



Social engineering overview

-  Art of convincing people to reveal confidential information
- Exploits peoples
 - **unawareness** about importance of data or social engineering attacks
 - **careless** about protecting data
 - **trust**
 - **fear** of consequences of not providing the information
 - **greed** for promised gain for providing requested information
 - **moral obligation** sense
- Type of [footprinting](#).
-  Well-known social engineering examples
 - **RSA attack**: \$66 million loss based on e-mail with attachment exploiting [zero day](#) Flash vulnerability through an Excel macro.
 - **Ubiquiti networks scam**: \$47 million stolen by impersonation of executives with requests to companies finance department.
 - **US Department of Justice attack**: One employee e-mail was hacked, then hacker pretended to be a new employee and asked for all access codes, ended up with leak of 30.000 FBI and DHS employee data
 - **Yahoo Customer Account Attack**: 3 billion users data was stolen and used for social engineering (e.g. if two people are connected)

Steps of social engineering

1. Research

- Gather enough information about the target company
- Collected by e.g. [dumpster diving](#), scanning, company tour, search on the internet...

2. Select target

- Choose a target employee
- Some employees are more vulnerable than others
 - Easy targets also known as **Rebecca** and **Jessica** mean a person who is an easy target for social engineering such as the receptionist of a company
 - E.g. receptionists, help-desk personnel, tech support, system administrators, clients.
- A frustrated target is more willing to reveal information

3. Relationship

- Earn the target employee's trust e.g. by creating a relationship

4. Exploit

- Extract information from the target employee

Identity theft

- Stealing someone else's personally identifiable information to pose as that person
 - E.g. name, credit card number, social security or driver license numbers

- Can be used to impersonate employees of a target

Steps of stealing an identity

1. Gather targets information
 - Through e.g. bill from social networks, dumpster diving
 - Information include usually first and last name, date of birth, address, social security number, bank accounts, id card and passport numbers.
2. Fake identity proof: get fake IDs
 - Can be driving licence, ID card, etc...
 - E.g. using stolen bills you can claim the person lost driving license and get new one to an address you choose.
3. Fraud: spend money, unauthorized access, use ID for frauds, etc...
 - Can open new credit card accounts on the victim's name
 - Can sell identity information

Identity theft countermeasures

- Check the credit card reports periodically
- Safeguarding personal information at home and in the workplace
- Verifying the legality of sources.

Impersonation on social network sites

Gaining information through social network sites

- Information is used for spear phishing, impersonation, and identity theft.
- Can e.g. create a fake user group "Employees of the company" in **Facebook**
 - Invite people to group and collect credentials such as birth date, employment/education backgrounds.
- Can scan profile pages in **LinkedIn** and **Twitter**.

Steps of social media impersonation

1. Gather personal information from Internet including social network sites
 - E.g. full name, date of birth, email address, residential address.
2. Create an account that is exactly the same
3. Carry out social engineering attacks with the account e.g.:
 - Introduce it to targets friends in a convincing way to reveal information
 - Join the target organization's employee groups where they share personal and company information.

Corporate threats from social network sites

- Social network has vulnerable authentication as it's not isolated like corporate network.
- The employee while communicating on social network may not take care of sensitive information.

Physical security

- **Physical measures**
 - E.g. air quality, power concerns, humidity-control systems
- **Technical measures**
 - E.g. smart cards and biometrics
- **Operational measures**
 - E.g. policies and procedures to enforce a security-minded operation.
- **Access control**
 - **Biometrics**
 - Something you are
 - **False rejection rate (FRR)**
 - When a biometric rejects a valid user
 - **False acceptance rate (FAR)**
 - When a biometric accepts an invalid user
 - **Crossover error rate (CER)**
 - Combination of the FRR and FAR; determines how good a system is
- **Environmental disasters**
 - E.g. hurricanes, tornadoes, floods.
- See also [Physical security](#) | [Information security controls](#)


The Social-Engineer Toolkit (SET)

- [Open-source tool](#) for Linux and macOS
- Available in [Kali Linux](#)
- Templates and cloning for credential harvesting
- Functions such as website attack vectors, mass mailer attack, sms spoofing, QRCode generator, WAP attack...


Social engineering types

Human-based social engineering


Impersonation

- Also known as **masquerading**
-  Pretending to be someone else to learn needed information
- A form of identity theft
- E.g. as
 - target systems end user
 - technical support working with something that requires information to quickly build trust
 - maintenance personal that'll fix vending machine in canteen to install a honeypot
 - an authoritative figure such as FBI agent


Masquerading

-  Pretending to be someone who is authorized and/or requires that access.
- Convincing personnel to grant access to sensitive information or protected systems
- Masquerading is more passive compared to impersonating.



Eavesdropping

-  Secretly listening other peoples communication without consent.
- E.g. by listening a conversation or reading private messages.


Shoulder surfing

-  Observing victims when they're using devices such as ATMs, computers, kiosks...
- Can be done long distance with vision enhancing devices such as binoculars.
- E.g. looking at the keyboard as target types its password in an Internet café.

Dumpster diving


-  Collecting information from the target's trash bins
-  Shredded papers can sometimes indicate sensitive info
- Passive footprinting method
- E.g. bills, financial information, sticky notes, manuals.
- Countermeasure: A safe waste disposal policy

Reverse social engineering


-  Initiated by the victim that's tricked into contacting the attacker herself
- Attacker poses as an authority figure usually by creating a problem then offering a solution.
- E.g.

- befriending an employee
- causing problems (e.g. DoS) at work and offer help.
- often happens with tech support

Piggybacking

-  Convincing an authorized personal to let attacker into a secured area
- Can be physical (e.g. a building) or electronics (e.g. a database)
- Differs from tailgating as it includes consent of the personal.
- E.g. "it's a delivery just hold the door" or "'I forgot my ID badge, please help"

Tailgating


-  Gaining access to restricted areas by following another person
- 💡 Can hold a fake badge when doing it.
- Usually caused by employee's politeness like opening or holding the door
 - 💡 Using a wheelchair usually exploits this human vulnerability
- A countermeasure is using man traps as because they only allow single person at a time.

Vishing


- Use of the telephone to perform the attack (voice and phishing)

Computer-based social engineering


Phishing

-  Attack where the attacker sends a link to a malicious website to collect information
- Malicious website usually fakes a legitimate one with a similar URL.
- E.g. someone calls, asks to fill a form, and says it's a company survey and it'll help company a lot.
- URLs are usually sent through e-mail, but can also be sent through:
 - **Spimming** (SPIM=Spam over Instant Messaging)
 - **Spitting** (SPIT=spam over Internet telephony, VoIP spam)


Whaling

-  A very targeted attack on a high value victim called "Whale" (big fish)
- Usually targets high-level executives

Spear Phishing

-  Using specialized phishing content for a specific person or group of people
- Generate higher response rate as it's more personalized

Pharming

-  Redirect a website's traffic to a malicious one
- Can be done through
 - Exploiting DNS vulnerabilities such as DNS poisoning
 - Host file modification
 - Windows location: `C:\windows\System32\drivers\etc\hosts`
 - Linux location: `/etc/hosts`
 - MacOS X location: `/private/etc/hosts`

Phishing countermeasures

Detecting phishing e-mails

- Sense of urgency or a veiled threat
- From a bank, company, or social networking site
- Generic greeting
- From a person listed in your email address book
- Malicious attachment
- Official-looking logos
- Offers that seem to be too good to believe
- Links to spoofed websites
- Grammatical/spelling mistakes

Anti-phishing tools

- Netcraft: maintains malicious site blacklists against phishing.
- PhishTank: website containing phishing websites

Spam mail

- Sent by attacker with malicious links and attachments
- Can get information such as financial information, social security numbers, and network information.

Baiting

- Installing malware through "need and greed" impulse
- E.g. offering something free if you click a link on a website.

Pop-up window attacks

- To usually create urge to malicious websites or download malware
- E.g. distribute malware links with message "your machine is infected, click here to clean up"

Instant chat messenger

- Gathering personal information by chatting with a selected online
- Can get information such as birth dates and maiden names

Hoax letters

- Emails that issue warnings to the user on new malware that may harm the user's system.

Chain letters

- Emails that instructs user to forward the mail to the said number of persons
- Usually offer free gifts such as money and software

Mobile-based social engineering

Malicious apps

- Created and publish to infect phones and collect data.
- E.g.
 - a replica or similar copy of a popular application
 - ZitMo (ZeuS-in-the-Mobile), a banking malware that was ported to Android

Repackaging legitimate apps

- Repacking legitimate apps with malware and redistributing in third-party app stores.

Fake security apps

- Promises security but provides attacker victims data.
- E.g. apps that "victims" victims securely log on to their bank accounts

SMS phishing

- Also called **SMShishing** or **smishing**
- Sending malicious links through SMS messages and urge their targets to act

Insider attacks

- Authorized person unintentionally or intentionally compromises the security of a system.
- E.g. spying on competitor company through a job opening to extract information from its employees.
- See also [Insider attacks](#) | [Security threats and attacks](#).

Insider types

- **Malicious insiders**
 - Privileged users to inflict harm
 - E.g. dissatisfied or former employees that wants to take revenge
- **Careless and negligent insiders**

- Make errors and disregard policies
- E.g. uneducated employees
- **Infiltrators**
 - External actors
 - E.g. hackers
- **Compromised insiders**
 - Allow external threats to act with same privileges as the insider
 - E.g. Sony breach (2014-15) where attackers took over 100 TBs of data.

Social engineering countermeasures

- **Training**
 - Employee education to increase awareness
- **Separation and rotation of duties**
 - Employees should sign a statement acknowledging that they understand the policies.
- **Least privilege**
 - Giving a user account only those privileges which are essential to perform their intended job function
 - E.g. a user whose sole job function is to creating backups does not need the ability to install software
 - User account will only have rights to run backup and backup-related applications.
- **Monitoring, logging and auditing**
- **Multi-factor authentication**
 - At least for high risk network services e.g. VPNs, cloud services.
- **Strong password policies**
 - Strong authentication
 - Periodic change
 - Complexity requirements
 - Blocks after failed attempts
- **Physical security policies**
 - Access area restrictions
 - Identification of employees by issuing ID cards, uniforms, etc.
- **Access control**
 - For data through e.g. operational guidelines.
- **Proper incidence response time**
 - Proper guidelines for reacting in case of a social engineering attempt.
- **Change-management process**
 - Better documented
- **Anti-virus and anti-phishing defenses**
- **Background check and proper termination process**
 - Insiders with a criminal background and terminated employees are easy targets for procuring information.

