

T.C.
İSTANBUL ÜNİVERSİTESİ
ADLİ TIP ENSTİTÜSÜ

Danışman
Dr. Öğr. Üyesi Mustafa Okudan

ANA AKIM MEDYADA TELEFON DOLANDIRICILIĞI HABERLERİNİN
İNCELENMESİ

SOSYAL BİLİMLER ANA BİLİM DALI

YÜKSEK LİSANS TEZİ

HATİCE TUĞSAVUL

İSTANBUL, 2018

**İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA
ADLI TIP ENSTİTÜSÜ MÜDÜRLÜĞÜ
SOSYAL BİLİMLER ANABİLİM DALI BAŞKANLIĞINA**

Lisansüstü Öğretim Yönetmeliğinin 36. maddesi uyarınca Enstitünüz Sosyal Bilimler Anabilim Dalı'nın yüksek lisans öğrencisi Hatice TUĞSAVUL'un,

"Ana Akım Medyada Telefon Dolandırıcılığı Haberlerinin İncelenmesi"

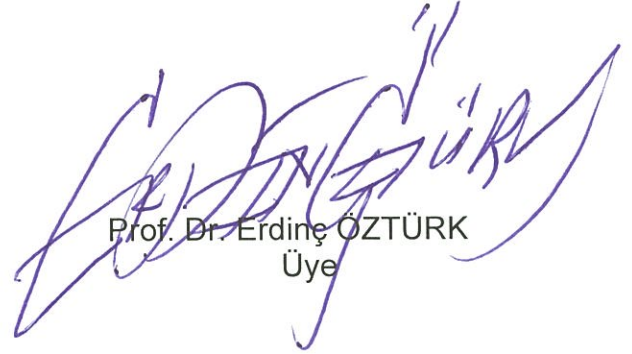
Adlı tezi jürimizce tetkik edilmiş ve kendisine tez savunması yaptırılmıştır.

Yukarıda adı geçen tezin ve tez savunmasının kabul edilmesine oy birliğiyle karar verilmiştir.

Dr. Öğr. Üyesi Y. Tunç DEMİRCAN
Jüri Başkanı



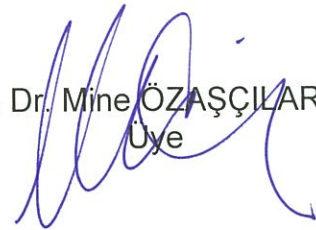
Prof. Dr. Erdiñ ÖZTÜRK
Üye



Doç. Dr. Neylan ZİYALAR
Üye



Doç. Dr. Mine ÖZAŞÇILAR
Üye



Dr. Öğr. Üyesi Mustafa OKUDAN
Danışmanı



T.C.
İSTANBUL ÜNİVERSİTESİ
ADLİ TIP ENSTİTÜSÜ

Danışman
Dr. Öğr. Üyesi Mustafa Okudan

ANA AKIM MEDYADA TELEFON DOLANDIRICILIĞI HABERLERİNİN
İNCELENMESİ

SOSYAL BİLİMLER ANA BİLİM DALI

YÜKSEK LİSANS TEZİ

HATİCE TUĞSAVUL

İSTANBUL, 2018

Özet

Dolandırıcılık; insanlık tarihi kadar eski olup, en genel anlamıyla aldatma amacı ile yapılan kasıtlı eylemlerdir ve gündelik hayatta insanların en çok karşılaştığı suçlardan birisi olarak karşımıza çıkmaktadır. Gelişen teknolojiler, örneğin mobil teknolojiler hayatımıza rahatlık getirmekle birlikte suçun işlenmesini kolaylaştıran bir etken olmaktadır.

Sosyal mühendislik; aslında binalara, sistemlere veya verilere insan psikolojisini kullanarak erişim kazanma sanatıdır. Sosyal mühendislik saldırıları, çevrimiçi saldırılardan e-postalara ve telefon aramalarına kadar pek çok farklı biçimde ortaya çıkmaktadır. Son yıllarda Türkiye'de telefon dolandırıcılığının önemli bir sorun haline geldiğini gözlemlemekteyiz.

Bu araştırmanın amacı, 2017 yılında Türkiye'deki telefon dolandırıcılığı vakalarının mağdur profilini belirlemektir. Bunun için mağdurlarla; deneyimleri, tepkileri ve raporlama tutumlarına dayalı derinlemesine mülakatlar yapılmıştır.

Çalışmanın bazı önemli sonuçları; güncel medyadaki telefon dolandırıcılığı haberlerinin incelenmesi yoluyla mağdur profilinin incelenmesi, mağdurlarla yapılan derinlemesine mülakat etkenlerinin araştırılması, sosyal mühendislik saldırıları hakkında farkındalığın artırılması, vatandaşların bilgilendirilmesi ve yukarıda bahsedilen gazete haberleri ve vakalardan yararlanarak yeni şikayetlerin ortaya çıkmasını önlemek ve önleyici tedbirler önermektir.

Anahtar Kelimeler: Mağduriyet, Dolandırıcılık, Sosyal Mühendislik, Mobil Teknolojiler, Telefon Dolandırıcılığı

Abstract

Fraud, which is as old as the history of humanity, can be defined as deliberate action with deceptive intent and is one of the most common crimes people encounter in their everyday lives. Although emerging technologies such as mobile technologies make life easier for their users, they also become a factor in facilitating crime.

Social engineering is essentially the art of gaining access to buildings, systems or data by exploiting human psychology. Social engineering attacks come in many different forms ranging from online attacks, perhaps via email, to phone calls. It's observed that telephone fraud has become a substantial issue in Turkey in recent years.

This research aims to identify the victim profile of the telephone fraud cases in Turkey in 2017. In order to achieve this, in-depth interviews has been conducted with the victims based on their experiences, reactions and reporting attitudes.

According to the some important results of the study are the identification of the victim profile through examination of phone fraud news in the current media and the investigation of the factors in-depth interviews with victims, the raising awareness of social engineering attacks, informing citizens, and recommending preventive measures and precautions to prevent new grievances from emerging from the newspaper reports and events mentioned above.

Key Words: Victimization, Fraud, Social Engineering, Mobile Technologies, Phone Scams.

Önsöz

Tez çalışmam sırasında kıymetli tecrübeleri ve bilgi birikimi ile bana yol gösteren ve destek olan değerli danışmanım Dr. Öğr. Üyesi Mustafa OKUDAN hocama; önerilerini, bilgilerini sürekli paylaşarak ilham veren Enstitü Müdür Yardımcısı Doç. Dr. Neylan ZİYALAR hocama sonsuz teşekkür ve saygılarımı sunarım.

Gerek mesai içinde, gerekse mesai dışında desteklerini esirgemeyen başta Aslı ŞAHİN olmak üzere; Aslı DÖKER, Seda SATIR, Işılart ARTUT, Özge SELİK-MİNİÇ, Nil GİRĞİN-KALIP, Tuğçe ASLAN, Burçak VATANSEVER, Gül BAKIRTAŞ, Dalya ÇALIŞAN, Murat ÜNVER, Dr. Öğr. Üyesi Selçuk TUZCUOĞLU'na;

Dolandırıcılık suçunun hukuk sistemindeki yeri konusunda yardımlarını esirgemeyen Dr. Öğr. Üyesi M. Sinan ALTUNÇ ve Dr. Öğr. Üyesi Melis TAŞPOLAT-TUĞSAVUL'a;

Rahmetli Babam Necmettin ŞAHİNLER, annem Müzeyyen ŞAHİNLER, kayınvalidem Refhan TUĞSAVUL'a;

Eğitim ve öğretim hayatımda ve tüm hayatımda bana örnek olan, desteklerini esirgemeyen ağbim Prof. Dr. İsmet ŞAHİNLER ve ablam Hacer ŞAHİNLER'e;

Beni Adli Bilimler ile buluşturan, lisans üstü eğitimimin başlangıç aşamasından son anına kadar destek olan sevgili eşim Kimya Yüksek Müh. H. Cihangir TUĞSAVUL'a;

“Yüksek lisansı birlikte mi bitireceğiz acaba?” diye bana destek veren, literatür tarayarak zamanını ve öğrendiklerini benimle paylaşan, en büyük ilham kaynağım ve öğretmenim sevgili oğlum Ahmet Cüneyt TUĞSAVUL'a,

teşekkürlerimi sunarım.

İçindekiler

Özet	i
Abstract	ii
Önsöz.....	iii
İçindekiler.....	iv
Tablo ve Şekil Dizinleri	vi
Kısaltmalar	vii
1.Giriş ve Amaç.....	1
2.Genel Bilgiler	5
2.1. Sosyal Mühendislik	5
2.1.1. Sosyal mühendisliğin tanımı	5
2.1.2. Sosyal mühendisliğin amacı ve hedef kitlesi	9
2.1.3. Sosyal mühendislik saldırı yöntemleri	11
2.1.4. Sosyal mühendislik saldırı evreleri	22
2.2. Dolandırıcılık ve Telefon Dolandırıcılığı	24
2.2.1. Dolandırıcılık suçunun tanımı ve kapsamı	24
2.2.2. Dolandırıcılık suçunun tarihsel gelişimi	28
2.2.3. Dolandırıcılık suçunun benzer suçlardan farkları	30
2.2.4. Nitelikli dolandırıcılık.....	31
2.2.5. Telefon dolandırıcılığı	35
2.3. Dolandırıcılık Suçunun Türk Hukuk Sistemindeki Yeri	43
2.3.1. Suç tipi hakkında genel bilgiler	43
2.3.2 Korunan hukuki değer.....	44
2.3.3.Suçun unsurları	45
2.3.3.1. Tipikliğin maddi unsurları.....	45
2.3.3.2. Tipikliğin manevi unsurları	48
2.3.4. Suçun nitelikli halleri.....	48
2.3.4.1. Cezada artırım yapılmasını gerektiren nitelikli haller	48
2.3.4.2. Daha az cezayı gerektiren nitelikli haller	54
2.3.5. Suçun hukuka aykırılık unsuru	54
2.3.6. Şahsi cezasızlık sebepleri veya cezada indirim yapılmasını gerektiren şahsi sebep	54
2.3.7. Teşebbüs-etkin pişmanlık	54
2.3.8. Suçluların çokluğu (suça iştirak)	55
2.3.9. Suçların çokluğu (suçların içtimai).....	55

2.3.10. Yaptırım	55
2.3.11. Muhakemesi	56
3. Gereç ve Yöntem	57
4. Bulgular	60
5. Tartışma ve Sonuç	64
6. Kaynakça	74
7. Ekler	
EK 1-Bilgilendirilmiş Gönüllü Olur Formu Örneği	
EK 2-Derinlemesine Mülakat Soruları	
EK 3-2017 Yılında En Çok Satış Yapan Ulusal Gazete Yayımlanan Telefon Dolandırıcılığı Haberleri	
EK 4-Telefon Dolandırıcılığına Maruz Kalan 30 Vaka	
8. Özgeçmiş	

Tablo ve Şekil Dizinleri

Şekil 1: Kevin Mitnick'in sosyal mühendislik saldırı döngüsü.....	13
Şekil 2: Bir sosyal mühendislik saldırısının ontolojik modeli.....	14
Şekil 3: Sosyal mühendislik saldırı çerçevesi.....	15
Şekil 4: Sosyal mühendislik saldırılarının izledikleri evreler.....	23



Kısaltmalar

ABD	Amerika Birleşik Devletleri
ATM	Automated Teller Machine
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
CD	Compact Disc
CGTİK	Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun
CMK	Ceza Muhakemesi Kanunu
DNS	Domain Name System
DVD	Digital Video Disc
EFT	Elektronik Fon Transferi
FETÖ	Fetullahçı Terör Örgütü
GBRC	Global Business Research Congress
GSM	Global System for Mobile communication
IEEE	Institute of Electrical and Electronics Engineers
ID	Identification Documents
IP	Internet Protocol
ISCTURKEY	Information Security Criptology Turkey
m.	madde
PTT	Posta ve Telgraf Teşkilatı
TCK	Türk Ceza Kanunu
USB	Universal Serial Bus
vd	ve diğerleri
VoIP	Voice over Internet Protocol

1.Giriş ve Amaç

Dolandırıcılık, en genel anlamıyla aldatma amacı ile yapılan kasıtlı eylemlerdir ve gündelik hayatta insanların en çok karşılaştığı suçlardan birisi olarak karşımıza çıkmaktadır. Dolandırıcılık, insanlık tarihi kadar eski olup, tüm toplumlarda suç olarak kabul edilmiştir (Hafizoğulları, 2011: 316: 405-440). Gelişen teknoloji, hayatımıza rahatlık getirmekle birlikte suçun icrasını kolaylaştıran bir etken olmaktadır. Gelişen sanayi ve ekonomiye paralel olarak yükseliş gösteren yoğun insan trafiği de suç oranını arttıran bir başka etken olarak ortaya çıkmaktadır (Soyaslan, 2010: 416).

Bilgi güvenliği denildiğinde akla ilk gelen kendimize ait olan bilginin başkasının eline geçmemesidir. McCumber Bilgi Güvenliği Modeli'ne göre; bilgi güvenliği, "gizlilik", "bütünlük" ve "erişilebilirlik" olarak üç unsurdan oluşmaktadır. Gizlilik, bilginin yetkisiz kişilerin eline geçmemesidir. Bütünlük, bilginin yetkisiz kişiler tarafından değiştirilmemesidir. Erişilebilirlik ise bilginin ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır. Bu üç unsurdan herhangi biri zarar görürse "güvenlik açığı" oluşur (McCumber, 1991).

Bilgi güvenliğinin sağlanmasından herkes sorumludur. Çoğu kişi, kendisinin kandırılma olasılığının çok düşük olduğunu düşünür ve genellikle güvenlik gündeme geldiğinde teknik tedbirlerden bahseder. Fakat bilgi güvenliği sağlanırken insan faktörünün payı teknik önlemlerden çok daha fazladır. Bilgi güvenliğinin en zayıf halkası, "insan faktörü"dür. Bilgisayar korsanı olan Kevin Mitnick, bunu şu sözleriyle açıklamaktadır:

"Ben nadiren teknik saldırı düzenlerim. Bilgisayar güvenliğinde insan unsuru sürekli gözden kaçırılır ve daha kolay kandırılabilir. Şirketler güvenlik duvarlarına, şifrelemelere ve bağlantı cihazlarına milyonlarca dolar yatırırlar ve bu para uçar gider çünkü; bu tedbirlerden hiçbiri en zayıf halkayı işaret etmez." (Wilding, 2006).

Bilişim güvenliğine yönelik bu saldırıların temel hedefi sistem iken, günümüzde bu tip saldırılardan farklı şekilde hedefin insan olduğu ayrı bir saldırı tipi bulunmaktadır. Bu saldırı türü ise “sosyal mühendislik” olarak isimlendirilmektedir (Akca, 2016: 112).

Sosyal mühendislik, sosyal mühendis Christopher Hadnagy tarafından “insan yaşamlarının bazı yönlerinin harekete geçmesi için ustaca manevra yaptırılması bilimi ya da sanatı” olarak tanımlanmaktadır. Sosyal mühendislik, çoğu insanın düşündüğünden daha kolaydır. Teknolojideki gelişmelerle, sosyal mühendisliğin herhangi bir yerden yapılması kolaylaşmıştır. Sosyal mühendislik, saldırganların mağdurlarından değerli bilgiler edinmelerini ve istedikleri şekilde kullanmalarını sağlar. Saldırgan, mağdur veya mağdurlar için hayati önem taşıyan bilgileri elde etmek üzere saldırı gerçekleştirir. Sosyal mühendislik saldırıları, çevrimiçi saldırılardan e-postalara ve telefon aramalarına kadar pek çok farklı biçimde ortaya çıkmaktadır (Wright, 2015).

Sosyal mühendislik saldırısının amacı sadece bir bilgi sistemine erişim sağlamak ya da kontrolü sağlamak değildir, aynı zamanda para ve diğer önemli finansal kaynakları da elde etmektir. Sosyal mühendisler, hedefleriyle güven ilişkisi geliştirmek için yeteneklerine güvenirliler (Atkins ve Huang, 2013).

Dünya’da ve ülkemizde özellikle 21.yüzyılın başından itibaren herkesin telefon sahibi olması ile beraber dolandırıcılar, kişileri telefon üzerinden kandırıp mal varlıklarını tehlikeye atmaya başlamışlardır. Özellikle kendini polis, savcı, banka memuru şeklinde tanıtan suçlular; masum vatandaşların tüm şahsi bilgilerini bilgisayar korsanları sayesinde ele geçirip kamuoyu gündemini teşkil eden konular üzerinden dolandırmaktadırlar. Dolandırılanların profilleri; eğitim seviyeleri, yaş ya da toplumdaki statüsüne bakılmaksızın çok geniş bir perspektifte dağılım göstermekte ve aralarında profesör, emekli general, savcı, yüksek rütbeli polis, öğretmen, sanatçı, ev hanımları, emekliler gibi bir çok meslek grubunu etkileyen bir mağdur havuzu oluşmaktadır (Akbal, Doğan, Varol, 2016).

İstanbul Emniyet Müdürlüğü Asayiş Şube Müdürlüğü, Yankesicilik ve Dolandırıcılık Büro Amiri Başkomiser Kıvanç Taşçı dolandırıcıların kim olduğunu şu sözlerle tanımlamaktadır:

“Vatandaşları hipnoz eden kişiler bunlar. Telefon açıyorlar size, çok güçlü bir senaryoları var. Bugüne kadar karakolun kapısından girmemiş namuslu Vatandaşlara kurdukları senaryoyu öyle bir anlatıyorlar ki, hipnoz oluyorsunuz! Ve tüm dediklerine inanmaya başlıyorsunuz. Hukuk biliyorlar, öyle terimler kullanıyorlar ki, sanıyorsunuz karşınızdaki gerçekten bir savcı ya da polis. Bir call center kuruyorlar, tüm mali bilgilerinizi size telefonda söylüyorlar. İnanırcı olmak için her yolu deniyorlar. Dolandırıcılık suçu komplike bir suç. Eğer suçlu profili ikna ediciyse bu konu da kabiliyete sahipse çok kolay bir şekilde kandırabiliyor. Zaten bu iknadan sonra ortaya çıkan bir suç tipi olduğu için farkındalık sonra oluşuyor. Mağduriyet sonrası farkındalık olduğundan ötürü teşebbüs sırasında görebilmek zor. Vatandaşın uyanık olması ve hukuki işlemleri iyi bilmesi gerekiyor. İyi niyetin suistimal edilmesi de var tabii.” <http://www.gazetevatan.com/dolandiricilar-15-gunlugune-oto-galeri-kuruyor-912310-pazar-vatan/>

Dünyanın her yerinde rastlanılan ve kişilerin binlerce lirasına mal olan bu suç, güvenlik güçlerine çeşitli sebepler yüzünden zorluklar yaratmaktadır. Bu zorlukların en belirginini ise; ne dolandırıcılık yapanların, ne de dolandırılan vatandaşların belirli bir tiplmesi olmaması ile alakalıdır (Murphy, 2017). Fakat çeşitli verilere göre yaşlı veya sosyal hayattan izole olmuş vatandaşların telefon dolandırıcıları tarafından diğer kişilere göre daha kolay kandırıldığı görülmektedir (Cross, 2016). Telefon dolandırıcılığı konusunda son yıllarda Emniyet Genel Müdürlüğü ve çeşitli sivil toplum kuruluşları tarafından farkındalık çalışmaları yapılmakta ve kamu spotu gibi tüm yazılı ve görsel medya mecralarında çalışmalar hızla yürütülmektedir.

Yapılan çalışma doğrultusunda ulaşılan kaynaklar çerçevesinde, akademik yazında özellikle telefon dolandırıcılığı konusunda yapılan incelemede herhangi bir Türkçe teze rastlanmamıştır. Dolayısıyla özellikle Türkçe literatüre bu konuda bir çalışmanın yansımaları daha sonra yapılacak akademik çalışmalara ışık tutacağı düşünülmektedir.

Bu tezin amacı, üç başlıkta toplanabilir:

1. Ana akım medyada telefon dolandırıcılığı haberlerinin incelenmesi yoluyla mağdur profilinin ortaya çıkarılması

2.Mağdurlarla derinlemesine mülakatlar yoluyla; olay, oluş biçimi, mağdur tepkileri, yasal bildirimlerde bulunma gibi faktörlerin incelenmesi

3.Yukarıda bahsi geçen gazete haberi ve yaşanmış olaylardan yola çıkarak sosyal mühendislik saldırılarına karşı farkındalık oluşturmak, vatandaşları bilgilendirmek, yeni mağduriyetlerin oluşmaması için gerekli koruyucu tedbir ve önlemlerin önerilmesidir.



2.Genel Bilgiler

2.1. Sosyal Mühendislik

Günümüzde iktisadi ya da stratejik bakımdan değer ifade etmekte olan her tür bilgi, bir saldırı hedefi haline gelmektedir. Dolayısıyla bilgilerin insanlar tarafından kullanımı yanında, bu bilgilerin korunması ve güvenli biçimde iletilmesi hususları önem kazanmaktadır. Kurumlar ve kuruluşlar hackerlara karşı çeşitli yöntemlerle savunma sergilerken, güvenlik duvarları (firewall) politikalarına odaklanmakta, internet üzerinden gelebilecek tehditlere karşı server sistemlerini kuvvetlendirmekte, kurum içi belge aktarımlarında ağ güvenliğinin sağlanmasına ilişkin tedbirlerini arttırma yoluna gitmektedir. Hiçbir bilgisayarın insan unsurundan bağımsız olmadığı göz önünde bulundurulduğunda, bilgi güvenliği hususunda sistemin en zayıf unsurunun da insan olduğu söylenebilir. Bilgi güvenliğinde insan boyutunu manipüle eden hackerlar, günümüzde sıklıkla sosyal mühendislik faaliyetleriyle güvenlik açıklarından faydalanmakta ve bu açıkları kendi çıkarları için kullanmaktadırlar. Gerek bireyler, gerekse de kurum ve kuruluşlar, bilgi güvenliği hususundaki açıkları saldırı eylemi meydana gelene kadar görememekte, sosyal mühendislik eylemlerinin hangi zafiyetlerden kaynaklanmakta olduğu çoğu zaman anlaşılamamaktadır (Bağcı, 2009: 43).

Bilgisayar ve ağ güvenliği bakımından sosyal mühendislik, insan davranışlarında bulunan çeşitli unsurları güvenlik açıkları şeklinde değerlendirip, bu açıklardan yararlanma yöntemi ile güvenlik süreçlerini aşmak suretiyle sistem yöneticisi veya kullanıcıların yetkilerine erişim tekniklerini kapsamakta olan bir terimdir (İlbaş, 2009: 31).

2.1.1. Sosyal mühendisliğin tanımı

Teknoloji günümüzde gerek bireyler gerekse de kurumlar tarafından son derece yoğun bir şekilde kullanılmaktadır. Teknoloji kullanımı hususunda özellikle son yıllarda yaşanmış olan artış neticesinde teknolojinin güvenliği konusu da büyük bir önem kazanmış durumdadır. Bu durumda da bilişim güvenliği kavramı ortaya çıkmıştır. Bilişim güvenliği, sanal ortam

üzerinde saklanmakta olan verilerin erişim izni bulunmayan bireyler tarafınca ulaşılmasını engellemek, sistemlere üçüncü kişilerin girmesini önlemek, aktarılan verilerin problemsiz biçimde karşı tarafa gönderilmesini sağlamak vb. konuları içermektedir. Gerek bireyler gerekse de kurumlar tarafından ihtiyaç duyulan bilgisayar tabanlı yazılımlar devamlı şekilde saldırılara maruz kalmaktadır. Bu saldırılarda temel maksat, hedef sistemi tamamıyla ele geçirme, geçici veya kalıcı biçimde hizmet dışı bırakma şeklindedir. Bilişim güvenliğine yönelik bu saldırıların temel hedefi sistem iken, günümüzde bu tip saldırılardan farklı şekilde hedefin insan olduğu ayrı bir saldırı tipi bulunmaktadır. Bu saldırı türü ise sosyal mühendislik olarak isimlendirilmektedir (Akca, 2016: 112).

Sosyal mühendislik; etkileme, zorlama, aldatıcı ilişkiler geliştirme; sorumluluğu, etik değerleri, dürüstlüğü veya bağlılığı azaltma maksatlı metodlar kullanmak suretiyle bireyleri gizli bilgi vermeleri ya da erişim sağlamaları hususunda aldatma sürecine verilen isimdir (Bağcı, 2009: 43). Sosyal mühendislik, çalışanlar ile tüketicileri kandırmak suretiyle ağlar ya da hesaplara ulaşmak üzere bunları kullanma sanatıdır (Conteh and Schmick, 2016'dan akt. Acılar ve Baştuğ, 2016: 291).

Psikoloji ve güvenlik konuları çerçevesinde pek çok farklı biçimde tanımlanabilmekte olan sosyal mühendislik, temel olarak insanları kullanmak suretiyle bir kurumun güvenliğini kırmak şeklinde belirtilmektedir (Barışkan, 2017: 3). Bir başka tanımda; sosyal mühendislik, insanları aldatma sanatı şeklinde ifade edilmektedir. Bu bağlamda sosyal mühendislik, siber suçlular tarafından kullanılan popüler bir araç niteliğindedir (Trend Micro: 1).

2011'de yapılan bir tanımlamaya göre ise; sosyal mühendislik, bilişsel önyargılar şeklinde bilinmekte olan insan mantığına dair açıklardan yararlanarak arzu edilen bilgilere ulaşmak üzere kötü niyetli saldırganlar tarafınca kullanılmakta olan bir tekniktir (Luo, Brody, Seazzu and Burd, 2011'den akt. Acılar ve Baştuğ, 2016: 291). Sosyal mühendislik, organizasyon güvenliğinin insanlar ile etkileşime girilmek suretiyle kırılması biçiminde veya

insanların ortak duygularındaki boşluklardan fayda sağlamak olarak ifade edilebilmektedir (Bağcı, 2009: 43).

Sosyal mühendisler teknolojiyi kullanarak veya kullanmaksızın bilgi elde etmek üzere insanlardan yararlanmakta ve etkileme ile ikna tekniklerini kullanmaktadırlar. Bu bağlamda sosyal mühendislik, normal şartlarda insanların tanımadıkları bir birey için yapmayacakları şeyleri yapmalarını sağlama sanatı, teknoloji kullanımından ziyade insanların hileyle kandırılmak suretiyle bilgi elde edilmesi şeklinde tanımlanabilmektedir (Tatar, 2011: 8-9). Sosyal mühendislikle gerçekleştirilen saldırılar, hedef olarak seçilmiş olan bireyi kandırıp bu bireyin dikkatsizliğinden faydalanmak suretiyle normal koşullarda ulaşamayacağı bilgilere erişerek sisteme veya bireye zarar vermeyi amaçlayan saldırılardır (Akca, 2016: 112).

Federal Bureau of Investigation (Federal Soruşturma Bürosu) tarafından bir dönem en çok arananlar listesinde yer alan bilgisayar korsanı Kevin Mitnick'e göre sosyal mühendislik, insanların saflıklarının kullanılması suretiyle bireyleri etkileyip, ikna edip, manipüle edip kritik öneme sahip bilgilerin ele geçirilmesidir (Mitnick ve Simon, 2006: 303). Sosyal mühendislik, bilgi güvenliği hususunda potansiyel bir tehdit niteliğine sahip olup, bilgi güvenliğinde teknolojik tehditler ile birlikte eşit derecede öneme sahiptir (Luo et al., 2011'den akt. Acılar ve Baştuğ, 2016: 291).

Sosyal mühendislik; kişiler arası, kişi ile kurum arası ve/veya kurumlar arası iletişim süreçlerinde meydana gelen açıklardan veya insan davranışlarında bulunan istismara açık alanlardan yararlanmak suretiyle güvenlik süreçlerini etkisiz duruma getirme metotlarına dayalı yasadışı müdahale süreçleri şeklinde tanımlanabilmektedir (Bağcı, 2009: 43). Teknolojik denetim dışında ve insan doğasına konu olduğundan sosyal mühendislik, kuşkusuz bilgi sistemleri güvenlik yönetimi alanında en zayıf halkalardan birisi konumundadır (Luo et al., 2011'den akt. Acılar ve Baştuğ, 2016: 291).

İnsanlar genelde sahip oldukları değerli bilgilerin farkında değildirler ve bu sebeple bu değerli bilgileri koruma hususunda son derece dikkatsiz bir şekilde hareket etmektedirler. Bu bağlamda sosyal mühendislik, internet üzerinde insanların zafiyetlerinden yararlanarak birtakım ikna ve kandırma teknikleriyle arzu edilen bilgilerin ele geçirilmeye çalışılması şeklinde ifade edilmektedir ve insanların karar alma süreçlerini değiştirmeye ilişkin teknikler içermektedir. Sosyal mühendisler saldırılarını güven üzerine kurmakta, birey üzerinde baskı kurmak suretiyle bireyin korkmasını sağlamakta, bilgiyi açığa vurmaya üzere hedefleri cezbetmektedir (Çatak, 2016: 4-5).

Bilgi güvenliği sistemlerinde en zayıf unsurun insan olduğu varsayımına dayanmakta olan sosyal mühendislikte saldırgan, bireylerin eğilimleri ile kişisel ilişkilerden yararlanarak gizli bilgilere ulaşmaya çalışmaktadır. Sosyal mühendis, bireylerin sanal ortam üzerinde paylaşmış olduğu herkes tarafından ulaşılabilen kişisel verileri, tek başına bir gizlilik içermemesine karşın, farklı kaynaklar üzerinden temin etmek suretiyle sistematik şekilde bütünleştirmekte ve gizlilik içeren ya da önem ve değer arz eden bilgi haline dönüştürmektedir (Bayraktar, 2014: 138).

Sosyal mühendislik kavramının farklı bir açılımı olarak “tersine sosyal mühendislik” kavramından da literatürde bahsedilmektedir. Bu kavram ise, sosyal mühendislik yöntemleriyle saldırıya uğrayan kurbanın, yardım almak üzere farkında olmadan sisteme saldırıda bulunan sosyal mühendis ile iletişim kurması şeklinde tanımlanmaktadır (Mitnick, 2002’den akt. İlbaş, 2009: 31).

Sosyal mühendislik ile hacking arasında çeşitli farklılıklar bulunmaktadır. Teknik yollarla, yasaklanmış sistemlere girmeye çalışma anlamına gelen hacking eylemlerinde hackerlar güvenlik açıklarından faydalanarak avantaj elde etmeye çalışmaktadır. Sosyal mühendisler ise normal yollar ile elde edemeyecekleri şifre, kripto anahtarı, kullanıcı ID’si gibi birtakım bilgileri, insanları manipüle etmek suretiyle ele geçirmeye çalışmaktadır. Dolayısıyla

sosyal mühendislik de, teknik yollar kullanılması suretiyle elde edilmesi oldukça güç olan bilgilerin ele geçirilmesi hususunda faydalanılan bir yöntem şeklinde karşımıza çıkmaktadır (Bağcı, 2009: 43).

2.1.2. Sosyal mühendisliğin amacı ve hedef kitlesi

Günümüzde bir değere sahip olan her tür bilgi, bir saldırı hedefi durumuna gelmektedir. Bu sebeple hem bireyler hem de kurum ve kuruluşlar sosyal mühendislik saldırılarının hedefi durumuna dönüşmektedir. Sosyal mühendislik saldırıları neticesinde bireyler ve/veya kurumlar birtakım risk durumları ile karşılaşmaktadır. Başkalarına yanlışlıkla söylenen bir şifre, kişi veya kurumlar ile ilgili oldukça hassas bilgilerin dışarı sızmasına sebep olabilmektedir (Bağcı, 2009: 43-44). Bu bağlamda sosyal mühendisliğin kullanmakta olduğu en büyük silah, insan zafiyetleri olup; insan, bilgi güvenliğinin en zayıf halkası konumundadır (Tatar, 2011: 10).

Sosyal mühendislik saldırılarının birtakım amaçları bulunmaktadır. Bu amaçlardan biri, hedeflenen bir sistem veya ağ yapılanmasını bozarak kullanılamayacak duruma getirmektir. Başka bir amaç; kurumsal ağ yapısı, işletim sistemi versiyonu, kimlik hırsızlığı, kripto anahtarları, yazılım versiyonları, çalışanların ve yöneticilerin kişisel bilgileri, şifreler ve saldırıda kullanılacak her tip materyalin toplanmasıdır. Bir diğer amaç ise kişi veya kurumun itibarı ile güveninin zedelenmesi olabilmektedir. Sosyal mühendislik eylemleri sebebiyle zarara uğrayan kişi ve kurumlar aynı zamanda bir itibar ve güven kaybına da uğramaktadır. Burada kaybedilen itibar ile güvenin bedeli ise, en başta alınması gerekli olan tedbirlerin maliyetlerinden çok daha fazla olmaktadır (Bağcı, 2009: 44). Sosyal mühendis isimli aldatma sanatçılarının bir başka amacı ise, bilgiye ulaşma yetkisi bulunan kullanıcılar vasıtasıyla güvenlik teknolojilerinin atlatılmasının (by-pass) sağlanmasıdır (Vural, 2007: 8). Çatak (2016: 22) ise sosyal mühendislik saldırılarının temel amaçlarını hedef kurum ya da kişi yapısı, kurumsal ağın yapısı, çalışanların/yöneticilerin kişisel bilgileri, parolalar ve saldırıda kullanılacak her tür materyalin toplanması şeklinde ifade etmektedir.

Sosyal mühendisler, elde ettikleri parolalarla erişimi kısıtlı olan çeşitli belgeleri indirmekte ya da bant genişliği, işlemci zamanı, disk alanı vb. sınırlı kaynakları kullanmak suretiyle hizmet hırsızlığında bulunmaktadır. Kişi veya kurumlara ilişkin bilgileri bu şekilde elde eden sosyal mühendisler, bu bilgileri daha fazla suiistimal etme hususunda değerlendirebilecekleri gibi, bu bilgileri satarak kişi ya da kurum aleyhine de kullanabilmektedir. Ayrıca sosyal mühendisler, kişinin veya kurumun bu bilgilere erişimlerini de istedikleri takdirde engelleyebilmekte, sistemde kayıtlı olan bilgileri silebilmekte ya da bilgilerin doğruluğunu etkileyecek biçimde çeşitli değişiklikler gerçekleştirebilmektedir (Bağcı, 2009: 44). Sosyal mühendisler, bireysel ve/veya kurumsal sosyal uygulamalar ile elektronik posta hesaplarının parolalarını kırabilmekte, sistemlere izinsiz şekilde sızabilmekte, ulusal ve uluslararası güvenlik sırlarına erişebilmekte ve ulaştıkları bilgileri çalabilmektedirler (Kara, 2013: 10).

Sosyal mühendislik eylemlerinin temel hedef kitlesi durumunda bulunan kurum çalışanları şu şekilde ifade edilmektedir (Acılar ve Baştuğ, 2016: 292; Bağcı, 2009: 44-45):

- i. *Doğrudan erişilebilir çalışanlar:* Yaptığı iş gereğince dışarıdan gelen kişiler ile doğrudan teması bulunan çalışanlardır. Danışma görevlileri, güvenlik görevlileri, telefon santrali görevlileri buna örnektir.
- ii. *Üst düzey yöneticiler ve yetkili çalışanlar:* Kurum içerisindeki görevleri gereğince zorunlu şekilde ayrıcalıklı yetkiye sahip bulunan ya da gizli bazı bilgilere birtakım sebeplerle erişim hakkı bulunan çalışanlardır. Kendilerine sistemde sınırsız erişim yetkisi sağlayan parolalar verilen, fakat eksik bilgilendirme ya da mesai yoğunluğu sebebiyle parolaları hatırlama hususunda zorluk çeken, bu sebeple oldukça basit parolalar kullanmakta olan, parolaları bir yerlere yazmak suretiyle hatırlamaya çalışan veya yanında çalışan bireylere parolalarını veren yöneticiler, sosyal mühendislerin doğrudan hedefi durumuna dönüşmektedir.

- iii. *Zaafları bulunan, aldatılmaya ve ikna edilmeye müsait çalışanlar:* Kuruma karşı zayıf bir bağlılığı bulunan, çeşitli zaaflara sahip, aldatılmaya ve ikna edilmeye uygun durumdaki her düzeyde çalışan personel bu gruba girmektedir.
- iv. *Yararlı olma konusunda arzulu sempatik personel:* Diğer bireylere yardım etmekten zevk duyan, görev ve yetkisini aşmak suretiyle yardım ve destek talebinde bulunan kişilerin yardımına koşan, sempatik davranışlar sergilemek suretiyle yetki ve itibar sağlamaya çalışan personel, bu gruba girmektedir. Sosyal mühendisler, bu gibi personelden giriş hakkı ya da bir hesaba giriş hususunda yardım isteyerek işe başlamakta, işin uzmanına danışmış gibi davranarak bu bireylerden hassas ve değerli birtakım bilgileri elde etmeye çalışmaktadırlar.
- v. *Desteğe muhtaç konumdaki çalışanlar ya da kullanıcılar:* Kurumsal hizmetlerden faydalandıklarından dolayı sisteme erişim hakkı tanınan fakat sistemle ilgili yeterince bilgisi bulunmayan, bu sebeple yardıma gereksinim duyması halinde gerçekten kurumsal destek sağlayan çalışanlar ile sosyal mühendisleri ayırt edemeyen çalışanlar ve kullanıcılar bu grupta yer almaktadır.
- vi. *Düşük bağlılık düzeyine sahip çalışanlar:* Kurumsal amaçlar ile politikaları kavrama hususunda zorlanan, özellikle alt kademelerde görev yapan memurlar, güvenlik görevlileri, resepsiyon görevlileri, hizmetliler gibi çalışanlar bu gruptadır. Sosyal mühendisin sorduğu sorular neticesinde ne elde etmek istediğini anlama hususunda kabiliyetli olmayan, yaptığı görevin gerekleri ile kendilerine sorulan sorular arasında bulunan bağlantıyı tam olarak kavrayamayan çalışanlardır.

2.1.3. Sosyal mühendislik saldırı yöntemleri

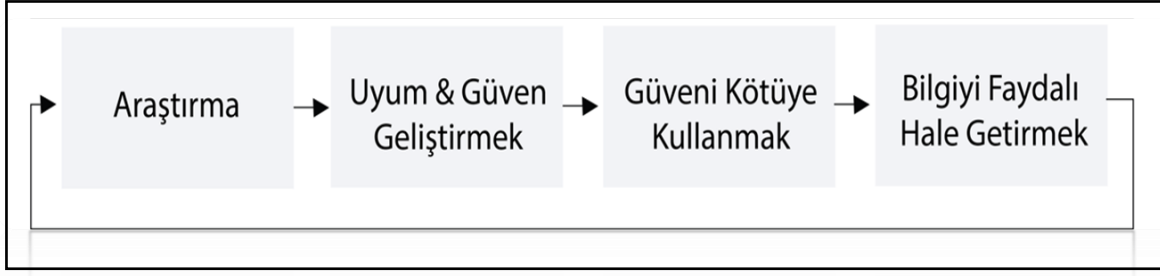
Sosyal mühendislikle gerçekleştirilen saldırılar tamamıyla karşıda bulunan kişiyi aldatmaya ilişkin olduğundan, bu konuda oldukça fazla yöntem ve teknik bulunmaktadır. Bir saldırganın sosyal mühendislik tabanlı saldırılarda kullanabileceği teknikler teknoloji

kullanımını içermektedir. Farklı saldırı yöntemlerinin anlaşılması, bu saldırıların nasıl gerçekleştiğini ve bir sosyal mühendislik saldırısına kurbanların düşürülebilmesini sağlamak için saldırganın odaklanmasını açıklamaktır. Saldırganların nasıl çalıştıklarını ve sonuçların ne anlama geldiğini anlamak, farkındalık konusunda daha iyi bir algı oluşturmaktadır. Saldırganın yüz yüze etkileşime ihtiyacı yoktur. Saldırganların çoğu, sosyal mühendislik taktiklerini dünyanın her yerinden kullanabilir (Akca, 2016: 112).

Sosyal mühendislik eylemleri kapsamında kullanılmakta olan tekniklerin pek çoğu, bireylerin psikolojik birtakım özelliklerinin istismar edilmesine dayanmaktadır (Bağcı, 2009: 43). Bütün sosyal mühendislik yöntemleri, insan davranışlarında bulunan önyargılar üzerine kurgulanma olup, bu önyargılar ise insana ilişkin sistem açıkları şeklinde ifade edilmektedir. Sosyal mühendislik yöntemlerinden faydalanan saldırgan, insan davranışları üzerinde etkisi bulunan önyargıları harekete geçirecek teknikleri büyük bir beceriyle kullanabilen kişidir (Türkiye Bankalar Birliği, 2015: 5).

En çok bilinen saldırı modeli; Kevin Mitnick'in "*Aldatma Sanatı: İnsan Güvenliği Unsurlarını Kontrol Etmek*" adlı kitabında anlatılan sosyal mühendislik saldırı döngüsüdür. Mitnick'in saldırı modeli dört aşamalıdır: Araştırma, uyum ve güven geliştirme, güveni kullanma ve bilgiyi kullanma (Mouton ve ark., 2014). Sosyal mühendislik saldırısını etkili bir şekilde tamamlamak için kullanılan herhangi bir teknik, bu dört farklı aşamanın kullanılmasını gerektirmektedir. İlk aşama, saldırganın kurban hakkında olabildiğince fazla bilgi topladığı araştırma aşamasıdır. Uyum ve güven geliştirme aşaması olan ikinci aşamada; saldırının gerçekleştirilmesi için iyi bir uyum sağlamak ve kurbanların güvenini kazanmak şarttır. Üçüncü aşama güveni sömürme aşamasıdır. Saldırgan şimdi kurbanların güvenini kazanmış ve onlara karşı kullanmıştır. Dördüncü ve son aşama ise saldırganın saldırı kapsamında aldığı tüm bilgileri kullanma aşamasıdır.

Şekil 1, farklı aşamalarının akışını ve işleyişini göstermektedir:

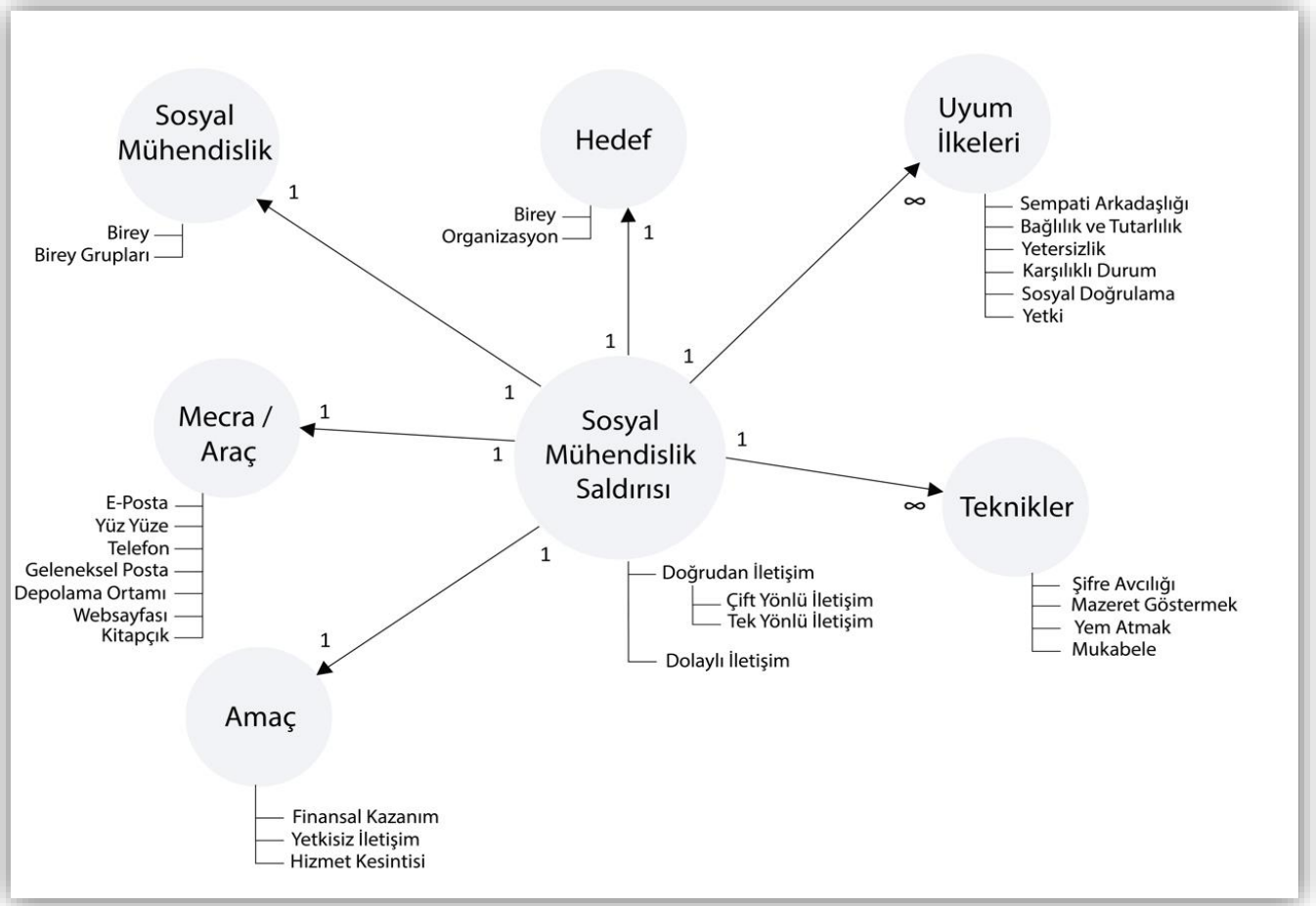


Şekil 1: Kevin Mitnick'in sosyal mühendislik saldırı döngüsü "Aldatma Sanatı: İnsan Güvenliği Unsurunun Kontrol Edilmesi ”

Kaynak: Mouton ve ark., 2014, Güney Afrika Bilgi Güvenliği, IEEE, s. 2

Ontolojik model, bir sosyal mühendislik saldırısının doğrudan ya da dolaylı iletişimi kullandığını ve bir sosyal mühendise, bir hedefe, bir ortama, bir amaca, bir ya da daha fazla uyum ilkesine ve bir ya da daha fazla tekniğe sahip olduğunu tanımlamaktadır (Mouton ve ark, 2014). Doğrudan iletişim, konuşmaya katılan iki veya daha fazla kişi olduğunda geçerli olmaktadır. Doğrudan iletişim bir e-posta veya telefon görüşmesi şeklinde olabilir. Bununla birlikte; dolaylı iletişim, saldırgan ve kurban arasında hiçbir iletişimin olmadığı süreci içermektedir. Bu, kurbanın aldığı bir USB cihazı sayesinde kurulabilmektedir. Kurbanın USB diske ücretsiz bir tanıtım kapsamında erişebilmektedir.

Ontolojik model aşağıda Şekil 2’de gösterilmektedir:

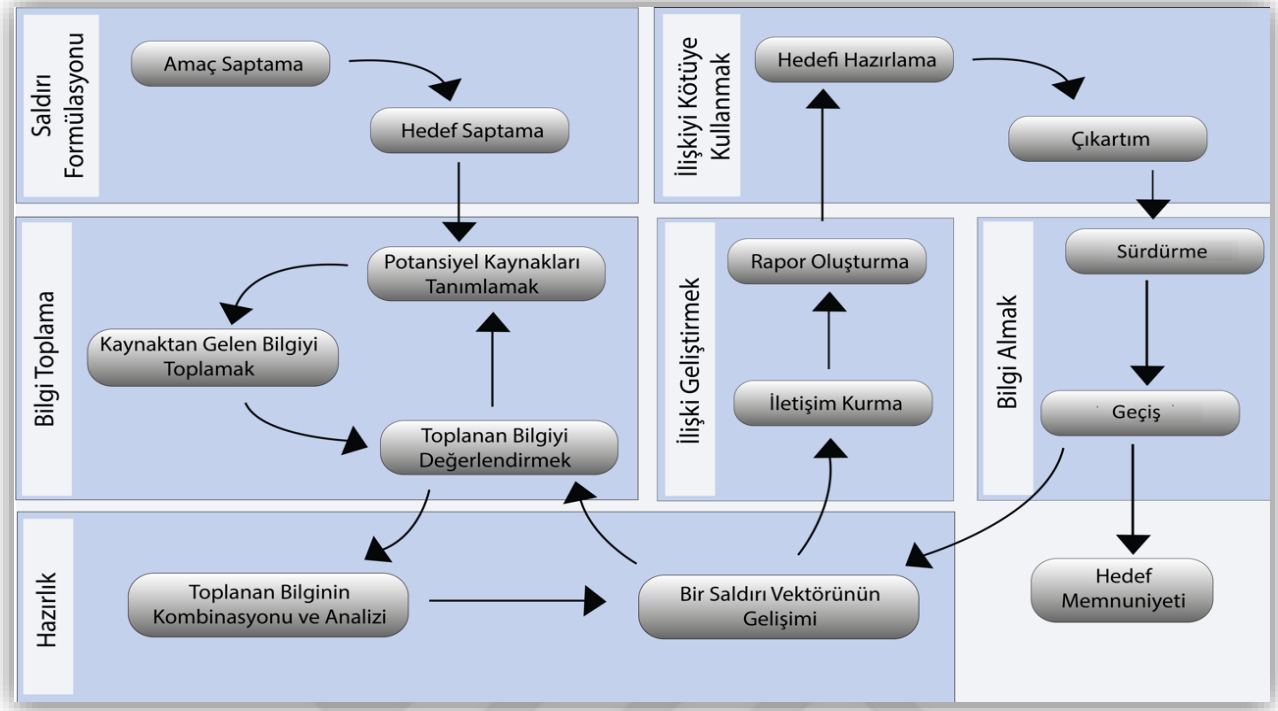


Şekil 2 : Bir sosyal mühendislik saldırısının ontolojik modeli "Aldatma Sanatı: İnsan Güvenliği Unsurunun Kontrol Edilmesi ”

Kaynak: Mouton ve ark., 2014, Güney Afrika Bilgi Güvenliği, IEEE, s. 2

Bir başka model, Mitnick'in mevcut sosyal mühendislik saldırı modeline bir ilave önermektedir. Mitnick'in saldırı döngüsü kapsamlıdır ve bazı yönlerden yoruma açıktır (Mouton ve ark., 2014).

Şekil 3 yeni önerilen sosyal mühendislik saldırı çerçevesini göstermektedir:



Şekil 3: Sosyal mühendislik saldırı çerçevesi "Aldatma Sanatı: İnsan Güvenliği Unsurunun Kontrol Edilmesi "

Kaynak: Mouton ve ark., 2014, Güney Afrika Bilgi Güvenliği, IEEE, s. 3

Sosyal mühendisler insanları çeşitli şekillerde aldatarak kişi ve/veya kurumlara ilişkin bilgileri fark ettirmeksizin almaya çalışmakta ve bu hususta değişik birtakım saldırı tekniklerinden faydalanmaktadır. En iyi bilinen fiziksel nitelikli sosyal mühendislik yöntemleri arasında kurumlara personel şeklinde girmek, personel ile arkadaş olmak, teknik servis veya destek alınan bir kuruluştan arıyormuş gibi davranarak bilgi elde etmek, hedef birey ile dost olmak suretiyle bu bireyin zaaflarından faydalanmak, hedef bireylerin parolalarını ele geçirmek üzere elektronik postalarına tuzak postalar göndermek, sistem sorumlusu olduğunu söylemek suretiyle kullanıcıların parolalarını elde etmeye çalışmak, teknisyen kılığında kuruma girmek, çöpleri karıştırmak suretiyle bilgi elde etmek gibi teknikler bulunmaktadır (Bağcı, 2009: 45).

Fiziksel nitelikli sosyal mühendislik yöntemleri içerisinde bilgisayar tabanlı olarak gerçekleştirilen saldırılar, genel olarak teknoloji kullanmak suretiyle kurban yakalama maksatlı yapılan saldırılardan meydana gelmektedir. Türkiye’de bu tarz saldırılar, sıklıkla gündeme gelmektedir. İşyerinde gerçekleştirilen saldırılar ise genel olarak en zor saldırı türüdür. İşyerinde yapılan saldırılarda sosyal mühendisin bireysel şekilde bir personelin yerine geçmesi gereklidir. Genellikle alt kademelerde çalışmakta olan bu personel, diğer personelin ve şirketin önem arz eden bilgilerini kulak kabartmak suretiyle alabilmektedir. Özellikle ülkemizde son yıllarda çokça duyulan bir başka saldırı türü ise, telefonla gerçekleştirilen sosyal mühendislik saldırılarıdır. Kendilerini müşteri hizmetleri, belediye elemanı, zabıta, savcı, asker, polis, sağlık görevlisi vs. biçimde tanıtmakta olan kişiler kurbanlarını tehdit ederek veya yardım etme bahanesiyle dolandırmakta ve kişisel bilgileri ele geçirmektedir. İnternet üzerinden ise sosyal mühendisler kurbanın elektronik postasına anlık mesajlaşma platformları üzerinden ya da sosyal medya üzerinden gönderilen mesajlar ile kişinin bilgilerini isteme üzerine gelişmektedir. Bu tip saldırılara ise genel olarak “oltalama” ismi verilmektedir (Barışkan, 2017: 4). Oltalama, bir insanın merakını sömüren bir sosyal mühendislik biçimidir. Oltalama bazen diğer sosyal mühendislik saldırılarıyla karışır; bununla birlikte, ana karakteristiği, hackerların kurbanları aldatmak için kullandıkları bir iyilik vaadidir (Paganini, 2017). Oltalama tüm fiziksel ortamlar kullanılarak yapılır. Ancak, oltalamayı diğer sosyal mühendislik türlerinden ayıran şey, hackerların kurbanlarını ikna etmek için bir eşya ya da mal vaat etmesidir (Bisson, 2015).

Fiziksel nitelikli sosyal mühendislik yöntemlerini İlbaş (2009: 33-35) şu şekilde ifade etmektedir:

- i. *Sahte (fake) elektronik posta:* Genel olarak elektronik posta hizmetlerindeki kullanıcı parolalarına erişmek üzere kullanılmakta olan sosyal mühendislik tekniğidir. Gönderildiği elektronik posta sunucusu tarafından bir hata neticesinde

kullanıcıya parola sorması hususunda hazırlanmış olan internet sitesinin görünüş olarak kopyasının açılabilir bir internet bağlantısı şeklinde gönderilmesi biçiminde gerçekleştirilmektedir. Açılan sahte internet sitesine girilen parola bilgileri, sunucu yerine “ortadaki adam” (man in the middle) şeklinde isimlendirilen sosyal mühendise ulaşmaktadır. Sahte elektronik posta saldırılarının sayısı yılbaşı, bayram vb. özel günlerde bilhassa artmakta ve genel olarak elektronik kart, promosyon duyurusu biçiminde düzenlenmek suretiyle kullanıcıların dalgınlıklarından yararlanma metodu tercih edilmektedir.

- ii. *Oltacılık (Phishing – Password Harvesting Fishing)*: Genel olarak banka ve finans kuruluşlarının internet sayfalarından gönderilmiş gibi hazırlanmakta olan ve kullanıcıları tedirgin edecek ifadelerle beraber ilgili kuruluşun sahte internet sitesi bağlantısını içermekte olan elektronik posta iletilerinden oluşmaktadır. Bu iletilerin açılması halinde kullanıcılar tarafından girilen bilgiler, ortadaki adam şeklinde tanımlanmakta olan saldırgan aktarılmakta, kullanıcıya ise sistemin geçici şekilde servis dışı olduğu hususunda bir mesaj iletilmektedir.
- iii. *Elektronik dolandırıcılık (cyberfraud)*: Sosyal mühendislik, çeşitli sistemlere yetkisiz şekilde erişme ve kişisel bilgileri ele geçirme maksadı taşımakta olduğu gibi, haksız kazanç elde etme hususunda da kullanılabilir. Birtakım sürekli şekilde tekrarlanan senaryolar vasıtasıyla gerçekleştirilen saldırı eylemlerinin en yaygın örnekleri arasında yeşil kart, loto, kara para transferi, sahte ürün tuzakları bulunmaktadır.
- iv. *Bilgisayar virüsleri*: Çeşitli bilgisayar virüsleri, yayılma hızlarını arttırmak üzere sosyal mühendislik yöntemlerinden faydalanmaktadır. İlk örneği Win32/Sober ismini taşıyan bu virüsler, yerleştikleri bilgisayar sistemlerinde yer alan belge

isimlerini incelemek suretiyle bilgisayar kullanıcısının iş ya da hobi nitelikleri ile uyumlu bir adla kopyalarını adres defterinde bulunan bireylere göndermektedir.

v. *Yığın elektronik postalar (spam mail)*: Yığın elektronik postaların global bir probleme dönüşmesi neticesinde kullanıcıların elektronik postaları açmaksızın silme davranışı geliştirmeleri sebebiyle, posta göndericileri sosyal mühendislik teknikleri uygulamaya başlamıştır. Elektronik postaların konu başlıklarında “re:” ibaresinin bulunması, bir başvurunun tamamlanması veya bir hizmetin süresinin sona ermesine yönelik sahte mesajların bulunması vb. örnekler, yığın elektronik postaların yayılması konusunda sosyal mühendislik tekniklerinin uygulama örneklerini teşkil etmektedir.

vi. *Elektronik posta aldatmacaları (hoax)*: Elektronik posta adreslerini yığın elektronik posta gönderen kişi ve kurumlara temin etmek üzere hazırlanmış olan sahte içeriğe sahip elektronik postalarda sosyal mühendislik yöntemleri yaygın şekilde kullanılmaktadır. Bu tip elektronik postalar, toplumsal bakımdan tepki oluşturmaya hedeflenen aldatıcı, yanlış bilgiler içermekte ve genel olarak bu postaların son bölümlerinde çok sayıda kişiye aktarılması hususunda telkinler bulunmaktadır. Bir ülke veya kuruma ilişkin gerçek dışı bilgiler, sağlığa ilişkin tehditler, kan aranması, zor durumda bulunan bireylere yardım talebi vb. türleri bulunmakta olan elektronik posta aldatmacaları uzun senelerdir faydalanılmakta olan etkili bir yöntem konumundadır.

Acılar ve Baştuğ (2016: 292-293) ile Balcı (2018) ise son yıllarda sıklıkla karşılaşılmakta olan sosyal mühendislik saldırı yöntemlerini şu şekilde özetlemektedir:

i. *Sahte senaryolar uydurmak (Pretexting)*: Hedefteki bireyin kişisel ya da işe ilişkin bilgilerini ele geçirmek üzere bireyi hiç şüphelendirmeyecek biçimde saldırgan tarafınca inandırıcı sahte senaryoların üretilmekte olduğu yöntemdir. Özellikle

telefonla gerçekleştirilen saldırılarda bu yöntemle başvurulmaktadır. İnternet üzerinden ya da saldırı hedefi olan bireyin yakın çevresinden edinilen bilgiler çerçevesinde saldırgan, hedef bireyle temasa geçmektedir. Korku uyandırmak, yetkili biri gibi davranmak, işe yeni başlamış biri gibi davranmak, aciliyeti vurgulamak gibi davranışlarla farklı senaryolar üreten saldırgan, bireyleri kandırarak saldırı hususunda yararlanabileceği bilgiler elde etmeye çalışmaktadır.

- ii. *Oltalama saldırıları (Phishing)*: Hedef bireye ilişkin parola, kart bilgileri vb. hassas ve değerli bilgileri genel olarak elektronik posta aracılığıyla aldatarak ele geçirme yöntemidir.
- iii. *Tuzak donanımlar (Baiting)*: Elektronik postalar yerine USB, DVD, CD gibi donanım cihazlarına zararlı yazılımlar yüklenmek suretiyle gerçekleştirilen saldırı tipidir.
- iv. *Çöp karıştırmak (Dumpster diving)*: Değerli bilgileri çöpte araştırmayla ilintilidir. Bir sistemi ya da bir kullanıcının potansiyel yararlı bilgilerini ele geçirmek üzere bir köşeye atılmış kağıt, CD vb. öğeleri çöp torbasından ayırtılmaya ilişkin yöntemdir.
- v. *Omuz sörfü ve kulak misafirliği*: Kullanıcı giriş bilgileri gibi personele ilişkin verileri ele geçirmek üzere omuz üzerinden başkasının klavye veya ekranlarına bakmak vb. doğrudan gözlem tekniğine dayalı yöntemdir. Bu yöntemde çalışan birey konuşturulmak suretiyle dikkatinin dağıtılması, başarı oranını arttırmaktadır. Bunun yanında, kulak misafirliği yapılmak suretiyle çalışanlar gizli bir şekilde dinlenerek, bilgiler herhangi bir muhtemel saldırı hususunda kullanılabilir. Bu yöntemin yanında, kulak misafirliği yapılmak suretiyle çalışanlar gizli bir şekilde dinlenerek, bilgiler herhangi bir muhtemel saldırı hususunda kullanılabilir.
- vi. *Tersine sosyal mühendislik*: Hedef kişiyle doğrudan bir ilişki kurmak yerine, saldırganın hedef bireyi güvenilir bir kaynak olduğuna ikna etmek suretiyle hedef bireyle yakın ilişki kurmaya çalışmasıdır. Bu yöntem; sabotaj, bildirme ve yardımcı olma şeklinde üç aşamadan oluşmaktadır. Birinci aşamada kurumun bilgisayar

sistemine sabotaj yapılmakta ve kurumun bilgisayar ağından hedef bireylere hileli yazılım uygulamaları bulaştırılmaktadır. İkinci aşamada saldırgan, hedef bireye bu sorunu çözebileceğini bildirmektedir. Üçüncü aşamada ise, hedef yardım istediğinde saldırgan kendisinin sebep olduğu sorunu çözmektedir.

- vii. *Başka bir siteye yönlendirme (Pharming)*: Hedefteki kişinin bilgisayarının host dosyasının değiştirilmesi ya da DNS sunucusunun sömürülmesi suretiyle sahte bir domain kaydı oluşturularak, yasal siteye ilişkin bütün girişlerin direkt olarak sahte siteye yönlendirildiği pasif bir saldırı yöntemidir.
- viii. *Sesle/telefonla oltalama (Vishing)*: Saldırganların, IP üzerinden ses (VoIP) uygulamasından faydalandığı yeni bir sosyal mühendislik saldırı yöntemidir. Bu yöntemde, güvenilir bir kullanıcıya geçerli bir telefon bankacılığı hizmeti gibi görünen bir numarayı aramasını bildiren sesli mesaj gönderilmekte ve bu neticede kullanıcının gerçekleştirdiği aramaya saldırgan tarafınca müdahalede bulunmaktadır. Doğrulama hususunda telefonda girilen banka hesap numaraları ya da parolalar çalınmak suretiyle arzu edilen bilgilere erişilmektedir.

Sosyal mühendisler seçmiş oldukları hedef kişilerle ilgili olarak birtakım psikolojik saldırı tekniklerden de yararlanmaktadır. Bu tekniklerden önem arz edenleri şu şekildedir (Barışkan, 2017: 4-6; Acılar ve Baştuğ, 2016: 291; Bağcı, 2009: 45-46; İlbaş, 2009: 32-33):

- i. *Otorite*: Bireyleri kandırmak üzere üst düzey bir yetkili (kamu görevlisi, kolluk kuvveti gibi) ya da itibar sahibi bir müşteri olduğuna kişiyi ikna etmek, en çok faydalanılan tekniklerden birisidir (Bağcı, 2009: 45). Bu doğrultuda sosyal mühendis, hedefinde bulunan kişiye otoriter bir kimlikle yaklaşmakta ve kişisel bilgiler ve/veya parola elde etmek üzere kurban farkına varmadan adli bir soruşturmaya maruz kaldığını ve hesap bilgilerinin elde etmiş olan bir kişi ya da grup

tarafından zor durumda bırakılmış olduğunu ifade ederek bu bilgileri almaya çalışmaktadır (İlbaş, 2009: 32).

- ii. *Bağlantı ve benzerlik:* Hedef bireylerle yakın bağlantıya geçilmek, kişisel ilişkiler kurulmak suretiyle çeşitli ipuçları elde etmeye çalışılmasıdır. Bireyler kendilerine benzeyen diğer bireylere yakınlık duyduğundan, bu durum sosyal mühendislerin de yararına olmaktadır (Bağcı, 2009: 45). Bu doğrultuda sosyal mühendisler hedef bireyin çeşitli ilgi alanları doğrultusunda ilişkiler kurmakta, ardından kişiye güven duygusu vererek onu ikna etmeye çalışmaktadır (İlbaş 2009: 32).
- iii. *Mukabele etmek:* Yapılan bir iyilik hususunda bir karşılık önerilmesi anlamına gelmektedir. Bu hususta sosyal mühendisler, hedef seçtikleri bireylerle güvenilir bir iletişim ortamı geliştirip, çeşitli küçük etkileşimler vasıtasıyla ilişki kurmakta ve güven ilişkisinin sömürüleceği zamanı beklemektedir.
- iv. *Birbirine göre ayarlama:* Hedef seçilen bireyle çatışma durumuna girilmemesi gerektiğinden, ilişki ortamının gerektirdiği ses tonuyla zekice ve sabırlı bir sunuş yapılmasını ifade etmektedir. Sinirli davranışlar, emir tümcelerinin kullanılması ya da bir siparişte bulunma şeklinde kişiye talimat verilmesi bu hususta sosyal mühendis tarafından tercih edilmemektedir. Bu sebeple sosyal mühendisler rica etme, uydurma bir durum belirleme, kişisel ikna vb. metotlara daha çok başvurmaktadır.
- v. *Uydurma durum:* Bir olay ya da bir organizasyonun niteliği çerçevesinde elde edilen bilgiler vasıtasıyla üretilen suni bir durum, bir kriz ya da özel bir ana ilişkin olarak, bu durumdan yararlanma anlamına gelmektedir. Sosyal mühendisler anlık yardım gerektiren kriz durumlarını oldukça etkili kullanmakta, personelin güvenini sarsmaksızın yardım edilmeye ilişkin suni ortamları oluşturma hususunda taktiklerden faydalanmaktadır.

- vi. *Doğal eğilimlerden yararlanma:* İnsanların en temel özelliklerinden biri olan diğerlerine yardım etme duygu ve eğiliminden faydalanılmasıdır. Yardım ihtiyacı bulunan müşteri şeklinde davranma veya çalışanları yetkili bir personel olduğuna ikna ederek onların boşluklarından yararlanmak, en çok faydalanılan teknikler arasındadır (Bağcı, 2009: 45). ATM cihazlarında işlem yapmakta olan kurbanların ATM cihazında kalması sağlanan banka kartının iptali hususunda parola bilgisinin istenmesi bu duruma örnek teşkil etmektedir (İlbaş, 2009: 32).
- vii. *Sorumluluğun yayılımı:* Personelin yalnızca kendi hareketlerinden sorumlu olmadığı, diğerlerinin görev konusu içine giren hususlardan da sorumlu olduklarına ikna edilmeleridir. Sosyal mühendisler birtakım etkenlerin de yardımıyla oluşturmuş oldukları ortamlarda, kişisel sorumluluk meselesini abartmak suretiyle personeli şaşırtmakta ve bir karar almaya zorlamaktadır. Karar alma sürecinde diğer personelin adlarının kullanılması ya da yüksek kademedeki yetkilendirilmiş bir görev olduğunun iddia edilmesi bilinen teknikler arasındadır.
- viii. *Bağlılık ve dürüstlüğün suiistimali:* Hedef bireyin zaaflarının saptanmasının ardından, bu zaafların birey ve kurum aleyhine kullanılması, kurum menfaatleri ile bağdaşmayacak davranışların sergilenmesi sağlanmak suretiyle kuruma olan bağlılığın zayıflatılmasıdır.

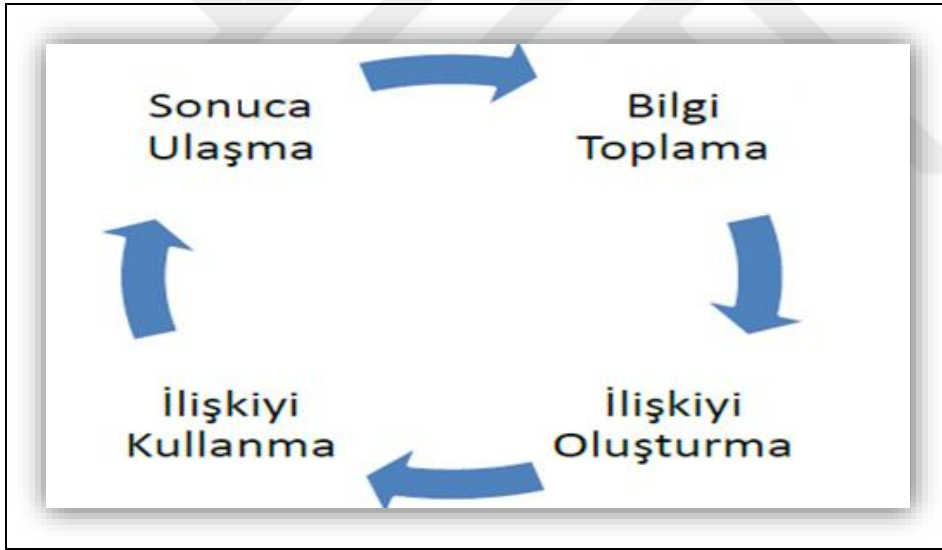
2.1.4. Sosyal mühendislik saldırı evreleri

Sosyal mühendislik saldırılarının temel olarak dört evresi bulunmaktadır. Bilgi toplama, ilişkiyi oluşturma, ilişkiyi kullanma ve sonuca ulaşma şeklinde betimlenen bu evreler şu şekilde özetlenmektedir (Barışkan, 2017: 4; Çatak, 2016: 7):

- i. *Bilgi toplama evresi:* Bireylerin bilinçsiz sosyal medya kullanımları, internet siteleri, işyeri internet sayfaları gibi sistemler üzerinden kolay bir şekilde bilgi toplanabilmektedir (Barışkan, 2017: 4). Bilgi toplama, pasif bilgi toplama ve aktif bilgi

toplama şeklinde ikiye ayrılmaktadır. Pasif bilgi toplamada hedef sistem ile etkileşim bulunmamaktadır. Aktif bilgi toplamada ise hedef sistemde arama/tarama gerçekleştirilmektedir (Çatak, 2016: 8). Gerekli bilgiler ise internet ve elektronik posta arşivleri, port ve servis taramaları, arama motorları, sosyal paylaşım siteleri, DNS üzerinden sağlanabilmektedir (Çatak, 2016: 9).

- ii. *İlişkiyi oluşturma evresi:* Bu evrede sosyal mühendis, elde ettiği bilgileri kullanmak suretiyle kurbanla iletişime geçmektedir.
- iii. *İlişkiyi kullanma evresi:* Bu evrede kurbanın güvenini kazanmış olan sosyal mühendis, iletişime geçtiği bireyin kişisel bilgilerini, kredi kartı bilgileri, giriş parolalarını vs. ele geçirmektedir.
- iv. *Sonuca ulaşma:* Son evrede sosyal mühendis, nihai hedefine ulaşmaktadır.



Şekil 4: Sosyal mühendislik saldırılarının izledikleri evreler

Kaynak: Barışkan, M.A., 2017. Türkiye’deki siber güvenlik bilinci ve sosyal mühendislik ataklarına karşı savunma önlemlerinin geliştirilmesi. Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi FBE, s. 3.

2.2 Dolandırıcılık ve Telefon Dolandırıcılığı

Günümüz itibariyle, bilişim teknolojilerinin sürekli gelişimi, artan çeşitliliği ve yaygınlaşması neticesinde klasik dolandırıcılık yöntemlerine yeni dolandırıcılık yöntemleri eklenmektedir. Bu durum ilerleyen zaman içerisinde de dolandırıcıların yeni yöntemler geliştireceklerinin göstergesidir. Gelişen teknoloji ve sürekli değişim gösteren piyasa koşulları çerçevesinde bir taraftan internet, kredi kartı ve cep telefonlarının kullanılmakta olduğu yeni dolandırıcılık yöntemleri ortaya çıkarken, diğer yandan ise eski dolandırıcılık yöntemleri de farklı biçimlerde yeniden kullanılmaktadır. 1920'lerde İtalyan göçmen Charles Ponzi'nin geri gönderim pulları vasıtasıyla para kazandığını iddia etmek suretiyle halkı dolandırmasından ötürü "Ponzi Dolandırıcılığı" adıyla bilinmekte olan dolandırıcılık yöntemi, günümüzde "foreks yatırımı", "sahte tahvil" ve "sahte hedge fonu" satışı şekilleriyle karşımıza çıkmaktadır. Günümüzde giderek yaygınlaşmakta olan sanal para birimi "Bitcoin" sistemi de benzer bir dolandırıcılık örneği olarak değerlendirilmektedir (Yılmaz, 2015: 3). Bu bağlamda çalışmanın bu bölümünde dolandırıcılık suçunun tanımı ve kapsamı, dolandırıcılık suçunun tarihsel gelişimi, dolandırıcılık suçunun benzer suçlardan farkları, nitelikli dolandırıcılık ve telefon dolandırıcılığı konuları aktarılmaktadır.

2.2.1. Dolandırıcılık suçunun tanımı ve kapsamı

Dolandırıcılık, hileli davranışlar ile karşıda bulunan kişinin kandırılması suretiyle menfaat temin edilmesidir. Dolandırıcılık suçunun en temel özelliği; failin sahip olduğu kurnazlık, plan yapma, uyum sağlama ve ikna kabiliyetiyle mağdurların tecrübesizliği, dikkatsizliği ve kolay yoldan para kazanma hırsını kullanmak suretiyle gelir elde etmesidir (Bilen, 2012: 6).

Dolandırıcılık suçu, İtalyan hukukunda "*Truffa*", Fransız hukukunda "*Escroquerie*", Alman, İsviçre ve Avusturya hukukunda "*Betrug*", İngiliz hukukunda ise "*Fraud*" terimleriyle ifade edilmektedir (Tümerkan, 1987: 1).

Dolandırıcılık suçu, malvarlığına yönelik olarak işlenen suçlar içerisinde yer almaktadır. Hukuki açıdan çeşitli vasıtaları harekete geçirmekte olan bir suç konumundadır. Kriminolojik bakımdan genç sayılabilecek bir suç niteliğine sahiptir. Zeka düzeyinin yüksekliğinden ötürü, sosyal yaşama kolay şekilde uyum sağlama özelliğine sahiptir. Dolandırıcılık suçunun mağduru olan kişiler, bu suçta hem mağdur hem de suçlu durumundadır. Çoğu zaman suçun kendilerine yönelik olarak işlenme nedeni, mağdur kişilerin gereken dikkat, önem ve özeni göstermemeleri ile daha fazla kazanma hırısından kaynaklanmaktadır (Dönmezer, 2004: 449).

Dolandırıcılık suçu, başka bir kişinin malvarlığına yönelik olarak hissedilmekte olan duyguların incelik ile gizlenmek suretiyle işlenmekte olduğu özel bir suç niteliğindedir (Soyaslan, 2005: 340). Dolandırıcılık, iyi niyet kuralının ihlali ve gündelik insani ilişkilerde, ticari yaşamda serbest ile yaşağın ince çizgisi konumundadır (Hafizoğulları ve Özen, 2010: 370).

Kişiler arasında iktisadi ilişkiler kurulması ve korunmasıyla karşılıklı güvenin muhafaza altına alınması hususundaki sosyal menfaat, dolandırıcılığın suç şeklinde düzenlenmesinin en temel nedenlerindedir (Artuk, Gökçen ve Yenidünya, 2009: 3563). Dolandırıcılığın özü, failin hile yapmak suretiyle bir kimsenin pozitif ya da negatif bir fiil gerçekleştirmesine sebebiyet vermesidir. Lakin bu hareket, hareketi uygulayanın malvarlığında azalmaya, failin ya da başka bir kimsenin malvarlığında artışa neden olmaktadır. Mağdur bu hareketi kendi isteğiyle yapmaktadır. Lakin bu istem, hileyle elde edilmiş olduğundan, dolandırıcılık suçunu karakterize eden de hiledir (Soyaslan, 2005: 341).

Günümüz itibariyle malvarlığına yönelik olarak en çok işlenmekte olan suçlardan biri olan dolandırıcılık; iktisadi ve toplumsal yaşamdaki gelişmeler, insanın tarihin başlangıcından itibaren içerisinde bulunan yağmalama ve karşı taraftaki kişinin malvarlığını ele geçirme içgüdüsünün doğal bir sonucu niteliğindedir (Erem ve Toroslu, 2003: 525).

765 sayılı Türk Ceza Kanunu (TCK) m. 503'ün 1. fıkrasına göre;

“Bir kimseyi kandırabilecek nitelikte hile ve desiseler yapmak suretiyle hataya düşürerek onun ya da bir başkasının zararına, kendine ya da başka birine haksız bir yarar sağlamakta olan kişiye 1 yıldan 3 yıla kadar hapis ve sağlamış olduğu haksız yararın bir misli kadar ağır para cezası verilir.” ifadesi yer almıştır. 2. fıkrada ise; *“Fiili, mağdur kişide esasen bulunan hatadan, hile ve desise kullanarak yararlanıp gerçekleştiren kişi hususunda da 1. fıkrada yazılı ceza uygulanır.”* denilmektedir (Yalvaç, 2015: 212).

5237 sayılı TCK'nın “Kişilere Karşı Suçlar” başlıklı 2. kısmının “Malvarlığına Karşı Suçlar” başlıklı bölümünde “Dolandırıcılık” suçunun tanımı, hileli davranışlarla bir kimsenin aldatılarak, onun ya da başkasının zararına olacak şekilde, kendisine ya da başkasına bir fayda sağlamak şeklinde ifade edilmektedir (TCK m.157). Dolandırıcılığın basit hali TCK m. 157’de, nitelikli hali m. 158’de, daha az cezayı gerektiren hali ise m.159’da düzenlenmiş durumdadır (Yılmaz, 2015: 1). Bununla birlikte, TCK m. 167’de dolandırıcılık suçunun şahsi cezasızlık nedenleri ya da cezada indirim yapılmasını gerektirmekte olan şahsi nedenlerden, m. 168’de ise etkin pişmanlığın dolandırıcılık suçu bakımından geçerli kurallarından bahsedilmiştir (Can, 2014: 3).

Dolandırıcılık suçunun faili, dış görünüşü ile toplumda bir iş adamı, ticaret adamı görüntüsüyle yer alan zeki ve kurnaz bir şahıstır. Dolandırıcının hedefine almış olduğu kişi dolandırıldığını ancak belli bir zaman sonra anlamaktadır. Dolandırıcı, planlı davranışlarını sonlandırarak haksız bir fayda elde ettiği zaman, iş yaşamında kendisini başarıya erişmiş saymaktadır. Hedeflerine kolay bir şekilde erişebilmek ve muhatabını tedirgin etmemek üzere dolandırıcı dış görünüşü, giyimi ve konuşmasına özen göstermektedir (Yalkut 1979: 231).

Dolandırıcılık, malvarlığına yönelik olarak işlenen suçlar arasında faili tarafınca en fazla maharet ve yetenekten faydalanılması gereken suç konumundadır. Dolandırıcı, kendine ait olmayan bir şeyi hırsızlık yoluyla almamaktadır. Bu şeyi bizatihi mağdur kişinin kendine vermesini sağlamaktadır. Bunun yanında dolandırıcılığın hedefinde bulunan kişi, bu teslimi cebir ve tehdit altında ya da şantajla yapmamaktadır. Bunların aksine mağdur kişi, fail

tarafından talep edilen malvarlığına ilişkin unsurları kendi rızası çerçevesinde teslim etmektedir. Zira dolandırıcı malın teslimi hususunda güç kullanmaktan ziyade ikna edici araçlardan faydalanmaktadır (Dursun, 2016: 4).

Dolandırıcılık suçu malvarlığına yönelik işlenen bir suç olup, korunan hukuki yarar bakımından bu suç, malvarlığı değerlerini korumaktadır. Lakin bununla birlikte fail, hileli birtakım davranışlar sergileyip karşısında bulunan kişiyi kandırarak kendisi ya da bir başkası için yarar sağladığından, bu suçla malvarlığı değerlerinin yanı sıra kişinin irade serbestisi ile rıza özgürlüğü de korunmaktadır (Artuç, 2007: 360). Bu bağlamda dolandırıcılık suçunu diğer malvarlığına yönelik olarak işlenen suçlara göre farklı kılan unsur, dolandırıcılık suçunun aldatma temeline dayalı bir suç niteliğinde bulunmasıdır (Yaşar, Gökcan ve Artuç, 2010: 4603).

Dolandırıcılık suçu açısından mağdur, hileli davranışa maruz kalmak suretiyle malvarlığında azalma ortaya çıkan kişidir. Dolandırıcılık suçunun konusu, hileli davranışlar ile bir kişinin aldatılması neticesinde, onun ya da başkasının zararına olarak elde edilen menfaattir (Meran, 2008: 225). Bu doğrultuda, bir şahsın sahibi olduğu ve hukuk düzeni tarafından koruma altında olan, iktisadi bir değere sahip varlık veya menfaatlerin tamamı dolandırıcılık suçunun konusu içerisine girmektedir (Dönmezer, 2004: 467).

Dolandırıcılık suçu, TCK m. 157 ve devamındaki maddelerde düzenlenmiş olup, bu doğrultuda hileli davranışlarda bulunup bir kişiyi aldatmak suretiyle onun ya da bir başkasının zararına olacak şekilde kendisi ya da bir başkasına fayda sağlamakta olan kimse, suçta ve cezada kanunilik ilkesi uyarınca cezalandırılacaktır. Suçun maddi unsuru bakımından ise dolandırıcılık suçu, serbest ve icrai-ihmalî hareketli bir suç konumunda bulunmaktadır. Suçun manevi unsuru bakımından dolandırıcılık suçu, kasten işlenebilen bir suçtur. Dolandırıcılık suçunda hileler ya da sanialar kullanmak suretiyle yanıltma ve aldatma, yarar sağlama ve başkasına zarar verme bilinç ve iradesi suç kastını meydana getirmektedir (Selçuk, 1986: 17). Dolandırıcılık faili doğrudan kastla hareket edebileceği gibi olası kastla da hareket edebilmekte

olup, dolandırıcılık suçunun basit ve bilinçli taksir ile işlenebilmesi ise mümkün değildir. Bununla birlikte basit dolandırıcılık açısından genel kast söz konusu iken, nitelikli dolandırıcılık bakımından ise özel kast söz konusudur (Maviş, 2015).

Dolandırıcılık suçunun özü ve diğer suçlarla farkını meydana getiren hileli davranışlar; iletişim ve bilgi teknolojilerinde yaşanan gelişmelerle sosyal ve iktisadi yapıda ortaya çıkan değişimler ve yenilikler sebebiyle günümüzde sayı ve tür açısından artış göstermiş ve oluşum koşulları da giderek kolaylaşmıştır. Bu doğrultuda, dolandırıcılık suçu dışında hileli davranışları içinde bir unsur olarak barındırmakta olan çeşitli başka suç türleri de ortaya çıkmış durumdadır (Dursun, 2016: 2).

Dolandırıcılık suçunun oluşumu hususunda, aynı diğer suçlarda olduğu gibi çevresel unsurların etkisi önem arz etmektedir. Gelir dağılımında yaşanan adaletsizlik, iktisadi yaşamda ortaya çıkan değişimler, insanlarda oluşan ahlaki çöküntüler, toplumun nüfusunun yükselmesi, şehirleşme ve göç sebebiyle şahıslar arasında ortaya çıkan güvensizlik ortamı, fertlerin gelir elde etmek üzere bütün yolları meşru görmeleri, şahısların bireysel ve ailevi özellikleri ile yetiştikleri çevre ve eğitim düzeyi gibi faktörler dolandırıcılık suçunun yaygınlaşmasına önemli biçimde etki etmektedir (Yılmaz ve Ergün, 2005: 4).

Dolandırıcılık suçunun cezalandırılması, sosyal menfaatten ötürü olup, kanun yapıcılar dolandırıcılık suçunun cezalandırılmasında sosyal menfaat gördüklerinden dolayı dolandırıcılık fiili suç sayılmaktadır (Soyaslan, 2005: 348).

2.2.2. Dolandırıcılık suçunun tarihsel gelişimi

Dolandırıcılık suçu, kaynağını hırsızlıktan almakta olan, ticaret ve sanayideki modern ve aynı zamanda global, karmaşık iktisadi ilişkiler neticesinde ortaya çıkmış olan bir suç türüdür (Yılmaz ve Ergün, 2005: 3). Dolandırıcılık suçu, eski zamanlarda daha ziyade hırsızlık suçunun bir türü şeklinde değerlendirilmiş olup, daha sonrasında ayrı bir suç niteliği kazanmıştır. Dolandırıcılığın bağımsız bir suç şeklinde düzenlenmesinin uzunca bir zaman

sonunda gerçekleşmesinin en temel nedeni, suçun işlenmesi hususunda faydalanılan aracın niteliğinden kaynaklanmaktadır (Selçuk, 1982: 34).

Dolandırıcılık, Roma Hukuku'nda yer alan ve “*furtum*” adıyla anılan hırsızlık suçundan türetilmiş bir suç türüdür. Romalılar döneminde “*contrectatio rei fraudulosa*” terimi; hırsızlık, dolandırıcılık ve güveni kötüye kullanma suçlarını içerecek biçimde geniş anlamda kullanılmıştır (Selçuk, 1986: 3). Dolandırıcılık suçu, uzunca bir zaman boyunca menkul bir malın çalınması biçiminde algılanmış, Roma İmparatorluğu'nun ilerleyen dönemlerine değin üçüncü şahıslara zarar vermekte olan çeşitli hileli hareketler de buna dahil edilmiştir (Selçuk, 1982: 36).

Antik Yunan'da hırsızlık, mala zarar verme vb. suçlar detaylı şekilde düzenlenmiştir. Ancak dolandırıcılık suçuna ilişkin olarak açık bir şekilde belirtilmiş bir düzenlemeye rastlanmamıştır (Sami, 1982: 35).

Fransız hukukunda, dolandırıcılık suçu başlangıçta ayrı bir suç şeklinde düzenlenmeyip, hırsızlık suçunun nitelikli hali biçiminde değerlendirilmiş olup, ilk defa 1810 tarihli Fransız Ceza Kanunu kapsamında müstakil bir suç şeklinde düzenlenip belirtilmiştir. Suçun ağırlaştırıcı sebepleriyle takip eden yıllar içerisinde Fransız Ceza Kanunu içerisinde yer almıştır (Tezcan, Erdem ve Önok, 2008: 589).

İslam hukukuna Fıkıh ismi verilmektedir. İslam Ceza Hukuku'nun ismiyle Ukubat'tır. İslam Ceza Hukuku kapsamında suçlar, Allah'ın haklarına karşı işlenen suçlar, bireyin çıkarına karşı işlenen suçlar ve taziren cezalandırılan fiiller şeklinde üçe ayrılmaktadır (Artuk, Gökçen ve Yenidünya, 2009: 64). İslam hukuku çerçevesinde gizlice ve zorla gerçekleştirilen hırsızlık suçu tanımlanmış olmasına karşın, dolandırıcılık suçu tanımlanmamıştır (Selçuk, 1982: 39). Aynı durum Osmanlı Devleti'nde de görülmektedir (Tümerkan, 1987: 3). Osmanlı'da dolandırıcılık suçu ancak 1858 tarihli Osmanlı Ceza Kanunu kapsamında düzenlenmiş olup,

dolandırıcılık suçu için çeşitli zamanlarda kürek cezası, çeşitli diğer zamanlarda ise kalebentlik cezası verilmiştir (Tümerkan, 1987: 4).

Cumhuriyetin kurulmasının ardından 1926'da yürürlüğe girmiş olan 765 sayılı TCK'nın 503 vd. maddelerine göre dolandırıcılık suçu, hile ve desiseler yapmak suretiyle bir kişiyi hataya düşürerek onun ya da başkasının zararına, kendine ya da başkasına haksız bir menfaat sağlama şeklinde belirtilmiştir. 5237 sayılı TCK'da ise, hileli davranışlar ile bir kişiyi aldatarak, onun ya da başkasının zararına olarak, kendine ya da başkasına bir fayda sağlama şeklinde tanımlanmaktadır.

2.2.3. Dolandırıcılık suçunun benzer suçlardan farkları

Dolandırıcılık suçu, çeşitli bazı diğer suçlarla karıştırılabilmektedir. Bunlardan birisi güveni kötüye kullanma suçudur. Güveni kötüye kullanma suçunun basit hali, TCK m. 155/1'de belirtildiği üzere, zilyetliği kendisine devredilmiş mal üzerinde kendisi veya bir başkasının faydasına tasarrufta bulunmak şeklinde belirtilmiştir. Bu suçun nitelikli hali için ise, TCK m. 155/2'ye göre; söz konusu malın meslek, sanat, ticaret vb. sebeple devredilmiş olması gereklidir. Dolayısıyla dolandırıcılık suçu ile güveni kötüye kullanma suçu arasındaki temel fark, malın devri ile ilgilidir. Her iki suç kapsamında da mal, maliki tarafınca faile rızaen devredilmektedir. Ancak dolandırıcılık suçunda fail, karşısında bulunan kişiyi hileli davranışlar ile aldatmakta olduğundan, esasen malın maliki veya zilyedinin rıza göstermeyecek olmasına rağmen rıza göstermesini sağlamaktadır. Güveni kötüye kullanma suçunda ise, güven ilişkisinin oluşturulması sırasında failde suç işleme kastı bulunmaması, sonradan ortaya çıkması gerekmektedir (Meraklı, 2009: 1661-1662).

Dolandırıcılık suçu ile benzer görülen bir başka suç hırsızlıktır. Hırsızlık suçu TCK m. 141'de tanımlanmıştır. Hırsızlık suçunda korunan hukuki fayda zilyetlik yani malvarlığı değeri iken, dolandırıcılık suçunda ise malvarlığı değerleri yanında irade serbestisi de koruma altındadır. Hırsızlık yalnızca taşınır mallara yönelik işlenebilirken, dolandırıcılık ise taşınır

mallar yanında, taşınmaz mallara yönelik olarak da işlenebilmektedir. Hırsızlıkta suçun maddi konusu her daim mevcut olup, iktisadi bir değere sahip olan taşınır bir maldır. Dolandırıcılıkta ise suçun maddi konusu kimi zaman tek kimi zaman ikidir. Hırsızlık suçu hem zilyet hem de malike yönelik olarak işlenebilirken, dolandırıcılık suçu ise sadece zilyede yönelik olarak işlenebilmektedir (Selçuk, 1986: 6-9).

Dolandırıcılık suçuyla karıştırılabilecek başka bir suç da yağma suçudur. Her iki suç bakımından da korunan hukuki değer aynıdır ve malvarlığı değerleri ile irade özgürlüğüdür. Yağma suçunda konu, senedin yağması haricindeki hallerde taşınır mallar olurken, dolandırıcılıkta ise malın taşınır ya da taşınmaz olması önemli değildir. Suçun maddi unsuru bakımından yağma suçunda mal cebir ya da tehditle alınırken, dolandırıcılıkta ise hileli davranışlarla irade sakatlanmak suretiyle alınmaktadır. Mağdur dolandırıcılıkta yanıltılmaktadır, yağmada ise bir araç konumuna düşürülürken iradesi de ortadan kaldırılmaktadır (Selçuk, 1986: 26).

2.2.4. Nitelikli dolandırıcılık

İktisadi ve toplumsal yaşamda meydana gelen gelişme ve değişimlere paralel şekilde dolandırıcılık suçunun işleniş şekilleri de değişip çeşitlenmiş ve dolandırıcılık suçunu işleme eğiliminde de artış yaşanmıştır. Dolandırıcılık suçunun işlenmesiyle ortaya çıkan zararın ağırlığı, failin sahip olduğu sıfat ve bu sığata karşı hissedilen güvenin kötüye kullanılması, fail tarafınca faydalanılan hileli davranışın niteliđi, mağdur kişinin psikolojik ve fizyolojik açılarından durumu ve bir kısım tüzel kişiliklerin iktisadi ve toplumsal yaşamda sahip oldukları önemi göz önünde bulunduran yasa koyucu, dolandırıcılık suçunun “basit haline” kıyasla daha ağır cezayı gerektirmekte olan “nitelikli halleri” düzenlemiştir (Hafizođulları ve Özen, 2010: 408-409).

Suçun kurucu unsurları yanı sıra kanun koyucu tarafınca belirlenmiş olan çeşitli durumların bulunması halinde, suçun daha ağır ya da daha hafif sayılmasını gerektirmekte olan

haller, nitelikli hal şeklinde isimlendirilmektedir. Somut olaylarda nitelikli hallerin bulunması durumunda fail, duruma göre daha fazla ya da daha az ceza almaktadır (Hakeri, 2011: 127).

Dolandırıcılık suçuna ilişkin nitelikli haller 765 sayılı TCK döneminde m. 504'te düzenlenmiştir. Bahsi geçen maddede 1990'da gerçekleştirilen değişiklik vasıtasıyla nitelikli dolandırıcılık hallerinin sayısı artırılmıştır. Ardından 2004 yılında yapılan düzenlemeyle nitelikli dolandırıcılık hallerinin sayısı yeniden artırılmış ve 5237 sayılı TCK m. 158'de bu hallere yer verilmiştir. Nitelikli dolandırıcılık hallerinin zamanla çeşitlenmesindeki nedenler; toplumsal yaşamda ve teknolojik alanda yaşanan gelişmelerden ötürü dolandırıcılık suçunun işlenme alanının genişlemesi ve suçun işlenmesinin kolay hale gelmesi, yasa koyucunun suç siyaseti çerçevesinde belli yapı, kişi, kurum ve kuruluşları iktisadi ve toplumsal amaçlar kapsamında özel bir koruma altına almayı istemesi ile bir kısım çıkar gruplarının yasa koyucuyu etkilemesi şeklinde ifade edilebilmektedir (Tezcan, Erdem ve Önok, 2008: 608).

Nitelikli dolandırıcılık hallerinden birinin gerçekleştirilmiş olması halinde kanun kapsamında faile, basit dolandırıcılığa kıyasla daha ağır bir cezai yaptırım öngörülmüştür. Failin gerçekleştirdiği suç eylemi, nitelikli hallerden biri veya daha fazlasını içerebilmektedir. Birden çok nitelikli hale ilişkin suçun işlenmesi durumunda faile daha ağır bir yaptırım uygulanacağına ilişkin kanunda sarıh bir düzenlemeye rastlanmamaktadır.

Nitelikli dolandırıcılık suçunun işlenmiş olduğundan bahsedebilmesi hususunda, yapılan eylemin suçun basit halinde aranmakta olan koşulları taşıması gereklidir. Nitelikli dolandırıcılık halleri, dolandırıcılığın basit şeklinden ayrılmamaktadır. Dolandırıcılığa ilişkin suçun tanımı ile unsurlarından genel olarak TCK m. 157'de bahsedilmektedir. Buna göre; *“Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beş bin güne kadar adli para cezası verilir.”* denilmiştir. Bu doğrultuda bir eylemin, tanımı ve unsurları belirtilmiş olan temel/basit dolandırıcılık suçuna sebep olmasının ardından; failin amacı, eylem içinde

kullanılmış olan araçlar, failin ya da mağdurun sahip oldukları birtakım özellikler ve nitelikler göz önünde bulundurularak dolandırıcılık suçunun nitelikli hallerine sebep olabilmektedir. Bu bağlamda, nitelikli dolandırıcılık halinin ortaya çıkıp çıkmadığının belirlenmesinden evvel, failin bilerek ve isteyerek hileli davranışlardan yararlanmak suretiyle bir kimseyi aldatıp, onun ya da bir başkasının zararına olacak şekilde, kendine ya da bir başkasına bir yarar sağlayıp sağlamadığının belirlenmesi gereklidir. Bu tespitin ardından ise işlenen dolandırıcılık suçunun nitelikli olup olmadığı araştırılabilmektedir (Dursun, 2016: 228-229). Bu bağlamda nitelikli dolandırıcılık halleri ve bu hallere ilişkin cezai yaptırım usulü 5237 sayılı TCK m. 158'de şu şekilde belirtilmiştir;

Dolandırıcılık suçunun;

- a) *Dini inanç ve duygular istismar edilerek:* Burada dinin bir aldatma aracı olarak kullanılması hususuna dikkat edilmesi gereklidir. Bu suçun gerçekleşmesi hususunda dini inanç ve duyguların aldatma aracı şeklinde kötüye kullanılması gerekmektedir.
- b) *Bireyin içerisinde yer aldığı tehlikeli hal ya da güç koşullardan faydalanılarak:* Bireyin içerisinde olduğu tehlikeli durum ya da güç koşullar, başkalarına güven duymaya en çok gereksinim duyulan anlardır. Bu gibi durumlarda kişinin içinde bulunduğu çaresizlik durumundan faydalanılarak aldatılması daha kolay olmaktadır.
- c) *Bireyin algılama yetisinin zayıflığından faydalanarak:* Bir kimsenin algılama yeteneğindeki zayıflıktan faydalanılarak aldatılması daha kolay olmaktadır.
- d) *Kamu kurum ve kuruluşları, kamu meslek kuruluşları, siyasi parti, vakıf ya da dernek tüzel kişilikleri araç şeklinde kullanılarak:* Bu dolandırıcılık hali, suçun nitelikli bir unsuru şeklinde kabul edilmiştir. Zira, kamu kurum ve kuruluşları,

kamu kurumu niteliğindeki meslek kuruluşları, siyasi parti, vakıf ya da dernek tüzel kişilikleri toplum nezdinde güven veren müesseseler şeklinde kabul edilmektedir.

- e) *Kamu kurum ve kuruluşlarının zararına olarak:* Bu kapsamda kamu kurum ve kuruluşlarının zarar görmesine sebebiyet verecek olan dolandırıcılık eylemleri, suçun daha ağır cezayı gerektirmekte olan nitelikli hali şeklinde kabul edilmiştir.
- f) *Bilişim sistemleri, banka ya da kredi kuruluşları araç şeklinde kullanılarak:* Bilişim sistemlerinin veya güven veren kurumlar niteliğindeki banka ve kredi kuruluşlarının araç şeklinde kullanılması, dolandırıcılık suçunun işlenmesi bakımından önemli kolaylıklar sağlamaktadır.
- g) *Basın ve yayın araçlarının sağlamakta olduğu kolaylıktan faydalanarak:* Bu bağlamda, dolandırıcılık suçunun basın ve yayın organlarının kolaylıkları üzerinden işlenmesi, dolandırıcılık suçu bakımından bir nitelikli unsur şeklinde kabul edilmiştir.
- h) *Tacir ya da şirket yöneticisi durumunda bulunan veya firma adına hareket eden kimselerin ticari aktiviteleri esnasında; kooperatif yöneticilerinin kooperatifin aktiviteleri kapsamında:* Burada, ticari aktiviteleri meslek olarak yürütmekte olan kimselerin güvenilirliğinin sağlanması amacıyla, dolandırıcılık suçunun tacir ya da şirket yöneticisi konumundaki veya şirket adına hareket etmekte olan kimselerin ticari aktiviteleri esnasında; kooperatif yöneticilerinin kooperatifin aktiviteleri çerçevesinde işlenmesi, suçun temel şekline kıyasla daha ağır bir cezayı gerektirmektedir.
- i) *Serbest meslek sahibi kimseler tarafınca, mesleklerinden ötürü kendilerine duyulmakta olan güvenin kötüye kullanılması suretiyle:* Dolandırıcılık eylemlerinin serbest meslek sahibi kimseler tarafınca meslekleri sebebiyle kendilerine

duyulmakta olan güvenin kötüye kullanılmasıyla gerçekleşmesi halinde, bu durum suçun nitelikli bir unsuru şeklinde belirtilmiştir.

j) *Banka ya da diğer kredi kuruluşlarınca tahsis edilmemesi gerekli olan bir kredinin açılmasının sağlanması amacıyla:* Banka ve kredi kuruluşlarından bir kredinin temin edilmesi maksadıyla hileli davranışlar sergilenmesi ve bu doğrultuda kredi adı altında bir menfaat sağlanması halinde bu nitelikli unsur oluşmaktadır.

k) *Sigorta bedelinin alınması amacıyla:* Bu nitelikli hal, sigorta eden kimsenin dolandırılması ile ilgilidir. Failin sigorta edilen ya da sigorta bedelini alacak kişi olması zorunlu değildir. Sigortalanan riskin türü de önem arz etmemektedir.

l) (Ek: 24/11/2016-6763/14 md.) *Bireyin kendini kamu görevlisi ya da banka, sigorta veya kredi kuruluşlarının çalışanı şeklinde tanıtmaya ya da bu kurum ve kuruluşlar ile ilişkili bulunduğunu söylemesi suretiyle,*

işlenmesi halinde, 3 yıldan 10 yıla kadar hapis ve 5.000 güne kadar adli para cezasına hükmolunur. Ancak (e), (f), (j), (k) ve (l) bentlerinde sayılmış olan hallerde hapis cezasının alt sınırı 4 yıldan, adli para cezasının miktarı suçtan elde edilen menfaatin 2 katından az olamaz.

2.2.5. Telefon dolandırıcılığı

Telefon günümüz itibariyle sadece birbirinden uzakta yaşamakta olan insanların birbirleriyle iletişim kurma gereksinimini karşılamak üzere faydalanılan bir araç konumunda bulunmamaktadır. Bu doğrultuda, sosyal ve ticari yaşamda normal şekilde yüz yüze yapılan pek çok iş ve işlem, iletişim ve bilgi teknolojileri tarafından insanlığın hizmetine sunulan imkanlar kapsamında internet üzerinden ya da telefon cihazı vasıtasıyla uzaktan gerçekleştirilmekte ve buna imkan veren hukuki zemin de devamlı şekilde genişlemektedir. Örnek olarak bankacılık hizmetleri kapsamında sunulmakta olan pek çok ürün ve hizmet telefon ve internet vasıtasıyla gerçekleştirilmektedir. Bunun yanında günümüzde pek çok ürüne ilişkin alım satım işlemleriyle hizmet tedarikleri de telefon aracılığıyla yapılabilmektedir. Telefon

cihazı bugün vadettiği imkanlardan ötürü hem fertler hem de kuruluşlar bakımından bir fırsatken, kötüye kullanılması hususundaki rahatlık, muhatabını aldatması konusundaki kolaylık ve kullanıcılarının tespiti ile yakalanması hususundaki güçlük sebebiyle önem arz eden potansiyel bir tehdit niteliğindedir (Dursun, 2016: 318).

Telefon hatları ve bu hatlar üzerinden verilmekte olan hizmetler aracılığıyla işlenmekte olan dolandırıcılık suçları, telefon dolandırıcılığı olarak isimlendirilmektedir (Dursun, 2016: 36). Telefon dolandırıcılığı suçu bakımından, ortaya konulan hilelerin somut ve sağduyulu ortalama zeka düzeyine sahip makul bir kimseyi aldatabilecek nitelikte olması gerekliliği genel olarak kabul edilmektedir. Aksi halde hileli davranışın bu suça neden olmayacağı kabul edilmektedir (Dursun, 2016: 106).

Telefonla işlenmekte olan dolandırıcılık suçlarının fertler ve toplum bakımından oluşturduğu tehlikelilik durumunun, basit dolandırıcılık suçlarına kıyasla oldukça fazla olduğu belirgindir. Nitekim bu tip hallerde suçun mağduru, kendisiyle dolaylı şekilde iletişim kuran faili yüz yüze görmediği için, sergilenen hileli davranışların meydana getirdiği psikolojik baskıyla kolayca etki altına girebilmektedir. Ülkemizde cep telefonu kullanımında yaşanan sürekli artış ve sektörün kayıt altına alınması hususunda yaşanmakta olan zorluklardan ötürü failer kendilerini kolay bir şekilde gizleyebildiği için bu failerin tespit edilmesi ve yakalanması zordur. Bu sebeple potansiyel mağdur kitlesi de gittikçe artış göstermektedir (Dursun, 2016: 319).

765 sayılı TCK m. 504'ün 1. fıkrasının 3. bendinde; “Posta, Telgraf ve Telefon (PTT) İşletmesi'nin haberleşme araçlarının araç şeklinde kullanılması suretiyle suçun işlenmesi” durumunda faile nitelikli dolandırıcılık kapsamında ceza verilmekteydi. Yeni düzenleme kapsamındaysa haberleşme araçları ifadesi kaldırılarak yerine “basın ve yayın araçları” ifadesi getirilmiş olup, bu bağlamda telefonun araç biçiminde kullanılmasıyla dolandırıcılık eyleminin gerçekleştirilmesi durumunda faile 5237 sayılı TCK m. 157 çerçevesinde dolandırıcılık

suçunun basit hali üzerinden ceza verilmeye başlanmıştır (Can, 2014: 67). Telefon vasıtasıyla işlenmekte olan dolandırıcılık suçu sayısının hızlı bir şekilde yükselmesi, suç ve suçluluk ile mücadele çerçevesinde izlenen suç siyaseti göz önünde bulundurulduğunda, telefon dolandırıcılığı eylemlerinin nitelikli dolandırıcılık kapsamı içerisine girmesi zaruri olmaktadır. Zira pek çok hukuk sisteminde (İngiltere, ABD vs.) benzer düzenlemeler bulunmakta olduğundan bahsedilebilmektedir (Dursun, 2016: 478). Bu bağlamda 5237 sayılı TCK m. 158 üzerinde, 6763 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 14. maddesi çerçevesinde değişiklik gerçekleştirilmiştir. Değişikliğin gerekçesine göre, nitelikli hallerle ilgili düzenleme gerçekleştirilmesine gereksinim hissedilmesinin ve TCK'nın 158. maddesinde gerçekleştirilen değişimlerin temel amacı; kendilerini polis, hakim, savcı ya da banka, sigorta veya kredi kuruluşlarının çalışanı şeklinde tanıtan şahısların, telefon vasıtasıyla eriştikleri mağdur kişileri çeşitli senaryolarla inandırmak suretiyle önemli miktarda haksız fayda sağlamaları ve bu durumun son zamanlarda artan bir sosyal duyarlılığın konusu olmasıdır (Tüysüz, 2017: 68).

Dolandırıcılık suçunun nitelikli hallerinin düzenlenmiş olduğu 5237 sayılı TCK m. 158'in 1. fıkrasına (1) bendi eklenmiştir. Buna göre failin eylemini, kendini kamu görevlisi ya da banka, sigorta veya kredi kurumlarının çalışanı şeklinde tanıtmayı ya da bu kurum ve kuruluşlarla ilişkili olduğunu ifade etmesi halinde dolandırıcılık eylemi, nitelikli dolandırıcılık kapsamında değerlendirilmektedir. Bunun yanında maddede failer için üç yıldan on yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunmuştur. Ancak maddeye eklenen (1) bendinde belirtilen suçu işleyen failer için hapis cezasının alt sınırının dört yıl olduğu, adli para cezasının miktarının ise suç dolayısıyla sağlanan faydanın iki katından az olamayacağı belirtilmiştir.

Mağdur kişilere ait olmakla birlikte önceden temin edilen birtakım kişisel veriler ile kurgulanan senaryonun unsurlarını kullanmakta olan suç faileri, mağdur kişilerde güven

yaratabilmektedir. Bunun yanında suça ilişkin eylemleri çoğu zaman telefon üzerinden gerçekleştirdikleri için mağdur kişilerin denetim olanağı da önemli oranda sınırlanmaktadır. Mağdur kişilerin, herkes tarafınca bilinme imkanı olmayan çeşitli kişisel, ailevi, sosyal ve iktisadi durumlarına ilişkin gerçek verileri de içermekte olan hikayeler karşısında, telsiz ve siren sesleri ile kuvvetlendirilmiş bir senaryo içerisinde emniyet müdürlüğünden arandıklarına inanabildikleri görülmektedir. Durumun ciddi ve acil olduğuna inanan mağdurların çoğu zaman konuşmayı sonlandırıp konunun gerçek olup olmadığını araştırma olanakları da kalmamaktadır. Bu doğrultuda yoğun yalan ve hileler ile aldatılan mağdur kişiler, ciddi seviyede iktisadi kayıp yaşamakta ve maddi birikimlerini tamamen kaybetme noktasına gelebilmektedirler (Tüysüz, 2017: 68).

ABD Federal Kanunu'nun ceza ve ceza usulünü düzenlemekte olan 18. kitabında 1343. madde kapsamında telefon, radyo ve televizyon dolandırıcılığına yer verilmiş olup (Dursun 2016: 17), ABD'deki uygulamada telefon dolandırıcılığı suçunun oluşması hususunda mağdurun maddi açıdan doğrudan şekilde zarar görmesi zorunlu değildir. Mağdur kişinin zarar görme olasılığının doğması, suçun oluşumu hususunda yeterli olmaktadır. Bu bağlamda hileli davranışlarla bir firmaya ilişkin bilgilerin ele geçirilmesi ya da gizli verilerin elde edilmesi de zarar şeklinde kabul edilmiştir (Dursun, 2016: 182).

Ülkemizde son dönemlerde cep telefonu hatları ve sabit telefon hatları üzerinden aranarak işlenmekte olan telefon dolandırıcılığı suçuyla bu eylem sonucunda nitelik ve nicelik bakımından ortaya çıkan mağduriyetin sayısı önemli ölçüde artış göstermiştir. Hem yazılı hem de görsel medyada bu hususta pek çok yayın yapılmasına, sorumlu idari ve adli birimler tarafınca insanların bilgilendirilmesi ve bilinçlendirilmesine ilişkin çalışmalar gerçekleştirilmesine rağmen, telefon dolandırıcılığı suçunun sayısında önemli bir azalma yaşanmamıştır (Dursun, 2016: 316-317).

Telefon dolandırıcıları tarafınca pek çok değişik yöntemden faydalanılmaktadır. Telefon aracılığıyla potansiyel dolandırıcılık mağduruyla iletişime geçen fail, ikna edici bir ses tonuyla konuşmakta ve dolandırıcı tarafınca pek çok argümandan faydalanılmaktadır. Bunların içerisinde en önemli olanları failin kendini hakim, savcı ya da emniyet görevlisi gibi kamu görevlileri şeklinde tanıtmasıdır. Bu doğrultuda arama gerçekleştiren fail, mağdura sim kartının, kredi kartına ilişkin bilgilerin, banka hesap bilgileri ve şifreleriyle diğer kişisel verilerinin terör ya da suç örgütleri tarafınca ele geçirildiğini, işlenmiş olan suçtan zarar görmemesi hususunda adli makamlara yardımcı olması ve ele geçirilmiş olan verileri geri kazanması için kendilerine yardımcı olması gerekliliğinden bahsederek, mağduru ikna etme çabası içerisinde bulunmaktadır. Çoğu zaman inandırıcılık seviyesini artırmak üzere telefon görüşmesi esnasında mağdura telsiz sesi dinletilmekte, böylece kurgulanmış olan senaryonun gerçeklik algısı da pekiştirilmeye çalışılmaktadır. Yapılan görüşme doğrultusunda ikna olan mağdur kişinin, kendine verilmiş olan hesap numarasına para yatırması ya da elinde bulunan parayı belli bir yere bırakması istenerek mağdur kişinin zarar görmesi sağlanmaktadır. Bununla birlikte, mağdurlardan yüklü miktarda kontör ya da kart şifresi gönderilmesi istenebilmekte, ardından gelen kontörler piyasada satılmak suretiyle fayda elde edilmektedir (Dursun, 2016: 317).

Telefon dolandırıcılığında genel olarak sahte senaryo üretimi yönteminden yararlanılmaktadır. Fail, internet üzerinden ya da saldırı hedefinin yakın çevresi sayesinde elde ettiği bilgiler doğrultusunda mağdurla iletişime geçmektedir. Korku uyandırmak, yetkili biri gibi davranmak, işe yeni başlamış kimse gibi davranmak, aciliyeti vurgulamak suretiyle çeşitli senaryolar üretip mağdurları aldatmaktadır (Acılar ve Baştuğ, 2016: 292).

Telefon dolandırıcılığına ilişkin bir başka yöntem telefon oltalamasıdır (*vishing*). “*Voice phishing*” sözcüklerinden türetilmiş olan telefon oltalaması yönteminde, mağdura gönderilen elektronik postada yer alan sahte link yerine bir telefon numarasının ifade edilmesi

ve bu numaranın aranması suretiyle bilgilerin güncelleştirilmesi hedeflenmektedir. Bu şekilde mağdurların bilgileri elde edilmektedir (Gündüz ve Daş: 3).

Telefon dolandırıcılığı suçunun ülkemizde eskiden bu yana yaygın durumda olmasının nedenleri arasında değerlerin yozlaşmış olması, bireyler arasındaki güven ve güvenlik duygusunun erozyona uğramış olması, çağdaş ve bilişim çağının gerektirdiği kültürel, iktisadi, politik ve sosyal hayat model ve sisteminin tamamen yaşama geçirilememiş olması gösterilebilmektedir. Bunun yanında dolandırılan mağdurlarda var olan koşullanma ve yaşamları süresince edinmiş oldukları yanlış sosyal öğrenmeler ile iç dünyalarında bulunan korkular da telefon dolandırıcılığı suçunun işlenmesi olasılığını kolaylaştırmaktadır (Dursun, 2016: 317).

Son yıllarda sosyal mühendislik vakaları yaygın biçimde gerçekleşmekte olup, her statü ve kesimden insanlar telefon dolandırıcılığı kapsamında hedef alınabilmektedir. Telefon dolandırıcılığının temelinde, mağdur kişinin teknik birtakım olanaklarla da desteklenmekte olan bir senaryoya inanarak, senaryoda kendisine verilmiş olan rolü oynaması bulunmaktadır. Mağdurlar telefon dolandırıcılığı vakasında bazen bir tehlikeden kurtarılacakları, bazen ise devlete yardıma bulunduğu ve gerçekleştirdiği ödemeleri geri alacağı biçiminde telkinler vasıtasıyla yönlendirilmektedir. Tansu Çiller'in başbakanlığı döneminde Selçuk Parsadan'ın Çiller'i arayarak kendini emekli Orgeneral Necdet Öztoran olarak tanıttığının ardından Kemalistler Derneği için 5,5 milyar TL istemesi ve örtülü ödenekten alınan paranın ertesi gün Parsadan'a gönderilmesi, telefon bankacılığının en ilginç ve önemli örneklerinden biridir (Yılmaz, 2015: 8-9).

Yılmaz (2015) tarafından gerçekleştirilmiş olan çalışmaya göre, Türkiye'de dolandırıcılık vakalarının %16,5'i sosyal mühendislik vakasıdır. Sosyal mühendislik yöntemi aracılığıyla gerçekleştirilen dolandırıcılık vakalarının ise %75'i telefon dolandırıcılığı şeklindedir. Bu oran içerisinde %65'lik kısım "Kendisini kamu görevlisi şeklinde tanıtmak"

vakasıdır. Buna göre; telefon hattının dolandırıcılar ya da terör örgütü tarafınca kullanıldığı, banka hesabının terör örgütünün eline geçtiği, teröristlerin peşinde olduğu vb. senaryolar ile mağdur kişinin belirtilen hesaba para yatırması veya para/altın gibi birikimlerini tenha bir yere bırakması sağlanmaktadır. %12'lik kısım ise “*Kendisini firma/kuruluş yetkilisi gibi tanıtmaya*” şeklinde gerçekleşmektedir. Buna göre; mağdur kişi telefonla aranmak suretiyle, bir sağlık merkezi adına aranıldığı, poliçe/ferdi kaza sigortası borcunun var olduğu, ödemediği takdirde icraya verileceği şeklindeki senaryolara inanan mağdur kişiden kredi kartı bilgileri talep edilmekte ve kredi kartından çekim yapılmaktadır.

Sosyal mühendislik yöntemi yanında ön ödeme yöntemiyle de telefon dolandırıcılığı vakalarına sıklıkla rastlanmaktadır. Ön ödeme yöntemi, dünya genelinde son derece yaygın bir yöntem olmakla birlikte, bu durumun en temel nedeni zaman ve mekandan bağımsız şekilde e-posta veya cep telefonu üzerinden ya da yüz yüze şekilde gerçekleştirilebilir olmasıdır. Sistemin özünde, sunulan büyük bir vaat ile bu vaade erişilmesi hususunda ödenmesi gereken küçük bir miktar para bulunmaktadır. Yılmaz (2015) tarafından gerçekleştirilen çalışmaya göre, Türkiye’de dolandırıcılık vakalarının %3,5’i ön ödeme yöntemiyle yapılmaktadır. Ön ödeme yönteminin yaklaşık %60’lık kısmı ise telefon dolandırıcılığı ile gerçekleştirilmektedir. Bu oran içerisinde %34’lük kısım çekiliş/kampanya mesajlarıyla yapılmaktadır. “*Değerli abonemiz çekiliş kampanyasından TL ödül kazandınız. Ödülünüzü almak üzere numaralı hattımızı arayın*” gibi mesajlarla mağdur kişinin belirtilen numarayı araması sağlanmaktadır. Netice itibarıyla ise mağdura ödülü alabilmesi hususunda vergi ya da masraflar için bir ön ödeme gerçekleştirilmesi gerekliliğinden bahsedilerek, kontör veya kredi kartı bilgileri istenmektedir. Ön ödeme yönteminin %5’lik kısmı mevduatta biriken para veya sigorta geri ödemesi gibi vaatlere ilişkindir. Bu bağlamda mağdur kişilere “*Banka kartından fazla kesilen paraları iade edeceğiz*” veya “*Bankada biriken paranızı alabilmek üzere dosya masrafını ödemeniz gerekmektedir*” gibi mesajlar atılmakta ya da kişi telefonla aranmaktadır. Netice

itibariyle kişiden bu paraları alabilmesi hususunda vergi ya da masraf adı altında bir ön ödeme gerçekleştirilmesi gerekliliğinden bahsedilmekte, kişinin kredi kartı bilgileri talep edilmekte veya belirli bir hesaba para yatırması istenmektedir. Ön ödeme yönteminin %21'lik kısmını oluşturan diğer vaatler içerisinde bulunan geçmişe yönelik kredi aidatlarını geri alma, kredi temin etme vb. vaatler çerçevesinde de mağdur kişilerden cüzi miktarda masraflar talep edilmektedir.

Unutulmaması gereken nokta şudur ki; adli bir dava için hakkında dava açılan kişi telefonla aranmaz. Tebligat Yasası'na göre kendisine dava açılan kişiye hangi mahkemede dava açılmışsa resmi yolla tebligat gönderilir. Hakkında dava açılan kişiye oturduğu mahallenin polis merkezinden çağrı gelebilir. Burada da yine resmi evrakla şahsa ulaşıp yazılı olarak tebliğ tebellüğ edilir. Aslında artık e-devlet hesaplarından kişiler kendileri adına açılmış bir dava olup olmadığını da görebilmektedirler (Altun, 2016).

İsa Altun'un Ortam Sanal Suç Gerçek kitabında Türkiye'de telefon dolandırıcılığını ilk başlatan, askerlik hariç köyünden hiç ayrılmamış, ilkokul mezunu dolandırıcı A.Z.'nin röportaj esnasında anlattıkları şöyledir:

“ ... Bu yöntemde ekibimiz genellikle internet üzerinden kurbanlarını seçiyordu. Arama motorlarında saygın iş adamları ve eli yüzü düzgün insanlar belirleniyordu. Bu kontör işi tutunca bu işten para kazanmak için işi profesyonel şekilde yapmaya başladık... Bu işi yaparken milletin zaaflarını, korkularını çok iyi kullandık. Neden korkar bu insanlar? Mesela bu toplumun polisten, savcıdan, hakimden, askerden, mahkemeden ödü kopar... Toplumun her kesiminden insanlar temiz ve masum olduklarını bildikleri halde ne olur ne olmaz diye düşünerek kendilerini sağlama almak için söylenenleri harfi harfine yerine getiriyorlardı... Uygulama teknik yardımıyla gerçekleştiriliyordu. Bu işi yapan her kişinin bir dizüstü bilgisayarı mevcuttur...İnternette indirilen bir polis telsizi programı ile bir kurban seçilir. Kurbanın tüm kişisel bilgileri arama motorlarında ya da bir şekilde bir yerden temin edilir. Daha doğrusu hackerler var; e-ticaret programlarından da bilgiler kopayalanır...Yöntemin işleyişi profesyoneldir. VOIP (Internet üzerinden telefon numarası arayabilen programlar) yazılımları kullanılır. Ciddiyet içinde soğukkanlı bir tonda telefonla arayan ikna edici bir şekilde tane tane konuşur. “Sosyal Mühendislik” stratejisiyle önce korkutup, sonra da güven duygusu verilip kumpasa düşürülür...Telefonla arayan kendinden öylesine emindir ki kurban kısa süreli akıl tutulması yaşar. Robota dönüşmüştür artık. Ne söylene yapar. Hele işin içinde gözaltı ya da tutuklama sözü geçiyorsa yelkenleri hemen indirir. Telefondaki kişiye telefonu kapatmaması, kimseye bilgi vermemesi, aksi takdirde operasyonun bozulacağı, bu yüzden de derhal tutuklanacağı ve en yakın ATM'ye gitmesi söylenir. Kurban ATM'ye gider ve hesap numarası için tuşlara yönlendirilir; çünkü hesap numarası verilirse bir kağıda yazacağından hesap numarasının deşifre olmaması gerekir... Yöntemler inandırıcı olması açısından günün gelişmelerine göre sürekli değişmek durumunda. Çete içindeki iki grup iş birliği halinde çalışır. Mesela bir grup kurbanın evini arar. Eşi telefona çıkar. Kendini polis, asker ya da savcı olarak tanıtan elemanlar polis telsizi sesi de vererek eşiyile ilgili bazı sorular sorarlar. Bu sorulardan birisi de tabii ki eşinin cep telefonudur. Görüşmenin gerçekçi olması için ardından diğer bilgiler istenir. Adam işte ya da ev dışındadır. İkinci grup da kurbanın cebini arar. Terör örgütü ya da Ergenekon bağlantısı ile ilgili önce korkutma, ardından da güven verici konuşmalar yapılır. Polislerin evde

olduklarını söylerler. Tuzak taktiklerinden birisi evin reisine hemen uygulanır. Bu sırada internet üzerinden bir yazılım aracılığı ile telekonferans sağlanarak polisler sanki evdeymiş gibi kadınla eşini telefonda konuştururlar. Parayı hesaba yatırdıktan sonra tekrar kendisine iade edileceğini söylerler. Adam telekonferansla eşiyile konuştuğundan habersiz bir şekilde polislerin evde olduğuna emin olmuştur artık. Kendisine telefonda verilen hesaba da parayı yatırır... Bu iş organizasyon işidir. Bu işi organize eden kişi asla kendi adına bankada hesap açmaz. Onun emrinde yüzde hesabıyla çalışanlar komisyon alırlar...” (Altun, 2016)

2.3. Dolandırıcılık Suçunun Türk Hukuk Sistemindeki Yeri

2.3.1. Suç tipi hakkında genel bilgiler

Dolandırıcılık, malvarlığına karşı işlenen suçlardandır. Dolandırıcılık suçu 5237 sayılı TCK'nun 157-159. maddeleri arasında düzenlenmiştir (Koca ve Üzülmez, 2016: 645).

Suçun temel şekli 157. maddede tanımlanmıştır. TCK madde 157'ye göre; suçun temel şekli;

“(1) Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası verilir.”

şeklinde tanımlanmıştır.

Madde 158 “nitelikli dolandırıcılık” başlığını taşımaktadır. Bu maddede, dolandırıcılık suçundan verilecek cezada artırım yapılmasını gerektiren nitelikli haller yer almaktadır. Bu maddeye göre;

“(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,

l) (Ek: 24/11/2016-6763/14 md.) Kişinin, kendisini kamu görevlisi veya banka, sigorta ya da kredi kurumlarının çalışanı olarak tanıtması veya bu kurum ve kuruluşlarla ilişkili olduğunu söylemesi suretiyle,

İşlenmesi halinde, üç yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur. (Ek cümle: 29/6/2005 – 5377/19 md.; Değişik: 3/4/2013-6456/40 md.) Ancak, (e), (f), (j), (k) ve (l) bentlerinde sayılan hâllerde hapis cezasının alt sınırı dört 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.

(3) (Ek fıkra: 24/11/2016-6763/14 md.) Bu madde ile 157 nci maddede yer alan suçların, üç veya daha fazla kişi tarafından işlenmesi halinde verilecek ceza yarı oranında; suç işlemek için teşkil edilmiş bir örgütün faaliyeti çerçevesinde işlenmesi halinde verilecek ceza bir kat artırılır.”

Madde 159’da ise dolandırıcılık suçunun daha az ceza verilmesini gerektiren haline yer verilmiştir. Bu maddeye göre;

“(1) Dolandırıcılığın, bir hukukî ilişkiye dayanan alacağı tahsil amacıyla işlenmesi hâlinde, şikâyet üzerine, altı aydan bir yıla kadar hapis veya adli para cezasına hükmolunur.”

Bu üç madde haricinde malvarlığına karşı suçlar bakımından ortak hüküm niteliğinde olan TCK 167 ve 168. maddelerin de bu suç tipi bakımından göz önünde bulundurulması gerekmektedir.

Adalet Bakanlığı, Adli Sicil ve İstatistik Genel Müdürlüğü’nün 2016 yılı Eylül ayında yayınladığı, “Adalet İstatistikleri Judicial Statistics 2015” yayınına göre; Cumhuriyet Başsavcılıkları’nca şüpheliler hakkında verilen kararlardan, malvarlığına karşı işlenen 1.931.191 adet suçun %39,2’si hırsızlık, %19,4’ü mala zarar verme, %19,6’sı dolandırıcılık, %3,6’sı yağma ve %18,2’ sinin bu gruptaki diğer suçlara ait olduğu görülmektedir. 1.931.191 adet suçun 756.537’si hırsızlık, 379.294’ü dolandırıcılık suçlarıdır (Adalet Bakanlığı, 2016).

2.3.2 Korunan hukuki değer

Dolandırıcılık, malvarlığına karşı işlenen suçlardan olduğundan dolayı öncelikle malvarlığı hakkı korumaya alınmıştır. Diğer taraftan bireyin irade özgürlüğünün de korunduğu kabul edilmektedir (Soyaslan, 2006: 342). Bu yönüyle dolandırıcılık suçu ile birden fazla

hukuki deęerin korunduęu sylenebilir, ancak n plana ıkan deęerin malvarlıęı olduęu ifade edilmelidir. Nitekim TCK’da da “Malvarlıęına Karşı Sular” bařlıęı altında dzenlenmesi bunu ortaya koymaktadır.

2.3.3.Suun unsurları

2.3.3.1. Tipiklięin maddi unsurları

a) Suun hukuki konusu

Mal varlıęına iliřkin tařınır, tařınmaz, alacak hakkı gibi herhangi bir deęer suun hukuki konusunu oluřturur.

b) Fail-maędur

Su tipinde faile iliřkin herhangi bir zellik belirtilmemiřtir. Bu ynyle bu suun faili herkes olabilir. Bu su maędur bakımından da herhangi bir zellik gstermez. Dolayısıyla her gerek kiři bu suun maęduru olabilir. Ancak fiilin bir insan zerinde gerekleřebileceęinden dolayı tzel kiřiler sutan zarar gren olarak kabul edilebilir.

Cezayı aęırlařtıran haller arasında ise fiilin

“Tacir veya řirket yneticisi olan ya da řirket adına hareket eden kiřilerin ticari faaliyetleri sırasında; kooperatif yneticilerinin kooperatifin faaliyeti kapsamında: Serbest meslek sahibi kiřiler tarafından, mesleklerinden dolayı kendilerine duyulan gvenin ktiye kullanılması suretiyle”

(m.158/1 h ve i) iřlenmesi yer almaktadır. Dięer taraftan;

“Grevinin saęladıęı gveni ktiye kullanmak suretiyle gerekleřtirdięi hileli davranıřlarla, kendisine veya bařkasına yarar saęlanması veya bu yolda vaatte bulunulmasını bir kimseyi ikna eden kamu grevlisi”

ikna suretiyle irtikap suunu iřlemiř olur (m.250/2) (zbek ve ark., 2017: 694).

Suun eylem unsurunun gerekleřmiř sayılması iin aldatılan ile zarara uęrayanın aynı kiři olmasının zorunlu olmadığı; su tipinde “bir kimseyi aldatıp, onun veya bařkasının zararına olarak” ibaresinin bulunmasından dolayı sylenmelidir. Ancak aldatılanın malvarlıęı zerinde tasarruf edebilme yetkisinin bulunması gerekir. Bu tr durumlarda hileye maruz kalarak

aldatılan kişi mağdurdur. Malvarlığında azalma meydana gelen kişi ise suçtan zarar gören olarak kabul edilmelidir. (Özbek ve ark., 2017: 695)

Mağdurun algılama yeteneğine sahip olması şart değildir, ancak hükümde “*Hileli davranışlarla bir kimseyi aldatmak*”tan söz edildiğine göre mağdurun failin hareketlerinin hileli olduğunu algılayabilecek yetenekte olması zorunlu görünmektedir. (Tezcan, Erdem ve Önok, 2009: 556)

c) Hileli davranışların gerçekleşmesi

Suç tipine uygun eylemin varlığı için; hileli davranışlarla bir kimseyi aldatıp, mağdurun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamış olması gerekir. Buna göre; eylemin hareket kısmını hileli davranışlarla bir kimseyi aldatmak; eylemin netice kısmını ise mağdurun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamış olmak kısmı oluşturur (Özbek ve ark., 2017: 696).

Dolandırıcılık suçunun oluşumu açısından öncelikle hileli bir davranışın gerçekleştirilmiş olması şarttır (Koca ve Üzülmüş, 2016: 648). Hile; diğerinin düşüncesi üzerinde etki yaratan hataya düşürücü her türlü davranış olarak tanımlanabilir. Böylece mağdurun gerçek hakkında yanlış bir düşünce ve inanca sahip olması sağlanmaktadır (Soyaslan, 2006: 342).

Dolandırıcılık suçunun unsurunu oluşturan hile, her halükarda bir olgu ile ilgili olmak zorundadır. Belli bir olgu ile ilgili olarak kişinin yanılgıya sevk edildiği hallerde hile bulunmaktadır. Bu haller; mevcut olmayan bir hususu mevcutmuş gibi göstermek, vuku bulmuş bir olayı bütünüyle veya belli unsurları itibarıyla gerçekleşmemiş göstermek ve nihayet gerçekleşmiş bir olgunun oluşum şekline başka unsurlar ilave etmek suretiyle gerçekleştirilir (Özgenç, 2002: 19).

d) Muhatabın aldatılmış olması

Hile; mağduru aldatacak ve mağdurun iradesi üzerinde etkili olarak onu hataya düşürecek nitelikte olmalıdır. Mağdurun içinde bulunduğu aldanmış olma durumu ile hileli davranışlar arasında nedensellik ilişkisi mevcut olmalıdır. (Centel, Zafer, Çakmut, 2007: 453) Aldatmaya elverişli davranışın varlığı failin cezalandırılması için yeterlidir. Mağdurun aldanmış olması neticenin meydana gelmiş olması değildir; mağdurun veya başkasının zararına olarak failin kendisine ya da başkasına bir yarar sağlanmadığı sürece dolandırıcılık suçu tamamlanmış olmaz. Hileli davranışa rağmen mağdurun aldanmadığı durumlarda, suç teşebbüs aşamasında kalmış olur. Aynı şekilde, hileli davranış sonucunda mağdurun aldandığı ve fakat menfaatin sağlanmadığı durumlarda da suç yine teşebbüs aşamasında kalmış olur (Özbek ve ark., 2017: 699).

e) Aldatılan kişinin, malvarlığı, üzerinde belli bir yönde tasarrufta bulunmuş olması suçun oluşumu bakımından mağdurun failin hileli davranışı sonucunda düştüğü hata ile malvarlığı üzerinde bir tasarrufta bulunması gerekir. Mağdur böyle bir tasarrufta bulunmadan malvarlığı fail tarafından alınırsa bu dolandırıcılık suçu değil, hırsızlık suçudur. Dolandırıcılık suçunda mağdur, üzerinde tasarruf yetkisine sahip olduğu malvarlığının zilyetliğini kendi iradesiyle devretmektedir (Önder, 1994: 377).

f) Bir zararın meydana gelmesi ve buna karşılık bir yararın sağlanmış olması

Hileli davranışlarla aldatma sonucu mağdura ya da bir başkasına bir zarar meydana gelmiş olmalıdır. Zararın bulunup bulunmadığı asıl olandır, zararın miktarı ve bu miktarın belirlenmesi önemli değildir. Zararın niteliği ise; zararın malvarlığına ilişkin olmasıdır. Malvarlığı kişiye ait, ekonomik değeri olan her şeydir (Özbek ve ark., 2017: 700).

Yarar da malvarlığına ilişkin olmalıdır. Faile ya da bir başkasına sağlanması arasında bir fark yoktur. Yararın sağlanması dolandırıcılık eyleminin netice kısmını oluşturur. Yararın aldatmanın sonucu olarak elde edilmesi gerekir (Özbek ve ark., 2017: 700)

2.3.3.2. Tipikliğin manevi unsurları

Dolandırıcılık suçu ancak kastla işlenebilir. Failin gerçekleştirdiği davranışın hile teşkil ettiğini ve aldatıcı nitelikte olduğunu bilmesi gerekir. Ayrıca fail mağdurun veya başkasının malvarlığına zararına olarak, kendisine veya başkasının malvarlığına ise bir yarar sağlamayı biliyor ve istiyor olması gereklidir (Özbek ve ark. 2017: 715).

Bu suçta özel kast aranmaz. Suç tipinde bir açıklık bulunmadığına göre dolandırıcılık suçunun olası kastla işlenmesinin de mümkün olduğu söylenebilir. Suçun nitelikli hallerinden bazılarında dolayı sorumluluğun doğması ve failin sorumlu tutulabilmesi için failin belirli bir maksatla hareket ettiğinin tespiti gerekir. (Koca ve Üzülmöz, 2016: 657)

2.3.4. Suçun nitelikli halleri

2.3.4.1. Cezada artırım yapılmasını gerektiren nitelikli haller

a) Suçun dini inanç ve duyguların istismar edilmesi suretiyle işlenmesi

Dolandırıcılık suçunun icrasında dini inanç ve duyguların bir aldatma aracı olarak kötüye kullanılması cezada artırım yapılmasını gerektiren nitelikli hal olarak kabul edilmiştir. Dolandırıcılık eyleminin bireyin dini inanç ve duygularının sömürülmesi, onlardan yararlanılması suretiyle işlenmesi durumunda bu nitelikli hal uygulanır. Madde gerekçesinde şöyle ifade edilmektedir:

“Bu nitelikli unsurun gerçekleşebilmesi için, dini inanç ve duygular, aldatma aracı olarak kötüye kullanılmasıdır.

Suçun oluşabilmesi için, dini inanç ve duyguların kötüye kullanılması suretiyle gerçekleştirilen hile ile haksız bir yarar da sağlanmış olmalıdır”. (Özbek ve ark., 2017: 702)

b) Suçun kişinin içinde bulunduğu tehlikeli durum veya zor şartlardan yararlanmak suretiyle işlenmesi

Dolandırıcılık suçu kişinin içinde bulunduğu tehlikeli durum veya zor şartlar varsa daha kolay işlenebilir. Bu tehlikeli durum ve zor şartların olması dolayısıyla; kişi, başkalarına güven

duymaya en fazla ihtiyaç duyduğu andadır. Bu neden; bu nitelikli halin kabul edilmesinin nedenidir (Özbek ve ark., 2017: 702).

c) Suçun kişinin algılama yeteneğinin zayıflığından yararlanmak suretiyle işlenmesi

Akıl zayıflığı, sarhoşluk, yaş küçüklüğü, yaşlılık algılama yeteneğinin zayıfladığı hallere örnek olarak gösterilebilir. Algılama yeteneği zayıf kişilerin aldatılması, bu yeteneği normal olanlara göre daha kolaydır. Bu nedenle madde gerekçesinde suçun kişinin algılama yeteneğinin zayıflığından yararlanmak suretiyle işlenmesi durumu, daha ağır ceza ile cezalandırılmayı gerektiren nitelikli unsur olarak kabul edilmiştir (Özbek ve ark., 2017:702).

Bu nitelikli hal, algılama yeteneği zayıflamış kişilere karşı işlenebilir. Algılama yeteneği ortadan kalkmış bir kişinin malvarlığına yönelik suçlar dolandırıcılık suçu kapsamında değil, hırsızlık suçu kapsamında değerlendirilebilir (Koca ve Üzülmöz, 2016: 660).

d) Suçun kamu kurum ve kuruluşlarının, kamu meslek kuruluşlarının, siyasi parti, vakıf ve dernek tüzel kişiliklerinin araç olarak kullanılması suretiyle işlenmesi

Kamu kurum ve kuruluşlarına örnek olarak Bakanlıklar, Sayıştay, Belediyeler verilebilir. Kamu meslek kuruluşları arasında ise ticaret ve sanayi odaları, ticaret borsaları, odalar ve borsalar birliği sayılabilir.

Bu bente göre; adı geçen kurum veya kuruluşların suçun işlenmesinde kolaylık sağlayacağı düşüncesinden dolayı; bu kurum veya kuruluşların dolandırıcılık suçunda araç olarak kullanılması nitelikli haller içinde düzenlenmiştir. Bu ağırlaştırıcı sebebin uygulanması bakımından; kurum veya kuruluşların tüzel kişiliklerine zarar verilmesi gerekli değildir. Önemli olan hileli davranışların icrasında bu kurum veya kuruluşların araç olarak kullanılmış olmasıdır (Özbek ve ark. 2017: 703).

Bu kurum ve kuruluşlarının araç olarak kullanılması; dolandırıcılık fiilinin gerçekleştirilmesinde bu kurum ve kuruluşlarının isminin geçirilmesi değil; hileli davranışların icrasında maddi olarak kullanılmış olmalarının gerektiğidir (Koca ve Üzülmöz, 2016: 661).

e) Suçun kamu kurum ve kuruluşlarının zararına olarak işlenmesi

Bu bentte suçun kamu kurum ve kuruluşlarının zararına olarak işlenmesi nitelikli hal olarak kabul edilmiştir. Bütün toplum adına kullanılması gereken bir malın dolandırıcılık suçu ile haksız bir şekilde belli bir kişiye veya kişilere yarar olarak sağlanması bu nitelikli halin kabulünü gerektirmiştir. Bu nitelikli halin uygulanabilmesi için; kamu kurum ve kuruluşlarının sadece isminin kullanılması yeterli olmaz. Maddi varlığının kullanılması da gerekmektedir. Araç olarak kullanılmaya örnek olarak; bu kurum veya kuruluşlara ait kimlik belgesinin, basılı evrakların, taşıtların amaç dışı olarak kullanılması gösterilebilir (Özbek ve ark., 2017: 706).

f) Suçun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi

Bu bentte iki ayrı nitelikli hale yer verilmiştir. Bu nitelikli haller; bilişim sistemlerinin araç olarak kullanılması ve banka veya kredi kurumlarının araç olarak kullanılmasıdır.

Gerçek kişilerin iradelerini sakatlamaya yönelik hileli davranışların bilişim sistemleri aracılığıyla gerçekleştirilmesi durumunda; dolandırıcılık suçunda bilişim sistemlerinin araç olarak kullanılmasından söz edilir. Burada hileli davranışların muhatabının gerçek bir kişi olması söz konusudur (Özbek ve ark., 2017: 707).

Dolandırıcılık filli gerçekleştirilirken bankaların olağan faaliyetlerinden hileli araçlar kullanılarak yararlanılması ve üçüncü kişilerin zararına haksız bir çıkar elde edilmesi veya banka ve kredi kurumlarının olağan faaliyetleri nedeniyle üretmiş oldukları maddi varlıkların suçta araç olarak kullanılarak haksız bir çıkarın elde edilmesi durumlarında; banka veya kredi kurumlarının araç olarak kullanıldığından söz edilebilir (Özbek ve ark., 2017: 708).

g) Suçun basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle işlenmesi

Her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim aracı; basın ve yayın aracıdır. İnternet, radyo, televizyon basın ve yayın aracına örnek olarak gösterilebilir. Eğer suçun

işlenmesinde bu basın ve yayın araçlarının kolaylık sağladığı ortaya konulursa; bu ağırlatıcı sebep uygulanabilir. Ağırlatıcı sebebin uygulanabilmesi için; basın ve yayın araçlarının kimin tarafından araç olarak kullanıldığı önemli değildir (Koca ve Üzülmez, 2016: 663).

h) Suçun tacir veya şirket yöneticisi olan ya da şirket adına hareket eden kişilerin ticari faaliyetleri sırasında; kooperatif yöneticilerinin kooperatifin faaliyeti kapsamında işlenmesi

Bu bentte de iki ayrı nitelikli hale yer verilmiştir. Dolandırıcılık suçunun oluşabilmesi için iki nitelikli hal şunlardır:

- tacir veya şirket yöneticisi olan ya da şirket adına hareket eden kişilerin ticari faaliyetleri sırasında işlenmesi,
- kooperatif yöneticilerinin kooperatifin faaliyeti kapsamında işlenmesi.

Kanun koyucu dolandırıcılık suçunun işlenişini kolaylaştırması ve tacir, şirket yöneticisi, şirket adına hareket eden kişiler ve kooperatif yöneticilerine olan güveni sarsması nedeniyle böyle bir ağırlatıcı sebebi kabul etmiştir (Koca ve Üzülmez, 2016: 664).

i) Suçun serbest meslek sahibi kişiler tarafından, mesleklerinden dolayı kendilerine duyulan güvenin kötüye kullanılması suretiyle işlenmesi

Burada fail, serbest meslek sahibi kişidir. Bu durumun nitelikli unsurlar içinde düzenlenmiş olması; ticari faaliyetlerin güven gerektiriyor olması ve serbest meslek sahibi kişilerin sıfatlarından yararlanarak dolandırıcılık suçunun işlenmesinin kolaylaşmasıdır. Bu nitelikli halin uygulanabilmesi için fiilin serbest meslek sahibi kişiler tarafından mesleklerinin icrası sırasında; mesleğin sağladığı güvenin kötüye kullanılması suretiyle işlenmesi gerekir (Özbek ve ark., 2017: 711).

j) Suçun banka veya diğer kredi kurumlarınca tahsis edilmemesi gereken bir kredinin açılmasını sağlamak maksadıyla işlenmesi

Bu nitelikli unsurun oluşması için; banka veya kredi kurumundan bir kredinin temini amacıyla hileli davranışlarda bulunulması ve buna bağlı olarak kredi adı altında bir yarar

sağlanması gerekir. Kredi kurumu deyiminden; banka olmamasına karşın, kanunen borç vermeye yetkili kılınan kurumlar anlaşılır (Özbek ve ark., 2017: 712).

Bu bente göre; suçun oluşumu bakımından failin kastın yanı sıra banka veya diğer kredi kurumlarınca tahsis edilmemesi gereken bir kredinin açılmasını sağlamak maksadıyla hareket etmesi gereklidir. Failin, banka veya kredi kurumlarının kredi tahsis etmekle görevli olan kişilere karşı hileli davranışları gerçekleştirmiş olması gerekir (Koca ve Üzülmöz, 2016: 666).

k) Suçun sigorta bedelini almak maksadıyla işlenmesi

Burada sigortanın türü ya da sigorta edilen riskin türü bu nitelikli halin uygulanması bakımından önemli değildir. Failin sigorta edilen veya sigorta bedelini alacak kişi olması şart değildir (Özbek ve ark., 2017: 712).

l) Suçun failin kendisini kamu görevlisi veya banka, sigorta ya da kredi kurumlarının çalışanı olarak tanıtması veya bu kurum ve kuruluşlarla ilişkili olduğunu söylemesi suretiyle işlenmesi

24/11/2016 tarih ve 6763 sayılı Kanun m.15 ile dolandırıcılık suçu bakımından yeni bir nitelikli hal öngörülmüştür. Değişiklik gerekçesinde şöyle ifade edilmektedir:

“kendilerini polis, hakim, savcı veya banka, sigorta ya da kredi kurumlarının çalışanı olarak tanıtan kişilerin, telefonla ulaştıkları mağdurları söyledikleri hikayelere inandırarak önemli miktarlarda haksız menfaat temin etmeleri, son dönemde artan bir sosyal duyarlılığın konusunu oluşturmaktadır. Mağdurlara ait olup, önceden temin edilen bazı kişisel bilgileri ve oluşturulan mizansel unsurları kullanan suç failleri, mağdurlarda güven oluşturabilmektedir. Ayrıca, eylemlerini çoğunlukla telefon gibi iletişim vasıtalarıyla gerçekleştirdiklerinden mağdurların denetim imkanı da büyük ölçüde kısıtlanmaktadır. Örneğin, mağdurların, herkesçe bilinmesine olanak bulunmayan bazı kişisel, ailevi, sosyal ve ekonomik durumlarına dair gerçek bilgileri de içeren umdurulmuş hikayeler karşısında, telsiz ve siren sesleriyle güçlendirilmiş bir mizansen içinde emniyetten arandıklarına inanabildikleri görülmektedir. Durumun ciddiyeti ve aciliyetine inandırılan mağdurların çoğu kez, görüşmeyi sonlandırarak konunun gerçekliğini araştırma imkanı da kalmamaktadır. Yoğun yalan ve hilelerle kandırılan mağdurlar, ciddi düzeyde ekonomik kayba uğramakta ve maddi birikimlerini kaybedebilmektedir. Bu şekilde gerçekleştirilen dolandırıcılık eylemlerinin sayısında önemli bir artış bulunmamakla birlikte, suç sebebiyle faillerce elde edilen haksız menfaat tutarında yıllar itibarıyla kayda değer bir artış izlenmektedir. Suç mağdurlarının profilinde belirgin bir ortak özellik görülmemekte; yaşlı veya genç, sosyo-ekonomik seviyesi düşük veya yüksek,

yüksek tahsilli veya değil, pek çok vatandaşı dolandırıcıların hedefi haline gelebilmektedir. Bu yönüyle konu, toplumun ortak sorunlarından biri haline gelmiştir. Söz konusu dolandırıcılık eylemleri, halihazırda basit dolandırıcılık suçu kapsamında vasıflandırılmakta ve tespit edilen failer 5237 sayılı Kanunun 157 nci maddesi uyarınca yargılanarak cezalandırılmaktadır. Ciddi ekonomik sonuçları dikkate alındığında, bu tür eylemlere, caydırıcılığı sağlayacak etkili yaptırımlar uygulanması gerekmektedir. Bu tür eylemlerin, dolandırıcılık suçunun nitelikli hallerini düzenleyen 158 inci madde kapsamında değerlendirilebilmesi ve suç faillerine daha etkili bir ceza verilebilmesi için anılan maddede düzenleme yapılmasına ihtiyaç bulunmaktadır. Suçla mücadele görevinin yerine getirilmesinde ceza siyasetinin belirlenmesi, bu çerçevede hangi eylemlerin ne tür ağırlıkta bir yaptırıma bağlanacağı, kanun koyucunun takdir yetkisi dahilindedir. Yukarıda açıklanan sosyal ve hukuki gerekçelere bağlı olarak, dolandırıcılık suçunun nitelikli hallerinin düzenlendiği yeni bir alt bent eklenmesine, ayrıca maddedeki ceza ihtiyacı duyulmuştur.”

Telefon dolandırıcılığı olarak bilinen, kişinin kendisini emniyet, jandarma, savcılık görevlisi olarak tanıtarak menfaat temin ettiği tüm haller bu fıkra kapsamında cezalandırılmaktadır.

m) TCK m.158/2’de yer alan ağırlatıcı sebep: Nüfuz Ticareti

Kamu görevlileriyle ilişkisinin olduğundan, onlar nezdinde hatırı sayıldığından bahisle ve belli bir işin gördürüleceği vaadiyle aldatarak, başkasından menfaat temin eden kişi; nitelikli dolandırıcılıktan dolayı cezalandırılacaktır. Söz konusu kamu görevlisinin kim ya da görevinin ne olduğu önemsizdir. Ancak failin genel olarak bir kurumdan söz etmesi yeterli değildir, “kamu görevlisini” açıkça zikretmesi gereklidir. Burada mağdurun da iyi niyet taşımadığı açıkça ortadadır. Ancak bu mağdurun hileli hareketlerle aldanmadığı ve bu nedenle iradesinin fesada uğramadığı demek değildir. Burada fail ile nüfuz ticaretinin konusunu oluşturan kamu görevlisi ayrı kişilerdir (Özbek ve ark., 2017: 713).

n) Suçun üç veya daha fazla kişi tarafından birlikte-örgüt faaliyeti çerçevesinde işlenmesi

24/11/2016 tarih ve 6763 sayılı Kanun m.14 ile, TCK m.158/3 fıkrası ilave edilmiştir. Bu fıkroda ilave edilen ağırlatıcı nedene göre dolandırıcılık suçunun üç veya daha fazla kişi

tarafından birlikte işlenmesi halinde verilecek ceza yarı oranında; suç işlemek için teşkil edilmiş bir örgütün faaliyeti çerçevesinde işlenmesi halinde verilecek ceza bir kat artırılır.

2.3.4.2. Daha az cezayı gerektiren nitelikli haller (m.159)

Dolandırıcılık suçunda da bir hukuki ilişkiye dayanan alacağı tahsil etmek amacıyla işlenmesi cezayı hafifleten nitelikli bir hal olarak düzenlenmiştir.

2.3.5. Suçun hukuka aykırılık unsuru

Dolandırıcılık bakımından mağdurun rızası hukuka uygunluk sebebi uygulama alanı bulabilir. Her ne kadar mağduru malvarlığına ilişkin değeri kendi rızasıyla veriyor olsa da hilenin varlığı rızayı sakatlar. Bu yönüyle söz konusu rızanın hukuki sonuç doğurduğundan söz edilemez (Centel, Zafer, Çakmut, 2007: 462).

2.3.6. Şahsi cezasızlık sebepleri veya cezada indirim yapılmasını gerektiren şahsi sebep

TCK; belli akrabalık ilişkilerini şahsi cezasızlık sebebi, bazılarını da fiili şikayete tabi hale getiren ve cezayı hafifleten şahsi bir sebep olarak kabul etmiştir. Bu konuda hırsızlık suçu başlığı altında yapılan açıklamalara bakılmalıdır (Özbek ve ark., 2017: 715).

2.3.7. Teşebbüs-etkin pişmanlık

Failin aldatmaya yönelik hileli davranışlarda bulunmuş olması ile icra hareketleri başlar ve suça teşebbüs mümkün hale gelir. Failin aldatmaya yönelik hareketleri suçun icrasına başladığı ve fakat mağdurun hileyi fark etmesi nedeniyle aldanmadığı veya failin hileli davranışlarda bulunup mağduru aldattığı ve fakat failin elinde olmayan nedenlerle yarar sağlayamadığı hallerde dolandırıcılık suçuna teşebbüs vardır. İcra hareketlerine başlandığının kabulü aldatıcı nitelikteki hileli davranışların varlığı yeterlidir. Bu suç, failin kendisine veya yarar sağlandıktan sonra, mağdurun uğradığı zararın giderilmesine yönelik olarak yapılanlar, etkin pişmanlık olarak şartlarının varlığı halinde m.168 kapsamında değerlendirilebilecektir (Özbek ve ark., 2017: 716).

2.3.8. Suçluların çokluğu (suça iştirak)

Dolandırıcılık suçu iştirak bakımından bir özellik arz etmez. Dolandırıcılık suçuna katılımda iştirakin her şekli mümkündür, ancak burada özellik gösteren konu; kendisine sadece haksız menfaat sağlanmış olmanın suçun hareket kısmına iştirak edilmediği sürece cezalandırılmayacağıdır. (Tezcan, Erdem ve Önok, 2009: 568). Yarar sağlayan ile hileyi gerçekleştiren kişinin birlikte suç işlemek için anlaşmış olması gerekir (Koca ve Üzülmez, 2016: 668).

2.3.9. Suçların çokluğu (suçların içtimai)

Dolandırıcılık suçunun aynı kişiye karşı farklı zamanlarda birden fazla işlendiği durumlarda, zincirleme suç hükümleri uygulanır (m.43/1). Koşullar varsa zincirleme suçun oluşması mümkündür, fakat bunun için de birden fazla dolandırıcılık fiilinin aynı mağdura karşı işlenmiş olması gerekir. Aynı zamanda, aldatılan ile zarara uğrayanın farklı kişiler olduğu hallerde, hileye muhatap olup aldatılan mağdur, malvarlığına zarar verilen kişi ise suçtan zarar görendir. Bu gibi hallerde de zincirleme suç hükümleri uygulanır (Özbek ve ark. 2017: 716). Madde 43/2 bendine göre; bir hileli davranışla birden fazla kişinin aldatıldığı ve zarara uğratıldığı dolandırıcılık fiilinin gerçekleştirildiği hallerde de aynı neviden fikri içtima söz konusudur ve zincirleme suç hükümlerine göre fail hakkında işlem yapılması gerekir (Koca ve Üzülmez, 2016: 668).

Madde 212' ye göre; dolandırıcılık suçunun hile unsurunun icrasında sahte belgeler düzenlenmiş ve kullanılmış olabilir. Bu gibi durumlarda; fail hem dolandırıcılık, hem de belgede sahtecilik suçundan sorumlu tutulacaktır (Koca ve Üzülmez, 2016: 668).

2.3.10. Yaptırım

Dolandırıcılık suçunun basit şeklinin cezası bir yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezasıdır. Adli para cezasının tayininde dolandırıcılığa konu olan ekonomik değerlerin mağdura veya suçtan zarar görene iade edilip edilmediği durumu göz

önünde bulundurulur. Nitelikli hallerin olması durumunda ise üç yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur. Ancak, (e), (f), (j), (k) ve (l) bentlerinde sayılan hallerde hapis cezasının alt sınırı dört yıldan, adli para cezasının miktarı suçtan elde edilen menfaatin iki katından az olamaz (Özbek ve ark., 2017: 717).

Dolandırıcılığın, bir hukuki ilişkiye dayanan alacağı tahsil amacıyla işlenmesi halinde altı aydan bir yıla kadar hapis veya adli para cezasına hükmolunur.

2.3.11. Muhakemesi

Dolandırıcılık suçu re'sen koğuşturulan bir suçtur. Ancak bu suçun, m.159'a göre bir hukuki ilişkiye dayanan alacağı tahsil amacıyla işlenmesi ya da m.167/2'ye göre fail ile mağdur arasındaki belli akrabalık ilişkisinin varlığı halinde suç şikayete tabi hale gelir. Bu durumda suç uzlaşmalı hale gelmektedir (Özbek ve ark., 2017: 717).

Dolandırıcılık suçu bakımından asliye ceza mahkemesi görevlidir.

3. Gereç ve Yöntem

Bu araştırma 2017 yılında, İstanbul ilinde gerçekleştirilmiş olup; hem telefon ile dolandırılanların hem de telefon dolandırıcılarının belirli bir tiplmesi olmaması nedeniyle gazete haberlerinden ve yaşanmış olaylardan yola çıkarak telefon dolandırıcılığı hakkında farkındalık oluşturmak, yeni mağduriyetlerin oluşmaması için gerekli koruyucu tedbir ve önlemlerin alınmasını sağlamayı amaçlamaktadır.

Araştırma, 2 basamaklıdır. Araştırmanın evreni ise telefon dolandırıcılığına maruz kalan tüm mağdurlardır.

Çalışmanın ilk basamağı en çok satan günlük gazetenin 1 yıllık arşivi taranarak telefon dolandırıcılığı haberleri ele alınıp kaç haber, mağdur yaşı, cinsiyet, çalışma hayatının içinde olup olmadığı, olayın çıkış biçimi, olayın sonuçları gibi parametreler bakımından incelenmiş; gazete haberlerinden oluşturulmuş bu veriler basit istatistiki yöntemle değerlendirilmiştir.

İkinci basamakta ise evreni tüm telefon dolandırıcılığı mağduru olan kişiler arasından 15 kadın ve 15 erkek örneklem belirlenmiştir. Araştırmada nitel araştırma yöntemi* kullanılmıştır. Veri toplama tekniği olarak ise derinlemesine mülakat yapılmıştır. Kendileri ile iletişime geçilmek suretiyle “Derinlemesine Mülakat”** yöntemi ile görüşme sağlanmıştır. Derinlemesine Mülakat sonucu elde edilen kayıtlar “İçerik Analizi” yöntemi kullanılmak suretiyle değerlendirilmiştir. Mülakat öncesinde katılımcılar ile “Bilgilendirilmiş Gönüllü Olur Formu Örneği” paylaşılmıştır (EK 1’e bakınız). Derinlemesine Mülakat yönteminde telefon dolandırıcılığına maruz kalan vakalara sosyo-demografik özellikleri ve olay ile ilgili sorular yöneltilmiştir. (EK 2’ye bakınız.)

* Nitel araştırma toplumsal gerçeklik hakkında bilgi edinmenin bir yoludur. Toplumsal bilimlerde niteliksel yaklaşım toplumsal bir olguyu keşfetmek, tanımlamak ya da açıklamak, insanların faaliyetlerine, durumlarına, olaylara ve eserlere yükledikleri anlamları açmak, toplumsal yaşamın bazı yönleri hakkında derin bir bakış açısı inşa etmek için kullanılmaktadır. İnsanları doğal ortamlarında inceleyerek, yeni veya araştırılmamış alanları keşfetmeyi;

bireylerle gruplar arası ilişkiler, kurumsal ve kültürel bağlamları aydınlatarak mikro ile makro arasında bağlantı kurabilmek amacıyla kullanılmaktadır (Leavy, 2014).

Nitel araştırma yapmadaki asıl amaç bireylerin kendi öznel koşullarını açıkça ifade edebilmesi ve onların deneyimlerinden yola çıkılarak anlaşılabilir sonuçlara ulaşmaktır. Nitel araştırmanın yerleşik bir tanımı olmadığı gibi araştırmaların tasarlanma süreci üzerine de pek çok teori vardır. Nitel araştırmada bütün sürece hakim olan mantıksal dizgeye 'araştırma deseni' denmektedir: Nitel araştırma varsayımlarla ve bireyler veya grupların bir sosyal ya da insan sorununa atfettikleri anlamlara değinen ve araştırma problemlerinin incelenmesini içeren yorumlayıcı/kuramsal çerçevelerin kullanımı ile başlar. Bu problemi araştırmak için, nitel araştırmacılar; araştırmada, çalışmadaki insan ve yerlere duyarlı olan doğal ortamdaki veri koleksiyonlarını ve hem tümevarım hem de tümdengelimli, örüntü ve temalar kuran veri analizlerini içeren nitel bir yaklaşım kullanırlar. Nihai yazılı bir rapor veya sunum; katılımcıların seslerini, araştırmacının derin düşüncelerini, problemin kompleks bir açıklama ve yorumlamasını, ve literatüre katkısını veya değişim çağrısını içerir (Creswell, 2013).

Çalışmada telefon dolandırıcılığı konusunda mağduriyet yaşamış kişiler ile derinlemesine mülakatlar yapılmıştır.

** Yıldırım ve Şimşek (2013) derinlemesine mülakatı; önceden belirlenmiş ve ciddi bir hedefe yönelik yapılan, karşılıklı soru sorma yöntemiyle yanıtlar alan etkileşime dayalı bir iletişim süreci olarak tanımlamaktadırlar. Derinlemesine görüşmelerde açık uçlu sorular sorulup cevaplar dinlenerek kaydedilirken konuyla ilişkili ek sorular sorularak araştırma konusunun detaylı incelenmesi mümkün olur. Bu görüşmeler konuşma ve ilişki başlatma sürecini kapsadığından, teknik beceri, duyarlılık, konsantrasyon gibi özelliklerin yanı sıra karşılıklı anlama içe bakış ve disiplin gerektirmektedir. Görüşmeci güven duygusu oluşturmalı, katılımcıyı konuşma konusunda cesaretlendirmeli, bu sürecin bir karşılıklı öğrenme ve paylaşımına dayandığını bilincini yaratmalıdır (Kümbetoğlu, 2015).

Yapılan derinlemesine mülakatlardan sonra "İçerik Analizi" yapılmıştır. Yıldırım ve Şimşek (2013) içerik analizini "verileri açıklayabilecek kavram ve ilişkileri belirleme yöntemi" olarak ele almıştır. Bu doğrultuda toplanan verilerde saklı bulunan gerçekler kavramsallaştırılıp, buna göre düzenleneceği belirtilmiştir (Yıldırım ve Şimşek, 2013).

Araştırma kapsamında, zaman ve maliyet açısından Türkiye'nin tümünde yapılması zor olacağından araştırma İstanbul ilinde telefon dolandırıcılığına maruz kalan kişiler ile derinlemesine mülakat yapılmıştır. Bu çalışma daha sonraki çalışmalara ışık tutacak nitelikte olup aynı çalışma Türkiye genelinde gerçekleştirilebilir. Araştırmaya katılanların soruları dürüst olarak doğru cevapladıkları varsayılarak, elde edilen sonuçlarda sadece İstanbul ili olarak genellenebilir. Telefon dolandırıcılığına maruz kalmış kişilerin bilgileri araştırmacıda var olmasına rağmen çalışmada gizlilik açısından ismi belirtilmemiş ve demografik özelliklerle

ilgili sorular sınırlı verilmiştir. Yapılan çalışmanın ikinci araştırma konusu ise ulusal nitelikte olan bir gazetede çıkan haberlerin taranmasıdır. Bu doğrultuda daha sonraki çalışmalar tüm ulusal ve yerel gazetelerin taranması olarak gerçekleşebilir.



4.Bulgular

Araştırmanın ilk basamağında; Ek 3’de yer alan bir ulusal gazetede 2017 senesi boyunca yayımlanan 29 telefon dolandırıcılığı ile ilgili haber incelendiğinde bir dizi sonuca ulaşmak mümkündür (29 haberin 7 tanesi topluma uyarı niteliğinde olup, 22 tanesinde bir dolandırıcılık haberi bulunmaktadır):

1. Dolandırıcılar; avukat, polis, savcı gibi toplum nezdinde güvenilirliği bulunan meslek gruplarının adlarını sıkça kullanmaktadır: 22 örnek olaydan 16 tanesinde bu üç meslek grubunun çeşitli kademeleri kullanılmıştır. Bu mesleklerin yanında Valilik ve Belediye Başkanı’nın adının kullanıldığı iki vakaya da rastlanmıştır. Burada; toplumun saygın bulunduğu ve ihtiyaç anında sarılacağı meslek grupları özenle seçilmekte, böylece mağdurların bazı tereddütler yaşasalar da itaat etmeleri yönünde subliminal mesajlar verilmektedir. 29 haberin 18’in de bu mesajlar verilmektedir.

2. Dolandırıcılar; toplumun hassasiyet gösterdiği maneviyatı kullanmaktadırlar. Bunlar; anne/baba sevgisi, terör örgütü üzerinden vatan sevgisi, takım sevgisi ve gelecek kaygılarıysa da terör örgütü üzerinden yapılan “vatana can feda” ifadeleri en çok kullanılan model olarak karşımıza çıkmaktadır. Bu başlıklardaki habere konu olma sayıları anne/baba sevgisi 1, vatan sevgisi 12, takım sevgisi 1, gelecek kaygısı 2 gazete haberinde yer almaktadır. 22 olayın onaltısında mağdurlar maneviyatları üzerinden dolandırılmışlardır.

3. Dolandırıcılar; muhakeme yeteneğinin azalmış olma ihtimali yüksek olan yaşça büyük ya da çok küçük vatandaşları hedef almaktadırlar. İzlenen haberlerin 8 tanesinde kurbanların yaşları açıkça belirtilmiş ve kurbanların büyük çoğunluğu (%90) 60 yaş ve üstü yaşlı ya da yaşça küçük çocuklardan oluşmaktadır.

4. Cinsiyetleri belli olan mağdur grubu için Kadın/Erkek dağılımı hemen hemen eşittir. Cinsiyeti belli olan 6 Kadın ve 5 Erkek haberi mevcuttur.

5. Mağdurların meslek durumları hakkında çok az bilgiye ulaşılmıştır: 1 mağdur polis memuru, 1 mağdur da büyükelçi olarak ülkesine hizmet etmiş emekli vatandaşlarımızdır.

Araştırmanın ikinci aşamasında; telefon dolandırıcılığına maruz kalan 15 kadın ve 15 erkek örneklem belirlenmiştir. Bu örneklem ile nitel yöntemle araştırma gerçekleştirilmiş ve derinlemesine mülakat yöntemi ile veriler toplanmıştır. Toplanan veriler içerik analizi kullanılarak değerlendirilmiştir. 30 vaka ile görüşme notları Ek 4'te yer almaktadır.

Görüşülen 30 vaka içerisinde 11 vakada telefon dolandırıcılığına maruz kalan mağdurların maddi kayba uğradığı görülmüştür. Bu 11 vakanın cinsiyet dağılımı 5 erkek ve 6 kadındır. Maddi kayıp aralığı 278 TL ile 130.000 TL arasındadır. Maddi kayba uğramış 11 vakanın; 5 tanesi yargıya başvurmamış, 6 tanesi ise polis ya da savcılığa müracaat etmiştir. Savcılığa müracaat edenlerin sayısı 3'tür. Bunlardan bir tanesinin işlemi devam etmektedir, iki tanesinde ise takipsizlik kararı verilmiştir. Polis müracaatlarında ise herhangi bir sonuç yoktur. Polis müracaatlarında mağdura söylenen; "bu tür kişilere kanmamaları gerektiği" olmuştur. Maddi kayıp olan 11 vakanın 9 tanesi hafta içi ve 2 tanesi hafta sonu gerçekleşmiştir. Aranma saatleri ise; hafta içi aranan vakalarda mesai saatleri içinde gerçekleşmiş olduğu dikkat çekmektedir. 6 tanesi banka, 2 tanesi terör, 1 tanesi arama motorunda çok görüntüleme sağlayan şirket, 1 tanesi dernek, 1 tanesi ise bir GSM operatörü tarafından arandığını mağdurlara söylemişlerdir. Sözkonusu 11 vakada dolandırıcılığa maruz kalanlardan 1'i ilkokul, 2'si lise, 3'ü lisans, 4'ü yüksek lisans ve 1'i de doktora mezunudur. Yani 11 vakada yer alan ve dolandırıcılığa maruz kalanlardan 8 tanesi lisans ve lisans üstü mezunudur.

Görüşülen dolandırıcılık olayları 2008-2017 yılları arasında gerçekleşmiştir. 4 tanesi 2008-2011 yılları arasında, 26 tanesi ise 2011-2017 arasında olmuştur. Görüşülen 30 vakanın; 5 tanesi görüşme yapılan yıl olan 2017 yılında, 8 tanesi 1 yıl önce, 8 tanesi 2 yıl önce, 4 tanesi 3 yıl önce, 1 tanesi 4 yıl önce, 3 tanesi 7 yıl önce ve 1 tanesi de 9 yıl önce gerçekleşmiştir. Yani olay 0 ila 9 yıl önce arasında gerçekleşmiştir.

9 yıl önce gerçekleşen en eski vakada; mağdura Emniyet Müdürlüğü tarafından arandığı söylenmiş ve isminin terör örgütüne karıştığı belirtilmiştir. 2008-2011 yılları arasında olan vakalarda mağdurun “terör örgütüne yardım ve yataklık ettiği” nedeniyle ve Emniyet Müdürlüğü tarafından arandığı belirtilmiş; ancak 2011-2017 yılları arasında olan vakalarda 10 tanesi banka, 7 tanesi Emniyet, 3 tanesi terör örgütü, 1 tanesi dernek, 1 tanesi arama motorunda daha çok görüntüleme sağlayan şirket, 1 tanesi GSM operatörü, 1 tanesi telefon faturasını sehven ödeme, 2 tanesi özel sağlık sigorta şirketi tarafından arandığını belirterek aranmışlardır.

Görüşülen dolandırıcılığa maruz kalanlardan olay gerçekleştiğinde yaşı en küçük olan vaka 20 yaşındadır, en yaşlı vaka ise 81 yaşındadır. Görüşülen 30 vakanın 6 tanesi 20-29; 3 tanesi 30-39; 12 tanesi 40-49; 4 tanesi 50-59; 1 tanesi 60-69; 3 tanesi 70-79 yaş aralığındadır. 1 tanesi ise 80 yaş ve üzerindedir. 50 yaş ve üzeri vaka sayısı 9'dur.

Mağdurlara medeni durumları sorulduğunda ise 30 vakadan 9 tanesinin bekar, 2 tanesinin dul ve 19 tanesinin evli olduğu yanıtı alınmıştır.

Mağdurların eğitim durumları ise 2 tanesi ilkokul, 5 tanesi lise, 1 tanesi önlisans, 10 tanesi lisans, 10 tanesi yüksek lisans, 1 tanesi doktora mezunu olduklarını belirtmişlerdir. 1 tanesi ise halen öğrencidir.

Görüşülen telefon dolandırıcılığına maruz kalan 30 vakanın 15 tanesi ücretli olarak çalışmaktadır. Serbest çalışan vaka sayısı 5 kişidir. Emekli olan kişi sayısı 7'dir. Çalışmayanların sayısı ise 3'tür.

Emekli olan 7 vakadan 4'ü emniyet güçleri tarafından arandığı belirtilerek aranmıştır. Bu 7 vakadan 5 tanesinde herhangi bir maddi kayıp olmazken; 1 tanesinde 900 TL'lik kalan limit kadar kredi kartından para çekildiği; 1 tanesinde ise çeşitli bankalarda olan 130.000 TL olan mevduatını çekip, arayanların belirttiği yerlere bırakan, 78 yaşında olan mağdur olduğu görülmüştür.

Telefon dolandırıcılığına maruz kalanlara aranma sayıları sorulduğunda ise; 30 vakadan 21 tanesi sadece bir kez arandığını belirtmiştir. 2 kez arandığını belirten kişi sayısı 7'dir. 2'den fazla arandığını belirten kişi sayısı ise iki kişidir. İki'den fazla arananlar ilk aramadan hemen sonra aranmamışlardır.

3 tanesi hafta sonu, 27 tanesi ise hafta içi arandıklarını belirtmişlerdir. 7 tanesi 9:00-11:00 saatleri arasında; 10 tanesi 11:00-13:00 saatleri arasında; 1 tanesi 14:00'da; 10 tanesi 16:00-18:00 arasında arandığını belirtmiştir. 19:00 ve sonrasında arandığını belirtenler ise 2 kişidir.

Görüşülen telefon dolandırıcılığına maruz kalan vakalara "telefon görüşmesinin yaklaşık kaç dakika" sürdüğü sorusu da yöneltilmiştir. Vakalardan 1 tanesi 2-3 dakika kadar çok kısa sürdüğünü belirtirken; en uzun konuşma süresi 90 dakika ile 78 yaşındaki vakaya aittir. Erkek vakalarda en uzun görüşme süresi 30 dakikadır. Yine erkek vakalarda ortalama görüşme süresi 11,66 dakikadır. Kadın vakalarda ortalama görüşme süresi 22,33 dakikadır. 30 vakanın ortalama görüşme süresi ise 16 dakikadır. 30 vakadan 11'i görüşme süresinin yaklaşık 5 dakika, 6 tanesi 10 dakika, 3 tanesi 15 dakika, 4 tanesi 20 dakika, 3 tanesi 30 dakika, 2 tanesi 45 dakika ve 1 tanesi de 90 dakika olduğunu söylemişlerdir.

Telefon dolandırıcılığına maruz kalan 30 vakanın 19 tanesi akıllı telefonundan aranmıştır. Tuşlu telefonundan aranan sayısı 5'tir. 6 vakada ise arananlar sabit telefondan aranmıştır.

5.Tartışma ve Sonuç

Dolandırıcılık, gündelik yaşamımızdaki ciddi tehditlerden birisi olmaya devam etmektedir. Suçun dinamik yapısı, insanları yeni yöntemlere karşı tetikte olmaya zorlamaktadır. Özellikle teknolojideki gelişmeler de faillerin işini daha da kolaylaştırmaktadır. Vatandaşın devletin korumasından en etkin şekilde yararlanması sağlanmalıdır.

Dolandırıcılar, telefon dolandırıcılığı faaliyetlerinde veri toplama, sosyal mühendislik ve resmi belgeleri ele geçirme yöntemlerini kullanarak kişi ile ilgili bilgileri elde etmekte, insanları amaçları doğrultusunda yönlendirmeye çalışmaktadır (Akbal, Doğan ve Varol, 2016).

Sosyal mühendislik, hedeflenen kurbanlardan fayda sağlamak için insan psikolojisini manipüle eden bir alan haline gelmiştir. Sosyal mühendislik, davranışçılık, insan iletişimi, bilgi teknolojisi ve psikoloji gibi farklı alanları incelemeyi gerektirdiği için dinamik bir olgudur . Sosyal mühendislik kapsamındaki tehditleri anlamak, sosyal problemlerin teknik sorunlardan çok daha karmaşık olan birçok sosyal-psikolojik sorunla ilişkilidir. İnsanlar yalanları tespit etmede iyi olduklarını düşünürler; ancak araştırmalar, insanların sosyal mühendislik saldırılarını tespit etmede yetersiz olduğunu ortaya koymaktadır (Algarni, 2016).

Kişisel özellikler sosyal mühendislik saldırılarındaki en önemli tetikleyici faktörler olarak kabul edilmektedir. Çeşitli araştırmalar, sosyal mühendislik saldırılarına katkıda bulunan kişisel özellikler arasında nevroitiklik, anlaşmazlık, dışadönüklük, vicdanlılık ve açıklık gibi özellikler olduğunu ortaya koymuştur (Cho ve ark., 2016).

Kişisel özelliklerin yanısıra demografik faktörlerin de bu tür saldırılarda savunmasızlığa neden olduğu düşünülmektedir. Yaş faktörü bunlardan bir tanesidir. Yapılan çalışmaların çoğu, sosyal mühendislik saldırılarının kurbanı olma ihtimali olan yaşlar arasında bir ilişki tespit etmektedir. İnternet kullanıcıları arasında, yaşlı insanların sosyal mühendislik saldırılarına düşme olasılığı daha düşükken, 18 ila 25 yaşlarındaki gençlerin sosyal mühendislik saldırılarının mağduru olma olasılığı daha yüksektir (Darwish, El Zarka ve Aloul,

2012). Yapılan çalışmada ise telefon dolandırıcılığına maruz kalan ve görüşülen 30 vakanın 12'si 40-49 yaş aralığındadır.

Araştırmalar ayrıca, cinsiyetin demografik bir özellik olarak, kullanıcının sosyal mühendislik saldırısına karşı savunmasızlığını artırdığını da göstermiştir. Kadınların erkeklere göre daha savunmasız olduğu düşünülmektedir. 2010 yılında yapılan araştırmaya göre kadınların %53.1'i sosyal mühendislik saldırılarına açıkken, erkeklerde bu oran %41 olmaktadır (Sheng, Holbrook, Kumaraguru, Cranor and Downs, 2010'dan akt. Darwish ve ark. 2012). Yapılan çalışmada ise yayımlanan telefon dolandırıcılığı ile ilgili gazete haberlerinde cinsiyeti belli olanlarda kadın/erkek dağılımı hemen hemen aynı çıkmıştır. 11 haberde mağdurun cinsiyeti belirtilmiştir. Bunlardan 6 tanesi kadın, 5 tanesi ise erkektir.

Psikolojik tetikleyicilerden aşırı yükleme, mağdurun zihinsel olarak pasif hale geldiği veya bir saldırganın beklenmedik bir perspektiften yararlanarak kişilere olmayan sözler vermesi ve bu şekilde kişileri acele ettirerek kişisel bilgilerini vermeye ikna etmesi tekniği olarak tanımlanmaktadır (Scheeres, 2008). Aşırı yükleme olduğunda, mağdur ya pasif ya da uyumlu hale gelecektir. Çok fazla bilgi ile çok hızlı bir şekilde ilgilenmek, mağdurun doğru bir karar verirken düşünmesini engelleyebilir. Saldırganın hızlı bir şekilde hareket etmesi gerekir, böylece kurban ne olup bittiğinden habersiz olacaktır. Böyle bir saldırı telefonla veya şahsen en iyi sonuçlara ulaşır. Bu şekilde mağdura, saldırganın taleplerine direnmesi ve boyun eğmesi için daha az zaman kalmaktadır.

İnsanların dolandırıcılık faaliyetlerine maruz kalmamaları için yeterince bilgilendirilmeleri gerekmektedir. Sanal ortamda yapılan dolandırıcılık faaliyetlerinin önlenmesinde devletin güvenlik ve gizlilik politikaları büyük önem teşkil etmektedir. Kişisel bilgilerin korunması ve gizliliğinin muhafaza edilmesi yolunda devlet bünyesinde yetişecek insan gücünün ve yapılacak çalışmaların artırılması ile insanların gizli bilgilerinin üçüncü şahıslar tarafından ele geçmesinin önlenmesi sağlanmalıdır. Telefon aracılığı ile yapılan

dolandırıcılık faaliyetlerinde insanların bir anlık korku, zafiyet, endişe gibi duygu değişimlerinden faydalanılmaması için önceki yaşanan vakalarda tespit edilen başlıklar resmi platformlar üzerinden duyurulmalı ve böylece insanların resmi platformlarda karşılaşılabilecekleri ve karşılaşamayacakları durumlar üzerine bir bilinç oluşturması sağlanabilmelidir (Akbal, Doğan ve Varol, 2016).

Sosyal mühendislik saldırılarının birtakım olumsuz etkileri bulunmaktadır. Türkiye Bankalar Birliği (2015: 11) bu olumsuz etkileri temel olarak; itibar kaybı, iyi niyet kaybı, finansal zarar, bilgilerin geri dönülemez ifşası, hukuksal problemler ve cezalar, kurumsal varlıklara yönelik zararlar, önlemeye ilişkin yatırım maliyetleri, zaman kaybı, işgücü kaybı ve güven kaybı şeklinde açıklamaktadır.

Başarılı sosyal mühendislik saldırıları, kurum ve kuruluşlar açısından birtakım tehlikelerin ortaya çıkmasına sebebiyet verebilmektedir. Bu tehlikeleri (Acılar ve Baştuğ, 2016: 294) şu şekilde belirtmektedir:

- i. *Yetkisiz erişim:* Saldırgan, sisteme erişmek üzere gereken bilgileri ele geçirebilmektedir.
- ii. *Hizmet hırsızlığı:* Ele geçirilen parolayla saldırı, erişim hakkı bulunmayan dosyalara ulaşabilmekte veya bant genişliği, işlemci zamanı, disk alanı gibi sınırlı kaynakları kullanabilmektedir.
- iii. *İtibar ve güven kaybı:* Sosyal mühendislikten ötürü zarara uğrayan bir kurum, müşterileri ile toplumun gözünde değer kaybedebilmekte ve tekrardan güven kazanabilmesinin bedeli, genellikle en baştan önlem almaktan çok daha fazla olabilmektedir.
- iv. *Dağıtık hizmet engelleme:* Elde edilen sistem ve kaynaklar, kötü maksatlı bireyler tarafınca başka sistem ve kaynakların ele geçirilmesi veya zarar verilmesi

hususunda kullanılabilir. Bu durumda dolaylı şekilde başka saldırılara neden olunabilmekte ve saldırının kaynağı aynı zamanda kurban olabilmektedir.

- v. *Hassas bilgiye erişim ve veri kaybı:* Başarılı bir yöntem ile kuruma ve müşterilere ilişkin bilgiler elde edilebilmektedir. Bu bilgiler kurum aleyhinde suiistimal hususunda kullanılabilir ve satılabilmektedir. Saldırgan yalnızca kurumun zarar görmesini istiyor olsa bile, bilgiye erişimi önleyebilir, şifreleme, silme vb. yöntemler ile erişimi imkansızlaştırabilmektedir.
- vi. *Yasal yaptırıma uğramak:* Müşteri ve iş ortakları ile gerçekleştirilen gizlilik ve güvenlik anlaşmalarının ve hassas bilgiyi korumak üzere önlem almamanın kanuni neticeleri ve yaptırımları olabilmektedir.

Sosyal mühendislerin saldırılarını önlemeye yönelik olarak, tüm açıkları kapamayı sağlayacak kesin bir yöntem yoktur. Ancak sosyal mühendislik eylemlerinin risklerini azaltabilecek ve bu eylemler neticesinde oluşabilecek muhtemel zararları en az düzeye indirebilecek birtakım yöntemler bulunmaktadır. Siber saldırılar hususunda bilgisayar ve ağ altyapısı ile ilgili tedbirler alınırken, sosyal mühendislik eylemleri için ise daha farklı savunma teknikleri oluşturulması gereklidir. Genel hacker eylemlerinden farklı şekilde, sosyal mühendislik eylemlerinde bireylerin bilgi seviyeleri ile kimlikleri önem kazanmaktadır. Bilgilerin yüksek hassaslık düzeyine ve değere sahip bulunduğu ortamlarda, sosyal mühendislik eylemleri yüksek düzeyde teknik bilgiye sahip bireyleri hedef alabileceği gibi, temizlik görevlisi ya da gece bekçisi gibi düşük düzeyde bilgiye sahip olan kişileri de hedef alabilmektedir. Bu bağlamda sosyal mühendisler, güvenlik zincirindeki en zayıf halka konumunda bulunan insan faktörüne odaklanmaktadır (Bağcı, 2009: 46).

Kurumların sosyal mühendislik saldırılarına maruz kalmalarına neden olan çeşitli önemli sebepler bulunmaktadır. Çatak (2016: 6) bu sebepleri yetersiz eğitim, güvenlik politikalarının eksikliği, bilgiye erişimde yeterli kural olmaması ve farklı birimler arasında iletişimsizlik

şeklinde ifade etmektedir. Bu bağlamda, sosyal mühendislik saldırılarından korunmak üzere uygulanabilecek yöntemler eğitim ve eğitim dışı tedbirleri şeklinde şu şekilde ikiye ayrılmaktadır (Bağcı, 2009: 46-47):

- i. *Eğitim tedbirleri:* Sosyal mühendislik saldırılarına karşı etkin bir güvenlik düzenlemesi yapılabilmesi hususunda gerçekleştirilen işin her bir safhasında ve bölümünde personel tarafından kullanılan bilgisayarlarla ilgili güvenlik düzenlemeleri yapılması gerekmektedir. Örgüt içerisinde yer alan bireylere güvenlikle ilgili bilgilerin tam ve net şekilde aktarılması, personele ağ güvenliğiyle ilgili sorumluluk duygusu aşılması örgütün faydasına olacaktır. Esasen en etkin savunma yöntemi, bireylerin sosyal mühendislik eylemleri ile her an istismara uğrayabileceklerinin öğretilmesidir. Bununla birlikte, kimliğini kanıtlayamayan kimseye personelin kesin suretle bilgi vermemeleri ve iş yaşamı ile özel yaşamlarını birbirinden ayırmaları konusunda gereken uyarıların yapılması ve önlemlerin alınması önem arz etmektedir. Bu sebeple personele güvenlik öngörülere ve güvenlik bilgileri hususunda bilgi güvenliği farkındalığı programı uygulanması gerekmektedir.
- ii. *Eğitim dışı tedbirler:* Eğitim faaliyetleri dışında da kurumların sosyal mühendislik saldırılarından korunmak üzere uygulayabilecekleri çeşitli tedbirler bulunmaktadır. Bu tedbirler ise temel olarak şu şekildedir:
 - a. *Fiziksel güvenliğin geliştirilmesi:* Kurumların sahip oldukları hassas ve değerli bilgilerin sosyal mühendislik saldırılarına karşı fiziksel güvenliğinin geliştirilmesi gereklidir. Fiziksel güvenliğin sağlanması, kurum dışında bulunan sosyal mühendislere karşı yararlı olabilecektir, fakat sosyal mühendisin kurum içerisinden olması halinde etkili bir fiziksel savunma söz konusu olmamaktadır. Bu sebeple sistemlere fiziki erişim olanağı bulunan bireylerin güvenilir olup olmadığının

gözden geçirilmesi, fiziki tehditlerin bulunma olasılığı çerçevesinde gereken önlemlerin alınması zaruridir. Ayrıca kurumda bulunan birtakım kullanıcı profillerinin sisteme erişim olanakları göz önünde bulundurularak, kullanıcı güvenlik politikalarında sıkılaştırma uygulamalarına önem verilmesi ve bütün kullanıcı profillerinin yetkilerinin belirlenmesi gereklidir.

- b. *Güçlü güvenlik politikası:* Hassas ve değerli bilgilere ilişkin kuvvetli denetim mekanizmalarının oluşturulması sosyal mühendislerin saldırıları hususunda caydırıcı bir unsur niteliğindedir. Kurum tarafından oluşturulan güvenlik politikalarının açık, anlaşılır, mantıklı, uygulanabilir, ulaşılabilir ve kapsayıcı olması gereklidir. Bu denetim mekanizmaları eğitim yoluyla desteklenmek suretiyle güçlendirilmelidir. Personele kurumsal güvenlik politikalarına ilişkin eğitimler verilmek suretiyle, güvenliğe ilişkin görev ve sorumlulukların öğretilmesi gerekmektedir. Bunun yanında, güvenlik politikalarının hazırlanma sürecinde kurum ile personel arasında makul bir güven düzeyi oluşturulmalıdır. Zira personele yeterli oranda güvenilmemesi halinde personelin kurumsal bağlılığı zayıflayacak, gereğinden çok güvenilmesi halinde ise personelden veya personel üzerinden gelebilecek sosyal mühendislik saldırılarına karşı sistem savunmasız kalacaktır.
- c. *Parola güvenliği politikası:* Kurumsal sistemlerde bulunmakta olan her tip bilginin parolalarla korunduğu, bu bilgilere sadece parolalar aracılığıyla erişimin sağlandığı bir ortamda, sosyal mühendisler açısından en önemli hedef kullanıcıların parolalarıdır. Parolalar, kullanıcıların erişmeyi arzu ettikleri bilgilere erişme yetkilerinin bulunup bulunmadığının kontrol edilmesine yaramakta olan bir araç niteliğine sahip olduğundan, parolaların yanlış ve kötü maksatlı kullanılması güvenlik problemleri ortaya çıkmasına sebebiyet verebilmektedir. Kullanıcılara ait hesapların izinsiz şekilde kullanılmasına karşı, kullanıcıların basit ve kolay şekilde

tahmin edilebilen parolalar tercih etmelerinin engellenmesi, belirlenen kriterlerle uyumluluk göstermeyen zayıf parolaların tespit edilerek gerekli uyarıların yapılması, gerektiği takdirde parola tercihlerine müdahalede bulunulması, bu hususta personelin bilgilendirilmesi ve bilinçlendirilmesi önem arz etmektedir. Bazı kullanıcılara ait parolaların tahmini kolay olmakta, bazıları iş bilgisayarlarına parola koymamakta, bazıları ise parolalarını bir kağıda yazarak masa üstüne bırakmaktadır. Sosyal mühendisler ise kullanıcıların parolalarını tahmin etmek üzere olası parolaları denemek suretiyle doğru parolayı bulmaya çalışmakta, bazı otomatik programlar aracılığıyla çok sayıda parolayı kısa bir zaman içerisinde deneyebilmektedir. Bu sebeple üst üste belli bir limitin üzerinde yanlış şifre girilmesi halinde kullanıcının hesabının devre dışı bırakılmasını sağlayacak güvenlik mekanizmalarının kullanılması önem arz etmektedir. Her bir hesap hususunda ayrı bir parolanın kullanılması ve parolaların belirli aralıklar ile değiştirilmesi, kullanıcıların parolalarının çalınması ya da hesaplarına izinsiz şekilde girildiğinden kuşkulı hallerinde uygulanması gerekli olan prosedürlerin saptanarak gereken önlemlerin alınması gerekmektedir.

- d. *Güvenlik kurallarına uymamanın yaptırımı:* Kurum tarafından uygulanan güvenlik politikalarına verilen önemin personel tarafınca yeterli şekilde anlaşılabilmesi durumunda, bu güvenlik politikalarının fazla bir değeri kalmamaktadır. Bu sebeple, eğitim faaliyetleriyle birlikte güvenlik denetimlerinin düzenli biçimde gerçekleştirilmesi, personelin uygulanan politikaların önemi hususunda farkındalıklarının artırılması gereklidir. Bunun yanında gerçekleştirilen denetimlerde güvenlik politikalarına aykırı davranışlar sergileyenlerin üst kademe tarafınca cezalandırılacağına ve güvenlik ihlallerinin affedilmeyeceğine ilişkin bilincin yerleştirilmesi gerekmektedir.

e. *Yönetim prosedürlerindeki olayların detaylandırılması:* Sosyal mühendislik saldırılarına karşı bilinçlendirme aktiviteleri önem arz etmekte olduğu gibi, saldırı esnasında uygulanacak metotların ve gerçekleştirilecek işlerin saptanması da önem arz etmektedir. Kurumda çalışan personelle iletişime geçmeye çalışan bireylerin kimliklerinin ne şekilde doğrulanacağı, saldırı eylemini fark eden çalışanın öncelikle hangi yetkili kişiye haber vereceği, kullanıcıların elektronik posta iletilerinin esas kaynaklarını ne şekilde belirleyecekleri, şüpheli elektronik postaları ne şekilde işleyecekleri, internet adreslerinin kimlik doğrulama bilgilerini ne şekilde denetleyeceği vb. detaylandırılmış prosedürlerin hazırlanarak uygulamaya geçirilmesi gereklidir. Sosyal mühendislik eylemleri genellikle bireysel zaafılar kullanılmak suretiyle gerçekleştirilmekte olduğundan, hedef bireyler saldırının farkına varmayabilmekte veya fark etse dahi kendi itibar ve güvenilirliğini zedeleyeceğini düşündüğünden eylemi ilgili mercilere iletmeyebilmektedir. Bu nedenle, saldırı eyleminin meydana gelmesinin ardından durumun yetkili personele aktarılması hususunda gereken prosedürler oluşturulmalıdır.

T.C. Sağlık Bakanlığı tarafından 16 Aralık 2015 tarihinde yayımlanmış olan “Sosyal Mühendislik Zafiyetleri ve Sosyal Medya Güvenliği” isimli belgede sosyal mühendislik saldırılarından korunmak üzere alınması gereken kişisel önlemler belirtilmiştir. Bu belgede yer alan önlemler arasında; kişinin taşınan ve işlenen verilerin öneminin bilincinde olması, özellikle telefon ile gerçekleştirdiği haberleşme faaliyetlerinde özel bilgilerin paylaşılmaması, kişiye özel bilgi olan parolanın sistem yöneticisi de dahil olmak üzere telefon ya da başka herhangi bir yol ile paylaşılmaması, “*Bilmesi Gerektiği Kadar*” prensibi çerçevesinde hareket edilmesi sayılabilir (T.C. Sağlık Bakanlığı, 2015).

Sosyal mühendislik saldırılarının önlenmesinde eğitim ve farkındalık hayati öneme sahiptir. Eğitim, çalışma ve farkındalık yaratılması ve bunların kullanılması, sosyal

mühendislik saldırılarının azaltılmasında yardımcı olacaktır. İnsanlar, durumun ne kadar farkında olursa, basit talimatları takip etmek konusunda o kadar duyarlı hale gelirler. Organizasyon, kapsamlı bir bilgi güvenliği stratejisi uygulayarak sosyal mühendislik saldırılarının etkisini azaltabilir (Baker ve Matar, 2011). Bu stratejiler, iyi yazılmış bir güvenlik politikasının yayınlanmasından, devam eden güvenlik bilincinin ve eğitim programlarının uygulanmasına, politika uyumluluğunu izlemek için denetleme programları kullanılmasına, güvenlik araçlarına izinsiz erişim ve güvenlik saldırılarına karşı sigorta satın alınmasına ve güvenlik cihazlarının kurulmasına kadar çeşitli önlemleri içermektedir (Baker & Matar, 2011). Bu süreçlerin uygulamaya koyulması, sadece şirket ortamında değil, aynı zamanda kişisel düzeyde de yararlı olabilir. Bireyleri çok fazla saldırıya karşı sorumlu tutmak ya da uygun politika ve prosedürleri izlememek, insanların bu saldırıların mağdurları olmasına izin vermektedir.

Yaşanan olayların sonuçlarına göre bilincin artırılabilmesi için eğitim gereklidir (Sheng ve ark., 2010). Sürekli gelişen veya değişen teknolojiye uyum sağlamak için, insanların sürekli eğitime ihtiyaçları vardır. Sosyal mühendislik taktiklerinin sürekli olarak gelişmesi, eğitim süreçlerinin sürekli değişen ortamlarla güncel kalması için düzenli olarak yapılması gerektiğini göstermektedir (Abraham & Chengalur-Smith, 2010).

Tüm çalışanlar yalnızca güvenlik için değil, aynı zamanda çok seviyeli bir savunmanın bir parçası olarak direnç göstermek konusunda eğitilmelidir (Gragg, 2002). Bir organizasyondaki anahtar personel; resepsiyonistleri, sekreterleri, müşteri hizmetlerini ve asistanları içerebilir. Bu kişiler bazı açılardan ilk savunma hattı niteliğindedir. Bu eğitim konuları sadece şirketler için değil, aynı zamanda kişisel düzeyde de kullanılmaktadır. Uygun direnç eğitimi verilmesi, saldırıya maruz kalanın bilgi vermek için kolayca ikna edilmemesini sağlayacaktır (Gragg, 2002).

Eđitim ve farkındalıđının etkili bir programa dđnüştürölmesi ile tüm bireylerin en güncel bilgilere sahip olmaları sağlanabilir. Saldırganlar sürekli olarak yöntemlerini deđiřtirmekte ve saldırılar daha karmařık hale gelmektedir (Kellyk, 2016). Deđiřimlere ayak uydurmak, bir sosyal mühendislik saldırısını önlemek konusunda çok önemlidir.

Sonuç olarak, sosyal mühendislik ve bir sosyal mühendislik saldırı çeřidi olan telefon dolandırıcılıđı saldırılarının devam etmesi ve durdurulamamasının bilinmesi; ancak önlenebileceđinin fark edilmesi, bu saldırıları başarılı bir řekilde anlamının anahtarıdır. Eđitim ve farkındalık temel olarak sosyal mühendislik saldırılarını önleyen faktörlerdir. Bir kiřinin sosyal mühendislik saldırılarına karşı kullanabileceđi en iyi savunma, çevresindekilerin farkında olmaktır. Kiři bu konu hakkında ne kadar çok řey bilirse, řüpheli bir durumla o kadar iyi başa çıkabilir. Teknoloji ne kadar deđiřirse deđiřsin; insanlar ikna edilmeye karşı her zaman savunmasız olacaktır. Bu nedenle, bir kiřinin bu tür saldırılara karşı alabileceđi en iyi önlem, çevresinde olup bitenin farkında olmaktır.

6. Kaynakça

- Abraham, S., ve Chengalur-Smith, I., 2010. An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32 (3), 183-196.
- Acılar, A. ve Baştuğ, A., 2016. İşletmelerde bir bilgi güvenliği tehdidi olarak sosyal mühendislik. *Global Business Research Congress (GBRC)*, May 26-27, Istanbul, Turkey.
- Adalet Bakanlığı, Adli Sicil ve İstatistik Genel Müdürlüğü “Adalet İstatistikleri Judicial Statistics 2015”, Eylül 2016.
- Akbal, E., Doğan, Ş., ve Varol, N., 2016 ‘Karar Ağaçları ile Telefon Dolandırıcılığı Verilerinin Analizi’, *Fırat Üniversitesi Fen ve Mühendislik Bilimleri Dergisi*, 29(01): 171-177.
- Akca, M.A., 2016. Sosyal mühendislik ile yapılan saldırıların doğal dil işleme teknikleri ile engellenmesine yönelik web servis geliştirilmesi. *Selçuk Üniversitesi Mühendislik Fakültesi Dergisi*, 4 (2), ss. 111-120.
- Algarni, A. A. M., 2016. The impact of source characteristics on users' susceptibility to social engineering Victimization in social networks. Doktora Tezi, Queensland University of Technology. Alıntı:
https://eprints.qut.edu.au/95604/1/Abdullah%20Ayed%20M_Algarni_Thesis.pdf
- Altun, İ., 2016. *Ortam Sanal Suç Gerçek*. İskenderiye Kitap, İstanbul.
- Artuç, M., 2007. *Malvarlığına Karşı Suçlar*. Ankara: Kartal Yayınevi.
- Artuk, M.E., Gökçen, A. ve Yenidünya, A.C., 2009. *Türk Ceza Kanunu Şerhi*. Ankara: Adalet Yayınevi.
- Atkins, B. ve Huang, W., 2013. A study of social engineering in online frauds. *Open Journal of Social Sciences*, 1(03), 23-32.
- Bağcı, H., 2009. Sosyal mühendislik ve denetim. *Denetışim Dergisi*, Kış, ss. 42-51.

Baker, A. ve Matar, A. (Eds.) 2011. Threat: Palestinian political prisoners in Israel.

Pluto Press.

Balcı, Y., 2018. Phishing and social engineering. Milli Savunma Üniversitesi Hezarfen Havacılık ve Uzay Teknolojileri Enstitüsü, 24 Ocak.

Barışkan, M.A., 2017. Türkiye'deki siber güvenlik bilinci ve sosyal mühendislik ataklarına karşı savunma önlemlerinin geliştirilmesi. Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi FBE.

Bayraktar, G., 2014. Harbin beşinci boyutunun yeni gereksinimi: siber istihbarat. Güvenlik Stratejileri Dergisi, 10 (20), ss. 119-147.

Bilen, M., 2012. Türk Ceza Hukuku'nda dolandırıcılık suçu. Doktora Tezi. Konya: Selçuk Üniversitesi SBE.

Bisson, D., 2015. 5 Social engineering attacks to watch out for. Alıntı:

<https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/>

Can, E.G., 2014. Dolandırıcılık suçu. Yüksek Lisans Tezi. Ankara: Çankaya Üniversitesi SBE.

Centel, N. Zafer, H. Çakmut, Ö. 2007 Kişilere karşı işlenen suçlar C.I. beta basım yayın İstanbul Nisan 2007

Cho, J. H., Cam, H., ve Oltramari, A., 2016. Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. In Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2016 IEEE International Multi-Disciplinary Conference, 7-13. IEEE. doi: 10.1109/COGSIMA.2016.7497779

Conteh, N.Y. and Schmick, P.J., 2016. Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks, International Journal of Advanced Computer Research, 6 (23), ss. 31-38.

- Creswell, J. W., 2013. Nitel Araştırma Yöntemleri: Beş Yaklaşımına Göre Nitel Araştırma Ve Araştırma Deseni. Siyasal Yayınevi, Ankara.
- Cross, C., 2016, 'They're Very Lonely': Understanding the Fraud Victimization of Seniors', International Journal of Crime, Justice and Social Democracy, 5(4): 60-75.
Araştırma Deseni. Siyasal Yayınevi, Ankara.
- Çatak, F.Ö., 2016. Bilgi toplama ve sosyal mühendislik ders notları. İstanbul: İstanbul Şehir Üniversitesi.
- Darwish, A., Zarka, A. E., ve Aloul, F., 2012. Towards understanding phishing victims' profile.
In Computer Systems and Industrial Informatics (ICCSII), 2012
International Conference on, IEEE, 1-5.
- Dönmezer, S., 2004. Kişilere ve mala karşı cürümler, 17. Basım. İstanbul: Seçkin Yayınları.
- Dursun, H., 2016. Türk ceza hukukunda dolandırıcılık suçu. Doktora Tezi. Ankara: Ankara Üniversitesi SBE.
- Erem, F. ve Toroslu, N., 2003. Türk ceza hukuku, özel hükümler. Ankara: Savaş Yayınları.
- Gündüz, M.Z. ve Daş, R., 2012. Sosyal mühendislik: yaygın ataklar ve güvenlik önlemleri. 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı ISCTURKEY 2012.
- Gragg, D., 2002. A multi-level defense against social engineering. Alıntı:
<http://taupe.free.fr/book/psycho/social%20engineering/Social%20Engineering%20-%20Sans%20Institute%20-%20Multi%20Level%20Defense%20Against%20Social%20Engineering.pdf>
- Hadnagy, C., 2013. Sosyal Mühendislik, İnsan Kandırma Sanatı, Paloma Yayınları, İstanbul.
- Hafizoğulları, Z., 2011. Türk ceza hukukunda dolandırıcılık suçları. Ankara Üniversitesi Yayınları.
- Hafizoğulları, Z. ve Özen, M., 2010. Türk ceza hukuku özel hükümler kişilere karşı suçlar. Ankara: Seçkin Yayıncılık.

- Hakeri, H., 2011. Ceza hukuku genel hükümler. Ankara: Seçkin Yayıncılık.
- İlbaş, Ç., 2009. Bilişim suçlarının sosyo-kültürel seviyelere göre algı analizi. Yüksek Lisans Tezi. Ankara: Başkent Üniversitesi FBE.
- Kara, B., 07.02.2016. <http://www.gazetevatan.com/dolandiricilar-15-gunlugune-oto-galeri-kuruyor-912310-pazar-vatan/> (01.05.2018)
- Kara, M., 2013. Siber saldırılar - siber savaşlar ve etkileri. Yüksek Lisans Tezi. İstanbul: İstanbul Bilgi Üniversitesi SBE.
- Kellyk, 2016. Social engineering basics: How to educate your staff. Alıntı.
<https://www.tracesecurity.com/blog/social-engineering-for-dummies-how-to-educate-your-staff#.Wf47U1uCxdg>
- Koca M., ve Üzülmöz İ., 2016. Türk Ceza Hukuku Özel Hükümler Adalet Yayınevi, Ankara, 3.baskı
- Kümbetoğlu, B., 2015. Sosyolojide ve Antropolojide Niteliksel Yöntem Ve Araştırma. Bağlam, İstanbul.
- Leavy, P. (Ed.), 2014. The Oxford Handbook Of Qualitative Research. Oxford University Press, New York.
- Luo, X., Brody, R., Seazzu, A. ve Burd, S., 2011. Social engineering: the neglected human factor for information security management. Information Resources Management Journal, 24 (3), ss. 1-8.
- Maviş, V., 2015. Dolandırıcılık suçunun hile unsuruna ilişkin sorunlar. İnönü Üniversitesi Hukuk Fakültesi Dergisi, 1 (1), ss. 597-626.
- McCumber, J., 1991. Information systems security: A comprehensive model. Proceedings 14th National Computer Security Conference. Baltimore: National Institute of Standards and Technology.

- Meraklı, S., 2009. Güveni kötüye kullanma suçu (TCK m. 155). Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 11, ss. 1657-1713.
- Meran, N., 2008. Yeni türk ceza kanununda sahtecilik- malvarlığı- bilişim suçları ile ekonomi ve ticaret alanında suçlar. 2. Basım. Ankara: Seçkin Yayınevi.
- Mitnick, K., 2002. The Art of deception. U.S.A.: John Wiley and Sons.
- Mitnick, K.D. ve Simon, W.L., 2006. Aldatma sanatı, Nejat Eralp Tezcan (Çev.). Ankara: ODTÜ Yayıncılık.
- Mouton, F., Malan, M. M., Leenen, L., Venter, H. S. (2014). Social engineering attack framework. Güney Afrika Bilgi Güvenliği, IEEE, 1-9.
- Murphy, L. L., 2017, 'Fraud', Salem Press Encyclopedia
- Önder, A., 1994. Şahıslara ve mala karşı cürümler ve bilişim alanında suçlar, Filiz Kitapevi. İstanbul.
- Özgenç, İ., 2002, Ekonomik çıkar amacıyla işlenen suçlar. Seçkin Yayıncılık.
- Paganini, P., 2017. The most common social engineering attacks. Alıntı:
<http://resources.infosecinstitute.com/common-social-engineering-attacks/#gref>
- Scheeres, J. W., 2008. Establishing the human firewall: Reducing an individual's vulnerability to social engineering attacks. Alıntı:
<http://www.dtic.mil/docs/citations/ADA487118>
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F. ve Downs, J. 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382. ACM.
- Selçuk, S., 1982. Dolandırıcılık evrimi, suç genel kuramı içindeki yeri. Ankara.

Selçuk, S., 1986. Dolandırıcılık cürümünün kimi suçlardan ayrımı ve çeklerle ilgili suçlar.
Ankara.

Soyaslan, D., 2005. Ceza hukuku özel hükümler, 5. Basım. Ankara: Yetkin Yayınları.

Soyaslan D., 2006. Ceza hukuku özel hükümler 5.Baskı Ankara

Soyaslan, D. 2010. Ceza hukuku özel hükümler, Yetkin Yayınları, Ankara.

Tatar, Ü., 2011. Sosyal mühendislik saldırıları. 4. Ağ ve Bilgi Güvenliği Sempozyumu, 25-26
Kasım, TÜBİTAK-BİLGEM.

T.C. Sağlık Bakanlığı, 2015. Sosyal mühendislik zafiyetleri ve sosyal medya güvenliği. 16
Aralık.

Tezcan, D., Erdem, M.R. ve Önok, M., 2008. Teorik ve pratik ceza özel hukuku. Ankara.

Tezcan, D., Erdem, M.R. ve Önok, M., 2009. Teorik ve pratik ceza özel hukuku. Ankara 5.baskı

Trend Micro, (t.y.). TrendLabs Dijital yaşam e-kılavuzu: sosyal mühendislik numaralarının işe
yaramasının 5 nedeni.

Tümerkan, S. 1987. Dolandırıcılık Suçu. Kazancı Hukuk Yayınları. İstanbul

Türkiye Bankalar Birliği, Dolandırıcılık Eylemleri ve Korunma Yöntemleri, Aralık 2015.

Tüysüz, F., 2017. Dolandırıcılık suçu. Yüksek Lisans Tezi. Ankara: Başkent Üniversitesi SBE.

Özbek v. Ö., Doğan K., Bacaksız P., Tepe İ. Türk Ceza Hukuku özel hükümler, Seçkin
Akademik ve Mesleki Yayınlar, Ankara, Eylül 2017, 12.baskı.

Vural, Y., 2007. Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri. Yüksek Lisans
Tezleri. Ankara: Gazi Üniversitesi FBE.

Wilding, E., 2006. Information Risk and Security, Gower, Aldershot, UK.

Wright, O., 2015, Hacking without computers - an introduction to social engineering.

Alıntı: <https://www.contextis.com/blog/hacking-without-computers-an-introduction-to-social-engineering> 21 Eylül 2017.

- Yalkut, N., 1979. Türk, Fransız ve İtalyan ceza hukuku açısından dolandırıcılık suçu. Adalet Dergisi, (3-4)
- Yalvaç, G., 2015. Ceza ve yargılama hukuku yasaları; T.C. Anayasası, TCK, CMK, CGTİK ve ilgili mevzuat, 7. Basım. Ankara: Adalet Yayınevi.
- Yaşar, O., Gökcan, H.T. ve Artuç, M., 2010. Yorumlu-uygulamalı Türk ceza kanunu, Cilt 4. Ankara: Adalet Yayınevi.
- Yıldırım, A. ve Şimşek, H., 2013. Sosyal Bilimlerde Nitel Araştırma Yöntemleri. Seçkin Yayıncılık, Ankara.
- Yılmaz, A., 2015. Türkiye deki dolandırıcılık tiyolojiieri: dolandırıcılık olaylarının kategorik tasnifi ve yapıliş şekilleri. Hacettepe Üniversitesi Sosyoloji Araştırmalar E-Dergisi, ss. 1-26.
- Yılmaz, Z. ve Ergün, İ., 2005. Yeni Türk ceza kanununda dolandırıcılık suçları. Ankara: Seçkin Yayıncılık.

7.Ekler

EK 1-Bilgilendirilmiş Gönüllü Olur Formu Örneđi

Deđerli Katılımcı,

Katılmanızı istediđimiz bu alıřma, İstanbul Üniversitesi Adli Tıp Enstitüsü Sosyal Bilimler Anabilim Dalı'nda yürütölmekte olan bir yüksek lisans tezi kapsamında gerçekleştirilmektedir.

Arařtırmada, telefon dolandırıcılıđına maruz kalanların incelenmesi hedeflenmektedir.

alıřmaya katılım gönüllölük esasına dayalıdır. Arařtırmaya toplam 30 katılımcının dahil edilmesi planlanmaktadır. Kararınızdan önce arařtırma hakkında sizi bilgilendirmek istiyoruz.

Bu alıřma bilimsel bir alıřma olup, size dođrudan bir fayda sađlamamaktadır. Bu bilgileri okuyup anladıktan sonra arařtırmaya katılmak isterseniz onay kutusunu iřaretleyiniz. Bu alıřmaya katılmanız için sizden herhangi bir ücret istenmeyecektir. alıřmaya katıldıđınız için size ek bir ödeme de yapılmayacaktır.

Arařtırma tamamen gizlilik esasına dayanmaktadır. Bu nedenle sizden kimlik bilgilerinizi ortaya koyabilecek hi bir veri talep etmemekteyiz. alıřmamızın sonuçları sadece akademik amalı kullanılacak olup, bařka hibir platformda kullanılmayacak, herhangi bir kiři ve kurumla paylařılmayacaktır.

Arařtırmanın herhangi bir ařamasında sizi rahatsız eden veya yanıt vermek istemediđiniz herhangi bir durum oluřursa, arařtırmadan istediđiniz zaman ayrılmanız mümkündür.

alıřmamızın ilk kısmında sizden birkaç anket ve form doldurmanız istenecektir. Bu formlar karar verme stillerinizi ölçmeye ve kiřilik özelliklerinizi belirlemeye yönelik anket ve formlardır. Form ve anket doldurma ařamasından sonra ise size verilen bir senaryo ile ilgili nasıl bir karar verdiđiniz sorulacaktır.

alıřmamız ve sonuçları hakkında ayrıca bilgi edinmek istemeniz halinde, ařađıda ekli olan telefon numarası veya e-posta adresi aracılıđıyla arařtırmacılarla iletiřime geebilirsiniz.

Verdiđiniz destek ve katılımınız için teřekkür ederiz.

Hatice TUĐSAVUL

Dr. Öğretim Üyesi Mustafa OKUDAN

İstanbul Üniversitesi Adli Tıp Enstitüsü Sosyal Bilimler Anabilim Dalı

İletişim: Hatice TUĐSAVUL

Telefon: 0 505 4452058

E-posta: htugsavul@gmail.com

Bilgilendirilmiş gönüllü olur formundaki tüm açıklamaları okudum. Bana yukarıda konusu ve amacı belirtilen “.....” isimli araştırma ile ilgili yazılı açıklama yapıldı. Araştırmaya gönüllü olarak katıldığımı, istediğim zaman gerekçeli veya gerekçesiz olarak araştırmadan ayrılabilceğimi biliyorum. Söz konusu araştırmaya hiçbir baskı ve zorlama olmaksızın kendi rızamla katılmayı kabul ediyorum.

Katılımcı ad soyad:

Uygulayıcı ad soyad:

Tarih:

Tarih:

İmza:

İmza:

EK 2-Derinlemesine Mülakat Soruları

1. SOSYO-DEMOGRAFİK ÖZELLİKLER

- YAŞ (ŞİMDİKİ)
- MEDENİ DURUM
- ÖĞRENİM DURUMU
- ÇALIŞMA DURUMU

2.OLAY İLE İLGİLİ SORULAR

- OLAYIN GERÇEKLEŞTİĞİ ZAMANDAKİ YAŞI
- OLAYIN KAÇ YIL ÖNCE GERÇEKLEŞTİĞİ
- HANGİ GÜN VE SAATTE ARANDIĞI
- GÖRÜŞME SÜRESİ
- ARANAN TELEFONUN ÖZELLİĞİ
- ARANMA NEDENİ
- MADDİ KAYIP OLUP/OLMADIĞI
- POLİSE/SAVCILIĞA GİDİP/GİTMEDİĞİ
- TEKRAR ARANIP/ARANMADIĞI

3.Eklemek istedikleriniz?

EK 3-2017 Yılında En Çok Satış Yapan Ulusal Gazete Yayımlanan Telefon Dolandırıcılığı Haberleri

1- Savcı ve Polisten Sonra Şimdi de Avukat. (2017, 30 Kasım). Hürriyet Akdeniz (Ref.

No: 72212643). s.3.

SAVCI VE POLİSTEN SONRA ŞİMDİ DE AVUKAT

Antalya/HÜRRİYET

ANTALYA'da avukatların ismini kullanarak "Sigorta borcunuz var, icra takibi başlatıyoruz" diyen dolandırıcılar, vatandaşın 500 ila 2 bin lira arasında değişen ödeme talep ediyor. Dolandırıcılık yönteminin detaylarını Hürriyet'e anlatan mağdur Hakan Dinçkan (48), "Cep telefonumdan ulaşan bir şahıs, kendisini avukat olarak tanıtıp birkaç yıl önce sigorta yaptırdığımı ancak prim ödemelerimi geciktirdiğimi söyledi. Şahıs, mevcut borcumun 3 bin liraya ulaştığını, hemen ödeme yaparsam bu bedelin 540 liraya ineceğini anlattı" dedi.

'EK ÖDEME İSTEDİLER'

Şaşkınlık yaşadığını anlatan Dinçkan, "Ödemeyi yapacağımı söyleyince bana banka hesap numarasını verdiler. Telefonu kapatıp ödemeyi yaptım. Hatta avukatın ismini internet üzerinden doğruladım. 1 saat sonra yeniden aradım. İcra takibi masraflarının karşılanması için 1100 lira daha ödeme yapmam istenince avukatımı aradım" diye konuştu.

Avukatı ile yaptığı görüşmeden sonra dolandırıldığını anladığını vurgulayan Dinçkan, şöyle dedi: "Sigorta borcum falan yokmuş. Beni arayan kişi de avukat değilmiş. İsmi kullanılan avukatın Ankara'da görev yaptığını ve yaşananlardan haberdar olmadığını sonradan öğrendik. Bu olay bana 540 liraya mal oldu."

'HAKLARIMIZI BİLMİYORUZ'

Tüm uyarılara rağmen vatandaşların telefon dolandırıcılarının tuzağına düştüğünü kaydeden Tüketiciler Birliği Derneği Antalya Şube Başkanı Neşet Gündüz, "Maalesef tüketici olarak haklarımızı öğrenmiyoruz. Telefondaki kişilere hemen inanıyoruz. Lütfen parasal işlem yapmadan önce 2 kez düşünelim" dedi.



Özel bir sigorta şirketi ve Türkiye'nin çeşitli illerinde görev yapan avukatların ismini kullanan telefon dolandırıcıları, Antalya'da onlarca vatandaşı mağdur etti.

'Ben dolandırmadım, onlar bana dolandı'

ADANA'nın Seyhan ilçesinde kendisini polis olarak tanıtan Emin A., Günay D.'yi (79) arayıp, "FETÖ ile bağlantınız var, adınız bazı olaylara karışmış, sizin masum olduğunuzu biliyoruz. Evinizde ne kadar altın ve para varsa vermeniz lazım" dedi. Yaşlı kadın, evinde bulunan yarım kilo külçe altın, 10 bin TL ve 1000 Euro'yu poşete koyup evine gelen Emin A.'ya verdi. Emin A., daha sonra Ömer T.'yi (65) aynı yöntemle arayıp bankadaki 80 bin TL'sini çekti ve poşet içerisinde bıraktığı parktaki ağacın dibinden aldı.

Mağdurların şikâyeti üzerine Yankesicilik ve Dolandırıcılık Büro Amirliği 50 güvenlik kamerasını inceleyerek dolandırıcının kimliğini ve adresini tespit etti. Şafak vakti düzenlenen operasyonla Emin A, dedesinin evinde yakalandı. Sorgusunda, "Sarhoştum, bir şey hatırlamıyorum" iddiasında bulunan Emin A, sağlık kontrolüne götürülürken gazetecilere, "Ben kimseyi dolandırmadım, onlar bana dolandı. Benim alakam yok, varsa cezamız yatarız. Bende vicdan ne gezer, ben kendime aileme acımıyorum" dedi.

■ Çağlar ÖZTÜRK/DHA



Emin A. "Bende vicdan ne gezer, ben kendime, aileme acımıyorum" dedi.

ALO...SPOR

DOLANDIRICILAR

Beşiktaş, F.Bahçe ve G.Saraylıları işte böyle kandırıyorlar

- 1** KONGRE ÜYELERİNİ VE TARAFKARLARI TELEFONLA ARAYIP, 'LİSANSLI ÜRÜNLERİ İNDİRİMLİ SATIYORUZ' DİYORLAR.
- 2** GÜVEN TELKİN ETMEK İÇİN ÜRÜNÜ KARGO İLE ADRESE GÖNDERİP, KAPIDA ÖDEME YÖNTEMİNİ SEÇİYORLAR
- 3** KAPIDA TESLİM EDİLEN PAKETİN İÇİNDE 10 TL'LİK LİSANSLI ÜRÜN YERINE 10 TL'LİK TİŞÖRT YA DA KAŞKOL ÇIKIYOR

Ödeme belgesi gönderen adreste boş bir oda çıktı!

BEŞİKTAŞ, Fenerbahçe ve Galatasaray kulüpleri Call Center yöntemi ile dolandırıcılık işlemlerini sık sık yetkililerle paylaşarak ediyorlar. Ama ne yazık ki bir basın eylemi değil. En fazla 1903, 1905, 1907 gibi uzantılı olan telefon numaralarını izip edebiliyorlar. Beşiktaş, ödeme belgesi gönderen

Hürriyet, Fikret Orman-Fellaini görüşmesinde ne konuşulduğunu açıklıyor

FELLAINI'E BAŞ BAŞA

Orman, siyah beyazlı takımın Monaco'yu 2-1 yendiği gün tesadüfen bir araya geldiği Fellaini'ye, "Beşiktaş'a gelir misin?" diye sordu. Belçikalı yıldız, önceliğinin Manchester United olduğunu, orada bir sorun çıkmaya halinde gelebileceğini söyledi.



ÖNCEKİ aksam İngiliz Daily Mirror gazetesinin haberi Beşiktaşlılar heyecanlandırdı. Gazete, Manchester United'da forma giyen Belçikalı oyuncu **Marouane Fellaini**'nin 8 milyon sterlin karşılığında siyah beyazlı kulübe transfer olacağını yazdı.

Haberin ayntısında Manchester United'ın son Chelsea mağlubiyetinden sonra Portekizli menajer **Jose Mourinho**'nun Fellaini'ye mac sorusu ovgular yağdırdığı, bu sözlerin ise Belçikalı orta sahanın takımdan ayrılacak olması sebebiyle ayakta olduğu bilgisi verildi.

Mirror'un bu haberi karnen doğrudur. Fellaini de Beşiktaş bir görüşme yaptı. Görüşme siyah beyazlıların Monaco'yu 2-1 yendiği gün yani 17 Ekim'de Monaco'da gerçekleşti. **Fellaini**, Belçikalı'nın Bosnia Hersek ile oynadığı milli maçta sakatlanması ve onun yerine Man Utd formasından uzak kalması.

UEFA'YA GÖRE HANGİSİ DAHA BÜYÜK?

Fenerbahçe mi, Galatasaray mı?

TARİH: 1 Kasım 2017. Yar Uskumru Restaurant. UEFA Yönetim Kurulu Üyesi **Servet Yardımcı**, UEFA'nın medya sorumlusu **Pedro Pinto**, 10 ülkenin önemli gazetecileri ve Türkiye'deki spor müdürlerini Beşiktaş-Monaco maçını izlemek için Beşiktaş'a davet etti. UEFA eski başkanı **Joseph S. Blatter** de katıldı. **Beşiktaş'ta hangi taraftarlar daha büyük?**

Sonra arka plana yaslanıyor ve Türk gazetecileri zor durumda bırakmanın mucizeleri ile galibiyetleri. Vatandaşlar da Beşiktaşlılar ile görüşüyor. Vatandaşlar da Beşiktaşlılar ile görüşüyor. Vatandaşlar da Beşiktaşlılar ile görüşüyor.

UEFA'YA GÖRE HANGİSİ DAHA BÜYÜK?

Fenerbahçe mi, Galatasaray mı?

TARİH: 1 Kasım 2017. Yar Uskumru Restaurant. UEFA Yönetim Kurulu Üyesi **Servet Yardımcı**, UEFA'nın medya sorumlusu **Pedro Pinto**, 10 ülkenin önemli gazetecileri ve Türkiye'deki spor müdürlerini Beşiktaş-Monaco maçını izlemek için Beşiktaş'a davet etti. UEFA eski başkanı **Joseph S. Blatter** de katıldı. **Beşiktaş'ta hangi taraftarlar daha büyük?**

UEFA'YA GÖRE HANGİSİ DAHA BÜYÜK?

Fenerbahçe mi, Galatasaray mı?

TARİH: 1 Kasım 2017. Yar Uskumru Restaurant. UEFA Yönetim Kurulu Üyesi **Servet Yardımcı**, UEFA'nın medya sorumlusu **Pedro Pinto**, 10 ülkenin önemli gazetecileri ve Türkiye'deki spor müdürlerini Beşiktaş-Monaco maçını izlemek için Beşiktaş'a davet etti. UEFA eski başkanı **Joseph S. Blatter** de katıldı. **Beşiktaş'ta hangi taraftarlar daha büyük?**

UEFA'YA GÖRE HANGİSİ DAHA BÜYÜK?

Fenerbahçe mi, Galatasaray mı?

TARİH: 1 Kasım 2017. Yar Uskumru Restaurant. UEFA Yönetim Kurulu Üyesi **Servet Yardımcı**, UEFA'nın medya sorumlusu **Pedro Pinto**, 10 ülkenin önemli gazetecileri ve Türkiye'deki spor müdürlerini Beşiktaş-Monaco maçını izlemek için Beşiktaş'a davet etti. UEFA eski başkanı **Joseph S. Blatter** de katıldı. **Beşiktaş'ta hangi taraftarlar daha büyük?**

UEFA'YA GÖRE HANGİSİ DAHA BÜYÜK?

Fenerbahçe mi, Galatasaray mı?

TARİH: 1 Kasım 2017. Yar Uskumru Restaurant. UEFA Yönetim Kurulu Üyesi **Servet Yardımcı**, UEFA'nın medya sorumlusu **Pedro Pinto**, 10 ülkenin önemli gazetecileri ve Türkiye'deki spor müdürlerini Beşiktaş-Monaco maçını izlemek için Beşiktaş'a davet etti. UEFA eski başkanı **Joseph S. Blatter** de katıldı. **Beşiktaş'ta hangi taraftarlar daha büyük?**

UEFA'YA GÖRE HANGİSİ DAHA BÜYÜK?

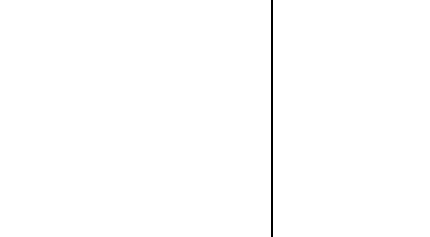
Fenerbahçe mi, Galatasaray mı?

TARİH: 1 Kasım 2017. Yar Uskumru Restaurant. UEFA Yönetim Kurulu Üyesi **Servet Yardımcı**, UEFA'nın medya sorumlusu **Pedro Pinto**, 10 ülkenin önemli gazetecileri ve Türkiye'deki spor müdürlerini Beşiktaş-Monaco maçını izlemek için Beşiktaş'a davet etti. UEFA eski başkanı **Joseph S. Blatter** de katıldı. **Beşiktaş'ta hangi taraftarlar daha büyük?**

UEFA'YA GÖRE HANGİSİ DAHA BÜYÜK?

Fenerbahçe mi, Galatasaray mı?

TARİH: 1 Kasım 2017. Yar Uskumru Restaurant. UEFA Yönetim Kurulu Üyesi **Servet Yardımcı**, UEFA'nın medya sorumlusu **Pedro Pinto**, 10 ülkenin önemli gazetecileri ve Türkiye'deki spor müdürlerini Beşiktaş-Monaco maçını izlemek için Beşiktaş'a davet etti. UEFA eski başkanı **Joseph S. Blatter** de katıldı. **Beşiktaş'ta hangi taraftarlar daha büyük?**



Beşiktaş'ın lisanslı ürününü satkılarını iddia eden şirketin gönderdiği paketten 10 liralık spor çeyrek çıkar.

ERFENDİM FENERBAHÇE SPOR KULÜBÜ NEDEN ARIYORUZ?

Beşiktaş Kartal Yuvaları'nın rahatsız ediyoruz.

Galatasaray Kulübü adına arıyoruz.

Bu gibi telefonlarla taraftarlara ürün pazarlıyorlar. Üstelik indirimi ürünün.

Sayın başkan Fikret Orman, kulüp üyeleri arasında 100 kişilik VIP sipariş beliledi. Bunların içinde siz de varınız. Kulübe katılı için 169 TL'lik formayı size indirimli olarak 110 TL'ye satıyoruz.

MÜŞTERİ BİR MAĞAZA İÇİN BİR DÜNYA YÖNTEMLERİ OLUNCA ÇARPICI

'Transfere para bulmak için ürün satıyoruz!'

MÜŞTERİ bulmak için bedelleriyle yönetilen birisi bu. Bir diğeri ise oldukça çarpıcı ve yaratıcı. Diyelim ki gazetesinde X futbolcunun X kulübüne transferi için bir haber çıktı. **Erfendim X'in transferi için katkı sağlamak ister misiniz? Kulübümüzün ürünü satma ile bu transferi gerçekleştiriyoruz.** Kulüpün bir şekilde elde ettikleri datalara sahip oldukları için taraftarlar

üzerinde inandırıcı oluyorlar. Güven telkin etmek için de ürünü kargo ile adrese gönderiyorlar ve kapıda ödeme yöntemini seçiyorlar. Kulüp tarafından arandığını düşününler de sipariş veriyor. Ancak kapıda teslim alıp ürünün paketini açmadan ödemeyi yapmaları dolandırıcıların çok çabuk öğreniyorlar. Kulübün lisanslı ürünü diye 110 TL aldıkları formanın yerine paketten 10 liralık tişört ya da kaşkol çıkıyor.

HÜSEYİN MİCAN, KARGO İLE GÖNDERİLEN ÜRÜNLERİ KABUL ETMEDİ

Kartal Yuvaları'nın yöneticisini bile aradılar!

DOLANDIRICILAR istiyorsa her tür şeyleri yapabilirler. Beşiktaş Kulübü'nün Kartal Yuvaları'ndan Her iki Beşiktaş yöneticisi de taraftarlara bu yöntemi uygulamalarını tavsiye ediyorlar. **Hüseyin Mican** bu dolandırıcılık yöntemini müthiş bir okunmuş yarıttığını söylüyor.

CALL CENTER ALDATICI İLE MİLYONLAR KAZANIRLAR

Data toplamak için taraftarla anket yapıyorlar

HÜSEYİN MİCAN a taraftarları 'telefonla satış' yoluyla dolandıran bu yöntemin hacimlerini soruyorum. **-1-2 milyon TL var mıdır?** Daha da fazladır. En az 5 milyon TL'ye ulaşmıştır. Bunun da açıklanmasını yapıyor. **-Öncelikle bir Call Center açıyorlar. Burada en az 10 kişi çalışıyor. Üstelik inandırıcı olan diye telefonla ulaşıyorlar taraftarlar telefon numarası diğer taraftan Call Center çalışanlarını seçerler de**

Telefonla satış yapmak isteyenleri sorgulayın

PEKİ, kulüp üyeleri ve taraftarları telefonla arayarak lisanslı ürün satkılarını iddia eden dolandırıcılara karşı ne yapmalı. Kulüp yöneticilerinin önerisi şu: Bu tür telefonlar gelince karşı tarafı sorgulayın. Çünkü pek çok çalışan yöneticisi isimlerini bile biliyor. Ayrıca sipariş verseniz bile imza yapmadan sipariş verin ve adrese teslimde ürünü almayın. Böylece dolandırıcılar o türünden tamamen zarar etsinler.

BEŞİKTAŞ VE GALATASARAY CALL CENTER İLE SATIŞ YÖNTEMLERİNİ SORUYOR.

FENERBAHÇE: 0850 300 1907 ve 0212 200907 numaralı ile satış yapıyor.



BEŞİKTAŞ VE GALATASARAY CALL CENTER İLE SATIŞ YÖNTEMLERİNİ SORUYOR.

4- Telefon Dolandırıcısı Yakalandı. (2017, 11 Kasım). Ankara Hürriyet (Ref. No: 71646488). s.4.

Telefon dolandırıcısı yakalandı

ESKİŞEHİR’de telefonda kendisini **polis** olarak tanıttığı kadının 4 bin 800 TL parasını ve altınlarını dolandıran 19 yaşındaki F.K., **Ankara**’da yakalandı. Edinilen bilgilere göre, F.K., telefon ile aradığı A.İ.’ye, "Kimlik bilgileriniz **terör örgütünün** eline geçmiş, banka da bulunan paranızı sahte belgeler ile çekecekler, şahısları takip ediyoruz. Yakalamamız için evinizdeki altın ve paraları bir poşete koyup, görevlimize teslim edin" dedi. A.İ. de poşet içerisine koyduğu 4 bin 800 lira para ile 4 altın **bilezik**, 9 Cumhuriyet altını ve 1 altın yüzüğü eve gelip kendisini **polis** olarak tanıtan F.K.’ya teslim etti. Bir süre sonra dolandırıldığının farkına varan A.İ., **polise** ihbarda bulundu. F.K.’nın **otobüsle Ankara**’ya gittiğini belirleyen ekipler, **Başkent polisine** bilgi verdi. Altın ve paralarla kısa sürede yakalanan F.K., **Eskişehir**’e gönderildi. ■ Eyüp KELEBEK/DHA

Dolandırıcı uyarısı

■ UŞAK Belediyesi, kentte dolandırıcıların Belediye Başkan Yardımcısı Mustafa Dayıođlu'nun adını kullanarak para talebinde bulduklarını belirterek, vatandaşları dikkatle olmaları konusunda uyardı. Yapılan yazılı açıklamada, belediyenin, personelin veya yöneticilerin asla vatandaşları telefonla arayarak para isteyeceđi vurgulanarak, "Bu tip telefonlara itibar edilmemeli" dedi. ■ UŞAK, (DHA)

Sahte savcı TELEFONUN UCUNDA

ETİMESGUT'ta yaşayan G.K.'yı telefonla arayan dolandırıcı, kendisini 'hakim ve savcı' olarak tanıttı. G.K.'nın sahibi olduğu

para ve ziynet eşyalarının seri numaralarının terör örgütü tarafından ele geçirildiğini söyleyen dolandırıcı, bu durumdan kurtaracağını vaat ederek para ve ziynet eşyalarını istedi. Paniğe kapılan G.K., 13 bin 500 dolar, 10 altın bi-



lezik ve 25 altınını dolandırıcıya verdi. Daha sonra dolandırıldığını anlayan G.K, durumu jandarmaya bildirdi. Şüphelinin kimliğinin tespiti ve yakalanması için çalışma başlatan jandarma ekipleri, teknik takip sonucu cezavi firarisi olduğunu tespit ettiği V.V.'yi (29) bir kafeye düzenlediği operasyonla yakaladı. Operasyonda üzerinden sahte kimlik çıkan şüphelinin Bahçelievler'de yaşayan F.G.'yi de 4 Ekim'de yine aynı yöntemle 30 bin lira dolandırdığı belirlendi. Şanlıurfa merkezli bir dolandırıcı çetesinin üyesi olduğu değerlendirilen şüphelinin bağlantılarının tespiti için çalışmaların sürdüğü öğrenildi. ■ AA

7- Hollanda'da Kazandı Aydın'da Kaptırdı. (2017, 2 Kasım). Hürriyet Almanya (Ref.

No: 71353189). s.3.

HOLLANDA'DA KAZANDI AYDIN'DA KAPTIRDI

Yıllarca Hollanda'da çalıştıktan sonra Aydın'a yerleşen Muammer Arpalı (70), 230 bin lirasının, telefonla arayan ve kendisini polis olarak tanıtan kişilerce alındığını ileri sürerek şikayetçi oldu.



CUMHURİYET Mahallesi'nde yaşayan Muammer Arpalı, polisi arayıp, kendisini telefonda polis olarak tanıtan kişilerin, "Hesabınızın bulunduğu banka yolsuzluk yapıyor. Hesabındaki tüm parayı çekip bizim söylediğimiz hesaba havale et" diyerek para talep ettiğini, ilk olarak 80 bin lirayı istenilen hesaba yatırıldığını daha sonra da eve gelen bir kişiye 150 bin lira verdiğini, ardından dolandırıldığını anladığı için şikay-

etçi olduğunu bildirdi.

Birikimlerinin dolandırılmasından dolayı çok üzgün olduğunu belirten Arpalı, şöyle dedi:

"Sabahleyin bir telefon geldi. Kendilerini komiser olarak tanıttılar. Bir bankada yolsuzluk olduğunu ve operasyon yapılacağını söylediler. Bizi de çok korkuttular. Bizi kandırdılar bütün paralarımızı aldılar. Operasyon falan yalanmış. 80 bin lirasını bankadan havale ile gön-

derdik. 150 bin lirayı da bankadan para çektik ve eve gelip bizden teslim aldı."

'TV'DE İZLİYORDUK'

"Yıllarca Hollanda'da tekstil fabrikasında çalıştım bu paraları biriktirmek için. Şimdi yıllardır biriktirdiğim paralarım gitti. Biz de her gün televizyonlarda dolandırılanları izledik. Nasıl inanıyorlar diyorduk ama işte bizi de kandırdılar." ■ AA

8- Bu Defa Dolandırıcı Tuzağa Düştü. (2017, 20 Ekim). Bursa Hürriyet (Ref. No: 70948059). s.3.

Bu defa dolandırıcı tuzağa düştü



Bursa'da yaşlı adamı dolandırmak isteyen dolandırıcılar, para yerine ellerine kum dolu poşet verilerek kısıvrak yakalandı.

Nilüfer ilçesinde yaşayan R.Ş'yi arayan telefon dolandırıcıları, kendilerini komiser olarak tanıtip, hesabından FETÖ terör örgütüne para aktarıldığını, bu şahısları yakalamak için operasyon yaptıklarını söyledi. Dolandırıcılar, R.Ş'den bankadaki parasını çekmesini istedi. Karşısın-

dakilerin dolandırıcı olduğunu anlayan R.Ş, hemen polise haber verdi. R.Ş ile irtibata geçen ekipler, dolandırıcı ile telefon görüşmesini sürdürmesini istedi. R.Ş, dolandırıcıyı polislerin istediği adrese çekerek, içine kum doldurulmuş poşeti verdi. Poşeti alan E.U. olay yerinden uzaklaşırken, polis ekipleri tarafından kısıvrak yakalandı. Ekipler tarafından ifadesi alınan E.U. adliyeye sevk edildi.

DOLANDIRILMaktan KOMŞULARI KURTARDI

Nabi YAZICI/DHA

KOCAELİ'nin Körfez İlçesi'nde, 52 yaşındaki Salih İrak, telefon dolandırıcılarına parasını kaptırmaktan komşuları sayesinde kurtuldu.

Kuzey Mahallesi Esentepe Caddesi'nde oturan Salih İrak'ı arayan telefon dolandırıcıları, kendilerini polis olarak tanıttı. Dolandırıcılar, terör örgütlerinin hesabından 25 bin lira kredi kullandığını söyledikleri İrak'ı bankaya yönlendirdi. Evden dışarı çıkan Salih İrak'ın telaşlı



halini gören komşuları, devreye girdi. Komşularının uyardığı Salih İrak, polise haber verdi. Dolandırıcılar ise başarısız olacaklarını anlayınca telefonu kapattı. İhbar üzerine gelen polis ekibi, Salih İrak'ı polis mer-

kezine götürerek ifadesini aldı.

ALTINLARI SORDULAR

Salih İrak telefon dolandırıcılarının çok inandırıcı olduklarını söyleyerek, "Benim bile hatırlamadığım özel bilgilerimi sıraladılar. Bana öncelikle emekli olduğumu ve şu anda terör

örgütlerinin hesabımdan 25 bin lira kredi kullandıklarını, operasyon yapacaklarını söylediler. Evde altınım olup olmadığını da sordular. Beni bankaya yönlendireceklerdi ki; komşularım durumu anlayıp, uyardı" dedi.

Yaşlıları telefonda dolandırma ÇETESİ

ESKİŞEHİR’de, önceki gün 61 yaşındaki M.A.’yı telefonla arayan ve kendilerini polis olarak tanıtan dolandırıcılar, “Kimlik bilgileriniz terör örgütünün eline geçmiş. Bankadaki paranızı çekecekler. Ayrıca kuyumcu soyulmuş, kimlik bilgileriniz bırakılmış” dedi. Dolandırıcılar, M.A.’dan evdeki altınlarla paraları poşete koyup, eve gönderecekleri sivil polise teslim etmesini istedi. M.A.’nın o sırada evdeki yakınları, telefonda kişilerin dolandırıcı olabileceği şüphesiyle polisi aradı. Olay yerine gelen polisler bir süre sonra para ve altınları almaya gelen S.İ. ve H.D.’yi yakaladı. Şüphelilerin, önceki gün de S.U.’yu (61) dolandırdığı belirlendi. **DHA**



SAHTE POLİSLERE PARASINI KAPTIRDI

Telefonla aradıkları kişilere kendilerini 'savcı' ve 'polis' olarak tanıtır, hesaplarının FETÖ'nün eline geçtiğini öne sürerek dolandırıcılık yapan 3 kişilik şebeke yakalandı.

AYNI gün içinde telefonla aradıkları 2 kişiye kendilerini polis ve savcı olarak tanıtan 3 dolandırıcı, iddiaya göre, aradıkları kişilere banka hesaplarının FETÖ'nün eline geçtiğini söyleyip korkutarak paralarını kendilerine teslim etmelerini söyledi. Dolandırıcılar mağdurlara, bazı kişilerin telefon edip kendilerini polis olarak tanıtabileceklerini, bu nedenle arayanlara parola sormalarını, 'tavşan' yanıtı vermeyenlere güvenmemelerini söyledikleri belirtildi. Dolandırıcıların konuşmalarına inanan mağdurlardan 38 yaşındaki A.D. 35 bin lira parayı buluşma noktasına götürüp dolandırıcılara teslim etti.

KAÇARKEN YAKALANDILAR

Daha sonra dolandırıldığı anlayan A.D. durumu polis ekiplerine bildirdi. Asayiş Şube Müdürlüğü Yankesicilik ve Dolandırıcılık Büro Amirliği ekipleri 60 iş yeri güvenlik kamerasından yaptığı incelemede şahısların



İstanbul'da yaşayan 30 yaşındaki Şeyhmus S. ve 30 yaşındaki Ercan Y. olduğunu belirledi. İstanbul Emniyet Müdürlüğü ekipleri ile birlikte evlerinden alınan Şeyhmus S. ve Ercan Y., ifadelerinde 30 yaşındaki Hüseyin B.'nin de dolandırıcılık şebekesinde olduğunu söylemeleri üzerine Hüseyin B. memleketi Şanlıurfa'ya kaçarken Atatürk Havalimanı'nda yakalandı. Yankesicilik ve Dolandırıcılık

Büro Amirliği ekipleri yaptığı araştırmada 40 yaşındaki B.G.'nin de 45 bin lirasını dolandırıcılara kaptırdığı, olay nedeniyle kendisini telefonla arayan polis ekiplerine inanmayarak parola sorduğu belirtildi. İstanbul'dan Bursa'ya getirilen şüpheliler emniyetteki işlemlerinin ardından adliyeye sevk edildi. Şeyhmus S., adli kontrol koşulu ile serbest bırakılırken diğer iki şüpheli tutuklandı.

Dolandırıcılar için KREDİ ÇEKİ

Karacabey'de telefon dolandırıcılarının ağına takılan A.A.'nın parasını polis kurtardı. Başka bir vatandaş ise dolandırıcılara 7 bin lirasını kapırdı.

KARACABEY'DE meydana gelen **dolandırıcılık** olayında; bir vatandaşın **ATM** önünde sürekli telefonda konuştuğunu ve işlem yapmaya çalıştığını görenler, durumdan şüphelenerek **polis** ekibi, vatandaşın dolandırıcıların hesabına **ATM**'den 2 bin lira aktardığı ve 19 bin lira parayı da **PTT**'den dolandırıcının verdiği hesaba yeni gönderdiği bilgisini aldı. Vatandaşın hesabına bloke koyduran **polis** ekiple 19 bin lira paranın dolandırıcıların eline geçmesini engelledi.

ŞOK YAŞADI

A.A.'nın dolandırıcılara **PTT** şubesinden gönderdiği parayı **bankadan** kredi çekerek temin ettiği öğrenildi. **Polisin** "dolandırılıyorsunuz" uyarısına inanmakta güçlük çeken vatandaş, yaşadığı şokun ardından ifa-



desi alınmak üzere emniyete götürüldü.

Karacabey'de yaşanan bir diğer **dolandırıcılık** olayında ise; B.O. isimli vatandaş, kendisini **polis** olarak tanıtan kişiye 7 bin lirasını kapırdı. İddiaya göre B.O., parayı toparlayabilmek için evinde bulunan ziynet eşyalarını bozdurdu ve parayı **ATM**'den direkt olarak dolandırıcının hesabına aktardı. **Polis**, her iki dolandırıcılık olayı ile ilgili soruşturma başlattı. ■ **Yasin KESKİN**

13- Çocuğu Kandırıp Dolandırıcılık Yapan Çete Çökertildi. (2017, 24 Eylül). Ankara

Hürriyet (Ref. No: 70181961) s.3.

Çocuğu kandırıp dolandırıcılık yapan çete çökertildi

Telefonda kendilerini polis ve savcı gibi tanıtır, anne ve babasının tehlikede olduğunu söyledikleri 11 yaşındaki çocuktan 20 bin lira değerinde ziynet eşyası alan dolandırıcı 5 şüpheli, jandarma ekiplerince yakalandı. Şüpheliler, çıkarıldıkları mahkemece tutuklandı.

Etimesgut Bağlıca Mahallesi'nde takibe aldıkları 11 yaşındaki bir çocuğu 13 Eylül'de telefonla arayıp, kendilerini polis ve savcı olarak tanıtan şüpheliler, "Annen ve baban tehlikede" diyerek çocuktan evlerindeki değerli eşyaları, söyledikleri otobüs durağındaki "polislere" teslim etmesini istedi.

Bu sırada iş yerinde olan anne ve babası için endişelenen çocuk, evlerindeki ziynet eşyaları talimatlara uyarak dolandırıcılara teslim etti. Eve döndüklerinde çocuklarından olayı dinleyen anne ve baba durumu jandarmaya bildirdi.

Etimesgut Merkez Jandarma Komutanlığı bünyesinde kurulan özel ekip, çocuğun parayı

teslim ettiği otobüs durağının çevresindeki güvenlik kameraları ile o bölgedeki MOBESE kameralarının kayıtlarını incelemeye aldı. Kameralardan şüphelilerin kullandığı aracın plakasına ulaşan ekipler, plakanın kayıtlı olduğu adrese gittiklerinde evin fuhuş suçundan mühürlendiğini gördü.

Jandarma, bunun üzerine mühürlenmeden önce evde ikamet eden şüpheli Tuncay A'yı ailesinden öğrenilen yeni adresinde gözaltına aldı.

Tuncay A. sorgusunda, dolandırıcılık çetesinde Gülşah T'ye bağlı olduğunu itiraf etti. Tuncay A'ya telefonda aratılan ve bir yerde buluşmaları sağlanan Gülşah T. de gözaltına alındı. Gülşah T. ifadesinde çetenin diğer üyeleri İbrahim Bahtiyar D, Bayram Emrah A. ve Halil İbrahim K'yi deşifre etti.

Jandarmanın soruşturması sonucunda tek tek gözaltına alınan şüphelilerin, aralarında telefon bağlantısını sağlayanları "atıcılar", dolandırma olayının yapılacağı yere gidenleri

"aracılar" ve para ile değerli eşyaları alanları "alıcılar" diye kodlayarak organize oldukları tespit edildi.

Ankara'da bugüne kadar 4 dolandırıcılık olayına karıştıkları belirlenen ve haklarında çok sayıda aynı suçtan kaydı bulunan 5 şüpheli, çıkarıldıkları mahkemece tutuklandı.





Banka taklidi yapan dolandırıcılar sesli yanıt yöntemiyle bütün kredi kartı bilgilerini alıp vatandaşa hizmet vermiş gibi gösteriyor ve tüm parasını çekiyor. Vatandaş da bilinçsizce bu alışverişe onay verdiği için hukuki olarak da hakkını aradığında zor duruma düşüyor.

Bankalar Birliđi'nden dolandırıcılık uyarısı

VATANDAŞ BU OYUNA KANMA!

TÜRKİYE Bankalar Birliđi (TBB), yeni bir dolandırıcılık taktiđi ile ilgili vatandaşları uyardı. Uyarıya göre, banka görevlisi gibi arayan dolandırıcılar promosyon verileceđi veya para iadesi yapılacağı bahanesiyle müşterileri sesli yanıt sistemine aktararak kart bilgilerini alıyor. Bu sistem üzerinden müşterilerden elektronik olarak onay da alan dolandırıcılar itiraz haklarını da kısıtlamış oluyor.

TBB'den yapılan açıklamada, şöyle denildi: "Vatandaşların kendilerini banka yetkilisi olarak tanıtan kişilerce arandıkları, ikna edildikten sonra kimlik ve kart bilgileriyle birlikte şifrelerin doğrudan veya tuşlama yoluyla istendiđi, benzer bilgilerin bankalara ait telefon numaralarını taklit eden numaralardan gönderilen SMS, e-posta ve sosyal medya mesajlarıyla da talep edildiđi ve müşterilerin dolandırıldığı tespit edilmiştir. Müşterileri ikna etmek için promosyon verileceđi, para iadesi yapılacağı, hesaplarındaki sorun olduđu, bu sorunların giderileceđi ve bilgilerinin

güncelleneceđi gibi söylemler kullanılmaktadır."

SAHTE İNTERNET SİTELERİ

Dolandırıcıların yaptıđı aramaların ve işlemlerin bankaların sistemleri üzerinden gerçekleştirildiđi izlenimi verildiđine dikkat çekilen açıklamada, müşterilerin, bankalara ait olmayan sahte internet sitelerine veya bilgi işlem sistemlerine yönlendirildiđi vurgulandı.

Açıklamada şu uyarılar yapıldı:

● Müşteriler kişisel bilgilerini, parolalarını, banka tarafından telefonlarına gönderilen şifreleri; telefonda sözlü olarak, tuşlayarak ya da farklı bir yolla asla paylaşmamalı, yönlendirildikleri internet sitelerinin bankalarına ait olduđunu kontrol etmelidir.

● Şüphe oluşması durumunda görüşme sonlandırılarak hızla bankaya bilgi verilmeli.

● Kişisel bilgiler, parolalar ve cep telefonuna gönderilen şifrelerin paylaşılmaması, olası bir dolandırıcılık olayına maruz kalınmaması bakımından büyük önem taşımaktadır.



Nurayet Şahsuvar'ın eşi Necmi Şahsuvar ise "Bu olaydan önce beni de 'Bankadan arıyorlar' diye dolandırıyorlardı. İnanmadığım için telefonu kapattılar. Ancak arayan kişiler benim tüm bilgilerimi biliyorlardı. Bu kadar bilgiyi nereden alıyorlar, araştırılması gerekiyor" dedi.

Böyle dolandırıcılık GÖRÜLMEDİ

UYARILARA rağmen kendilerini 'polis veya savcı' gibi tanıtan telefon dolandırıcıları vatandaşları mağdur etmeye devam ediyor. Dolandırıcıların son kurbanı ev kadını Nurayet Şahsuvar (52) oldu. Dolandırıcılar Şahsuvar'ı arayıp, telefonu hiç kapattırmadan 120 bin liraya aldığı otomobilini 95 bin liraya sattı ve parayı aldı.

Büyükçekmece'de yaşayan bir çocuk annesi Nurayet Şahsuvar'ı ev telefonundan arayan dolandırıcılar, "FETÖ mensupları şu anda sahte

kimlik ile aracınızı noterde satıyor" dedi. Kendisini "Başkomiser Hakan Bulut" olarak tanıtan dolandırıcı, Şahsuvar'a operasyon için üç ay önce 120 bin TL'ye aldığı sıfır kilometre otomobilini bir galeriye giderek satmasını söyledi. Dolandırıcıların söylediklerini yerine getiren Şahsuvar, otomobilini 95 bin liraya galeriye sattı. Şahsuvar içerisinde 95 bin lira bulunan para dolu poşetle noterden ayrıldı.

Şahsuvar, sürekli telefonda konuştuğu dolandırıcının yönlendirmesiyle

le para dolu poşeti bir ara sokakta bırakarak uzaklaştı. Arkadan gelen dolandırıcı parayı alarak kaçtı. Evine gelen Şahsuvar başından geçenleri eşine anlatmasıyla dolandırıcının anlattığı Şahsuvar'ın şikâyetinde bulunması üzerine polis ekipleri, güvenlik kameralarından parayı alan dolandırıcının eşkalini belirledi. Dolandırıcıları arama çalışmaları devam ederken Şahsuvar'ın galerici hakkında savcılığa yaptığı şikâyet üzerine de otomobile "satılmaz" şerhi koyuldu.

■ Firat ALKAÇ/İSTANBUL

FETÖ bahanesiyle VURGUN

KESTEL'de bir kişi, "Senin adın FETÖ örgütüne karışmış" diyen dolandırıcı tarafından 29 bin lira dolandırıldı.



Edinilen bilgiye göre, telefonla M.A. isimli şahsı arayan dolandırıcı, "Senin adın FETÖ terör örgütüne karışmış. Senin üzerinden para çekiyor. Seni bu işten kurtaracağız" diyerek 29 bin 100 lira dolandırdı. Bir süre sonra şahısların dolandırıcı olduğunu fark eden M.A. soluğu poliste aldı. Savcılığın talimatı üzerine polis ekipleri de geniş çaplı araştırma başlattılar. ■ İHA

Müdür dolandırıcılara karşı vatandaşları uyardı

SON gün-
lerde
Bandırma'da
telefon do-
landırıcılığı-
na yönelik
olayların
artış göster-
diğine işaret
eden **Ali**
Haydar Kılıç,
“ Telefon

dolandırıcı-
lığı son günlerde hareketlilik
kazandı. Biz **emniyet** olarak
banka, **PTT** ve **kuyumcuları**
sık sık konuyla ilgili uyarıyo-
ruz. Özellikle yaşlı insanların
yaptığı **alışverişlerde** duyarlı
olmalarını ve şüphelendikleri
bir durumla karşılaştıkları
takdirde bize ulaşmaları
gerektiğini belirtiyoruz.
Banka duvarlarında devriye
hizmetlerini artırdık. **Polis**,
asker, **jandarma**, savcılık gibi
kurumlar telefonla kimseden
para, kontur talep etmez.
Vatandaşlarımızın bunu
akıldan çıkartmaması gereki-
yor ve karşılaştıkları şüpheli

Bandırma İlçe
Emniyet Müdürü
Ali Haydar Kılıç,
telefon dolandı-
rıcılığı konusunda
halkı uyararak,
emniyetin yaptığı
çalışmalar hakkın-
da bilgi verdi.



durumlarda muhakkak bize
başvursunlar.” dedi.

Son olarak 72 yaşında bir
vatandaşın telefon yoluyla
dolandırıldığını ve mağdur
edildiğini aktaran Kılıç, bu
konuda çalışmaların sürdü-
ğünü belirtti. **Emniyet** Müdü-
rü Kılıç “Vatandaşımızın ban-
ka görevlisi uyardığı halde
parayı çekerek, dolandırıcıla-
ra teslim ettiğini öğrendik. Bu
konuyla ilgili çalışmalarımız
devam etse de, önemli olan
halkın bu konuya duyarlı
davranması” diye konuştu.

Dolandırıcılar bu kez yanlış teyzeye çattı

ADANA'da kendilerini polis olarak tanıtırak telefonda dolandırıcılık yaptığı iddiasıyla gözaltına alınan çetenin elemanlarının, Balıkesir'deki bir kadını dolandırmak isterken baltayı taşa vurdukları ortaya çıktı. Adana Emniyet Müdürlüğü Asayiş Şubesi Yankesicilik ve Dolandırıcılık Büro Amirliği ekipleri, 25 Temmuz'da Adana, İstanbul, Ankara, İzmir, Adıyaman, Elazığ, Kırklareli, Sivas ve Şanlıurfa'da operasyon yapmış, 40 kişi gözaltına alınmış 35 kişi tutuklanmıştı. Operasyon detaylarında çetenin kandıramadığı vatandaşların da olduğu ortaya çıktı.

'KOBRA TEYZE' KÂBUS OLMUŞ

Balıkesir'de bir kadın, kendisini arayan dolandırıcıyı, inanmış gibi yapıp evine para almaya çağırmış ve yakalatmış. Çetenin diğer elemanları kadını arayınca aralarında geçen ilginç diyalog polis dinlemesine takılmış: **» Dolandırıcı: Durdu Hanım, iyi günler efendim. » Kadın: Size de iyi günler. » D: Nasılsınız? » K: Çok mu lazım size. » D: Çok lazımsınız, şikayetinizi geri çekin. » K: Sebep? » D: Sebep, kobra gibi niye... » K: Sen dolandırıcısın, ben de vatandaşlık görevimi yaptım. » D: Kobra gibi, bir adamımızı uyuttun dağ gibi adam. K: Ben vatandaşlık görevimi yaptım. » D: Sana bir soru soracağım. Sen kobra mısın, değil misin? » K: Hayır. » D: E peki bu bütün dolandırıcılar neden senin adını kobra koymuş? » K: O yani, bükemediğiniz eli öpmeniz gerekiyor.**

Dolandırıcılar Valilik Özel Kalem adını da kullandı

Başkentte bazı dolandırıcıların **Ankara Valiliği** Özel Kalem Müdürü adını kullanarak bazı taleplerde buldukları belirtildi.

Ankara Valiliği'nden yapılan açıklamada şöyle denildi:

“Bazı **şirket** ve şahısların telefonla aranmak suretiyle, kendisini **Ankara Valiliği** Özel Kalem Müdürü olarak tanıtan dolandırıcılar tarafından hayır işleri konusunda yardım istendiği, hesap numaraları verilerek sahte hesaplara para yatırılmasının talep edildiği anlaşılmaktadır.

Vatandaşlarımızın bu tür taleplere itibar etmemeleri, verilen hesap numaralarına hiçbir şekilde para aktarmamaları, kendilerini arayan kişilerin telefon numaralarının,

112 Acil hattına veya **Ankara Valiliği**'nin 0 (312) 306 66 66 numaralı telefonuna bildirilmesinin, dolandırıcıların yakalanması ve muhtemel mağduriyetlerin önlenmesi açısından önemli olduğu hususu, kamuoyuna saygıyla duyurulur.”



Tele-dolandırıcı çetesi çökertildi

Aydın'da yapılan operasyonda, ülke genelinde telefonla dolandırıcılığı yaptığı gerekçesiyle gözaltına alınan zanlılardan 16'sı tutuklandı.



■ AYDIN İl Emniyet Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Şubesi ekipleri, ülke genelinde telefon dolandırıcılığı yaptıkları tespit edilen Aydın merkezli suç çetesini çökertti. Şüphelilerin telefonla aradıkları vatandaşları daha önceden yaptıkları hayat sigortasını yenileme bahanesiyle kandırıp hesaplarına para aktarma konusunda ikna ettikleri belirlendi. Teknik takibe alınan şüphelilere yönelik operasyon kapsamında 31 kişi hakkında gözaltı kararı çıkarıldı. ■ Burhan CEYHAN, (DHA)

6 MERKEZDE EŞ ZAMANLI

■ İzmir, Ankara, İstanbul, Kırklareli, Afyonkarahisar ve Aydın'da yapılan eş zamanlı operasyonda, 24 kişi gözaltına alındı. Şüphelilerin adreslerinde yapılan aramalarda ise bulunan dijital verilere el konuldu. Gözaltına alınan 24 kişiden 8'i, emniyetteki işlemlerinin ardından serbest bırakıldı. Dün adliyeye sevk edilen 16 kişi tutuklandı. Operasyon kapsamında 7 kişinin yakalanması için çalışmaların sürdüğü bildirildi.

24.5 MİLYON LİRA

■ Öte yandan; çete üyesi oldukları belirtilen 22 kişinin hesaplarına yatan paranın toplam miktarının 24 milyon 557 bin 608 lira olduğu açıklandı. Çete üyelerinin, PTT'den günlük çektikleri paraları başka hesaplara aktararak kendilerini gizlemeye çalıştıkları bildirildi.

Dolandırıcıların yeni oyunu: **MASAK**

MALİYE Bakanlığı'ndan telefon dolandırıcıları ile ilgili uyarı geldi. Bakanlık, bazı şahısların vatandaşları telefonla arayarak, adlarının **Mali Suçları** Araştırma Kurulu'nun(**MASAK**) incelemesinde geçtiğinden bahisle, **MA-**



SAK'taki işlerini halledebilecekleri yönünde vaatlerde bulunmak suretiyle para veya sair menfaatler talep ettiklerini belirterek, bu tür girişimlere vatandaşların hiçbir şekilde itibar etmemeleri gerektiğini bildirdi. **Maliye Bakanlığı**'ndan **MASAK** ile ilgili yapılan açıklamada, dolandırıcılık amacıyla yapıldığı anlaşılan bu tür girişimlere vatandaşların hiçbir şekilde itibar etmemeleri gerektiği

vurgulandı. Açıklamada, şunlar kaydedildi: "Diğer taraftan bu şekilde talepte bulunulduğu durumlarda bakanlığımıza bilgi verilmesi halinde yetkili makamlar nezdinde gerekli işlemler tarafımızca yapılacaktır. Ayrıca, vatandaşlarımız bu tür durumlar ile karşılaşmaları halinde yetkili **emniyet** makamlarına veya cumhuriyet savcılıklarına suç duyurusunda bulunabilirler."

KREDİ YALANINA POLİS BİLE İNANDI

KOSGEB'in faizsiz kredi uygulamalarını rant kapısına dönüştüren dolandırıcılar, "Krediniz onayladı" yalanıyla Antalya'da vurgun yaptı. KOSGEB yetkilileri, kredi başvurusu yapmayan vatandaşların bile dolandırılmaya çalışıldığını söyledi.

Salım UZUN/HÜRRIYET

KÜÇÜK Orta Ölçekli İşletmeleri Geliştirme ve Destekleme İdaresi Başkanlığı'nın (KOSGEB) 50 bin liralık sıfır faizli destek kredisi dolandırıcıların iştahını kabarttı. Antalya'da kredi başvurusu yapan kişilerin mesaj ve sesli çağrı ile ulaşan hayal tacirleri, "Krediniz onayladı. Paranın hesaba geçmesi için 500 liralık dosya masrafı ödememiz gerekiyor" diyerek vurgun yaptı.

'SEVİNDİM KABUL ETTİM'

Daha önce de aynı yöntemle binlerce kişiyi dolandıran kişilerin yöntemlerini Hürriyet muhabirine anlatan emekli polis memuru İ.U., "KOSGEB başvuru sonuçları açıklanmadan hemen önce cep telefonumdan arandım. Karşımdaki kişi KOSGEB yetkilisi olduğunu söyleyerek, "Hesabına 50 bin lira

faizsiz, 2 yıl geri ödemesiz para yatıracağız" dedi. Tabi ki sevindim ve teklifi kabul ettim" dedi.

'KAMU KURUMLARINA AKTARILACAK'

Telefondaki kişinin 50 bin liralık kredinin blokesini açtırmak için 500 lira talep ettiğini vurgulayan İ.U., "Bu parayı neden istediklerini sordum. Bana yasal bir talepte bulduklarını, alınan paranın kamu kurumlarına aktarılacağını söylediler. Son derece kurumsal bir görüşme olduğu için şüphelenmedim ve parayı yatırdım" diye konuştu.

'BEKLEDİM PARA YATMADI'

500 lirayı yatırmasına rağmen 50 bin liralık krediyi alamayınca dolandırıldığını anladığını belirten emekli polis memuru, şöyle dedi: "Yaklaşık 1 hafta bekledim. Sürekli hesabımı kontrol ettim.



Para yatmayınca yetkili kuruma başvurudum. Bana böyle bir uygulamalarının olmadığını söylediler. O an ne yapacağımı şaşırđım. Büyük bir hayal kırıklığı yaşadım."

VALİLİK VE KOSGEB UYARDI

Vatandaşları telefon ya da internet yoluyla kendilerine ulaşan ve KOSGEB'in ismini kullanarak para talebinde bulunan kişilere

itibar etmemesi konusunda uyar an Antalya Valiliđi, KOSGEB Antalya Hizmet Merkezi Müdürlüğü yetkilileri, "Kredi başvuru yapmayan vatandaşlarımıza bile ulaşp dolandırmayı denemişler. Bu kişilerle ilgili bilinçli olunmalı. En ufak bir şüphede 444 1 567 numaralı hattı arayarak bilgi alınabilir. KOSGEB personeli hiçbir şekilde telefonda para talep etmez" dedi.



Dolandırıcılık amaçlı suç duyurusunda bulunun

İzinsiz atılan bu tip SMS ve e-maillerin yüzde 70'i dolandırıcı amaçlı. Vatandaşlarımız, uygun fiyatlı ürün, çekiliş, ücretsiz check-up, kaplica gibi vaatlerle dolandırılıyor. Kesinlikle bu telefon ve mesajlara kanmayın. Bu şekilde dolandırılmıyorsanız, bu suçtur. Konunun takibi açısından cumhuriyet başsavcılığına suç duyurusunda bulunun.

İSTE BHD'NİN TÜKETİCİLER İÇİN HAZIRLADIĞI YOL HARİTASI

1 Mayıs 2015'ten itibaren onay alınmaksızın gönderilen e-posta ve kısa mesaj ile yapılan otomatik aramalara ilişkin şikâyetler şöyle yapılabilir:

1-Şikâyet başvurusu, alıcının ikametgâhının bulunduğu yerdeki Cumhuriyet ve Ticaret Bakanlığı İl Müdürlüğü'ne yapılır. Şikâyet edilen hizmet sağlayıcının sicile kayıtlı merkezinin başta bir ilde bulunması halinde, bu başvuru ilgili İl Müdürlüğüne gönderilir.

2-Şikâyet başvurusu, yazılı olarak isak imzaya veya elektronik ortamda e-Devlet kapısı üzerinden güvenli elektronik imza ya da mobil imza yoluyla İl Müdürlüğü'ne yapılabilir.

3-Şikâyetçi; gerçek kişi ise adı ve soyadı ile imzası ve ikametgâh adresini; tüzel kişi ise unvanı ve temsil yetkili kişinin veya vekilinin adı ve soyadı, iş adresi ve imzasının başında yer alması gerekir.

4-Kısa mesaj yoluyla yapılan ticari iletişimde; şikâyetçinin telefon numarası, şikâyetçinin aboneliği GSM operatörünün adı, şikâyetçi konu ile ilgili gönderilen numarası, bu numaradan alınmaması halinde marka ve işletme adı gibi alfanümerik bilgisi, iletinin gönderilme tarihi, saati ve içeriği ile esnaf veya tacir olmaları halinde bu bilgisine yer verilir. İletinin yazılı veya görsel bir örneği başvuruya eldenir.

5-Elektronik posta yoluyla yapılan ticari iletişimde; şikâyetçinin elektronik posta adresi, şikâyetçiye elektronik posta hizmeti sağlayan işletmenin adı, şikâyetçi konu ile ilgili gönderilen elektronik posta adresi, iletinin gönderilme tarihi, saati ve içeriği ile esnaf veya tacir olmaları halinde bu bilgisine yer verilir. İletinin yazılı veya görsel bir örneği başvuruya eldenir.

6-Sesli arama yoluyla yapılan ticari iletişimde; şikâyetçinin telefon numarası, şikâyetçinin aboneliği GSM veya sabit hat operatörü adı, şikâyetçi konu ile ilgili gönderilen numarası, bu numaradan alınmaması halinde marka ve işletme adı gibi bilgisi, iletinin gönderilme tarihi, saati ve içeriği ile esnaf veya tacir olmaları halinde bu bilgisine yer verilir.

7-Diğer elektronik iletişim araçları ile yapılan ticari iletişimde, iletişim aracının türüne bağlı olarak gerekli bilgilere yer verilir.

8-Şikâyet başvurusu, ticari elektronik iletinin gönderildiği tarihten itibaren en geç 6 ay içinde yapılır. Şikâyetçi ancak kendisine ait elektronik iletişim adreslerine gönderilen iletlere ilişkin şikâyetçi olabilir. Bu maddede yer alan şartları taşımayan başvuru İl Müdürlüğünce işleme konulmaz.

9-İl Müdürlüğü tarafından, halkında şikâyet bulunan hizmet sağlayıcı tespit edilir. Konuya ilişkin bilgi ve belgeler ilgilisinden temin edilerek şikâyet sonuçlandırılır. Ancak, gerekli hallerde İl Müdürlüğünce denetim için görevlendirilen personel tarafından yerinde denetim yapılabilir.

10-Hizmet sağlayıcı, İl Müdürlüğü tarafından söz konusu şikâyetle ilgili olarak talep edilen bilgi ve belgeleri, bu talebin tebliğinden itibaren 15 gün içinde teslim etmekle yükümlüdür. Gerekli hallerde bu süre bir defaya mahsus olmak üzere 15 gün uzatılabilir. Aksi takdirde, hizmet sağlayıcıya Kanunda öngörülen idari para cezası uygulanır.

11-İl Müdürlüğü, hizmet sağlayıcının doğrudan tespit edilmesine imkân bulunmadığı hallerde, ilgili kamu kurum ve kuruluşları ile elektronik haberleşme hizmeti sunan işletmelerden bilgi ve belge talep edebilir.

Dolandırıcılara da cep servislerine de dikkat

CEP telefonu üzerinden verilen servislerle, izinsiz atılan SMS ve e-maillere dikkat edilince şikâyet alınır. Üstelik izinsiz SMS ve e-mail göndermek 1 Mayıs 2015'ten itibaren kanunla yasaklandı. Mail atan okurların gibi, anasının, karını kurumunda çalışan bir arkadaşının ve bizzat benini de başına çekti.

Özellikle dokunmatik telefonlara SMS yoluyla gönderilen "hediyeli soru servisi", İngilizce kelime soru servisi, spor servisi" vs gibi kampanya mesajlarına şikâyet edenler yanlışlıkla onaylayabilmektedir. Ya da "RET" veya "İPTAL" mesajı atmaya unuttukları olabilmektedir...

FATURA DETAYLARINA DİKKAT

Sorun ne mi oluyor? Farkına bile varmadan bu servislerin ücretlerini her ay düzenli ödüyorsunuz. Hele cep telefonu faturalarınız otomatik ödeme ve e-fatura durumuna da incelemediğiniz. Aydır sonra farkına varınca bu kez iptal çilesi yapmışsınız. İstemediğiniz bir servisi "İptal" için günlerce uğraşmak zorunda kalıyorsunuz. Serinkanlı ve son derece kibar müşteri temsilcilerinden şu yanıt



alıyor musunuz?

"Şu tarihte siz SMS/e-mail kampanyanızla abone olmuştunuz. Geçmişe dönük ücret izdesi de maalesef yapılmıştır."

Meğer ben de geçen yıl Haziran'da bir İngilizce soru servisine abone olmuştum. İşim için yahu önce döndürüp sonra bittim kapattığım cep telefonuma bu sorular gönderilmiş. Yarışmalara katılmışım.

Bu servis için her ay 15 TL ödediğimi müşteri temsilcisinden öğrendim. Benim

adına kayıtlı aynı operatörün cep telefonu hattını kullanarak aramın de başına aynı şey geldi. O da SMS'le "hediyeli soru" servisine abone olmuş. 25 TL olması gereken faturasını hediyeli soru servisi nedeniyle 66 TL olarak ödenmiş aylarca.

SUSMAK ONAY ANLAMINA GELMEZ

Bilgin Huloğlu Derneği (BHD) Başkanı Avukat Kürşat Ergün'le konuşum. Kanunen yasaklanmasına rağmen izinsiz SMS/e-mail gönderimini bu tip servislere farkına bile varmadan onay veren ya da "RET" mesajı atmadıkları için abone yapılan vatandaşlarımızın izlenmesi gereken haksız yollar sorulan. İşte Ergün'ün

yanıtı: "1 Mayıs 2015'ten itibaren reklam amacıyla izinsiz SMS ya da e-mail yarda her türlü faks, akülü ses kaydedici sis-

HAKEM HEYETİNE BASVURUN

■ İzinsiz atılan SMS, yapılan servis aboneliği işlemleri nedeniyle bir zarara uğradıysanız ilgili Tüketici Hakem Heyetlerine müracaat edebilirsiniz. O servisten şikâyetçi olabilirsiniz.

temler ve telefon gibi iletişim araçlarının reklam amaçlı olarak izinsiz kullanılması kanunla yasaklandı. Çevresiz çağrı olmasa ya da "RET" mesajı göndermemek onay anlamına gelmez. Ayrıca tüketici istediği her an onayına son verme hakkı ve yetkisine sahiptir. Tüketicilerin gerçekleştirdiği alışverişler esnasında kendisi ile iletişime geçilmesi amacıyla firmaya iletişim bilgilerinin verilmesi halinde bu durum onay kabul edilebilir. Bu tip bilgileri gerekli görmediğiniz firmalara vermeyin.

SMS VE MALLERİ ŞİKÂyet EDEBİLİR SİNİZ

Günümüzde ve Ticaret Bakanlığı, kendi internet sitesine izinsiz reklam SMS'lerini ve maileri şikâyet etme hakkını oluşturdu. Bu mesajları şikâyet edebilirsiniz. (Şikâyet sisteminin adresi: tss.gtb.gov.tr). Bu adrese ya da bakanlığın resmi internet sitesine girdiğinizde e-devlet şifrenizle işlem yapabilirsiniz.

Cepten dolandıranlara cep servislerine dikkat

CEP telefonu üzerinden verilen servislerle, izinsiz atılan SMS ve e-mailelere dönük onlarca şikayet alıyorum. Üstelik izinsiz SMS ve e-mail göndermek 1 Mayıs 2015'ten itibaren kanunla yasaklandığı halde.

Mail atan okurlarım gibi, annemin, kamu kurumunda çalışan bir arkadaşımın ve bizzat benim de başıma geldi. Özellikle dokunmatik telefonlara SMS yoluyla gönderilen "hediyeli soru servisi, İngilizce kelime soru servisi, spor servisi" vs gibi kampanya mesajlarını siliyorum derken yanlışlıkla onaylayabilirsiniz. Ya da "RET" veya "İPTAL" mesajı atmaya unutmuş olabilirsiniz...

FATURA DETAYLARINA DİKKAT

Sonra ne mi oluyor? Farkına bile varmadan bu servislerin ücretlerini her ay düzenli ödüyorsunuz. Hele cep telefonu faturalarınız otomatik ödemede ve e-faturalarınızı da incelemiyorsanız. Aylar sonra farkına varınca bu kez iptal çilesi yaşıyorsunuz. İstemediğiniz bir

"İptal" için günlerce uğraşmak zorunda kalıyorsunuz. Serinkanlı ve son derece kibar müşteri temsilcilerinden şu yanıtı alıyorsunuz?

"Şu tarihte siz SMS/e-mail kampanyamızla abone olmuşsunuz. Geçmişe dönük ücret iadesi de maalesef yapmıyoruz"

Meğer ben de geçen yıl Haziran'da bir İngilizce soru servisine abone olmuşum. İşin ilginç yanı önce dondurup sonra hattını kapattığım cep telefonuma bu sorular gönderilmiş. Yarışmalara katılmışım. Bu servis için her ay 15 TL ödediğimi müşteri temsilcisinden öğrendim. Benim adıma kayıtlı aynı operatörün cep telefonu hattını kullanan annemin de başına aynı şey geldi. O da SMS'le "hediyeli soru" servisine abone olmuş. 25 TL olması gereken faturasını hediyeli soru servisi nedeniyle

Cep telefonu dolandırcılarına da servislerine de fatura detaylarına da gelen SMS ve e-maillere de dikkat. En basitinden cep telefonu servisi, daha kötüsü dolandırcıların kurbanı olup binlerce lira zarara uğrayabilirsiniz.



66 TL olarak ödemişiz aylarca.

SUSMAK ONAY ANLAMINA GELMEZ

Bilişim Hukuk Derneği (BHD) Başkanı Avukat Kürşat Ergün'le konunun uzmanı olarak konuştum. Kanunen yasaklanmasına rağmen izinsiz SMS/e-mail gönderimi ile bu tip servislerle farkına bile varmadan onay veren ya da "RET" mesajı atmadıkları için abone yapılan vatandaşların izlemesi gereken

hukuki yolları sordum. İşte Ergün'ün yanıtları:

"1 Mayıs 2015'ten itibaren reklam amacıyla izinsiz SMS ya da e-mail yanında her türlü faks, akıllı ses kaydedici sistemler ve telefon gibi iletişim araçlarının reklam amaçlı olarak izinsiz kullanılması kanunla yasaklandı. Cevapsız çağrı olması ya da "RET" mesajı göndermemek onay anlamına gelmez. Ayrıca tüketici istediği her an onayına son verme hak ve yetkisine sahiptir. Tüketicilerin gerçekleştirdiği alışverişler esnasında kendisi ile iletişime geçilmesi amacıyla firmaya iletişim bilgilerinin verilmesi halinde bu durum onay kabul edilebiliyor. Bu tip bilgileri gerekli görmediğiniz firmalara vermeyin.

İZİNSİZ SMS VE MAİLLERİ ŞİKAYET EDEBİLİRSİNİZ

Gümrük ve Ticaret Bakanlığı, kendi internet sitesine izinsiz reklam SMS'lerini ve mailleri şikayet etme bölümü oluşturdu. Bu mesajları şikayet edebilirsiniz. (Şikayet sisteminin adresi tiss.gtb.gov.tr Bu adrese ya da bakanlığın resmi internet sitesine girdiğinizde e-devlet şifrenizle işlem yapabiliyorsunuz)

İzinsiz reklam SMS/e-mail'i gönderme 1 Mayıs 2015'ten itibaren yasaklandı. Buna rağmen SMS/e-mail yağmuru devam ediyor. İzinsiz SMS'leri üşenmeyin e-devlet üzerinden şikayet edin.

HAKEM HEYETİNE BAŞVURUN

İzinsiz atılan SMS, yapılan servis aboneliği işlemleri nedeniyle bir zarara uğradıysanız ilgili Tüketici Hakem Heyetlerine müracaat edebilirsiniz. O servisten şikayetçi olabilirsiniz.

DOLANDIRICILIK AMAÇLI SUÇ DUYURUSUNDA BULUNUN

İzinsiz atılan bu tip SMS ve e-maillerin yüzde 70'i dolandırma amaçlı. Vatandaşlarımız, uygun fiyatlı ürün, çekiliş, ücretsiz check-up, kaplıca gibi vaatlerle dolandırılıyor. Kesinlikle bu telefon ve mesajlara kanmayın. Bu şekilde dolandırıldıysanız, bu suçtur. Konunun takibi açısından cumhuriyet başsavcılığına suç duyurusunda bulunun.

Kızının altınlarını kendi elleriyle dolandırıcıya verdi

Fatih KARACALI/DHA

ADANA'da 74 yaşındaki Hatice Altıncok, kendisini telefonla arayıp polis olarak tanıtan dolandırıcıya, kızının emanet bıraktığı 15 bin lira değerindeki para ve altınları elleriyle verdi.

Merkez Seyhan ilçesi

Akkapı Mahallesi'nde oturan Hatice Altıncok'u, dün öğle saatlerinde telefonla arayan bir kişi kendisini polis olarak tanıttı. Altıncok'a, "Kuyumcu soyulmuş, senin kimliğini kullanan kadın hem adına telefon çıkartmış, hem de o nüfus cüzdanını kuyumcuda bırakmış. Savcım ile birlikte evine gelip arama yapacağız. Biz gelmeden önce, sana bir polis göndereceğiz, sen evde ne kadar altın varsa onları teslim et. Gelip baktığımızda bulursak seni hapse atarız" diye tehdit etti. "Evde kızımın emanet bıraktığı altınlar var. Onları veremem" diyen Hatice Altıncok'u ikna etmeye çalışan dolandırıcı, "Teyze biz seni



düşünüyoruz. Savcı gelip evde arama yapar, altın bulursa seni de kızını da hapse atar. Hem o altınları kuyumcudan çalınanlarla karşılaştıracamız, aynı değilse geri alacaksın" dedi.

**VEREMEM DEDİ
DİNLETEMEDİ**

Dolandırıcının sözlerine inanan Hatice Altıncok kızına ait 3 bileklik, 5 çift küpe, 12 çeyrek altın ile bin 800 lirayı poşete doldurdu. Hatice Altıncok telefonla konuşurken, dolandırıcı evin kapısına geldi. Hatice Altıncok, kapıya gelen dolandırıcıya kızına ait toplam 15 bin lira değerindeki altın ve parayı teslim etti. Bir süre sonra dolandırıldığını anlayan Hatice Altıncok, durumu polise bildirdi. Eve gelen polis ekiplerine başından geçenleri anlatan Hatice Altıncok, "Götürdükleri altınlar benim değil. Kızımın emaneti olduğunu, veremeyeceğimi söyledim. Ama dinletemedim" dedi.



Kara liste vurgunu!

DOLANDIRICILAR, vatandaşın cebindeki paraya göz dikerek şimdi de 'kara liste' oyunu ile vurgun yapmanın peşine düştü. Antalya'da yüzlerce kişiyi telefonla arayan şebeke, "Özel sigorta borcunuz var. Ödemezseniz 5 yıl boyunca kredi çekemeyecek, kredi kartı kullanamayacaksınız" yalanıyla tüketicileri dolandırıyor. Dolandırıcıların tuzağına isimlerden biri olan S.T. (37), dolandırıcılık yönteminin tüm ayrıntılarını Hürriyet muhabirine anlattı. Sabah saatlerinde 800'lü bir numaradan arandığını kaydeden S.T. "Telefondaki ses bana isimle hitap etti ve adıma yapılan özel sigorta nedeniyle 1800 lira borcum olduğunu söyledi" dedi.



Abdullah
Özçulcu

'ADRESLERİMİ SÖYLEDİ'

Borç bilgisi karşısında neye uğradığını şaşırıldığını anlatan S.T., "Asgari ücretle çalıştığımı söyleyip 'Ne sigortası, ne borcu?' dedim. Onlarda bana borcun sistemde kayıtlı olduğunu ödenmemesi halinde bankalar tarafından kara listeye alınacağımı söyledi. Hatta iki ayrı adresimi söyleyip 'İcra takibi de

başlatabiliriz' dedi. Karşımdaki kişi adreslerimi ve kimlik bilgilerimi doğru söyleyince ikna oldum" diye konuştu. Yakın zamanda ev almayı düşündüğünü bu nedenle de kara listeye alınmaktan korktuğu için parayı ödemeyi kabul ettiğini dile getiren S.T., şöyle devam etti: "Parayı PTT yoluyla söylenen hesaba yolladım. Fakat daha sonra yaptığım araştırmada dolandırıldığımı anladım."

'BİLİNÇLİ OLUNMALI'

Kara liste oyunu ile birçok tüketicinin mağdur edildiğini doğrulayan Tüketiciyi Koruma Derneği (TÜKODER) Antalya Şube Başkanı Abdullah Özçulcu, "Tüketici banka işlemlerinin engellenmesinden korkarak maalesef dolandırıcıların tuzağına düşüyor. Bunu önleyebilecek tek sistem vatandaşın bilinçlenmesi. Hiçbir kurum, kuruluş telefonda para istemez, kişisel bilgi sormaz. Tüketici kendisini arayan numaranın niteliğine göre de davranabiliyor. Unutulmamalı ki bu telefon numaraları satın alınabilir. Eğer dolandırıcılara karşı hazır olmak istiyorsak bilinçli ve duyarlı olmalıyız" diye konuştu.

■ Salim UZUN/HÜRRİYET

SAHTE POLİSLER TUTUKLANDI

Yaşlı çifti FETÖ yalancıyla kandıran dolandırıcılar, 87 bin liranın hayaliyle aceleyle İstanbul'dan Bursa'ya gelip, camdan uzatılan paraları tam teslim alırken polis tarafından yakalandı. Kendini polis ve savcı olarak tanıyan telefon dolandırıcısı, Osmangazi'de yaşayan E.T. (60) ve N.T. (57) çiftini arayarak, hesaplarından FETÖ terör örgütüne para aktarıldığını söyledi. Uzun süre telefonu kapatmayarak ne yapmalarını gerektiğini belirten İ.K. (35), yaşlı çiftten hesaplarındaki bütün parayı ge-



lecek kişilere teslim etmelerini istedi. Uzun süre telefonda olan anne ve babasından şüphelenen çocukları, arayanların dolandırıcı olduğunu anlayanca polise

ihbarda bulundu.

Polis ekiplerinin oyunu devam ettirmelerini istemesi üzerine, paraların tamam olduğunu belirten karı koca, İstanbul'dan yola çıkan M.E. (33) ve A.A.'yı (34) beklemeye başladı. Emniyet Müdürlüğü Yankesicilik ve Dolandırıcılık Büro Amirliği ekipleri de evin etrafında önlem aldı. Dolandırıcılar, yaşlı çiftin camdan uzattığı paraları tam alırken suçüstü yakalandı. Suçüstü yakalanan 2 kişi, emniyetteki sorgularının ardından sevk edildiği mahkemece tutuklandı. ■ İHA

Emekli büyükelçi de **DOLANDIRICI KURBANI**

Emekli büyükelçi ve eşi aynı anda arayan telefon dolandırıcıları, çiftin bankadaki 103 bin lirasını aldı. Bununla yetinmeyip, çiftin evlerini de satmalarını isteyince gerçek ortaya çıktı.

Eyüp SERBEST/İSTANBUL

BAKIRKÖY'de yaşayan emekli büyükelçi A.A.'yı (73) 22 Aralık'ta arayan bir kişi, Bakırköy İlçe Emniyet Müdürlüğü'nde görevli başkomiser olduğunu söyledi. Telefonda kişinin iddiasına göre, terör örgütü PKK emekli büyükelçi ve tüm ailesinin hesaplarını ele geçirmiş ve para trafiğini yönlendirmişti. Sözde başkomiser telefonu, sözde Bakırköy Adliyesi'nde görevli bir savcıya verdi. Büyükelçi A.A. kendisine söylenen savcının ismini internetten kontrol etti, verilen isim doğruydü. Bu sırada A.A.'nın eşi N.B.A.'nın da telefonu çaldı. Kendisini Bakırköy Cumhuriyet Başsavcısı olarak tanıtan bir kişi A.A. ve N.B.A.'dan ayrı odalarda bulunmalarını istedi. Sözde başsavcı N.B.A.'dan bankadaki hesabını boşaltmasını istedi.

SÖZDE POLİS BANKA ÖNÜNDE BEKLEDİ

N.B.A. eşi içeride halen telefonla konuşurken banka şubesine gitti ve çektiği 103 bin TL'yi banka önünde bekleyen 'polise' teslim etti. Bu sırada sözde başkomiser de A.A.'dan 100 bin TL kredi çekmesini istedi. A.A. bankaya gittiğinde, eşinin birkaç dakika önce tüm parayı çektiğini söyleyen banka görevlileri kredi veremeyeceklerini söyledi. Bu kez de A.A.'dan evini satmasını ve parayı kendilerine vermesini istediler. A.A. bunun üzerine dolandırıldıklarını anladı ve Bakırköy Cumhuriyet Başsavcılığı'na başvurarak şikâyetçi oldu.

Polis ekipleri, parayı teslim alan ve telefonda konuşanların tespiti için çalışma başlattı.

SAHTE POLİSE SUCÜSTÜ



KOCAELİ'nde yaşayan Alper Kivisoğlu'nu arayan telefon dolandırıcıları kendilerini polis olarak tanıtarak, "Annen ve babana ait kimlikler FETÖ'nün elinde. Bu kimlikler kullanılarak bir kuyumcu soygunu yapıldı ve çalınan altınların yarısı elimizde. Evde ne kadar altın ve para varsa bir torbaya koyup gelecek polis arkadaşlara ver" dedi. Aile durumu polise bildirdi. Önlem alan ekipler, altınları almak için gelen iki kişiyi kısıvrak yakaladı. ■ **Nabi YAZICI / DHA**

EK 4 Telefon Dolandırıcılığına Maruz Kalan 30 Vaka

Telefon Dolandırıcılığına Maruz Kalan 15 Erkek Vakası

1.VAKA

Şu an 31 yaşımıdayım, olay 7 sene önce 24 yaşımıdayken gerçekleşti.

Bekarım, yüksek lisans mezunuyum, kendi evimde tek başına yaşıyorum ve ücretli çalışıyorum.

Hafta içi, iş yerimdeyken, saat 9:00-11:00 arası arandım. Cep telefonumdan aradılar. Cep

telefonum akıllı telefon. İlk görüşme 10 dakika sürdü. Arayan kişi kendisini Ankara'nın bir

ilçesinin İlçe Emniyet Müdürlüğü'nden Polis Amiri olarak tanıttı. Arka

tarafından telsiz sesi gibi herhangi bir ses gelmiyordu. Hesabımdan terör örgütü hesabına para

aktarıldığını, maddi yardım edildiğini belirttiler. Suç unsurunun ortadan kaldırılması için

yardım edeceğini belirten, kendini polis amiri olarak tanıtan kişi; yardım edebilmesi için

bankaya gitmem gerektiğini, para yatırmam gerektiğini, kendisinin beni yönlendireceğini

belirtmiştir. Polis amirine kimliğim ile ilgili bilgiler sorduğumda sinirlenmiştir. Bankaya

gidemeyeceğimi, işte olduğumu söyleyerek zaman kazanmak istedim. Ama arayan suçlu

durumundan kurtulmam için gitmem gerektiğini vurguladı. "Nedenli, niçinli sorular"

sorduğumda cevap alamadım ve arayan bu duruma sinirlendi. Sonra telefonu kapattım.

Telefonu kapattıktan sonra avukatımı aradım. Beni arayanın belirttiği Ankara'daki İlçe Emniyet

Müdürlüğü'nün telefonunu bulup aradım. Ancak Emniyet Müdürlüğü tarafından böyle bir

aramanın söz konusu olmadığını öğrendim. 155'i aradım. Polis herhangi bir yönlendirme

yapmadı, "telefon numaraları geçici, kanmayın" dedi.

Aynı gün, yarım saat sonra tekrar aynı kişi aradı. Artık dolandırıcı olduklarını bildiğim için

dalga geçerek konuştum. Arayan sinirlendi, küfür edip telefonu kapattı.

Bu olaydan sonra savcılığa suç duyurusunda bulunmadım.

2.VAKA

41 yaşımdayım, olay 15 gün önce gerçekleşti.

Bekarım, yüksek lisans mezunuyum, hane halkı sayısı 3 kişi, kendi evimizde yaşıyoruz, ücretli çalışıyorum.

Pazartesi günü iş yerindeyken saat 10:30'da arandım. Görüşme 17 dakika sürdü. Cep telefomundan arandım. Cep telefonum akıllı telefon.

Yakın zamanda bankalara ödediğim yıllık aidat ücretlerini geri almak üzere başvurmuştum. Yapı ve Kredi Bankası Kredi Kartları Merkezi'ne de ödediğim geçmiş dönem aidatlarının geri ödenmesi için dilekçe vermiştim. Dilekçem Hakem Heyeti'nde idi.

Telefonla arayan kişi Yapı ve Kredi Bankası'ndan aradığını, Hakem Heyeti'ne başvurumun olduğunu belirtti. İnternet bankacılığını kullanıp kullanmadığımı sordu. Kullanmadığımı belirtince, “yeniden” şifre tanımlanması gerektiğini belirtti. Bu tanımlama için de kredi kartımın son 6 rakamı ve güvenlik kodunu istedi. Telefonuma sürekli mesaj geldi ama bu mesajların içeriğine bakmadım. Mesajlar Yapı ve Kredi Bankası'ndan geliyordu. Arayan “hızlı” konuşuyordu.

Mesaj içeriğine bakmadan sadece gelen şifreleri arayanlara söyledim ve adıma 3 yerden işlem yapıldığını telefonu kapattıktan sonra öğrendim. Hemen bankayı aradım ve “işlemler tarafımda yapılmamıştır” dedim. Banka “Savcılığa suç duyurusunda bulunun” dedi.

1.çekim 1.400 Türk Lirası idi ama çekim gerçekleşmemişti, 3.çekim 3.700 Türk Lirası idi bu çekim de gerçekleşmemişti; 2. çekim ise 3.600 Türk Lirası tutarında idi ve medikal malzeme alımı olan bu çekimin gerçekleşmiş olduğunu öğrendim.

Savcılığa suç duyurusunda bulunmadım, bulunmayacağım ve hesabımdan çekilen miktarı ödeyeceğim.

3.VAKA

73 yaşımdayım, olay 3 yıl önce oldu. Olay gerçekleştiğinde 70 yaşımdaydım.

Evliyim, lise mezunuyum, hane halkı sayısı 2 ve kendi evimde yaşıyorum, emekliyim.

Cep telefonundan arandım. Ama telefonum akıllı telefon değil, tuşlu telefonlardan. Arama Pazar günü, akşam üzeri gerçekleşti. 5 dakika sürdü.

İlk aramayı eşim cevapladı. Telefonumu evde bırakmıştım ve eşim gelen aramayı açmış.

Arayan kişi Yapı ve Kredi Bankası'nın sağlık sigortası şirketinden aradıklarını belirtmiş.

Kişisel bilgilerimi doğru olarak söylemiş. Aradıkları şirketten 2 yıllık sağlık sigortası yaptırdığımızı belirtmiş. "İlk yıl bizden size hediye idi, ama bu yıl için 700 Türk lirası ödemeniz gerekiyor" demiş. Bu ödemeyi banka kartınızdan gerçekleştirebilmeniz için biz size yardımcı

olacağız demişler. Eşim "biz ödemeyiz" deyince önce ikna etmeye çalışmışlar, ikna olmayınca iptal edelim demişler. Ama iptal edebilmek için de mesaj ile şifre göndereceklerini belirtmişler.

Eşim, telefonun tuşlu olduğunu belirtip yapamayacağını söylemiş ve telefonu kapatmış.

Ertesi gün beni ben dışarıdayken aradılar. Bu görüşmede mesajla gönderdiğimiz şifreyi tuşlamayın, okuyun dediler. Gelen şifreyi okuyunca kredi kartında kalan limit olan 900 Türk

Lira tutarında harcama yapmışlar.

Başka arama olmadı. Bankaya itiraz ettik, ama banka geri ödeme yapmadı. Savcılığa da gitmedik. Şifreyi kendi rızam ile söylediğim için hiçbir sonuç çıkmadı.

4.VAKA

52 yaşımdayım, olay olduğunda 45 yaşımdaydım. Olay 7 yıl önce gerçekleşti.

Evliyim, yüksek lisans mezunuyum, hane halkı sayısı 3, kirada oturuyoruz ve çalışıyorum.

Cumartesi günü eşimin doğum gününde saat 16:00-17:00 gibi arandım. Arama 20 dakika sürdü.

Cep telefonundan arandım, telefonum tuşlu idi. Karlı bir gündü. Eşimin doğum günü olduğu için yaşlı annemi evine götürmek üzere yolda iken ve alışveriş yaptığımdan ellerim dolu iken

arandım. Arayan kişi doğu illerimizden birinin Emniyet Müdürlüğü'nden aradıklarını belirterek

görüşmeye başladı. Adımı ve soyadımı doğru söyledikten sonra “telefon sizin adınıza mı kayıtlı?” diye sordular. Evet cevabını alınca da “telefonunuz dün akşam yanınızda mıydı?” diye sordular. Yine evet cevabı verince ise dün akşam benim numaramdan güvenlik güçlerine telefon açıldığını, küfredildiğini ve bu nedenle soruşturma açıldığını belirttiler. Ama benim numaramı tespit ettiklerini, bu numaranın terör örgütü tarafından kullanıldığını, operasyon yapılacağını ve bu operasyon için de 100 kontür ödemem gerektiğini söylediler. Arka taraftan ise sürekli telsiz sesi geliyordu. Telefonumun hatlı olduğunu belirttim, kontür yüklemesi için telefoncuya gitmemin gerektiğini ama kimseye operasyondan bahsetmemem gerektiğini, hatta kimseyle konuşmamamı söylediler. Yaşlı annemi ve elimdeki alışveriş torbalarını eve teslim edip kontür yüklemek için kimseye bir şey söylemeden dışarı çıktım.

Verilen numaraya 100 kontür yükledikten sonra, savcı için de 100 kontür yüklememi söylediler. Operasyonda yer alacak 16 kişinin numaralarını yazdırdılar ve her biri için de 100 kontür, toplamda 1.600 kontür yüklememi isteyince dolandırıldığımı anladım ve telefonu kapattım. Telefoncu ise kontür yüklediği kişilerin arkadaşlarım olduğunu ve bu nedenle kontür yükletmemde bir gariplik olmadığını zannetmiş.

Telefonu kapattıktan sonra arayan numarayı aradım ama açan olmadı. Tekrar aranmadım. Polis ya da savcılığa gitmedim. Neden gitmediğimi ise hatırlamıyorum.

5.VAKA

52 yaşındayım, ilk arama Mart 2017 ayında oldu.

Evliyim, yüksek lisans mezunuyum, hane halkı sayısı 3, kirada oturuyorum ve çalışıyorum.

Hafta içi öğlen saatlerinde bir kişi arayarak yanlışlıkla benim telefon faturamı ödediğini belirtti.

Siz de bana geri ödeyin diyerek aramış. Ben bankada otomatik talimatım olduğunu, faturamın ayın 15’inde ödendiğini, o tarihten önce inceleme yapmadan ödeme yapamayacağımı belirttim.

Arayanın ödediğini söylediği miktarı hatırlamıyorum.

Bu aramadan yaklaşık 10 gün sonra, ayın 15'inden önce, bir Pazar günü, akşam saatlerinde aynı kişi tekrar aradı. "Karnım aç, babamdan para isteyemem, lütfen biraz para gönder" dedi. Ben ayın 15'inden önce gönderemeyeceğimi tekrar belirtip telefonu kapattım.

Ayın 15'inde hesap ekstremi kontrol ettiğimde; arayanın belirttiği tarihte bir ödeme yaptığını gördüm. Bu tutarı göndermek üzere arayan numarayı tekrar aradım ama telefon numarasının iptal olduğunu anladım.

Ekim 2017'de Savcılık vasıtasıyla ifade vermeye çağırıldım. Beni arayan aynı bahane ile başkalarını da aramış ve faturalarını ödediğini belirtmiş. Ama tüm bu ödemeleri dolandırdığı başka bir kişinin kredi kartından gerçekleştirmiş. Kredi kartı kullanılarak dolandırılan bu kişi faturası ödenenlerden davacı oldu. Kredi kartı kullanılarak dolandırılan kişi ifadesinde; şifresini bu dolandırıcılara verdiğini ifade etmiş. Dava sürüyor.

6.VAKA

42 yaşındayım, olay olduğunda 40 yaşındaydım. Olay 2 yıl önce gerçekleşti.

Evliyim, üniversite mezunuyum, hane halkı sayısı 4, kiracıyım ve kendi işimi yapıyorum.

Cep telefonumdan arandım. Cep telefonum akıllı telefon. Hafta içi, işyerindeyken arandım.

Akşam üzeriydi. Görüşme yaklaşık 15-20 dakika sürdü.

Beni arayanlar aradıkları şirketin adını söyledikten sonra Google ile özel bir anlaşma yaptıklarını, 5 anahtar kelime girdikleri şirketi aramalarda ön sıraya çıkardıklarını söylediler.

Bu işlemin ücretinin de 600 Türk Lirası olduğunu belirttiler.

Ben iş yerinde ve bilgisayar başında olduğum için arayanın verdiği şirketin web sayfasına girdim, telefonla görüşürken şirketi araştırdım, referanslarını bile inceledim.

Söyledikleri rakam verdiklerini taahhüt ettikleri ücrete göre cazip geldiği için hemen 600 Türk Lirasını kredi kartından telefonla görüşürken ödedim. Aradan 1 ay geçti ve herhangi bir aramada ön sıralarda çıkmadığımızı görünce şirketi tekrar aradım. Sistemlerinde iyileştirme

yaptıklarını, en kısa zamanda arayacaklarını belirttiler. Geri dönüş almayınca tekrar aradım ve telefon kapalı olduğu için dolandırıldığımı anladım.

Olayı savcı arkadaşım ile paylaştım. Arkadaşım “herhangi bir şey yapılamaz” dediği için de suç duyurusunda bulunmadım.

7.VAKA

30 yaşındayım. Olay geçen yıl gerçekleşti. Olay olduğunda 29 yaşındaydım.

Evliyim, yüksek lisans mezunuyum, hane halkı sayısı 2, kirada oturuyorum ve çalışıyorum.

Cep telefonum akıllı telefon. Hafta içi 16:00 civarında cep telefonumdan arandım. Arayan numara da cep telefonu numarasıydı. Görüşme yaklaşık 5 dakika sürdü. Yapı ve Kredi Bankası’ndan aradığını belirten kişi Çin’den kredi kartımdan para çekilmeye başlandığını ve kart limiti olan 5.000 liraya kadar da çekme işlemi gerçekleştireceklerini söyledi ve kartımı kapatmak için onay istedi. O kadar limitim olmadığını belirttiğimde; arayan kişi destek hesabımın olduğunu ve en azından onu iptal etmemizi söyledi. İptal etmek için “sizi başka birine aktarıyorum” dedi. İptal etmek istemediğimi tekrarlayınca arayan kişi sert bir şekilde konuşmaya başladı, ben de telefonu kapattım.

Telefonu kapattıktan sonra bankamı aradım ve görüştüğüm görevli 5.000 lira destek hesabım olduğunu belirtti ve istersem destek hesabımı kapatabileceğini söyledi. Ben “hayır kapatmayın. Ama siz bana daha önce destek hesabım olduğu ile ilgili herhangi bir bilgi vermediniz, sizi dava edeceğim.” deyip telefonu kapattım.

1 gün sonra tekrar bankayı aradım ve bana herhangi bir destek hesabımın olmadığını söylediler. Aynı tarihlerde ise; İş Bankası ile başka bir tecrübe yaşadım. Bir e-ticaret şirketinden alışveriş yaptıktan sonra (alışveriş tutarı 15 Türk Lirası idi) İş Bankası tarafından arandım ve böyle bir işlem yapıp yapmadığımı sordular. Ben bu işlemi gerçekleştirdiğimi banka yetkilisine söyledikten sonra, miktar az olmasına rağmen neden aradıklarını sordum. İş Bankası görevlisi

ise alışveriş yaptığı e-ticaret şirketinin isminin kara listede olduğundan dolayı aradıklarını söylediler.

Bu işlemten sonra ise Yapı ve Kredi Bankası'ndaki hesabımı kapattım.

Polise ya da savcılığa gitmedim.

8.VAKA

23 yaşındayım. Olay geçen yıl gerçekleşti, olay olduğunda 22 yaşındaydım.

Bekarım, üniversite öğrencisiyim, hane halkı sayısı 3, ev kendimizin ve öğrenciyim, çalışmıyorum.

Cep telefonum akıllı telefon. Cep telefonumdan hafta içi, 19:00-20:00 aralığında arandım.

Görüşme yaklaşık 5 dakika sürdü.

Arayan kişi polis memuru olduğunu belirtti ve adı soyadını verdi. Ben arayan sosyal medya hesaplarımda kullandığı ad ve soyadını söylediği için dolandırıcı olduklarını görüşmenin ilk dakikasında anladım ama görüşmeyi sürdürdüm.

Arayan kişi ismini belirttiği sosyal medya hesaplarımdan birinde 15 Temmuz'dan önce bir paylaşım yapıldığını belirtti. Bu paylaşımında her şeyin bir anlamının olduğunu; örneğin paylaşımında direk olduğunu ve bunun "1" rakamını simgelediğini söyledi. Diğer söylenenleri hatırlamıyorum ama arayan paylaşımında bu 15 Temmuz'un 1'i, şu 15 Temmuz'un 5'i, şu 15 Temmuz'un "T" si vs vs diyerek benim FETÖ'den olduğumu ve 15 Temmuz'u önceden bildiğim için bu fotoğrafı paylaştığımı belirtti. En yakın ATM'ye gidip 10.000 Türk Lirasını belirteceği hesaba yatırmam gerektiğini söyledi.

Ben dalga geçerek konuştum. Karakola gideceğimi belirtince de arayan kişi küfür edip, telefonu kapattı.

Karakola gittim. Aranan numarayı verdim, şikayet ettim. Tekrar aynı numaradan aranmadım.

9.VAKA

53 yaşımdayım, olay Eylül 2017'de gerçekleşti.

Evlüyüm, üniversite mezunuyum, hane halkı sayımız 4 kişi, kirada oturuyoruz, emekliyim ama çalışıyorum.

Cep telefonum akıllı telefon. Hafta içi, evdeyken, akşam üstü, cep telefonumdan arandım.

Görüşme birkaç dakika sürdü.

Arayan kişi; benim TC kimlik numaramı, adım ve soyadımı söyledi. Kişisel bilgilerimin çalındığını, kredi kartımın tehlikede olduğunu ve şifremi vermem gerektiğini belirttiler. Ben gülmeye başlayınca arayan sinirlendi, küfür edip kapattı.

Arayan numarayı aradım ama açan olmadı.

10.VAKA

21 yaşımdayım, olay olduğunda 20 yaşımdaydım. Olay geçen yıl gerçekleşti.

Bekarım, ön lisans mezunuyum, hane halkı sayımız 5 kişi, kirada oturuyoruz ve çalışıyorum.

Cep telefonum akıllı telefon. Hafta içi, evdeyken, 09:00-11:00 arasında arandım. Görüşme yaklaşık 5 dakika sürdü. 0 850 ile başlayan bir numaradan arandım.

Arayan kişi adım ve soyadımı söyledikten sonra; Anadolu Sağlık Danışmanlık şirketinden aradığını, kendileri ile 2 yıllık bir sözleşme imzaladığımı söyledi. İlk yılımın dolmasına çok az bir süre kaldığını; 2. yıl için de 400 TL ödemem gerektiğini ve ödemeyi gerçekleştireceğim kredi kartının bilgilerini istedi.

Ben böyle bir taahhütte bulunmadığımı, sözleşme imzalamadığımı söyledim. Arayan kişi telefonda taahhütte bulunduğumu ve ses kaydımın olduğunu belirtti. Ben ses kaydımı dinletin şeklinde cevap verdim. Arayan ise dinletemeyeceklerini, eğer benim ile anlaşmazsa hukuk yoluna başvuracaklarını söyledi. Ben de siz bilirsiniz, o zaman mahkemede görüşürüz dedim ve telefonu kapattım.

Savcılığa suç duyurusunda bulundum.

11.VAKA

49 yaşımdayım. Olay bu yıl, 2017 yılında oldu.

Evliyim, üniversite mezunuyum, kamu çalışanıyım ve kendi evimizde 4 kişi oturuyoruz.

Olay hafta içi gerçekleşti. Öğle vakti, ev telefonumdan arandım. Özel numaradan aranıyordum, yani arayan numara gözükmüyordu. Benim adımlı söyleyip Emniyetten arıyorum, komiser dediler. Kredi kartınız var mı diye sorduktan sonra hangi banka diye sordu. Etki altına almaya çalışır gibi konuşuyordu. Kredi kullanmışsınız. Bununla ilgili şikayet var dedi. Ama bu şikayetin ne olduğunu sorduğumda söylemedi kontrol altına almaya çalışıyordu. Hangi karakola gitmem gerekiyor, ben geleyim dedim. Sicil numaranı kimliğini söyle dedim. Bağırma başladı. Kapattım telefonu. Görüşme yaklaşık 5 dakika sürdü.

20 gün sonra yine evden, yine özel numaradan arandım. Ama arayan kişi farklı idi. Aynı sorular, aynı kontrol altına alma durumu. Bu sefer de bir soruşturma ile ilgili Cumhuriyet Savcılığı'na gitmem gerektiğini söylediler. Hangi Savcılık, nereye geleceğim dedim. Kamu görevlisine yakışmaz yaptığınız dedim telefonu kapattım.

12.VAKA

45 yaşımdayım, olay 2 yıl önce 40 yaşımdayken gerçekleşti.

Evliyim, ilkokul mezunuyum, bakkal dükkanım var. Kendi evimde oturuyorum ve 3 kişi yaşıyoruz.

Hafta içi, öğlen, cep telefonumdan arandım. Görüşme yaklaşık 5 dakika sürdü. Cep telefonum akıllı telefon değil. Bankadan aradıklarımı söylediler. İsmi verdikleri bankada zaten hesabım var. Kredi kartı verelim dediler. Benim de kredi kartına ihtiyacım olduğu için tamam dedim. Kendi işimde çalıştığım için zamanım yoktu ve hazır kart bana ulaşacaktı. Tüm istedikleri bilgileri verdim. Onlar da mevduatımdaki 3.000 TL paramı başka hesaba aktarmışlar.

Polise gittim, ifade verdim. Ama bir şey çıkmadı. Tekrar aramadılar.

13.VAKA

38 yaşımdayım. Olay 2 yıl önce, 36 yaşımda iken gerçekleşti.

Evliyim. İş adamıyım. Üniversite mezunuyum. Kirada oturuyorum.

Sabit numaradan eşimi aramışlar. Polis tarafından arandığımızı söylemişler. Kendi telefon bilgilerini paylaşmışlar. Konferans yolu ile eşimi telefona bağlayan dolandırıcılar beni eşimle telefon üzerinden konuşturdular. Eşim polislerin geldiğini belirtti. Polisler evde karşıdaki komşu ile ilgili suç duyurusu var demiş. Kredi kartları ile ilgili problemlerden dolayı evde olduklarını söylediler. Ben sitenin güvenliğini çağırmasını istedim. Çocuklarımı rehin aldıklarını ve para vermezsem onları öldüreceklerini belirttiler. Ben işteki çalışanlarıma mesaj atıp evi kontrol etmeleri gerektiğini söyledim. Evde böyle bir problem olmadığını söylediler. Hem eşimi, hem de beni kandırdıklarını anladım. Eşimi ise “eşin bizim elimizde ve karşıdaki komşu yüzünden polisler evde demezseniz eşini öldürürüz” şeklinde tehdit etmişler. İki tarafı da konferans yoluyla bağlayarak birbirimize düşürmeye çalıştılar. Evde bir problem olmadığını öğrenince durumu anladım ve telefonu para göndermeden dolandırıcıların yüzlerine kapattım. 30 dakika süren bu telefon görüşmesi hafta içi sabah 11:00 civarında yaşanmıştı. Polise başvurduk. Savcılığa gidin şikayetçi olun dediler. Ama savcılığa başvurmadık.

14.VAKA

45 yaşımdayım. Olay 9 yıl önce; 36 yaşımdayken gerçekleşti.

Evliyim, lisans mezunuyum, emekliyim.

Hafta içi, akşam üzeri 4:00-5:00 civarı arandım. Çalışmıyordum. Sabit telefondan aradılar. Kendini komiser olarak tanıtan dolandırıcı, kredi kartımdan para çekildiğini söyledi. Konuşma 2-3 dakika kadar sürdü.

Telefon görüşmesi devam ederken kredi kartımdan para çekildiğini belirttiler. Arkadan telsiz sesleri geliyordu. Neden Emniyet Müdürlüğü'nden arandığımı sorduğumda ise bankadan bilgi geldiğini söylediler. Bende o zaman engelleyin dedim. X Karakoluna geleceksiniz dediler. Sadece ismimi söylediler ve hakkımda başka bilgi paylaşmadılar. Kredi kartımın şifresini istediler. Karakolun ismini tekrarlattıktan sonra bir gariplik olduğunu hissettim. Acelemiz var,

vaktimiz yok dediler. Tekrar söyleyin avukatımla geleceğim dediğimde ise vaktimiz yok paranız gidiyor, siz verin biz halledeceğiz diye panik yaptırmaya çalıştılar. Vermiyorum deyince ise küfür etti ve kapattılar.

Polise veya savcılığa şikayet etmedim.

15.VAKA

55 yaşındayım. Olay 2 yıl önce, 53 yaşında iken gerçekleşti.

Evliyim, lisans mezunuyum, emekliyim ve çalışıyorum.

Taksi ile eşimle Nişantaşı'na giriyordum. Hafta içi, saat 19:30 civarı cep telefonumdan arandım. Arayan kişi Finansbank'tan aradığını belirtti. Telefon ekranında sanki kurumsal bir şirketten aranıyormuşçasına 0 850'li numara görünüyordu. 5 dk önce bir adet alışveriş yapıldı siz mi yaptınız diye sordular. Son 2-3 saattir işlem yapmadım dedim.

Ama şu an kartınızdan alışveriş yapılıyor o zaman sanırım kopyalanmış dediler. Telaşlanınca eşime anlattım. Ne yapacağız diye sorunca; arayan bu işlemleri iptal edebilirsiniz dedi. Size şifre gönderiyorum, iki işlemi de iptal edeceğiz dedi. Finansbank'tan mesaj geldi. Gelen eski mesajları görebiliyordum. İkinci şifreyi söyledim. Şimdi kartın iptali yapılacak 15 gün içinde yeni kartınız gelir dedi. Kart 15 gün sonra tarafıma ulaşmayınca; ilgili bankanın müşteri hizmetlerini aradım. Müşteri hizmetleri bana dolandırılmaya çalışılmışsınız 150 Euro ve 450 Euro tutarında alışveriş yapılmaya çalışılmış fakat bakiye yetmemiş diye beni bilgilendirdiler. Görüşme 10 dakika sürdü.

Eşim mali müşavir, ben ise bankacıyım ve dolandırıldığımızı fark etmedik. Herhangi bir yere şikayette bulunmadık.

TELEFON DOLANDIRICILIĞINA MARUZ KALAN 15 KADIN VAKASI

1.VAKA

40 yaşındayım. Olay 7 yıl önce, 33 yaşımdayken gerçekleşti.

Evliyim, yüksek lisans mezunuyum, hane halkı sayısı 3, kendi evimizde oturuyoruz. Çalışıyorum.

Hafta içi, iş yerimdeyken öğleye doğru arandım. Kendilerini polis olarak tanıttılar. Arka taraftan telsiz sesleri geliyordu. Görüşme 5 dakika sürdü.

Telefonla arayıp kendisinin polis olduğunu söyleyen kişi; benim adımı ve soyadımı söyledi. Adıma İstanbul dışında bir yerden kontür alındığını belirtti. Ben sürekli sorular sorarak ve hızlı hızlı konuşarak daha fazla bilgi almaya çalıştım. Hatta “siz kapatın, ben sizi arayacağım” dedim. Birkaç dakika süren bu görüşmede dolandırılmak maksadıyla arandığımı anladım ve telefonu kapattıktan sonra eşimi aradım. Eşim avukat ve beni arayan numarayı tekrar aradı, numara doğruymuş. Bu numarayı Bilişim Suçları’nda görev yapan savcı arkadaşımıza verdik. Ama sonuçta bir şey çıkmadı.

Bu numaradan daha sonra aranmadım.

2.VAKA

70 yaşındayım, olay geçen yıl gerçekleşti.

Evliyim, lise mezunuyum, hane halkı sayımız 2, kendi evimizde oturuyoruz, emekliyim.

Ev telefonundan arandım. Arayan numara gözüküyordu. Hafta içi saat 16:00 civarında aradılar. Görüşme yaklaşık 2 dakika sürdü.

Arayan kişi; adımı soyadımı söyleyip polis memuru olduğunu belirtti. Benim kimlik bilgilerimin kullanılarak terör örgütü hesabına para yardımında bulunduğu belirtti.

Ben dolandırıcıların aradığını anlayıp, eşimin de polis olduğunu söyleyip; arayan kişinin ismini tekrar sordum. Arayan telefonu hemen kapattı.

Polise şikayette bulunmadık. Başka bir arama da olmadı.

3.VAKA

45 yaşındayım, olay 2 yıl önce gerçekleşti.

Evliyim, lisans mezunuyum, hane halkı sayımız 4, kendi evimiz ve çalışıyorum.

Hafta içi, iş yerindeyken, saat 12 gibi “.....Sağlık Sigortası yaptırmışsınız” diye cep telefonumdan aradılar. Ben o an bilgisayar başında olduğumdan aradıklarını belirttikleri şirketin web sayfasını aradım. Web sayfasının mevcut olduğunu gördüm.

Böyle bir sağlık sigortası yaptırmadığımı belirttim. Yapı ve Kredi Bankası kredi kartımın numarasını ve son kullanma tarihini bildiklerini, parayı çekeceklerini belirttiler. Ben siz bilirsiniz, yapabiliyorsanız yapın dediğim zaman da küfredip telefonu kapattılar.

Ben arayan numarayı aradım ama açmadılar.

Web sayfasına tekrar baktığımda sayfanın altında, çok küçük puntolarla “şirketimizin adını kullanarak sizleri arayanlar olabilir, o biz değiliz” gibi bir ibare olduğunu fark ettim.

Görüşme yaklaşık 5 dakika sürdü.

Tekrar aranmadım..

4.VAKA

82 yaşındayım, olay geçen yıl yaşandı.

Dulum, ilkokul mezunuyum, yalnız yaşıyorum, kendi evim ve emekliyim.

Cep telefonumdan, hafta içi, sabah 10:30 gibi arandım. Cep telefonum akıllı değil, tuşlu telefon. Telefon oğlumun üzerine kayıtlı ve kamu hattı. Oğlum da aynı saatlerde cep telefonundan 6 kez aranmış, ama numarayı tanımadığı için açmamış. Görüşme yaklaşık 30 dakika sürdü.

Telefonla arayan kişi; Emniyet Müdürlüğü’nden aradığını, oğlumun ismini vererek onun terör örgütüne yardım etmekten tutuklandığını, ama bankadaki paramı verirsem herhangi bir soruşturmaya gerek olmadan oğlumu serbest bırakacaklarını söyledi. Ev adresimi doğru olarak söylediler ve birazdan bir sivil ekip otosu göndereceklerini, beni evimden alacaklarını ama kimseye söylemememi hatta konuşmamam gerektiğini, ev telefonu çalarsa cevap vermememi, cebimi ise kapatmadan onlar ne derse yapmam gerektiğini söylediler. Bana sivil ekip otosunun rengini verdiler, sivil ekip otosunun apartmanımın önüne geldiğini, aşağıya inip şoförle de konuşmadan banka şubesine gitmemi söylediler.

Ben denilenleri yaptım. Sivil ekip otosu sandığım arabaya bindim ve banka şubesinin evimin yakınındaki hastanenin içinde bulunduğunu söyledim. Adam banka şubesinin önüne gelince arabadan indim ve banka şubesine girip, tüm paramı nakit olarak çekmek istediğimi söyledim. Veznedeki görevli bakiyeme bakarken, diğer görevli beni tanıdı ve oğlumun yalnız geldiğimde işlem yapmamalarını söylediğini belirtti.

Görevliler iyi olup olmadığımı sorduklarında bir problem olduğunu anlayıp hastane polisini çağırdılar. Sivil oto ise o sırada kaçmıştı.

Savcılığa suç duyurusunda bulunduk. Ancak takipsizlik kararı verildi. Gerekçe ise maddi kayıp olmaması idi.

5.VAKA

62 yaşımdayım, olay 2 yıl önce gerçekleşti, olay gerçekleştiğinde 60 yaşımdaydım.

Dulum, lise mezunuyum, yalnız yaşıyorum, kendi evim ve emekliyim.

Hafta içi, öğle saatlerinde ev telefonundan arandım. Arayan numara gözüktüyordu. Görüşme 10 dakika dürdü.

Arayan kişi kendini polis memuru olarak tanıttıktan sonra adımı ve soyadımı söyledi. Terör örgütüne yardım ve yataklık yaptığımı belirtti. Adres bilgilerimi de doğru olarak söyledikten sonra; sizinle aynı ikametgahı paylaşan bir kişi var ve o kişi terör örgütü üyesi dedi. Kendilerinin bana yardım edeceklerini, yaşlı olduğumu geri kalan ömrümü hapiste geçirmememi söylediler. Evimde tahmini olarak şu kadar altın bulunduğunu söylediler (ki tahmini olarak arayanların söyledikleri miktar kadar evde altın vardı) ve bu altınları güzelce sarıp sarmalayın, biz sizi tekrar arayacağız dediler. Tekrar aradığımızda sardığım altınları evimin bahçesine koymam gerektiğini, kendilerinin altınları oradan alacaklarını ve benimle aynı ikamette gözüken terör örgütü üyesinin bilgilerini ikametimden sileceklerini belirttiler.

Ben telefonu kapattıktan sonra erkek yeğenimi aradım. Yeğenim polisin altın istemeyeceğini, eğer böyle bir durum varsa eve gelip polis otosu ile alacağını belirtti ve hemen evime, yanıma geleceğini söyledi. Erkek yeğenim evime geldikten sonra ev telefonu tekrar çaldı, yeğenim telefona cevap verdi. Ben de polis memuruyum, sicil numaram şu; sizin sicil numaranızı öğrenebilir miyim dedi. Arayan kişi herhangi bir şey söylemeyince; yeğenim küfür edip telefonu kapattı.

2 gün sonra arayan kişi tekrar aradı küfür ettiğiniz için size tazminat davası açacağım dedi; bu sefer de ben küfür ettim ve telefonu kapattım.

Polis ya da savcılığa gitmedim ama ev telefonumun numarasını değiştirdim.

6.VAKA

45 yaşımdayım. Olay 2 yıl önce gerçekleşti.

Evliyim, üniversite mezunuyum ve serbest çalışıyorum. Kendi evimiz ve 4 kişiyiz.

İstanbul'a yeni taşındığım bir dönemdi. Eşim yanımda yoktu. Hem evin taşınma işlerini, hem çocukların okul nakil işlerini halletmeye çalışıyordum. Zihinsel olarak yorgun olduğum bir andı. Yeni taşındığımız için yüklü de paramız vardı. Hafta içi saat 16:00-17:00 gibi, ev

telefonumdan arandım. Numara gözükmüyordu ve cep numarasıydı. Arka fondan telsiz sesleri geliyordu. Komiser olduğunu, Üsküdar Emniyet Müdürlüğü'nden aradığını söyledi. Ailemden birkaç isim ve soyisim söyledi (Kayınpeder ve kayınbiraderimin isimleri). Manipüle etmeye çalışıyordu. Kuyumcudan altın çalınmış dedi. Benim ismimi bilmiyordu. İsmimi almaya çalıştı. Buradakiler senin numaranı verdiler. Siz de işin içindeymişsiniz dedi. Biz düzgün bir aileyiz dedim. Emniyet'e geleyim dedim. Küfür etti. Küfür edince dolandırıcı olduklarını anladım ve telefonu suratına kapattım. 155 i aradım. Sonra sürekli aramaya başladılar ama numara gözükmüyordu. Görüşme 10 dakika sürdü.

Bir daha aramadılar.

7. VAKA

45 yaşındayım, Olay Eylül 2017 ayında gerçekleşti.

Evlüyüm, üniversite mezunuyum ve serbest çalışıyorum. Kendi evimiz ve 4 kişiyiz.

0 850'li numaradan hafta içi, 16:00-17:00 arası aradılar. Görüşme yaklaşık 10 dakika sürdü. Cep telefonumdan aradılar. Cep telefonum akıllı telefon. Bankacı jargonuyla konuşuyordu. Akbank Genel Müdürlüğü'nden aradıklarını belirttiler. Mobil bankacılık kullandığımı ve versiyon güncellemesi yapacaklarını belirttiler. Akbank'ta hesabım vardı ve mobil bankacılık kullanıyordum. O nedenle bir anda versiyon güncellemesi için dediklerini yaptığım ve tuşlamayı gerçekleştirdiğim anda hesabımdan 5.000 TL EFT yaptılar. Dolandırıldığımı o anda anladım. Bankanın telefon bankacılığını aradım, olayı anlattım, EFT'yi iptal edin dedim. Banka şubem İstanbul dışında olduğu için en yakın şubeye gidin dedi. Şubedekiler ilgili gibi davrandılar ama bir sonuç çıkmadı. 1 hafta uğraştım. BDDK'ya yazdım. Savcılığa şikayette bulundum.

8. VAKA

46 yaşındayım. Olay 1 yıl önce 45 yaşındayken gerçekleşti.

Bekarım, lise mezunuyum, çalışıyorum, evde 2 kişi yaşıyoruz., kirada oturuyoruz.

Hafta içi, 11:00-12:00 gibi, cep telefonumdan arandım. Cep telefonum akıllı değil. Birkaç kez aradılar. Toplam 20 dakika civarında görüşmüşüzdür. Yanında bir kişi daha vardı. Mecidiyeköy'deİletişim Merkezi'nden aradıklarını belirttiler. Sabit tel numarasından aradılar. Numara gözükmüyordu.

Yıllık kredi kart ücretlerini geri almak için aradıklarını belirttiler. 10 yıllık kredi kart aidat ücretlerini geri alabileceklerini belirttiler ve bunun karşılığında da alacakları ücreti belirttiler. Bankaya ödediğimin 7.500 TL olduğunu, kendilerinin alacağı miktarın ise 1.250 TL olduğunu söylediler. Sürekli soru soruyordum, arkadan sesler geliyordu, kalabalık bir ortam olduğu izlenimi vermeye çalışıyorlardı. Hangi bankanın kredi kartını kullandığımı sordular. Hem banka ismini, hem de hesap numaramı söyledim. Güvenlik numarasını sorunca ise vermedim. Güvenlik numarasını vermeyince başka bir yetkiliye bağladı. O zorlayınca güvenlik numarasını verdim. Bu sefer de kredi kartı şifresini istedi. O zaman uyandım. Neden diye sorunca mantığa uygun olmayan bir şeyler anlatmaya başladı. Ben de telefonu kapattım.

Arayan numarayı aradım ama arızalı gibi çalışıyordu. Bankayı aradım. Kartımı iptal ettirdim.

Polise de savcılığa da gitmedim.

9.VAKA

45 yaşındayım. Olay 3 yıl önce, 42 yaşımdayken gerçekleşti.

Bekarım, yüksek lisans mezunuyum, çalışmıyorum, kirada oturuyoruz ve hane halkı sayısı 4 kişi.

Cepten arandım, cep telefonum akıllı telefon. Pazar günü, öğleden sonra aradılar, görüşme 15 dakika sürdü. Arayan numara gözüküyordu. Ankara'dan aradıklarını Terörle Mücadele'den komiser.... olduğunu söyledi. Bir teröristi yaklaşık 6 aydır takip ediyoruz dedi. Kimliğimin kopyalandığını ve kopyasının o teröristin üzerinden çıktığını belirtti. Ben sizi başka bir birime aktaracağım ve size kredi kartınız ile ilgili bir şey soracaklar, bilgi isteyecekler dedi. Ne yapılması gerektiğini sordum. İstanbul'da nereye gitmem gerekiyorsa giderim dedim. Arayan kişi sürekli bağıyordu. Başka birine aktardı. Aktardığı kişi de sürekli bağırarak konuşuyordu. Sanki sorguda gibiydim. Eski bankacıyım ve bu olay olmadan 1 ay önce de bu konu ile ilgili bir mail almıştım. Gitmem gereken yeri söyleyin dedim, herhangi bir şekilde cevap almayınca telefonu kapattım. Aynı numara tekrar aradı.

Polisi aradım. Polis kredi kartı bilgilerinizi vermeyin ve savcılığa gidin dedin.

10.VAKA

46 yaşındayım. Olay geçen yıl, 45 yaşımdayken gerçekleşti.

Evliyim, lise mezunuyum, çalışıyorum. Hane halkı sayısı 2 kişi ve kendi evimiz. Akıllı cep telefonum var.

Hafta içi akşam saatlerinde iş yerindeyken bir iş arkadaşımızın eşi arkadaşımıza mesaj gönderdi. Arkadaşımız da bu mesajı bizimle sözlü olarak paylaştı. Biz eşi olduğunu zannettik ama olmadığını çok sonra fark edecektik. Gelen mesajda Turkcell numaralar için Teknosa çekilişi 300 TL para puan vereceği yazıyordu. Ben de o sıralar Teknosa'dan kettle alacaktım, yaklaşık o kadar fiyatı vardı. Ben de sevindim. Tüm Turkcell li numaraları eşine söyledik. Sonra Turkcell numaramıza gelen mesajı da söyleyin diyordu. Biz de gelen tüm şifreleri söyledik. Bir sonraki ay Turkcell'in telefon faturamıza 278 TL yansıttığını fark ettim Turkcell'i aradım. Merdiven altı firmaların böyle dolandırıcılık yaptıklarını Turkcell'in böyle bir iade yapamayacağını belirtti.

Şikayette bulunmadım.

11.VAKA

30 yaşındayım. Olay 2 yıl önce, 28 yaşındayken gerçekleşti.

Evliyim, yüksek lisans mezunuyum, kendi evimiz ve eşim ile birlikte 2 kişi yaşıyoruz. Çalışmıyorum. Akıllı cep telefonum var.

Cep telefonumdan arandım. Hafta içi öğlen saatleri. Görüşme yaklaşık 45 dakika sürdü. Hakim ya da savcıyız dediler. Arka fondan sürekli sesler geliyordu. Çok inandırıcıydılar. İsim soyisim, baba ismim gibi bilgilerimi söylediler. Panikletmeye çalıştılar. Adıma açılmış bir dava olduğunu bu dava için para yatırmam gerektiğini söylediler. Bankamatik'e gidin parayı havale edin dediler. Telefonu kapattım.

Polise şikayette bulundum. Ama polis inanmayın dedi, savcılığa gidin dedi. Savcılığa gitmedim.

12. VAKA

41 yaşındayım, olay geçen yıl yaşandı.

Bekarım, yüksek lisans mezunuyum, hane halkı sayısı dört kişi, kendi evimiz, çalışıyorum.

Cep telefonumdan, Pazartesi günü, sabah 11:00 gibi arandım. Cep telefonum akıllı telefon. Görüşme yaklaşık 45 dakika sürdü.

Telefonda arayan kişi; Yapı Kredi World Card kullanılarak internete girilmiş hesabınızdan adına para çıkışı yapılıyor, kredi başvurusu yapılıyor biz bunları geri alacağız dedi. 1 saat önce cepten banka hesabıma girildiğini söylediler. Şifreler göndereceğiz. İnternet şifrenizi

değiştirelim dediler. Şifreyi söylemedim ama sürekli öğrenmeye çalıştılar. Şüphelenince ise eski adresler, kredi kartı kullanım alışkanlıkları, en son nereden para çektiğime kadar detaylı bilgiler paylaştılar. Nihayetinde şifremi tuşladım. Tuşladıktan sonra ise telefonuma mesajlar gelmeye başladı. Referans numarası vererek şifreleri söyledim, onay işlemlerini gerçekleştirdiklerini söylediler. Adnan Demirel adına 9.650 TL kredi karttan nakit çekip EFT yapmışlar ve 100 TL cep telefonu faturasını ödemişler. Kredi başvurusu yapılmış fakat ön onaya düştüğü için onaylanmamış. En son “biz sizin paranızı çektik ... hanımla bu paraları tatilde yiyeceğiz” dedikten sonra dolandırıldığımı anladım. İyi günler dedikten sonra kapatsa asla şüphelenmezdim. Konuşmadan sonra Yapı ve Kredi Bankası’ni aradım ve kesinlikle yardım etmediler. Ben içeriden adamların bu işleri yaptığına inanıyorum. Sadece kredi başvurusuna müdahale edildi. Yapı ve Kredi Bankası Çağrı Merkezi banka şubesine gitmem gerektiğini belirtti. Şubeye gittim. Şube öğle tatiline gireceğinden 13:30’da tekrar gelmemi söyledi. Banka “Siz şifrenizi verdiğiniz için yapabileceğimiz bir şey yok” dedi. Bankaya 20 senedir bu tarz işlemler yapmayan biri olarak yarım saat içinde bu tarz işlemler gerçekleştirilince güvenlik engeline nasıl takılmıyorum diye sordum. Cevap olarak dolandırıcılarla aynı şehirde yaşadığınız için güvenlik engeline takılmaz bilgisi verildi.

Polisi aradım şirkete polis geldi fakat bir şey yapılamadı.

Savcılığa suç duyurusunda bulundum ama bir işe yaramadı. Faizi ile beraber ödemek zorunda kaldım. Savcılıktan takipsizlik kararı geldi. Bayrampaşa’da 93. Sırada olduğumu belirtmişler. Takipsizlik kararı çıktı isterseniz soruşturmaya dahil olabilirsiniz dilekçe vermeniz gerekiyor dediler. Dahil olabilmek için dilekçe verdim fakat geri dönüş bekliyorum. Soruşturmaya dahil olup olmadığımı dair bir bilğim yok. Tutar düşük olduğu için çok yardımcı olunmayacağını düşünüyorum. Adamın ismini ve adresini kendi imkanlarımızla bulduk fakat savcılığa bu bilgi verilemeyeceği için bilgiler olmasına rağmen bir şey yapamıyoruz. Adnan Demirel adlı kişinin ya hesabı kullanılıyor ya da sahte kimlik olabilir. Şifre verdiğin için suçlusun şeklinde geri dönüş geldi. Merdiven altı çağrı merkezi olarak adlandırılıyorlarmış. Tanıdıklarımın dolandırıcıların çağrı merkezi eğitimi aldıklarını öğrendim. 45 dakika boyunca sorular sormama rağmen her soruya doğru cevap aldım. Telefonda konuşulurken bankanın hattına ulaşmaya çalıştım fakat hızlı cevap talep ettikleri için ulaşamadım.

13.VAKA

32 yaşımdayım. Bu olay yaklaşık 3 yıl önce oldu, olay olduğunda 29 yaşımdaydım.

Bekarım, lisans mezunuyum, tek başıma yaşıyorum. Çalışıyorum.

Cep telefonumu sabit bir telefondan Engelliler Derneği'nden aradıklarını belirterek aradılar. Hafta içi, saat 13:00 gibi arandım. Görüşme 10 dakika sürdü. Dernek yararına bir tiyatro düzenlediklerini, 50 liralık bilet alarak yardımcı olmak isteyip istemeyeceğimi sordular; kabul ettim ve tiyatro saatlerini ve yerini sordum onlar da size bir davetiye getireceğiz ve açık bir davetiye olacak istediğiniz zaman bu hakkı size yakın olan bir tiyatro organizasyonunda kullanabilirsiniz dediler. Tekliflerini kabul ettim, arayan kişi bileti teslim etmek için ikametgah adresini istedi. Bizzat elden teslim etmek istediklerini söyledi. Ben de adresimi verdim, fakat çalıştığım için akşam eve geliş saatimi belirttim ve o saatten sonra veya hafta sonu elden teslim alabileceğimi söyledim. Karşı tarafta, biz sizi gelmeden önce ararız dedi ve telefonu kapattı. Ertesi gün aynı numaradan arandım akşam kaçta evde olabileceğimi ona göre bileti akşam ulaştıracaklarını söylediler ben eve varış saatimi paylaştım. Aynı günün akşamı eve geldiğimde kapının anahtar kilidinin kırıldığını ve içeri hırsızın girmiş olduğunu gördüm. Evden bir şey almadan çıkmışlar. Tabi olay polise kadar intikal etti. Sonrasında aklıma tiyatro bileti getirecek adamlar geldi ve o taraftan hiç ses seda çıkmadığı için şüphelendim. Arayan numarayı aradım, telefonu kimse açmadı. Bu durumdan şüphelendiğimi polise anlattım. Poliste bu tip vakaların olduğunu ve telefonla arayan kişilerin yapmış olma ihtimalinin üzerinde durdu. Sonuç olarak polis eve girenleri yakalayamadı, aranan telefondan da bir şey çıkmadı. Arayan numarayı internetten aratınca dolandırıcı telefonu olarak bir başlıkta gördüm.

14.VAKA

55 yaşımdayım. Olay 4 yıl önce, 51 yaşımdayken gerçekleşti.

Bekarım, yüksek lisans mezunuyum. 2 kişi yaşıyoruz, kendi evimiz. Akıllı telefona sahibim. Ücretli çalışıyorum.

Hafta içi, sabah saatlerinde arandım. Kendini Cumhuriyet savcısıolarak tanıtan kişi "biz sizi özel görevli olarak seçtik, adınıza Denizbank'tan kredi çıkartıyoruz. Parayı siz değil, biz devlet adına bu krediyi çıkartıyoruz ve miktarı 40.000 lira" dediler. Ben yapamam dedim. Her gün aradılar, bakın üstünüze yeşil elbise giymişsiniz, ray-ban gözlük takıyorsunuz, biz savcıyız dediler. Söylediklerinden beni tanıdıklarını ve takip ettiklerini anladım. Şu bankamatikten şu kadar para çektiniz diye yaptığım tüm işlemleri söylediler. Ben yapamam toplantım var dedim.

Toplantınızı erteleriz dediler. Sonra toplantıyı yapacağım kişinin sekreteri aradı ve toplantımızın başka güne alındığını belirtti. Sizi ikna etmek için sizi kendi numaranızdan arayacağız dediler ve onu da yaptılar. Sonra ikna oldum. Banka şubesine gittim ama o sırada ilk söyledikleri rakamdan daha da yükseltmişlerdi. Miktar 50.000 TL olmuştu. Bir günde banka krediyi çıkarttı.

Dolandırıcılar krediyi benim adıma çıkartmış. Acil istediğimden krediyi bir günde çıkarttılar. Yalova vapurunda kötü görünümlü Kürtçe konuşan iki çocuğa parayı verdim. Tamam görevi tamamladınız dediler. Şimdi şu karakola gidin bilgi verin diye belirttiler. Karakola gidip bilgi verdim, komisere anlattım. Komiser bana “siz dolandırılmışsınız” dedi. Ancak o zaman anlayabildim.

16 yaşlarında olan 2 çocuğu yakalamışlar. Krediyi kendim ödedim.

15.VAKA

81 yaşındayım. Olay 3 yıl önce, 78 yaşındayken gerçekleşti.

Profesörüm. Evliyim. doktora mezunuyum, emekliyim. Tek başıma yaşıyorum. Bakıcım var ama gece kalmıyor.

Hafta içi, gündüz vakti 10:00-11:00 gibi cep telefonumdan arandım. Görüşme 1,5 saat sürdü ve telefon sürekli açık kaldı.

Terör örgütü ile alakalı aradıklarını söylediler, korkmuştum. Kimseye söylemeyeceksiniz dediler. Evdeki bakıcıma polis gelirse hiçbir şey söylemiyorsun ben gidiyorum dedim. Bakıcı ev telefonumdan kızımı aramış. Kızım bakıcıya annemi evde tut kapıyı kilitle demiş. Ev telefonumdan kızım aradı, hiç bir yere gitme kandırılıyorsun dedi ama dinlemedim. Bankaya gittim. Telefon sürekli açıktı görüşme kesilmedi. Bankacıların dikkatli olması gerekiyor bu gibi durumlarda. Bankadan krediyi çektim. Başka bankadan da kredi çektim. İki bankadan ortalama 130.000 TL para çektim.

Önce bana gitmemi söyledikleri semte gittim. Çektiğim parayı dedikleri yerlere koydum. Mesela paranın bir miktarını bir arabanın altına koymamı istediler. Tüm parayı almışlar.

Polise gittik. Durumu anlattım. Polis hiçbir şey yapamayız dedi. Savcılığa şikayette bulunduk, Takipsizlik kararı çıktı.

8.Özgeçmiş

Hatice TUĞSAVUL, 1972 yılında Sivas'ta doğdu. 1989 yılında Kocamustafapaşa Lisesi, Matematik Bölümü'nden mezun oldu. 1989 yılında İstanbul Üniversitesi, İktisat Fakültesi, İktisat (İngilizce) Bölümü'nde başladığı lisans eğitimini 1994 yılında tamamladı.

2007 yılında multidisipliner olması dolayısıyla İstanbul Üniversitesi, Adli Tıp Enstitüsü, Sosyal Bilimler Anabilim Dalı'nda yüksek lisans eğitimine başladı.

