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 predeter- 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.

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

(17-chatbased attack)

Phishing is a type of social engineering attack that focuses on gaining sensitive information by disguising as a trustworthy entity. Electronic communications, such as email or text message are common platforms for delivering phishing attacks. Phishing has been shown to be an effective attack over the years, deceiving a broad range of people.

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”).

(4- Social engineering using NLP)

Personality

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 analyzes 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 [33]:

- **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 extend 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 behaviors that accompany emotional distress"

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

(17-chatbased attack)

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.

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.

Social engineering tricks	Persuasive message	Risk

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 favorite pet?

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 question 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

Training and increasing users' awareness of such threats is essential for maintaining continuous and safe use of social networking services. Identifying the most vulnerable users in order to target them for these training programs is desirable for increasing the effectiveness of such programs

Key language patterns and psychological factors that indicate susceptibility

Positive susceptibility (Higher risk):

- Authority: susceptible to higher authoritative figures and language
- Reciprocity: agreeing to disclose confidential data indirectly
- Fear: giving into emotional manipulation
- Uncertainty and hesitation: words like “maybe”, “I am not sure” show a willingness to comply
- Over polite: extra politeness indicates a desire to please
- Excitement: not cross verifying with sources
- Unquestioning trust: easily trusting without verifying the identity of the attacker

Negative Susceptibility (Lower Risk):

- Scepticism: being more cautious by asking more proof “I need to know why and need more proof”
- Refusal: denying to give personal information “No”, “I can’t provide that”
- Questioning: cross verifying and being risk-conscious “why do you need this information”

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/reused-security-questions-can-pose-a-high-risk-learn-tips-tricks-to-mitigate-the-threat>.