Introduction

Social engineering is a complex phenomenon that requires interdisciplinary research combining technology, psychology, and linguistics. Attackers treat human personality traits as vulnerabilities and use the language as their weapon to deceive, persuade and finally manipulate the victims as they wish. Social Engineering is also recognized as the second reason for security breaches at 35%, right behind traditional hacking methods. Furthermore, today, it is a very common practice in workspaces to enable employees to use their own computers or other electronic mobile devices under 'bring your own device' (BYOD) policies. This increase in working at home magnifies the SE problem due to insufficiently protected personal computers. A social engineer's successful attack on an employee could results also in compromise of entire employer' s information system. Trying to uncover the social engineer's behaviour, cyber security researchers noticed that this category of attacks needed an interdisciplinary approach that would help understand the inner workings of the attack, and the methods of social engineers in combination with the psychological characteristics of the human being manipulated. SE attacks are here to stay and threaten all users in enterprises, government agencies and every single individual.

In a typical social engineering attack, the attacker acts in a predator- mined manner, where she initially gathers information using every possible technique or tool, then approaches the potential victim and develops a trust relationship. Next, she exploits this trust relationship to manipulate the victim to perform an action that would enable her to violate the respective information system. In order for the attacker to develop a trust relationship, she relies on specific human (victim) personality traits treating them as vulnerabilities and adapting her tactics accordingly. Her aim is to influence the victim's way of thinking, and to persuade him to behave in a mistaken way. The act of deception is underlying throughout the attacker's effort.

Psychology

In psychology, human personality "refers to individual differences in characteristic patterns of thinking, feeling and behaving" and, although there is no universal acceptance, the Big-5 Theory analyses a five-factor model (FFM) of the personality traits, or otherwise called factors to classify personalities. These factors are believed to capture most of the individual differences in terms of personality. The five factors, usually measured between 0 and 1, are:

- **conscientiousness**: "The degree to which individuals are hardworking, organized, dependable, reliable, and persevering versus lazy, unorganized, and unreliable."
- **extraversion**: "The extent to which individuals are gregarious, assertive, and sociable versus reserved, timid, and quiet."
- **agreeableness**: "The degree to which individuals are cooperative, warm, and agreeable versus cold, disagreeable, rude, and antagonistic."

- **openness**: "the extent to which an individual has richness in fantasy life, aesthetic sensitivity, awareness of inner feelings, need for variety in actions, intellectual curiosity, and liberal values."
- **neuroticism**: "the degree to which one has negative effect, and also disturbed thoughts and behaviours that accompany emotional distress"

high values on conscientiousness, extraversion and openness sometimes increase and sometimes decrease susceptibility to social engineering attacks. High values on agreeableness increase susceptibility and high values on neuroticism decrease susceptibility to social engineering attacks

(Tsinganos et al., 2018)

SE Attack Cycle

• Information Gathering (IG)

• Development of Relationship (RD)

• Exploitation of Relationship (RE)

• Execution to achieve objective (EX)

The attacker gathers information from various public sources at "Information Gathering", develops a trusting relationship with the victim at "Relationship Development", exploits this relationship in order to steal valuable information at stage "Relationship Exploitation" and finally, having all necessary knowledge, attacks the real target in stage "Execution". These four stages correspond to the attacker's steps during a SE attack (Tsinganos et al., 2018)

According to the study of psychology, human being has nature to be helpful when people are in real need, the tendency to trust people, the fear of getting into trouble and tries to escape from it, get something free or without doing much of work. Hacker and crackers tries to attack this technique hence people need to be trained to defend against it (Hasan et al., 2010).

A social engineering attack can be subdivided into at least 3 parts:

Pretext - The act of pretexting is the creation of a scenario to persuade the target to either provide the desired information, or perform the desired action. We define the pretext of the attack as the communication which is used by the attacker to present the pretext to the target. The context of the pretext will define a false identity for the attacker which is trusted by the target to some degree. The pretext may be as simple as a false introduction such as, "Hi, I am Joe from the bank", but it may also include a detailed description of a false situation which would justify the communication attempt from the attacker's false identity. For ex- ample, the pretext might be, "Hi, I am Joe

from the bank and we have detected strange activity on your account. We will need to verify your account information before we can fix the problem". This pretext defines a false, trusted identity, and justifies requests for account information.

Elicitation - is the process of building a rapport with the target in order to make the target comfortable enough to provide the desired information or perform the desired action. The target needs to trust the attacker and elicitation is the act of building that trust through communication. The degree of elicitation required depends on the self-awareness of the target; a naive target may immediately accept the pretext but a more sophisticated target might not. Intelligence field agents are often trained in elicitation, so a significant body of work exists exploring the different techniques available. Common techniques include the following:

- Appealing to Someone's Ego - Subtle flattery can coax person into participating in an inappropriate conversation.
- Expressing a Mutual Interest - People tend to trust a person who seems to share the same interests and values.
- Volunteering "Private" Information - People tend to trust a person who shares information which seems to be private. Sharing private information can also create a sense of obligation in the target, creating that feeling that he should reciprocate by providing his own private information.

Information/Command Goal - The culmination of the social engineering attack is to either request private information or ask the target to perform an inappropriate operation. The goal will vary based on the information desired ("Please confirm your social security number") or the operation desired ("Please click on the link").

(Kim et al., 2018)

higher degrees of normative, affective and continuance commitment, obedience to authority and trust, to be more susceptible to phishing. Furthermore, submissiveness and trust predicted higher susceptibility to phishing emails.

Few of the types of social engineering skills-

1. Impersonating staff: This is an art of inventing scenario to persuade a target to release information or perform an action and is usually done through email or telephone. Most powerful and danger trick for gaining physical access to the system is to pretend to be someone from inside the company. Users gave their password to a "stranger" on a phone call to a member of the IT staff. This is especially true if the caller implies that their account may be disabled and that they might not be able to get important e-mail or access needed network shares if they don't cooperate [3]. It is the most time consuming attack as it requires research to get information regarding target to establish the legitimacy in the mind of target.

2. Playing on users' sympathy the social engineer may pretend to be a worker from outside, perhaps from the phone company or the company's Internet service provider. Nature of people is to help a person who's in trouble.

3. Intimidation tactics social engineers may need to turn to stronger stuff: intimidation. In this case, the social engineer pretends to be someone important -- a big boss from headquarters, a top client of the company, an inspector from the government, or someone else who can strike fear into the heart of regular employees. He or she comes storming in, or calls the victim up, already yelling and angry. They may threaten to fire the employee they don't get the information they want.

(Hasan et al., 2010)

Linguistic Attributes for Analysis

Sentiment Analysis:

Positive Sentiment: Users who frequently exhibit positive sentiment may be more trusting and thus more susceptible to manipulation.

Negative Sentiment: Users displaying negative sentiment might be more cautious but can also be manipulated through fear or stress.

The Use of Security Questions

Social engineering attacks consists of a believable story or pretext that tricks users into divulging sensitive data. A pretext of casual, harmless conversation can gradually lead to extracting sensitive data and one such method the attacker deploys is by trying to acquire personal information indirectly. This data is usually stored as security questions in the event of account recovery. Every individual who has access to services or applications has to pre-define these answers as an initial response to security questions. The purpose of these questions is to re-affirm our identity, or to regain forgotten password.

Examples include-

- In what city were you born?
- What is the name of your favourite pet?
- What is your favourite sport?

Why Are Common Security Questions a Problem?

Common security questions and our responses to them are problematic because they can turn into liabilities if the information is released online—for instance, as a result of a data breach—or if it is made public through social media or other channels. Why? due to the possibility that thousands of websites utilize the same security questions. There is minimal variety between sites, and each user's questions unavoidably and

usually overlap across all of their numerous accounts. There is a significant, needless risk associated with this uniformity of security questions.

Users and security experts should be aware that they should never use the same password for several accounts. This is due to the fact that once an account is hacked, the password is no longer hidden, is connected to your identity and credentials, and may be used in future attacks against any other accounts you may share the same (or a similar username). When passwords are reused on numerous accounts, the compromise of one account has the ability to compromise all other unrelated accounts as well as your identity in the end.

What makes the security questions stronger?

While we do usually have control over the passwords we choose, as individuals, we do not have the power to change the security questions these websites and services require. However, we can answer these questions in creative ways to make our accounts more secure and eliminates the threat of multiple accounts being compromised. Here is some basic guidance on how make security questions stronger:

- Choose different security questions across sites: As much as is possible, do not select the same security questions across multiple sites. Keep your selections unique when the site allows you to pick your own questions. This will help limit the fallout and compromise of other accounts if the security question/answer is ever leaked.

- Use special characters in the answers: Do not answer security questions in plain English (or your native language). That is what is expected, but it's a security misstep. Treat your answers like passwords and introduce complexity in your response and its characters. For example, let's say I was born in Little Rock, Arkansas. The security questions for, "what city where you born in" would require the response, "Little Rock". Now, add some password complexity. The new entry could therefore be, "L!ttl3 r0ck".

- Using fictitious information: In many instances, the best course of action is to provide fictitious information to these questions to keep them unique. You could use a personal password manager to populate the answer fields with password-like responses. Next, store each question and response in your password manager. For example, for an ecommerce site, you could create the entry "ecommercesite.com/question_birthcity" as the account and then enter a random, recommended password as the security response. This provides the secure storage you need in case of a password problem, while keeping your answers to same security question completely random and unique across sites and applications (Haber, 2022).

Predicting user's susceptibility

Key language patterns and psychological factors that indicate susceptibility include:

Positive susceptibility (Higher risk):

These indicate that the user is more likely to be a victim of the social engineering attack. It could be any of the following cues that gets the user to divulge sensitive information without being aware of it.

- **Authority Compliance:** susceptible and excessively complies to higher authoritative figures and language.
  Psychological sources - Milgram's obedience studies, hierarchical social structures
  Phrases like "Sure boss", "Alright sir", or "Understood sir" indicates obedience to authority
  Risk Level: High (3 Points) – By agreeing to the authoritative figure blindly, it can lead to significant security breaches

- **Reciprocity:** attackers exploit users by offering something or doing a small favour, by creating a sense of obligation to reciprocate.
  Psychological sources – norm of reciprocity, social exchange theory
  Statements like "You've been so helpful and nice, of course I can do that for you" or "It's the least I can do to help out" without proper verification
  Risk Level: Medium (2 points) – extracts sensitive information

- **Emotional manipulation:** giving into emotions based on fear, sympathy or excitement driven tactics without critical thinking. User may be prone to showing urgency or distress.
  Psychological basis – emotional decision-making, affect heuristic
  Examples such as "I'll do it right away", "Please don't report me" or "I'll send it right away to prevent any account lockouts"
  Risk Level: High (3 points) – bypasses the users rational decision-making process

- **Uncertainty and hesitation:** User indicate lack of confidence. This is where the user uses filler words, pauses or hedging language.
  Psychological basis – social pressure, cognitive dissonance
  Examples like "I guess, it should be okay", "I am not sure", "I'm not sure if I should, but…" shows a willingness to comply if further pushed by the attacker
  Risk Level: Medium (2 points) – it indicates potential to be persuaded

- **Excessively Agreeable:** extra eagerness to assist or comply indicates a desire to please. User repeatedly offers help and agrees without second thoughts. This does not involve simple “yeah” but a more enthusiastic approach to any request and proceeding without second thoughts.
  Psychological basis – people pleasing behaviour.
  Statements like – “I’d be happy to help”, “I totally agree, and will provide you whatever you need”
  Risk Level: Low (1 point) – leads to over-sharing or unjustified access

- **Impulsively Excited:** it shows that user is quick and emotion driven to requests without proper verification.
  Linguistic cues including exclamations and expressions of enthusiastic nature.
  Psychological basis- reward seeking behaviour
  Statements like- “This sounds amazing, where do I sign up?”, “Can’t resist the temptations to get started”
  Risk Level: Medium (2 points) – could lead to hasty actions and a blind eye to security protocols

- **Unquestioning trust:** easily trusting without verifying the identity of the attacker. Purely trusting the identity based on face-value without verification.
  Linguistic cues include- lack of questioning and blind trust
  Psychological basis- in-group bias, fundamental attribution error
  Examples- “I can trust you with these documents”, “If you are from that department, it’s totally fine”
  Risk Level: Medium (2 points) – straight path to security breach.

Neutral Cues (Requires Context for interpreting)

These cues are used when user tried to further clarify or continue normal conversational norms when interacting without providing any sensitive data.

Seeking Clarifications:
Requesting more information without stating clearly that you accept or reject it.
For instance: "Could you provide more information about what you're looking for?"
Risk Level: None

Acknowledgement:
Recognition of the request without taking any further action.
For example: " I see, that's an interesting request.", “Oh, that’s great”
Risk Level: None

Deferral:

The act of delaying a choice or action until it is obviously accepted or rejected.
For instance: "Let me think about that and get back to you."
Risk Level: None

Conditional Responses:
User gives answers that are hypothetical or non-committal that are referred to as conditional.
For instance: "Typically, we would handle such requests through our official channels."
Risk Level: None

Reflection:
Responses that are paraphrased to further gain time and clarity upon
Example: "So, you're asking for access to the financial records, is that correct?"
Risk Level: None

Negative Susceptibility (Lower Risk):

These indicate the user has strong understanding and resistance to manipulation. The user constantly displays such indicators when the request is breaching security protocol. A strong way to be vigilant against attacks and giving the social engineer nothing to feed upon.

- **Healthy Skepticism:** User displays doubt and requests additional verification.
  Linguistic cues include- expressions of doubt, user persists on asking for evidence.
  Psychological basis- Critical thinking
  Examples- "I'd like to verify and ask you more about this request", "Can you provide some proof of your ID" or "we could discuss more about this in-person"
  Risk Level: Low (-1 points) – reasons with the attacker and indicates a resistance to manipulation.

- **Assertive Refusal**: denying to give personal information by displaying clear and firm rejection to inappropriate requests.
  Linguistic cues include- refusing requests that are suspicious and personal
  Psychological basis- Boundary setting behaviour
  Examples- "Its unauthorized to share", "I'm sorry, I can't provide that"
  Risk Level: Protective (-3 points) – User awareness of security protocols

- **Critical Questioning:** User uses open-ended questions by cross verifying and being risk-conscious.
  Linguistic cues include- requests for more clarification on the request
  Psychological basis- information seeking behaviour, analytical thinking
  Statements like- "why do you need this information".", "For what will this be used?"

Risk Level: Protective (-2 points) – Actively engaged to seek and provide resistance to the breach in security.

- **Escalation:** User identifies the request to be consulted with higher board members before disclosing information.
  Linguistic cues include- References to higher authorities for divulgence of data
  Psychological basis- Distributed decision-making
  Statements like- “Let me consult with my supervisor on this”.”, “I’m going to validate this request with the manager”
  Risk Level: Protective (-2 points) – Understands the necessity of using proper channels

- **Policy Compliance:** References to following the appropriate security protocol established in the company.
  Linguistic cues include- Mentioning the right use of guidelines, policy and procedures.
  Psychological basis- Rule following behaviour and organizational commitment.
  Statements like- “Let me check with our protocols for this”.”, “According to the policy, I need to…”
  Risk Level: Protective (-2 points) – Indicates strong understanding of security culture

User Susceptibility Score -

The calculation of user susceptibility score framework methodology is applied in practical security awareness evaluations and training. This is an explanation of how to use it using text:

1. Assigning weights to each susceptibility indicator
   High impact: 3 points
   Medium impact: 2 points
   Low impact: 1 point
   Protective cue- -2 to -3 points
2. Count the occurrence of each indicator across the conversation
3. Multiply the count and assigned weight for each indicator used in the conversation
4. Sum up all the weighted score to get a raw susceptibility score
5. Use the calculated raw susceptibility score and divide it with maximum possible score.
   If all the positive cues were used which is Total possible points = 15
   Percentage = (Raw score/ Total Possible Points) * 100
6. Final calculation of the susceptibility score:
   - 0%: Great awareness
   - 1-20%: Low susceptibility
   - 21-40%: Below average susceptibility
   - 41-60%: Average susceptibility

- 61-80%: Above average susceptibility
- 81-100%: High susceptibility

- If the points scored is negative, it falls under good security awareness category

This helps to better analyse where the user went wrong and provide the right and considerate recommendation when faced with such an attack.

Real-World Case Studies

(Tessian, 2023) has gathered few case studies on advanced social engineering attacks, and how companies were scammed by falling victims to this pretexting attack

1. **$60 Million CEO Fraud Lands CEO in Court**

Chinese plane parts manufacturer FACC lost nearly $60 million in a so-called “CEO fraud scam” where scammers impersonated high-level executives and tricked employees into transferring funds. After the incident, FACC then spent more money trying to sue its CEO and finance chief, alleging that they had failed to implement adequate internal security controls.

While the case failed, it’s an important reminder: cybersecurity is business-critical and everyone’s responsibility. In fact, Gartner predicts that by 2024, CEOs could be personally liable for breaches.

2. **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.

This type of phishing—which relies on human error combined with weak defences—has thrived during the pandemic. Phishing rates doubled in 2020, according to the latest FBI data.

3. **$75 Million Belgian Bank Whaling Attack**

Perhaps the most successful social engineering attack of all time was conducted against Belgian bank, Crelan. While Crelan discovered its CEO had been “whaled” after conducting a routine internal audit, the perpetrators got away with $75 million and have never been brought to justice.

Crelan fell victim to “whaling” — a type of spear-phishing where the scammers target high-level executives. Cybercriminals frequently try to harpoon these big targets because they have easy access to funds.

Countermeasures of an Ongoing Suspicious Attack

If the user suspects that they are being targeted, (Zimperium, 2023) has provided a guide to ensure the user takes the appropriate action during the incident-

- **Stay calm**. Do not rush, since most social engineers will try to create an artificial sense of urgency. They do this to make sure action is taken quickly without contemplating the decision.
- **Verify the identity** of the person contacting you. The user should contact through a known, verified method. That is if the user is asking something confidential sensitive data
- **Do not provide any personal information** that you have also used as security questions for your account recovery. No password or financial document is to be provided no matter how official the request seems. Asking for an in-person meeting method is preferable.
- **User must trust their instincts**, if something feels off, it’s better to be cautious rather than fall victim to the attack.
- If the user has already shared the sensitive information, the **passwords must be changed immediately** and relevant financial institution must be contacted or company’s IT department to block the request.
- It is **okay for the user to decline** or take time to verify the request. Legitimate organizations understand and respect the boundary and caution exhibited.

PREVENTION

The foremost and most effective defence against social engineering is user education. This must be supported by clearly stated, written policies indicating when users can or cannot disclose their passwords or reveal financial documents. Stringent procedures must be in place. Implementing advanced authentication systems such as smart cards, tokens or better still, biometrics can thwart many social engineering attempts. Even if the social engineer gets a password, it will be of no use without the second authentication factor.

An effective defence against social engineering has strict policies that involve all the employees in an organization. Since this sort of attack has immense power to exploit human unpredictability rather than software vulnerabilities, specific countermeasures can prevent it.

These policies and procedures must be applied; this will only be possible by way of training on current social engineering incidents to ensure it is implemented effectively.

Finally, training employees on real-life pretexting examples, often helps users to familiarize with pretexting tactics and spot unusual requests they receive. A paradox of social engineering: probably the biggest security threat is from people, and yet it is people who might also provide the maximum protection against this attack. This requires that organizations have the motive to defend against social engineering by creating definitions of roles and responsibilities through policies and procedures for all users—not just those in charge of security—to execute their roles correctly (Hasan et al., 2010).

References-

Haber (2022) Security Questions Can Pose a High Risk: Learn Tips & Tricks to Mitigate the Threat [Internet]. Available from: <https://www.beyondtrust.com/blog/entry/reusedsecurity-questions-can-pose-a-high-risk-learn-tips-tricks-to-mitigate-the-threat>.

Hasan, M., Prajapati, N. and Vohara, S. 2010. Case Study On Social Engineering Techniques for Persuasion. International Journal on Applications of Graph Theory In wireless Ad Hoc Networks And sensor Networks. **2**(2), pp.17–23.

Kim, M., Song, C., Kim, H., Park, D., Kwon, Y., Namkung, E., Harris, I.G. and Lootcore, M.C. 2018. Catch me, Yes we can!-Pwning Social Engineers using Natural Language Processing Techniques in Real-Time. Pwning Social Engineers using Natural Language processing Techniques in Real-Time,[online] .

Tessian (2023) 15 Examples of Real Social Engineering Attacks [Internet].

Available from: <https://www.tessian.com/blog/examples-of-social-engineering-attacks/>.

Tsinganos, N., Fouliras, P., Sakellariou, G. and Mavridis, I. 2018. Towards an automated recognition system for chat-based social engineering attacks in enterprise environments In: ACM International Conference Proceeding Series. Association for Computing Machinery.

Zimperium (2023) Social Engineering Attack: A Guide to Protect Your Data [Internet].Available from: <https://www.zimperium.com/glossary/social-engineering-attack/>.