hide هايد
Cyber Security

Social Engineering

& it’s menace.

To know more about services reach us at info@hidecybersecurity.com

www.hidecybersecurity.com

Table of Contents

What is Social Engineering ?

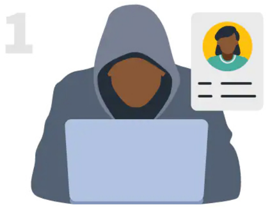
Social Engineering is the art of manipulating people so they give up confidential information. It is a term that describes a non-technical attack that relies on human interaction and tricking people to break normal security procedures. Criminals use social engineering tactics because it is comparatively easier that other attacks. It is one of the most successful attacks, because its victims innately want to trust other people and are naturally helpful.

The victims of social engineering are tricked into releasing information that they do not realize will be used to attack a computer network. Almost all attacks target a Human error.

Social Engineering Explained

"Also known as Human hacking, social engineering is the manipulation of some one to divulge confidential information that can be used for fradulent purposes."

- Norton



The social engineer gathers information about their victims.

The social engineer poses as a legitimate person and builds trust with their victims.

The social engineer gathers information about their victims.

The social engineer poses as a legitimate person and builds trust with their victims.

2

Some common types of social engineering!

2.1 Phishing

It is the most widespread type of attack. It exploits human error by tricking him to a malicious web page in order to obtain the credentials for all of his accounts. False emails, chats, or websites are used to impersonate legitimate websites in order to capture sensitive data. A message from a bank or a well-known institution may arrive requesting that you "verify" your login information. Typically, it will be a mocked-up login page with all of the logos made to look real.

A broad term used to describe cyberattacks with the goal of tricking users into compromising their own data.

The first recorded use of the term "phishing" was in the cracking toolkit AOHell created by Koceilah Rekouche in 1995; however, it is possible that the term was used before this in a print edition of the hacker magazine 2600.

Some common types of social engineering!

2.2 Spear Phishing

It is a phishing scam that targets a specific person or a company's top executive. Spear phishing involves an attacker directly targeting a specific organization or person with tailored phishing communications. This is essentially the creation and sending of emails to a particular person to make the person think the email is legitimate. In contrast to bulk phishing, spear phishing attackers often gather and use personal information about their target to increase their probability of success of the attack.

SPEAR PHISHING EXPLAINED

Spear phishing is a targeted cyberattack toward an individual or organization with the end goal of receiving confidential information for fraudulent purposes.

- Norton

1.

A cybercriminal **identifies a piece of data** they want and **identifies an individual** who has it.

2.

The cybercriminal **researches the individual** and **poses as one of their trusted sources**.

3.

The cybercriminal **convinces their victim to share the data** and uses it to commit a malicious act.

Some common types of social engineering!

2.3 Baiting

A type of social engineering attack where a scammer uses a false promise to mislead a victim into a trick in which personal and financial information is stolen or malware is installed on the device. A malicious attachment with an interesting name could be used as the trap.

Baiting example

For a physical example of baiting, a social engineer might leave a USB stick, loaded with malware, in a public place where targets will see it such as in a cafe or bathroom. In addition, the criminal might label the device in a compelling way — “confidential” or “bonuses.” A target who takes the bait will pick up the device and plug it into a computer to see what’s on it. The malware will then automatically inject itself into the computer.

- Norton

BAITING EXPLAINED

Baiting is similar to phishing. However, baiting promises goods or items to entice victims. Baiters may offer free downloads or software to trick users into clicking on links or inputting login credentials.

How to prevent baiting

Prevent the attack by stopping to ask if the offer is too good to be true; otherwise, you might end up being the "Lucky winner" of a malware infection or virus or end being hacked of your personal information or financial information.

Some common types of social engineering!

2.4 Impersonation

In this type of social-engineering attack, the hacker pretends to be an employee or valid user on the system. A hacker can gain physical access by pretending to be a janitor, employee, or contractor.

Impersonation examples

- Posing as a fellow employee
- An employee of a vendor or partner company, or auditor
- As a new employee requesting help
- Pretending to be from a remote office and asking for email access locally
- As someone in authority
- A system manufacturer offering a system update or patch

Some common types of social engineering!

2.5 Shoulder surfing

shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder. Unauthorized users watch the keystrokes inputted on a device or listen to sensitive information being spoken, which is also known as eavesdropping.

SHOULDER SURFING EXPLAINED

Looking over your shoulder as you enter a password

Shoulder surfing is the name given to the procedure that identity thieves use to find passwords, personal identification number, account numbers, and more

Simply, they look over your shoulder or even watch from a distance using binoculars, in order to get those pieces of information

Some common types of social engineering!

2.6 Vishing

Vishing, a combination of 'voice' and 'phishing,' is a phone scam designed to get you to share personal information. In 2018, phishing crimes cost victims $48 million, according to the FBI's Internet Crime Complaint Center. During a vishing phone call, a scammer uses social engineering to get you to share personal information and financial details, such as account numbers and passwords. The scammer might say your account has been compromised, claim to represent your bank or law enforcement, or offer to help you install the software. Warning: It's probably malware.

VISHING EXPLAINED

The ultimate goal for both phishing and vishing is the same—**to exploit victims in order to profit in some way,** whether financially or otherwise.

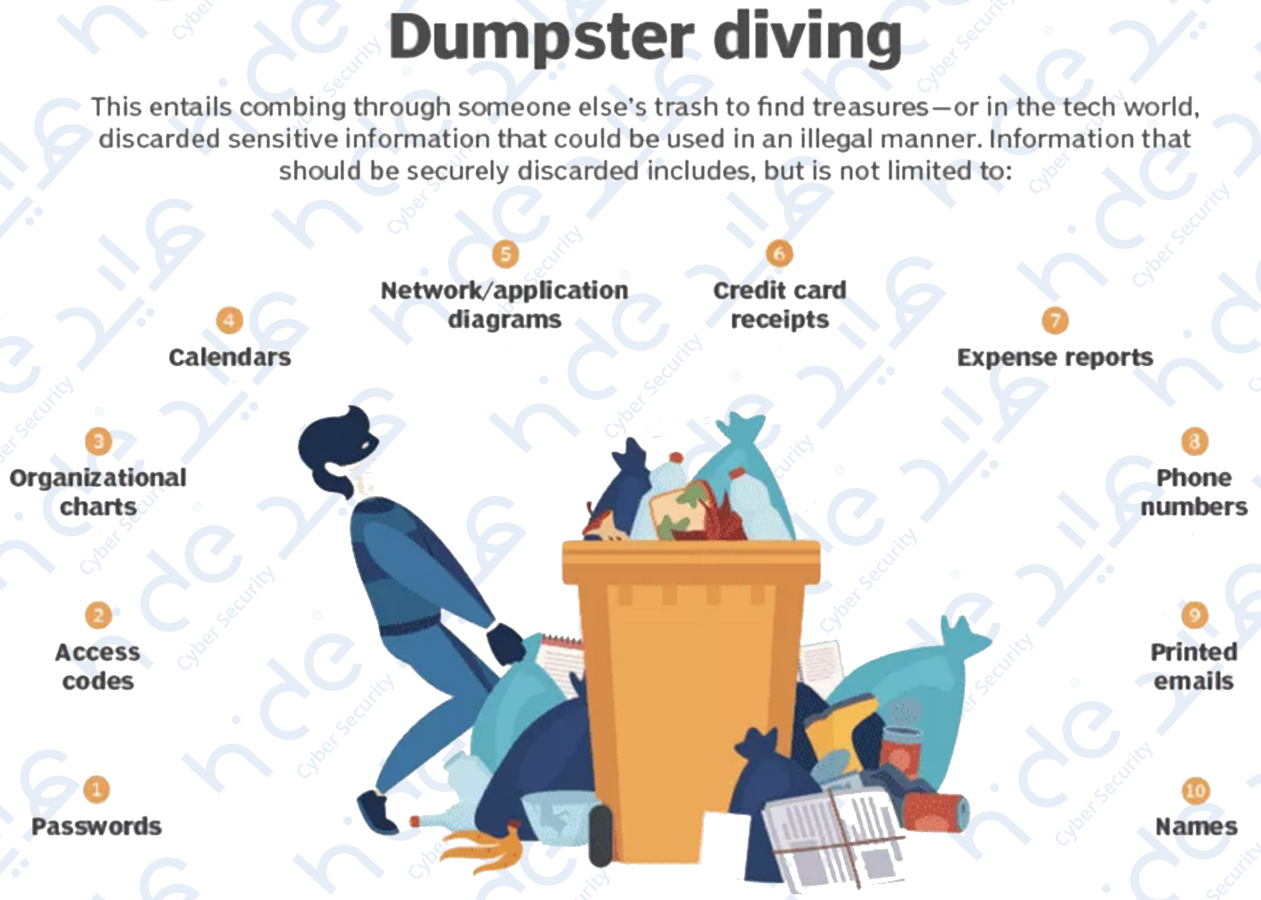
Source: Panda Security

Some common types of social engineering!

2.7 Dumpster diving

Dumpster diving is the exploitation of a person's or company's trash in order to gather information that can be utilised to attack a computer network. Dumpster diving is an interesting attack that produces an immense amount of information on an organization, firm, individual, or entity. You can learn a lot about a person or company from the trash they throw away. It’s also extremely surprising how much personal and private information is thrown out for those to find.

SHOULDER SURFING EXPLAINED



Dumpster diving

This entails combing through someone else’s trash to find treasures—or in the tech world, discarded sensitive information that could be used in an illegal manner. Information that should be securely discarded includes, but is not limited to:

Most famous cases of social engineering!

3.1 Google & Facebook Spear Phishing Scam

$100 Million Google and Facebook Spear Phishing Scam: The biggest social engineering attack of all time (as far as we know) was perpetrated by Lithuanian national, Evaldas Rimasauskas, against two of the world's biggest companies: Google and Facebook. Rimasauskas and his team set up a fake company, pretending to be a computer manufacturer that worked with Google and Facebook. Rimsauskas also set up bank accounts in the company's name.

The scammers then sent phishing emails to specific Google and Facebook employees, invoicing them for goods and services that the manufacturer had genuinely provided — but directing them to deposit money into their fraudulent accounts. Between 2013 and 2015, Rimasauskas and his associates cheated the two tech giants out of over $100 million.

Most famous cases of social engineering!

3.2 Microsoft 365 phishing scam

Microsoft 365 phishing scam steals user credentials: In April 2021, security researchers discovered a Business Email Compromise (BEC) scam that tricks the recipient into installing malicious code on their device. Here's how the attack works, and it's actually pretty clever.

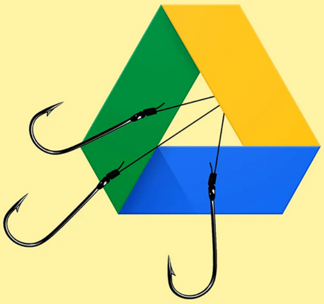
The target receives a blank email with a subject line about a "price revision." The email contains an attachment that looks like an Excel spreadsheet file (.xlsx). However, the "spreadsheet" is actually a .html file in disguise. Upon opening the (disguised) .html file, the target is directed to a website containing malicious code. The code triggers a pop-up notification, telling the user they've been logged out of Microsoft 365, and inviting them to re-enter their login credentials. You can guess what happens next: the fraudulent web form sends the user's credentials off to the cybercriminals running the scam.

Most famous cases of social engineering!

3.3 Google Drive collaboration scam

Google Drive collaboration scam: In late 2020, a novel but simple social engineering scam emerged that exploited Google Drive's notification system. The fraud begins with the creation of a document containing malicious links to a phishing site.

The scammer then tags their target in a comment on the document, asking the person to collaborate. Once tagged, the target receives a legitimate email notification from Google containing the comment's text and a link to the relevant document. If the scam works, the victim will view the document, read the comments, and feel flattered at they're being asked to collaborate. Then, the victim will click one of the malicious links, visit the phishing site, and enter their login credentials or other personal data. This scam is particularly clever because it exploits Google's email notification system for added legitimacy. Such notifications come straight from Google and are unlikely to trigger a spam filter. But like all social engineering attacks, the Google Drive collaboration scam plays on the victim's emotions: in this case, the pride and generosity we might feel when called upon for help.



Most famous cases of social engineering!

3.4 High-Profile Twitters Users' Accounts Compromised After Vishing Scam

High-Profile Twitters Users' Accounts Compromised After Vishing Scam: In July 2020, Twitter lost control of 130 Twitter accounts, including those of some of the world's most famous people — Barack Obama, Joe Biden, and Kanye West.

The hackers downloaded some users' Twitter data, accessed DMs, and made Tweets requesting donations to a Bitcoin wallet. Within minutes — before Twitter could remove the tweets — the perpetrator had earned around $110,000 in Bitcoin across more than 320 transactions.
Twitter has described the incident as a "phone spear phishing" attack (also known as a "vishing" attack). The calls' details remain unclear, but somehow Twitter employees were tricked into revealing account credentials that allowed access to the compromised accounts.

4 Preventions

- Check the source: Don’t open emails and attachments from suspicious sources – If you don’t know the sender in question, you don’t need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider’s site. Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.
- Activate multifactor authentication: One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account’s protection in the event of system compromise.
- Be mindful of tempting offers: If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you’re dealing with a legitimate offer or a trap.

References: https://www.tessian.com/blog/examples-of-social-engineering-attacks/