**MÜHENDİSLİK FAKÜLTESİ**

# SOSYAL MÜHENDİSLİK

**Mervenur ÇETİN**
**Ebubekir GÜLEN**
**Adem BARIŞ**

**BİLGİSAYAR MÜHENDİSLİĞİ**

**BOLU, 2022**

# SOSYAL MÜHENDİSLİK

**Mervenur ÇETİN**
**Ebubekir GÜLEN**
**Adem BARIŞ**

**Anahtar Kelimeler:** Sosyal Mühendislik, Sosyal Mühendislik Saldırıları, Sosyal Mühendislik Saldırılarına Karşı Alınması Gereken Önlemler

**Özet:** Günümüzde siber saldırılara karşı teknik açıdan bir çok önlem olsa da insan psikolojisini hedef alan saldırganlara karşı alınabilecek önlemler kısıtlı. Bu tarz sosyal mühendislik saldırılarından korunmanın temeli sosyal mühendislik saldırılarını ve yöntemlerini tanımakla başlıyor. Maklemizde bu tarz saldırıları ve yöntemleri anlattık ve nasıl korunulacağı, nasıl fark edileceği hakkında bilgileri paylaştık.

## İÇİNDEKİLER

# 1. Sosyal Mühendislik Nedir?

Sosyal mühendislik birçok alanda kullanılan bir terimdir. Genel anlamıyla kendimiz çıkarları doğrultusunda karşı tarafı yani mağdur kişiyi psikolojik yöntemlerle manipüle ederek ihtiyacımız olan bilgiyi elde etmek veya istediğimiz davranışları sergilemesini sağlamak olarak açıklayabiliriz. Sosyal mühendislik yalnızca bir kişiye yönelik değil toplumlara yönelik de uygulanmaktadır. Siber Güvenlik alanında ise 'teknik alan' ve 'teknik olmayan alan' olarak ikiye ayrılan saldırı türlerinden teknik olmayan saldırı türlerindendir. Sosyal mühendislik savaş literatüründe "silah türü" olarak tanımlanmıştır [1]. Sosyal mühendislik ilk olarak 1894 yılında Hollandalı bir Sanayici olan JC Van Marken tarafından yazılan bir makalede yer almıştır.

# 2. Sosyal Mühendislik Nitelikleri

Mağdurdan istediği bilgileri alabilmek için ikna etme kabiliyetleri gelişmiş olmalı. Karşı tarafın saldırganı ciddiye alması gerekli bu yüzden bilgili ve donanımlı olduğunu karşı tarafa gösterebilmeli. Birçok sosyal mühendislik yöntemleri senaryolar üstünden ilerlediğinden iyi senaryo yazabilmelidirler. Bunların yanı sıra yalan söylemekten, aldatmaktan çekinmezler etik, ahlak kuralları yoktur.

# 3. Sosyal Mühendislerin Hedefinde Olan Kişiler

## 3.1. Direkt Ulaşılabilir Personel

Bir kurumu temsil eden ve müşterilere ilk ulaşıp iletişimi ilk kuran insanlar olduğu için hedefteki insanlardır.

## 3.2. Önemli Personel

Kurumun her alanında bir yetkisi, kurum içinde kıdemli olan personellerdir. Sosyal mühendis yetkili personeli manipüle ederek istediği bilgileri kolaylıkla ele geçirebilir.

## 3.3. Sempati Sahibi Personel

Kurumda çalışanların ve müşterilerin sevdiği, yetkilerini daha iyi hizmet için açabilen insanlardır. Bu tarz bireylerin iyi niyetleri sömürülerek kendi amaçları için kullanırlar.

## 3.4. Destek ihtiyacı Olan Son Kullanıcılar

Kurumsal sistemlere erişim yetkisi olan fakat meşru bir yardıma ihtiyacı olduğunda saldırganı ayırt edemeyen profillerdir.

### 3.5. Aldatılmış, İkna Edilmiş Personel

Kuruma karşı bağlılığı zayıf ve dikkatsiz personellerdir. Sosyal mühendisler, her türlü profile uygun ve insanlara karşı ikna kabiliyeti konusunda uzman insanlardır. Bu durumlarda saldıran karşı tarafı tedirgin etmeden istediklerine ulaşabilir. [2]

## 4. Sosyal Mühendislik Sistemindeki Saldırı Amaçları

- Sistemi Ele Geçirme
- Kritik Bilgilere Erişim
- Hedef Sistemlere Erişim Sağlama
- Yönetici Hakkı Elde Etme
- Sistemde Kalıcı Olma
- Gizlilik

## 5. Sosyal Mühendislik Teknikleri

Bir sosyal mühendis kurbanı yönetmek için onu etkilemeli ve bunu yaparken etik, ahlaki açıdan uygun olmayan yolları da dener ve işinin bir gereği olduğunu düşünür.

### 5.1. Yalan Söyleme

İnsan doğası gereği, eğer yalan söylemiyorsa karşısındakinin de yalan söylediğini düşünmez. Sosyal mühendislerin karşı tarafı manipüle etmesi gerektiğinden yalan söylemekten kaçınmazlar.

### 5.2. Kısmen Gerçeği Söyleme

Bu teknik ise söyledikleri yalanları takip edemeyenler için güzel bir tekniktir. Teknik uygulanırken önce gerçeğin bir kısmı söylenir karşı tarafın güveni kazanılır daha sonra kötü niyetli düşüncelerini gerçekleştirmeye başlarla bir nevi yalan söyleme tekniğini uygulamaya başlarlar.

### 5.3. Gerekçe Sunmak

Bu teknikte sihirli kelimemiz “Çünkü” kelimesidir [3]. Sebep saçma olsa bile hedefteki kişinin kabul etmesi daha olasıdır. Bu konu hakkında bir deney yapılmış. Bu deney fotokopi makinası bulunan bir kütüphanede gerçekleşir. Birçok insan makalelerini kopyalamak için sıraya girmiştir. Bir kişiden sırayı bozması ve öne geçmesi istenir. Birinci grupta sırayı bozmak isteyen kişi “Affedersiniz, beş sayfam var. Fotokopi makinesini kullanabilir miyim çünkü acelem var” der. Bu teklife katılımcıların %94’ü olumlu yanıt verir.

İkinci grupta ise sırayı bozmak isteyen kişi “Affedersiniz. Beş sayfam var. Fotokopi makinesini kullanabilir miyim?” sorusunu yöneltir. Bu grupta ise %60’lık bir kesim olumlu yanıt verir. Son gruba gelindiğinde “Affedersiniz, beş sayfam var. Fotokopi makinesini kullanabilir miyim, çünkü kopya çıkarmam gerekiyor.” gibi anlamsız bir sebep yöneltilerek soruluyor. Buna rağmen gruptakilerin %93’ü onun sıraya girmesine izin veriyor. Bu deneyde anlaşılacağı üzeri insanların sadece çünkü kelimesini duyması bile izin vermelerine yeterli olabiliyor. [4]

### 5.4. Kaçınma ve Sapma

Sosyal Mühendisler tarafında sıklıkla kullanılan tekniklerden biridir. Hedefteki kişi bir soru sorduğunda saldırgan soruyu yanıtlamamak için fark ettirmeden konuyu değiştirir veya alakasız başka şeylerden bahseder. Ayrıca inandırıcı olabilmek ya da hedefte suçluluk hissettirmek için masumiyet, kafa karışıklığı, öfke gibi yüz ifadeleri takınarak içinde bulundukları olayı rahatlıkla atlatabilirler.

### 5.5. Karşılıklı İlişki

Bu teknikte mağdur kişiye cevap vermek zorunda kalacağı bir hediye vermeyi veya bir iyilik yapmayı içerir. Amaç kurban ile arada bir bağ kurmaktır. Daha sonra sosyal mühendis mağdur kişiden dostça olmayan bir ricada bulunur. Mağdur kişi kendini borçlu hissettiğinden sosyal mühendise olumlu yanıt verecektir.

### 5.6. Mizah Kullanımı

Önceden hazırlanmış güzel esprilerle mağdur kişi rahat ve mutlu hissettirilir. Rahat ve mutlu kişinin istenileni yapmasının daha kolay olacağı düşünülmektedir. Bunların dışında ise saldırı mizah içerikli olduğundan saldırı gibi görünmez daha samimi bir görüntü oluşur. Eğer aksi bir durum olur ise saldırgan bu zor durumu esprileriyle komik bir duruma dönüştürebilir.

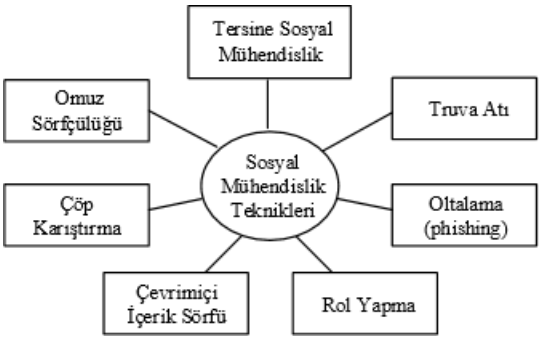
### 5.7. Evet-Evet Tekniği

Bu teknikte, hedefteki kişiye çok fazla ‘evet’ cevabını vereceği soru sorulur bir süre sonra hedefteki kişi pek düşünmeden evet demeye başlar böylece ikna olma süresi azalmış olur. En son evrede saldırgan kendi kabul ettirmek istediği soruyu sorar ve yüksek ihtimalle ‘evet’ yanıtını alır. [5]

### 5.8. Önce Ver Sonra Geri Al Tekniği

Diğer adıyla ‘top atma’ atma tekniği olan bu teknikte mağdura birçok harika teklifte bulunulur. Her yeni teklifte mağdur, saldırganın tekliflerine daha sıcak bakmaya başlar. Mağdurun artık cayamayacağı bir noktaya gelindiğinde saldırgan gerçek isteğini söyleyerek eğer isteğini yerine getirmezse vaatlerini gerçekleştiremeyeceğini söyler. Mağdur kişi bu vaatlerden vazgeçmek istemediğinden saldırganın isteklerini yerine getirir. [5]

## 6. Sosyal Mühendislik Saldırılarında Kullanılan Yöntemler




(Şekil-1)

### 6.1. Tersine Sosyal Mühendislik (RSE)

Saldırgan hedef bir ağ belirler ve bu ağa bir saldırı olduğuna dair e-posta gönderir. Uygun zaman geldiğinde kendini güvenlik danışmanı olarak bu tarz saldırılara karşı mücadele etmek isteyen bir kuruluş olduklarını ve yardımcı olabileceğini açıklar. Bu planlı çalışmadan sonra saldırının hedefi olan şirket veya kişi bağlantıya geçer.


(Şekil 2)

Bağlantıya geçildikten sonra saldırganın hedefi erişimi olmayan veya yetkisi olmayan bilgileri verileri çalmak veya sistem üzerinden istediği yetkileri almaktır.

### 6.2. Omuz Sörfü (Shoulder Surfing)

Elde etmek istediğimiz verileri hedeflenen kişinin özel hayatını izleyerek gerçekleştirmektir. Örneğin klavyelerini izleyerek parolalarını öğrenmek, otobüste, ofiste v.b yerlerde telefonunun pin kodunu girerken izlemek.

### 6.3. Çöp Karıştırma (Dumpster Diving)

Erişmek istediğimiz veriyi veya verileri hedefteki kişinin çöplerini karıştırarak elde etmektir. Genellikle kurumun dışında bulunan çöpler karıştırılır ki bu tamamen yasaldır böylece saldırganın riski yok denecek kadar azdır. Saldırganlar çöplerden ne bulabilir buna bakarsak. Şifreler, faturalar, müşteri listeleri, imla hatasından atılmış raporlar, dosyalar belgeler v.b birçok bilgi çöplerden elde edilebilir. [3]

### 6.4. Rol Yapma (Role Playing)

Ülkemizde çok sık rastlanan bir saldırı yöntemidir. Genellikle telefonla iletişime geçirilerek gerçekleştirilen bir yöntemdir. Saldırgan içinde mağdurunda

bazı bilgilerinin de olduğu bir senaryo yazılır. Bu senaryo mağdurun da bazı bilgilerinin olmasıyla daha ikna edici olur. Saldırgan bu seneryo doğrultusunda kendi istediği hedefe kolayca ulaşabilir.

### 6.5. Oltalama (Phising)

Amaç hedefteki internet kullanıcısını genellikle e-mail yoluyla kandırarak kimlik numarası, kart bilgileri, banka hesap numaraları, parolalar gibi mağdurun özel bilgilerini ele geçirmeyi hedefler.

### 6.6. Truva Atı (Trojen Horse)

Çoğunlukla ücretsiz indirilen yazılımlardan bulaşan programcıklardır.

## 7. Saldırılarda Ortaya Çıkan Zararlar

Bireysel hedeflere yapılan saldırılar genelde para odaklı dolandırıcılıkları kapsıyor. Ancak şirketlere yapılan saldırılarda şirketlerin gizli bilgileri, kurumun itibarına zarar verecek mesleki detaylar elde edilebiliyor.

Sosyal mühendislik saldırıları ile ortaya çıkan zararlara bakıldığında da maddi veya manevi olarak büyük zararlar verilebildiğini görüyoruz. Dünya genelinde siber saldırılara bakıldığında ulusal çaptaki firmalar, kurumlar ve markaların milyon dolarlık zararlar gördüğü aşikardır.

Siber saldırganlar sosyal mühendislik saldırıları ile erişim elde ettikleri zaman;

- Bilginiz başkalarının eline geçebilir,
- Verileriniz çalınabilir,
- Verileriniz kopyalanabilir,
- Fidye isteyebilirler,
- Kişisel verileriniz internet ortamında yayınlanabilir,
- Bağlı olduğunuz kurum veya kuruluşun onuru, toplumdaki imajı zarar görebilir,
- Donanım, yazılım, veri ve kurum çalışanları zarar görebilir,
- Önemli verilere erişim engellenebilir,
- Parasal kayıplar ve vakit kaybı yaşanabilir.

Daha birçok zarar verebilmektedirler. Bu nedenle saldırılardan korunmak için kurum olarak çalışanlara sıklıkla bilinç eğitimi vermek ve sonraki başlıkta değineceğimiz tedbirleri almak önem arz etmektedir.[6]

## 8. Alınması Gereken Önlemler

Alınması gereken önlemleri en basit şekilde 4 başlık altında inceleyebiliriz.

### 8.1. Güvenlik Bilinci Eğitim

Bir şirkette her seviyede çalışanın eğitilmesi gereklidir. E-posta veya telefon yoluyla tuzaklara düşmemek için çalışanlar arasında zaman zaman yapılmalıdır. Bu yöntem sosyal mühendislikten korunmak için ilk adımdır.

### 8.2. Antivirüs Ve Uç Nokta Güvenlik Araçları

Diğer bir temel korunma yöntemi kullanıcı cihazlarına antivirüs gibi uygulamalar yüklenmelidir. Modern uç nokta koruma araçları, bariz kimlik avı mesajlarını, kötü amaçlı web sitelerini veya IP adreslerini tanımlayabilir.

### 8.3. Penetrasyon Testi

Bir nevi sızma testi olarak adlandırabileceğimiz bu yöntemle bir bilgisayar korsanın berilerine sahip olan kişilerin etik yollarla sistemin zayıflıklarını bulmasını sağlar.

### 8.4. SIEM ve UEBA

Sosyal mühendislik saldırılarına yakalandığımız zaman verilerimizi korumanın da yollarını düşünmeliyiz. Hızlı veri toplama, neler olduğunu belirleme ve önlem alabilmeleri için güvenlik personelini bilgilendiren araçlara sahip olunmalıdır. Hassas önlemler için otomatik olay yanıt kılavuzları da kullanılabilir.

SIEM, güvenlik bilgileri ve olay yönetimini ifade eder. Olaylarla ilgili bilgileri merkezi bir sistemde toplar. SIEM aracı, gündelik topladığı tüm bilgiler arasında ilişkiler kurarak tehditleri belirlemeye çalışır. SIEM sisteminin avantajlarından bazıları şunlardır:

-Siber güvenlik olaylarının yönetimini ve müdahalesini iyileştirir.

-Toplanan veriler, gerçek zamanlı olay izlemeleri sayesinde güvenlik savunmalarını geliştirir.

UEBA, kısaca varlıklarını izlemek ve analiz etmek için kullanılan bir sistemdir. UEBA sisteminin avantajlarından bazıları şunlardır:

-Anormal davranışları tespit eder.

-Veri kaybını önlemek için de kullanılır.

-Erişim haklarına uygun kullanımı sağlar.

-Geliştirilen davranış analitiği ile saldırı yüzeyini ve düzeyini azaltır.

Fakat bu başlıkları daha detaylı açacak olursak temel güvenlik önlemlerinden şu şekilde bahsedebiliriz.

## 8.5. Temel Güvenlik Önlemleri

- Çöpe atılacak belgeler okunamayacak şekilde yırtılmalıdır. Bunun için kırpıcılar kullanılabilir.
- Elektronik aletlerde ekran koruyucular şifreli olmalıdır
- Temiz masa / temiz ekran politikası uygulanmalıdır.
- İşten ayrılan çalışanlar için uyulması gereken prosedürler hazırlanmalıdır.
- İşten ayrılan personellerin kullandıkları sistem parolaları pasif hale getirilmelidir.
- Kuruma ziyaretçi olarak gelen kişilerden kimlik alınmalı, gerekirse çalışanlardan biri kişiye refakat etmelidir.
- Kişiye özel bilgiler (şifre, kredi kartı numarası gibi) kimseyle paylaşılmamalıdır.
- Bilgi güvenliği için birden fazla e-posta kullanmanın bazı durumlarda daha etkili olabileceği bilinmelidir.
- Hassas kişisel bilgilerin her yerde, özellikle sosyal medyada paylaşılmamasına özen gösterilmelidir.
- İnternette verilen tüm kişisel bilgilere ve paylaşımlara kişilerin ulaştığını bilerek kontrollü hareket edilmelidir.
- Sosyal mühendisliğe karşı alınabilecek önlemlerden en etkilisi human-firewall (insan güvenlik duvarı), yani kendi yaşamında davranışlarıyla uygulayacağı güvenlik duvarıdır.
- Şifrelerin kâğıtlar üzerine yazılmaması, yazılıysa da görünebilecek yerlerde olmamasına dikkat edilmelidir.
- Şifre girilirken, giriş yapan kişinin fark etmeyeceği şekilde gözetlenmesi anlamına gelen omuz sörfü yapanlara karşı dikkatli olunmalıdır.
- Kurumdaki tüm personele periyodik olarak bilgi güvenliği bilinçlendirme eğitimleri verilmelidir.
- Güncel sosyal mühendislik saldırılarının takip etmek önemlidir. İlgili vakaları farkındalığı artırmak ve yeni çıkan sosyal mühendislik yöntemlerini bilmek için gereklidir.
- Sistemlere en çok zarar verecek kişi ne yaptığını bilmeyen kişidir. Bu nedenle sosyal mühendislik saldırı vakaları içeren, bilgi güvenliği testleri sık sık gerçekleştirilmelidir.
- Telefonda kendisini polis, savcı, asker vb. şeklinde tanıtan bir telefon araması alınması durumunda155 polis hattı aranarak durum bildirilmelidir. Mümkünse sosyal mühendisinin tekrar araması sağlanıp polis ile koordineli şekilde çalışılarak kişinin yargıya teslimi sağlanmalıdır.
- Kişisel bilgileri ele geçiren sosyal mühendislerin habersizce tanımadıkları kişiler adına telefon hatları çıkarması mümkündür telefon kullanımının kontrolünün sağlanması için operatörlere ait sitelerden çevrimiçi kontroller yapılabilir.
- Sosyal mühendislik konusunda farkındalığın artırtılması için sosyal mühendislik içerikli olan Catch me if you can (Sıkıysa Yakala), Who am I (Ben Kimim), Plastic gibi güncel filmler izlenebilir/izletilebilir. [8]

## KAYNAKÇA

[1] Thornburgh T., (2004), “Social engineering: the dark art” ,Proceedings of the 1st Annual Conference on Information Security Curriculum Development, 133– 135, Kennesaw, GA, USA, 4-8 October.
[2] Östlund, David (2007). "Makinelerin değil, insanların bildiği ve arkadaşı: Sosyal mühendislik terminolojisinin iş kariyeri, 1894–1910" . Tarihte Fikirler . 2 (2): 43–82. ISSN 1890-1832 . Erişim tarihi: 2016-09-05 . (tarihle ilgili bilgiler.)

[3] Acilar & Bastug, 2016
[4] Şeydanur A. Gelişmiş sosyal mühendislik saldırıları analizi ve tespiti/ Analysis and detection of advanced social engineering attacks (Yüksek Lisans Tezi, Gebze Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Ana Bilim Dalı, Siber Güvenlik Bilim Dalı)

[5] Ghafir I., Prenosil V., Alhejailan A., Hammoudeh M., (2016), “Social engineering attack strategies and defence approaches”, In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud),145- 149, Vienna, Austria,22-24 August.

[6] Nursel Y. , Ayça A., Sosyal Mühendislik Atakları Ve Alınması Gereken Önlemler Gazi Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Ankara

[7] Hasan B., SOSYAL MÜHENDİSLİK VE DENETİM, Dergipark, Yıl 2009, Cilt , Sayı 1, 42 - 51, 14.07.2016

[8] Aydaner, G. (2019). Genç tüketicilerin sosyal mühendislik ile siber güvenlik farkındalıklarının online alışveriş niyetleri üzerindeki etkisinin ölçülmesi (Master's thesis, Sosyal Bilimler Enstitüsü).

Şekil-1 Sosyal Ağ Ortamlarında Karşılaşılan Tehditlerin Analizi Yücel BÜRHAN, Resul DAŞ, Muhammet BAYKARA

Şekil-2 : Barışkan, M. A. (2017). Türkiye'deki Siber Güvenlik Bilinci ve Sosyal Mühendislik Ataklarına Karşı Savunma Önlemlerinin Geliştirilmesi, İstanbul Üniversitesi Fen Bilimleri Enstitüsü, İstanbul. Bars, A.(2019). Kurumsal Mimari Odaklı Siber Güvenlik (Doctoral dissertation, Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir).