Introduction

A typical social engineering attack involves the attacker acting in a predatory manner, first gathering information with every tool or technique available, then approaching the potential victim and building a rapport of trust (Montañez et al., 2020). They then take advantage of their mutual trust to coerce the victim into doing something that will allow them to breach the relevant information system. The attacker uses particular human (victim) personality qualities to establish trust, viewing them as vulnerabilities and adjusting their strategies accordingly. Their objective is to sway the victim's perspective and convince him to act inappropriately. The foundation of the attacker's operation is deceit.

Psychology

(Cusack and Adedokun, 2018) explains the Big-5 Theory. It examines a five-factor model (FFM) of personality traits, also known as factors to classify personalities, although there is no universal agreement on this definition. In psychology, human personality refers to individual differences in characteristic patterns of thinking, feeling, and behaving. It is thought that these variables account for the majority of personality differences among individuals. Typically assessed on a scale of 0 to 1, the five elements 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 conscientiousness, extraversion, and openness values can occasionally make people more vulnerable to social engineering attempts, and vice versa. High agreeableness scores make one more vulnerable to social engineering attempts, whereas high neuroticism scores make one less vulnerable (Tsinganos et al., 2018).

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

Pretexting a convincing narrative formed by the social engineer to deceive users into disclosing personal information. Security questions present a way for hackers to gain unauthorised access through obtaining personal information indirectly under the guise of a light hearted discussion. As a preliminary response to security questions, any user with access to services or applications must pre-define these answers. These inquiries are used to verify our identity or help us retrieve lost passwords (Haber, 2022)(Rabkin, 2008).

Certain questions that are asked as security questions are –

- What is the name of your first pet?
- What is your grandmother's favourite recipe?
- What was the location you met your spouse?

What makes these Questions Problematic?

Frequently asked security questions and the answers to them are troublesome because they might become liabilities if the information is made public through social media or other channels, or if it is exposed online (for example, as a result of a data breach). Due to several websites leveraging the same procedure, each user's answer is bound to remain same and consistent across numerous accounts (Haber, 2022).

A study by (Nyblom et al., 2020) highlights how in 2017 usernames and passwords were compromised and that accounted to about 7.5 security incidents every month from November 2016 to March 2018, with a total of 250 compromised accounts at Norwegian University of Science and Technology. Social engineering being the primary cause known for these issues. Since these credentials are a part of the users'

identity, these maybe shared on numerous accounts and the compromise of one could lead to unrelated accounts being hacked as well.

How to Make These Answers More Robust?

Although we are generally in charge of selecting our own passwords, we are unable to alter the security questions that these websites and services ask. But by coming up with innovative answers to these questions, we can increase the security of our accounts and remove the possibility of numerous accounts being hacked. The following are few guidelines which could help in strengthening the account from being compromised:

These are also prevention measures

1) Including special characters in the answers – adding extra letters, symbols or numbers increases the complexity of these answers from being easily cracked. Simple English is easy to understand and guess. Answering normal questions like “The name of the city you were born in?” and the answer to that could be something like “F!$$le T0wn”

2) Choose distinctive answers for each site - Try not to use the same security questions on more than one site. If the website lets you choose your own questions, be sure your choices are distinct. In the unlikely event that the security question and answer are compromised, this will lessen the impact and protect additional accounts.

3) Encouraging non-truthful answers: the user must be encouraged to provide answers that are not easily accessible or guessable by providing answers that are not literally true. For instance, using a fictitious answer that they only know could be used in place of an actual answer that is not likely to be found directly through their social network (Rabkin, 2008).

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. According to research by Cialdini and Goldstein, people are more inclined to obey orders from those they perceive to be in positions of authority because compliance is frequently motivated by the need to preserve social ties and prevent unfavourable outcomes (Cialdini and Goldstein, 2004). The combination of authoritative languages and urgent requests pressure users to act quickly without critically evaluating the request.
  Psychological Basis - Milgram's obedience studies, hierarchical social structure
  Statements like “You’re the boss”, “Definitely sir, I’ll get the requested information for you”, or “I understand sir, I’ll provide access to the shared drive right away” 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. Small favours can cause a disproportionate drive to return the favour, according to research by Cialdini and Goldstein (2004), increasing the likelihood that people will comply with subsequent requests. The effect is further amplified if the initial favour asked is personal or unexpected.
  Psychological Basis – 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. According to research, attackers construct their messages to elicit strong emotional reactions, which hinders rational decision-making and increases compliance. For example, phishing emails could invent tales of suffering to arouse compassion or threaten catastrophic consequences such as account suspension, to instil fear and urgency (Siddiqi et al., 2022).
  Psychological Basis – emotional decision-making, affect heuristic
  Statements like - “It seems urgent, 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. According to research by Cialdini and other experts in the fields of persuasion and social influence, people who are uncertain may be more susceptible to advice and direction from others as they look for guidance and comfort. Attackers take advantage of this by projecting a sense of confidence and knowledge, which wins the unconfident user's trust and cooperation. It is also known as social proof mention in Robert Cialdini's list in principles of persuasion (Cialdini and Goldstein, 2004)(Zhou and Zhang, 2008).
  Psychological Basis – cognitive dissonance, social pressure
  Statements 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. According to research, individuals with high agreeableness ratings are likely to be more targeted by social engineers due to their cooperative and trustworthy nature and one of the big five personality traits (Cusack and Adedokun, 2018).
  Psychological Basis – people pleasing behaviour.
  Statements like – "I'd be more than happy to help", "I totally agree, and will provide you whatever you need", "No problem, I can take care of that right away"
  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. (Asfour and Murillo, 2023) research indicates that people with high neuroticism—which is typically associated with impulsiveness—are more vulnerable to social engineering attacks because of their emotional and instinctive reactions.
  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. Research by (Parsons et al., 2015) highlights that people who demonstrate high levels of trust tend to fall victims to the attack. They do not use skepticism to any verification process to raise suspicion.
  Psychological Basis - in-group bias, Halo effect
  Statements like- "I can trust you with these documents", "If you are from that department, it's totally fine", "No need to verify, I'm sure its legitimate"
  Risk Level: Medium (2 points) – straight path to security breach.

- **Sensitive information:** attackers try to gain interest and increase a sense of familiarity by asking individuals to share personal information in a casual conversation indirectly seemingly in a harmless conversation. This key information may be used to exploit an account recovery mechanism - a security question set in place. (Rabkin, 2008) talks about these "fall-back authentication" mechanisms and how they may not provide sufficient protection against modern cyber threats. The inclination to lend confidential data is also indicative to fall for a social engineering attack.

  Psychological Basis – self disclosure bias
  Statements include – personal information When the user discloses really crucial information such as financial reports, credentials/codes or an answer to a security question
  Risk Level – Very High (Raw Score * 2) – Directly favours the attacker to succeed in their attack

Neutral Cues (Requires Context for interpreting)

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

- **Seeking Clarifications:**
  Requesting additional details without making it apparent whether you accept or reject them.
  Statements like: "Could you provide more information about what you're looking for?"
  Risk Level: None

- **Acknowledgement:**
  Recognition of the request without taking any further action.
  Statements like: " 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.
  Statements like: "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.
  Statements like: "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
  Statements like: “So, you're asking for access to the financial records, is that correct?"
  Risk Level: None

Negative Susceptibility (Lower Risk):

These are several preventive measures that talk about the right preventive measures when faced with a social engineering attack. Based on the insightful blogposts by Chavez (2024) and Firch (2024) the study concludes on few awareness cues that demonstrate persistence to resist attempts of being victim to a social engineering attack.

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
  Statements like- "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: Protective (-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
  Statements like - "Its unauthorized to share", "I'm sorry, I can't provide that"
  Risk Level: Protective (-1 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 (-1 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 (-1 points) – Understands the necessity of using proper channels

- **Policy Compliance:** References to following the appropriate security protocol established in the company.
  Statements like - 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 (-1 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: -1 point
2. Sum up all the weighted score of the positive cues to get a **vulnerability score**
3. Multiply the frequency/occurrence of each negative susceptibility cue by its assigned weight if the cue appears more than once in the conversation, and reduce it from the **vulnerability score** to get **raw susceptibility score**
4. If any **financial reports, login credentials or any sensitive data** is shared, double the raw susceptibility score to make the percentage higher
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 can be categorised under:
   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 Result 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. Users must be educated about the risks of oversharing personal data. These data can sometimes be used by an attacker to indirectly gain access to their account through fall-back authentication mechanisms. These users must always remember to use non-personal answers to security questions and they must resist attempts that try to extract personal information through casual conversation.

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-

Asfour, M. and Murillo, J.C. 2023. Harnessing Large Language Models to Simulate Realistic Human Responses to Social Engineering Attacks: A Case Study. *International Journal of Cybersecurity Intelligence & Cybercrime*. **6**(2), pp.21–49.

Chavez, P. 2024. Guardians of the Digital Realm: How to Protect Yourself from Social Engineering. *Proofpoint*. [Online]. [Accessed 6 August 2024]. Available from: https://www.proofpoint.com/uk/blog/user-protection/five-ways-prevent-social-engineering-attacks.

Cialdini, R.B. and Goldstein, N.J. 2004. Social influence: Compliance and conformity. *Annual Review of Psychology*. **55**, pp.591–621.

Cusack, B. and Adedokun, K. 2018. THE IMPACT OF PERSONALITY TRAITS ON USER'S SUSCEPTIBILITY TO SOCIAL ENGINEERING ATTACKS *In*: *Proceedings of the 16th Australian Information Security Management Conference, AISMC 2018*. Edith Cowan University, pp.83–89.

Firch, J. 2024. How To Implement Social Engineering Awareness Training. *Purplesec*. [Online]. [Accessed 18 July 2024]. Available from: https://purplesec.us/learn/social-engineering-awareness-training/.

Haber, M.J. 2022. Security Questions Can Pose a High Risk: Learn Tips & Tricks to Mitigate the Threat. *BeyondTrust*. [Online]. [Accessed 13 July 2024]. Available from: https://www.beyondtrust.com/blog/entry/reused-security-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.

Montañez, R., Golob, E. and Xu, S. 2020. Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*. **11**.

Nyblom, P., Wangen, G., Kianpour, M. and Østby, G. 2020. The Root Causes of Compromised Accounts at the University *In*: *International Conference on Information Systems Security and Privacy*. Science and Technology Publications, Lda, pp.540–551.

Parsons, K., Butavicius, M., Pattinson, M., Mccormac, A., Calic, D. and Jerram, C. 2015. Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails? *In*: *Australasian Conference on Information Systems* .

Rabkin, A. 2008. Personal knowledge questions for fallback authentication: Security questions in the era of Facebook *In*: *In Proceedings of the 4th Symposium on Usable Privacy and Security* [Online]., pp.13–23. Available from: http://www.i-forgot-my-password.com/.

Siddiqi, Murtaza Ahmed, Pak, W. and Siddiqi, Moquddam A. 2022. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences (Switzerland)*. **12**(12).

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.

Zhou, L. and Zhang, D. 2008. Following linguistic footprints: Automatic deception detection in online communication. *Communications of the ACM*. **51**(9), pp.119–122.