecektir. md. 244/4 hükmünde "suçun başka bir suç oluşturmaması", md. 245/3 hükmünde ise "fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde" ifadelerine yer verilmiş olduğundan içtimaya ilişkin belirleme yapıldığı söylenebilir (Acar 2010)."

3.2.2 Suçun Nitelikli Halleri

Kanun koyucu bir suçun temel şekline bazı haller ilave ederek, bu suçla benzer nitelikte başka suç tipleri türetilebilmektedir. Düzenlenen suç tipinin temel şekline ilave olarak aranan ve suça daha ağır veya daha hafif nitelik katan böylelikle failin daha çok ya da daha az ceza almasına neden olan hallere, suçun nitelikli halleri denmektedir (Bilen 2012).

Dolandırıcılık suçunun cezasının ağırlaştırılmasını gerektiren nitelikli haller TCK 158. maddesinde, daha az cezayı gerektiren nitelikli hal ise TCK 159. maddesinde düzenlenmiştir.

3.2.2.1 Cezanın Artırılmasını Gerektiren Nitelikli Haller (TCK md.158)

"Madde 158- (1) Dolandırıcılık suçunun;
a) Dinî inanç ve duyguların istismar edilmesi suretiyle,
b) Kişinin içinde bulunduğu tehlikeli durum veya zor şartlardan yararlanmak suretiyle,
c) Kişinin algılama yeteneğinin zayıflığından yararlanmak suretiyle,
d) Kamu kurum ve kuruluşlarının, kamu meslek kuruluşlarının, siyasi parti, vakıf veya dernek tüzel kişiliklerinin araç olarak kullanılması suretiyle,
e) Kamu kurum ve kuruluşlarının zararına olarak,
f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle,
g) Basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle,
h) Tacir veya şirket yöneticisi olan ya da şirket adına hareket eden kişilerin ticari faaliyetleri sırasında; kooperatif yöneticilerinin kooperatifin faaliyeti kapsamında,
i) Serbest meslek sahibi kişiler tarafından, mesleklerinden dolayı kendilerine duyulan güvenin kötüye kullanılması suretiyle,
j) Banka veya diğer kredi kurumlarınca tahsis edilmemesi gereken bir kredinin açılmasını sağlamak maksadıyla,
k) Sigorta bedelini almak maksadıyla,
İşlenmesi halinde, iki yıldan yedi yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur. (Ek cümle: 29/6/2005 – 5377/19 md.; Değişik: 3/4/2013-6456/40 md.) Ancak, (e), (f), (j) ve (k) bentlerinde sayılan hâllerde hapis cezasının alt sınırı üç yıldan, adli para cezasının miktarı suçtan elde edilen menfaatin iki katından az olamaz.
(2) Kamu görevlileriyle ilişkisinin olduğundan, onlar nezdinde hatırı sayıldığından bahisle ve belli bir işin gördürüleceği vaadiyle aldatarak, başkasından menfaat temin eden kişi, yukarıdaki fıkra hükmüne göre cezalandırılır." hükümleri ile nitelikli haller düzenlenmiştir.

Tezimizin konusu itibarıyla sadece f bendinde düzenlenen "Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle" nitelikli hali incelenecektir.

Dolandırıcılık Suçunun Bilişim Sistemlerinin, Banka veya Kredi Kurumlarının Araç Olarak Kullanılması Suretiyle İşlenmesi (TCK Md. 158/1-f)

Suçun Bilişim Sistemlerinin, Banka veya Kredi Kurumlarının Araç Olarak Kullanılması Suretiyle İşlenmesi, suçun basit halinin düzenlendiği TCK 157. maddeye göre daha ağır cezayı ön görmektedir. Bu maddede iki ayrı nitelikli hal düzenlenmiştir. Bunlardan birincisi dolandırıcılık suçunun bilişim sistemleri aracılığıyla işlenmesi, ikincisi ise suçun banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesidir.

Madde gerekçesinde, "Bilişim sistemlerinin ya da birer güven kurumu olan banka veya kredi kurumlarının araç olarak kullanılması, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağlamaktadır. Banka ve kredi kurumları açısından dikkat edilmesi gereken husus, bu kurumları temsilen, bu kurumlar adına hareket eden kişilerin başkalarını kolaylıkla aldatabilmeleridir."

Yukarıda ayrıntılı olarak bahsettiğimiz gibi dolandırıcılıktan söz edilebilmesi için failin hileli hareketlerle mağduru aldatması gerekmektedir. Bu suçun nitelikli halinin oluşabilmesi için hileli hareketin bilişim sistemleri aracılığıyla gerçekleştirilmesi yani fail tarafından bilişim sistemi üzerinden hileli bir işlemin gerçekleştirilmesi gerekmektedir. Örneğin internet üzerinden aldatıcı reklamlar yapılarak veya mağdura gönderilen e-mail ile sonradan bir takım avantajlar sağlanacağına yönelik vaatlerde bulunularak hileli davranışlar gerçekleştirilip, mağdur sözleşme yapılmasına ikna edilerek haksız bir yarar sağlanması halinde eylem bilişim sistemi kullanılarak dolandırıcılık suçunu oluşturacaktır (Bilen 2012). Yine internet üzerinden gerçekleştirilen alışveriş işlemlerinde mağdurun hileli hareketlerle aldatılarak menfaat elde edilmesi halinde dolandırıcılık suçunun nitelikli hali oluşacaktır (Gökçen ve Balcı 2008).

Uygulamada en çok karşılaşılan bilişim sistemleri aracılığıyla dolandırıcılık eylemi, failin sıradan bir kişinin sosyal paylaşım ya da anlık yazışma program şifresini ele geçirerek, kendisini profil sahibi gibi tanıtmak suretiyle zorda olduğunu belirtip para ya da kontör istemesi ya da bir yardım kuruluşuna bağış yapması için ikna etmesi şeklinde

gerçekleşmektedir. Burada hile ile aldanan mağdurlar faile doğrudan para ya da kontör gönderimi yapabilecekleri gibi mağdurun cep telefonu numarasının elde edilmesi ile telefonuna gönderilen sözde yardım kampanyasının mesajı olduğu söylenen ancak gerçekte mobil ödeme yöntemiyle oyun kredisi alma onay mesajı olan gönderinin onaylanması durumunda fail oyun kredisi alarak haksız menfaat temin edecektir. Burada fail, gerçek profil sahibinin arkadaşları ya da yakınları olan mağdurların iyi niyetinden, güveninden ya da saflığından faydalanarak haksız menfaat elde etmektedir (Dülger 2013).

Dolandırıcılık suçunda bilişim sisteminin araç olarak kullanılması, TCK 243. maddede düzenlenen hukuka aykırı olarak bilişim sistemine girme ya da TCK 244. maddede düzenlenen sisteme veya veriye müdahale etmek suretiyle de gerçekleşebilmektedir. "Dolandırıcılık suçunun bilişim sistemine girme suçu ile birlikte işlenmesi halinde gerçek içtima kurallarının uygulanması gerekir. Bu durumda birbirinden bağımsız iki ayrı suç vardır. Dolandırıcılık suçunun sisteme veya verilere müdahale etmek suretiyle işlenmesi halinde ise; yardımcı normun sonralığı ilkesinin gereği olarak fail sadece dolandırıcılık suçundan cezalandırılır (Yırtımcı 2010)."

5411 Sayılı Bankacılık Kanunu'nun tanımlar ve kısaltmalar başlıklı 3. maddesine göre, "Banka, mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını", "Mevduat bankası: Bu Kanuna göre kendi nam ve hesabına mevduat kabul etmek ve kredi kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini", "Katılım bankası: Bu Kanuna göre özel cari ve katılma hesapları yoluyla fon toplamak ve kredi kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini", "Kalkınma ve yatırım bankası: Bu Kanuna göre mevduat veya katılım fonu kabul etme dışında; kredi kullandırmak esas olmak üzere faaliyet gösteren ve/veya özel kanunlarla kendilerine verilen görevleri yerine getiren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini" ifade etmektedir.

5411 Sayılı Bankacılık Kanunu'nun 48. maddesinin gerekçesinde, kredi kurumları; banka olmamasına rağmen kanunen borç para vermeye yetkili kılınan kurumlar olarak

açıklanmıştır. Kredi kurumu, mevduat kabul edip borç veren kuruluş anlamına da gelmektedir (Karagülmez 2011).

5411 Sayılı Bankacılık Kanunu'nun Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme başlıklı 157. maddesinde bu kanuna tâbi kuruluşların, Türk Ceza Kanunu'nun 244. maddesinde tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu açısından banka veya kredi kurumu olarak kabul edileceği açıkça belirtilmiştir.

Bankaların veya kredi kurumlarının sağlamış olduğu olağan faaliyetlerden hileli araçlar kullanılarak yararlanılması ve üçüncü kişilerin zararına haksız bir çıkar elde edilmesi durumunda veya banka ve kredi kurumlarının yine olağan faaliyetleri kapsamında üretmiş oldukları maddi varlıkların (çek, hesap cüzdanı, dekont vb.) suçta araç olarak kullanılması neticesinde haksız çıkar elde edilmesi durumunda bu bent kapsamındaki suç oluşacaktır. "Örneğin sahte kimlik bilgileri ile banka görevlisini hesap sahibi olduğu konusunda aldatarak, banka görevlisinin hesaptan ödeme yapmasını sağlayan failin eylemi bu bent kapsamındaki suçu oluşturur. Buna karşılık sırf suça konu paranın banka aracılığıyla faile gönderilmiş olması yani bankanın sırf ödeme aracı olarak kullanılmış olması eylemin bu bent kapsamında değerlendirilmesi açısından yeterli olmayacaktır (Bilen 2012)."

3.2.2.2 Cezanın Azaltılmasını Gerektiren Nitelikli Hal (TCK Md. 159)

"Madde 159- (1) Dolandırıcılığın, bir hukuki ilişkiye dayanan alacağı tahsil amacıyla işlenmesi halinde, şikayet üzerine, altı aydan bir yıla kadar hapis veya adlî para cezasına hükmolunur." şeklinde düzenleme yapılmıştır.

Daha az cezayı gerektiren bu nitelikli halin söz konusu olabilmesi için failin mağdurdan bir alacağının bulunması, bu alacağın hukuki ilişkiye dayanması ve alacağın tahsili amacıyla mağdurun hileli davranışlarla aldatılması gerekmektedir.

5237 sayılı TCK'da dolandırıcılık suçu ile ilgili daha az ceza gerektiren tek hal bu maddede düzenlenmiştir. Bu hüküm, 765 sayılı ETCK'nın 308. maddesinde yer alan

“ihkak-ı hak” (kendiliğinden hak alma) suçunun özel şekli olarak düzenlenmiştir. TCK’da kendiliğinden hak alma şeklinde bağımsız bir suça yer verilmemiştir. Bunun yerine, TCK’nın Malvarlığına Karşı Suçlar bölümünde yer alan hırsızlık, yağma, dolandırıcılık suçları ve Kamu Güvenine Karşı Suçlar bölümünde yer alan sahtecilik suçları bakımından “bir hukuki ilişkiye dayanan alacağın tahsili amacı”, cezanın azaltılmasını gerektiren nitelikli hal olarak düzenlenmiştir (Acar 2010).

TCK’nın 159. maddesinin gerekçesinde de belirtildiği üzere, kişinin hukuki bir ilişkiye dayanan alacağının tahsili amacıyla hileli davranışlarda bulunması durumunda eylem dolandırıcılık vasfını muhafaza edecek ancak faile daha az ceza verilecektir. Soruşturma ve kovuşturmanın yapılabilmesi için mağdurun şikâyette bulunması gerekmektedir.

Taşdemir (2009)’e göre, bu özel durumun uygulanabilmesi için faille mağdur arasında; Birincisi, hukuken geçerli bir sözleşme bulunmalı, bu sözleşme yazılı veya sözlü olarak yapılabilmektedir. İkincisi, alacak bu sözleşmeye dayalı olmalı, bu alacak ile hileli hareketler sonucu tahsil edilen miktarın orantılı olması gerekmektedir. Sonuncusu, failin de bu hakkını alabilmek için ortaya koyduğu hileli bir davranışının olması gerekmektedir. Satılan otomobilin parasının ödenmediği durumda, fail hileli hareketlerle alacağını tahsil etmişse bu madde uygulanacaktır. Taraflar arasında hukuken bir sözleşme olmayıp, fail haksız bir fiil nedeniyle örneğin failin, trafik kazası sonucu zararını tahsil etmek için hileli hareketlere başvurması durumunda bu madde uygulanmayacaktır.

4. ÜLKEMİZDE KULLANILAN ÖDEME SİSTEMLERİ

Teknolojik gelişmeler doğrultusunda bankaların ürün ve hizmet çeşitliliği de gelişme göstererek artmıştır. Bu gelişmeler neticesinde alışverişlerde klasik olarak kullanılan nakit para yerini nakit olmayan ödeme sistemlerine bırakmıştır. Bankalar ve çeşitli özel sektör kuruluşları öncülüğünde müşteriler elektronik ödeme sistemleri ile tanışmış ve sektörel gelişmelerle elektronik ödeme sistemlerinin farklı türleri ortaya çıkmıştır.

6493 sayılı Ödeme Ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri Ve Elektronik Para Kuruluşları Hakkında Kanunu'nun tanımlar başlıklı 3. maddesinin v fıkrasında, "Ödeme sistemi: Üç veya daha fazla katılımcı arasındaki transfer emirlerinden kaynaklanan fon aktarımlarının gerçekleştirilmesini sağlamak amacıyla yapılan takas ve mutabakat işlemleri için gerekli altyapıyı sunan ve ortak kuralları olan yapıyı" ifade etmektedir.

Diğer bir tanıma göre ödeme sistemi, "ekonomik birimler arasında mal ve hizmetlerin değişimini kolaylaştıran araçları, yasal düzenleme ve standartları, kurumsal ve örgütsel çatıyı, işletim süreçlerini ve haberleşme ağını kapsamaktadır (Merkez Bankası 2014)."

Ödeme sisteminin anlaşılabilmesi için öncelikle takas ve mutabakat işlemlerinin anlaşılabilmesi gerekmektedir. "Takas, sisteme gönderilen transfer emirlerinin aktarımı, bu emirlerin karşılıklı olarak iletilmesine aracılık edilmesi, bazı sistemlerde mutabakat öncesi provizyon alınması ve sisteme giren ödeme emirlerinin netleştirilmesini ifade etmektedir. Mutabakat, iki ya da daha fazla taraf arasındaki fon ya da menkul kıymet aktarımından kaynaklanan yükümlülüklerin yerine getirilmesidir (Merkez Bankası 2014)."

4.1 Kartlı Ödeme Sistemleri

4.1.1 Kredi Kartları

Ülkemizde kullanılan ödeme araçları nakit ve nakit-dışı olmak üzere ikiye ayrılmaktadır. Gelişen teknoloji ile dünya genelinde alternatif ödeme araçlarına

yönelim her ne kadar fazla olsa da, nakit para kullanımı halen yaygın olarak kullanılan bir araç olma özelliğini sürdürmektedir. Ülkemizde nakit dışı ödeme araçları içerisinde en yaygın kullanılan ödeme aracı ödeme kartlarıdır. Ödeme kartları, banka kartları ve kredi kartlarından oluşmaktadır. Ödeme kartları arasında en yaygın olarak kullanılanı ise kredi kartlarıdır (Merkez Bankası 2014).

Kartlı ödeme fikri ilk olarak 1887 yılında Edward Bellamy'ın "Looking Backward or Life in The Year 2000" adlı bilim kurgu romanında, 2000'li yıllarda yapılacak alışverişlerde ödemelerin karttan koparılan parçalarla yapılabileceği ve bu ödemelerin kart bitene kadar sürebileceği fikriyle ortaya atılmıştır. Dünyada bilinen ilk kredi kartı uygulaması kredi kartlarının ana yurdu olan Amerika'da başlamıştır. 1894 yılında Hotel Credit Letter Company tarafından turizm sektörüyle sınırlı, seçkin iş adamları için sadece belirli otellerde geçerli olan dünyanın ilk ödeme kartı kullanıma sunulmuştur (Kaya 2009).

Bazı yazarlara göre gerçek manada ilk kredi kartı Western Union tarafından 1914 yılında seçkin müşterilerin kullanımı için hizmete sunulan kredi kartıdır. Kullanım alanı ve bölgesel sınırlaması olmayan ilk kredi kartı 1950 yılında Frank Mc Namara tarafından geliştirilen Diners Clup kartıdır. Bu kart 1977 yılından itibaren geliştirilerek dünyaya yayılmıştır. İlk uluslararası niteliğe sahip kredi kartı ise 1958 yılında Amexco tarafından çıkarılan American Express kredi kartıdır (Eralp 2012).

Uluslararası gelişmelere paralel olarak ülkemiz ilk kredi kartı uygulaması ile 1968 yılında önce Diners Club, hemen sonrasında American Express kartları ile tanışarak kartlı ödeme sistemlerini kullanmaya başlamıştır (İnt. Kyn. 8).

Diners Club kartları, Koç grubuna bağlı Servis Turistlik A.Ş.'nin Diners Club'dan yurt içi kart çıkarma izni alarak çıkarmış olduğu kredi kartları ile başlamış, Türk Express Havacılık ve Turizm Limited şirketinin American Express kredi kartlarını piyasaya sürmesi ile 1975 yılına kadar devam etmiştir (Eralp 2012).

1975 yılından sonra İnterbank grubuna bağlı Eurocard, Mastercard ve Access kredi kartları piyasaya girmiştir. Bu kredi kartlarının temsilciliği daha sonra Pamukbank ve Genel Sigortanın önemli oranda hissedarı oldukları Anadolu Kredi Kartları Turizm A.Ş.'ye devredilmiştir. 1980 yılı itibarıyla piyasada kredi kartlarının görmüş olduğu ilgi ve sağladığı döviz girdisi nedeniyle, diğer bankalar da kredi kartı uygulamasına geçmişlerdir. Bu dönemde, Gold ve Classic gibi farklı kart tipleri piyasada kullanıma sunulmuştur (Kaya 2009).

"Türkiye'de ilk kredi kartı 1968'lerde piyasaya sürülmüş olmasına rağmen, o dönemlerde yaşanan yüksek enflasyon, yüksek faizler ve sık yaşanan krizler nedeniyle kullanımı sınırlı kalmıştır. 1990'ların sonlarında kullanımı artmaya başlayan kredi kartlarının, o döneme kadar yavaş bir büyüme seyri göstermesinde, bankaların aracılık fonksiyonlarını yerine getirmek yerine devleti finanse eden kurumlar olarak çalışmaları etkili olmuştur. Türkiye kredi kartı piyasası 1990'lı yılların sonlarına doğru hızlı bir büyüme sürecine girmiş, bu büyüme 2002-2007 yılları arasında ivme kazanmıştır. 2002-2007 döneminde %137 büyüyen kredi kartı sayısı bu dönemde yaklaşık 3 kat artış göstererek 2007 sonunda 37.3 milyona ulaşmıştır. 2008-2012 döneminde ise büyüme daha yavaş seyretmiş, buna rağmen kredi kartı sayısı 2012 sonu itibarıyla 54.3 milyona ulaşmıştır (Özkan 2014)."

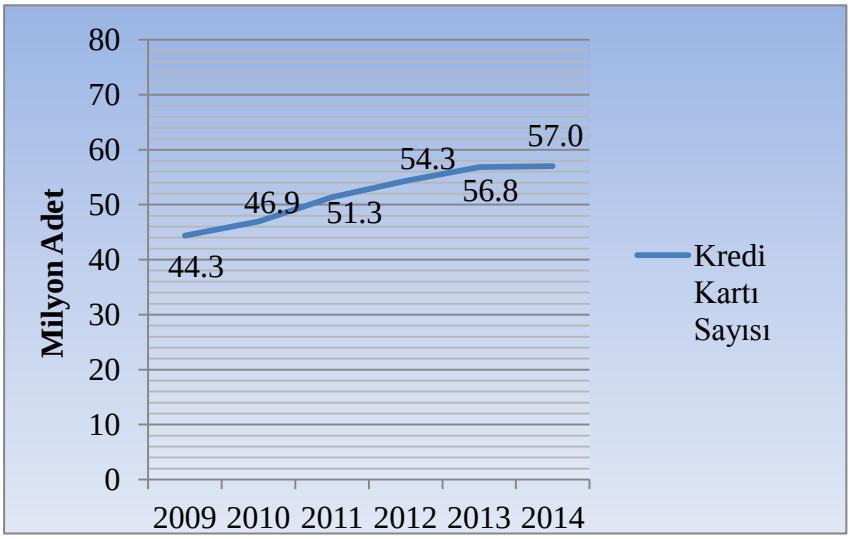
5464 sayılı Banka Kartları Ve Kredi Kartları Kanunu'nun tanımlar başlıklı 3. maddesinin e fıkrasında, "Kredi kartı: Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fizikî varlığı bulunmayan kart numarası" olarak tanımlanmıştır.

Başka bir tanıma göre kredi kartı, "Kart sahibine belirli iş yerlerinden nakit ödemeksizin mal ve hizmet satınalma ve banka şubeleri ile otomatik para çekme cihazlarından kredi çekme imkânı veren ödeme ve kredi aracıdır (Yılmaz 2000)."

Kredi ya da banka kartının ön yüzünde kart hamilinin adı, soyadı, kartın son kullanma tarihi ve 16 haneli kart numarası ve logo (Uluslararası kart çıkarmaya yetkili kuruluş olan Visa, Master, Diner, American Express vb. logosu) yer almaktadır. Kredi

kartlarındaki on altı haneli kart numarasının; ilk dört rakamı bankayı tanımlayıcı, 5. rakamı kredi kartının türünü (Gold, Klasik, Premium vb.) 6. rakamı ise ortaklık kartı (Co Branded Card, Affinty Card vb.) olup olmadığına ilişkindir. Kredi kartlarındaki bu ilk 6 rakam BIN (Bank Identification Number/Banka Kimlik Numarası) kodunu oluşturmaktadır. Daha sonraki on rakam ise müşteri hesap numarasına ilişkin olup, bu on rakamın sonuncusu kontrol rakamıdır (Kaya 2009).

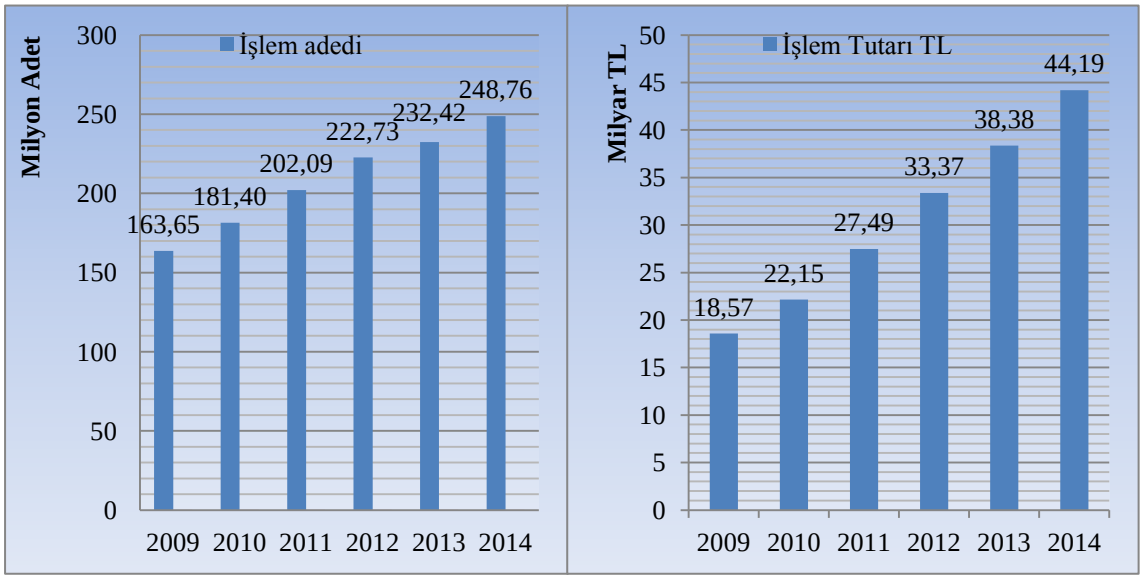
Şekil 4.1'de gösterilen Bankalararası Kart Merkezinin yayınlamış olduğu dönemsel bilgiler doğrultusunda, ülkemizde 2009 yıl sonu itibarıyla 44,3 milyon olan kredi kartı sayısının 2014 yılı sonunda 57,0 milyona ulaştığı görülmektedir. 2009-2013 döneminde düzenli bir büyüme kaydeden kredi kartı sayısı, 2014 yılı içerisinde artışını durdurmuştur (İnt. Kyn. 9).



Şekil 4.1 2009-2014 yılları arasında kredi kartı sayısının gelişimi

Şekil 4.2'de gösterilen Bankalararası Kart Merkezinin yayınlamış olduğu dönemsel bilgiler doğrultusunda, ülkemizde kredi kartları ile yapılan alışveriş ve nakit çekim işlem adedi 2009 yılında 163,65 milyon adet iken bu rakam 2014 yılı sonu itibarıyla 248,76 milyonu bulmuştur. Yine kredi kartları ile 2009 yılında alışveriş ve nakit çekim olarak 18,57 milyar TL'lik işlem yapılmış iken bu rakam 2014 yılı sonu itibarıyla 44,19 milyar TL'ye ulaşmıştır (İnt. Kyn. 9). Kredi kartı ile gerçekleştirilen işlemlerin ve

ödenen tutarlarının yıllara göre düzenli bir artış sergilediğinden hareketle, ödeme araçları arasında kredi kartının halen liderliğini sürdürdüğü görülmektedir.



Şekil 4.2 2009-2014 yılları arasında kredi kartları ile yapılan alışveriş ve nakit çekme işlem adet ve tutarlarının gelişimi

Bulunduğumuz dönemde artık kartlarla yapılan ödemelerde kartın POS cihazına herhangi bir teması olmaksızın da ödeme işlemi gerçekleştirilebilmektedir. Temassız ödeme araçları, ülkemizde ödeme sistemleri alanında kullanılmaya başlanılan en yeni yöntemlerden birisidir. Bu yöntem kredi kartı, banka kartı veya diğer ödeme kartlarının üye iş yerlerinde kullanılan POS cihazlarına herhangi bir şekilde temas etmeden kullanılması yöntemidir. Bu yöntem ülkemizde kartlı ödeme sistemleri alanında öncü birkaç banka tarafından müşterilerinin hizmetine sunulmaya başlamıştır. Bu hizmet kapsamında gerekli altyapıya sahip iş yerlerinde kredi kartını POS cihazına okutmadan, sadece temassız kredi kartının takılı olduğu cep telefonu, saat veya anahtarlık gibi bir aracı ilgili cihaza 3-4 cm. yanaştırarak ödeme işlemi gerçekleştirilmektedir (Karpuz 2012).

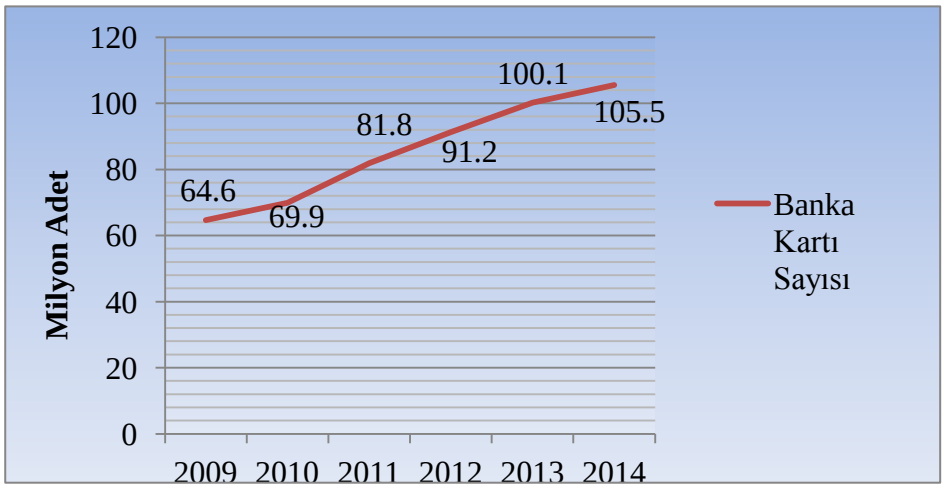
4.1.2 Banka Kartları

5464 sayılı Banka Kartları Ve Kredi Kartları Kanununun tanımlar başlıklı 3.maddesinin d fıkrasında, "Banka kartı: Mevduat hesabı veya özel carî hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan kart" olarak tanımlanmıştır.

“Banka kartları, ait olduğu bankanın kartlı sistemi içerisinde hamiline mevduat hesabı ile bağlantılı olarak doğrudan ya da elektronik veya benzeri işlem cihazları aracılığı ile hesabın kullanımını ve diğer bankacılık hizmetlerini sağlayan, mülkiyeti kendilerine ait olmak üzere bankalarca çıkarılan plastik kartlardır. Banka kartlarının kullanım amacı öncelikle hesap sahibinin şube dışında günün 24 saati ATM (Otomatik Ödeme Makineleri) cihazları ile hesabına ulaşarak tasarruf yapma olanağı sağlamaktadır. Bu kartların başlıca işlevi hesap sahiplerine şubelerinden verilen güvenlik şifreleri ile hesaplarından para çekmeyi kolaylaştırmasıdır. Hesap sahibi bu şifre ile ATM cihazı tarafından teşhis edilir. Banka tarafından verilen bu şifre, şubede yapılan işlemler yerine geçer. Banka kartları aracılığıyla yapılan para çekme işlemleri on-line biçiminde yapıldığı için şifre girildiği anda hesaptaki son durumun görülmesi mümkündür. Aynı şekilde para çekilmesi durumunda bu işlem anında hesaba yansır (İnt. Kyn. 10).”

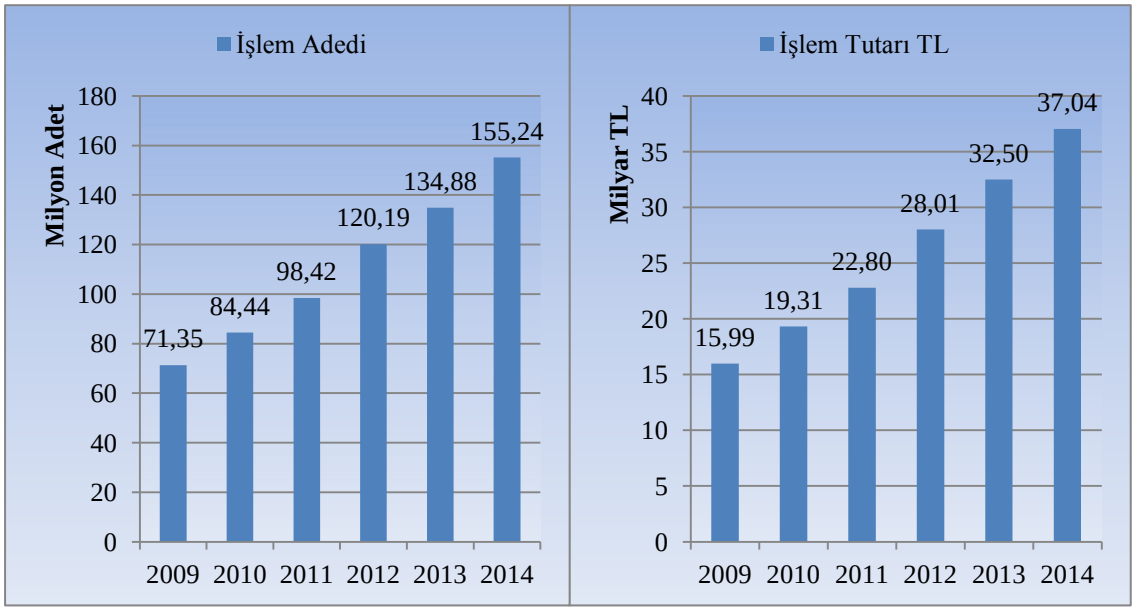
Banka kartı, kart kullanıcısının bankadaki hesabına ulaşmasını sağlayarak bankacılık işlemleri yapmasına, mal ve hizmet alımında kullanmasına, nakit çekmesine imkân tanıyan bir üründür. Uluslararası kart kuruluşlarının logoları bulunan banka kartları ile dünyanın her yerinde mal ve hizmet alımı, aynı logoları taşıyan ATM’ler den nakit çekimi yapılabilir (Türkiye Bankalar Birliği 2008).

Şekil 4.3’de gösterilen Bankalararası Kart Merkezinin yayınlamış olduğu dönemsel bilgiler doğrultusunda, ülkemizde 2009 yıl sonu itibarıyla 64,6 milyon olan banka kartı sayısının 2014 yılı sonunda 105,5 milyona ulaştığı görülmektedir (İnt. Kyn. 9).



Şekil 4.3 2009-2014 yılları arasında banka kartı sayısının gelişimi

Şekil 4.4'de gösterilen Bankalararası Kart Merkezinin yayınlamış olduğu dönemsel bilgiler doğrultusunda, ülkemizde banka kartları ile yapılan alışveriş ve nakit çekim işlem adedi 2009 yılında 71,35 milyon adet iken bu rakam 2014 yılı sonu itibarıyla 155,24 milyona ulaşmıştır. Yine banka kartları ile 2009 yılında alışveriş ve nakit çekim olarak 15,99 milyar TL'lik işlem yapılmış iken bu rakam 2014 yılı sonu itibarıyla 37,04 milyar TL'ye ulaşmıştır (İnt. Kyn. 9).



Şekil 4.4 2009-2014 yılları arasında banka kartları ile yapılan alışveriş ve nakit çekme işlem adet ve tutarlarının gelişimi

Banka kartı ile kredi kartını birbirinden ayıran en belirgin özellik ödeme aracı olarak kullanıldığı zaman kullanıcının ödeme işlemine ilişkin fon aktarımının gerçekleşme zamanıdır. Kredi kartı ile yapılan ödemelerde ödeme işlemini, müşteri adına banka yapmakta ve kart son ödeme tarihine kadar kart kullanıcısından kartı çıkaran kuruluşa herhangi bir fon transferi gerçekleşmemektedir. Banka kartında ise kart kullanıldığı anda fon karşı hesaba eş zamanlı olarak aktarılmaktadır (Karpuz 2012).

Debit kart olarak da adlandırılan banka kartları ile ilk zamanlar ATM'ler üzerinden para çekilip hesaba ilişkin işlemler yapılabilmekte iken günümüzde banka kartları ile hesapta para bulunmak kaydıyla internet üzerinden alışveriş yapılabilmekte, puan kazanılıp harcanabilmektedir. Teknolojik gelişmelerle birlikte bankalar müşterilerine sunmuş

oldukları banka kartlarına birçok özellik katarak işlevselliğini artırmışlardır. Hatta Finans Bank dünyanın ilk taksit yapan banka kartını müşterilerine duyurmuştur.

4.1.3 Ön Ödemeli Kartlar

Bankalarca veya kart çıkarmaya yetkili kuruluşlarca, herhangi bir hesaba bağlı olmaksızın çıkarılan ve önceden karta yüklenen tutar kadar harcama yapmaya imkân veren kartlardır. Kredi kartlarında olduğu gibi bir kredi limiti bulunmaz. Kartın içerisine yüklenen tutar kadar harcama yapılabilir. Anlaşmalı banka ve kuruluşlardan ön ödemeli kartlara para yükleme işlemi yapılabilmektedir.

Ön ödemeli kartlar, tıpkı bir banka kartı veya kredi kartı gibi ödeme kartıdır. Kartın üzerinde kart numarası, son kullanma tarihi ve güvenlik numarası bulunur. Genel olarak banka kartı ve kredi kartı kabul eden tüm işyerlerinde bu kartlar kullanılabilir. Birçok banka ön ödemeli kartla ilgili farklı ürün alternatifleri sunmaktadır. Bunlardan bazıları, genel kullanım kartları, hediye kartları, ön ödemeli sanal kartlar ve harçlık kartları olarak adlandırılmaktadır. Seçilen kart türüne göre ön ödemeli kartlar, kullan-at ve kullan-doldur olarak iki tipte bulunmaktadır.
Kullan-at: Hediye kartları bu kategoridedir. Karta aktarılmış olan para bittiğinde kartın kullanımı da sona ermektedir.
Kullan - doldur: Bu kartlar kontörlü cep telefonları gibi işler. Karta aktarılmış olan para azaldığında veya bittiğinde tekrar para yükleyerek kart kullanılabilmektedir (İnt. Kyn.11).

Ön ödemeli kartlar temelde ödeme işlemi gerçekleştirilebilmek için tasarlanmıştır. Ancak sektörel rekabet neticesinde ödeme sistemlerinde de yenilikler ortaya çıkmıştır. Bunlarda birisi de PayPal'ın TEB, Master Card ve İninal işbirliğiyle geliştirdiği ön ödemeli PayPal nakit kartıdır. Bu kart ile aynı zamanda tüketicinin karta yüklediği parayı ATM'den geri çekme imkânı da sunularak ön ödemeli karta piyasada olmayan farklı bir özellik getirilmiştir (İnt. Kyn. 12).

4.2 Dijital Cüzdanlar

Eskiden sadece nakit para ile yapılabilen alışveriş günümüzde evrimleşerek, kartlı alışveriş, tele alışveriş, on-line alışveriş, temassız alışveriş ve mobil alışveriş olarak gelişimine devam etmektedir. Fiziksel olarak cüzdanda sakladığımız para artık bankadan dışarıya çıkmadan sanal cüzdanlar vasıtasıyla bankalararası dolaşımını sağlamakta ve alışverişlerde ödeme hızlı, güvenli ve kolay hale gelmektedir.

Dijital cüzdanı tanımlamadan önce kavramla bağlantılı olan elektronik para (e-para) kavramını açıklayacak olursak, Yurtçiçek (2013)'in On'lar (2002) grubunun elektronik para üzerine hazırladıkları rapora atfen aktarmış olduğu tanımda e-para, "internet gibi açık bilgisayar ağı üzerinde ödemeleri gerçekleştiren ön ödemeli veya depolanmış değer mekanizmaları ve 'elektronik cüzdan', ya da 'depolamış değer kartları' olarak da tanımlanan, çok amaçlı ön ödemeli kartlar gibi bir çok piyasada hali hazırda denenen ve uygulanan perakende ödemelerin yeni elektronik ödeme aracı" olarak tanımlanmıştır. E-para, nakit paranın elektronik görünümü olarak karşımıza çıkmaktadır. Kullanıcı, kağıt ya da madeni para ile paranın elektronik muadilini satın almakta ve nakit para başka bir ödeme aracı ile değiştirilmektedir.

Gün geçtikçe nakit paranın yerini alan e-para, teknolojik gelişmelerle birlikte kullanım alanına göre çeşitli formlarda karşımıza çıkmaktadır. Yaygın olarak paranın taşınmasında ve muhafazasında kullanılan cüzdanlar zamanla içerisinde e-paranın bulunduğu dijital bir yapıya bürünmüştür.

Dijital cüzdan, paranın saklanmasına ve harcanmasına imkân veren ve kullanıcının elektronik cihazında kurulu bulunan bir yazılımdır. Kredi kartlarının, banka kartlarının veya ön ödemeli kartların tek bir yere tanımlanabileceği elektronik bir cüzdandır. Dijital cüzdanlar kullanıcı ve banka arasındaki iletişimi sağladıklarından cüzdan üzerinde yapılacak işlemlerde yetki kullanıcıya ait olmakla birlikte güvenlik çoğunlukla bankaların sorumluluğundadır. Dijital cüzdanlar, e-cüzdan ve m-cüzdan olarak ikiye ayrılabilir. Bazı uygulamalar iki platformda da hizmet verirken bazıları ürün stratejilerini sadece on-line ya da mobil olarak kurgulamıştır (İnt. Kyn. 13).

4.2.1 On-line Cüzdan/ E-Cüzdan

Dünyadaki kullanıma paralel olarak 1997 ortalarından itibaren ülkemizde, internet ve ticaret olgusuyla tanışmış ve birçok banka müşterilerine internet üzerinden kişisel bankacılık hizmeti vermeye başlamıştır. Yine 1997 sonlarına doğru, deneme amaçlıda olsa bazı bilindik alışveriş merkezleri internet üzerinden alışveriş imkânlarını yavaş yavaş müşterilerine sunmaya başlamıştır (İnt. Kyn. 14).

Türkiye'de ilk elektronik ticaret uygulaması Ocak 1997 tarihinde Remzi Kitabevi'nin açmış olduğu elektronik mağaza ile başlamıştır. Bu mağazayı takiben 1998 ve 1999 yıllarında çok sayıda benzer mağazaların açılmasıyla mağaza sayısında hızlı bir artış gözlenmiştir (Tağıyev 2005).

Ülkemizde internet üzerinden yapılan on-line alışverişlerde ödeme aracı olarak en çok kredi kartları kullanılıyor olsada diğer ülkelerde farklı ödeme sistemlerinin öne çıktığı görülmektedir. Örneğin, Romanya'da kredi kartı ile yapılan ödemeler güvenilir bulunmadığından dolayı yapılan on-line alışverişler de genellikle kapıda ödeme sistemi tercih edilmektedir. Polonya'da ise kredi kartı kullanımı pek yaygın olmadığından ödemeler EFT / Havale yoluyla gerçekleştirilmektedir. Güney Afrika'da ise gelişmiş bir bankacılık sistemi bulunmaması nedeniyle ödemeler mobil ödeme sistemleri aracılığıyla yapılmakta ve bu sistem oldukça gelişme kaydetmektedir (İnt. Kyn. 15).

On-line cüzdan ödeme sisteminde, kullanıcılarına on-line cüzdan hesabı açma imkânı sunan Bkm Express, İninal, İpara, İyzico, Mikro Ödeme ve Paypal gibi ödeme hizmeti veren firmaların sistemlerine, bir defaya mahsus banka kartı, kredi kartı veya ön ödemeli kartın kayıt edilmesi gerekmektedir. Sonrasında, internet üzerinden yapılan alışverişlerde Bkm Express ile öde, Paypal ile öde gibi alışveriş sitesinin anlaşmalı olduğu ödeme firmasının ödeme seçeneği seçilerek kart bilgisi girilmeden sistemde oluşturulan on-line cüzdan hesabı üzerinden ödeme işlemi yapılabilmektedir.

4.2.2 Mobil Cüzdan

Yakın geçmişimizde sadece sesli görüşme yapılabilen sabit telefon hatlarını açtırabilmek için PTT'ye isim yazdırılıp hat çıkması durumunda eve kablolu telefon hattı çekilerek telefon kullanılabilmekteydi. Günümüzün sınır tanımayan teknolojik gelişmeleri doğrultusunda telefonlar mobil hale gelerek akıllanmış, telefondan alışveriş yapılırken bir yandan da ödeme yapılabilir hale gelinmiştir. Telefonun ödeme aracı olarak kullanılması gsm firmaları ve bankaların katılımı ile gelişen mobil cüzdanlar sayesinde mümkün olabilmektedir.

Mobil cüzdan sisteminin kullanılabilmesi için tablet ve telefon gibi mobil cihazlara, m-cüzdan uygulamasının yüklenerek bir defaya mahsus kart bilgilerinin tanımlanması gerekmektedir.

Mobil cüzdan, ödeme bilgilerini ödeme terminaline iletmek için akıllı telefonların ve tabletlerin içinde bulunan NFC (yakın alan iletişim) çiplerini kullanmaktadır. Müşteri mobil cüzdanı ile ödeme yapacağında, mobil cihazında kurulu bulunan uygulamayı çalıştırır ve m-cüzdan uygulamasına şifresi ile giriş yapar. Ödeme seçeneği seçildikten sonra mobil cihaz ödeme terminaline 3-5 cm yaklaştırılarak ya da dokundurularak ödeme işlemi gerçekleştirilir (İnt. Kyn. 16).

4.3 Mobil Ödeme Sistemleri

Telefonlar ödeme aracı olarak mobil cüzdanlar dışında mobil ödeme sistemleri aracılığıyla da kullanılabilmektedir. Bankacılık sisteminden bağımsız olarak gsm operatörlerinin alt yapısı kullanılarak hizmet veren mobil ödeme platformu alışverişlerde güvenlik gerekçesi ile kredi kartı bilgilerini paylaşmak istemeyen müşteriler için alternatif bir ödeme aracı olarak tercih edilmektedir.

Mobil ödeme sisteminde ödeme telefon üzerinden gerçekleşmektedir. "Buna göre, mobil ödeme hizmetinin geçerli olduğu üye iş yerinden alışveriş yapan bir müşteri, iş yerindeki görevliye cep telefonu numarasını vermekte, görevli cep telefonu numarasını ilgili cihaza girerek mobil telefon operatörüne ödeme işlemine ilişkin sorgu mesajı

gönderilmesini sağlamaktadır. Söz konusu ödeme işlemi ile ilgili mesajı alan mobil ödeme operatörü, müşterisine işlem ile ilgili sorgu mesajı göndermekte ve müşteri de gelen mesajı onaylayarak cevaplamaktadır. Müşterinin ödeme işlemini onaylamasının ardından mobil ödeme operatörü üye iş yerini onay konusunda bilgilendirmektedir. Bu kapsamda, müşteri anlaşmalı iş yerinden mal veya hizmeti almakta, mobil telefon operatörü işleme ilişkin ödemeyi üye iş yerine yapmakta ve söz konusu tutarı müşterinin cep telefonu faturasına yansıtmakta, müşteri de alışveriş işlemine ilişkin tutarı cep telefonu faturasını öderken operatöre ödemektedir. İnternet üzerinden gerçekleştirilen mobil ödeme işlemlerinde ise ödeme, alışveriş yapılırken cep telefonu numarasının müşteri tarafından ilgili bölüme girilmesinin ardından müşterinin cep telefonuna gelen onay mesajını yanıtlaması yoluyla gerçekleşmektedir (Karpuz 2012).”

Mobil ödeme sistemi kullanımı kolay ve hızlı bir ödeme imkânı sunması nedeniyle kötü niyetli kullanımın engellenmesi adına her gsm firması farklı olarak işlem başına veya aylık olarak limit sınırlaması getirmiştir. Avea, mobil ödeme servisi için maksimum günlük limit 100 TL ve maksimum aylık limit 300 TL olarak belirlemiştir. Yine bu servisin kullanılabilmesi için faturalı hatlarda 3 ay, faturasız hatlarda 1 ay zaman geçmesi gerekmektedir (İnt. Kyn. 17). Vodafone, mobil ödeme servisi olarak sadece tahsilât hizmeti sunmaktadır. Abonelerine tek seferlik ve günlük olarak maksimum 100 TL, aylık toplam da 150 TL işlem limiti belirlemiştir (İnt. Kyn. 18).

4.4 Ülkemizde Kartlı Ödeme Sisteminde Bulunan Diğer Kuruluşlar

4.4.1 BankalarArası Kart Merkezi

Bankalararası Kart Merkezi; 13 kamu ve özel Türk bankasının ortaklığıyla 1990 yılında kurulmuştur. “Bankalararası Kart Merkezi'nin (BKM) faaliyetleri, ödeme sistemleri içerisinde; nakit kullanımı gerekmeksizin her türlü ödemeyi veya para transferini sağlayan veya destekleyen sistem, platform ve altyapıları oluşturmak, işletmek ve geliştirmektir.” Bunun yanı sıra, “Kredi kartı ve banka kartı uygulaması içinde bulunan bankalar arasında uygulanacak prosedürleri geliştirmek, standardizasyonu sağlamaya yönelik çalışmalar yaparak kararlar almak, Türkiye genelinde uygulamalar ile yurt içi

kuralları oluşturmak, bankalar arasındaki takas ve hesaplaşmayı yürütmek, yurt dışı kuruluş ve komisyonlarla ilişkiler kurmak ve gerektiğinde üyelerini bu kuruluşlarda temsil etmek, halen her banka tarafından devam ettirilen işlemleri daha güvenli, süratli ve daha az maliyetli tek bir merkezden yürütmek, BKM'nin ana faaliyetleri arasındadır (İnt. Kyn. 19)."

BKM aracılığıyla bankalar, birbirleri adına yaptıkları banka kartı veya kredi kartı ödemelerinin takasını ve mutabakatını sağlamaktadırlar. Takas ve mutabakat, üye işyeri ile anlaşmalı banka ve kartı çıkaran banka arasında para transferi işlemidir. Otorizasyon ve Takas/Mutabakat işlemlerine yurtiçinde BKM, yurtdışında ise Visa ya da Master Card aracılık yapmaktadır. BKM kurulmadan önce POS çekimini yapan iş yeri kredi kartları ile ilgili tahsilât işlemini, POS cihazından çıkan slipleri manuel olarak kartı çıkaran bankaya teslim etmek suretiyle gerçekleştirmekteydi.

BKM ürün ve hizmetleri arasında BKM Expres, en yakın ATM, temassız işlemler, NFC, ulaşım projeleri, POSPara, kamu tahsilât çözümleri, yurt içi takas, switch ve 3D Secure bulunmaktadır (İnt. Kyn. 20).

4.4.2 Kredi Kayıt Bürosu

Kredi Kayıt Bürosu; "1990'lı yılların başından itibaren giderek önem kazanan ve hızla gelişen bireysel kredi pazarlama faaliyetleri, "Kredi Risk Yönetimi", "Müşteri İlişkileri Yönetimi" ve "Veri Ambarı Yönetimi" gibi çağdaş kavramları da beraberinde getirmiştir. Özellikle, bireysel kredi portföy hacminin hızla büyümesi, kredi kararı aşamasında kredi riskinin doğru olarak ölçülebilmesine olanak sağlayan yöntemlerin önemini daha da artırmıştır.

Yukarıda bahsi geçen kavramlar için gerekli en önemli hammaddenin 'bilgi' olduğu gerçeğinden yola çıkılarak, kurumlar arasında kredi müşteri bilgilerinin paylaşımıyla ilgili kanun engelinin, 1993 yılında 3182 sayılı Bankalar Kanunu'nun 83. maddesine eklenen ve kredilerin takip ve kontrolüne olanak sağlayan bir hükümle aşılmasıyla birlikte mali kurumların ihtiyaç duyduğu "kurumlar arasında kredi müşterilerine yönelik bilgi paylaşımı" mümkün hale gelmiştir.

Bu yeni düzenleme doğrultusunda, Bankalar Birliği'nin de desteği ile, ana faaliyet konuları para ve sermaye piyasaları ile sigortacılık olan mali kurumlar arasında bireysel kredilerin takip ve kontrolünü sağlamak üzere gerekli olan bilgi paylaşımını gerçekleştirmek amacıyla, 1995 yılında 11 bankanın ortaklığı ile Kredi Kayıt Bürosu A.Ş. kurulmuştur (İnt. Kyn. 21).”

Kredi kayıt bürosuna üye olan kredi kuruluşları ve finansal kuruluşlar, 5411 sayılı Bankacılık Kanunu doğrultusunda müşterilerine ait kredi bilgilerini kendi aralarında paylaşmaktadırlar (Kaya 2009).

Kredi Kayıt Bürosu, güncel olarak bireylere ve reel sektöre yönelik olarak Findeks isimli yeni finansal hizmet platformunu sunmaya başlamıştır. Bireyler, Findeks aracılığıyla bankalar ve diğer finansal kurumlar nezdindeki kredi notunu sorgulayabilmektedirler (İnt. Kyn. 22).

5. BİLİŞİM YOLUYLA DOLANDIRICILIK YÖNTEMLERİ

5.1 İnternet Üzerinden Banka, Kredi Kartı ve Hesap Bilgilerinin Ele Geçirilmesi

5.1.1 Sosyal Mühendislik

Bilişim sistemleri insan hayatının her alanında yaygınlaşarak kullanılmaktadır. Bu sistemlerin gizlilik, bütünlük ve sürekliliğinin sağlanması adına güvenlik unsuru da büyük bir önem taşımaktadır. Geliştirilen sistemlerin paralelinde sistemleri koruyucu güvenlik yazılım ve donanım teknolojileri de geliştirilmektedir. Bu kadar üzerinde çalışılıp test edilerek kullanıma sunulan sistemlerin zamanla tespit edilen açıkları her ne kadar güvenlik yamaları ile kapatılsada, insan unsurunun yapacağı hatalardan kaynaklı açıkları kapatacak bir yama henüz bulunmuş değildir.

Güvenlik unsurunun en zayıf halkasını insan zaafiyetleri oluşturmaktadır. Kötü niyetli insanların sistem güvenliğini aşamayarak gerçekleştiremediği işlemleri, insan doğasında bulunan güven, korku ve yardım etme duygularını kullanarak aşmaları mümkün olmaktadır (Burlu 2013).

Canbek ve Sağıroğlu (2006) sosyal mühendisliği, "Bir bilişim korsanının ilgilendiği bilgisayar sistemini kullanan veya yöneten meşru kullanıcılar üzerinde psikolojik ve sosyal numaralar kullanarak, sisteme erişmek için gerekli bilgiyi elde etme tekniklerine verilen genel addır." şeklinde tanımlamışlar, telefon ile şifre ve kullanıcı bilgilerinin elde edilmesini en belirgin örnek olarak belirtmişlerdir.

Ünver ve Mirzaoğlu (2011) sosyal mühendisliği, "Karşı tarafın zaaflarından yararlanarak, onu, kişisel bilgilerini ifşa etmek veya belli eylemleri yerine getirmek üzere yönlendirmektir. Adi dolandırıcılıkla birlikte; sosyal mühendislik, genellikle, bilgisayar sistemlerine giriş parametrelerini elde etmek suretiyle, bu sistemlere yetkisiz erişim sağlamak veya kredi kartı bilgileri gibi finansal bilgileri ele geçirmek suretiyle bilgisayar yoluyla dolandırıcılık yapmak amacıyla uygulanmaktadır. Sosyal mühendislikte, çoğu zaman, suçu işleyen kişi ile hedef alınan kişi yüz yüze

gelmemektedir.” Etkileme ve ikna etme noktasında kadın sesinin erkek sesine göre daha başarılı olduğu bilinmektedir.

Hadnagy (2013) sosyal mühendisliği, “İnsanoğlunu hayatlarının bir yönünde harekete geçmesi için becerikli bir şekilde yönlendirme sanatı ya da bilimi” olarak tanımlayarak daha geniş bir tanımı “bir kişiyi hedefin en fazla çıkarına olabilecek ya da olmayabilecek bir harekette bulunması için maniple etme edimi” olarak yapmıştır.

Burlu (2013) sosyal mühendisliği, “Etkileme ve ikna etme yöntemlerini kullanarak kurbandan bilgi alma ya da istenilen işleri yapmasını sağlamak” olarak tanımlamıştır.

Wikipedia internet sitesinde sosyal mühendislik, bilgi güvenliği bağlamında insanları bazı davranışlarda bulunmak ya da gizli bilgileri söyletmek için maniple etme, güven sağlayarak ya da hileli hareketlerle aldatarak bilgi toplama, dolandırıcılık ya da bilişim sistemine erişim sağlama olarak açıklanmıştır (İnt. Kyn. 23).

“Sosyal mühendislik, insanlar arasındaki iletişimdeki ve insan davranışındaki açıklıkları tanıyıp, bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir. Bu tanım çerçevesinde iletişim kavramından kasıt, kişiler arasında, kişiyle kurum arasında ya da kurumlar arasındaki etkileşimdir. İnsan davranışlarındaki açıklıklarsa, insanların gündelik sergiledikleri, niyetlerinden bağımsız hareketlerin güvenlik açısından istenmeyen durumlara sebep olması ihtimalleridir. Müdahale derken de güvenlik açısından kritik bilgileri elde etmek eylemini anlıyoruz (İnt. Kyn. 24).”

Sosyal mühendislik teknikleri kullanılarak hedef kişinin, kurumun ya da sistemin normal yollarla ulaşılamayacak bilgilerine ulaşılabilmektedir. Bu bilgiler kullanılarak kişiler doğrudan ya da sistemler üzerinden dolaylı olarak dolandırılabilmektedir (Akarslan 2011).

Sosyal mühendislik yöntemleri, “verinin kaynağına, verinin gizliliğine, verinin nasıl korunduğuna göre değişmektedir. İyi bir sosyal mühendis anlık analiz yaparak ya da

uzun zamanlı bir araştırma ile ilgili senaryoyu bilgisi ve hayal gücüyle tasarlar ve uygulamaya koyar. Sosyal mühendislikte metodlar uygulanacağı kriterlere göre değişmektedir. Kurbanın merakı, vicdanı, inancı, güveni, acıma duygusu, zaafları (makam, mevki, hırs, para, cinsellik, ego) gibi duygularını kullanarak veri hırsızlığı yapılabilir (İnt. Kyn. 25)."

Sosyal mühendislik denince akla Kevin Mitnick gelmektedir. Tarihin ilk hackerlarından olan Mitnick; Pentagon, Sun Microsystems, Motorola gibi büyük kuruluşların bilgisayar sistemlerine erişim sağladığından dolayı ismi bir zamanlar FBI'ın arananlar listesinde bulunuyordu. Yakalanarak yargılanan Mitnick hapis cezasının yanısıra elektronik cihazlara yaklaşmama cezası da almıştır. Yaptıklarını "Aldatma Sanatı" isimli kitabında anlatan Mitnick, bilgi güvenliğinin en zayıf halkasını insan unsurunun oluşturduğunu ve sosyal mühendislik teknikleri kullanılarak birçok gizli bilginin elde edilebileceğini belirtmiştir (Mitnick and Simon 2005).

Burlu (2013), sosyal mühendislik saldırılarını, insan tabanlı ve bilgisayar tabanlı olmak üzere iki şekilde incelemiştir. İnsan tabanlı sosyal mühendislikte insani ilişkiler bağlamında iletişim becerileri ve ikna etme yöntemleri ile istenilen bilgiye ulaşılabileceğini, bilgisayar tabanlı sosyal mühendislikte, e-posta ekleri, web siteler ve spam e-postalar kullanılarak hazırlanan sahte içeriklerle karşıdaki kişiden istenilen bilgilerin elde edilebileceğini belirtmektedir. Sosyal mühendisliğe karşı koyma noktasında en büyük silah kullanıcıların bilinçli olmasıdır. Kullanıcılar bilinçlenmediği müddetçe bilgisayar korsanları başarıya ulaşmaya devam edeceklerdir.

5.1.2 Kötücül Yazılımlar

Kötü amaçlı yazılım veya malware (malicious software), bilgisayar sistemlerine zarar vermek, bilgi çalmak veya kullanıcıları rahatsız etmek gibi amaçlarla hazırlanmış yazılımlara verilen genel addır. Bilgisayar sahibinin bilgisi ve rızası dışında sisteme yetkisiz erişim yapmak veya zarar vermek için üretilen yazılımlardır. Bu yazılımlara örnek olarak virüsler, solucanlar, truva atları ve rootkitler verilebilir (İnt. Kyn. 26).

5.1.2.1 Virüs

"Virüsler, yayılmak için kullanıcı etkileşimini gerektiren zararlı program kodlarıdır. Virüsler genellikle işletim sistemlerinin ya da yazılım uygulamalarının açıklarından bağımsız olarak çalışırlar (Çakar 2013)."

Bilinen en tehlikeli ve en eski kötücül yazılımlardandır. Biyolojik virüslerden esinlenerek adlandırılan bilgisayar virüsleri yayılabilen ve kendi kendine çoğalabilen programlardır. Cd/dvd, flash bellek, internet ya da e-posta ekleri ile sistemlere bulaşırlar. Dosya virüsleri, ön yükleme (boot) virüsleri, makro virüsleri, betik (script) virüsleri olmak üzere dört sınıfa ayrılmaktadırlar (Canbek ve Sağıroğlu 2006).

Tarihte ilk olarak virüs fikri teorik manada 1948 yılında John Von Neuman tarafından kendisini kopyalayabilen bilgisayar programı olarak ortaya atılmıştır. Çalışan ilk virus ise 1982 yılında Rick Skrenta tarafından Elk Cloner ismiyle yazılmıştır. Bu virüs Apple DOS 3.3 işletim sistemine bulaşıp disketler vasıtasıyla yayılmıştır. Rick Skrenta isimli lise öğrencisinin arkadaşlarına şaka amacıyla hazırlamış olduğu bu program oyun dosyaları içerisine kendini gizlemekte ve oyunun 50. kez çalıştırılmasında virüs aktif hale gelmekteydi (İnt. Kyn. 27).

Virüslerin ortaya çıkarak yayılmaya başlamasıyla birlikte virüslerin sistemlere bulaşmasını engellemek ya da virüs bulaşmış sistemlerden virüsleri temizlemek için anti virüs programları yazılmaya başlamıştır. Mcafee ve Symantec firmaları öncülüğünde piyasaya sunulan anti virüs programları zamanla piyasaya katılan yeni firmalar ile ciddi bir anti virüs endüstrisini oluşturmuştur.

5.1.2.2 Solucan (Worm)

İnsan etkileşimi olmaksızın kendi kendine çalışabilen ve bir kopyasını veri iletim ağında bulunan diğer bilişim sistemlerine kopyalayabilen zararlı yazılımlardır. En çok virüslerle karıştırılmaktadırlar. Virüslerin alt kategorisinde bulunan solucanlar, sistem içinde zarar vermeksizin de bulunabilirler (Dülger 2013).

Solucanlar sistemlere girdiklerinde dosya veya bilgi iletim sisteminin denetimini ele geçirirler. Sistemde kendi başına ilerleme ve en tehlikeli yönü de kendisini çok sayıda çoğaltabilme özelliğine sahiptirler. Bu nedenle sistem belleğini ve ağ bant genişliğini tüketerek sistemi yavaşlatırlar ya da tamamen kullanılmaz hale getirebilirler. E-postalar, web siteleri ya da hafıza birimleri aracılığıyla sistemlere bulaşabilirler (Eralp 2012).

Solucanlar bazen yapılış amaçlarına göre bulundukları sistemlere zarar vermezler ancak sistemi gizli bir saldırgan haline getirebilirler. Bulundukları sistemi bir botnet'e dahil eden solucanlar, sistemi spam göndermek veya başka bilgisayarlara saldırıda bulunmak amacıyla bilgisayar korsanlarının kullanımına açabilirler (Çakar 2013).

Solucanlar virüsler gibi çalıştırılabilir dosyalara kendilerini iliştirmezler veya bu programın parçası olmazlar. Herhangi bir etkileşime ihtiyaç duymaksızın çoğalarak hareket ederler. "Solucan ismi, 1975 yılında John Brunner tarafından yazılan "Shockwave rider (şok dalgası binicisi)" isimli bilim kurgu romanında, bir bilgisayar ağı üzerinden kendi kendini yayan bir programa verdiği isimden gelmektedir (Canbek ve Sağıroğlu 2006)."

Tarihte ilk solucan vakası 2 Kasım 1998 tarihinde ABD'de o günkü adıyla Arpanet iletim ağına yüklenen yazılım ile ortaya çıkmıştır. Yazılım hızlı bir yayılım göstererek bilim ve askeri sistemlere bulaşmıştır. Yapılan tespitlerde 2000 bilgisayar bu saldırıdan etkilenmiş, yaklaşık 150 000 dolarlık zarar ortaya çıkmıştır (Dülger 2013).

5.1.2.3 Trojan (Truva Atı)

Trojan, ismini Yunan mitolojisinde yer alan Truva atı efsanesinden almakta ve bu mantık üzerine çalışmaktadır. Normal bir program içerisine sonradan eklenen zararlı kodlar nedeniyle kullanıcısının bilgisi dışında sisteme işlem yaptıran zararlı programlardır (Akarslan 2011).

Trojanlar, virüsler gibi kendi kendine çoğalmazlar. İçerisinde trojan barındıran program, çeşitli sosyal mühendislik yöntemleri ile kullanışlı, faydalı bir programmış gibi karşı

taraf ikna edilerek bizzat çalıştırılmaları ile aktif hale gelirler. Aktif hale gelen trojan sistem arka planında çalışarak kişisel ve bankacılık bilgilerini toplayabilir, ses ve görüntü sistemine erişerek bu verileri başka sistemlere gönderebilir (Burlu 2013).

Trojanlar, internet üzerinden ücretsiz dağıtılan program ve oyunların içerisine hatta resim ve video dosyalarının içerisine gizlenebilmektedirler. Programın kurulumu ya da dosyanın açılması esnasında sisteme kendisini yükleyerek aktif hale gelirler. Bilişim suçlarının çoğu ve casusluk faaliyetleri trojanlar vasıtasıyla gerçekleştirilebilmektedir.

Truva atı yöntemiyle, dosya içeriğini değiştirme, silme, şifreleme ve başka sistemlere gönderme-alma, bunun yanısıra sistemi uzaktan erişime açarak DOS saldırılarında zombi bilgisayar olarak kullanma, sistem üzerinden spam e-mail (istenmeyen e-mail) gönderme gibi birçok bilişim sistemi işlemi gerçekleştirilebilmektedir (Eralp 2012).

5.1.2.4 Diğer Kötücül Yazılımlar

Temelde yukarıda belirtmiş olduğumuz türlerin dışında Spyware (casus yazılım), Rootkit (kök kullanıcı takımları), Adware (reklam yazılımları), Exploit (korunmasızlık sömürücüleri) ve Browser Hijacking (tarayıcı soyma) gibi birçok kötücül yazılım türü bulunmaktadır.

5.1.3 Kimlik Avı

Sosyal mühendisliğin bilişim alanında karşımıza çıkan en yaygın biçimi kimlik avı, literatürdeki adıyla phishing dolandırıcılığıdır. Başkasına ait kişisel bilgilerin elde edilerek o kişiymiş gibi hareket edilmesi ve bu bürünülen yeni kimlikle haksız menfaat temin edilmesi yaygın dolandırıcılık yöntemlerindendir (Çakar 2013).

Hekim ve Başıbüyük'e göre kimlik hırsızlığı, "başkasına ait kişisel verilerin ele geçirilmesi ve bu verilerin dolandırıcılık veya aldatma amacıyla kullanılmasıdır." Kimlik hırsızlığı genellikle ekonomik kazanç elde etmek için yapılmaktadır. Bununla birlikte kişinin itibarını zedelemek amacıyla da yapılabilmektedir. Kişinin kimlik

bilgileri ile internetten pornografik materyaller sipariş etmek bu duruma örnek verilebilir (Hekim ve Başıbüyük 2013).

Karimi ve Korkmaz (2013) kimlik hırsızlığını, "gerçek veya tüzel kişilere ait kişisel bilgilerin yetkisiz kişilerce, dolandırıcılık veya diğer suçların işlenmesinde kullanılmak üzere ele geçirilmesi, iletilmesi (transferi), muhafaza edilmesi veya kullanılması" olarak tanımlamışlardır. Kişisel verilerin korunması çalışmalarında kimlik hırsızlığının, klasik (off-line) veya çevrimiçi (on-line) olmak üzere iki farklı ortamda işlenebileceğini belirtmişlerdir.

Klasik Off line yöntemler

-Çöp karıştırma (dumpster diving)

-Bahane yaratma (pretexting)

-Omuz üstünden seyir (shoulder surfing)

-İş kayıtları hırsızlığı

Çevrim içi On line yöntemler

-Kötü niyetli yazılım veya programlar (malware)

-Aldatıcı nitelikte e-posta veya internet siteleri

1) Oltalama (phishing)
2) İstenmeyen elektronik posta (spam)

-Sistem veya yazılımların açıkları (hacking) yöntemleri kullanılmaktadır.

5.1.3.1 Phishing

Alataş ve Atan (2007) phishing'i, "sosyal mühendislik teknikleri kullanılarak, kurbanın şifreleri, banka hesap numaraları, kredi kartı bilgileri gibi özel ve yüksek güvenlik isteyen bilgilerini, kurbanı aldatarak elde etme yöntemi" bununla birlikte "insanların kavramadaki yanılmalarından ve algısal zaaflarından faydalanarak insanlardan çıkar sağlamak" olarak tanımlamışlardır.

Phishing kavramının, İngilizce password (şifre) ve fishing (balık avlamak) sözcüklerinin birleşmesiyle türetilmiş bir terim olduğu, ingilizce "password harvesting fishing" (şifre hasadı avcılığı)' in bir kısaltması olduğu ya da 1980'de ilk kez

psikolojik teknikler kullanarak kredi kartı bilgilerini elde eden Brien Phish'e bir atıf olduğu belirtilmektedir (Canbek ve Sağıroğlu 2006).

Phishing, yemleme olarak da ifade edilmektedir. Türk Dil Kurumu'nun web sitesinde yeralan bilim ve sanat terimleri ana sözlüğünde yemleme, "İnternet kullanıcıların şifreler, kullanıcı adları gibi kişisel tanımlama bilgilerini ve finansal hesap erişim bilgilerini soysal mühendislik ve teknik hileler kullanılarak elde etmeyi hedefleyen saldırılar" olarak tanımlanmıştır (İnt. Kyn. 28).

Dolandırıcılığın ilk adımı olarak, sosyal mühendisliğin uygulama alanı olan phishing yöntemi ile internet bankacığına giriş bilgileri ve kredi kartı bilgileri elde edilebilmektedir. Bu bilgilerin gerek satılması gerekse de kullanılması ile haksız menfaat temin edilmekte bununla birlikte hesap sahipleri de mağdur olmaktadırlar.

5.1.3.2 Phishing Yöntemleri

E-posta Yöntemi

2000'li yılların başlarında e-posta hesaplarına bankalardan geliyormuş gibi görünen e-postalar gönderilerek müşterilerin bilgilerini güncellemesi istenilmekteydi. Bu e-postalara inanarak müşteri bilgilerini ilgili kutucuklara giren kullanıcıların girmiş olduğu bankacılık bilgileri bu yöntemle bilgisayar korsanlarının eline geçmekteydi. Bu şekilde dolandırılan birçok kullanıcı o dönem mağdur olmuştur. Gerek internet bankacılığı sistemine alışan müşteri profili gerekse de bankalarca oluşturulan farkındalık sayesinde müşteriler bu türden e-postalara itibar etmemeye başlamışlardır. Bu nedenle bu yöntem inandırıcılığını yitirdiğinden günümüzde pek kullanılmamaktadır.

İnternet kayıtlarına göre tarihteki ilk Phishing yönteminin örneğine 2 Haziran 1996 tarihinde Usenet haber grubunda rastlanmıştır (İnt. Kyn. 29). Tarihe geçen bu olaydan 2003 yılı ortalarına kadar geçen dönemde phishing dolandırıcılığı, genellikle inandırıcılık özelliği olmayan salt yazı bazlı ve haber grubu iletileri ile yapılmaktaydı.

2003 yılının ikinci yarısından itibaren büyük bir değişim geçiren phishing, çok değişik teknikler kullanılarak inandırıcılığı yüksek bir şekilde yapılmaya başlanmıştır. Bu değişimin sebebine gelince o dönemde, göz aldanması sağlaması için alınan geçici alan adları ve HTML bazlı dinamik web yapısı inandırıcılığı artırmada büyük rol oynamıştır. Phishing'in ülkemizde kullanılmaya başlaması 2004 yılı sonlarını bulmuştur. Yurtdışında olduğu gibi ilk phishing örnekleri inandırıcılıktan uzak ve basit bir yapıda karşımıza çıkmış iken zamanla gelişen tekniklerle yapılan phisihing saldırıları ile mağdur sayısı da artmıştır (Altaş ve Atan 2007).

Phishing yöntemi on-line iletişim ortamı üzerinden gerçekleştirildiğinden, düzenlenen sahte bir e-mail içeriğinin kısa süre zarfında çok sayıda kullanıcıya ulaşması mümkündür. Bu yönüyle büyük risk oluşturmaktadır. Phishing'in daha iyi anlaşılabilmesi için daha önce gerçekleşmiş somut olaylar irdelenerek resimler üzerinden bilgi aktarımı yapılacaktır.

Bankalara ait internet sitelerinin sahteleri oluşturularak gerçekleştirilen phishing yönteminin yaygın olduğu dönemde, Akbank isimli bankadan geliyormuş izlenimi veren, resim 5.1 ve 5.2'de gösterilen e-posta içerikleri kurgulanarak birçok kullanıcının e-posta hesabına gönderilmiştir.

Resim 5.1 Phishing amaçlı oluşturulmuş sahte e-mail içeriği (İnt. Kyn. 30).

Resim 5.2 Phishing amaçlı oluşturulmuş sahte e-mail içeriği (İnt. Kyn. 30).

Bu ve buna benzer e-mail içeriklerinde; internet bankacılığı hesabının hizmet süresinin dolacağı bildirilerek, e-mail içeriğinde belirtilen linkin açılması ile hesaba ulaşılabileceği ve buradan hesabın tekrar aktif edilebileceği belirtilmektedir. Bankaya ait bir linkmiş izlenimi veren linkin üzerine mouse'un oku ile gelindiğinde, aslında linkin altında gömülü çok farklı bir siteye ait link olduğu görülecektir. Link tıklanarak açıldığında ise hangi bankaya ait e-mail içeriği gönderildi ise o bankaya ait internet sitesinin benzeri bir site karşımıza çıkacaktır. Sahte oluşturulan bu sitede, internet bankacılığı hesabına ait kullanıcı adı ve şifre ya da banka/kredi kartı numarası ve şifresinin girilmesi istenmektedir. Bu bilgileri giren müşterinin internet bankacılığı hesabı ele geçirilerek hesapta bulunan paralar çok kısa zaman aralığında başka hesaplara aktarılmakta ya da elde edilen kart bilgileri ile sahte kartlar oluşturularak kullanılabilmektedir.

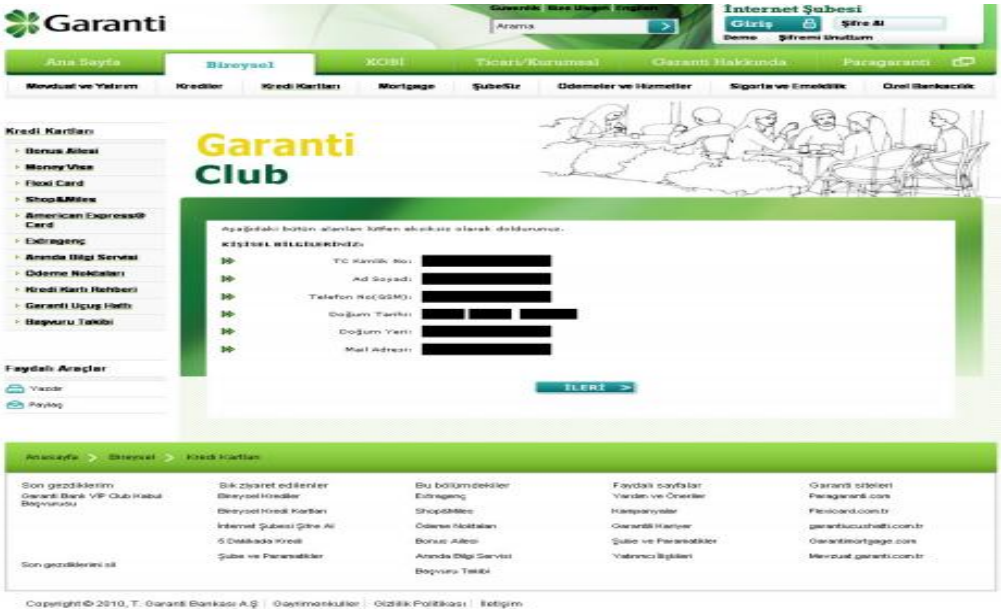
Üyelik ve kredi kartı bilgilerinin elde edildiği başka bir phishing örneği de resim 5.3'de gösterilen Garanti isimli bankadan geliyormuş izlenimi veren e-posta içeriğidir. Kullanıcıya 100TL bonus ve kredi kartı için extra vip özellikler kazandığını müjdeleyen bir e-posta içeriği gönderilmektedir. İçeriğe inanan kullanıcının hediyelerini alabilmesi için başvuru yapabileceği başvuru butonu konularak kurbanının ikinci aşamaya geçmesi sağlanmaktadır.

Resim 5.3 Phishing amaçlı oluşturulmuş sahte e-mail içeriği (İnt. Kyn. 31).

Başvuru butonu tıklanarak açıldığında resim 5.4'de görülen Garanti isimli bankanın internet sitesine benzeyen site açılmaktadır. Bu aşamada olayın inandırıcılığı daha da artırılarak kullanıcının şüpheleri kırılmaktadır. Hediyelerin alınabilmesi için kurbanın katıl butonuna tıklayarak bir sonraki aşamaya geçmesi sağlanmaktadır.

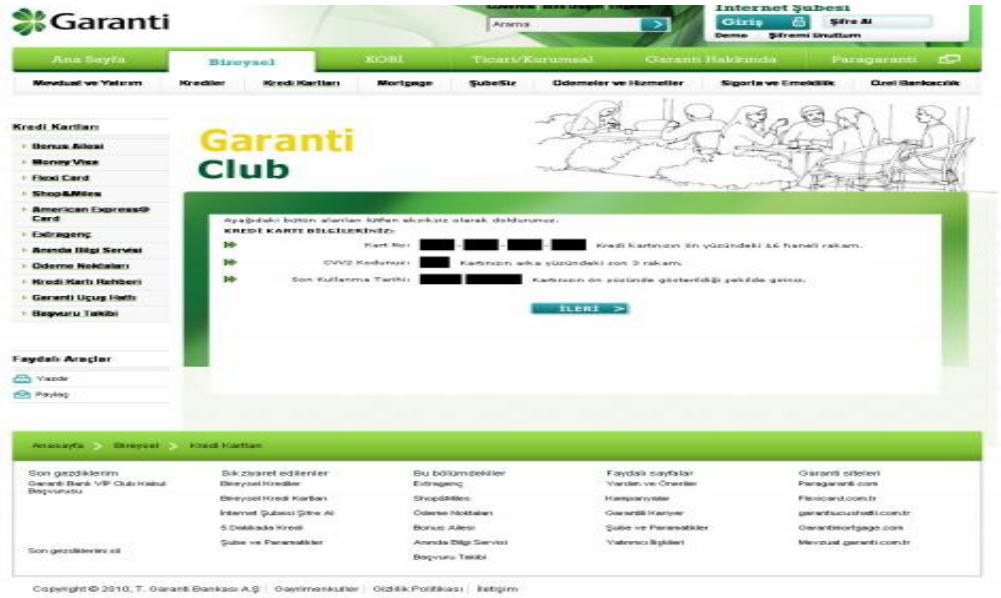
Resim 5.4 Phishing amaçlı oluşturulmuş sahte internet sitesi (İnt. Kyn. 31).

Katıl butonuna tıklanılarak açıldığında farklı bir giriş ekranı kullanıcıyı karşılamaktadır. Bu alana resim 5.5'de görülen, T.C. kimlik no, ad ve soyad, telefon numarası gibi kişisel bilgilerin girilmesi istenilmektedir.



Resim 5.5 Phishing amaçlı oluşturulmuş sahte internet sitesi (İnt. Kyn. 31).

İleri butonu tıklanarak bir sonraki adıma geçildiğinde, bilgisayar korsanının asıl niyeti ortaya çıkmaya başlamaktadır. Bu alanda kullanıcıdan resim 5.6'da görülen, kredi kartı üzerinde bulunan bilgileri girmesi istenilmektedir.



Resim 5.6 Phishing amaçlı oluşturulmuş sahte internet sitesi (İnt. Kyn. 31).

İleri butonuna tıklanarak bir sonraki adıma geçildiğinde, resim 5.7'de görülen, çok mahrem olan ve yüksek güvenlik barındıran anne kızlık soyadı ve on-line işlem ve alışverişte istenmeyen kredi kartına ait pin kodu bilgisinin girilmesi istenilmektedir. Hatta inandırıcılığı artırma adına pin kodunun sanal klavye ile girilmesi sağlanmaktadır.

Resim 5.7 Phishing amaçlı oluşturulmuş sahte internet sitesi (İnt. Kyn. 31).

Tamamla butonuna tıklanarak işlem sonlandırıldığında, işlemin başarılı bir şekilde gerçekleştiğini belirtir, resim 5.8'de gösterilen bilgilendirme ekranı kullanıcının karşısına çıkmaktadır. Aslında bu aşamada kredi kartına ait tüm bilgiler bilgisayar korsanının eline geçmiş bulunmaktadır. Bu aşamadan sonra bu bilgiler kullanılarak internet üzerinden alışveriş yapılabileceği gibi fiziksel olarak kredi kartı üretilerek ATM'den nakit çekilebilir ve kart ödeme işlemlerinde kullanılabilir. Ayrıca kişisel bilgiler kullanılarak müşteri hizmetleri çalışanı ikna edilerek kartın limiti yükseltilebilir, hatta yeni ek kartlar çıkartılabilir.

Resim 5.8 Phishing amaçlı oluşturulmuş sahte internet sitesi (İnt. Kyn. 31).

Sahte Web Sitesi Yöntemi

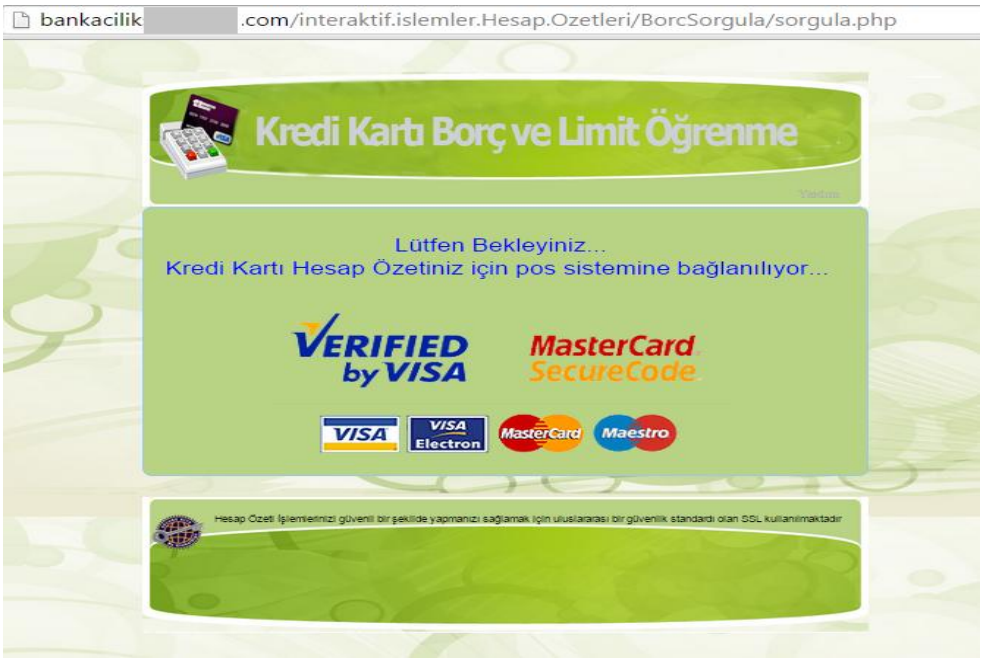
Günümüzde yazılım teknolojilerindeki gelişmeler web sitelerinin taklit edilmesini kolaylaştırmıştır. Bu kolaylık on-line dolandırıcılık yapan bilgisayar korsanlarının elinde ciddi bir silaha dönüşmektedir. Dolandırıcılar, bankalar başta olmak üzere on-line ödeme kabul eden resmi ve özel kuruluşların web ara yüzlerini kolayca kopyalayarak sahte web sayfaları oluşturabilmektedirler. Phishing amaçlı oluşturulan bu siteler genellikle yazım ve dil bilgisi hataları, tehdit niteliğinde ve abartılı ifadeler içermektedir (Çakar 2013).

Sahte site oluşturularak yapılan dolandırıcılık en yaygın olan phishing yöntemidir. Güncel olaylar doğrultusunda farklı yapıda sahte siteler karşımıza çıkmaktadır. Örneğin Ocak ve Temmuz aylarında ödemiş olduğumuz motorlu taşıtlar vergisinin ödendiği günlerde vergi tahsilâtı yaptığını belirten birçok sahte web sitesi internet üzerinden yayına çıkmaktadır. Mağdurlar arama motorlarına kredi kartı borcu ödeme, mtv ödeme, kontör yükleme, fatura ödeme ya da herhangibir banka ismini yazarak sahte oluşturulmuş gerçek sitenin bire bir kopyası bir siteye yönlendirilmektedir. İşlemler neticesinde mağdurlara ait başta kredi kartı bilgileri olmak üzere kişisel ve bankacılık bilgileri elde edilmektedir. Bu siteler çok kısa süreliğine yayında bulunurlar ve çoğu yurtdışından yayın yaptığı için siteyi yayınlayanların tespiti oldukça güçtür.

Konunun daha iyi anlaşılabilmesi için 21 Mart 2015 günü yayında bulunan canlı bir site üzerinde çalışma yapılarak, aşamalar tek tek irdelenip bilgi aktarımı yapılmıştır. İnternet üzerinde herkes tarafından erişilebilen Google arama motoruna "kredi kartı borcu ödeme" şeklinde ibare yazılarak yapılan sorgulamada, birçok sitenin listelendiği görülmüş, rastlantısal olarak listenin beşinci sırasında yer alan www.kredikartıborç*********.com isimli site tıklanarak açılmak istendiğinde sitenin başka bir siteye yönlendirildiği ve bankacilik**********.com/interaktif.islemler.Hesap. Ozetleri/BorcSorgula/ isimli sitenin açıldığı görülmüştür. Sitenin üst kısmına resim 5.9'da gösterilen, "Kredi Kartı Borç ve Limit Öğrenme" şeklinde başlığın yerleştirildiği ve orta kısımda kredi kartı bilgilerinin girilebileceği kutucukların bulunduğu yine inandırıcılığı artırmak adına siteye sanal klavye yerleştirildiği görülmektedir.

Resim 5.9 Phishing amaçlı oluşturulmuş sahte internet sitesi (İnt. Kyn. 32).

Sitenin orta noktasında bulunan kutucuklara rastgele bilgiler girilerek tamam tuşuna basıldığında, resim 5.10'da görülen, bankacilik**********.com/interaktif.islemler. Hesap.Ozetleri/BorcSorgula/sorgula.php isimli sayfanın açıldığı, sayfanın başlığında "Lütfen bekleyiniz kredi kartı hesap özetiniz için POS sistemine bağlanıyor" şeklinde ibarenin yer aldığı ve sayfanın bu şekilde bir müddet beklemede kaldığı görülmüştür.



Resim 5.10 Phishing amaçlı oluşturulmuş sahte internet sitesi (İnt. Kyn. 33).

Bir müddet geçtikten sonra sitede kendiliğinden bankacilik**********.com/interaktif. islemler.Hesap.Ozetleri/BorcSorgula/smspay.php isimli sayfanın açıldığı görülmüştür. Sayfanın başlığında, resim 5.11'de görülen, "Lütfen telefonunuza gönderilen 3D şifrenizi giriniz" ibaresinin bulunduğu görülmüştür. Kutucuğa rastgele rakamlar girilerek gönder butonuna basıldığında sayfada herhangi bir hareketliliğin olmadığı, sayacın geri sayımına devam ettiği görülmüştür.

Resim 5.11 Phishing amaçlı oluşturulmuş sahte internet sitesi (İnt. Kyn. 34).

Sonuç olarak; arama motoruna girilen bilgiler doğrultusunda phishing amaçlı oluşturulan siteye yönlendiren kullanıcı, hiçbir güvenlik özelliği bulunmayan sıradan oluşturulmuş sayfa ile karşılaşmaktadır. Kutucuklara kredi kartı üzerinde yazan bilgiler girilerek tamam butonuna basıldığı andan itibaren girilen bilgiler bilgisayar korsanının veri tabanına gitmekte tabiri caizse eline geçmektedir. Bu bilgiler ile sahte kredi kartı oluşturulacağı gibi anlık olarak da özellikle yurt dışı kaynaklı sitelerden alışveriş yapılarak ödeme bilgisi olarak bu kredi kartı bilgileri girilmektedir. Resim 5.10'da görüleceği üzere "Lütfen bekleyiniz kredi kartı hesap özetiniz için pos sistemine bağlanıyor" şeklinde bir müddet ekran beklemektedir. Bu bekleme esnasında dolandırıcılar bu bilgileri kullanarak yukarıda belirtilen alışveriş işlemlerini gerçekleştirmekle meşguldürler. Dolandırıcılar tarafından ödeme bilgileri sisteme girildikten sonra olayın son aşaması olan resim 5.11'de görünen, üç boyutlu doğrulama

(3D) şifresinin de elde edilmesi için üçüncü bir sayfa açılmaktadır. Herhangi bir güven telkin etmeyen sayfaya kullanıcının telefonuna gelen şifrenin yazdırılması suretiyle bu bilgide elde edilerek alışveriş sistemine girilmekde ve işlem sonlandırılmaktadır. Kullanıcı, kredi kartına ait borç bilgilerinin ekrana çıkmasını beklerken çoktan kredi kartına yansıyan borç ile dolandırılmaktadır.

Bahse konu sitenin hosting bilgileri incelendiğinde, sitenin yurtdışından Amerika'dan yayın yaptığı ve üyelik bilgilerinin eksik olarak verildiği görülmektedir. Bu yönüyle bile sitenin güvenli olmadığı anlaşılmaktadır.

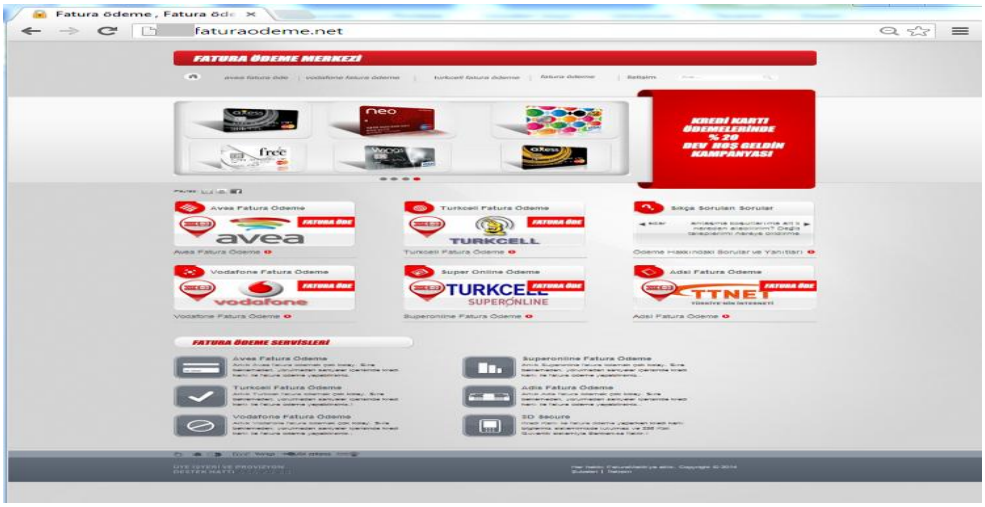
Konunun pekiştirilmesi adına birkaç sahte web sayfası örneği daha inceleyecek olursak; www.***odememerkezi.net Erişim Tarihi: 20.09.2013

Kontör yükleme teması üzerine kurulu sitede, resim 5.12'de gösterilen, kontör yüklenecek telefon numarası ve kredi kartı bilgileri ile birlikte kredi kartının şifresi de istenilmektedir. Siteyi cazip kılma adına ödemlerde %15 indirim yapılacağı belirtilmektedir. Yine inandırıcılığı artırmak adına sanal klavye ekranı ve sayfanın alt kısmında SSL güvenlik standartlarının kullanıldığı belirtilmektedir.

Resim 5.12 Phishing amaçlı oluşturulmuş sahte internet sitesi (İnt. Kyn. 35).

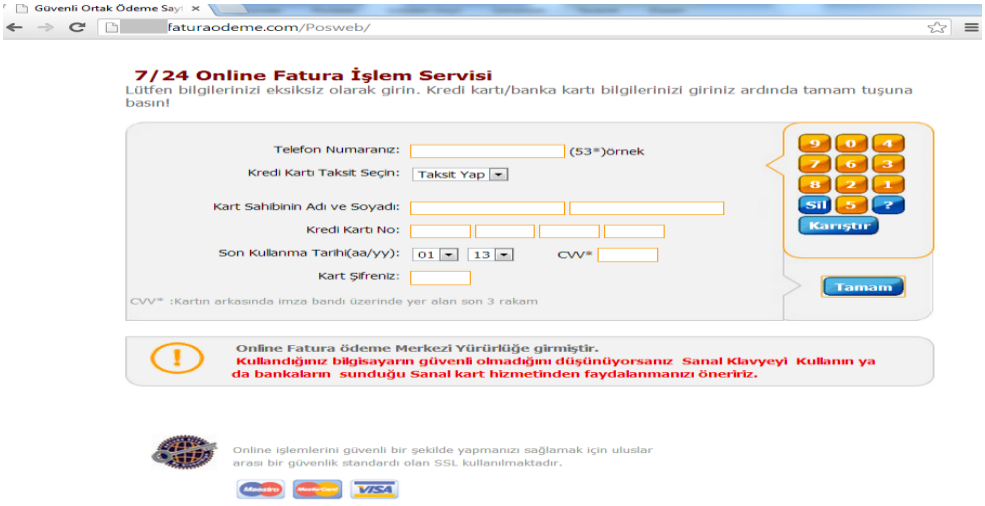
www.***faturaodeme.net Erişim Tarihi: 13.01.2014

Fatura ödeme teması üzerine kurulu site içeriğinde, resim 5.13'de gösterilen, telefon ve internet aboneliklerine ait faturaların ödenebileceği belirtilerek hangi firmaya ait fatura ödenecekse linkine tıklamak suretiyle ödeme sayfasına yönlendirilmektedir.



Resim 5.13 Phishing amaçlı oluşturulmuş sahte internet sitesi (İnt. Kyn. 36).

Operatöre ait logoya tıklandığında sitede www.***faturaodeme.net/Posweb ismli sayfanın açıldığı ve açılan ödeme sayfasında, resim 5.14'de gösterilen, telefon numarası ile birlikte kredi kartı ve kredi kartına ait şifrenin de girilmesi istenilmektedir. İnandırıcılığı artırmak adına sanal klavye ekranı ve sayfanın alt kısmında SSL güvenlik standartlarının kullanıldığı belirtilmektedir.



Resim 5.14 Phishing amaçlı oluşturulmuş sahte internet sitesi (İnt. Kyn. 36).

Scam E-Mail Yöntemi

E-posta yoluyla genellikle İngilizce ya da ülkemiz için tam çevrilememiş Türkçe içerikli olarak para ya da her türlü ürün kazandırma vaadiyle gönderilen aldatmaya yönelik e-mail içeriğidir. Nijerya mektubu, saadet zinciri, piramit entrikası ve mektup zinciri en sık rastlanan web sahtekârlıklarındandır (Canbek ve Sağıroğlu 2006).

Gönderilen e-posta içeriklerine bakıldığında, piyangodan para çıktığı, rüşvet paralarının ya da ölmüş bir vatandaşın ortada kalan servetinin yurt dışına çıkarılabilmesi için yardım talebinde bulunan kurguların yapıldığı görülmektedir.

Bu alanda en çok bilinen yöntem Nijerya mektubudur. Nijerya, Zimbabwe, Zaire ve Kongo kaynaklı olduğu için bu isimle adlandırılan bu dolandırıcılık yöntemi, kendisini avukat, bürokrat, ya da zengin bir iş adamı olarak tanıtan dolandırıcılar, internet üzerinden çok sayıda kullanıcıya içeriğinde farklı hikâyeler bulunan e-mailler göndermektedirler. E-maillerin ortak noktasını yüklü miktarda bulunan paranın çeşitli sebeplerden dolayı ülke dışına çıkması gerektiği ve e-maili alan kişinin hesabına gönderilebilmesi için yardımına ihtiyaç duyulduğu belirtilmektedir. E-maili alan kişinin güvenini kazanmak için telefon, adres, kimlik bilgileri hatta böyle bir paranın mevcut olduğunu gösterir sözde belgeler bile gönderilmektedir. Bu bilgilendirmeden sonra paranın ülke dışına çıkabilmesi için havale masrafının gönderilmesi gerektiği belirtilmektedir. Bu hikâyeye inanıp havale masrafı için para gönderen kişiler bu şekilde dolandırılmaktadırlar (İnt. Kyn. 37).

E-mail olarak gönderilen Nijerya mektubu örneği;

“Kimden : webemaildelivery006@....
Tarih : 29 Ağustos 2006
Konu : Sayın Bay/Bayan

Sayın Bay/Bayan
Bunu çok (kişiye) yazdım ama hiç cevap alamadım. Anlatmaya çalıştım ama aldığım

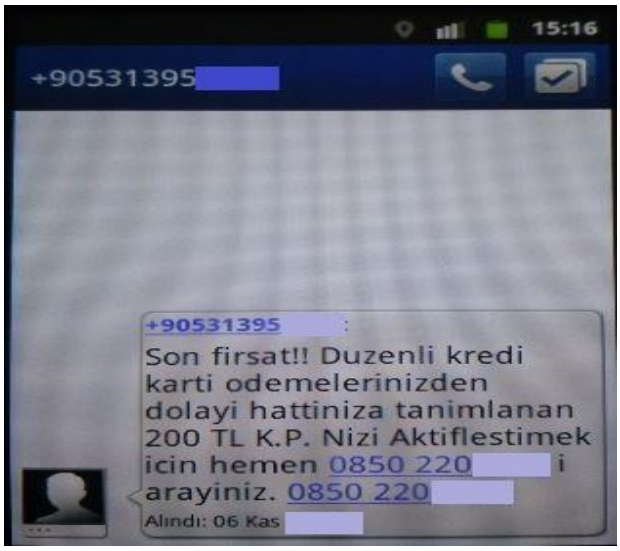
cevapların çoğu şaka yapıyor olduğum şeklindeydi. Umarım size de şaka gibi gelmez Bay/Bayan. Emailinizi bir internet dergisinde gördüm şu sıralarda internet kullanımını geliştirmek üzere ofislere dağıtılan ve tüm personelin paylaştığı dergide. Umarım kötü ingilizcemi maruz görürsünüz. İngilizcem iyi değil, zaten pek eğitimli birisi de değilim. Ben Bay Kola Fashonu. First Bank of Nigeria'nın Portharcourt'taki Doğu Şubesi'nde temizlikçiyim. Bankama, işime bağlı birisiyim. Bu nedenle şube müdürü (Bay Sam Sumalo) bana çok güvenirdi. Eşimin cenazesini kaldırdığımızdan dolayı bir hafta boyunca ofise gidemediğimden dolayı işlerin çok biriktiği bir Pazartesi günüydü ki şube müdürümüz beni ofisine çağırdı. Ortaya bir kutu çıkardı ve onu saklamamı istedi. Kutunun içinde para olduğunu biliyordum ama kaç para olduğunu bilmiyordum. Kutunun içinde 20 milyon 10 bin dolar olduğunu ve bu parayı banka hesaplarından çaldığını söyledi. Kutuyu geri isteyene kadar evimde saklamamı, bunun karşılığında bana paranın yüzde 10'unu vereceğini söyledi. Neden beni seçtiğini sordum. Güvenebileceği tek kişinin ben olduğumu söyledi. Kabul ettim çünkü ben sadece sıradan bir temizlikçiydim; zengin olmak istiyordum. Eve dönerken bir video kamera ödünç aldım; 15 yaşındaki oğlum, paraları sayarken filmimi çekti. Parayı söz verdiğim gibi sakladım. Size bu epostayı gönderme nedenim, müdürün evine silahlı soyguncuların baskın yaptığını ve bunun sonucunda öldürüldüğünü öğrenmiş olmam. Artık parayı kullanabilmemin hiç bir yolu yoktu çünkü sıradan bir temizlikçi olarak bu kadar parayı nereden bulduğumu açıklayacak bir yalan bulamazdım. Size bu e postayı bu nedenle gönderiyorum – parayı yabancı birisine göndermek istiyorum. Bu şekilde paranın bulunması imkansız olacaktır. Sizden para ya da banka hesap bilgilerinizi istemiyorum. Tek istediğim isminizi ve adresinizi göndermeniz. Kutuyu UPS'in doğu şubesinin müdürü olan ablama vereceğim. O da kutuyu şahsen sizin ev adresinize ulaştıracak. Bu yolla paket kontrolden geçirilmeyecek çünkü ablam UPS'teki tüm kontrolörlerin başıdır. Bir ev veya ofis adresine ihtiyacım var çünkü ablam kimseyle otel, restaurant, park, havaalanı gibi yerlerde buluşmaz, para değiş tokuşu yapmaz. Onunla ancak bir ev veya ofiste buluşabilirsiniz. Eğer sizin için uygun değilse, size yanıt vermeyeceğim çünkü parayı kaybetmek istemem. Harcamalar bu şekilde halledilecek, sizin ödemeniz gereken bir şey olmayacak. Parayı aldığınızda lütfen bana bilgi verin, kutudan temin ettiğim biraz para ile alacağım biletlerle oğlumla Nijerya'dan sizin ülkenize geleceğiz. Ben geldiğimde paranın yüzde 30'u sizin olacak, yüzde 70'ini

bana verirsiniz. Lütfen bundan kimseye bahsetmeyin, avukatınıza bile. Ancak bu şekilde bu işi yapabiliriz. Ben de sadece ablama söyledim çünkü kutuyu taşımada bize yardım etmesi gerekiyor. Sizden cesaretlendirici bir cevap almayı umuyorum. Size bu mesajı gönderdiğim eposta adresi bir arkadaşıma ait olduğundan lütfen cevabınızı (kolafashonu0@...) email adresime gönderin. Aksi durumda bir arkadaşın epostasından yazışmaya başlamak uygun olmaz. İyi günler Kola Fashonu (İnt. Kyn. 38).”

Smishing (Sms Phishing) Yöntemi

Mobil telefon kullanıcılarını hedef alan bir phishing çeşididir. Dolandırıcılık amaçlı hazırlanan sms içeriğiyle özellikle güvenlik bilinci ve farkındalığı yeterli düzeyde olmayan kullanıcıların kişisel ve bankacılık bilgileri ele geçirilmektedir (Çakır ve Doğan 2014).

Gönderilen mesaj içeriklerinde genellikle hediye kazanıldığı belirtilmektedir. İkna edici ve merak uyandırıcı ibareler kullanılarak kişilerin mesaj içeriğinde bulunan numarayı aramaları sağlanmaktadır. Bu numara herhangi bir gsm operatörüne ait olabileceği gibi çağrı merkezi numarası da olabilmektedir. Numara arandığında hediyenin gönderilebilmesi için kişisel ve kredi kartı bilgilerinin belirtilmesi istenilmektedir. Böylece kişisel ve kart bilgileri elde edilerek başka yerlerde kullanılabilmektedir (Resim 5.15).



Resim 5.15 Phishing amaçlı oluşturulmuş sms içeriği (İnt. Kyn. 39).

Smishing yönteminde mesaj içeriğinde iletişim için numara belirtilebileceği gibi url adresi de verilebilmektedir. Daha tehlikeli olan bu yöntemde belirtilen link açıldığı andan itibaren mobil cihaza kötücül yazılım yüklenmeye başlamaktadır. Bu kötücül yazılım aracılığıyla telefonda yapılan görüşmelerin dinlenmesi, ortam dinlemesi, telefona tam erişimle birlikte kişisel ve bankacılık bilgileri elde edilebilmektedir.

Vishing (Voice Phishing) Yöntemi

Vishing, ses aldatmacası kullanılarak kişilerin bankacılık ve kişisel bilgilerini ele geçirmeyi hedefleyen bir saldırı türüdür. Vishing, temelde phishing yönteminin alt kategorisinde bulunmasına rağmen saldırı boyutunun büyüklüğü ve inandırıcılığı açısından sıradan bir phishing saldırısına oranla daha çok zarar meydana getirmektedir (İnt. Kyn. 40).

Bu yöntemde, kişilere bankadan geliyormuş gibi hesap bilgilerinin güncellenmesi temalı mesaj, sesli mesaj ya da e-posta gönderilerek, mesaj içeriğinde belirtilen telefon numarasının aranması sağlanmaktadır. Telefon numarası arandığında sahte kimlik bilgileri ile kiralanmış sesli yanıt sistemi ya da çağrı merkezi cevap vermektedir. Sistemin yönlendirmesi neticesinde söylenen ya da tuşlanan bilgiler sisteme kaydedilerek kişisel ve bankacılık bilgileri elde edilmektedir (İnt. Kyn. 41).

Ülkemizde Vishing yöntemi ile benzerlik gösteren telefon ile dolandırıcılık vakaları oldukça fazladır. Kendisini kamu görevlisi (Polis, Asker, Savcı vb.) olarak tanıtarak ikna ve korku salmak suretiyle yapılan bu yöntemin sade vatandaştan tutunda üst düzey yöneticilere varıncaya kadar geniş bir yelpazede mağdur profili bulunmaktadır. Dolandırıcılar önceden elde ettikleri kişisel bilgileri kullanarak, başkaları üzerine açılmış hatlar vasıtasıyla mağdurları aramaktadırlar. İnandırıcılığı artırmak için arka fonda dinletilen telsiz sesi ile başlayan telefon görüşmesi, mağdurun düşünmesine ve çevresinden fikir almasına imkan vermemek için tüm işlemler bitinceye kadar açık kalmaktadır.

Telefon dolandırıcılığında kullanılan belli başlı kurgular;

Terör örgütü sim kartınızı kopyaladı ya da adınıza hat çıkardı kullanıyor kurgusu,
Terör örgütü banka hesabınızı ele geçirdi ve bu hesaptan teröristlere para aktarılacak kurgusu,
Yapılan operasyonun bir parçası olduğu belirtilerek daha sonra devlet tarafından ödenmek üzere operasyon için para göndermesi gerektiği kurgusu,
Hattınızdan üst düzey bir bürokrat eşi taciz edildi, başınızın belaya girmemesi için şahısların yakalanması gerektiği ve bunun içinde kontöre ihtiyaç olduğu kurgusu (İnt. Kyn. 42).

Bu kurgular üzerine yapılan görüşmeler neticesinde dolandırıcılıkta kullanılan başkaları adına açılmış hatlara kontör gönderimi yaptırılmakta ya da bazı bankalar tarafından sunulan kartsız işlem hizmetiyle ATM'ler üzerinden para transferi yaptırılarak kişiler mağdur edilmektedir. Kullanılan hatlar başkaları üzerine açıldığından ve para transferinde hesap numarası bilgisi kullanılmadığından dolandırıcılığı gerçekleştiren şahıs/şahıslara ulaşmak pek mümkün olmamaktadır.

5.1.4 Pharming (Dns Saldırısı)

Pharming (Site Trafiği Yönlendirme), "phishing" (kimlik avı) ve "farming" (çiftçilik) sözcüklerinin birleştirilmesiyle oluşturulmuş bir sözcüktür (İnt. Kyn. 43). Pharming, kullanıcının internet tarayıcısı üzerinden açmak istediği web sayfasının dışında farklı bir web sayfasına yönlendirilmesine dayanan saldırı metodudur.

Pharming'de saldırganlar IP adresinin alan adı sunucusu (DNS) tarafından çözümlenmesi aşamasına müdahale etmektedirler. DNS sunucusu, tarayıcı adres satırına girilen site ismini, girilmek istenen sitenin IP adresine yönlendiren veri tabanına sahip bilgisayar sunucusudur. Kötücül yazılımlar yardımıyla bilgisayardaki daha önce girilmiş olan internet adreslerinin listelendiği "host" datasını değiştirmek suretiyle kendi internet tarayıcısına bankasının alan adını giren kullanıcıyı, tarayıcının adres kısmına doğru adresi yazmasına rağmen yanlış adrese yönlendirme yapılmaktadır. Bu sayede kullanıcının internet bankacılığına girişte kullanmış olduğu kullanıcı adı, parola ve şifre gibi güvenlik bileşenleri dolandırıcıların eline geçmektedir (İnt. Kyn. 44).

Host dosyası Windows işletim sistemlerinde C:\Windows\System32\drivers\etc klasöründe yer almaktadır ve içeriğinde açıklamalar dışında sadece 127.0.0.1-localhost ibareli bir satır bulunmaktadır. Bunun dışında herhangi bir satır eklentisi bulunması durumunda, bu satırın kaynağı araştırılarak yönlendirme olup olmadığı bulunabilmektedir.

5.1.5 Man In The Middle Attact (Ortadaki Adam Saldırısı)

Kötücül yazılımlar vasıtasıyla iki sistem arasında yapılan bağlantının arasına girilmek suretiyle her iki tarafa da sanki karşıdaki gibi davranılarak ya da sistemlerden birini devre dışı bırakarak iletilen bilgilerin ele geçirilmesi yöntemidir (Gürçam 2008).

Dolandırıcılar bu yöntemle, "hedef aldıkları kişiler ile onların bağlanmak istedikleri yasal internet sitelerinin yer aldığı sunucular arasına girerek kullanıcıların yasal sitelere ilettikleri verileri ele geçirmekte ve çıkar amaçlı olarak kullanmaktadırlar (Ünver ve Mirzaoğlu 2011)."

5.1.6 Key Logger

Kullanıcının klavye üzerinden girmiş olduğu bilgileri yakalayarak kaydedip karşı tarafa gönderen casus yazılımlardır. Klavye tuşuna basılmak sureti ile girilen tüm şifre ve parolalar metin belgesine kaydedilerek karşı tarafa gönderilmektedir (Eralp 2012).

Özellikle bankacılık sistemine girişte kullanılan güvenlik parametrelerinin ya da alışveriş sonrasında ödeme aşamasında sisteme girilen kredi kartı bilgilerinin elde edilmesi için kullanılan bir yöntemdir.

Key logger, yazılım ve donanım temelli olmak üzere iki çeşittir. Yazılım temelli key logger sistemde gizli olarak çalışmaktadır, klavye ile işletim sistemi arasına girerek basılan tüm tuşları kaydeden programdır. Donanım temelli key logger ise klavye ile klavye portu arasına takılan fiziksel donanım parçasıdır, klavyeden basılan tuşlar bu donanımın hafızasına kaydedilmektedir. Donanım, her nekadar antivirüs ve anti key

logger programlarına yakalanmasada, donanımın sisteme takılabilmesi ve gizliliğinin sağlanabilmesi bu yöntemin riskli tarafıdır (Burlu 2013).

5.1.7 Screen Logger

Screen logger, key logger gibi aynı mantıkla çalışmaktadır. Kullanıcının ekran üzerinde yapmış olduğu hareketlerin tamamını ya da fare ile tıklanan noktalar merkez alınarak ekranın bir kısmını fotoğraf veya video şeklinde kaydederek karşı tarafa gönderen casus yazılımlardır (İnt. Kyn. 45).

Bu program, kullanıcının bilgisayarı açtıktan kapatıncaya kadar geçen zaman aralığında ekranda yapmış olduğu tüm hareketleri örneğin açmış olduğu tüm klasör ve dosyaları, girmiş olduğu internet sitelerini ya da ekrana yazmış olduğu tüm bilgileri kaydederek karşı tarafa göndermektedir. Kısacası kullanıcının tüm ekran hareketlerini izleyerek kaydetmektedir.

Legal manada şirketler iş verimliliğini artırma adına çalışanlarının bilgisayarda iş dışında oyun, sohbet, sosyal medya gibi başka şeylerle ilgilenmemelerini sağlamak için bu tarz programları çalışanlarına bildirerek kullanmaktadırlar. Yine ebeveynler çocuklarının bilgisayarda nelerle uğraştığını takip etmek maksatlı bu tarz programları kullanmaktadırlar.

5.2 Fiziksel Yöntemlerle Banka veya Kredi Kartı Bilgilerinin Ele Geçirilmesi

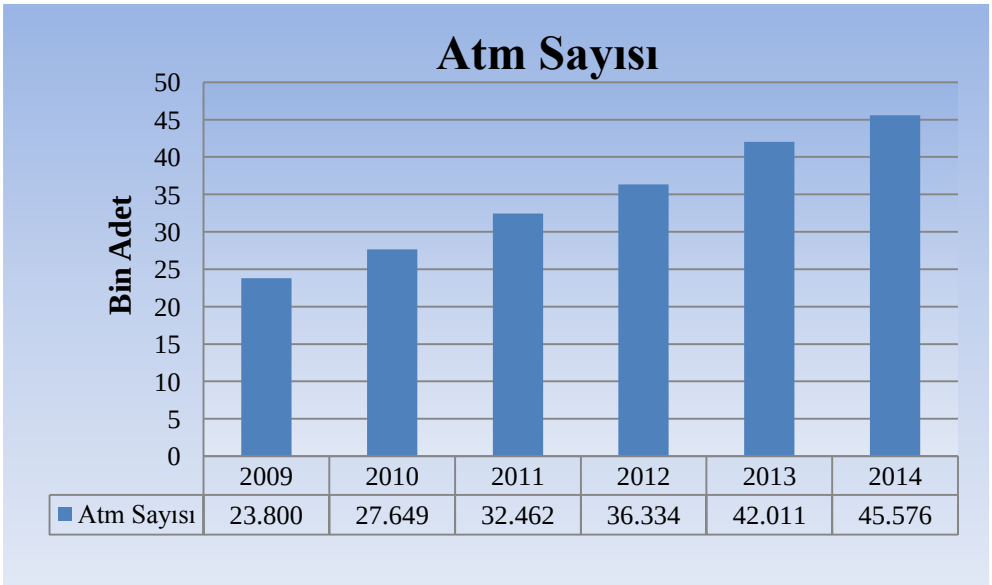
5.2.1 Banka veya Kredi Kartı Bilgilerinin Kopyalanması

Banka veya kredi kartı bilgileri sanal olarak bilgisayar ve internet dışında fiziksel olarak ATM ve POS cihazları aracılığıyla da ele geçirilebilmektedir. Maniple edilmiş ATM ve POS cihazlarından müşteri işlem yaptığı sırada kartın manyetik bilgileri kopyalanabilmekte ve bu bilgiler daha sonra fiziksel olarak boş kartlara basılmak suretiyle ödeme aracı olarak ya da nakit para çekiminde kullanılabildiği gibi bunun yanı sıra internet üzerinden veya MOTO (Mail order/Telephone order) yöntemiyle yapılan ödemelerde kullanılabilmektedir.

5.2.1.1 ATM Üzerinden Kopyalama

ATM, İngilizce Automated Teller Machine kelimelerinin kısaltmasından oluşmakta, otomatik vezne makinesi anlamına gelmektedir.Ticari bankalar tarafından kullanılmakta olan bir dağıtım kanalıdır. Önceleri sadece para ödeme ve ekstre basma gibi hizmetler sunabilirken, günümüzde para yatırma, eft yapma, fatura ödeme ve yatırım işlemleri gibi birçok konuda müşterilere hizmet vermektedir. ATM cihazı Türkiye'ye ilk defa 1982 yılında İş Bankası tarafından, Bankamatik ismiyle kurulmuştur (İnt. Kyn. 46).

Şekil 5.1'de gösterilen Bankalararası Kart Merkezinin yayınlamış olduğu dönemsel bilgiler doğrultusunda ülkemizde, 2009 yılında 23,800 olan ATM sayısı 2014 yılı sonu itibarıyla toplam 45,576'ya ulaşmıştır (İnt. Kyn. 9). Söz konusu ATM'lerin % 49'u şubede (on-site), % 51'i ise şube dışında (off-site) bulunmaktadır (BKM 2014).



Şekil 5.1 2009-2014 yılları arasında ATM sayısının gelişimi

Banka veya kredi kartları, bankaların müşterilerine nakit para olmaksızın POS cihazı üzerinden alışveriş yapma ya da ATM cihazı üzerinden bankacılık işlemleri gerçekleştirme imkânı sunmaktadır. Bu kartların yapısında, içerisinde kart bilgilerinin yeraldığı manyetik şerit bulunmaktadır.

Bankalar, 2007 yılında Chip & Pin sloganıyla müşterilerine daha güvenlikli kart imkânı sunmaya başlamışlardır. “Chip & Pin; kredi kartının kopyalanma, çalınma ve kaybolma risklerini azaltan bir ödeme yöntemidir. Kart bilgilerinin, kredi kartının manyetik bandının yanı sıra kart üzerinde bulunan ve güvenlik unsurları artırılmış bir mikroçipe de yazıldığı kart tipidir. Bankalar tarafından kartların ATM ya da POS cihazlarında kullanılabilmesi için kart sahiplerine PIN kodu verilir (Kaya 2009).”

Bu kadar üst seviyede alınan güvenlik önlemlerine rağmen kart bilgileri değişik yöntemlerle kopyalanarak elde edilebilmektedir. Bu yöntemlerden birisi de ATM üzerinden kart bilgilerinin kopyalanması yöntemidir. Müşteri işlem yapmak üzere kartını ATM cihazına taktığı esnada kart haznesinin önüne yerleştirilmiş olan ve papağan olarak tabir edilen skimmer (manyetik şerit kopyalama) cihazı aracılığıyla kart bilgisi kopyalanmaktadır (Resim 5.16 ve resim 5.17).

Resim 5.16 ATM üzerine takılı kart kopyalama cihazı (İnt. Kyn. 47).

Resim 5.17 ATM üzerine takılı kart kopyalama cihazı (İnt. Kyn. 48).

Bununla birlikte ATM üzerine özellikle de sonradan takılan aydınlatma lambası içerisine gizlenmiş micro kamera ya da şifre girilen pin pad (tuş takımı) üzerine yapıştırılmış ikinci bir pin pad aracılığıyla da karta ait şifre bilgisi elde edilebilmektedir. Bu bilgiler daha sonra boş kartlara yazdırılarak alışverişlerde kullanılabilmekte ya da nakit para çekilebilmektedir. (Resim 5.18 ve resim 5.19).

Resim 5.18 ATM üzerine takılı pin pad (tuş takımı) (İnt. Kyn. 49).

Resim 5.19 ATM üzerine takılı pin pad (tuş takımı) (İnt. Kyn. 50).

Dolandırıcılar, kurulan düzeneklerin fark edilerek güvenlik güçlerince el konulması durumlarını da ön görerek kurmuş oldukları düzeneklerde kablosuz iletişim alt yapılarını da kullanmaya başlamışlardır. Düzenek bir şekilde fark edilerek sökülmüş olsa bile o âna kadar yapılan işlemlerden elde edilen kart ve şifre bilgileri kablosuz iletişim teknolojileri sayesinde anlık olarak uzak sistemlere gönderilebilmektedir.

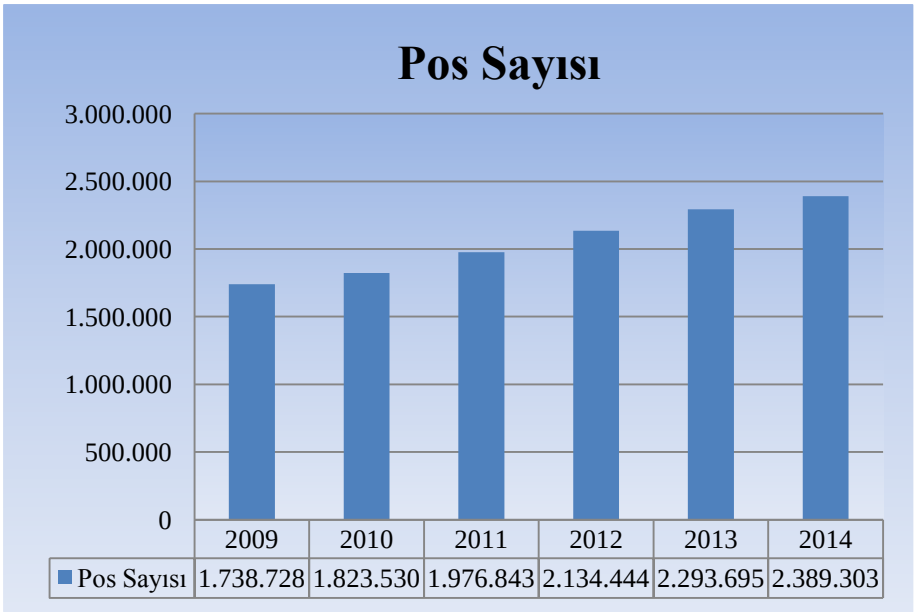
5.2.1.2 POS Cihazı Üzerinden Kopyalama

POS, İngilizce Point Of Sale kelimelerinin kısaltmasıdır. Satış noktası terminali anlamına gelmektedir. POS cihazı, banka ve kredi kartlarının işlem yapabilmesi için okutulduğu cihazdır. Kredi kartı üreten her bankanın müşterilerine kolaylık olması amacıyla üye işyerleri aracılığıyla, POS cihazı ile hizmet vermesi gerekmektedir (İnt. Kyn. 51).

POS cihazından kart geçirilerek ya da takılarak okutulduğunda, kredi kartında limit olup olmadığı ya da bankamatik kartı hesabının söz konusu alışverişi gerçekleştirebilmek için müsait olup olmadığı ile ilgili merkezden gerekli sorgulamayı yapmaktadır. POS üzerinde, kartın manyetik bandının ya da çipinin üzerinde bulunan bilgileri okuyan tarayıcı, bilgi girişinin sağlandığı tuş takımı ve bilgilerin izlendiği dijital ekran

bulunmaktadır. POS üzerinden genel olarak satış, taksitli satış, puanlı satış, iptal, iade ve gün sonu işlemleri gerçekleştirilebilmektedir.

Şekil 5.2'de gösterilen Bankalararası Kart Merkezinin yayınlamış olduğu dönemsel bilgiler doğrultusunda ülkemizde, 2009 yılında 1 738 728 olan POS cihazı sayısı 2014 yılı sonu itibarıyla toplam 2 389 303'e ulaşmıştır (İnt. Kyn. 9).



Şekil 5.2 2009-2014 yılları arasında POS sayısının gelişimi

Ülkemizde ticaret sektöründe, kullanım alanına göre Dial-up POS, Adsl POS, Mobil (Kablosuz) POS, Sanal POS (Web POS), Ortak POS, Dcc POS / Döviz POS ve Temassız POS olmak üzere yedi farklı POS çeşidi kullanılmaktadır (İnt. Kyn. 52).

Genellikle alışveriş merkezi, lokanta, petrol istasyonu, otel ve eğlence mekânı gibi yerlerde çalışan dolandırıcılık şebekesi üyeleri, kendilerine ödeme maksadıyla verilen kredi kartlarını POS cihazıyla birlikte el çabukluğuyla skimmer cihazından da geçirerek kartın manyetik şeridini kopyalamaktadır. Şifreyi de POS cihazına girilmesi esnasında bakıp ezberinde tutarak ya da üzerinde bulunan gizli kamera yardımıyla elde etmektedir. Bu bilgiler daha sonra boş kartlara yazdırılarak alışverişlerde kullanılabilmekte ya da nakit para çekilebilmektedir. Bu eyleme yaz aylarında ve turizm bölgelerinde daha sık rastlanmaktadır (Eralp 2012).

Bununla birlikte farklı bir yöntemde, maniple edilerek POS cihazına tıpa tıp benzetilen ve üzerinde banka logoları da bulunan skimmer cihazı aracılığıyla kart kopyalamadır. Ödeme esnasında kart, maniple edilmiş POS cihazından geçirilerek müşteriden şifreyi girmesi istenir. Şifre girildikten kısa bir süre sonra işlem reddedildi denilerek cihazdan sahte slip yazdırılır. Bunun üzerine işlem gerçek POS cihazından tekrar yapılarak işlem tamamlanır. Bu şekilde, ilk etapta yapılan işlem esnasında kredi kartı ve şifresi kopyalanmaktadır (Resim 5.20).

Resim 5.20 Maniple edilmiş POS cihazı (İnt. Kyn. 53).

5.2.2 Kart Kopyalamada Kullanılan Cihazlar

5.2.2.1 Reader & Encoder (Okuyucu / Kodlayıcı) Cihazı

Kart içeriğinde gömülü bulunan manyetik şerit bilgilerini okuyarak bağlantılı olduğu bilgisayar sistemine aktaran ve bilgisayar üzerinde bulunan manyetik şerit bilgilerini boş kartların manyetik şeritlerine kodlayan cihazdır. Teknolojik gelişmelerle birlikte boyutları hayli küçülmüştür (Resim 5.21 ve resim 5.22).

Resim 5.21 Msr 606 Reader & Encoder cihazı (İnt. Kyn. 54).

Resim 5.22 Msr mini dx3 Reader & Encoder cihazı (İnt. Kyn. 55).

5.2.2.2 Embosser (Kabartma Baskı) Cihazı

Boş plastik kartların üzerine istenilen bilgileri kabartma olarak yazan cihazdır. Dolandırıcılık yapılarak elde edilen kart bilgileri encoder cihazı ile boş kartlara kodlandıktan sonra kartın inandırıcılığını artırmak adına kart bilgileri normal kartlarda olduğu gibi kabartma olarak plastik kartlara basılmaktadır (Resim 5.23).

Resim 5.23 Embosser (Kabartma baskı) cihazı (İnt. Kyn. 56).

5.2.2.3 Tipper (Renklendirici) Cihazı

Boş plastik kartların üzerini istenilen şekilde renklendirmede kullanılan cihazdır. Üzeri kabartma yapılarak inandırıcılığı artırılan sahte kart son aşamada renklendirilerek piyasada kullanılabilir hale getirilmektedir (Resim 5.24).

Resim 5.24 Tipper (Renklendirici) Cihazı (İnt. Kyn. 57).

5.2.3 ATM' ye Kart Sıkıştırma

ATM'nin kart okuyucu bölmesine kâğıt, yapıştırıcı, röntgen filmi gibi yabancı maddeler yerleştirilerek müşteriye ait kart, kart okuyucu bölmeye sıkıştırılmakta böylelikle ATM herhangi bir işlem yapılamaz hale getirilmektedir (Eralp 2012). Bu yöntem bilinen en basit kart dolandırıcılığı yöntemidir ve "Lebanese loop" tekniği olarak da bilinmektedir. Bu aşamadan sonra kartın şifresini öğrenebilmek için birkaç yöntem bulunmaktadır.

İlk yöntemde, kartın sıkışması esnasında müşterinin arkasında bulunan dolandırıcılık çetesi üyesi şifrenin girilme anını gözetleyerek şifreyi öğrenmektedir, bu yöntem shoulder surfing (Omuz sörfü) olarak da bilinmektedir.
İkinci yöntemde, çevreden yardıma gelen dolandırıcılık çete üyesi kartın sıkıştığı yerden çıkabilmesi için müşteriye şifresini tekrar girmesini söylemekte, şifrenin girilme anını gözetleyerek de kartın şifresini öğrenmektedir.

Üçüncü yöntemde, çete üyesi müşteriye kartını iptal ettirmesi için ATM üzerine sonradan yazılmış sahte müşteri hizmetleri numarasını aramasını söylemekte, telefonun karşı tarafında bulunan diğer dolandırıcılık çete üyesi de konuşma esnasında kart şifresini öğrenmektedir.
Dördüncü yöntemde, çete üyesi müşteriye kartını iptal ettirmesi için ATM üzerine sonradan takılmış kablosuz telefon ile müşteri hizmetlerini aramasını söylemekte, telefonun karşı tarafında bulunan diğer dolandırıcılık çete üyesi de konuşma esnasında kart şifresini öğrenmektedir.

Kart şifresi öğrenildikten sonra müşteri ATM'den ayrılır ayrılmaz çete üyesi ATM'ye gelmekte, cımbız ya da benzeri alet yardımı ile kartı okuyucu bölmeden çıkarmaktadır. Öğrenmiş olduğu şifreyle gerek karttan nakit para çekimi yapmakta gerekse de kartı alışverişte kullanabilmektedir (Eralp 2012).

ATM üzerinden yapılan farklı bir sıkıştırma yöntemiyle de ATM'nin para verdiği bölmeye yapıştırıcı özellikli yabancı maddeler yerleştirilerek, bölmenin tamamen açılmaması ya da paranın bölmeye yapışarak sıkışması sağlanmaktadır. ATM'de sorun olduğunu zanneden müşteri ATM'den ayrıldıktan sonra dolandırıcılık çete üyesi gelerek sıkışan bölmeden parayı almaktadır.

5.3 Sosyal Medya Hesaplarının Ele Geçirilmesi

Yukarıda belirtmiş olduğumuz dolandırıcılık yöntemlerinde, kötü niyetli kişiler tarafından kişisel ve bankacılık bilgileri ya da banka veya kredi kartı bilgilerinin ele geçirilmesi esas hedef olarak belirlenip bu yönde kurguların yapıldığı görülmektedir. Sosyal medya hesaplarının ele geçirilmesi yönteminde durum farklıdır. Sosyal medya, iletişim ve eğlence kültürü olarak günümüz insanının vazgeçilmez bir parçası olma özelliğini halen devam ettirmektedir. Ülkemizde neredeyse her bireyin bir sosyal paylaşım sitesinde hesabı bulunmaktadır. Yine bu hesapların kontak listelerinde, görüşülsün ya da görüşülmesin birçok hesap sahibi eklenmiş şekilde bulunmaktadır. Bu kadar çok sosyal medya hesabının bulunması dolandırıcılara yeni yöntemler keşfettirmiştir.

Açıklayacağımız bu dolandırıcılık yönteminde öncelikle sosyal medya hesabının ele geçirilmiş olması gerekmektedir. Bu eylem için birçok teknik ve sosyal mühendislik yöntemi bulunmaktadır. Konumuzu ilgilendiren kısım bu aşamadan sonrasıdır. Sosyal paylaşım hesabını ele geçiren bilgisayar korsanı, daha önceki yazışma geçmişini inceleyerek kontak listesinde bulunan kişilerle bu yönde gerçek hesap sahibiymiş gibi yazışmaya başlamaktadır. Bu aşamadan sonra birçok kurguyla karşı taraf dolandırılabilmektedir. Bu yöntemlere bakacak olursak; birincisi, acil kontöre ihtiyacı olduğunu belirterek kontör kart numarası istemek (Dülger 2013). Diğer bir yöntemde fail, yazışma esnasında telefon numarasını kaybettiğini belirterek numarayı istemekte ve yardıma muhtaç ailelere yardım kampanyası olduğunu, yardım için telefonuna gelen mesaja EVET ya da ONAY yazarak cevap vermesi durumunda kampanyaya katılabileceğine ikna ederek, yine benzer bir yöntemde fail, yazışma esnasında hediye çeki dağıttığını ve çeki kazanabilmesi için telefonuna gelen mesaja EVET ya da ONAY yazarak cevap vermesi halinde çeki kazanabileceğine ikna ederek dolandırıcılık gerçekleştirilmektedir (İnt. Kyn. 71).

Bu tür dolandırıcılık konularının ana temasına baktığımızda, her insanın fıtratında bulunan muhtaçlara yardım etme duygusu ve yine birçok insanda bulunabilen karşılıksız bir şeyler kazanma isteğinin kullanılarak suistimal edildiği görülmektedir. Güvenilir bir arkadaş tarafından gelen bu iki istek karşısında, karşı koymak oldukça zordur.

Bu dolandırıcılık yönteminde önceki bölümlerde incelemiş olduğumuz mobil ödeme sistemi araç olarak kullanılmaktadır. Dolandırıcı konuşma esnasında elde etmiş olduğu telefon numarası ile internet üzerinden yapmış olduğu alışverişin ödemesini yapmakta ya da internet üzerinden oyun kredisi almaktadır. Ödeme ekranına mağdurdan elde edilen telefon numarası girilerek ödeme işlemi başlatılmakta ve mağdur telefonuna gelen mesaja EVET ya da ONAY yazarak cevap vermesi durumunda ödeme işlemi gerçekleşmektedir. Bu durumda ödeme tutarı mağdurun cep telefonu faturasına yansımaktadır. Oysa ki mağdur kendisine gelen ödeme mesajını tam olarak okuyup anlamış olsa bu mesaja kesinlikle onay vermeyecektir. Çünkü mesaj içeriğinde ne ile alakalı ödeme yaptığı ayrıntılı bir şekilde belirtilmektedir. İstek güvenli bir arkadaştan

geldiği için mesaj içeriği okunmamakta ya da okunup karşı tarafa itiraz edilmesi durumunda ise "bana güvenmiyor musun?" ya da "ben kefilim" gibi cümlelerle mağdur ikna edilmektedir.

5.4 İnternet Bankacılığında Kullanılan Tek Kullanımlık Sms Şifresinin Ele Geçirilmesi

İnternet bankacılığı, bankaların müşterilerine şubeleri aracılığıyla sunmuş oldukları hizmetleri, web siteleri üzerinden sağlayan sistemlerdir. Zaman sınırlaması olmaksızın internet bağlantısının bulunduğu tüm ortamlardan bankanın sistemine bağlantı yapılarak bankacılık işlemleri gerçekleştirilebilmektedir.

Ülkemizde, teknolojik gelişmeler doğrultusunda ilk internet şubesi 1998 yılında Türkiye İş Bankası tarafından hizmete sunulmuştur. Ardından Garanti Bankası, Osmanlı Bankası ve Pamukbank da aynı yıl içerisinde internet üzerinden bankacılık hizmeti sunmaya başlamıştır (Megep 2007).

"Hareketli (mobil) bankacılık, bankacılık işlemlerinin bir ağ üzerinden bağlanan hareketli (mobil) cihazlarla yapılabilmesini ifade etmektedir (Eralp 2012)." Zaman ve mekân sınırlaması olmaksızın mobil cihaza takılı bulunan gsm hattının internet alt yapısı sayesinde gerek web tarayıcılar gerekse de bankanın mobil uygulaması aracılığıyla bankacılık işlemleri gerçekleştirilebilmektedir.

Ülkemizde internet ve mobil bankacılığa giriş işlemlerinde genellikle kullanıcı adı/ müşteri numarası, şifre, parola ve tek kullanımlık şifreden oluşan güvenlik parametreleri kullanılmaktadır. 14 Eylül 2007 tarih ve 26643 sayılı Resmi Gazete'de yayımlanan Bankacılık Düzenleme ve Denetleme Kurumunun, bankalarda bilgi sistemleri yönetiminde esas alınacak ilkelere ilişkin tebliğinde, TKŞ (tek kullanımlık şifre) hizmetleri; tek kullanımlık SMS şifreleri, TKŞ üreten cihazlar (token), TKŞ üreten yüklenebilir programlar, Elektronik İmza çözümleri ve Biyometrik tanıma çözümleri olarak örneklendirilmiştir. Tebliğ gereği tek kullanımlık şifre kullanımı 1 Ocak 2010 tarihi itibarıyla yasal olarak zorunlu hale getirilmiştir.

Tek kullanımlık şifrenin zorunlu olmasıyla birlikte internet bankacılığı daha da güvenli hale gelmiştir. Dolandırıcılar da bu ciddi güvenlik doğrulamasını aşmak için yeni yöntemler arayışına girmişlerdir. Günümüzde özellikle internet bankacılığı ve mobil bankacılıkta müşteri doğrulamasında kullanılan tek kullanımlık SMS şifresi (SMS one time password-OTP) ile kredi kartı işlemlerinde kullanılan 3D Secure şifresini elde etmek amacıyla telefon ve sim kart odaklı dolandırıcılık yöntemleri kullanılmaktadır.

Bu durumda çoğunlukla iki farklı yöntem karşımıza çıkmaktadır. İlk yöntemde, gsm bayisine sim kartın kaybedildiği gerekçesiyle sahte evrak ibraz ederek yeni sim kartın çıkarılmasıdır (Eralp 2012). Böylelikle doğrulama şifresinin yeni sim karta gelmesi sağlanmaktadır. İkinci yöntemde, telefona bulaşan virüs türevli kötücül yazılımlar aracılığıyla, telefona gelen internet bankacılığı veya 3D secure şifresi virüs tarafından anında dolandırıcıya da iletilmektedir.

6. BİLİŞİM YOLUYLA DOLANDIRICILIKTAN KORUNMA YÖNTEMLERİ

6.1 Genel Güvenlik Önlemleri

Teknolojik gelişmeler insan hayatını çevreleyen her alana yenilikler getirerek olanaklarını artırmış, insan yaşamına hizmet etme noktasında büyük kolaylıklar sağlamıştır. Yine bu gelişen teknoloji kötü niyetli insanların eline geçtiğinde çok tehlikeli bir silah olarak insanın sosyal ve ekonomik yaşamını tehdit eder hale gelebilmektedir.

Bu bağlamda teknolojinin getirmiş olduğu nimetlerden faydalanırken mağdur olmamak için yapılması gereken en etkili davranış bilinçli ve bilgili olmaktır (İnt. Kyn. 66). Bilinç, insanın çevresinde olup bitenlerin farkında olmasıdır. İşlemleri gerçekleştirken bilinçli ve bilgili olarak hareket etmenin yanı sıra uyanık olmak da gerekmektedir.

Bankacılık ve internet üzerinden gerçekleştirilen işlemlerin güvenliği, geçilen her işlem basamağının sorgulanarak ve sonucunun farkında olarak gerçekleştirilmesi ile sağlanabilir. Bu bilincin sağlanması adına kamu ve özel sektör kuruluşları bilgilendirme programları, afişler ve kamu spotu gibi araçlarla halkta farkındalık oluşturmaya çalışmaktadırlar. Bu bilinç ve farkındalığın kazanılması sayesinde çoğu mağduriyetler baştan engellenebilmektedir.

Bilinçli olmak dışında genel olarak kişisel bilgilerimizi internet üzerinde herhangi bir platformda paylaşmamamız, bankacılık ve internet alışveriş işlemlerimizi bilmediğimiz bilgisayarlar (internetcafe vb.) üzerinden gerçekleştirmememiz, kartlarımızı fiziksel ve sanal olarak güvenliğinden emin olmadığımız yerlerde kullanmamamız genel olarak alınabilecek basit tedbirler arasında yer almaktadır.

6.2 Bankaların Alması Gereken Önlemler

ATM üzerinden gerçekleştirilen dolandırıcılık olaylarında müşterilerin bilinçli olması dışında bankalara da büyük görevler düşmektedir. 14 Eylül 2007 tarih ve 26643 sayılı

Resmi Gazete'de yayımlanan Bankacılık Düzenleme ve Denetleme Kurumunun, bankalarda bilgi sistemleri yönetiminde esas alınacak ilkelere ilişkin tebliğin 32. maddesinde bankalara ATM güvenliği konusunda 10 farklı sorumluluk getirmiştir.

"MADDE 32 – (1) Banka, ATM cihazlarına ilişkin hırsızlık, sahtekârlık, fiziksel saldırı gibi tehditlere ilişkin riskleri minimize edici önlemleri tesis eder ve ATM cihazlarının güvenli kullanımı hususunda müşterilerinde farkındalık yaratır.

(2) ATM cihazları üzerinde ön tanımlı olarak gelen her türlü parola/değişken parola, ATM cihazının bu ön tanımlı parolaları/değişken parolaları bilen kötü niyetli kişiler tarafından yönetilmesini engellemek amacıyla, kolaylıkla tahmin edilemeyecek şekilde değiştirilir.

(3) ATM cihazları üzerine, zararlı içerikli programların kötü niyetli kişilerce yüklenmesini ve yetkisiz erişimi engelleyecek gerekli tedbirler alınmalı, cihaza yetkisiz kişilerin herhangi bir şekilde başka bir elektronik cihaz bağlamasını sağlayacak bütün giriş noktaları erişime kapatılmalıdır. ATM'ler üzerine, güvenlik açıklıklarını gidermek amacıyla otomatik olarak veya düzenli periyotlar ile gerekli güncellemeler ve yamalar yüklenir. ATM cihazı ile banka arasındaki ağ bağlantısına yetkisiz olarak diğer cihazların bağlanmasını engelleyecek ek güvenlik tedbirleri uygulanır.

(4) ATM cihazları üzerinden gerçekleştirilen işlemler için kullanılan iletişim ağı veri güvenliği, gizliliği ve bütünlüğünü sağlayacak özellikte olmalıdır. Müşterilerin girdiği PIN bilgileri ve gerçekleştirilecek işlemlere ilişkin bilgiler cihaz içinde ve cihaz dışındaki ATM ağı boyunca şifrelenmiş bir şekilde iletilmelidir.

(5) 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 PIN bilgisi gibi bileşenler, "sahip olduğu" unsur olarak ATM kartı gibi bileşenler kullanılabilir. Bileşenler tamamen müşterinin şahsına özgü olmalı ve bunlar sunulmadan kimlik doğrulama gerçekleştirilememeli, hizmetlere erişim sağlanamamalıdır.

(6) ATM cihazlarının servis sürekliğinin sağlanması ve sahtekârlık, fiziksel saldırı gibi maruz kalabilecekleri risklerin erken tespiti adına, Banka tarafından ATM cihazları için uzaktan yönetim ve takip sistemleri kurulur.

(7) ATM operatörleri ve teknisyenleri, ATM cihazlarına ilişkin güncel bütün sahtekârlık yöntemleri konusunda eğitilir ve bu gibi personelin ATM cihazlarını düzenli olarak kontrol etmeleri sağlanır. ATM cihazları özellikle, üzerlerine yabancı aparatlar veya başka elektronik cihazlar (kart kopyalama cihazları, sahte klavye, kamera gibi) yerleştirilmiş olma ihtimallerine karşı, operatörler tarafından düzenli periyotlarla dikkatle incelenmelidir.

(8) ATM'e ilişkin mutabakatlar, yeterli sıklıkta ve görevler ayrılığı prensibine uygun olarak en az iki kişi tarafından gerçekleştirilir.

(9) Banka, müşterilerinin ATM hizmetlerinden güvenli bir şekilde faydalanmasını sağlamak amacıyla, ATM güvenliği ve güncel sahtekârlık yöntemlerinden korunma hususunda müşterilerini bilgilendirir ve bu konu hakkında müşterilerinde farkındalık oluşmasını sağlar.

(10) Banka, ATM cihazlarının bulunduğu yerlere güvenlik kamerası koyar, ancak bu güvenlik kamerası, müşterinin klavye hareketlerini göremeyecek biçimde konumlandırılır. Güvenlik kamerası kayıtları en az iki ay süreyle saklanır ve kamera teçhizatları çalıştıklarına dair düzenli olarak kontrol edilir. Görüntüleme alanı bakımından ATM'i de kapsayan ve bu fıkradaki koşulları karşılayan bir güvenlik kamerası altyapısının varlığı durumunda ATM'e özel ayrıca bir güvenlik kamerası kurulmasına gerek yoktur. Ayrıca kamu güvenlik ve istihbarat kurumlarının faaliyet bölgesinde bulunan ATM'ler için güvenlik kamerası kurulma şartı, ilgili kamu güvenlik ve istihbarat kurumlarından izin alınabilmesi koşuluyla yerine getirilir."

Bu önlemlerin yanı sıra;

Bankalar, ATM'lerin güvenliğini sağlamak için öncelikle ATM üzerine takılacak sahte ön yüz, sahte klavye, kart kopyalama aparatı, para giriş çıkış noktalarına yabancı madde, kablolu/kablosuz kamera benzeri yabancı maddelerin ATM üzerine takılmasını ve mevcut ATM ekipmanlarının ATM üzerinden sökülmesini engelleyici algılama sistemleri kurarak gerek ATM üzerinden sesli ikaz, gerekse de sistem üzerinden ilgili birimlere bilgi verilmesi sağlanmalıdır. Böyle durumlarda ATM'nin kendisini otomatik olarak kapatması sağlanmalı ve gerekli güvenlik kontrolleri yapıldıktan sonra yetkililerce işleme açılmalıdır.

ATM çevresi iyi aydınlatılmalı ve ATM üzerinde bulunan kameralar yüksek çözünürlükte kayıt yapma özelliğine sahip olmalıdır. Kameralar, ATM üzerinde işlem yapan şahsın yüzünü net gösterecek şekilde konumlanmalı bunun yanı sıra ATM önünde bekleyenleri de gösteren ayrı bir kamera bulunmalıdır.

ATM'lerin önünde çizgilerle belirlenmiş kişisel mahremiyet alanı oluşturulmalı ve omuz sörfü gibi sosyal mühendislik yöntemleri ile şifrenin ve yapılan işlemlerin yabancı kişiler tarafından görülmesi engellenmelidir. Mahremiyet alanının varlığı ve önemi ATM yakınına asılacak bilgilendirme ilanları ile müşterilere gösterilerek farkındalık oluşturulmalıdır.

6.3 İnternet Kullanıcılarının/Banka Müşterilerinin Alması Gereken Önlemler

6.3.1 SSL (Secure Socket Layer) Güvenlikli Siteler

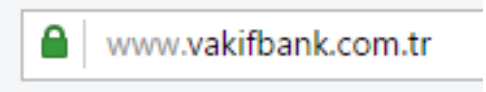
SSL (Secure Socket Layer /güvenli yuva katmanı) güvenlik protokolü, Netscape firması tarafından 1994 yılında kullanıma sunulmuştur. Bu protokol, internet üzerinden şifrelenmiş güvenli veri iletişimini sağlamaktadır. SSL teknolojisi sayesinde kullanmakta olduğumuz internet tarayıcılar (Explorer, Chrome, Firefox vb.) ile bağlanılan sunucu arasındaki veri trafiği şifrelenmiş şekilde yapılmaktadır. Bu sayede araya girerek veri trafiğini elde etmek isteyen üçüncü kişilerin bu bilgileri elde etmesi imkânsız hale gelmektedir (Çakar 2013).

SSL sertifikaları, kullanıcıların dolandırıcılık amaçlı oluşturulmuş siteleri güvenli sitelerden daha kolay ayırt etmelerini sağlamak için kullanılmaktadır. "SSL gönderilen bilginin kesinlikle ve sadece doğru adreste deşifre edilebilmesini sağlar. Bilgi gönderilmeden önce otomatik olarak şifrelenir ve sadece doğru alıcı tarafından deşifre edilebilir. Her iki tarafta da doğrulama yapılarak işlemin ve bilginin gizliliği ve bütünlüğü korunur (İnt. Kyn. 58)."

Kullanmış olduğumuz internet sitelerinde, SSL güvenlik sertifikası olup olmadığını iki şekilde anlayabiliriz. İlkinde, tarayıcı adres satırında sitenin adı http:// yerine https:// ile

başlıyorsa sitenin geçerli bir güvenlik sertifikası bulunduğunu ve güvenli olduğunu göstermektedir. İkincisinde, tarayıcı adres satırının sol baş tarafında ya da tarayıcının alt kısmında kapalı vaziyette bulunan kilit işareti sitenin güvenli olduğunu göstermektedir (Resim 6.1 ve resim 6.2) (Gürçam 2008).

Resim 6.1 Ssl güvenlik sertifikası bulunan site görünümü (İnt. Kyn. 59)



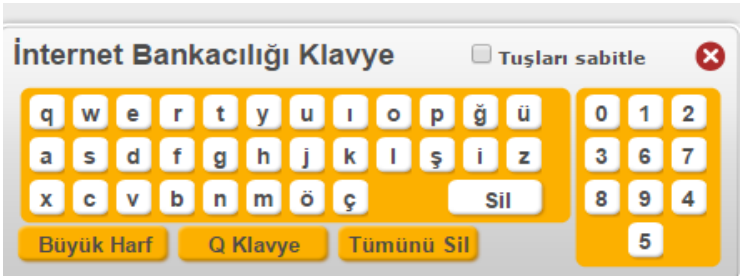
Resim 6.2 Ssl güvenlik sertifikası bulunan site görünümü (İnt. Kyn. 60)

Kullanıcı adı, şifre ve parola gibi güvenlik parametreleri giriş işlemlerinin yapıldığı internet bankacılığı giriş sayfalarında ya da alışveriş işlemlerinde kart bilgilerinin girildiği ödeme sayfalarında https:// ya da kapalı kilit simgesinin bulunup bulunmadığı kesinlikle kontrol edilmelidir. Olmadığı durumlarda kesinlikle işlem yapılmamalıdır. Bu tür hayli basit bir kontrolle dolandırıcılıklar baştan önlenmiş olacaktır.

6.3.2 Sanal Klavye (Ekran Klavyesi)

Bilgisayarın fiziksel klavyesine alternatif olarak yüksek güvenlik gerektiren bilgilerin mouse tıklamasıyla girişini sağlamak amacıyla geliştirilmiş programdır. Klavyede yer alan bütün tuşların, genelde klavyede bulunan yerlerine göre dizildiği ekranı bulunmaktadır. Program açılarak, bilgi girişi için giriş yapılacak kısma mouse ile tıklanır ve sanal klavye ekranından istenilen tuşa tıklanılarak veri girişi yapılmaktadır (Canbek ve Sağıroğlu 2006).

Sanal klavye, klavyede basılan tuşları izleyerek kaydeden key logger tarzı kötücül yazılımların, yüksek güvenlik gerektiren şifreleri çalmasını engellemeye yönelik ek güvenlik önlemi olarak kullanılmaktadır (Resim 6.3).



Resim 6.3 Sanal klavye görünümü (İnt. Kyn. 61).

Genellikle bütün bankaların internet bankacılığı giriş ekranlarında sanal klavye otomatik olarak açılmakta ya da butona tıklayarak başlatılabilmektedir. Yine alışveriş sitelerinin ödeme ekranlarında kart bilgilerinin girişi kesinlikle sanal klavye ile yapılmalıdır. Sanal klavyenin site içerisinde açılmadığı ya da bulunmadığı durumlarda kullanılan işletim sisteminin sanal klavye programı çalıştırılarak bu program aracılığıyla bilgi girişi sağlanmalıdır.

6.3.3 Parola/Şifre İşlemleri

Bilişim sistemleri üzerinde yapılan işlemlerin güvenli bir şekilde gerçekleştirilebilmesi için ilk etapta kimlik doğrulama işleminin başarılı bir şekilde sonuçlanması gerekmektedir. Bu manada parola ve şifre güvenlik sisteminin iki önemli bileşenini oluşturmaktadır. Bu iki bileşen sıklıkla birbirlerinin yerine kullanılmakta ve karıştırılmaktadır. Bu iki kavramı internet bankacılığı bağlamında irdelediğimizde;
14 Eylül 2007 tarih ve 26643 sayılı Resmi Gazete'de yayımlanan Bankacılık Düzenleme ve Denetleme Kurumunun, bankalarda bilgi sistemleri yönetiminde esas alınacak ilkelere ilişkin tebliğinde parola; "Kimlik doğrulamada kullanılan, değiştirilmesi zorunlu kılınmayan gizli alfabetik ve/veya rakamsal karakterler dizisini" ifade ettiği belirtilmiştir.
Şifre ise "Gizliliği olan şeylerin açılması veya kullanılması için gerekli olan sayısal değerdir (İnt. Kyn. 62)."

Bu iki tanımdan, parolanın harf ve rakamdan, şifrenin ise sadece rakamdan oluşan değerler alabileceği anlaşılmaktadır. İnternet bankacılığı hesabının güvenliğini

sağlamak adına oluşturduğumuz parola ve şifrelerde, kolay tahmin edilemeyecek, kişi ile bağlantılı isim, doğum yılı, memleket gibi bilgilerin kullanılmaması, bunun yerine büyük harf, küçük harf ve rakamlardan hatta sistemin izin vermesi durumunda sembollerden oluşan karmaşık ve anlam ifade etmeyecek nitelikte güçlü karakterlerin kullanılması sistem güvenliğini artıracak ve dolandırıcılık olaylarını otomatikman azaltacaktır.

İnternet bankacılığı güvenliğinin, parola ve şifre dışında farklı bir boyutunu da tek kullanımlık şifreler oluşturmaktadır. Tek kullanımlık şifre, "her kullanımda veya belirli bir süre geçtikten sonra geçerliliğini yitiren ve bir sonraki kullanım için yeniden üretilmesi gereken sayı ve/veya harf dizisi" olarak tanımlanmıştır (İnt. Kyn. 63).

En çok kullanılan tek kullanımlık şifre çözümleri, SMS şifre; müşterinin banka sisteminde kayıtlı cep telefonuna, internet bankacığına her girişinde gönderilen ve belli zaman diliminde sisteme girilmesi gereken şifredir. Şifre üreten cihazlar; müşterinin banka hesabı ile bağlantılı olarak üretilen ve her tuşuna basıldığında farklı şifre üreten cihaz/donanımdır. Bunun yanı sıra cep/mobil şifre adıyla gelişen teknoloji ile birlikte telefon ve mobil cihazlara kurulan ve şifre üreten uygulamalar bulunmaktadır. Şifre üreten cihazın veya telefonunun kaybedilmesi ya da telefona gelen şifrenin herhangi bir nedenle telefona ulaşmaması durumunda derhal banka ile iletişime geçilerek gerekli güvenlik önleminin aldırılması gerekmektedir.

6.3.4 3D Secure Sistemi (3D Şifresi)

İnternet üzerinden kart bilgileri girilerek yapılan alışveriş işlemlerinde güvenliği bir boyut ileriye taşıyarak, işlem güvenliğini artıran bir sistemdir. Visa ve Master Card'ın geliştirdiği bu güvenli alışveriş sistemiyle üye işyeri, banka ve kart sahibi arasında oluşan sorumluluk mekanizması ile sahtekârlıklara karşı önlem alınmaktadır (Kaya 2009).

3D secure sisteminde, "Kullanıcının kart bilgilerini girmesinden sonra bildiğimiz normal ödeme işleminin gerçekleşmesinden farklı olarak, ödeme esnasında kullanıcının

kartının bankası tarafından ek bir ekran (browser redirection ile) gösterilerek kullanıcıdan kayıtlı cep telefonuna gelen SMS şifresi ve/veya CVC2 bilgisini girmesi istenir. Kullanıcıya SMS şifresi ve/veya CVC2 bilgisi de sorulduğu için kart sahibinin kimliği doğrulanır ve kartın sahibi dışındaki kişilerce kullanılmasının önüne geçilmiş olunur (İnt. Kyn. 64).”

İnternet üzerinden güvenli alışverişin sağlanabilmesi için öncelikle bilindik ve kendini ticari ve güvenlik platformlarında kanıtlamış sitelerin tercih edilmesi, bunun yanı sıra sitenin ödeme ekranında 3D secure sistemini müşterisine tercih olarak sunan sitelerin tercih edilmesi alışverişi daha da güvenli kılacaktır. Farklı bir güvenlik önlemi de müşterinin sanal alışverişlerde kullanmış olduğu kredi kartını, bankasının 3D secure sistemine kayıt ettirerek, tüm sanal alışverişlerini 3D secure şifresi ile doğrulayarak gerçekleştirebilmesidir. Bu durumda müşterinin kart bilgileri kötü niyetli kişilerin eline geçmiş olsa bile sanal alışverişlerde kullanılamayacaktır.

6.3.5 Lisanslı İşletim Sistemi ve Antivirüs Programları

Lisanssız ve güncellemeleri yapılmamış bir işletim sistemi üzerinde güvenli bir işlem gerçekleştirebilmek pek mümkün değildir. Güvenlik açıkları bulunan ve uzaktan yetkisiz erişime açık bir işletim sisteminde, yüksek güvenlik gerektiren işlemler yapmak her zaman riskli olacaktır.

İşlem güvenliğinin sağlanabilmesi için öncelikle lisanslı ve güncelleştirmeleri zamanında yapılarak sistem açıkları kapatılmış, stabil olarak çalışan bir işletim sisteminin olması gerekmektedir. Bunun yanı sıra işletim sistemine dış etkenlerden, öncelikle internet ve harici depolama aygıtları aracılığıyla gelerek tehdit oluşturabilecek kötücül yazılımları engellemek için lisanslı ve güncelleştirmeleri yapılmış antivirüs programları kullanmak gerekmektedir (İnt. Kyn. 67). Bu iki güvenlik önlemi kişisel bilgilerin, kart ve güvenlik parametrelerinin kötü niyetli kişilerin eline geçmesini engelleyecektir.

6.3.6 Tarayıcı Ayarları ve Eklentileri

İnternet tarayıcılar (Explorer, Chrome vb.) bilgisayarların internet dünyasına açılan penceresini oluşturmaktadır. İnternet üzerinde yapılan tüm işlemler bu pencereler aracılığıyla yürütülmektedir. Bu pencereler ne kadar güvenli olursa, yapılan işlemler de o derece güvenli gerçekleşecektir.

"Tarayıcı, Web tarayıcısı, İnternet tarayıcısı, Ağ tarayıcısı veya Web göz atıcısı (İngilizce: Web Browser) kullanıcıların ağ sunucuları üzerinde yer alan HTML veya daha gelişmiş sayfaların açılmasını sağlayan bir yazılımdır. Standart web tarayıcısı; metin veya çoklu ortam dosyalarını açabilir, kaydedebilir, HTML'den HTTP'ye bütün protokolleri ve standartları destekler, açılan sayfada aranan nesneyi bulabilir, sık kullanılanlar ve geçmiş listesi yapabilir, genel ağa dosya yükleme ve genel ağdan dosya indirme yapabilir, eposta ve metin editörleriyle bütünleşebilir. Linkleri (bağlantı) izleyebilir. Dosya sistemlerini okuyabilir, bağlayabilir, kaydedebilir. Çoklu ortam dosyalarını oynatabilir veya kaydedebilir, sayfanın çıktısını alabilir, çevrimdışı çalışabilir (İnt. Kyn. 65)."

Bir çok önemli işlemin gerçekleştirildiği tarayıcıların güvenliği de önem arz etmektedir. Her tarayıcının farklı güvenlik ayarları bulunuyor olsada temelde aynı mantık üzerine güvenlik sağlamaktadırlar. Öncelikle hangi tarayıcı kullanılıyorsa kullanılsın güncelleştirmelerinin yapılmış olması gerekmektedir. Sonrasında her nekadar kullanıcıya kullanım kolaylığı sağlasada formları otomatik doldurma ve şifreleri kaydetme seçeneğinin deaktif edilmesi gerekmektedir. Yine kötücül yazılım ve kimlik avına (phishing) karşı gerekli eklentilerin çalıştırılması ve ayarlarının aktif hale getirilmesi gerekmektedir. Bu üç güvenlik ayarının kullanıcıyı dolandırıcılık olaylarına karşı koruyuculuğu oldukça fazladır. Bunun dışında tarayıcıların, kullanıcısının kullanım alanına göre yapabileceği birçok güvenlik ve gizlilik ayarları bulunmaktadır.

6.3.7 İnternet Bankacılığı Kişisel Güvenlik Ayarlarını Etkinleştirme.

6.3.7.1 İşlem Limiti Tanımlama

İnternet bankacığı üzerinden gerçekleştirilen havale, eft, swift ve döviz alış/satış gibi işlemlerde günlük veya aylık limitler belirleyerek, belli limitin üstünde işlem yapılması kısıtlanabilmektedir (İnt. Kyn. 68). Limit artırımları sadece müşteri hizmetleri ya da banka kanalı ile yapılabilmekte, internet bankacığı üzerinden limit artırımlarına ise izin verilmemektedir. Herhangi bir nedenle internet bankacılığı hesabına yetkisiz erişim sağlanmış olsa bile belirlenen limitin dışında işlem yapılamayacak bu sayede mağduriyetler azalmış olacaktır.

Bunun dışında belirlenen limitin üzerinde yapılan işlemler için cep telefonuna doğrulama kodu gönderilmesi seçeneği de aktif hale getirilerek, hesap sahibinden onay alınmadan belli limitin üstünde işlem yapılması engellenmiş olacaktır.

6.3.7.2 IP Numarası Kısıtlama

IP (Internet Protocol) numarası, internete bağlanan her cihaza internet hizmeti alınan firma tarafından atanan numaradır (Avşar ve Öngören 2010). İki sistem arasındaki iletişim bu IP numaraları aracılığıyla gerçekleşmektedir. Bankalar kullanıcılarına bankanın internet bankacılığı sistemine bağlanmak için sabit bir IP numarası tanımlama ve sadece bu IP numarası üzerinden sisteme yapılacak bağlantılara izin vererek kısıtlama imkânı sunmaktadırlar. Sabit IP numarası kullanan kullanıcılar için ideal bir güvenlik çözümüdür. Herhangi bir şekilde şifre, parola ve tek kullanımlık şifre elde edilmiş olsa bile banka sistemine tanımlanan sabit IP numarası üzerinden bağlantı sağlanmazsa işlem yapılamayacaktır. Bu yönüyle etkin bir güvenlik önlemidir.

6.3.7.3 Servis Sağlayıcı Kısıtlama

Kullanıcılar internet hizmetini ülkemizde faaliyet gösteren internet servis sağlayıcılar aracılığıyla almaktadırlar (İnt. Kyn. 69). Sabit internet hizmeti veren servis

sağlayıcıların başında, Ttnet, Süperonline, Türknet ünvanlı firmalar gelmekte iken mobil internet hizmeti veren servis sağlayıcıların başında Turkcell, Vodafone ve Avea ünvanlı firmalar gelmektedir. Bu firmaların dışında birçok servis sağlayıcı lisansı bulunan firma bulunmaktadır.

Her servis sağlayıcıya farklı olarak belli IP blokları tanımlanmıştır ve bu IP bloğunda bulunan IP numaraları ile müşterilerine hizmet vermektedirler. Kısacası, IP numarasının hangi servis sağlayıcıya ait olduğu bellidir. Bu özellikten yola çıkarak bankalar müşterilerine servis sağlayıcı bazında kısıtlama imkânı sunmaktadırlar (İnt. Kyn. 70). İnternet bankacılığı ayarları yapılırken hangi servis sağlayıcı firma seçildi ise sadece seçilen servis sağlayıcı üzerinden gelen bağlantılara izin verilmektedir. Farklı servis sağlayıcılardan gelen bağlantı isteklerine ise izin verilmemektedir. Sabit IP numarası kullanma imkânı olmayan kullanıcılar için ideal bir güvenlik çözümüdür.

6.3.7.4 İşlem Zamanı Kısıtlama

İnternet bankacılığı üzerinden gerçekleştirilen işlemlerin belirlenen saat aralığında yapılmasına izin verilerek bu saatlerin dışında işlem yapılması engellenmiş olmaktadır (İnt. Kyn. 70). Yine haftanın belli günleri belirlenerek bu günlerin dışında işlem yapılması engellenebilmektedir. Bu sayede önemli ölçüde güvenlik sağlanmış olmaktadır.

6.3.8 Sanal Kart Oluşturma

Kredi Kartı bilgileri girilerek yapılan internet alışverişlerinde işlem güvenliğiyle birlikte kart güvenliğinin de sağlanması adına, bankalarca ana kart ile bağlantılı olarak oluşturulan ancak fiziksel olarak basılmayan sanal kredi kartı hizmeti sunulmaktadır (Kaya 2009).

Sanal kredi kartı, kredi kartında bulunan tüm özellikleri taşımakla birlikte her işlem için yeni limit belirleme ya da banka ile iletişime geçilerek kart bilgilerini değiştirebilme

esnekliği sağlamaktadır. Bu sayede kart bilgileri kötü niyetli kişilerin eline geçmiş olsa bile işlem sonunda limit sıfırlanacağından, karttan herhangi bir işlem yapılamayacaktır.

6.3.9 Güvenli POS Cihazı Kullanımı

POS cihazı ile gerçekleştirilen ödeme işlemlerinde, kart sahibi bizzat POS cihazının yanında bulunmalı, şifre çevrede bulunan ilgisiz kişilere gösterilmeden tuşlanarak işlem gerçekleştirilmelidir. Bu durum önemli bir güvenlik önlemidir. Bunun dışında ödemeyi alacak görevliye kartın ve şifrenin verilmesiyle işlemin uzak bir alanda gerçekleştirilmesi durumlarında, kartın kötü niyetli bir çalışan tarafından kopyalanabileceği riski asla göz ardı edilmemelidir.

Ödeme esnasında kartın POS cihazı dışında, el çabukluğuyla başka yabancı bir cihazdan da geçirilip geçirilmediğine dikkat edilmelidir. Özellikle lokanta, dinlenme yeri, alışveriş merkezi gibi yerlerde çalışan dolandırıcılık çetesi üyeleri ödeme için kendilerine verilen kartları ikinci bir okuyucudan geçirerek kopyalamaktadırlar (Eralp 2012). Çok küçük boyutlarda üretilebilen kart kopyalama cihazları POS cihazlarının yanında gözden kaçabilmekte bu manada büyük risk oluşturmaktadırlar. Bu bağlamda alışverişlerde, POS cihazlarını gözle görülebilen açık alanlarda bulunduran işletmeler tercih edilmelidir.

POS cihazlarını, kasa elektronik aksamı ve dış yüzeyine banka logoları yapıştırılmak suretiyle değiştirilerek oluşturulan sahte POS cihazlarının, normal banka POS cihazlarından ayırtetmek hayli güçtür. Dolandırıcılık olaylarında, ödeme esnasında kart öncelikle sahte POS cihazından geçirilerek kopyalanmakta, kullanıcıya işlem geçersiz oldu denilerek cihazdan sahte slip yazdırılmaktadır. Bu durumun akabinde işlem normal POS cihazından tekrar gerçekleştirilerek işlem tamamlanmaktadır. Böyle durumlarda ilk işlemin yapıldığı sahte POS cihazından çıkan slip dikkatle incelenmelidir. Slip üzerinde banka logosu, tarih ve saat bilgisi, iş yeri numarası ve terminal numarası gibi teknik bilgilerin bulunup bulunmadığı kontrol edilmeli, özensiz bir şekilde hazırlanmış sliplerden şüphelenilmelidir. Ödeme slipleri düzenli bir şekilde saklanarak ay sonu

gelen hesap özeti (ekstre) ile karşılaştırılmalıdır. Tespit edilen tutarsızlıklar bankaya bildirilerek, gerekli işlem adımları takip edilmelidir.

7. SONUÇ VE DEĞERLENDİRME

Sonuç olarak, bilişim yoluyla gerçekleştirilen dolandırıcılık olaylarının, maddi değer taşıması nedeniyle bankacılık ve on-line alışveriş sektörünü hedef aldığı görülmektedir. Bankacılık sektörünün önemli hizmet araçlarından olan ATM ve POS cihazları iktisadi alanda herkes tarafından yaygın olarak kullanılmaktadır. ATM cihazlarına yerleştirilen kopyalama düzenekleri ve maniple edilmiş POS cihazları temelde kart bilgilerinin kopyalanması ve karta ait şifre bilgisinin elde edilmesine yöneliktir. Elde edilen kart ve şifre bilgisi dolandırıcılar tarafından değişik şekillerde kullanılabilmektedir. Bunun önüne geçebilmek için ATM ve POS cihazlarının kullanımında kart ve şifre bilgisinin dışında kişiye özgü taklit edilemez biyolojik bir karakteristiğinin de sorgulanması gerekmektedir. Bunun için bankaların parmak izi okuma, retina tarama ve yüz tanıma sistemleri üzerine yatırım yapmaları, bu sistemleri ATM ve POS cihazlarına entegre ederek en kısa zamanda hayata geçirmeleri gerekmektedir.

Bankaların, ATM cihazları ile ilgili olarak alması gereken diğer bir güvenlik önlemi ise ATM üzerine takılacak sahte ön yüz, sahte klavye, kart kopyalama aparatı, para giriş çıkış noktalarına yabancı madde, kablolu/kablosuz kamera benzeri yabancı maddelerin takılmasını ve mevcut ATM ekipmanlarının ATM üzerinden sökülmesini engelleyici algılama sistemlerini kurması gerekmektedir. Bu sistemle ATM üzerinden sesli ikaz yapılırken diğer taraftan da sistem üzerinden ilgili güvenlik birimlerine bilgi verilmesi sağlanmalıdır.

On-line alışverişlerde ödeme aracı olarak kart bilgilerinin kullanılması oldukça yaygındır. Ödeme ekranına girilen kart bilgileri sanal POS'lar aracılığıyla bankaya iletilerek kartta yeterli limitin bulunması durumunda ödeme işlemi gerçekleştirilmektedir. Bu durumda kart üzerinde yazan bilgileri elde eden herhangi bir kişi bu kart bilgilerini on-line alışverişte sanal POS üzerinden kullanabilmektedir. Bu durum sistemin ne kadar istismara açık olduğunu göstermektedir. Bu ödeme sisteminin güvenli olabilmesi için sanal POS ile gerçekleştirilen her işlemde 3D doğrulamasının zorunlu hale getirilmesi gerekmektedir. Bunun için özellikle bankaların ve on-line alışveriş sitelerinin gerekli alt yapıyı oluşturmaları gerekmektedir. Bununla birlikte

bankaların, müşterilerine internet üzerinden gerçekleştirecekleri alışverişlerde kredi kartı üzerinde yazan bilgileri kullanmak yerine sanal kredi kartlarını kullanmayı teşvik edici çalışmalar yapmaları gerekmektedir.

Bankalar müşterilerine sundukları kredi kartı hizmeti için bünyelerinde ayrı bir birim kurmaları gerekmektedir. Kart talep eden müşterilerinin kimlik ve iletişim bilgilerini değişik kanallardan teyit ettikten sonra kartın basımına onay vermeleri yine kartın dağıtımının ve karta ait şifre bilgisi tesliminin bu birimler aracılığıyla gerekli kimlik doğrulamalarının yapılması neticesinde sağlanması gerekmektedir. Kartların; internet, yurtdışı, mail order ve telefon order kullanımına kapalı olarak teslim edilmesi, müşterinin talebi doğrultusunda bu birimlerce kullanıma açılması gerekmektedir.

Tek kullanımlık SMS şifresi internet bankacığı ve on-line alışveriş işlemlerinde kimlik doğrulamada kullanılmakta ve güvenlik için büyük önem taşımaktadır. Dolandırıcılar bu SMS şifresini elde edebilmek için sahte evraklar ibraz ederek kart sahibine ait yeni sim kart çıkarma (değiştirme) yoluna gitmektedirler. Bankalar, sim kart değişikliklerinden gsm firmaları aracılığıyla on-line olarak haberdar olmaktadırlar. Bu durumda sms şifre gönderimi durdurulmakta yine müşteri hizmetleri vasıtasıyla yapılan doğrulama neticesinde şifre gönderimi başlatılabilmektedir. Bunu engellemek için sim kart değişikliklerinde gsm firmalarının müşteriye ait kimlik bilgilerini değişik kanallardan teyit etmeden değişimi onaylamamaları yine bankaların sim kart değişim durumlarında şube aracılığıyla müşterinin yazılı beyanını almadan sms şifre gönderimine başlamamaları gerekmektedir.

Bilişim suçlarını ya da bilişim yoluyla işlenen suçları diğer klasik suçlardan ayıran birçok özellikten birisi de mağdur ile failin aynı ortamda bulunmamalarıdır. Dünyayı saran bilişim ağları vasıtasıyla herhangi bir ülkeden herhangi bir bilgisayar kullanıcısına karşı suç işlenebilmektedir. Bu yönüyle bu suç türünün sınır aşan suçlar kapsamında olduğu ve suç soruşturma süreçlerinde ülkeler arası karşılıklı adli yardımlaşma mekanizmasının etkin bir şekilde işletilerek suçun en hızlı şekilde aydınlatılması gerekmektedir. Adli yardımlaşma yönüyle, ülkemizin de taraf olduğu Avrupa Siber Suç

Sözleşmesinin bilişim alanında soruşturma yürüten kolluk birimlerinin suç soruşturma kabiliyetini güçlendireceği değerlendirilmektedir.

Bilişim teknolojileri hızla gelişim göstermektedir. Bu yönüyle teknoloji suç işlemeyi kolaylaştırırken bir yandan da yeni suç tiplerini ortaya çıkarmıştır. Teknoloji suçlarıyla mücadele de etkinliğin artırılması amacıyla teknolojik gelişimin hukuki mevzuata ve idari yapılanmaya yansıtılacak şekilde gözden geçirilmesi gerekmektedir. Emniyet Teşkilatında ihtisas birimi olarak kurulan ve yaygınlaştırılan Siber Suçlarla Mücadele birimleri gibi Adalet Teşkilatında da Bilişim Savcılıklarının her ilde olacak şekilde yaygınlaştırılması ve yargılamayı yapacak Bilişim Mahkemelerinin kurulması gerekmektedir. Bununla birlikte bu alanda çalışan görevlilerin belli periyotlarda yapılacak hizmetiçi ve uluslararası eğitimlerle bilgileri güncel tutulmalıdır.

Son olarak, teknolojinin getirmiş olduğu nimetlerden faydalanırken mağdur olmamak için yapılması gereken en basit ve etkili davranış bilinçli olmaktır. Bilinç, insanın çevresinde olup bitenlerin farkında olmasıdır. Bu farkındalığın oluşturulabilmesi için kamu ve özel kurumlara büyük görevler düşmektedir. Okullarda öğrencilere küçük yaşlardan başlanarak kademeli olarak teknolojinin güvenli kullanımıyla ilgili eğitimler verilmelidir. Bununla birlikte hayatın her evresinde halkı bilinçlendirmek için kamu ve özel sektör kuruluşları tarafından bilgilendirme programları, afişler/billboardlar ve kitle iletişim araçları vasıtasıyla kamu spotları yayınlanması gerekmektedir.

8. KAYNAKLAR

Acar, H. E. (2010). 5237 Sayılı Tck Kapsamında Dolandırıcılık Suçu, Yüksek Lisans Tezi, Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Alaca, B. (2008). Ülkemizde Bilişim Suçları Ve İnternetin Suça Etkisi (Antropolojik Ve Hukuki Boyutları İle), Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Alataş, Ş. ve Atan, M. (2007). Phishing: İnternet Denizinin Popüler Avlanma Yöntemi, XII. Türkiye'de İnternet Konferansı, Bilkent Üniversitesi, Ankara, 8-10 Kasım 2007, 226-236.

Artuç, M. (2007). Malvarlığına Karşı Suçlar, Kartal Yayınevi, Ankara.

Avşar, B.Z. ve Öngören, G. (2010). Bilişim Hukuku, Türkiye Bankalar Birliği, Yayın No: 270, İstanbul.

Aydın, E.D. (1992a). Bilişim Suçları ve Hukukuna Giriş, Ankara.

Aydın, E.D. (1992b). Bilişim Sistemlerinde Güvenlik, Güvenilirlik, Mahremiyet ve Bilişim Suçları, Marmara Üniversitesi İletişim Fakültesi, *Marmara İletişim Dergisi*, **1**:109-137.

Baş, E. (2013). Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Bilen, M. (2012). Türk Ceza Hukukunda Dolandırıcılık Suçu, Doktora Tezi, Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Konya.

Bilek, T. B. (2012). Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri, Yüksek Lisans Tezi, Gazi Üniversitesi, Bilişim Enstitüsü, Ankara.

BKM, Bankalararası Kart Merkezi (2014). Faaliyet Raporu, S:42, İstanbul

BTK, Bilgi Teknolojileri ve İletişim Kurumu (2015). Üç Aylık Pazar Verileri Raporu 2014 Yılı 4. Çeyrek Ekim – Kasım – Aralık, Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, Ankara

Boğa, U. (2011). Bilişim Suçlarıyla Mücadele Yöntemleri, Uzmanlık Tezi, Radyo Ve Televizyon Üst Kurulu, Ankara.

Akbulut Bozdoğan, B. (2000). Bilişim Suçları, *Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı*, **1-2**:546.

Burlu, K. (2013). Bilişimin Karanlık Yüzü, Nirvana Yayınları, Ankara.

Çakar, Y. (2013). Hacker Sırları 1, E-book.

Ocak, M.A., Yalman, Y., Çakır, H., Yalçın, N., Uluyol, Ç., Karataş, E., Benzer, R., Gökçearslan, Ş., Çubukçu, A., Aytekin, A., Kılıç, M.S., Özer, Ö., ve Doğan, T. (2014). Güncel Tehdit: Siber Suçlar, Seçkin Kitapevi, Ankara, 97-135.

Çakır, H. ve Topçu H. (2005). Bir İletişim Dili Olarak İnternet, *Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, **19**:71-96.

Dönmezer, S.(2004). Kişilere ve Mala Karşı Cürümler, 17. Bası, Beta Yayınevi, İstanbul,

Duramaz, S. ve Dündar, S. (2014). Elektronik Ödeme Sistemlerinin Karşılaştırılması: Türkiye ve İtalya Örneği, *Uşak Üniversitesi Sosyal Bilimler Dergisi*, **7(1):** 24-37.

Eker, Ö.U. (2006). "Türk Ceza Hukuku'nda Bilişim Suçları" Eski Tck Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler Ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu, *TBB Dergisi*, **62:**101-131.

Eralp, Ö. (2007). Hukukçular İçin Bilişim Terimleri Sözlüğü, Avbil yayınları.

Eralp, Ö. (2012). İnternet Bankacılığı Ve Kredi Kartı Dolandırıcılığının Teknik, Hukuki ve Cezai Boyutu, Eralp kitap.

Erdağ, A. İ. (2010). Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda), *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, **2:** 275-303

Erdoğan, Y. (2012). Bilişim Sistemine Girme Ve Kalma Suçu, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, **12:**1363-1433.

Ersoy, Y. (1994). Genel Hukuki Koruma Çerçevesinde Bilişim Suçları, *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, **3-4:**149-183, Ankara.

Gökcen, A. ve Balcı, M. (2008). Dolandırıcılık suçu (5237 s.lı TCK. m. 157-159), *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, **14**:1-2,

Gönenç, E.Ö. (2003). İnternet ve Türkiye'deki Gelişimi, *İstanbul Üniversitesi İletişim Fakültesi Dergisi*, **16**:87-98.

Gürçam, U. (2008). İnteraktif Dolandırıcılık, Yüksek Lisans Tezi, Eskişehir Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir.

Hadnagy, C. (2013). Sosyal Mühendislik, İnsan Kandırma Sanatı, Paloma Yayınları, İstanbul.

Hekim, H. ve Başıbüyük, O. (2013). Siber Suçlar Ve Türkiye'nin Siber Güvenlik Politikaları*, Uluslararası Güvenlik ve Terörizm Dergisi*, **4**:2.

Kahraman, E. (2009). Özel Hayatın Gizliliği, Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Kale, H. (2014). Bilişim Toplumuna Özgü Bir Suç Tipi: Bilişim Suçları, *Kamuda Sosyal Politika Dergisi (Nisan-Mayıs, -Haziran*), **2:**49.

Karimi, O. ve Korkmaz, A. (2013). Kişisel Verilerin Korunması, 18.Türkiye'de İnternet Konferansı-inet-tr'13, İstanbul Üniversitesi, İstanbul, 9-11 Aralık 2013.

Karpuz, E. (2012). Ödeme Sistemleri ve Araçlarının Artan Kullanımı: Kredi Kartı Kullanımının Para Politikası Etkinliğine Etkisi, TCMB Uzman Yeterlilik Tezi, Ankara.

Kaya, F.(2009). Kredi Kartları, Beta yayıncılık, İstanbul.

Mahmutoğlu, F.S. (2013). Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası,* **1:** 855-890.

MEGEP(2007). Mesleki Eğitim ve Öğretim Sisteminin Güçlendirilmesi Projesi, Pazarlama ve Perakende Elektronik Bankacılık, Milli Eğitim Bakanlığı, Ankara.

Merkez Bankası, (2014). Ödeme Sistemleri-Türkiye'de Ödeme Sistemleri, Ankara.

Mitnick, D.K. and Simon, W.L. (2005). Aldatma Sanatı, Odtü Geliştirme Vakfı Yayıncılık, Ankara.

Noyan, E.(2007) Ceza Davası, https://books.google.com.tr/books?id=nGRoBgAAQBAJ e-book, Ankara.

Özkan, C. (2014). Türkiye'de Kredi Kartı Kullanıcı Profili Ve Davranışı Analizi, Uzmanlık Yeterlilik Tezi, Türkiye Cumhuriyet Merkez Bankası Bankacılık ve Finansal Kuruluşlar Genel Müdürlüğü, Ankara.

Pala, Z. (2008). 34 Konuda Yeni Başlayanlar İçin Bilgisayar, Türkmen Kitapevi, İstanbul.

Rado, T. (1952). "Gaius'a Göre Klasik Roma Hukuku'nda Furtum Suçu", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, **1-2**: 479-519.

Selçuk, S. (1982). Dolandırıcılık, Yasa Yayınları.

Sevim, T. (2006). Elektronik İmza Uygulamasında Kullanılan Zorunlu Ve İhtiyari Dokümanlar, Yüksek Lisans Tezi, Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Tağıyev, R.(2005). E - Ticaret Ve İnternet Üzerinden Pazarlama, Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Topaloğlu, M.(2005). Bilişim Hukuku, Karahan Kitapevi, Adana.

Türkiye Bankalar Birliği, (2008). Banka Kartları ve Kredi Kartları Uygulamaları Hakkında Yararlı Bilgiler, Yayın No:257, İstanbul.

TÜİK, Türkiye İstatistik Kurumu, (2014). Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, Sayı: 16198.

Ünver, M. ve Mirzaoğlu, A.G. (2011). Yemleme ("Phishing"), Rapor, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, Ankara.

Yalçın, F. (2012). İnternet Pazarlamasında Müşteri Memnuniyeti: Günün Fırsatları Üzerine Bir Uygulama, Yüksek Lisans Tezi, Atılım Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Yazıcıoğlu, Y. (2004). "Bilişim Suçları", *Hukuki Perspektifler Dergisi*, Sonbahar 2004, **2**:142-146.

Yılmaz, E. (2000). Türkiye'de Kredi Kartı Uygulaması ve Ekonomik Etkileri, Türkmen Kitapevi, İstanbul.

Yılmaz, Z. ve Ergün, İ. (2005). Açıklamalı-İçtihatlı Yeni Türk Ceza Kanunda Dolandırıcılık Suçları Eski ve Yeni Ceza Kanunu Karşılaştırmalı, Adalet Yayınevi, Ankara.

Yırtımcı, E. (2010). Dolandırıcılık Suçu, Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Yurdadur, A. (2009). Akademik Kurumlarda Bilişim Sistemleri Yardımıyla Bilgi Yönetiminin Gerçekleştirilmesi: Afyon Kocatepe Üniversitesi Örneği, Yüksek Lisans Tezi, AKÜ Fen Bilimleri Enstitüsü, Afyon

Yurtçiçek, M. S. (2013). Hukuki Açıdan Elektronik Para, Seçkin Yayınları, Ankara.

8.1 İnternet Kaynakları

1- http://www.tdk.gov.tr/index.php?option=com_bilimsanat&view=bilimsanat, E.T. 01.11.2014

2-http://www.tdk.gov.tr/index.php?option=com_gts&view=gts, E.T. 01.11.2014

3-http://en.wikipedia.org/wiki/Computer E.T. 01.11.2014

4-http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/internet'in-tarih%C3%A7esi, E.T. 04.11.2014

5-http://tr.wikipedia.org/wiki/Tim_Berners-Lee, E.T. 12.11.2014

6-http://www.internetworldstats.com/stats.htm, E.T. 01.04.2015

7-http://www.ismailgurocak.av.tr/makale/B%C4%B0L%C4%B0%C5%9E%C4%B0M%20S%C4%B0STEM%C4%B0NE%20G%C4%B0RME%20SU%C3%87U-%C4%B0SMA%C4%B0L%20G%C3%9CROCAK.pdf, E.T.15.12.2014

8-http://www.bkm.com.tr/kronoloji.bkm, E.T.17.12.2014

9- http://www.bkm.com.tr/istatistik/secilen_aya_ait_genel_istatistik.asp, E.T.11.04.2015

10-http://www.muhasebedersleri.com/banka-islemleri/mevduat-2.html, E.T.05.03.2015

11-http://www.visa.com.tr/bireysel-kartlar/kartinizi-secin/on-odemeli-kartlar, E.T.09.03.2015

12-http://www.btnet.com.tr/90423-kredi-karti-kullanmayanlar-icin-paypaldan-on-odemeli-kart.html, E.T.05.03.2015

13-http://psmmag.com/haber/turkiye_nin-dijital-cuzdan-haritasi/577564, E.T. 06.03.2015

14-http://www.socialmediatr.com/blog/turkiyede-internetin-kisa-tarihi, E.T.07.03.2015

15-http://www.melihguney.com/turkiyede-ve-dunyada-e-ticaretin-dunu-bugunu-ve-yarini.html, E.T.07.03.2015

16-https://www.chasepaymentech.com/mobile_wallet_technology.html, E.T.06.03.2015

17-http://www.avea.com.tr/web/Destek/Servisler/AveaMobilOdemeServisi/AveaMobilOdemekullanimkosullarinelerdir, E.T.08.03.2015

18-http://www.vodafone.com.tr/Servisler/mobil-odeme-servisi.php, E.T.08.03.2015

19-http://www.bkm.com.tr/tarihce.bkm, E.T.01.02.2015

20-http://www.bkm.com.tr/bkm-express.bkm, E.T.01.02.2015

21-http://www.kkb.com.tr/kkb-hakkinda/kkbyi-tanıyın/tarihçe.aspx, E.T.10.02.2015

22-https://www.findeks.com/findeks-nedir, E.T.10.02.2015
23-http://en.wikipedia.org/wiki/Social_engineering_(security), E.T. 17.03.2015
24-http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=183&Itemid=6, E.T. 18.03.2015
25-https://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-ve-onemsenmeyen-veriler-2.html, E.T.18.03.2015
26-http://tr.wikipedia.org/wiki/K%C3%B6t%C3%BC_ama%C3%A7l%C4%B1_yaz%C4%B1l%C4%B1m, E.T. 22.03.2015
27-http://tr.wikipedia.org/wiki/Bilgisayar_vir%C3%BCs%C3%BC, E.T.22.03.2015
28-http://www.tdk.gov.tr/index.php?option=com_bilimsanat&view=bilimsanat, E.T.20.03.2015
29-http://www.phishing.org/history-of-phishing, E.T.19.03.2015
30- http://www.akbank.com/tr-tr/genel/Sayfalar/Guvenlik-Duyurulari.aspx, E.T.19.03.2015
31-http://assets.garanti.com.tr/assets/pdf/tr/diger/phishing_ornekleri.pdf,E.T.07.03.2015
32-http://bankacilik**********.com/interaktif.islemler.Hesap.Ozetleri/BorcSorgula, E.T.21.03.2015
33-bankacilik**********.com/interaktif.islemler.Hesap.Ozetleri/BorcSorgula/sorgula.php, E.T.21.03.2015
34-bankacilik**********.com/interaktif.islemler.Hesap.Ozetleri/BorcSorgula/smspay.php, E.T.21.03.2015
35-www.***odememerkezi.net, E.T. 20.09.2013
36-www.***faturaodeme.net, E.T.13.01.2014
37-http://www.gazetevatan.com/nijerya-dan-mektup-gelirse-acmayin-bile-59839-yasam, E.T.21.03.2015
38- http://ooofoffline.blogspot.com.tr/2006/09/nijeryadan-mektup-var.html, E.T.21.03.2015
39-http://www.difose.com/blog/index.php/sosyal-muehendislik/98-uyariyoruz-sosyal-muehendislik-yoentemleri-kullanan-dolandiricilar-ifsa-ediyor#, E.T.19.03.2015
40-http://www.olympos.net/belgeler/phishing/vishing-ile-tanisma-zamani-49491.html, E.T. 20.03.2015

41-http://www.sekerbank.com.tr/bireysel/onemliuyarilar.jsp?srgdnrgdezpezpoj, E.T. 20.03.2015
42-http://www.haberler.com/polisin-belirledigi-telefonla-dolandiricilik-4148296-haberi, E.T.20.03.2015
43-http://www.kaspersky.com/tr/internet-security-center/definitions/pharming, E.T.21.03.2015
44-http://www.chip.com.tr/ipucu/pharming-in-neden-oldugu-riski-en-aza-indirme_155.html, E.T.21.03.2015
45-http://www.turkcebilgi.org/teknoloji/guvenlik/kisisel-bilgilerin-ele-gecirilme-yontemleri-254549_3.html, E.T. 23.03.2015
46-http://tr.wikipedia.org/wiki/Bankamatik, E.T.11.02.2015
47-http://www.abendblatt.de/hamburg/article108198874/Geldautomaten-manipuliert-47-jaehriger-Schweizer-gefasst.html, E.T.03.05.2015
48-http://3dprinting.com/news/criminals-use-3d-printers-mass-produce-skimming-devices, E.T.03.05.2015
49-http://www.bankrate.com/financing/banking/thin-atm-skimmers-new-concern, E.T.03.05.2015
50-http://donanimgunlugu.com/kredi-karti-klonlama-canavarlari-pusuda, E.T.03.05.2015
51-http://tr.wikipedia.org/wiki/POS_cihaz%C4%B1, E.T.10.02.2015
52-http://www.tuketicifinansman.net/2011/01/adsl-pos-mobil-pos-ortak-pos-sanal-pos-basvurusu-yap.html, E.T.03.03.2015
53-http://www.ckom.com/story/police-profiling-card-skimming-fraud-awareness-month/46175, E.T. 03.05.2015
54-http://www.ecplaza.net/trade-leads-seller/magnetic-stripe-card-reader-writer--8220997.html, E.T 03.05.2015
55-http://www.indiamart.com/nk-infomatics/magnetic-stripe-card-reader.html, E.T.03.05.2015
56-http://dingword.com/store/index.php?main_page=product_info&cPath=&products_id=360, E.T.03.05.2015

57-http://www.aliexpress.com/item/TIPPER-EMBOSSER-HOT-FOIL-STAMPING-MACHINE-FOR-PVC-PAPER-CREDIT-CARD-WITH-A-FOIL-PAPER-HEAT/32288288141.html, E.T.03.05.2015
58-http://www.garanti.com.tr/tr/bireysel/subesiz/internet_bankaciligi/guvenlik/guvenlik_sertifikasi.page, E.T.26.03.2015
59-https://esube.ziraatbank.com.tr, E.T.20.04.2015
60-https://www.vakifbank.com.tr, E.T.20.04.2015
61-https://internetbankaciligi.vakifbank.com.tr/vb99/loginUser.aspx?, E.T.21.04.2015
62-http://www.eticaret.com/e-ticaret-sozlugu/sifre-nedir, E.T.27.03.2015
63-https://tekkullanimliksifre.wordpress.com/page/2, E.T.27.03.2015
64-http://www.odemesistemleri.org/3d-secure-ile-ilgili-tum-merak-ettikleriniz, E.T.27.03.2015
65-http://tr.wikipedia.org/wiki/Web_taray%C4%B1c%C4%B1s%C4%B1, E.T.28.03.2015
66-www.hsbc.com.tr/tr/kurumsal_isletme/e_bankacilik/sirket_internet/phishing.asp, E.T.25.05.2015
67-http://www.finansbank.com.tr/bankacilik/alternatif-dagitim-kanallari/internet-bankaciligi/sizin-sorumluluklariniz.aspx, E.T.25.05.2015
68-http://www.garanti.com.tr/tr/bireysel/subesiz/internet_bankaciligi/guvenlik/guvenlik_tanimlamalari.page, E.T.25.05.2015
69-http://tr.wikipedia.org/wiki/%C4%B0nternet_servis_sa%C4%9Flay%C4%B1c%C4%B1s%C4%B1, E.T.25.05.2015
70-http://www.odeabank.com.tr/tr-TR/guvenlik/Sayfalar/kisitlamalar.aspx, E.T. 25.05.2015
71-http://www.milliyet.com.tr/teknosa-dan-dolandiricilik-uyarisi/ekonomi/detay/1938697/default.htm, E.T.26.05.2015

9.ÖZGEÇMİŞ

Adı Soyadı : Emin GÜRSOY

Doğum Yeri ve Tarihi : Konya-1983

Yabancı Dili : İngilizce

İletişim (Telefon/e-posta) : egursoykonya@hotmail.com

Eğitim Durumu (Kurum ve Yıl)

Lise : Selçuklu Teknik Ve Endüstri Meslek Lisesi, Bilgisayar Bölümü, Konya (2001)

Ön Lisans : Polis Meslek Yüksek Okulu, Trabzon (2004)

Lisans : Anadolu Üniversitesi, İşletme Fakültesi, İşletme, Eskişehir (2007)

Yüksek Lisans : Afyon Kocatepe Üniversitesi, Fen Bilimleri Enstitüsü, İnternet ve Bilişim Teknolojileri Yönetimi, Afyon (Devam Ediyor)

Çalıştığı Kurum/Kurumlar ve Yıl : Emniyet Genel Müdürlüğü, Ankara (2004)

Yayınları (SCI ve diğer) :

Diğer konular