

## CHALLENGES OF CYBER SECURITY IN MODERN SOCIETY: THE IMPACT OF SOCIAL ENGINEERING

Assoc. Prof. Dr. Ilona Veitaitė  
Institute of Social Sciences and Applied Informatics, Vilnius University, Lithuania

**ABSTRACT:** Social engineering is a significant cybersecurity vulnerability that exploits human psychology to manipulate individuals into exposing confidential information. Unlike other forms of cyberattacks that target technological weaknesses, social engineering attacks leverage psychological aspects such as emotions, trust, and authority. These tactics often involve the use of “weapons of influence,” which include reciprocity, commitment, social proof, authority, liking, and scarcity. Social engineering can manifest in various forms, such as phishing, pretexting, baiting, and reverse social engineering, where attackers manipulate targets into reaching out to them for assistance. In 2024, statistics show that social engineering remains a prevalent threat, accounting for a significant portion of cybersecurity breaches globally. According to recent reports, nearly 70% of businesses have experienced at least one social engineering attack in the past year. High-profile examples of social engineering attacks include phishing emails disguised as official communications, pretexting to gather personal information under false pretenses, and baiting with enticing offers that lead to malware installation. As cyber threats become more sophisticated, the trends in social engineering are expected to evolve, incorporating advanced techniques such as deep-fake technology and artificial intelligence to enhance their effectiveness. Attackers are leveraging these technologies to create more convincing scenarios, making it increasingly challenging for individuals and organizations to differentiate between legitimate and fraudulent communications. To combat these threats, it is crucial to implement comprehensive training programs focusing on the psychological aspects of social engineering, emphasizing the importance of skepticism and verification before divulging sensitive information. Organizations should also consider employing interactive methods such as short videos to illustrate real-world examples of social engineering attacks, enhancing employee awareness and engagement. By fostering a culture of vigilance and continuous learning, individuals and organizations can better protect themselves against the growing threat of social engineering, ensuring a more secure cyber landscape in the years to come.

**KEYWORDS:** *Social Engineering, Phishing, Manipulation, Persuasion, Cybersecurity Attack, Psychological Attack, Weapons of Influence.*

### MAIN DEFINITIONS

Cybersecurity has become a critical concern in today's interconnected world as individuals and organizations face an ever-growing array of digital threats. Among these, phishing and social engineering stand out as particularly pervasive, exploiting human trust and psychological manipulation to gain unauthorized access to sensitive information. As technology evolves, attackers leverage sophisticated techniques, including personalized phishing campaigns and AI-driven tools, making the fight against these threats more complex than ever (Lewallen, 2020).

Phishing is a form of cybercrime in which attackers use deceptive techniques to manipulate individuals into revealing sensitive information such as usernames, passwords, credit card details, or other personal data. This is typically done through fraudulent emails, messages, or websites that appear to come from legitimate sources. The primary goal of phishing is to exploit human trust and gain unauthorized access to systems, financial accounts, or sensitive information. Phishing attacks come in various forms, each tailored to exploit specific vulnerabilities. Email phishing involves sending fraudulent emails to large groups, often containing malicious links or attachments. Spear phishing targets specific individuals or organizations with highly personalized messages to increase credibility. Whaling attacks focus on high-profile targets, such as executives, by crafting convincing messages that exploit their authority or access. Smishing and vishing use text messages and phone calls to deceive victims into revealing

sensitive information. Angler phishing occurs on social media platforms, where social media capabilities are used to persuade people to expose sensitive information or download malware. Data people post on social media to create highly targeted attacks could also be used. Awareness of these attack types is vital for recognizing and avoiding phishing threats in an increasingly digital world (Craig et al., 2014).

The main phishing challenges in modern society can be divided into several fields. Modern phishing attacks often employ advanced tactics like spear phishing, where attacks are tailored to specific individuals or organizations. This makes them more convincing and harder to detect. The pervasive use of email, social media, and instant messaging provides attackers with many platforms to exploit. Phishing messages can reach millions of users quickly. Artificial Intelligence enables the creation of highly personalized phishing content, while deepfakes can mimic voices or images of trusted individuals, making attacks more credible. Phishing attacks are often perpetrated across borders, making it difficult for law enforcement to track and prosecute offenders due to jurisdictional challenges. Attackers continually adapt their methods, using text messages (smishing), phone calls (vishing), and even QR codes to execute phishing campaigns. Phishing can lead to financial losses for individuals and organizations, reputational damage, and a loss of trust in digital communication channels (Schats, 2017).

Efforts to address phishing include public education, implementation of multi-factor authentication, deployment of sophisticated email filters, and global cooperation among cybersecurity organizations and governments. However, as technology evolves, the arms race between attackers and defenders continues, making phishing a persistent challenge (Hadnagy, 2018).

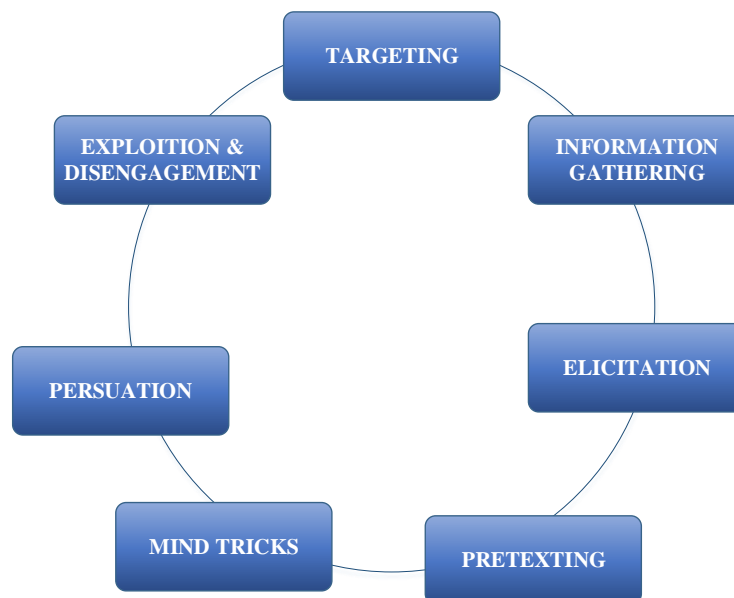
And still, despite advancements in cybersecurity, human error remains a significant vulnerability. Many people are not adequately trained to recognize phishing attempts. People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems. Technical security measures are constantly evolving, but people do not change. They remain the weakest link in information security with their weaknesses, stereotypes, and attitudes. As Albert Einstein said: “Only two things are infinite, the universe and human stupidity, and I’m not sure about the former”. Several facts can confirm this quote: during the past few years, the estimated cost of cyber-attacks on organizations globally was more than four hundred billion dollars; 35 percent of data breaches were attributed to human error or negligence; 47 percent of IT professionals describe collaboration between security risk management and business as poor or nonexistent (Walker, et al. 2020).

## **SOCIAL ENGINEERING**

In very common sense social engineering can be called an act that influences a person to take an action that may or may not be in his or her interests. Social engineering can be defined as the act of manipulating human beings, most often with the use of psychological persuasion, to gain access to systems containing data, documents, and information that the social engineer should not have access to. Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to access buildings, systems, or data. In the more technical sense, social engineering is a cyber-attack focused on tricking the victim into believing the criminal is someone they know and trust. The attacker will then request important information like passwords or fund transfers to their account. These attacks have become highly sophisticated with the advent of social media since these platforms have made it easy for attackers to uncover personal or work-related information. Attackers use this data to convince their victims that they are their friends, family members, or coworkers (Washo, 2021). Also, social engineering is one of the most insidious threats to businesses, particularly to small and medium-sized enterprises (SMEs). Unlike conventional computer attacks, which exploit technical vulnerabilities, social engineering targets human psychology to gain access to confidential information and IT systems, and compromise corporate security. Attackers use a variety of techniques to abuse users’ trust, inducing them to divulge confidential information or perform harmful actions. Social engineering is one of the most widespread and effective methods of accessing confidential information. Statistics show that attacks combining social engineering and phishing are extremely effective, resulting in considerable financial losses for organizations. Here are a few figures illustrating the scale of social engineering:

- Social engineering is behind 98% of all computer attacks.

- Over 70% of data breaches begin with phishing or social engineering attacks.
- In 2021, Google counted more than 2 million phishing sites.
- Some 43% of phishing e-mails impersonate well-known entities, such as Microsoft.
- SMEs with fewer than 100 employees are 3 times more likely to be the target of social engineering.
- 43% of IT professionals targeted by social engineering in previous years.
- A study by the Cyber Security Hub revealed that 3 out of 4 cybersecurity professionals considered social engineering or phishing attacks to be the “most dangerous” threat to their organization’s cybersecurity.
- According to the Information Systems Audit and Control Association, social engineering was the #1 attack vector in 2022.
- According to IBM’s 2022 Cost of a Data Breach report, the average cost of a social engineering attack is 4,55 million dollars.
- The same IBM report says that social engineering attacks can take up to 270 days to be detected and contained on average.
- Social engineering attempts increased by more than 500% in the past few years.



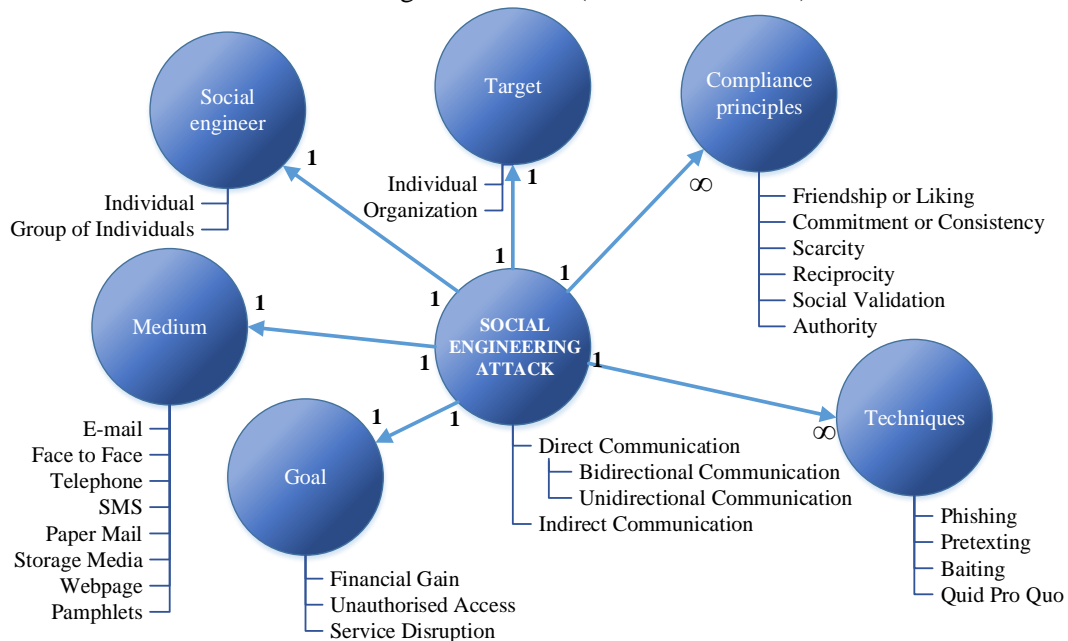
**Fig.1.** Steps of Social Engineering

Social engineering is a psychological manipulation technique attackers use to deceive individuals and gain access to sensitive information or systems. It typically follows a structured series of steps (Schats, 2017):

1. Targeting: The attacker identifies a specific individual, group, or organization to exploit, often selecting those with access to valuable information or systems.
2. Information Gathering: Detailed research is conducted on the target through publicly available sources, such as social media, corporate websites, or online databases, to gather information that can be used to build trust or craft convincing narratives.
3. Elicitation: The attacker engages the target in conversation, often using casual or indirect methods, to draw out additional information without raising suspicion.
4. Pretexting: The attacker creates a fabricated scenario or role to establish credibility and make the target believe they are interacting with a legitimate person or authority.
5. Mind Tricks: Psychological tactics, such as flattery, fear, urgency, or creating a false sense of trust, are employed to lower the target’s defenses and make them more likely to comply.
6. Persuasion: Using the information and rapport built so far, the attacker persuades the target to perform specific actions, such as clicking a link, sharing confidential information, or providing access credentials.

- Exploiting and Disengagement: The attacker uses the gained information or access to achieve their objective, such as stealing data, infiltrating systems, or committing financial fraud. After successfully exploiting the target, the attacker exits the interaction, often attempting to cover their tracks to avoid detection or suspicion.

The ontological model defines a social engineering attack as “employs either direct communication or indirect communication, and has a social engineer, a target, a medium, a goal, one or more compliance principles, and one or more techniques.” The attack can be split into more than one attack phase, each phase handled as a new attack according to the model (Merwe et al. 2017).



**Fig.2.** An Ontological Model of a Social Engineering attack (Merwe et al. 2017).

Direct communication in social engineering is divided into bidirectional and unidirectional communication. Bidirectional communication involves two-way interaction, such as when an attacker sends an email to a target and the target replies. In contrast, unidirectional communication is one-way, like when an attacker sends a letter with no return address, preventing a response from the target. Phishing attacks often use this form of communication. Indirect communication occurs when the attacker does not directly interact with the target but uses a third-party medium, such as leaving an infected flash drive for the target to find and unknowingly activate.

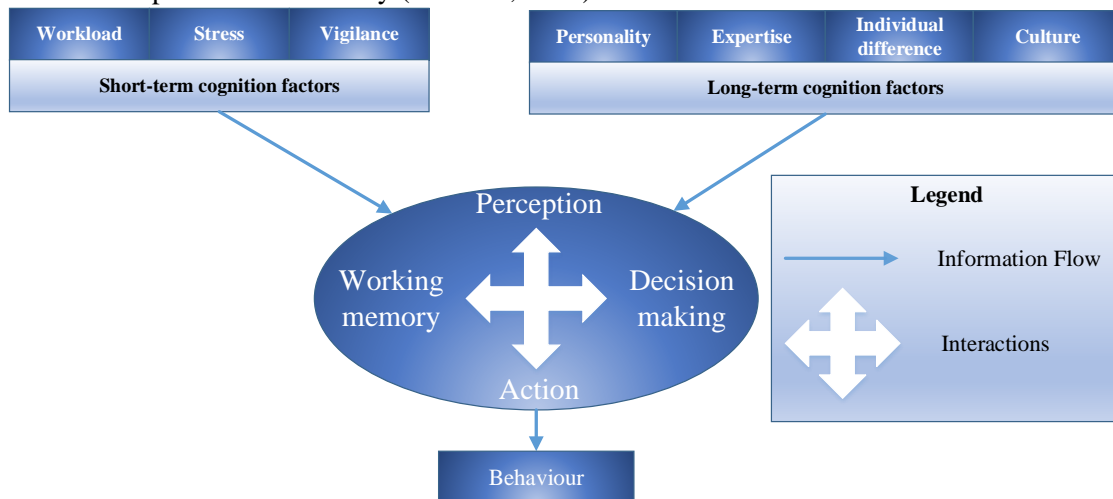
The ontological model of social engineering includes components such as the goal of the attack (e.g., financial gain, unauthorized access, or disruption), the medium (email, phone, face-to-face), the social engineer (individual or group), the target (individual or organization), compliance principles (why the target complies), and techniques (e.g., phishing, pretexting, baiting, and quid pro quo).

The social engineering attack implemented through one or several people can have serious consequences for a person or entire organization: leakage of sensitive data, and social engineering attacks are often aimed at obtaining confidential information. If successful, this can lead to the leakage of sensitive data, such as information on customers, employees, organization finances, or trade secrets; financial loss: attackers can use social engineering to defraud the organization of money, whether through fraud, unauthorized fund transfers or payments to fraudulent suppliers; reputational damage: successful social engineering attacks can seriously damage organization’s reputation. Customers and business partners may lose confidence in the organization if sensitive data is leaked or if it is involved in scams; disruption of operations: some social engineering attacks aim to disrupt organization operations. This can result in service disruption, loss of productivity, and significant costs to restore normal operations; legal liability: organizations can be held liable for breaches of their customers’ privacy or the financial consequences of a successful social engineering attack. This can lead to legal action; infiltration of networks and systems: social engineering attacks can enable attackers to break into corporate networks and systems, which can lead to cyber espionage, intellectual property theft, or

other forms of intrusion; malware propagation: attackers can use social engineering to induce employees to download malware, which can compromise the security of IT systems and data; loss of financial or accounting data: social engineering attacks can target employees responsible for finance or accounting, leading to the loss of crucial financial data or fraudulent manipulation (Bella, 2014).

### PSYCHOLOGICAL ASPECTS OF SOCIAL ENGINEERING

“Some authors advocate treating social engineering cyberattacks as a particular kind of psychological attack.” (Montañez et al. 2020). Social engineering is highly effective because it exploits fundamental aspects of human nature and behavior. People are inherently social, driven by a desire to connect and stand out, often influenced by others’ decisions. The instinct to be helpful and the tendency to trust strangers make individuals particularly susceptible to manipulation. Additionally, in an age of information overload, people often rely on mental shortcuts to save time and gravitate toward quick and effortless solutions, which attackers exploit. Fear of consequences, such as getting into trouble, can pressure targets into compliance. Compounding these factors, many lack sufficient security knowledge and share excessive personal information on social media, providing attackers with valuable tools to tailor their manipulations effectively (McLeod, 2023).



**Fig.3.** Steps of Social Engineering (Montañez et al. 2020)

Human cognitive functions, such as perception, memory, and decision-making, play a significant role in shaping behavior by influencing how individuals process information, respond to environmental changes, etc. In the context of social engineering, attackers exploit cognitive biases, such as the tendency to trust authority or react to urgency, to manipulate targets into making decisions against their best interests. A high cognitive workload, a high stress level, a low level of attentional vigilance, a lack of domain knowledge, and/or a lack of past experience make one more susceptible to social engineering cyberattacks (Montañez et al. 2020).

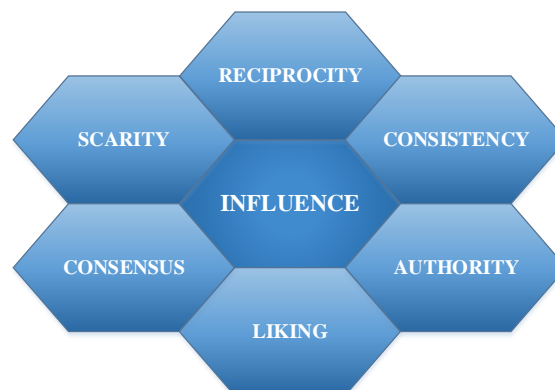
The psychology of online persuasion leverages cognitive biases and emotional triggers to influence individuals' decisions and actions in the digital realm. Various techniques are commonly used to create a sense of urgency, build trust, or induce a feeling of obligation, prompting users to comply with requests or make impulsive purchases. By understanding how people process information and respond to emotional cues, attackers and marketers alike can craft messages that exploit these psychological tendencies for manipulation or persuasion. Emotional manipulation provides attackers with a significant advantage in any interaction, as individuals are more prone to making irrational or risky decisions when experiencing heightened emotions.



*Fig.4. Heightened emotions*

Heightened emotions are powerful tools in social engineering and cyberattacks, as they can cloud judgment and prompt hasty actions (Cialdini, 2007).

- Fear: A phishing email claiming a victim's bank account has been compromised and requiring immediate action can trigger panic, leading the target to click on a malicious link.
- Excitement: An attacker may send a fake message about winning a contest or prize, enticing the victim to share personal information to claim their reward.
- Curiosity: A message stating, "Check out this surprising news about you," can spark the victim's curiosity, encouraging them to click on a link that leads to a harmful site.
- Helpfulness: An attacker may pose as a coworker needing urgent assistance, convincing the target to provide login credentials or download malicious files to "help."
- Guilt: A scammer might impersonate a friend in distress, claiming to need financial help and making the victim feel guilty enough to send money or personal details.
- Urgency: A fake notification claiming that a victim's account will be suspended unless immediate verification is completed can rush the target into giving away sensitive information.
- Sadness: A message claiming a close relative is in an emergency can manipulate the target into making hasty decisions, such as transferring money or disclosing private information.
- Anger: An attacker may send a message impersonating a customer service agent demanding immediate action or threatening to cancel an important service, evoking frustration and prompting rash decisions.
- Greed: A phishing email offering an incredible financial opportunity or a "too good to be true" investment can provoke greed, leading the victim to provide personal details or funds.



*Fig.5. Weapons of Influence*

Weapons of Influence refer to psychological principles used to persuade and manipulate behavior (Cialdini, 2007). Here are short definitions of the main types:

- Reciprocity: The tendency to return a favor or feel obligated to give back when someone does something for you.
- Consistency: The desire to act in ways that align with one's past behaviors, commitments, or beliefs.

- Authority: The influence exerted by individuals perceived as experts or authority figures, leading others to comply with their requests.
- Liking: People are more likely to be influenced by those they like or feel connected to, such as friends or individuals with similar traits.
- Consensus: The tendency to follow the actions of others, believing that if many people do something, it must be the right thing to do.
- Scarcity: The perception that something is more valuable or desirable because it is limited or in short supply.
- Unity: 7th principle of persuasion was later added. The feeling of shared identity or connection makes individuals more likely to trust and act in alignment with others in their group.

Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
Fantasy Aesthetics Feelings Actions Ideas Values	Competence Order Dutifulness Achievement Striving Self-Discipline Deliberation	Warmth Gregariousness Assertiveness Activity Excitement Seeking Positive Emotion	Trust Straightforwardness Altruism Compliance Modesty Tender-mindedness	Anxiety Hostility Depression Self-Consciousness Impulsiveness Vulnerability to Stress

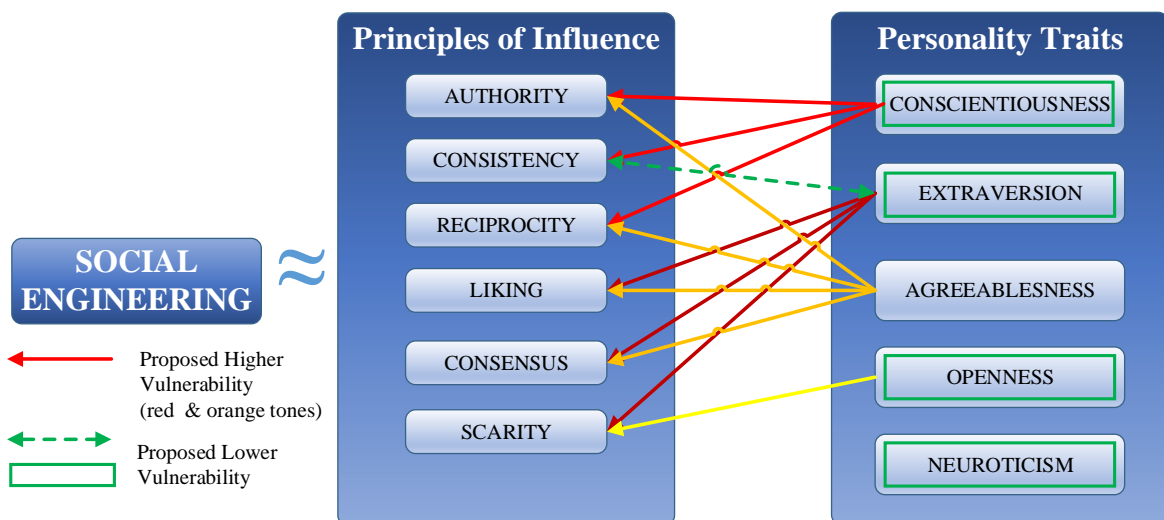


Fig.6. The Social Engineering Personality Framework (Cialdini, 2007).

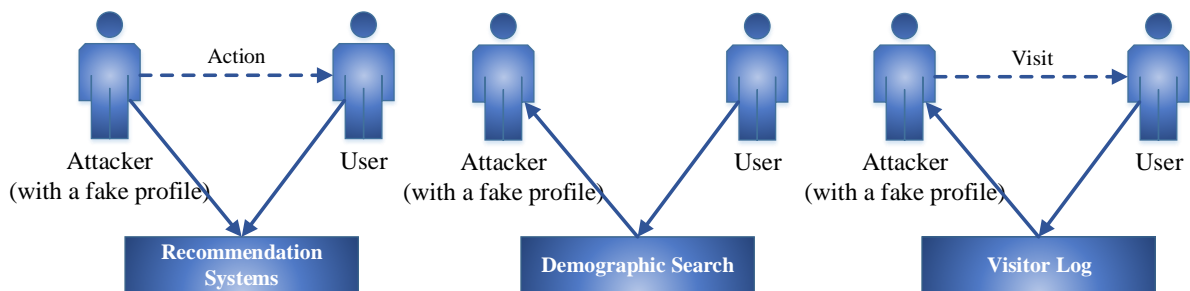
The Social Engineering Personality Framework (SEPF) is a model developed to understand how personality traits influence individuals' susceptibility to social engineering attacks. According to scientific literature, this framework categorizes personality traits that can make a person more vulnerable to manipulation, such as high levels of agreeableness (e.g., a willingness to help others), openness to experience (e.g., curiosity), and neuroticism (e.g., anxiety or fear). People with high conscientiousness may be less susceptible, as they tend to be more cautious and skeptical, while those with low self-esteem are often more easily manipulated by attackers preying on their insecurities. The framework also highlights the role of social traits, such as the need for affiliation or fear of conflict, which can drive individuals to comply with requests even when they might normally be suspicious. By understanding these personality factors, attackers can tailor their approach to exploit specific vulnerabilities in their targets, making the SEPF a valuable tool for both attackers and defenders in recognizing and mitigating social engineering risks.

## REVERSE SOCIAL ENGINEERING

Reverse social engineering is a psychological manipulation tactic where the attacker creates a situation in which the target seeks help or information from the attacker rather than the other way around. This technique often involves the attacker gaining the trust of the target through indirect means and then

waiting for the target to initiate contact. By positioning themselves as the solution to a problem, the attacker exploits the target's desire for assistance or resolution (Irani, 2011).

In reverse social engineering, the attacker does not make the first contact with the victim. Instead, the attack is designed in such a way that the victim reaches out to the attacker for assistance, establishing a relationship based on trust, as it is initiated by the victim. This process typically unfolds in three stages: first, a bait or pretext is created to spark the victim's interest or curiosity (for example, the victim's equipment is sabotaged or damaged). Second, the attacker ensures the target perceives them as an authoritative figure with the necessary skills to fix the issue. Finally, the attacker provides assistance, building trust and gaining access to the victim's information or other resources. Attacks can be classified as targeted or untargeted—in a targeted attack, the attacker focuses on a specific individual, whereas in an untargeted attack, the goal is to reach as many users as possible. They can also be direct or mediated—in a direct attack, the baiting action is visible to the victim, while in a mediated attack, an intermediary collects the bait and then distributes it, often in a different form, to the targeted users.



**Fig.7.** Reverse social engineering attacks examples

Several modern examples of reverse social engineering include recommendation systems, demographic searches, and visitor tracking (Irani, 2011).

- One example of reverse social engineering is through recommendation systems, which are commonly used by online platforms to suggest products, services, or content to users. These systems often rely on data collection and algorithmic predictions based on user behavior, creating a sense of personalized service. However, attackers can exploit these systems to manipulate individuals into making decisions that benefit the attacker. For instance, an attacker could set up a fake website or a malicious product recommendation that subtly persuades the target to click on a malicious link or purchase a fraudulent service, all under the guise of a trusted, personalized recommendation. The user, having been conditioned to trust recommendation systems, may unknowingly follow the suggestion, revealing personal information or falling into a trap.
- Another form of reverse social engineering occurs through demographic search, where attackers gather information based on demographic data to manipulate individuals. Attackers can identify personal details such as age, location, job, or interests by accessing publicly available information on social media profiles or other online sources. Using this information, they can tailor their approach, appearing as though they have a legitimate connection to the target's life. For example, an attacker might contact an individual claiming to be from a local organization offering exclusive deals for people of their demographic, leveraging the target's trust in personalized, relevant offers. Once the target engages, the attacker may then extract sensitive data or lead them into a phishing scam disguised as a legitimate transaction.
- Visitor tracking is another example of reverse social engineering that plays on an individual's online behavior. Websites often track visitors to gather data on their browsing habits, interests, and preferences. Attackers can use this information to create targeted and convincing interactions. For example, by tracking a user's online visits to certain websites, an attacker could craft a message that appears to be from a trusted vendor or service provider related to the user's interests. The message might offer support or solutions to a problem the user has not yet realized they need help with, prompting the target to reach out to the attacker. Once contact is made, the attacker can manipulate the victim into providing personal details, downloading malicious software, or engaging in harmful actions, all while the target feels they are receiving help from a trusted source.

In all of these examples, the core principle of reverse social engineering is the manipulation of trust and the creation of an environment where the victim feels compelled to initiate interaction with the attacker. By understanding and exploiting human behavior, attackers can effectively control the narrative and lead the target into a position where they willingly disclose information or make decisions that benefit the attacker.

## **TIPS TO PREVENT SOCIAL ENGINEERING**

Social engineering attacks pose a heightened risk to organizations in today's world, and this risk is only likely to increase in the future. As attacks become more sophisticated and techniques evolve, organizations must adapt to protect their data, assets, and reputation.

The key to defending against social engineering attacks is a combination of employee education, robust cybersecurity measures, and a proactive security culture. Organizations must continually update their defenses and prepare for evolving threats. The future of social engineering attacks is uncertain, but by staying vigilant and implementing best practices, organizations can better safeguard themselves against this growing menace.

Organizations and individual users need to prioritize education and awareness to prevent social engineering attacks. For organizations, this means regularly training employees on recognizing common social engineering tactics, such as phishing emails, pretexting, and baiting, and fostering a security-first culture. Training should cover identifying suspicious communication, verifying the legitimacy of requests for sensitive information, and understanding the risks of oversharing personal or organization data online. Implementing robust security measures like multi-factor authentication (MFA) and regularly updating software and security protocols can also significantly reduce the risk of successful attacks. Additionally, organizations should have clear incident response plans in place so employees know how to act if they suspect a social engineering attack.

Being vigilant about personal security and avoiding impulsive actions is key for individual users. Users should be cautious when receiving unsolicited emails, phone calls, or messages asking for sensitive information and always verify the source before responding. Password hygiene is crucial—using strong, unique passwords for different accounts and enabling MFA where possible can add an extra layer of defense. Users should also be mindful of their online presence and avoid oversharing personal details on social media, as attackers often use this information for targeted social engineering attempts. Lastly, fostering a healthy skepticism and always questioning the legitimacy of urgent requests or offers can help individuals recognize and avoid falling victim to social engineering attacks.

## **CyberPhish PROJECT**

The international project “Safeguarding against Phishing in the Age of 4th Industrial Revolution” (“CyberPhish”) initiated by Vilnius University Kaunas Faculty and partners started at the beginning of November 2020. The project duration period is 2 years. The objective of the project is to educate students of higher education institutions, educators, university staff (members of the community), education centers, and the business sector (employers and employees) and encourage critical thinking of the target group in the field of cyber security (CyberPhish, n.d.).

The project partners are going to design a curriculum, e-learning materials, a blended learning environment, knowledge and skills self-assessment, and knowledge evaluation system simulations for students and other users in order to prevent phishing attacks, raise competencies, which will help to focus attention to threats and take appropriate prevention measures (CyberPhish, n.d.).

The main intellectual outputs focus on enhancing cybersecurity competencies and addressing phishing threats. These include a study analysis with surveys on “Recognizing Phishing and Skills Gaps” and “Analysis of Existing Cybersecurity Training Programs” across multiple countries (EST, GR, LV, LT). A course curriculum was developed in both short and extended versions for dissemination and training material creation alongside an integrated CyberPhish online course. Additional outputs include online learning materials, gamified educational simulations, and self-evaluation tools, all incorporated into the online learning platform. Methodological guidelines for trainers and implementing “Phishing in the Age

of the 4th Industrial Revolution” were also created to support effective training and course delivery (CyberPhish, n.d.).

#### ACKNOWLEDGMENT

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

#### REFERENCES

- [1] Jonathan Lewallen, “Emerging Technologies and Problem Definition Uncertainty: The Case of Cybersecurity,” *Regulation & Governance* 15, no. 4 (July 14, 2020): 1035–52, <https://doi.org/10.1111/rego.12341>.
- [2] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, “Defining Cybersecurity,” *Technology Innovation Management Review* 4, no. 10 (October 30, 2014): 13–21, <https://doi.org/10.22215/timreview/835>.
- [3] Daniel Schatz, Rabih Bashroush, and Julie Wall, “Towards a More Representative Definition of Cyber Security,” *The Journal of Digital Forensics, Security and Law*, January 1, 2017, <https://doi.org/10.15394/jdfsl.2017.1476>.
- [4] Robert B. Cialdini, *Influence: The Psychology of Persuasion* (Rev. ed.; 1st Collins business essentials ed. New York: Harper Collins, 2007).
- [5] Christopher Hadnagy, *Social Engineering: The Science of Human Hacking* (John Wiley & Sons, 2018).
- [6] Danesh Irani et al., “Reverse Social Engineering Attacks in Online Social Networks,” in *Lecture Notes in Computer Science*, 2011, 55–74, [https://doi.org/10.1007/978-3-642-22424-9\\_4](https://doi.org/10.1007/978-3-642-22424-9_4).
- [7] Saul McLeod PhD, “Techniques of Compliance in Psychology,” *Simply Psychology*, June 14, 2023, <https://www.simplypsychology.org/compliance.html>.
- [8] Johannes Van de Merwe, Francois Mouton. “Mapping the anatomy of social engineering attacks to the systems engineering life cycle”. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2017), pp. 24-40
- [9] Rosana Montañez, Edward Golob, and Shouhuai Xu, “Human Cognition Through the Lens of Social Engineering Cyberattacks,” *Frontiers in Psychology* 11 (September 30, 2020), <https://doi.org/10.3389/fpsyg.2020.01755>.
- [10] Giampaolo Bella and Giampaolo Bella et al., “A Socio-technical Methodology for the Security and Privacy Analysis of Services,” *Workshops* 376 (July 1, 2014): 401–6, <https://doi.org/10.1109/compsacw.2014.69>.
- [11] Emile Walker, Dave Witkowski, Sarah Benczik, Pilar Jarrin. *Cybersecurity –the Human Factor. Prioritizing People Solutions to improve the cyber resiliency of the Federal workforce*. Retrieved from [https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017\\_Witkowski\\_Benczik\\_Jarrin\\_Walker\\_Materials\\_Final.pdf](https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf)
- [12] Amy Hetro Washo, “An Interdisciplinary View of Social Engineering: A Call to Action for Research,” *Computers in Human Behavior Reports* 4 (July 25, 2021): 100126, <https://doi.org/10.1016/j.chbr.2021.100126>.
- [13] “CyberPhish: Safeguarding Against Phishing in the Age of 4th Industrial Revolution,” CyberPhish: Safeguarding Against Phishing in the Age of 4th Industrial Revolution, n.d., <https://cyberphish.eu/>.