# Oltaya Gelmeyin!

# Phishing[1] Temelli Dolandırıcılık Yöntemleri ve Korunma Yolları

**Yazar: Kıvılcım Günbattı, CFE** | kivilcim.gunbatti@usiud.org | LinkedIn | **Ocak 2021**

"Phishing" (oltaya getirme), dolandırıcıların hedef aldıkları kişileri, e-posta, telefon ve kısa mesaj gibi çeşitli kanallardan sundukları argümanlara inandırarak para, altın, kişisel bilgi, ağ erişimi için gerekli kullanıcı adı, şifre veya bankacılık işlemleri gibi finansal İşlemleri yapabilmek için gerekli hesap numaraları, kredi kartı numaraları, kullanıcı adları ve parolalar gibi kritik bilgileri ele geçirmek için geliştirdikleri yöntemlerin genel adıdır. Phishing, farklı kombinasyonlarla şekil değiştirse de, özünde benzer temel bileşenlere sahip bir dolandırıcılık yöntemidir.

Bu yazıda, öncelikle anılan yöntemler açıklanarak, vaka örneklerine yer verilecektir. Ardından, bu yöntemlerin kullanıldığı dolandırıcılık girişimlerine karşı alınabilecek önlemler hakkında bilgiler sunulacaktır.

## Phishing ve Türevlerini İçeren Dolandırıcılık Yöntemleri

**Nedir?** Phishing türetilmiş bir kelimedir. Password/personal information + fishing (şifre-parola/kişisel bilgi + balık tutma) kelimelerinin bir kombinasyonu olarak, her ne kadar yüksek bir hayal gücü ve espri anlayışı ürünü olmasa da akılda kalıcı bir kavramdır.


Karikatür: Mike Keefe

**Nasıl yapılır?** Bireyler, kurumlar veya çalışanlarından kritik bazı bilgileri (kullanıcı adı ve şifre gibi) elde etmek için genelde bir banka, telekomünikasyon hizmeti sağlayan firma veya bunların müşterileri gibi, bazen de bir kamu kurumu veya resmi bir otorite

[1] Türkçe karşılığı: Oltalama, oltaya getirme, yemleme.

gibi davranılarak, seçilen hedef kişi ya da kurumu, yerine geçilen kişi veya kurum olduğuna ikna etmek suretiyle dolandırmaya dayanan bir dolandırıcılık yöntemidir.

**Phishing yöntemleri çeşitli olsa da, hepsinin merkezinde ikna edicilik ve aldatma bulunmaktadır.** Yani, ***hedefin bilgisi ve kontrolü dışında gerçekleşen bir hacklemeden (sızma, ele geçirme) ziyade, hack için gerekli anahtarın hedefin ikna edilerek temin edilmesi söz konusudur***. Bir benzetmeyle anlatmak gerekirse, bir hırsızın girmek istediği evin kapısını levye kullanarak zorla açması yahut basitçe açık olan bir pencereyi tespit ederek içeri girmesinden ziyade, çeşitli argümanlarla ev sahibini aldatarak kapıyı açmaya yahut anahtarı kendi eliyle vermeye ikna etmesi söz konusudur. Dolayısıyla, **sosyal mühendislik phishing temelli dolandırıcılık senaryolarının geliştirilmesinde ana unsurdur.**

Yöntemin aldığı spesifik isim genelde gerçekleştirildiği kanal veya mecraya göre belirlenmektedir. Bu yöntemler ise genelde özel veya kamu kurumuna ait bir web sitesinin, görünüm ve/veya adres olarak çok benzerini üreterek yahut bunlardan geldiği izlenimi verilen uyarı e-postaları/smsleri veya bunlara ait[2]/çok benzer/çağrı merkezini andıran veya rastgele telefon numalarından yapılan aramalarla yerine geçilen kişi/kurum gibi konuşarak, iletişime geçilen kişiye **kaçırılamayacak bir fırsat** veya bu kişide **korku/panik yaratmayı güdüleyen bir tehdit/risk unsuru** sunarak **kişinin etraflıca düşünmesine fırsat vermeden** çeşitli argümanlarla **ikna edilerek aldatılmasına dayanır.**

Dolandırıcıların olta olarak kullandıkları e-posta, sms veya telefon aramaları şekil ve içerik olarak gerçeğiyle çok benzer olabilir. Gerçek iş akışında yaşanması olası sıkıntılar veya reklam kampanyalarındakine benzer ürün ve teklifler, gündemde yer alan bir konu seçilebilir. **Sağlam güvenlik protokolleri olmayan kişi veya kurumların "yemi" yutup, "oltaya gelme" ihtimali bu nedenle oldukça yüksektir**. Bu yüksek başarı olasılığı nedeniyle, sürekli yeni argümanlar geliştirilerek, duruma ve zamanın şartlarına göre şekil ve kanal değiştirerek, yani çağa ayak uydurarak güncellenen phishing saldırıları var olmaya devam edecektir; çünkü bu dolandırıcılar için oldukça karlı olabilen bir iştir. Bir **phishing mağduru olmamak için** ise, her konuda olduğu gibi **"farkındalık" ilk ve en önemli adım**ı teşkil etmektedir.

## Her Dem Yeşil: Nijeryalı Prens Efsanesi

İnternetin ilk yaygınlaşmaya başladığı büyülü zamanlarında bugün çoğu insanın karikatürize bulacağı phishing e-postalarıyla dolandırıcılık yapılıyordu. Örneğin **kendisine kalan mirası bankadan çekebilmesi için Nijeryalı bir prensin sizin yardımınıza ihtiyacı oluyordu ve yardımınız karşılığında mirasın önemli bir kısmını cömertçe sizinle paylaşmayı vadediyordu**[3]. Sayısı muhtemelen (ve umulur ki) azalmış olmakla birlikte bugün bile hala bu ve benzeri fantastik hikayeye inanarak paralarını kaptıran insanlar olduğundan emin olabilirsiniz.

*Grafik: Futurama ekran görüntüsünden uyarlama*

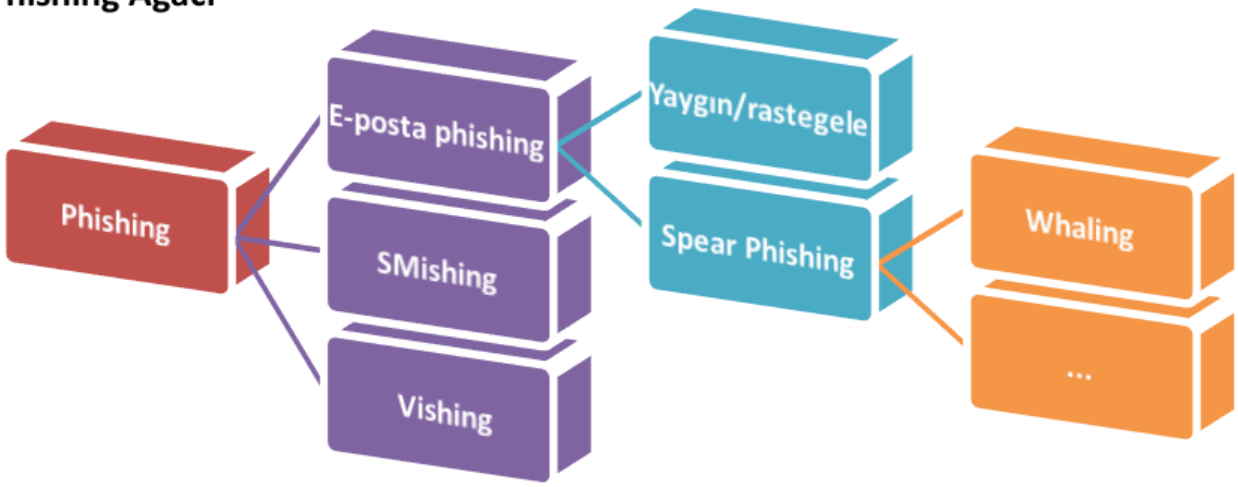
**Günümüzde işler biraz daha farklı yürüyor**; **çünkü dolandırıcılar gündemi, popüler akımları en az bizim kadar iyi takip ediyorlar**. Oltalarının ucuna, hafızamızın aşina

[2] Caller-Id spoofing, yani aranılan kişinin telefonunda sahte arayan kimliği görüntüleme yoluyla

[3] Nijeryalı Prens hikayesine dayalı ilk pishing mesajı aslında internetten bile eskidir ve teleks üzerinden gönderilen mesajlarla başlamıştır; internetle de asıl patlamasını yapmıştır.

olduğu ve defalarca sınanarak ve bu sınamalardan edinilen tecrübeyle sürekli iyileştirilmiş, durup detaylı düşünmezsek rahatlıkla inanabileceğimiz çok gerçekçi, "state of the art"[4] senaryoları takıyorlar. **Sosyal mühendislik ürünü olan bu senaryolar** hedef olarak seçilen kişilerde **korku, panik oluşturmayı** veya **kaçırılamayacak bir fırsat etkisi yaratarak aceleyle ve derinlemesine düşün(e)meden hareket etmeyi** güdüleyecek ince düşünülmüş unsurlar içeriyor. Belirli güvenlik protokollerine sahip olmayan kişiler ise bu senaryolara inanarak, maalesef dolandırıcıların "oltasına" geliyorlar.

**Phishing Ağacı**




## Örneklerle Phishing Türleri

### E-posta phishing

**Yaygın/rastgele alıcı listesine gönderimli:** Bu phishing türünde belirli bir hedef seçimi yoktur. Büyük internet satış sitelerinin veritabanlarından hacklenerek elde edilen listeler, kamu idarelerinin veritabanları hackelenerek elde edilen listeler, sosyal medya üzerinde herkese açık olarak gösterilen eposta adreslerinin toplanmasıyla oluşturulan çok geniş kapsamlı listelere gönderilen, alıcıya özgü detayları içermeyen ve genellikle ekinde önemli bir doküman yer aldığı belirtilen veya bir internet bağlantısını tıklamaya yönlendiren türden epostalar buna örnektir. Tıklanan internet bağlantısında kullanıcı bilgilerinin talep edilmesi veya açılan ekli dosyaya iliştirilmiş bir zararlı kod vasıtasıyla bilgilerin çalınması söz konusudur.

*Karikatür: Kaynağı belirsiz, düzenlendi*

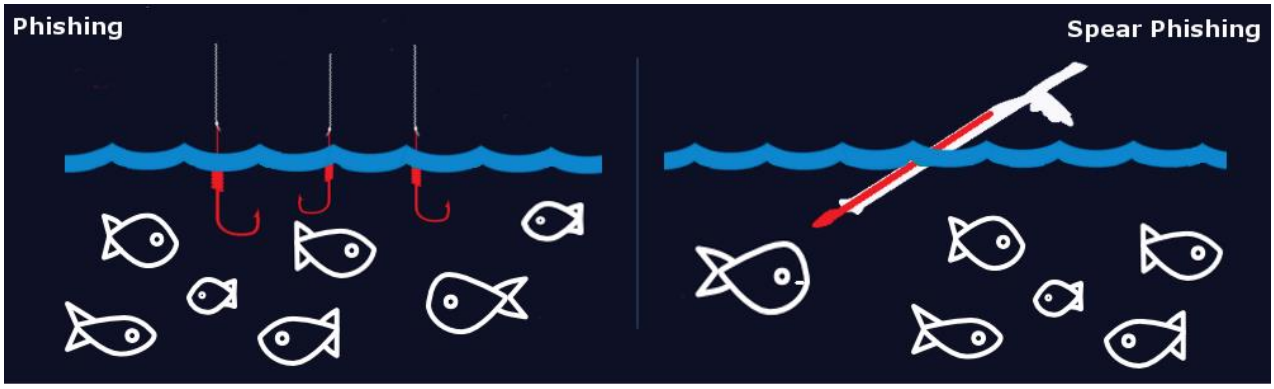
**Spear Phishing (Zıpkın avı, Hedefli Saldırı):** Bu da türetilmiş bir kelime kombinasyonudur: Zıpkın + Phishing. Zıpkınla balık avlama analojisinin tercih edilme nedeni ise olta avcılığının aksine zıpkın avcılığında, avlanacak balığın önceden seçilmesinin söz konusu olmasıdır. Phishing çok sayıda/defa oltayı suya salıp herhangi bir balığın yemi yutmasını beklemeye benzetilebilir. Yaygın/rastgele alıcı listesine yapılan bir phishing saldırısında, hedef çok geniş sayıda ve farklı profillerde bir insan kitlesi olabilir. Ancak **spear phishing saldırıları hedef gözeten,** özellikle **seçilmiş bireyler veya kurumların sistemlerine erişim sağlama saikiyle, genellikle haklarında önceden belirli miktarda bilgi**

[4] Bir tekniğin bilinen/ulaşılan en iyi hali

**toplanmış (sosyal medya, kurum internet siteleri, ticaret sicil kayıtları vs) kişilerin veya kurum çalışanlarının hedef alındığı saldırılardır**. Çalışanları, örneğin Bilgi Teknolojileri yahut İnsan Kaynakları birimindenmiş gibi aramak yahut e-posta göndermek yoluyla içeriden bilgi alma yahut erişim bilgilerini elde etme amaçlanır.

**Biliyor muydunuz?** **Şirketler ve kamu kurumlarının yaşadığı veri sızıntılarının yaklaşık %90'ının başlangıç noktasını spear phishing oluşturmaktadır.**[5]

*Grafik: Kıvılcım Günbattı*




**Tipik bir spear phishing senaryosunda** örneğin kuzenimizden, geçen yaz birlikte Burgazada tatilindeyken çekildiğimiz fotoğraflardan oluşan PDF albümü içeren bir eposta alırız. Kuzenimizin isim ve soyismini içeren bu epostaya ve masum gözüken PDF ekine tıkladığımızda belki de gerçekten birlikte çekildiğimiz o fotoğraları görürüz. Ama bilmeyiz ki; açtığımız PDF dosyayı açan PDF okuyucu yazılımda bulunan bir açıktan yararlanan, dosyaya gömülmüş bir zararlı kod da aynı anda çalıştırılmıştır ve bilgisayarımıza kurduğu bir malware(zararlı yazılım) sayesinde e-posta bağlantılarımıza, hassas dosyalarımıza, hatırlatma amaçlı şifrelerimizi ve kullanıcı adımızı sakladığımız notepad dosyasına, kameramıza, mikrofonumuza, klavye tuşlamalarımıza erişim sağlamıştır. **Sosyal medya** üzerinden yaptığımız **paylaşımlar** ve **internet**[6] **üzerinde bıraktığımız bilgi kırıntıları sayesinde bizi bir süredir takip eden ve hakkımızda arama motorlarında detaylı aramalar yapan bir kişinin erişebileceği bilgi miktarı sizi şaşırtabilir.**

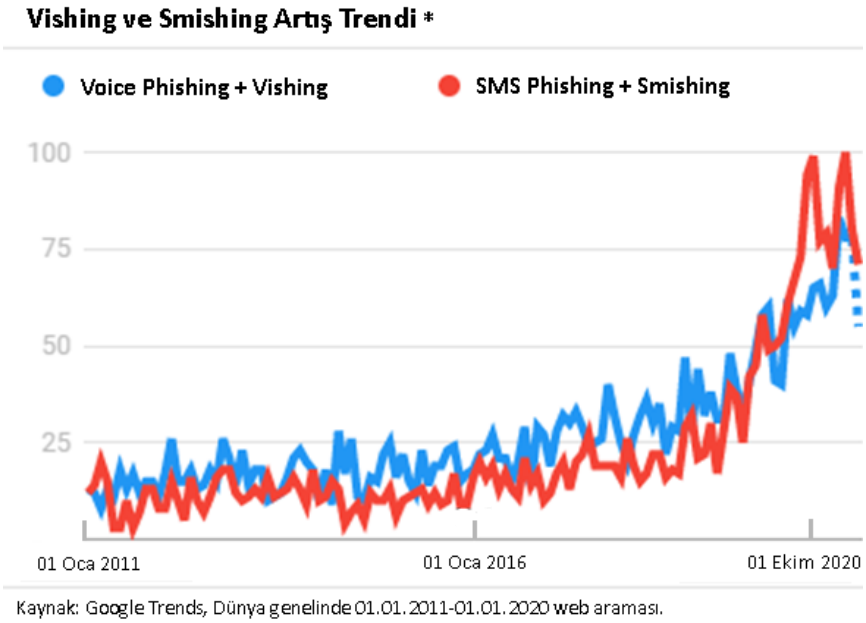
**Whaling (Balina avı):** Spear phishing'in bir alt türüdür diyebiliriz. Burada, hedef seçilen kişi bir kurumun üst düzey bir yöneticisidir, üst düzey bir yöneticinin şirketin kaynaklarına erişimi sıradan bir çalışana göre çok daha geniş ve yüksek olduğundan, amaç tek seferde büyük kazanç elde etmektedir.

**SMishing veya Tishing (Kısa Mesajla Oltaya Getirme): SMS/Text + fishing**

Gerçek kurumdan geldiği izlenimi verilen SMS'lerle kurbanı Vishing'e[7] hazırlamak üzere ön bağlantı kurmak için kullanılabilir. Bazen de SMS içeriğinde sağlanan kısa yollarla başka sitelere yönlendirerek, kişisel bilgilerinizi, kart no, hesap no, kullanıcı adı ve şifrenizi girmeniz istenirken, bazen ise aynı amaca hizmet etmek üzere uygulama kurdurmak amacıyla bağlantı/ kısa yollar gönderilebilmektedir. Örneğin yeni güvenlik güncellemesi adı altında bir uygulama kurdurulması çoğu zaman mümkün olabilmektedir.

[5] Trend Micro Incorporated Research Paper, *"Spear-Phishing Email: Most Favored APT Attack Bait"* syf 3, 2012.
[6] Donald J. Rebovich, D.J., Allen K., Platt J., "*The New Face of Identity Theft: An Analysis of Federal Case Data for the Years 2008 through 2013",* syf 9; 34; 49, 2015
[7] Vishing: Telefon aramasıyla hedefi ileri sürülen argümanlara inandırarak oltaya getirme(phishing) girişimidir.

**Biliyor muydunuz?** **Vishing ve smishing vakaları son yıllarda çok hızlı bir artış trendi içeresindedir.**




Kaynak: Google Trends, Dünya genelinde 01.01.2011-01.01.2020 web araması.

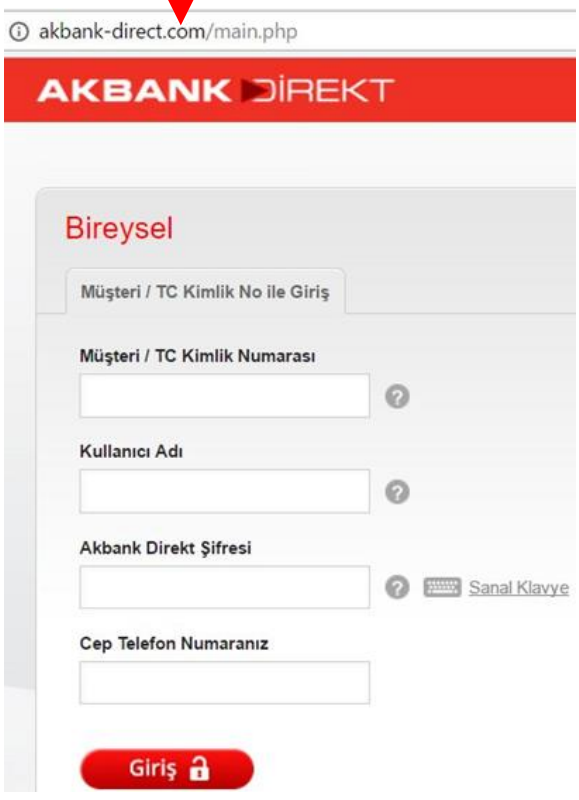
*Sayılar, arama ilgisini belirli bir bölge ve zaman için grafikteki en yüksek noktayla göreli olarak gösterir. 100 değeri, terimin en yüksek popülerliğe sahip olmasıdır. 50 değeri, terimin bunun yarısı kadar popüler olduğu anlamına gelir. 0 değeri ise bu terim için yeterince veri olmadığı anlamına gelir.

***Sahte SMS örneği 1***

Denizbanktan Size Ozel BonusPuan Kampanyasi! Internet Bankaciligina Giris Yapin Aninda 150TL Bonus-Puan Kazanin! KATILIM http://cepdenizbank.com B003

***Sahte SMS örneği 2***

AKBANK MUSTERILERIMIZE OZEL INTERNET BANKACILIGINA GIRIS YAPAN ILK 10.000 KISIYE 500 TL CHIP PARA HEDIYE KATILIM ICIN:https://www.akbank-direkmobil.com/ B372



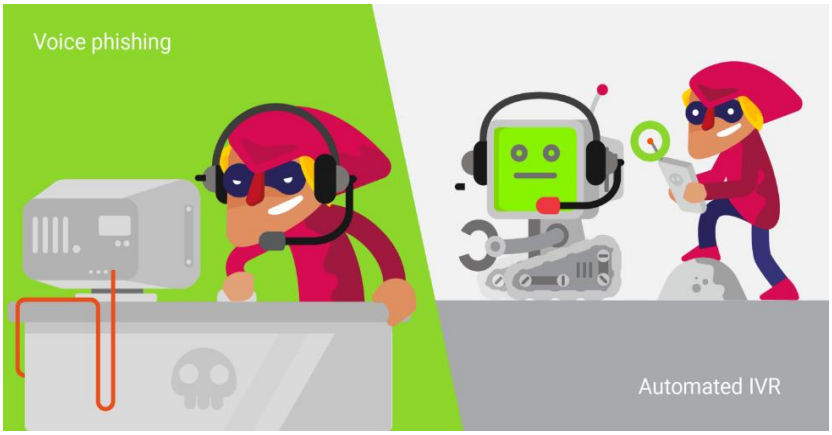

*Her iki örnekte de Türkçe karakter kullanmama, banka isimlerinden sonra gelen ekin tırnak işaretiyle ayrılmamış olması gibi unsurlar bir web servisi üzerinden dolandırıcılık amaçlı SMS gönderilmiş olabileceğine dair ipuçları içeriyor. Ayrıca dolandırıcıların her iki SMS'te de Banka markalarına çok benzer ve dikkatsiz bir anda inandırıcılığı yüksek adreslere yönlendirme yapmış olması dikkat çekici.*

*Örnek 2'de, kurbanın yönlendirildiği sahte sitede hesaplarına erişim için gerekli bilgiler talep ediliyor. Saldırganlar kurbanın internet bankacılığına erişmeye çalıştıklarında, kurbanın cep telefonuna Banka tarafından gönderilecek olası bir güvenlik kodu da, saldırganlarca önceden yapılacak bir telefon aramasıyla sosyal mühendislik yoluyla elde edilmeye çalışılacaktır.*

**Vishing (Telefon dolandırıcılığı): Voice(ses) + fishing** kombinasyonuyla türetilmiş bir kelimedir. Muhtemelen **ülkemizdeki en yaygın phishing temelli dolandırıcılık yöntemi olan bu yöntem**, uzun yıllardır ve kısa vadede önü alınabilecekmiş gibi de gözükmeyen bir şekilde, **dolandırıcıların** genelde sahte kimliklerle çıkarılmış SIM kartları kullanarak kurbanlarını arayıp **kendilerini banka, hakim, savcı, polis, istihbaratçı vb adlarla tanıtıp**, gerçek hayatta olması son derece mümkün ve ulusal basında yer bulmuş, bilinirliği olan güncel konulardan oluşturdukları **sosyal mühendislik senaryolarıyla kurbanlarını aldatmaya çalışmalarına dayanır**. Numara gizlemeden ve yerine geçilen kurumun numarasına benzer bir numaradan veya rastgele bir numaradan aramayla yapılabilmekle birlikte**, genelde VOIP (Voice over internet protocol – internet üzerinden ses iletimi protokolü) kullanılarak yapılan bir aramayla**, bir kurumun numarası sahte olarak hedefin telefonunda görüntülenir (caller ID spoofing). Genelde **acil aksiyon alınması gereken bir konuyla ilgili arama yapıldığı ifade edilir.** Örneğin hedef alınan kişinin müşterisi olduğu bankadaki hesabından yurtdışından para çekildiği, işlem kişinin bilgisi dahilinde değilse acilen X no.lu telefonu araması söylenir. Yahut da ilk aramada kullanıcı adı, şifre (internet bankacılığı erişim için) yahut kredi kart no, güvenlik no, şifre vb kritik bilgiler elde edilmeye çalışılır.Elde edilen bilgilerle dolandırıcı doğrudan internet bankacılığı yahut kredi kartı limitinden işlem yapmayı yahut bu bilgilerle müşteriymiş gibi çeşitli şubelerle iletişime geçerek işlem yaptırmaya çalışabilir.

*Karikatür: Kaynağı belirsiz*

**Gelişmiş, ancak çok büyük kaynaklar gerektirmeden gerçekleştirilebilen bir vishing yönteminde**, önceden kaydedilmiş bir ses kaydıyla arama başlatılır. Kurbanın ekranında caller ID spoofing yöntemi ile kurumun gerçek numarası yahut benzeri görüntülenir ve kişiye gerçek kurumun çağrı merkezinin ses kayıtlarının kaydedilmesi ve düzenlenmesiyle oluşturulmuş yahut bunun üzerinde hafif değişiklikler yapılmış bir ses kaydı dinletilir. Doğrudan bu aramada yahut acil durumda aranması gerektiği belirtilen bir telefona yönlendirme yapılarak bir aşamada kişiden kart/hesap/kimlik no/internet bankacılığı no gibi bilgileri ve bunlara ilişkin erişim şifreleri elde edilmeye çalışılır. Bazen ikna edicilik düzeyini arttırmak amacıyla, kişiden güvenlik nedeniyle şifresini söylememesi ve şifre doğrulama sistemi tarafından işlenmek üzere tuşlaması talimatı verilir. Genelde telefonlar tuş ses tonu açık olarak kullanıldığı ve çağrı merkezleri de bu şekilde çalıştığı için bu standart ses tonları dolandırıcı tarafından basit bir yazılımla tekrar nümerik formata çevrilir ve elde edilen bu bilgilerle sağlanan yetkisiz erişimle dolandırıcılık gerçekleşmiş olur.




*Karikatür: Kaynağı belirsiz / *Automated IVR(interactive voice response) otomatik sesli yanıt sistemi.*

**Teknik araçların çeşitliliği bakımından daha basit ama inandırıcılığı hala çok yüksek olabilen ve muhtemelen ülkemizde en sık yaşanan tipik bir vishing senaryosunda ise**, *arkadan gelen polis/jandarma telsizi sesleri ve polislere aitmiş gibi konuşmların yer aldığı gerçekçi bir fon eşliğinde* **kendisini polis veya jandarma gibi tanıtan dolandırıcı**, kurbanını banka hesaplarının ***terör örgütü tarafından ele geçirildiği, adının terör örgütü soruşturmasında geçtiği, bir hırsızlık vakasında olay yerinde kimlik fotokopisinin bulunduğu*** gibi **yalanlarla korkutarak** sözde kendileriyle birlikte çalışmaya davet etmektedir. Çeşitli argümanlarla neredeyse hipnotize edilen kurban, en sonunda dolandırıcıların verdiği hesap numaralarına para transferi ya da para veya altınlarını kameralardan ve gözlerden uzakta çöp tenekelerine, duvar köşelerine veya dolandırıcılarla bağlantılı üçüncü kişilere bırakma konusunda ikna olmaktadır.

## Film İçinde Film, Oyun İçinde Oyun

**Dolandırıcılar** *o kadar yenilikçi ve gelişmelere uyum sağlamakta da o denli başarılılardır ki*, **dolandırıcılık hakkında basında çıkan haberlerle oluşan farkındalığı bile kendi lehlerine kullanabilecekleri yeni senaryolar geliştirmektedirler**. Bu durumun bir örneği olarak geliştirilmiş senaryolardan birinde; dolandırıcı, dolandırıcı olduğunu bariz olarak belli edecek şekilde ve bilerek sergilediği acemi tavırlarla kurbanı aramaktadır. Aramanın ardından kurban, dolandırılma girişimini farkettiğini düşünerek ve belki tam polise yahut bankasına haber vermeyi değerlendirirken, telefonunun ekranında 155 olarak görüntülenen bir arama görmektedir. Arka plandan gelen polis telsizi sesleri ve ekip konuşmaları eşliğinde *"sizi emniyetten arıyoruz, teknik takibe aldığımız bir dolandırıcılık çetesi az önce telefonla sizi aradı, onları suç üstü yakalayabilmemiz için yardımınıza ihtiyacımız var. Eğer sizi tekrar ararlarsa bizimle görüştüğünüzü söylemeyin ve dediklerini aynen yapın, onları suçüstü olarak yakalayacağız."* cevabı alan kurban bu noktada ikna olduysa, artık her türlü manipülasyona açık bir hale gelmektedir. Sonrasında kendisini arayan kişinin dolandırıcı olduğunu bile bile sözde kanmış gibi yaparken, aslında gerçekten kandırıldığından ve içine düşürüldüğü trajikomik durumdan habersiz, dolandırıcıların talimatlarına uygun olarak istenen para veya altını bir poşete koyarak dolandırıcılarla önceden anlaştıkları noktaya götürerek suçüstü yapılacağı beklentisi içinde bırakmakta veya teslim etmektedir. **Bu derece aldatılmanın verdiği zararın sadece maddi olmayacağı, kurbanı manevi olarak da yıpratacağı konunun göz ardı edilmemesi gereken başka bir boyutudur.**

Basında kendine sıklıkla yer bulan ve artık önemli düzeyde bir farkındalık oluşmuş olması beklenen bu vakalar, maalesef halen yaşanmaya devam etmektedir. **Dolandırıcılara para kaptıranlar arasında** yaşlı ve yalnız olmaları sebebiyle dezavantajlı bir grup oluşturan vatandaşlarımız başta olmak üzere ev kadınlarından, her meslek grubundan ve her kademeden yönetici ve bürokratlara, **her yaştan ve her eğitim seviyesinden insanlar ve hatta kurumlar bulunabilmektedir.**

## Peki, Nasıl Korunulur?

**Bireysel olarak**, ***gerçek olamayacak kadar iyi fırsat/tekliflere*** ve **aciliyet hissi yaratarak**, **paniklemenize neden olabilecek** türden bir ***risk/tehdit içeren arama ve bilgilendirmelere*** **her zaman şüpheyle yaklaşın**. Soğukkanlılığınızı koruyarak iddia edilen konuyu okuduktan yahut bir aramaysa dinledikten sonra **kişisel hiçbir bilginizi vermeden iddiaları bağımsız başka bir kanaldan teyit edin**. Şüphenizi gidermek için kurumun teyit ettiğiniz sitesine ait adresi kullanarak kendiniz giriş yapın yahut kurumun **teyit ettiğiniz iletişim numarasını arayarak size sunulan argümanın doğruluğunu test edin** ve almanız gereken bir aksiyon varsa bu kanallar vasıtasıyla alın. Gerekiyorsa uzman bir tanıdığınıza veya bir hukukçuya danışın.

Bilgisayar ve telefon yazılımlarınızı her zaman güncel tutun.

Antivirüs(virüs önleme yazılımı), firewall(güvenlik duvarı), antimalware (zararlı yazılım önleme yazılımı) vb yazılımlar kullanın ve bunları **sürekli güncel tutun**.

Mümkün mertebe şifrelerinizi birbirinden farklı belirleyin, farklı sitelerde sürekli aynı şifreyi kullanmaktan kaçının ve **şifrelerinizin karmaşıklık bakımından yeterince güçlü olduğundan emin olun**.

SMS veya e-posta ile veya içeriklerinde sağlanan kısa yollarla başka sitelere yönlendirerek, kişisel bilgilerinizi, kart no, hesap no, kullanıcı adı ve şifrenizi girmenizi gerektiren taleplere şüpheyle yaklaşın. Bu kanallardan gelen **uygulama kurulumu vb yönlendirmelere her zaman şüpheyle yaklaşın**. Mesaj ve e-postalarda yazım kuralı, imla, kurum logoları vb detayları dikkate alın. **Kaynağından emin olmadığınız kısayol ve eklere hiçbir zaman tıklamayın. Kısayollara tıklamadan, sadece imlecinizi kısayolun üzerine getirerek kısayolun sizi hangi adrese yönlendirdiğini dikkatle inceleyin**. Aksiyon almanız gereken bir durum olabileceğini sezerseniz veya şüpheye düşerseniz, şüphenizi gidermek için sağlanan kısayolları değil, yine kurumun teyit ettiğiniz sitesine ait adresi kullanarak kendiniz giriş yapın yahut kurumun teyit ettiğiniz iletişim numarasını arayarak size sunulan argümanın doğruluğunu test edin.

Bir yakınınızdan veya iş arkadaşı, yöneticinizden geliyor gibi gözüken **eposta/sms içeriklerinde yer alan talep ve isteklerden olağandışı gözükenlere şüpheyle yaklaşın ve bu kişilerin bilinen telefonlarını aramak suretiyle birebir olarak teyit edin**.


Adres, kredi, kredi kartı, hesap ekstresi, telefon no, **kişisel bilgi**, uçuş bilgisi vb., çalıştığınız banka ve finansal kurumlar; finansal durumunuz; harcama ve kredi geçmişiniz gibi bilgiler dolandırıcılar için çok büyük girdi oluşturmaktadır. O nedenle bu gibi **önemli bilgileri içeren her türlü dökümanı atmanız gerekiyorsa tek parça olarak değil, tercihen bir kağıt öğütücüden geçirmek suretiyle imha ederek atın.**

**Kredi geçmişinizi, kredi kartı ve hesap ekstrelerinizi düzenli olarak kontrol etmeyi alışkanlık haline getirin.** Şüpheli bir hareket gördüğünüzde detaylı olarak inceleyin ve gerekmesi halinde vakit kaybetmeksizin bankanıza ve/veya ilgili mercilere durumu bildirin**.**

**Gelen aramalarda hiçbir zaman kişisel bilgilerinizi paylaşmayın.** Gördüğünüz telefon numarası kuruma ait olsa dahi, sadece size sağlanan bilgiyi dinleyin. Aramayı sonlandırın ve kuruma ait teyit ettiğiniz numarayı kendiniz arayın ve size daha önce sunulmuş olan bilgilerin doğruluğunu bu aramada sorgulayın. **Unutmayın, sizi arayan ve ekranda görünen numara gerçek numarayla birebir aynı olsa bile, caller-id spoofing yöntemiyle yönlendirilmiş bir aramayı yanıtlıyor olma riskiniz her zaman mevcuttur**.

**Kurumsal olarak, şirket dışından gelen e-postaları ayırt edip, phishing saldırılarını otomatik olarak engelleyecek sistemleri devre alma**nın yanında, şirket dışından gelen epostalarla ilgili aşağıdakine benzer bir uyarının görüntülenmesi faydalı olacaktır.

**DİKKAT:** Bu eposta ŞİRKETİMİZ DIŞINDAN bir kaynaktan gelmektedir. Kaynağını tanımadığınız eposta ve eklerini açmayınız, şüpheli epostaları bilgiguvenligi@bizimsirket.com.tr adresine iletiniz.


Zaman zaman **Bilgi Güvenliği ekipleri** tarafından şirket personeline çeşitli senaryolara göre oluşturulmuş **kontrollü phishing epostaları** iletilerek, çalışanların şirket dışından gelen şüpheli mailleri ve eklerini açıp açmadıkları, linklere tıklayıp tıklamadıkları, veri girişi yapıp yapmadıkları takip edilmeli, ilgili **çalışanlara** ve zaman zaman şirket geneline bu konuda **dikkatli olunması yönünde hatırlamalar yapılmalıdır.**

Phishing trendleri takip edilerek, en güncel senaryolar ve korunma yolları hakkında **personele düzenli olarak bilgilendirmede bulunulmalı/eğitim sağlanmalı**, personelin **suistimal farkındalığı her zaman yüksek tutulmalıdır.**

**Şirketlerden müşterilerine (özellikle bankacılık gibi yaygın müşteri ağına sahip olan, emtianın doğrudan paranın kendisi olduğu ve güvenin esas olduğu sektörlerde) yahut kamu kurumlarından vatandaşalara gönderilen e-posta ve SMS iletilerinde hiçbir zaman kişisel bilgi girişi istenmemeli,** şirket/Kamu olarak müşteriler nezdinde **bu türden bilgilerin istenmesinin normal olduğu algısı yaratılmamalı**, aksine zaman zaman **yapılacak hatırlatmalarla şirketin/kamu kurumunun müşterilerinden bu kanallardan hiçbir zaman kişisel veri/erişim bilgilerini istemeyeceği açıkça ifade edilmelidir**.

Aynı şekilde, **müşteri İletişim merkezlerinden yapılan aramalarda hiçbir zaman kişisel bilgi istenmemeli**; müşteri, gerekli bilgi verildikten sonra teyit edebileceği şirket/çağrı merkezi/şube telefon numaralarını aramaya davet edilmelidir. Diğer durumlarda, bu tür bilgilerin şirket tarafından istenmesinin normal olduğu yaygın kanaati oluşturulursa, şirket müşterileri phishing saldırılarına açık hale getirilmiş olacaktır.

**Yasal ve toplumsal olarak, "caller-Id spoofing" yasaklanabilir** veya sadece özel koşullar altında alınan özel izinlere/lisanslara istinaden ve **istismara karşı önlem ve taahhütler alındıktan sonra kullanılabilecek şekilde yasal düzenleme yapılabilir.**

Tehdit ve korku yaratılarak, bilhassa yaşlı ve engelliler gibi fiziksel, bilişsel veya sosyal bir **dezavantajı bulunan bireylerin bu durumları istismar edilerek gerçekleştirilen dolandırıcılık vakaları için daha ağır yaptırımlar içerecek şekilde kanuni düzenlemeler** yapılması caydırıcılık açısından önemlidir. Yaşlı ve engellilere dönük istismar türleri içerisinde en hızlı artış gösterenlerden bir tanesi finansal & ekonomik suistimal vakalarıdır. Örneğin, Amerikan Yetişkinlere Dönük Koruma Hizmetleri Birliği'nin tespitine[8] göre kolluk kuvvetlerine bildirilen

[8] Jackson S.J., Thomas L., *"Financial Abuse of Elderly People vs. Other Forms of Elder Abuse: Assessing Their*

suistimal vakalarında hedef alınan bireyler istatistiksel olarak incelendiğinde, her 20 yaşlı bireyden birinin finansal istismara maruz kaldığı anlaşılmaktadır. Ancak bu bilgi buzdağının sadece görünen yüzünü yansıtmaktadır. Yapılan başka bir araştırmaya[9] göre gerçek durumun bundan çok daha vahim olduğu ve gerçekleşen her 44 finansal suistimal vakasından yalnızca birinin kolluk kuvvetlerine bildirildiği anlaşılmaktadır. Çoğu yaşlı ve engelli birey, yaşadıkları aldatılmanın kafalarını çok karıştırmış olması, utanç duygusu veya duydukları korku nedeniyle, başlarına gelen suistimal vakalarını hiçbir zaman yetkili mercilere bildirmemektedir.

Bu nedenle, **toplumun tüm kesimlerinde suistimal farkındalığının arttırılmasına dönük eğitici ve bilgilendirici faaliyetlerin arttırılması ve desteklenmesi**, suistimalin önlenmesi ve sonrasında oluşan maddi ve manevi zararların sınırlandırılması açısından çok önemlidir.

Suistimal alanında uzmanlaşmış ekiplerin varlığı ve görünürlüğü, kredibilitesi, **CFE[10] sertifikasyonu gibi bu alanda çalışan profesyonellerin yetkinliklerini kanıtlamaya ve sürdürmeye teşvik eden sertifikasyon programları** ve bir platform olarak **alanında uzman meslek erbabını ve ürettikleri bilgileri bir araya getiren sivil toplum örgütlerinin (ACFE, IIA, ISACA, KRYD, TEİD, TİDE, USİUD gibi)[11] de bu farkındalığın sağlanmasında büyük rolü bulunmaktadır.**

**ACFE Türkiye-USİUD olarak, sağlıklı, demokratik bir toplum ve sağlıklı, verimli çalışan bir ekonomik hayat**; **güvenin esas olduğu bir ortamda mümkün olduğuna inanıyoruz.** Toplumda ve ekonomide güven ortamının tesis edilebilmesi için konunun ahlaki, etik boyutunun da dahil edilerek, **suistimalin bireyler ve toplum için oluşturduğu maddi ve manevi külfeti konusunda farkındalık yaratılması, suistimal yapma niyetinde olan kimselerin** bu yola başvurmaları halinde **ciddi bir yakalanma kaygısı, yakalanmaları halinde ise ciddi bir bedel ödeyeceklerine ilişkin bir korku duymaları ve daha baştan bu tür bir eyleme kalkışmaktan çekinmeleri gerekmektedir**. Bireylerin, toplumun ve iktisadi hayatın içinde olan her türlü birimin ise, suistimal ve bundan korunma yolları hakkında farkındalık ve bilgi sahibi olması ve suistimalcilere karşı tespit edici, önleyici ve caydırıcı beceri ve yetkilerle donatılmış profesyonel ekiplerin mücadele verdiğine ve gerekli yasal düzenlemelerin yapıldığına ve uygulandığına inanmaları gerekmektedir. Ancak bu durumda, güven ve istikrar norm, güvensizlik ve suistimal bir istisna olacak; ve ancak böylelikle sosyal ve ekonomik gelişimin önündeki önemli engellerden biri ortadan kaldırılmış olacaktır.

*Dynamics, Risk Factors, and Society's Response",* U.S. Department of Justice, Şubat 2011
Hafemeister,

[9] Holtfreter K., Reisig M.D., Mears D. P., Wolfe S. E., *"Financial Exploitation of the Elderly in a Consumer Context"*, U.S. Department of Justice, Mart 2014.

[10] Certified Fraud Examiner, yani Sertifikalı Suisitmal İnceleme Uzmanı.

[11] Association of Certified Fraud Examiners, The Institute of Internal Auditors, Information Systems Audit and Control Association, Kurumsal Risk Yönetimi Derneği, Türkiye Etik ve İtibar Derneği, Türkiye İç Denetim Enstitüsü, Uluslararası Suistimal İnceleme Uzmanları Derneği

## Teşekkür

Bu makalenin gözden geçirilmesinde ve iyileştirilmesinde sağladıkları desteklerden dolayı değerli dostlarım ve meslektaşlarım Abdülkerim Cura; Alp Buluç, SMMM, CIA, CRMA; C. Cengiz Gümüştüs, CFE, CPP; Fikret Sebilcioğlu, SMMM, CFE, TRACE Rüşvetle Mücadele Uzmanı ve Sabahattin Gündüz'e teşekkürlerimi sunarım. Bununla birlikte makaledeki her türlü hata ve noksandan şahsen sorumlu olduğumu beyan ederim.

## Kaynaklar

APWG, *"Phishing Activity Trends Report:* July-September 2020", Eylül 2020. https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf

Donald J. Rebovich, D.J., Allen K., Platt J., *"The New Face of Identity Theft: An Analysis of Federal Case Data for the Years 2008 through 2013",* Center for Identity Management and Information Protection Utica College, Kasım 2015.
https://www.utica.edu/academic/institutes/cimip/New_Face_of_Identity_Theft.pdf

Holtfreter K., Reisig M.D., Mears D. P., Wolfe S. E., *"Financial Exploitation of the Elderly in a Consumer Context"*, U.S. Department of Justice, Mart 2014.
https://www.ncjrs.gov/pdffiles1/nij/grants/245388.pdf

Jackson S.J., Thomas L., *"Financial Abuse of Elderly People vs. Other Forms of Elder Abuse: Assessing Their Dynamics, Risk Factors, and Society's Response",* U.S. Department of Justice, Şubat 2011.
https://www.ncjrs.gov/pdffiles1/nij/grants/233613.pdf

Lord N., *"What is a Phishing Attack?, Defining and Identifying Different Types of Phishing Attacks",* digitalguardian.com, Eylül 2018.
https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams

Trend Micro Incorporated Research Paper, *"Spear-Phishing Email: Most Favored APT Attack Bait*", 2012.
https://www.trendmicro.com.tr/media/wp/spear-phishing-email-whitepaper-en.pdf

## Okumalar

Proofpoint, *"2020 State Of The Phish Annual Report: An In-Depth Look At User Awareness Vulnerability And Resilience", 2020*

https://guides.codepath.com/websecurity/Social-Engineering

https://www.kaspersky.com/resource-center/definitions

https://us-cert.cisa.gov/report-phishing