Social Engineering Report

Full name: Tshimologo Makinta

Task 5: Research Report on Social Engineering Attacks

Date:14 december 2025

The objective of this report is to research and analyze the methods and impacts of social engineering attacks, with a particular focus on Phishing, Business Email compromise (BEC) and baiting. These techniques exploit human psychology rather than technical vulnerabilities, making them dangerous and difficult to detect. This report aims to highlight their mechanisms, examining how each attack operates, real-world consequences, and the reasons they remain effective against individuals and organizations.

Social Engineering

What is Social Engineering? (human hacking)

It is a manipulation technique that is used to exploit human errors to gain private valuables, information, or access. In a sense social engineering is about the psychology of persuasion, a threat actor will use tactics like impersonation to gain some form of trust from their targets to encourage them to take actions that can potentially harm or damage the company both internally and externally. The interesting part is that it is only the first part or step towards the actual cyberattack which is very much giving psycho vibes.

Among the most common and damaging techniques are Phishing and Business Email Compromise (BEC). Phishing campaigns typically rely on fraudulent emails, websites, or messages that trick victims into disclosing credentials or downloading malicious software. BEC attacks, on the other hand, target organizations by impersonating executives or trusted partners to authorize fraudulent financial transactions

Psychological factors that make Social Engineering effective:

1. Trust – is established through some form of relationship that can be exploited over time.
2. Authority- a threat actor will impersonate an individual with power or status.
3. Urgency – a threat actor persuades others to respond quickly and without questioning.
4. Familiarity – a threat actor will establish a fake emotional connection with the targets.

Types of Social Engineering

1. Phishing – a threat actor will use persuasion in order for the target to grant them access to their personal information. It is like a personalized attack where the threat actor collects all the information they can find to tailor the attack. For example, if the target loves Rhinos, they might create an ad that will lead to a website about saving Rhinos and asking you to donate, so by filling out the form that will be at the website the target will have willingly gave away their information.
2. Watering Hole attack- it is an attack to websites that are frequently visited by a specific group of users.
3. USB baiting – an attacker will leave a malware USB stick for an employee to find and install, to unknowingly infect a network.
4. Physical Social Engineering – a threat actor impersonates an employee, customer or vendor to obtain unauthorized access to a physical location.
5. Business Email Compromise(BEC) - a malicious email is sent from a threat actor who is impersonating themselves as an authority figure to their targets, in hopes to gain PII/SPII.
6. Pre-texting – an attacker will fabricate a story in order to gain access to PII/SPII.

Phishing

Phishing is a cybersecurity threat that targets users through email, text, or direct messaging. It is also one of the cybercrimes highlighted on the Federal Bureau of Investigation's Common Frauds and Scams page. Threat actors/ hackers

Types of phishing

1. Spear Phishing – A malicious email attack that targets a specific user or group of users in an organization.
2. Whaling – it is a form of spear phishing, but the threat actor targets company executives to gain access to their SPII.
3. Vishing - is the exploitation of electronic voice communication to obtain SPII. The threat actor will call the target using modern caller ID spoofing to convince the target that the call is from a trusted source.
4. Smishing – text messages are used to exploit targets and gain SPII.
5. Angler Phishing – like vishing but the threat actor will use a direct message from social media platforms instead of making a voice call.

Impacts of Phishing

- Loss of corporate funds
- Data loss and theft - identity theft that may lead to exposure to personal information of partners, clients and co-workers.

- Damage to reputation
- Disruption of business operations like files becoming locked and inaccessible.

Signs of Phishing

- Poor grammar or spelling
- Urgent requests for personal or sensitive Information
- Strange URLs
- Suspicious email addresses

How to Prevent Phishing

- Develop unique email conventions
- Avoid posting personal information online
- Deploy secure messaging platforms - block unreliable/suspicious websites and implement software security.
- Conduct regular training – create phishing awareness programs and stimulate attacks to train employees.
- Deploy tiered security solutions – by enforcing principles like of least privilege
- Implement the use of MFA

How to Respond to a Phishing Attack

- Change passwords immediately
- Report attack to IT department
- Create an incident report
- Monitor for unauthorized access and take necessary preventive measures.
- Follow up with feedback

Real world case about phishing

ETH Heist 2025

- On February 21, 2025, Threat actors successfully stole an estimated $1.4–$1.5 billion worth of ETH from the Bybit cryptocurrency exchange.
- Hackers exploited vulnerabilities in the system when it came to their Safe Wallet, which employed a multi-signature approval process, where multiple transactions need approval.
- Psychological factors used to deploy this attack was trust and authority, hackers gained access to PII/SPII by establishing trust through impersonation and sold it to the dark web.
- This is a clear example of spear phishing

- This attack had a great impact on the organization regarding data theft, financial loss and damage to reputation.

Business Email Compromise (BEC)

It is an email-based social engineering attack that impersonates (exploiting human trust) authority figures in an organization to gain PII/SPII or valuable data of the target/user. It is also an example of spear- phishing. The result of this attack is major financial loss, having organizations recover years and years of funds accumulated. The BEC is a very sophisticated scam that even the Federal Bureau of Investigation (FBI) has issued a warning to businesses about BEC scams, which have resulted in losses of almost $55.5 billion over the past decade.

Types of BEC

1. CEO Fraud – The threat actor will spoof the email account of an executive of the organization and impersonate the executive by sending emails to employees to authorize an action that will be beneficial for the threat actor.
2. Account Compromise – The attacker will break into real email accounts through stolen passwords. They monitor email traffic for weeks then strike when a major payment is due.
3. Attorney/ Legal Impersonation- Threat actors will pretend to be legal officials working on time sensitive matters like legal settlements or acquisitions and use fake legal documentations to convince employees or target into making hasty payments.
4. Invoice Manipulation and Vendor Impersonation – A cyber-criminal will pose a legitimate vendor or supplier that an organization does business regularly.
5. Payroll Diversion – Attacker will impersonate an employee's email account and submit a request to payroll to change their direct deposit information, redirecting future paychecks to an account controlled by the fraudster.

Signs of BEC

- Odd Requests from executives - especially after working hours.
- Unusual Email addresses or domain names
- Last minute changes to payments instructions
- Use of Unofficial Accounts or Free Software
- Suspicious Tone or Urgency

How to prevent BEC

- Report odd requests and pay attention to detail
- Implement multi-factor authentication processes (MFA)
- Stay well informed about latest threats on BEC
- Do regular security audits and training
- Perform frequent software updates and threat monitoring

How to respond to BEC

- Contain the damage- freeze the transaction and alert the bank.
- Alert IT team – to investigate further
- Review and update processes

Real world BEC cases/examples

A. Toyota 2019

- The leading Japanese car parts manufacturer Toyota Boshoku Corporation European Subsidiary become victim to a BEC attack, and the company lost approximately ¥4 billion, that occurred on the 14th of August 2019.
- The third-party hackers posed as business partners of Toyota subsidiary and sent emails to members of the finance and accounting department, requesting funds to be sent for payment into a specific bank account controlled by the hackers.
- After the attack ca me to their awareness, Toyota initiated an internal investigation and reported the incident to local authorities.
- This attack had a great impact on the organization regarding data theft, financial loss and damage to reputation.

B. Orion S.A

- Orion S.A a chemical manufacturing company lost $60 million in a BEC scam on the 10th August 2024.
- It is reported that the company employee who was not an executive was a targeted victim, who was manipulated into transferring funds to accounts controlled by the scammers.

I conclude that Social engineering will continue to evolve, adapt to new technologies and communication platforms while exploiting the same fundamental human vulnerabilities. Phishing and Business Email Compromise exemplifies the devastating impacts of these attacks, from stolen data to financial losses. Technical safeguards alone cannot fully protect against such threats so organizations need to reduce the likelihood of falling victim

to manipulation by understanding the mechanics of social engineering and recognizing the warning signs of phishing and BEC or any other form of cyber-attack early on.

Reference

- https://www.cisco.com/site/us/en/learn/topics/security/what-is-social-engineering.html
- What is Social Engineering? | IBM
- What is Phishing? Types, Risks, and Protection Strategies
- What Is Phishing? Examples and Phishing Quiz - Cisco
- eCommerce Fraud: The Ultimate Merchant's Guide for 2025