BİLİŞİM SİSTEMLERİ ARACILIĞIYLA DOLANDIRICILIK SUÇU

Ümit SÖNMEZ[1]

ÖZET

Gelişen teknoloji, bilişim[2]ürünlerine yönelik talebin artmasına ve gündelik yaşamdaki birçok işlemin dijital araçlarla yapılmasına olanak sağlamıştır.(2) Bunun başlıca nedeni bugün en basit e-devlet işlemlerinden banka işlemlerine, abonelik işlemlerinden sağlık hizmetlerine kadar birçok hizmetin işlemin türüne göre her yaşta, her yerde, zaman ve mekân farkı olmadan, istenilen bir zamanda yapılabilir hale gelmesidir. Teknolojide olumlu diyebileceğimiz bu gelişmelerin olumsuz yönü ise kötü niyetli kişiler için sistem boşluklarını bulup, internette insanların zafiyetlerinden faydalanıp çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaları sonucu bundan maddi ve manevi kazanç sağlama arayışı içinde olmalarını sağlamıştır. Bu çalışmada son dönemde eğilim gösterilen, günümüz popüler suçlarından olan ve dolandırıcılık suçunun nitelikli hali olarak düzenlenen bilişim sistemleri yoluyla işlenen dolandırıcılık suçu ile bu suçun mağduru olunmaması için alınması gereken önlemler değerlendirilecektir.

Anahtar Sözcükler: Bilişim Alanındaki Suçlar, Bilişim Suçları, Dolandırıcılık, Sosyal Medya

---

[1] Hukukçu, Bilişim Uzmanı, Diyarbakır Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü

[2]http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a861df8c1d475.05378586 Erişim tarihi, 16.02.2018. Türk Dil kurumuna göre; İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik.

ABSTRACT

Developing technology is enabled to increase of demand for information products and many actions in daily life can be done with digital tools. The main reason of is that people in every age can perform some their necessities without space and time easily such as electronic state process, banking transactions, subscriptions operations, health care services and e-Government Gateway. The negative side of these developments we can say positively in technology is they find system gaps, use of the people weakness on the internet and try to get personal information through various ways of convincing and deceit. And these negative sides also lead people to seek materially and morally gain. In this study, fraud crime is committed through information system which is one of the popular and as a significant form of organized crime and measures will be evaluated.

Keywords: Crimes In The Field Of Information, IT Crimes, Social Media

I.GİRİŞ

Teknolojinin geldiği son noktada bugün bilimin ilerlemesi ile birlikte bilişim ürün ve hizmetlerine yönelik arz ve talebin artması, teknoloji şirketleri tarafından da yapılan ar-ge çalışmaları neticesinde üretim sağlamaları hayatımızı kolaylaştıracak ürün ve hizmetlerin ortaya çıkmasını sağlamıştır. Bunun sonucu olarak da bugün bankacılık, e-devlet veya alışveriş işlemi gibi birçok konu vakit kaybı yaşanmaksızın birkaç işlemle halledilmektedir. Ancak olumlu denebilecek bu teknolojik gelişmeler kötü niyetli insanlar içinde yeni fırsatlar doğurmuştur. Bu durum, uygulamada çeşitli zorluklara, bazen hak kayıplarına ve bazen de teknolojik imkânlar kullanılarak işlenen suçların mağduru olmaya sebep olmaktadır.

Gelişen teknoloji ile birlikte suç olgusunda bilişim çağına dönük değişimler başlamış, gerek bilişim gerekse bilişim yoluyla işlenen asayiş suçlarında artış olmuştur. Yaşanan bu gelişmelerle adi hırsızlık ve dolandırıcılık gibi suçlar, teknoloji ve bilişim olanakları kullanılarak işlenebilmekte ve yeni suç

türleri oluşmaktadır.[3]Oluşan yeni suç türlerine genel hatlarıyla aşağıda başlıklar halinde değinilecek olmakla birlikte, bilişim sistemlerinin sağladığı kolaylıklar neticesinde yaşamımızın her alanında kullandığımız internet, cep telefonu, bilgisayar gibi teknolojilerin yeni suç işleme yöntemlerine zemin hazırlayan araçlar haline nasıl geldiğini ve nasıl haksız kazançlar elde edildiğini göstermesi açısından suçun özelliklerinin belirtilerek kamunun bilinçlendirilmesi sağlanacaktır.

A. KAVRAM

Asayiş suçları arasında yer alan dolandırıcılık suçunun, insanlık tarihi kadar eski olduğu belirtilmektedir.[4]Dolandırıcılık suçu, ekonomik suç türleri başlığı altında incelenmekte olup, 5237 sayılı Türk Ceza Kanunu'nun (TCK) 157. maddesinde "Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamak" şeklinde tanımlanmıştır ve TCK'nın 158. maddesinde dolandırıcılık suçunun nitelikli halleri belirlenmiştir.

Türk Ceza Kanununun gerekçe metninde dolandırıcılık suçu ile ilgili "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

[3] Kaya, Ahsen., Bilgin Umut Erdar, Mollaoğlu Abdullah., Koçak Aytaç ve Aktaş Ekin Özgür, "Türkiye Genelinde Bilişim Yolu İle İşlenen Dolandırıcılık Suçu" E.Ö. NWSA-SocialSciences, 3C0111, 8, (3), 101-105, Demir Oğuzhan Ömer. ve Sever Murat., (2011). Örgütlü Suçlar ve Yeni Trendler. Terörizm ve Sınıraşan Suçlar Serisi:4. Ankara: Polis Akademisi Yayınları, ss: 143-173.

[4]Hafızoğulları, Zeki., (2011). Türk Ceza Hukukunda Dolandırıcılık Suçları. Ankara, Ankara Üniversitesi Basımevi, ss: 405-440.

serbestisi etkilenmekte ve irade özgürlüğü ihlâl edilmektedir." şeklinde kapsayıcı bir açıklama getirilmiştir.

Dolandırıcılık suçunun nitelikli halleri ise, Türk Ceza Kanununun 158. maddesinin 1. fıkrasında belirtilmiştir.[5]

Dolandırıcılık suçu;

- Dini inanç ve duyguların istismar edilmesiyle,
- Kişinin içinde bulunduğu tehlikeli durum veya zor şartlardan ya da algılama yeteneğinin zayıflığından yararlanılmasıyla,
- Kamu kurum ve kuruluşları, kamu meslek kuruluşları, siyasî parti, vakıf veya dernek tüzel kişiliklerinin araç olarak kullanılmasıyla,
- Kamu kurum ve kuruluşlarının zararına olacak şekilde,
- Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılmasıyla,
- Basın ve yayın araçlarının sağladığı kolaylıktan yararlanarak,
- Şirket yöneticisi olan ya da şirket adına hareket eden kişilerin ticari faaliyetleri sırasında,
- Kooperatif yöneticilerinin kooperatifin faaliyeti kapsamında,
- Serbest meslek sahibi kişiler tarafından, mesleklerinden dolayı kendilerine duyulan güvenin kötüye kullanılması suretiyle,
- Banka veya diğer kredi kurumlarınca tahsis edilmemesi gereken bir kredinin açılmasını sağlamak maksadıyla işlenirse "nitelikli dolandırıcılık" kapsamında değerlendirilir.

5237 sayılı Türk Ceza Kanununun 158/1-f bendi içerisinde iki ayrı nitelikli hale yer verilmiştir. Bunlardan ilki, suçun "*bilişim sistemlerinin*"; ikincisi ise, "*banka ve kredi kurumlarının*" suçta araç olarak kullanılmasıdır. Yine Türk Ceza Kanununun gerekçe metninde bilişim sistemi ile ilgili açıklama "Bu bent anlamında "*bilişim sistemi*", verileri toplayıp yerleştirdikten sonra bunları

[5] Türk Ceza Kanunu. Kanun Numarası:5237, Kabul Tarihi:12.10.2004, Yayımlandığı Resmi Gazete Tarihi: 01.06.2005, Yayımlandığı Resmi Gazete Sayısı: 25611.

otomatik işlemlere tabi tutma olanağını veren manyetik sistemler olarak tanımlanabilir" şeklinde verilmiştir.

"Bilişim suçu" ve "bilişim yoluyla işlenen suçlar" birbirinden çok farklı kavramlar olsa da uygulamada birbirleriyle karıştırıldığı sıklıkla gözlemlenmektedir.Bilişim yoluyla işlenen suçlar; hırsızlık, dolandırıcılık, tehdit, hakaret, kişisel verileri yayma ve özel hayatın gizliliğini ihlal gibi asayiş suçlarının bilişim teknolojileri kullanılarak işlenmesi iken,Bilişim suçları ise genel tanımıyla; her türlü teknoloji kullanılarak, kanuni olmayan yollarla kişisel ya da kurumsal bilgisayarlarda, sistemler üzerinde zarar verici etki bırakmaktır.[6]

Bilişim sistemlerine doğrudan girerek veya bu sistemlerini aracı kılarak işlenen dolandırıcılık suçlarında fiiller çok hareketli bir yapıya sahiptir ve her geçen gün bu haksız fiilin çeşitliği artmakta ve yöntemleri sürekli değişmektedir. Özellikle internet kullanımının hızla artmakta olduğu bir dünyada doğrudan kullanıcıları hedef alan kısacası sosyal mühendislik[7] diye tabir edilen birçok dolandırıcılık türü bulunmaktadır.Bu açıklamalardan sonra aşağıda bu suçların kısaca işleniş yöntemlerini değerlendireceğiz.

1. OLTALAMA(YEMLEME)

Güvenilir bir şirket şeklinde bu genelde rüştü ispat olmuş ulusal bir firma olacağı gibi uluslararası bir firma şeklinde veya kişi kılığına girerek, hileli bir şekilde, mağdurun paylaşmayı mantıklı bulacağı şifreler veya kredi kartları gibi özel bilgileri elde etme eylemidir. Yemleme genellikle bir sosyal mühendislik

[6]Dijle Hikmet. ve Doğan Nurettin, (2011). Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı. Bilişim Teknolojileri Dergisi, Volume:4, Number:2, ss: 43-53. Atalıç Taş, Kezban, (2010). Bilişim Suçları ve Adana İlinde 2006- 2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi. Yüksek Lisans Tezi, Çukurova Üniversitesi Sağlık Bilimleri Enstitüsü.Tanrıkulu Cengiz ve ark., (2007). Bilişim Teknolojilerinin Kullanılmasının Hukuksal Boyutu. TBD-BİB Kamu Bilişim Platformu IX, 2. Çalışma Grubu. Bölüm 3,ss: 20-51.

[7] Gündüz, M.Zekeriya.,Daş Resul., (2016). Sosyal Mühendislik Yaygın Ataklar ve Güvenlik Önlemleri. ISCTURKEY 2016 - 9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, ODTÜ, 9(1),11-18. Yazarlara göre sosyal mühendislik bilişim sistemleri aracılığıyla insanların zaaflarını kullanarak çeşitli ikna ve aldatma teknikleriyle istenilen bilgileri elde etmeye çalışmaktır.

yöntemi kullanılarak e-posta veya anlık mesajlar gibi görünürde resmi olan elektronik mesajlarla yapılan bir dolandırıcılık türüdür.

Bu yöntemi biraz da detaylandıracak olursak, dolandırıcılar yemleme saldırılarında bankalardan veya alışveriş sitelerinden geliyor gibi görünen istenmeyen e-postaları yaygın olarak kullanarak resmi internet sitelerinden site kodları ve tasarımları birebir kopyalayıp kendilerine ait internet sitelerinde gerçek gibi görünen sahte internet siteleri yapmaktadırlar. Bu siteler oldukça iyi tasarlandığından insanlar güvenli internet kullanma bilgisine de sahip değilse aldatılma oranı çok yüksek olmaktadır.

2. SATIN ALMA DOLANDIRICILIĞI

Bu yöntemde dolandırıcının malını satmak için ilana koyan veya tam tersi ilana koyulan bir malı satın almak isteyen mağdura alışveriş önermesi ve bu alışveriş için çalıntı ya da sahte kredi kartı gibi hileli yöntemler kullanmasıdır. Böyle bir durum sonucunda mağdura ödeme yapılmayacağı gibi yapılan ödemeler bir başkasının kredi kartı bilgileri ise başka mağdurların ortaya çıkmasını sağlamaktadır.

3. ARKADAŞ DOLANDIRICILIĞI

Dolandırıcılar kimi zaman internetteki arkadaş sitelerini kullanarak burada tanıştıkları kişileri, kendilerine para gönderme konusunda ikna ederek dolandırıcılık suçunun gerçekleşmesi söz konusudur. Dolandırıcılar bu yöntemi izlerken genellikle kendilerini olduklarından çok daha farklı göstermeye çalışırlar. İnternet ortamında yakınlık kurduğu kişiden yardım istemek için kendisini ihtiyaç sahibi olarak tanıtabilir. Bu durumun sadece iki kişi arasında geçen bir konu olduğunu düşünmek yanıltıcı olabilir. Hedef kişinin internet ortamında yakınlık kurduğu kişinin, kendisine zararı dokunacak şeyleri yaptırmaya çalışan bir şebekenin üyesi olabileceği akıldan çıkarılmamalıdır. Dolandırıcıların hedef kişiden para talepleri tek seferlik olabileceği gibi zaman zaman tekrar edebilmektedir.

Arkadaşlık dolandırıcılığında yeni bir terim ise “Catfish” olup Urban Dictionary sitesinde, Facebook veya diğer sosyal medya ağlarında kendisini bir

başkası olarak gösteren ve çevrimiçi romantik aldatmacalar peşinde olanları tanımlamak için kullanılmıştır.[8]

4. BANKA HESAP DETAYLARININ DEĞİŞTİRİLMESİ, GÜNCELLENMESİ DOLANDIRICILIĞI

Bu yöntemde çoğunlukla ticari işletmelerin hedef alınmakta, dolandırıcılar çeşitli yöntemlerle şirketin diğer kişilerle yaptıkları yazışmalara ulaşmayı amaçlamaktadırlar. Bu amaçla çoğu zaman, şirket çalışanlarının eposta hesaplarına ait şifrelerin ele geçirilmeye çalışılmaktadır. Çeşitli yollarla çalışanların eposta şifrelerini elde etmeyi başaran dolandırıcılar şirket çalışanlarının yaptıkları yazışmaları takip ederek hareket geçmek için fırsat gözlemlerler. Dolandırıcılar takip ettikleri şirkete herhangi bir ödeme yapılacağını öğrendiklerinde, ödemeyi yapacak kişiye, şüpheye yer bırakmayacak şekilde yeni bir eposta göndermektedirler. Bu epostada genellikle alıcı şirketin banka hesap numaralarının değiştiğinden bahisle sözde şirkete ait yeni banka hesap numaraları yer almakta ve yapılacak ödemenin bu yeni hesaba yapılması istenmektedir. Dolandırıcılar ödemeyi yapacak kişinin aklında şüphe oluşmaması için bu yeni epostayı, şirketin kullandığı eposta adresine oldukça benzer bir adresten göndermeye çalışırlar. Ödemeyi yapacak kişi, alacaklı şirketin hesap numarasının değiştiğini zannederek ödemeyi dolandırıcılara yapmakta ve neticesinde mağdur olmaktadır.[9]

5. TRUVA YAZILIMLARI (TROJAN)

Bilinen eski yöntemlerden biri olmakla beraber genelde kullanıcıların yararlı yazılım veya uygulamalar eşliğinde bilgisayarlarına yükledikleri, güvenli olduğu düşünülen yazılıma bağlı olarak saklanan ve bilgisayarın normal fonksiyonlarını işlettiği sırada arka planda kendi kötü amacını gerçekleştiren virüsler “Truva atı” şeklinde tanımlanabilir.

[8] https://www.urbandictionary.com/define.php?term=catfish Erişim tarihi: 15.02.2018.
[9] http://www.siber.pol.tr/Duyurular/Sayfalar/Banka-Hesap-Detaylarinin-Degistirilmesi-Guncellenmesi-Dolandiriciligi.aspx Erişim tarihi, 15.02.2018.

Gayet güvenilir bir kaynaktan ve güvenli olduğu düşünülen epostalar Truva atı barındırabilirler. Hedef kişi kendisine gönderilen Truva atı içeren epostayı açarak Truva atının etkin hale gelmesine neden olabilir ancak bu durumun farkında olabilmesi pek mümkün görünmemektedir. Truva atı etkinleştikten sonra bilgisayarda yer alan bütün bilgilere erişebilir ve bunların kötü niyetli kişilere ulaşmasını sağlar. Arka planda herhangi bir belirti göstermeksizin çalışan Truva atı, kullanıcının hesap bilgileri, şifreleri, fotoğrafları ve akla gelebilecek her türlü bilgiyi, kullanıcının bilgisi dışında başka birine gönderebilir. Bu da çeşitli mağduriyetlerin doğmasına neden olabilmektedir.

6. TUŞ VE EKRAN KAYDEDİCİLER (KEYLOGGER VE SCREENLOGGER)

Dolandırıcıların, kullanıcı bilgilerini elde etmenin diğer yöntemleri arasında tuş kaydediciler ve ekran kaydediciler yer almaktadır. Tuş kaydediciler, klavye ile bilgisayara girilen bilgileri kopyalayarak bunların dolandırıcılara ulaşmasını sağlayan yazılımlardır. Bu sayede dolandırıcılar, hedef kullanıcıların şifre ve özel yazışmalarına ulaşabilirler.

Ekran kaydediciler ise, hedef kişinin bilgisayar ekran görüntülerinin kopyalanarak bunların dolandırıcılara ulaşmasını sağlayan yazılımlardır. Söz konusu yazılımlar ekran görüntüsünü fotoğraf karesi gibi yakalayıp dolandırıcılara iletmektedirler. Bu sayede kullanıcının bilgisayarda yaptığı işlemler dolandırıcılar tarafından görülebilmekte, hesap ve şifre bilgileri kötü niyetli kişilere gönderilebilmektedir. Tuş kaydedicilerin ve ekran kaydedicilerin dolandırıcılık eylemlerinde birbirlerini tamamlayan iki bileşen olduğu düşünülebilir. [10]

[10] Türkiye Bankalar Birliği, Aralık 2015. Dolandırıcılık Eylemleri ve Korunma Yöntemleri Syf:14-15

7. Wİ-Fİ DOLANDIRICILIĞI

Bu yöntemde öncelikli olarak ücretsiz internet hizmeti sağlayan kafe, otel, kütüphane gibi tesislere benzer isimle bu tesislere yakında bulunanların erişim sağlayabileceği wifi erişim noktası oluşturarak kullanıcıların işlemlerini bu wifi ağı üzerinden yapması sağlanmaktadır. Daha sonra çeşitli yazılım ve sahte web ara yüzleri ile kullanıcıların bağlantıda eriştikleri hesapların bilgileri temin edilebilmektedir. Temin edilen bu bilgiler dolandırıcılık amacıyla kullanılabilmektedir.

8. POP-UP EKRANLAR

Birçok web sitesinde bir uyarı, anlık ve kolay bilgi iletimi, reklam veya başka benzeri bir amaçla pop-up ekranların kullanıldığı görülmektedir. Bunu kendi amaçları doğrultusunda kullanmak isteyen dolandırıcılar tarafından hazırlanan ve genellikle arıza, geliştirme, erişim sorunu, yardım teklifi gibi içerikle kullanıcının karşısına çıkan pencerelere kullanıcı şifresi girilmesi istenmekte ve kullanıcının hesap bilgileri ele geçirilmektedir. Ayrıca kullanıcı web sitesinde gezinirken bir anda beliren söz konusu pop-up ekranlar çeşitli uygulamaların düzgün çalışmayacağını, yeni bir yazılım yüklenilmesinin kabul edilmesi gerektiği şeklindeki bir mesajla kullanıcının onay vermesi sağlanır. Onayın ardından kötü amaçlı yazılımın, bilgisayara yüklenip çalıştırılmasıyla bilgisayarın dolandırıcılar için açık hedef haline geleceği düşünülebilir.

II. SONUÇ

Yukarıda son zamanlarda bilişim sistemleri aracılığıyla dolandırıcılık suçunun işleniş biçimlerinden en yaygın olarak işlenen türlerine kısaca değinilmiştir. Elbette bu suçun işleniş şekli bu kadar dar olmamakla birlikte her geçen gün artmakta suçlular yeni yöntemler geliştirmektedir Buna bağlı olarak mağdurlar artmakta, bir diğer sonucu ise bu durumun ülke ekonomisine zarar vermesidir. Bu nedenle hem kurumlara hem de kişilere önemli sorumluluklar düşmektedir.

Bahsi geçen yöntemlerle bu suçun mağduru olunmaması için;

Sebebi ne olursa olsun kişisel bilgilerinizin internet ortamında paylaşılmaması ve kendinizle ilgili veya yakınlarınıza ait isim-soy isim, doğum tarihi, memleket gibi veya özel gün ve tarihler, telefon numarası gibi tahmine açık bilgiler şifre olarak seçilmemelidir. Bununla birlikte farklı web sitelerinde aynı şifrenin kullanılmamasına özen gösterilmelidir. Örneğin herhangi bir sosyal medya hesabına kayıt olurken kullanılan şifrenin e-posta şifresi olarak da kullanılmasından kaçınılmalıdır. Çünkü bu dolandırıcılık türünde e-postanın ele geçirilmesi asıl tehlikedir. Çünkü bugün birçok web site doğrulama kodunu eposta adreslerine göndermektedir.

Bugün birçok parasal işlemin yapıldığı internet bankacılığına ait önemli şifrelerin herhangi bir yere yazılmaması ve kimseyle paylaşılmaması gerekmektedir. Kullanıcı adları ve parolalar bilgisayara veya internet tarayıcılarına kayıt edilmemelidir. Ayrıca herkesin kullanımına internet kafe veya iş yeri gibi ortak kullanıma açık bilgisayarlara, zararlı yazılım yüklü olup olmadığı hususunda emin olunamadığından bankacılık, e-devlet veya fatura ödemesi gibi işlemlerin bu bilgisayarlarda yapılmasından kaçınılması gerekmektedir. İnternet bankacılığı girişlerinde sanal klavye kullanımına özen gösterilmelidir.

Bilgisayar ve erişim amacıyla kullanılan cihazlarda kopya veya lisansız yazılım kullanılmamalı, yazılımların güncel sürümleri tercih edilmelidir. Lisansı olmayan ve kırık olarak tabir edilen bir programın içine bilgi toplayan bir yazılım atılmış olabileceği akılda tutulmalıdır. Bunun yanı sıra, lisansız yazılımlarda güvenlik açıkları olabileceği gibi, fark edilen açıklar için güncelleme yapılamamaktadır. İşletim sistemi ve internet tarayıcısının güncel tutulması gerekmektedir. Bilgisayarın korunması ve sorunsuz çalışmasının sağlanması için, yazılımı üreten firmalar tarafından yayınlanan güncellemeler takip edilmeli ve güncellemeler zamanında yapılmalıdır. Bilgisayarlarda lisanslı "anti-virüs" yazılımları kullanılmalı ve bu yazılımlar güncellenmelidir. İnternet bankacılığı sitesine girişte adresin doğru bir şekilde tarayıcının adres alanına yazılması ve herhangi bir yönlendirici link kullanılarak internet bankacılığı sitelerine giriş yapılmaması önerilmektedir. İnternet üzerinden yapılan aramalar sonucu alınan adres bilgilerinin yanlış ve yanıltıcı olabileceği unutulmamalıdır. Güvenli

internet sitelerinde adresin geçerli ve güvenli olduğunu gösteren sertifikalar kontrol edilmelidir. İnternet güvenlik duvarı (firewall) kullanılmalı ve bu tür uygulamalar bilgisayarlarda aktif tutulmalıdır. Firewall yazılımları, bilgisayarlara yetkisiz erişimi engelleyebilir. Tarayıcıda otomatik tanımlama fonksiyonu kullanılmamalıdır. Otomatik tanımlama fonksiyonu, daha önce girilen şifreler de dâhil olmak üzere tüm bilgileri saklar. Güvenlik açısından otomatik tanımlama fonksiyonu devre dışı bırakılmalıdır. Ek olarak, "Şifreyi Hatırla (RememberPassword)" özelliği ayrıca uzak durulması gereken bir seçenektir. Bu seçenek kullanıldığında, bilgisayara erişen kişinin e-postalara, üyeliklere erişimi için hiçbir engel kalmamaktadır.

Mobil cihazlara uygulama marketleri dışındaki ortamlardan uygulama indirilmemesi gerekir. Bu ortamlardan indirilen uygulamalar ile kullanıcı bilgilerinin çalınması mümkündür. İşletim sistemi kırılmış mobil cihazlarla yapılan bankacılık işlemleri güvenlik risklerine açıktır. Zararlı uygulamalardan korunmak için cihaz ayarlarında bulunan "market dışı uygulamaların yüklenmesi" seçeneğinin kapalı durumda olması gerekir. Sözü edilen basit tedbirlerle büyük zararların önüne geçilebilir.[11]

İletiyi gönderen e-posta adreslerine şüpheci bakmaları ve doğru olduğundan emin olmaları, ödeme yapılmadan önce her ihtimale karşı ödeme yapacakları banka hesap numaralarını farklı yollarla (telefon, yüz yüze temas, bankadan kontrol vb.) teyit etmeleri, az bilinen alışveriş sitelerinden kredi kartı numaralarını ve kart güvenlik numarasını(CVV numarası olarak da bilinir) ürün almak için kullanmamaları, kullanıcıların aslında yapacakları bu gibi basit yöntemlerle bu suçların önüne geçilmesi sağlanabilir.

[11] Türkiye Bankalar Birliği, Aralık 2015. Dolandırıcılık Eylemleri ve Korunma Yöntemleri Syf:42-43

KAYNAKÇA

(1)Türk Dil kurumuna göre; İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik,

(2) Sönmez Ümit, Kara İlker, *"Türkiye'de Bilişim Sistemleri Yoluyla İşlenen Dolandırıcılık Suçunun Değerlendirilmesi"*Leges Hakemli Hukuk Dergisi Sayı: 65 Mayıs 2015; ;Sf.72-78.

(3) Kaya, Ahsen., Bilgin Umut Erdar, Mollaoğlu Abdullah., Koçak Aytaç ve Aktaş Ekin Özgür, *"Türkiye Genelinde Bilişim Yolu İle İşlenen Dolandırıcılık Suçu"* E.Ö. NWSA-SocialSciences, 3C0111, 8, (3), 101-105.

(4) (4) Demir Oğuzhan Ömer. ve Sever Murat., (2011). Örgütlü Suçlar ve Yeni Trendler. Terörizm ve Sınıraşan Suçlar Serisi:4. Ankara: Polis Akademisi Yayınları, ss: 143-173.

(5) Hafızoğulları Zeki, (2011). Türk Ceza Hukukunda Dolandırıcılık Suçları. Ankara, Ankara Üniversitesi Basımevi, ss: 405-440.

(6) Türk Ceza Kanunu. Kanun Numarası:5237, Kabul Tarihi:12.10.2004, Yayımlandığı Resmi Gazete Tarihi: 01.06.2005, Yayımlandığı Resmi Gazete Sayısı: 25611.

(7)Dijle Hikmet. ve Doğan Nurettin, (2011). Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı. Bilişim Teknolojileri Dergisi, Volume:4, Number:2, ss: 43-53.

(8) Atalıç Taş Kezban, (2010). Bilişim Suçları ve Adana İlinde 2006- 2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi. Yüksek Lisans Tezi, Çukurova Üniversitesi Sağlık Bilimleri Enstitüsü.

(9) Tanrıkulu Cengiz ve ark., (2007). Bilişim Teknolojilerinin Kullanılmasının Hukuksal Boyutu. TBD-BİB Kamu Bilişim Platformu IX, 2. Çalışma Grubu. Bölüm 3,ss: 20-51.

(10) Gündüz, M.Zekeriya.,Daş Resul., (2016). Sosyal Mühendislik Yaygın Ataklar ve Güvenlik Önlemleri. ISCTURKEY 2016 - 9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, ODTÜ, 9(1),11-18. Yazarlara göre sosyal mühendislik bilişim sistemleri aracılığıyla insanların zaaflarını kullanarak çeşitli ikna ve aldatma teknikleriyle istenilen bilgileri elde etmeye çalışmaktır.

(11) https://www.urbandictionary.com/define.php?term=catfish Erişim tarihi: 15.02.2018.

(12) http://www.siber.pol.tr/Duyurular/Sayfalar/Banka-Hesap-Detaylarinin-Degistirilmesi-Guncellenmesi-Dolandiriciligi.aspx

(13) Türkiye Bankalar Birliği, Aralık 2015. Dolandırıcılık Eylemleri ve Korunma Yöntemleri Syf:14-15, Syf:42-43