

A Proposed Strategy for Establishing Security Training and Awareness Programs for Early Detection of Social Engineering Threats

Atik Laala ^{1*}, Khemgani Badre Zamane ²

¹ University of Ouargla, Finance lab, Market Finance and Corporate Finance, - (Algeria), atik.laala@univ-ouargla.dz

² University of Qouargla, Finance lab, Market Finance and Corporate Finance, - (Algeria), khemgani.badrezzamane@univ-ouargla.dz

Received: 22/05/2025

Accepted: 28/05/2025

Published: 01/06/2025

Abstract:

This study aims to develop security training and awareness programs for early detection of social engineering threats, focusing on the human element—the weakest link in organizational cybersecurity. Using a descriptive method, it analyzed literature and current cybersecurity trends, particularly user behavior. A strategy was proposed involving target identification, behavioral analysis, training implementation, and ongoing evaluation. The study emphasized interactive methods like simulations and serious games, and recommended regular awareness assessments, incident reviews, and content updates to improve training effectiveness and adaptability.

Keywords:

Jel Classification Codes: D83, M15, L86, K24.

* Corresponding author

1. INTRODUCTION

The evolution of information security has witnessed significant changes. These changes resulted from the emergence of the open internet, which led to the emergence of a new security theory, a new basic technology, and new security principles. (Nan, 2021) Information Security is defined as: protecting data from unauthorized access, use, disclosure, disruption, alteration or destruction. (Gadhi & et.al, 2024) The biggest threat to security of information is Social Engineering (Ram & Harris, 2015) and attacks of this nature are considered the most commonly adopted by the attackers.

The nature of social engineered attacks is complex (Hussain & Geoffrey, 2018) where social engineers often use a hybrid approach targeting systems and sometimes people who run these systems (Washo, 2021) All social engineering attempts can be classified into computer -based (technology-based) deception and human deception (Abass, 2018), so some steps can be taken to reduce the risks of social engineering to a manageable level (Almutairi & Alghamdi, 2022). Therefore, defense strategies are considered necessary to protect data or information, information systems and networks from attacks or breaches (Mostofa & et.al, 2022) Research question:

Many Researchers and experts in the field of information security agree that the user is the weakest link in the information security chain in any system. (Ildikó, 2020) To stay ahead of the advanced social engineering techniques, Organizations should implement continuous educational programs for employees around latest threats and defense mechanisms including in that the mastery of the computer and internet tools (Chapagain & et.al, 2024) where organizations invest increasingly in security awareness programs and trainings, which aim to Educate employees about risks of social engineering attacks risks and how to identify and counter them (Konstantinos & Kritikos, 2024.) Information security awareness programs aimed at fostering a security-conscious environment by eliminating human behavior-related vulnerabilities is crucial for securing the organization's assets. (Jemal, 2014), based on the above, we present the following research question:

What are the procedures and methods required to design and implement training and awareness programs for the early detection of social engineering threats targeting the human element?

Management must be aware that employees can play a role in protecting the organization's assets when it comes to social engineering attacks. Therefore, user awareness programs and employee training should be established.

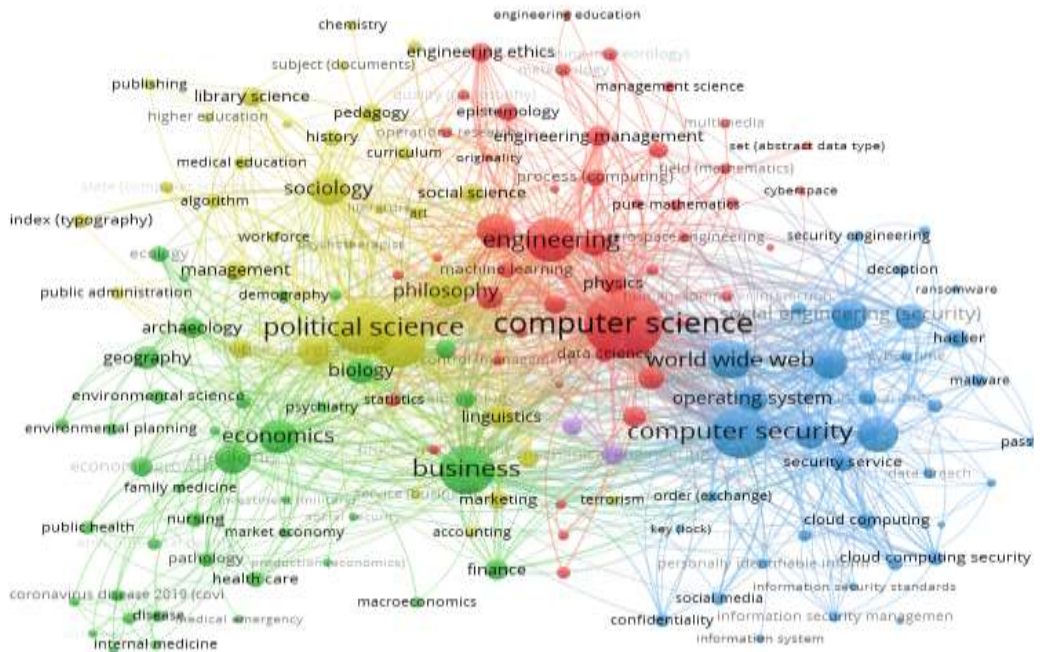
(Gyimah & et.al, 2022), where training and awareness programs represent one of the methods to enhance information security by implementing cybersecurity awareness programs that target where threats occur: end users or employees who are already using the internet and organization networks.

(Rana, 2019), This study is based on the hypothesis that: "The design of modern training and awareness programs contributes to the early detection of social engineering threats targeting the human element."

Network map of knowledge domains or academic disciplines, each node (circle) corresponds to a different field of knowledge, while the connecting lines illustrate conceptual or research-based relationships-such as co-citations or shared keyword usage.

the blue cluster centers on information security and cloud computing; the green cluster encompasses economics and public health; and the yellow cluster includes social sciences such as political science, sociology, and library science. The size of each node reflects the importance or prominence of the field, with larger nodes like "computer science" or "computer security" representing key hubs in the network. also highlights the strong overlap between disciplines, emphasizing the interdisciplinary nature of modern scientific research—such as the intersection of artificial intelligence with philosophy and sociology, or the connection between economics and public health.

A Proposed Strategy for Establishing Security Training and Awareness Programs for Early Detection of Social Engineering Threats



2. The Theoretical Framework for Security Training and Awareness Programs

with user training considered the most effective way to reduce users' susceptibility to social engineering threats (Aaron, Maria, & Steven, 2013).

The primary goal of information security training and awareness programs is to enable employees to develop the skills needed to identify, disable, and report any harmful social engineering attempts (Aldawood & Geoffrey, 2019). One of the key mechanisms for combating social engineering should be the education of potential victims, in order to increase their awareness of these techniques and how to detect them. Education, training, and awareness for employees or individuals are essential to defending against social engineering. In addition, policies, procedures, and standards are important components of a comprehensive anti-social engineering campaign (Anshul, Mansi, & Nagresh, 2015).

A security awareness program is defined as a formal initiative aimed at training users on potential threats to organizational information and how to avoid situations that may compromise the organization's data (Bill & Valerie, 2014). Security awareness is defined as the degree to which users understand the importance of information security, recognize their responsibilities, and act in ways that maintain adequate levels of control to protect the organization's data and networks (Shaw, Charlie, Albert, & Hui-Jou, 2009).

Security training and awareness programs should follow a continuous learning sequence, starting with awareness, then building into training, and eventually evolving into education (Azaabi, Benjamin, & Alex, 2022).

Cybersecurity awareness training is defined as "a proactive measure deployed to combat cybersecurity threats using various delivery methods to raise end-user awareness and promote secure behavior, with the overall goal of enabling users to recognize and report malicious activities in a timely manner and to apply cybersecurity best practices in their daily routines" (Alhashmi, Abdulbasit, & Jemal, 2021).

Employee training enables some companies to prevent and detect attempts that use social engineering techniques. Since training employees is often much easier than educating them about complex systems like firewalls, individuals will no longer be the weakest link in the security

A Proposed Strategy for Establishing Security Training and Awareness Programs for Early Detection of Social Engineering Threats

chain, but rather a protective shield provided that sufficient organizational measures are in place (Aisha, 2015).

The use of social engineering security awareness and training programs is aimed at improving user resistance and increasing awareness of social engineering attacks (Azaabi, Benjamin, & Alex, 2022). It is also essential to recognize the challenges that organizations may face in implementing training and awareness programs designed to raise the level of computer user awareness (Aldawood & Geoffrey, 2019).

3. Studies on Security Training and Awareness

Numerous studies have addressed the topic of security training and awareness in the context of social engineering. This section reviews the most important objectives, findings, and recommendations from those studies, and identifies areas of benefit relevant to the present research.

Study by Anshul, Mansi, & Nagresh (2015):

This study conducted a survey of social engineering concepts and the awareness methods associated with them. It focused on defining modern threats and the importance of awareness as a tool to counter these threats. The study provided several recommendations for defending against attackers using social engineering techniques, emphasizing that educating potential victims is one of the primary mechanisms for combating such attacks. The goal is to raise awareness of these techniques and how to detect them. Training and awareness are thus key, and policies, procedures, and standards form part of a broader strategy to fight social engineering.

Study by Grassegger & Nedba (2021):

This study aimed to analyze individual and organizational factors that influence employee awareness of information security, and how that leads to resistance to social engineering attacks. Based on a field survey of 136 employees, results showed that leadership and a tendency toward risk-prone behavior significantly affect employee security awareness. The findings affirmed that awareness is a central factor in information security.

The results also showed the relevance of applying the Theory of

Planned Behavior in the context of social engineering. It concluded that technical measures alone are not enough and recommended assessing employees' risk-taking tendencies and conducting workshops on awareness. It further advised expanding the survey to larger, targeted groups for more comprehensive data.

Study by Hussain & Geoffrey (2018):

This research highlighted the importance of increasing social engineering awareness and how it enhances both personal and organizational security. It explored how innovative information security education programs can effectively raise awareness and reduce cybersecurity incidents. The study found that security awareness is a crucial step toward creating a secure cyber environment and is the most effective method for combating social engineering threats.

Study by Aldawood & Geoffrey (2019):

This study reviewed existing training and awareness programs related to social engineering and emphasized persistent challenges, such as failure to adapt training to new developments and the lack of personalized needs assessments. It also discussed practical strategies to reduce training costs. Despite modern cybersecurity preparedness and trained staff, attackers were still successful in stealing sensitive organizational data. The study recommended designing strategies to address these challenges from the perspective of security decision-makers.

Study by George et al. (2020):

This study examined the continuous adaptation of cybersecurity training programs to the needs of trainees. It focused on improving the effectiveness of training against modern threats by combining educational practices with cybersecurity modeling to support dynamic, adaptive training processes. The study emphasized designing training programs based on trainee needs, and evolving these programs according to performance through tasks and assessments involving progressively advanced features.

Study by Ildikó (2020):

This research explored how to build an awareness program that maximizes user knowledge, attitudes, and behavior toward information

A Proposed Strategy for Establishing Security Training and Awareness Programs for Early Detection of Social Engineering Threats

security, resulting in positive cultural change in organizations. It compared traditional awareness programs with modern training methods and highlighted the role of communication channels and tools. The study found a positive correlation between users' knowledge, attitudes, and self-reported behavior. It recommended designing awareness programs tailored to specific organizational needs, using diverse tools to enhance employee awareness and build a suitable cybersecurity culture.

Study by Aldawood, Alashoor, & Skinner (2020):

This study investigated whether awareness of social engineering could predict and explain individuals' security protection practices. A survey was conducted with 265 employees in various Saudi organizations. The findings revealed that awareness of social engineering is a positive predictor of secure practices, even beyond simply having knowledge about information security. The study emphasized the importance of increasing employees' social engineering awareness as part of organizational investment in cybersecurity.

Study by Albladi & Weir (2020):

This study contributed to the development of a new model for predicting user vulnerability based on multiple user traits. The model included interactions between factors related to social media, such as level of engagement, motivation for using social networks, and ability to respond to threats. The findings showed that most user characteristics studied were directly or indirectly linked to user vulnerability. It also stressed the importance of considering individual traits when designing training and awareness programs.

Another study by Albladi & Weir (2020):

This study built a conceptual model to examine factors affecting social media users' judgment of social engineering-based attacks and identifying weaknesses in detection behavior. It showed that individual traits significantly impact user vulnerability and introduced a new socio-emotional perspective for predicting user behavior—an underrepresented factor in current literature.

Study by Alhashmi, Abdulbasit, & Jemal (2021):

This study focused on categorizing cybersecurity awareness delivery methods and presenting effective methodologies for addressing threats. The findings showed that well-designed awareness and training programs for end users significantly reduce their susceptibility to phishing attacks. However, the study also called for further research to enhance protection against phishing.

4. Proposed Strategy for Activating Security Training and Awareness Programs

Through innovative and interactive education, training, and awareness programs, organizations aim to equip their employees with the latest prevention techniques to avoid social engineering threats. The adopted measures include training materials, regulatory and policy frameworks, and training on safety procedures to be followed before and after attacks (Aldawood & Geoffrey, 2019).

This strategy aims to cover all necessary aspects of a comprehensive human-focused training process, which involves the following stages:

4.1 Identifying the Target Group and Assessing the Existing Security Level

One of the main challenges in implementing training is evaluating the user's baseline awareness level (Sutter & et al., 2022). The first step in developing an effective security program is to identify needs and problem areas, analyze root causes, and develop programs that include corrective measures (Ildikó, 2020).

To train users effectively, they must first understand the threats they face online, who the attackers are, and what their motivations might be (Bill & Valerie, 2014). To protect users from phishing, system designers and security professionals need to understand how users interact with such attacks and predict their behavior (Xun, John, & Jeremy, 2008).

The presence of unaware employees with limited knowledge of information

A Proposed Strategy for Establishing Security Training and Awareness Programs for Early Detection of Social Engineering Threats

security can widen the vulnerability to social engineering attacks (Alhashmi & et al., 2021). Identifying the most vulnerable users for targeted training improves the effectiveness of such programs (Albladi & Weir, 2020).

Personal traits are inherent characteristics in individuals that may pose a challenge to the effectiveness of training and awareness programs. Social engineers often choose their attack method based on the personality of the targeted employee (Aldawood & Geoffrey, 2019).

Although effective information security awareness is key to phishing prevention, many programs neglect human behavioral factors as a root cause of phishing vulnerability (Ayman, 2017).

Therefore, the first stage is to assess the current security posture and define the training and awareness target group. Recommended steps include:

- Identify sensitive information targeted in previous attacks or similar incidents.
- Define potential cyberattacks based on past social engineering threats faced by the organization.
- Conduct surveys or preliminary tests to gauge current awareness and knowledge among employees, revealing knowledge gaps and priority areas.
- Analyze the organizational structure to identify key roles and departments—particularly sensitive areas like IT.
- Understand daily tasks for each employee group and determine roles at greater security risk, especially those handling sensitive data.
- Segment the target audience into levels and align each group with appropriate training formats based on their technical expertise.

4.2 Behavioral Analysis

Proper cognitive and behavioral responses are vital when identifying phishing. These responses help users focus on detecting threats without being distracted by negative emotional triggers (Wang, Yuan, & Rao, 2017).

Effective information security requires both behavioral and technical components. Behavioral considerations in information systems security have grown due to the need for employees to access organizational information systems enterprise-wide (Burns & et al., 2017).

The Theory of Planned Behavior is a psychological model for predicting behavior. It defines “attitude toward the behavior” as a motivating factor, i.e., the level of effort a person is willing to exert to demonstrate a certain behavior (Siddiqi & et al., 2022).

Tools aimed at combating phishing must consider why and how people fall for phishing to be effective (Downs & et al., 2007). To understand and change individuals' security behavior, behavioral analysis is essential. Behavior change interventions are defined as:

"Coordinated sets of activities designed to change specific behavioral patterns." (Jansen & van Schaik, 2019)

Knowing how users behave helps design tools like toolbars and applications that provide phishing-related warnings (Downs & et al., 2007).

The Big Five Personality Traits model can be used to classify personality and predict behavioral vulnerabilities: (Tsinganos & et al., 2018):

1. Conscientiousness: Hardworking, organized, reliable vs. careless, disorganized.
2. Extraversion: Sociable, assertive vs. reserved, shy.
3. Agreeableness: Cooperative, warm vs. cold, hostile.

4. Openness: Imaginative, curious vs. narrow-minded.
5. Neuroticism: Emotionally unstable vs. calm.

4.3 Preparing the Training Program

One of the primary challenges faced by institutions in providing training and awareness programs against social engineering is the lack of a dedicated training budget (Aldawood & Geoffrey, 2019). Modern training methods for social engineering attacks are mostly developed by IT professionals (Aldawood & Geoffrey, 2019).

The steps for preparing the training program include:

- Identify employees in sensitive roles: Focus on those who have access to confidential information or leadership positions. These individuals require more comprehensive security training to ensure data protection.
- Ensure flexibility in scheduling: Training times should align with the job nature of the target employees. Some may require intensive training while others need less.
- Analyze the organization's existing culture: Determine how open employees are to hands-on training, and design interactive sessions that fit the prevailing culture.
- Analyze past incidents: Review and study past security incidents to identify departments or employees who may need additional attention in training.
- Continuously update the list of trainees: As the organizational structure or work technologies evolve, the target audience should be kept up to date to ensure comprehensive and consistent awareness.

- Educate on safe online behavior: Teach practices such as avoiding unknown attachments, refraining from clicking suspicious links, and being cautious when sharing personal or company data online (Zaoui & et al., 2024).
- Include common scams and tactics: Training sessions should incorporate engaging activities to help employees interact effectively with training content (Aldawood & Geoffrey, 2019).
- Password security training: Educate employees on creating strong passwords, and on the dangers of reusing or sharing them (Zaoui & et al., 2024).

Modern training methods often use simulations to help employees think critically and assess whether a message is a social engineering attempt. However, these simulations are usually standardized and may not cater to individual comprehension levels (Aldawood & Geoffrey, 2019).

4.4. Adopting a Motivational Learning Strategy

Another challenge for training and awareness programs is lack of employee interest. Many people lack the personal motivation to receive training regularly, even though it protects them and their organizations (Aldawood & Geoffrey, 2019).

Learning motivation refers to the activation of learning behaviors (Palmer, 2016). Motivated learning requires a mechanism that generates abstract goals and motivations, manages them, and oversees goal selection and achievement. These motivations are triggered by interactions with the environment and are influenced by competitive events and attention cues at any stage of development (Shi & et al., 2015).

Motivation acts as a driving force that helps determine objectives and overcome challenges.

The following table summarizes teacher self-assessment and learner

A Proposed Strategy for Establishing Security Training and Awareness Programs for Early Detection of Social Engineering Threats

analysis across five dimensions: attention, relevance, confidence, satisfaction, and volition (will):

Table 1. Teacher self-assessment and learner analysis across five dimensions

Teacher's Self-Assessment	Teacher's Analysis of Learners	Category
Am I excited about this experience? How can I make it engaging?	Will learners care? What tactics will spark curiosity and attention?	Attention
Do I believe this experience is valuable for my students?	Will learners find this valuable? How can I show its importance?	Relevance
Am I confident in leading this effectively and engagingly?	Will learners feel capable of learning this? How can I build confidence?	Confidence
Will I feel positive about this educational experience?	How can I make learners feel satisfied and want to continue learning?	Satisfaction

Source: John M. Keller, “Motivation, Learning, and Technology: Applying the ARCS-V Motivation Model,” Participatory Educational Research (PER), 2016.

Educational management is the process of making both learners and instructors satisfied with the training experience, assuming all expected tasks are well executed (Fereshteh & et al., 2016).

Motivational learning involves sensory input (via observation), followed by mutual transformation of perceptions through events. Identifying novelty, attention cues, and observations is essential before defining motivational learning algorithms (Shi & et al., 2015).

Practical actions to motivate employees to participate in security awareness training include:

A Proposed Strategy for Establishing Security Training and Awareness Programs for Early Detection of Social Engineering Threats

- Promote a sense of personal responsibility: Highlight the employee's role in protecting information and maintaining security.
- Activate interactive learning tools: Use games, competitions, and collaborative workshops to simplify complex topics in a fun, engaging way.
- Enable continuous feedback and diagnosis: Evaluate motivations and make adjustments at every stage of the training process.

4.5. Selecting Effective Training Methods

There are various methods for delivering security training and awareness programs, including: (Azaabi, Benjamin, & Alex, 2022)

- Face-to-face methods: Lectures, storytelling, and workshops.
- Self-directed learning: Videos and games.
- Instructor-supported formats: Such as online learning platforms.

Additional tools include simulations, serious games, virtual labs, awareness videos, and modular learning packages (Aldawood & Geoffrey, 2019).

Artificial Intelligence (AI) enables the creation of personalized and adaptive training experiences. By analyzing individual user behavior, past interactions, and even response times to simulated threats, AI can design training scenarios tailored to each user's competence level and vulnerabilities (Fakhouri & et al., 2024).

Modern awareness training approaches such as thematic videos and interactive modules—are creative alternatives. However, there is no one-size-fits-all solution, especially since the unpredictability of social engineering attacks often surpasses the designers' foresight (Aldawood & Geoffrey, 2019).

A suggested classification of cybersecurity awareness training delivery

methods consists of three main categories:

1. Face-to-face training
2. Self-directed training
 - a. Flexible (e.g., on-demand e-learning)
 - b. Fixed (e.g., scheduled video tutorials)
3. Embedded learning (e.g., integrated into daily tools or software)

Table 2. Comparison Between Traditional Training, Hands-on Learning, and Game-Based Learning

Criteria	Traditional Training	Hands-on Learning	Game-Based Learning
Cost-effective	☐	☐	☐
Low physical risk / liability	☐	☐	☐
Standardized evaluations / student comparison	☐	☐	☐
Highly interactive	✗	☐	☐
Personalized learning pace	✗	☐	☐
Immediate feedback on learner errors	✗	☐	☐
Easy transfer of learning to real-world	✗	☐	☐
Easy transfer of learning to real-world	✗	☐	☐

Source: Jin-Ning Tioh, Mani Mina, Douglas W. Jacobson, "Cyber Security Social Engineers: An Extensible Teaching Tool for Social Engineering Education and Awareness", 2019 IEEE Frontiers in Education Conference.

Serious games are a form of learning and training tool that use an interactive narrative format to convey information (Rana, 2019). Researchers and practitioners have increasingly embraced serious games for enhancing professional development by fostering active learning (Stefan & Kristina, 2016).

They've gained a strong reputation recently for engaging corporate employees in security-related activities in a fun and sustainable manner. A serious game is defined as:

"A game designed for a primary purpose other than pure entertainment."
(Dina, Kristian, & Sebastian, 2018)

Serious games complement traditional or computer-based training by providing an entertaining environment where learners practice cybersecurity concepts (Stephen, Andrea, Federica, & Vladimiro, 2020). Digital Game-Based Learning (DGBL) makes learning more engaging, motivating, and personalized from the learner's perspective. DGBL has been applied across disciplines, including cybersecurity education (Filippos, Georgios, & Stefanos, 2015).

Steps for Using Serious Games as a Security Awareness Tool

1. Define learning objectives: Specify what the game should achieve—e.g., improve communication skills, teach social engineering principles, increase risk awareness.
2. Design the game: Incorporate realistic scenarios involving social engineering. Include challenges that require critical thinking and social skill application, modeled on real-life events.
3. Use attack vector cards: Help participants understand that social engineering attacks come in many forms. These cards reinforce various innovative attack styles and scenarios (Muhly, Leo, & Caneppele, 2021).
4. Continuous updates: Adapt game mechanics and administration to maintain employee engagement, satisfaction, and interpersonal interaction.
5. Empower game facilitators: Game managers play a central role in guiding participants, ensuring procedural flow, and achieving learning outcomes.
6. Implement the game: Run the game in either physical or virtual environments, ensuring it is interactive and exciting enough to

capture and retain attention.

4.6. Implementing the Training Program and Achieving Security Maturity

Following the preceding stages of designing security training and awareness programs, the implementation phase is critical to the success of the proposed program. It requires activating several measures using all available resources within the proposed training timeframe.

Training typically aims to develop skills in information security (Jansen & van Schaik, 2019). Every educational system—large or small—must evaluate its training courses, plan educational development, and manage instructional activities by making optimal use of resources to achieve its goals (Fereshteh & et al., 2016).

A key success factor in security awareness programs is the relevance, timeliness, and consistency of the provided information, especially since information risk profiles change continuously (Schlienger & Teufel, 2003). A particularly important factor is the execution timeline, which refers to the estimated duration in hours, days, months, or years required to roll out the proposed program. It reflects the time investment needed to deploy the methodology and integrate it into the organization's infrastructure, operations, and existing security framework. While estimating this timeline is challenging, several factors can influence it (Konstantinos & Kritikos, 2024).

After receiving an effective awareness program, employees should be capable of moving from:

- Mere "awareness"
- To a state of "conscious vigilance"
- To "staying informed and alert" to evolving security threats (Schlienger & Teufel, 2003)

4.7. Evolutionary Diagnosis and Deviation Correction

A Proposed Strategy for Establishing Security Training and Awareness Programs for Early Detection of Social Engineering Threats

Information security diagnosis in organizations involves analyzing known security risks at the institutional level through: (Hwang & et al., 2010)

- Interviews with IT system managers
- Document review
- Field inspections

To correct any deviations in training and awareness procedures, evolutionary analysis must be conducted to determine the implementation level of the programs and identify any deviations.

Key steps for evolutionary diagnosis and deviation correction:

1. Re-evaluate the current security level and match it with the initial goals defined before implementing training.
 - a. Analyze security awareness disparities among staff.
 - b. Identify the awareness needs of each management level.
 - c. Measure employee responsiveness to training and awareness activities.
2. Evaluate the effectiveness of the training tools used.
 - a. Assess each tool's relevance, applicability, cost, and interaction level.
3. Evaluate the educational motivation strategies used and seek to create new ones that eliminate employee boredom or disengagement.
4. Determine the educational benchmarks to be achieved within specific timeframes.
 - a. Make corrective decisions at every phase of the training and awareness implementation process.

5. CONCLUSION

This study aimed to present a strategy for implementing security training and awareness, serving as the first foundational step in building robust defense mechanisms against social engineering threats. The focus was on establishing practices that equip individuals and employees with sufficient knowledge about social engineering methods.

The proposed strategy is based on cutting-edge approaches, such as simulating attack scenarios and conducting evolutionary diagnostics to assess the prevailing security culture.

From this, the study reached the following conclusions:

1. Security training and awareness practices are among the most effective methods for early detection of social engineering threats—especially those that target human vulnerabilities. Organizations must adopt advanced training tools and techniques that align with both past and emerging threats, with particular attention to fraudulent emails, suspicious phone calls, and psychological manipulation.
2. The proposed implementation mechanisms and steps for training and awareness programs were formulated based on intellectual foundations and practical practices. These steps, in order, include:
 - a. Identifying the target audience and assessing their current awareness levels
 - b. Behavioral analysis of the target group
 - c. Preparing the training program
 - d. Adopting a motivational learning strategy
 - e. Selecting effective training methods
 - f. Executing the training plan
 - g. Conducting evolutionary diagnosis and correcting deviations
3. Through innovative and interactive educational programs, institutions aim to prepare employees using the latest prevention techniques. These measures include:
 - a. Training materials
 - b. Policy and governance frameworks
 - c. Safety protocols for pre- and post-attack response
4. Along with regular training, organizations are encouraged to launch timely information security awareness campaigns that emphasize the importance of sustained vigilance.

6. Recommendations

A Proposed Strategy for Establishing Security Training and Awareness Programs for Early Detection of Social Engineering Threats

To achieve the desired outcomes of security training and awareness programs in the early detection of social engineering threats, the study recommends:

- Using effective tools and methods to measure employee awareness of social engineering practices, such as regular surveys and simulated penetration tests.
- Evaluating employee experiences with current technologies and policies—like data encryption tools, multi-factor authentication, and intrusion detection systems—and identifying implementation gaps.
- Analyzing previous social engineering incidents and how employees responded to them. Extract lessons and identify all the tactics used by attackers.
- Making cost-based comparisons between available training methods:
 - Traditional and electronic training methods are more cost-effective.
 - Simulation-based and serious-game-based approaches are more costly but immersive.
- Making effectiveness-based comparisons:
 - Simulations and serious games are more effective, as they realistically mimic actual social engineering tactics.
- Making continuity-based comparisons:
 - Field and electronic training methods offer better sustainability via periodic updates, making them more suitable for long-term awareness efforts.
- author's name, year, page**Fig.1.** Figure title (this is an example of figure 1)
author's name, year, page experimental section can be divided into subsections, the contents of which vary according to the subject matter of the article. It must contain all the information about the experimental procedure and materials used to carry out experiments. conclusion of a research paper needs to summarize the content and purpose of the article. The conclusion of a research paper needs to summarize the content and purpose of the article. The conclusion of

a research paper needs to summarize the content and purpose of the article. The conclusion of a research paper needs to summarize the content and purpose of the article. The conclusion of a research paper needs to summarize the content and purpose of the article. The conclusion of a research paper needs to summarize the content and purpose of the article.

5. Bibliography List :

1. Aaron, S., Maria, P., & Steven, M. F. (2013). Improving Awareness of Social Engineering Attacks pp. International Federation for Information Processing , 249–256.
2. Abass, I. (2018). Social Engineering Threat and Defense: A Literature Survey. Journal of Information Security, 9 , 257-264.
3. Aisha, S. A. (2015). The Awareness of Social Engineering in Information Revolution: Techniques and Challenges. The 10th International Conference for Internet Technology and Secured Transactions (ICITST) , 198-201.
4. Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity 3:0 , 1-19.
5. Aldawood, H., & Geoffrey, S. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet , 11, 73 , 1-16.
6. Aldawood, H., & Geoffrey, S. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet , 11, 73 , 1-16.
7. Aldawood, H., Alashoor, T., & Skinner, G. (2020). Does Awareness of Social Engineering Make Employees More Secure? International Journal of Computer Applications, 177(38), , 45-49.
8. Alhashmi, A. A., & et.al. (2021). Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats. International Journal of Advanced Computer Science and Applications, Vol. 12, No. 10, , 29-35.
9. Alhashmi, A., Abdulbasit, D., & Jemal, H. A. (2021). Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats. International Journal of Advanced Computer Science and Applications, Vol. 12, No. 10, , 29-35.

A Proposed Strategy for Establishing Security Training and Awareness Programs for Early Detection of Social Engineering Threats

10. Almutairi, B., & Alghamdi, A. (2022). The Role of Social Engineering in Cybersecurity and Its Impact. *Journal of Information Security*, 13, , 363-379.
11. Anshul, K., Mansi, C., & Nagresh, K. (2015). Social Engineering Threats and Awareness: A Survey. *European Journal of Advances in Engineering and Technology*, 2(11) , 15-19.
12. Ayman, S. (2017). , Understanding the Human Behavioural Factors behind Online Learners' Susceptibility to Phishing Attacks. This thesis is submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy November. Department of Educational Research, Lancaster University, UK .
13. Azaabi, C., Benjamin, W., & Alex, O. (2022). Improving Social Engineering Awareness, Training and Education (SEATE) using a Behavioral Change Model. *International Journal of Advanced Computer Science and Applications* Vol. 13, No. 5 , 606-613.
14. Bill, G., & Valerie, T. (2014). Building an Information Security Awareness Program. .: Syngress publications.
15. Burns, A. J., & et.al. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior* Volume 68 , 190-209.
16. Chapagain, D., & et.al. (2024). Deception Techniques in Social Engineering Attacks: An Analysis of Emerging Trends and Countermeasures. DO 10.48550/arXiv.2408.02092 , 1-10.
17. Dina, A., Kristian, B., & Sebastian, P. (2018). PERSUADED: Fighting Social Engineering Attacks with a Serious Game. *TrustBus in Trust, Privacy and Security in Digital Business - 15th International Conference, Regensburg, Germany, September 5-6, 2018* , 1-15.
18. Downs, J. S., & et.al. (2007). Behavioral Response to Phishing Risk . *Proceedings of the 2nd Annual Conference of the Anti-Phishing Working Groups* , 1-8.
19. Fakhouri, H. N., & et.al. (2024). AI-Driven Solutions for Social Engineering Attacks: Detection, Prevention, and Response. *2nd International Conference on Cyber Resilience (ICCR)* | 979 , 1-9.
20. Fereshteh, F., & et.al. (2016). Evaluating of Training and Internship

- Programs of University Hospitals. *Health*, 8 , 658-663.
21. Filippou, G., Georgios, K., & Stefanos, G. (2015). CyberAware: A Mobile Game-based app for Cybersecurity Education and Awareness. *International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)* , 54-58.
 22. Gadhi, A., & et.al. (2024). Cyber Resilience through Real-Time Threat Analysis in Information Security. *International Journal of Communications, Network and System Sciences*, 17 , 51-67.
 23. George, H., & al, e. (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Applied Sciences.* , 10, 5702 , 1-26.
 24. Grassegger, T., & Nedba, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia Computer Science* 181 , 59–66.
 25. Gyimah, A. S., & et.al. (2022). Social Engineering Attacks: A Clearer Perspective. *International Journal of Computer Applications* , Volume 184 – No.8, April , 53-62.
 26. Halida, E., & et.al. (2022). Strategy to Improve Employee Security Awareness at Information Technology Directorate Bank XYZ. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)* Vol.6No. 4 , 577-584.
 27. Hussain, A., & Geoffrey, S. (2018). Educating and Raising Awareness on Cyber SecuritySocial Engineering: A Literature Review. *International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*4-7 December , Wollongong, NSW, Australia , 62-68.
 28. Hwang, W. T., & et.al. (2010). Information security diagnosis for small and medium-size enterprises—A case study on a southern Taiwanese retail business. *Reliability, Risk and Safety – Ale*, Papazoglou & Zio Taylor & Francis Group, London , 1695-1702.
 29. Ildikó, L. (2020). BUILDING AN EFFECTIVE INFORMATION SECURITY AWARENESS PROGRAM. *CEE e|Dem and e|Gov Days* , 189-200.
 30. Jansen, J., & van Schaik, P. (2019). *International Journal of Human-Computer Studies* Volume 123 , 40-55.
 31. Jemal, A. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, Vol. 33, No. 3 , 236–247.