Revolutionizing Social Engineering Awareness Raising, Education and Training: Generative AI-Powered Investigations in the Maritime Domain

Michail Loupasakis, Georgios Potamos, and Eliana Stavrou(✉)

Open University of Cyprus, Nicosia, Cyprus
{michail.loupasakis1,georgios.potamos}@st.ouc.ac.cy,
eliana.stavrou@ouc.ac.cy

Abstract. Innovation in generative Artificial Intelligence (AI) has already been leveraged by cybercriminals to deliver AI-powered social engineering attacks, specifically phishing. This advancement adds to the challenges the cybersecurity community is facing, such as lack of motivation to change unsafe behaviors and low engagement with awareness raising, education and training activities. Often, the problem is attributed to the fact that activities communicate the same message across different audiences. This approach is not helpful to assist people relating to the problem, realizing the threat and how it can be transformed. To build cyber resilience against phishing, the workforce needs to realize how phishing can be delivered in the context of their working environment and what aspects a cybercriminal can leverage to make the attack more realistic and plausible. This requires the design of awareness raising, education and training activities that can deliver highly tailored and context-aware messages to different audiences, considering their job role and responsibilities. Generative AI has already demonstrated an ability of high degree of creativity which is imperative for creating tailored and effective awareness raising and training content. This study investigates how generative AI can be leveraged by stakeholders, such as educators and trainers, to develop phishing-tailored attack scenarios. The scenarios can be embedded in awareness raising and training activities that can be delivered e.g. over cyber ranges, aiming to enhance the workforce's cyber resilience against phishing attacks. Investigations are performed in the context of the maritime domain.

Keywords: Social Engineering · Phishing · ChatGPT · Generative AI · Maritime Cybersecurity · Cybersecurity Awareness Raising · Cybersecurity Education · Cybersecurity Training · Phishing Attack-Tailored Scenarios · Cyber Resilience

1 Introduction

Social engineering is a major threat that keeps challenging society and the cybersecurity community. The dimension of social engineering and its impact were made evident during COVID-19 pandemic [1] as cybercriminals exploited all aspects of personal and

A. Moallem (Ed.): HCII 2024, LNCS 14729, pp. 70–83, 2024.
https://doi.org/10.1007/978-3-031-61382-1_5

business life to engage their victims. During this time, a high degree of creativity in terms of phishing lures was observed, successfully engaging the victims that fell for the lure. Post pandemic period the problem remains [2], giving a clear message to the cybersecurity community that society has not reached a satisfactory level of cyber resilience against social engineering attacks, especially with regards to phishing [3]. The fact that ENISA has announced [4] that the theme of the EU Cybersecurity month, October 2023, will focus on increasing awareness on social engineering demonstrates that the cybersecurity community is prioritizing its actions to empower citizens against the social engineering pandemic. The evolution of generative Artificial Intelligence (AI) and the rise of malicious AI chatbots [3], which can be utilized to launch sophisticated phishing attacks, makes this prioritization imperative.

The cybersecurity community has launched many initiatives to raise awareness of the social engineering threat and educate citizens on cyber hygiene practices. A key challenge when designing cybersecurity awareness raising, education and training activities is to engage and motivate the audience to learn. One way to achieve this is by creating cybersecurity games and game genres [5], ranging from tabletop games, to serious games, to cyber range simulation environments. Although awareness and training were found to be the most effective way to reduce susceptibility to social engineering attacks [6], we still observe high percentages of compromisation. Different social engineering training and awareness programs [5, 7] have been developed. However, often the same message is communicated across different audiences; this approach does not help people to relate to the problem [8], realize the threat and how it can be transformed. This lack of understanding hinders an individual's understanding of the threat, can easily disengage them from the awareness raising activities and become unmotivated to change unsafe behaviors. Microsoft defense report 2023 [9] indicates the need to "*conduct innovative experimentation with user engagement strategies*" and recommends to "*develop tailored and context-aware education models that treat users as distinct individuals and be implemented at scale*". An innovative direction to consider is to investigate more actively the contextualization of phishing attacks in different use cases to empower user engagement and understanding of the threat. This approach is expected to deliver tailored messages to different audiences and lead to more appealing and engaging content that can lead to acquisition of new knowledge and motivate safer behaviors.

Contextualizing and developing phishing-tailored awareness raising content is not an easy task to perform, considering the variety of audience profiles that can be constructed, e.g., based on working domain, job roles, personal and or professional interests, etc. The power of generative AI [10] can be leveraged to guide content creation and the development of phishing-tailored attack scenarios, assisting cybersecurity professionals, e.g. educators, trainers, and curricula designers, optimize the content design process. As Tom Burt, Microsoft's Corporate Vice President, Customer Security & Trust, stated "*Artificial Intelligence will be a critical component of successful defense. In the coming years, innovation in AI powered cyber defense will help reverse the current rising tide of cyberattacks*".

This paper aims to investigate how generative AI can be leveraged to create phishing-tailored attack scenarios given a specific domain. The current study is performed in the context of maritime domain. Investigations are expected to provide insights to cybersecurity educators and trainers, guiding the design of AI-powered awareness raising and training initiatives, e.g. campaigns, tabletop games, phishing simulations, etc. A core aspect of the investigations is to empower them integrating phishing attack-tailored scenarios into the design of learning activities that the workforce can easily relate with, understand, and acquire new knowledge that can be adapted when a phishing attack is transformed. For example, the integration of attack scenarios can be valuable for activities delivered over cyber ranges. Cyber ranges can simulate a range of phishing attack scenarios, demonstrating how cybercriminals can deliver a tailored phishing attack and what aspects they can leverage to make the attack realistic and plausible. Enhancing the workforce's cyber situational awareness can contribute to empowering them to become cyber resilient against current and future social engineering attacks.

Section 2 presents relevant work. Section 3 discusses the study methodology. Section 4 briefly analyses the exploration aspects considered for crafting AI prompts. Section 5 presents the main observations derived from the generative AI tool (ChatGPT) responses. Section 6 critically discusses whether generative AI can be leveraged to create phishing-tailored attack scenarios and Sect. 7 concludes the work.

2 Relevant Work

The need to adopt a tailored approach in designing awareness raising activities and content is highlighted in [11] where the design of a new educational activity is presented, demonstrating how social engineering can be contextualized in a healthcare scenario. The work in [12] emphasizes that it is essential to understand people's behavior and prior knowledge to provide them with customized and effective security training. Authors propose to group people based on their awareness of social engineering threat prior to providing tailored security training. The importance of pursuing tailored security training is highlighted in the global Cyber Resilience Index (CRI) [13] which was developed by the World Economic Forum Centre for Cybersecurity, in collaboration with the Cyber Resilience Index Working Group and with Accenture. CRI is a framework of best practice, guiding organizations to develop and evaluate the level of their cyber resilience. As stated in the guidelines "*fundamental cyber resilience must be integral not only to technical systems but also in teams, the organizational culture and the daily way of working*". The framework also highlights the need to provide continuous training to stay up-to-date with the cyber threat landscape and to empower people identifying and communicating threats. Thus, demonstrating cyber resilience in their daily responsibilities. This indicates that initiatives should tailor the message to communicate through training, depending on the audience, and considering the workforce's job responsibilities. Such an approach can promote the development of a multidisciplinary workforce [14] that will be able to apply cyber hygiene and contribute towards an organization's cyber resilience. Creating a culture of cyber resilience across the organization is vital given how social engineering attacks have evolved since ChatGPT launched [3]. The "*State of Phishing 2023*" report [3] presents how cybercriminals leverage generative AI to systematically launch highly targeted phishing attacks. The rise of malicious AI chatbots, such as WormGPT, can assist cybercriminals to write professional emails and launch sophisticated phishing and Business Email Compromise (BEC) attacks.

Given the advancements of the cyber threat landscape, it is pivotal to upskill the workforce to realize how phishing attacks can be transformed and to identify how they can be tailored given a specific business environment. The work in [15] investigates detection aspects in the maritime domain and contributes towards a novel maritime cyber threat detection framework. The proposed framework guides the development of cyber threat detection skills in the maritime domain to effectively manage maritime-related cyber risks. It provides directions to tailor training initiatives considering the personnel's role and responsibilities in the maritime ecosystem. The framework specifies key capabilities that need to be developed such as identifying the maritime attack surface and the impact to business operations, explaining how specific cybersecurity threats may compromise the operation of maritime assets, and detecting a security incident. The work in [16] takes into consideration the guidelines provided in [15] and presents the design of an innovative training curriculum aiming to develop cybersecurity capacity in the maritime domain and defend against ransomware attacks.

3 Methodology

An exploratory methodology is utilized to investigate whether generative AI tools such as ChatGPT can generate tailored, realistic, and plausible phishing attack scenarios based on the presented business environment. The investigations are expected to provide insights and guide different stakeholders, e.g. educators, trainers, curricula designers, etc., to use generative AI tools to create phishing-tailored attack scenarios and inform awareness raising and training initiatives. Customizing awareness raising and training initiatives is envisioned to engage different users with the training and empower their understanding. ChatGPT 4.0 was preferred over the community version as it is reported to be more creative. Given that cybercriminals are being creative with the lures utilized and are successfully deceiving people, initiatives should leverage the creativity demonstrated by generative AI tools such as ChatGPT to create plausible attack scenarios that can be delivered in the context of a specific organization.

This work deployed the following methodology inspired by the work in [16]:

a) **Social engineering attack aspects**. Initially, attack-related aspects are specified, profiling the attack strategy of a social engineer. These aspects are considered for crafting generative AI prompts and for critically analyzing relevant responses.
b) **Business environment**. The business environment is dissected, specifying the mission, the processes, the organizational structure, and the internal and external stakeholders. This information can be considered for crafting opening prompts to contextualize phishing attacks considering the specific business environment.
c) **Preliminary analysis**. During the preliminary analysis, specific codes are extracted to facilitate subsequent qualitative analysis. The coding structure is organized under four thematic categories: (i) relevance to different departments/operations, (ii) realism and plausibility, (iii) psychological manipulation, and (iv) sophistication.
d) **Colour coding**. Prompts and relevant ChatGPT responses are included in a document to facilitate the analysis. An appropriate colour-coding scheme is applied considering the specified coding structure.

e) **Qualitative analysis**. A spreadsheet is created to facilitate the analysis. Prompts, responses, and observations are reported. The latter are utilized to fine-tune subsequent prompts.
f) **Prompt engineering**. The prompts to input to the generative AI tool are crafted based on the research aim and objectives, the business environment and social engineering attack aspects analyzed in this study.
g) **Exploration**: New prompts are created and/or existing prompts are amended, following ChatGPT's responses. The aim is to explore whether responses can lead to the creation of tailored attack scenarios.

4 Exploration Aspects

This section briefly analyses the key aspects that need to be taken into consideration to craft appropriate generative AI prompts and support the research objectives of the study. Initially, we profile social engineering attacks and identify key attack attributes, and then the business environment is scrutinized. These aspects are expected to drive the specification of tailored social engineering attack scenarios by using appropriate prompts.

4.1 Social Engineering Attacks

A range of social engineering attacks can be leveraged by cybercriminals, providing the means to use different attack methods, successfully engaging and compromising the target. Such methods, among others, include phishing, vishing, smishing, baiting, tailgating, dumpster diving, shoulder surfing, etc. Social engineering attacks often succeed because they are delivered in a context which the victim is familiar with. For example, a phishing attack is crafted considering the business environment of the victim or considering personal preferences. In such tailored cases, the social engineer increases the chances to engage the victim and successfully deploy the attack. To be able to create attack-tailored attack scenarios and inform awareness raising and training initiatives, it is imperative to identify exploitability attributes a social engineer might use when crafting and delivering a social engineering attack. These attributes can be utilized to develop relevant generative AI prompts that can lead to tailored attack scenarios. This study considers three exploitability attributes:

Attack Vector. This attribute reflects the means which will be utilized to deliver the attack. Typically, there are three main ways delivering a social engineering attack: (a) using the phone, (b) through digital means, and/or (c) through physical interaction.

Influence Tactics. Social engineers apply a range of psychological tactics to manipulate the victims and convince them to reveal sensitive information and/or take further actions that could lead to unauthorized access. Such tactics include: (a) conveying a sense of urgency, (b) causing fear, (c) creating a sense of obligation, (d) demonstrating authority.

Attack Lure. Social engineering attacks are customized to deliver tailored lures and increase the possibility to engage the victims. Often, social engineers profile the victim (personal preferences, relationships, etc.) and their business environment (domain, work role, business collaborators, etc.). This information is utilized to craft tailored lures that the victim will be familiar with and make the social engineering message realistic and more attractive to the victim.

4.2 Business Environment

Typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition [17]. The latter is a condition that can affect the likelihood of occurrence and success of a threat event. For example, the business environment can constitute a predisposing condition that social engineers can exploit for their benefit. The structure of the organization, its mission, the internal and external stakeholders, and the business processes are aspects that can be useful in a social engineering attack to create a realistic scenario which can effectively engage victims.

Given the advances of the maritime cyber threat landscape [14, 15], the maritime domain is selected to perform the investigations and support the study's research objectives. The adverse impact on critical infrastructures due to successful social engineering attacks can be devastating, and can have cascading effects on a local, national, and international level. For the purposes of the study, a fictional maritime organization (called maritime-FLE) is considered [18, 19]. The profile of the fictional organization follows, and it will inform the prompts' engineering task that is part of the study's methodology.

Mission. The company is specialized in the manufacturing, supply, and service of an extensive range of lifesaving and firefighting equipment, with a commitment to spearheading innovation and excellence in maritime safety and services. The company is operating globally, with warehouses and branches across Europe. Moreover, the company leverages an extensive network of service companies in every major commercial port worldwide. This strategic positioning enables it to efficiently supply and service commercial vessels all over the world.

Business Structure and Operations. The company consists of the following departments:

- Auditing: Ensures law compliance and financial integrity.
- Human Resource (HR): Manages workforce development.
- Sales: Focuses on revenue generation and customer relations.
- Marketing: Drives brand engagement and market penetration.
- Research & Development (R&D): Innovates and fine-tunes maritime products.
- Production: Ensures manufacturing processes of maritime products.
- Procurement: Handles the order process for raw materials and trade products.
- Shipping & Logistics: Manages efficient distribution and supply chain operations.
- Information Technology & Web Development: Supports digital infrastructure and online presence.
- Legal: Handles legal compliance and maritime law.

Internal Stakeholders

Employees. They are the backbone of the company and have specialized skills, contributing with their expertise across various departments. From the meticulous work of the R&D team, innovating and improving maritime safety products, to the production team ensuring high-quality manufacturing.

Management and Leadership. This group includes department managers, directors, and executives (COO, CCO, CEO). They are responsible for strategic decision-making and ensuring that departmental activities align with overall business goals.

External Stakeholders

Suppliers. They provide essential raw materials for product manufacturing, playing a crucial role in the supply chain. Their reliability and quality standards directly impact the company's product offerings and reputation in the market.

Logistics and Distribution Partners. This includes agents and forwarders who ensure the efficient and timely distribution of products globally. Their work is critical in maintaining a seamless supply chain, from warehousing to delivery at various international ports.

Regulatory Bodies and Maritime Authorities. These stakeholders ensure compliance with maritime laws and safety regulations. Their guidelines and standards shape the company's product development and operational procedures.

Clients and End-Users. These are the vessel operators, shipping companies, and other maritime entities that use the company's products. Their feedback and satisfaction levels are vital indicators of product performance and influence future product developments and service enhancements.

5 Analysis of Generative AI Responses

This section will analyze the investigations performed with the aim to provide insights about the potential of generative AI tools, such as ChatGPT, to assist educators, trainers and curriculum designers, creating tailored social engineering attack scenarios considering a specific business environment.

Initially, a prompt was crafted to set the task purpose and provide relevant context to the tool: *"Assume the role of a cybersecurity trainer and curriculum designer. You will create social engineering scenarios for user training. The users are working in a maritime company called maritime-FLE with different departments. The training social engineering scenarios should be tailored to each department, so they are focused and effective."* (prompt #1). The tool responded that it is waiting for details about the business environment, the specific departments within the company, and any specific aspects or challenges that we would like to address in the training. It has acknowledged that this information will help ensure that the scenarios are relevant, realistic, and effective for each department. Considering the tool's response, it was decided to provide input information that extended the business environment (which was the authors' first intention), covering exploitability aspects related to the social engineering attacks. Specifically, the subsequent prompt provided as input Sect. 4 of this paper that covered the business environment (mission, structure and operations, internal and external stakeholders) and the attack related aspects (attack vector, influence tactics, attack lure), and requested the tool to "*give an example of a phishing scenario targeting maritime-FLE company*" (prompt #2). Before delving into the specifics of the proposed attack scenario, it is worth mentioning that the tool has structured its response into *six sections*: 1) Background, 2) Attack setup, 3) Lure, 4) Targeted action, 5) Consequence, and 6) Preventive measures. The structure is very helpful in guiding educators and trainers to design learning material considering a specific business domain (*Sect. 1*) to increase awareness of a social engineering attack, e.g., how it is performed (*Sect. 2*), the message utilized to engage potential victims (*Sect. 3*), understand the attacker's motivation (*Sect. 4*), the impact (*Sect. 5*) and measures that the company should have implemented to address the attack (*Sect. 6*). The provided response structure was considered useful; thus, it was decided to keep it and not request any amendments. In terms of the suggested scenario, the tool selected a department (*Procurement*) which was included in the input business information and elaborated the attack details which are discussed next.

Investigations focused on the diversity of attack scenarios and their *relevance to different departments and business operations*. In total, ten pairs of prompts have been crafted to investigate this aspect; each pair included a prompt considering the format *"create a phishing scenario for the <name> department"*, and a subsequent prompt "*to change the lure"*. A total of ten departments have been considered as per maritime-FLE company profile, yielding a total of twenty prompts. The main observations are discussed next.

Observation 1. All phishing attacks were delivered through email.

Observation 2. The expected action from the victim side was to visit a website that closely resembled the official website and provide sensitive information, and/or open a malicious attachment.

Observation 3. The attack storyline considered typical operations delivered by the respective department as per each prompt, making the attack more relatable and enhancing its realism. This can increase users' engagement in a potential attack which makes it imperative to expose users to these scenarios, so they increase their awareness and resilience. For example, the tool considered that Procurement is dealing with "*ordering of raw materials and trade products*" and suggested a phishing email with the subject "*Urgent Update Required for Order Processing*". The email scenario stated that there has been a critical update in the supplier's order processing system and that all clients must immediately update their account details to ensure uninterrupted service and delivery schedules. When the tool was prompted to change the attack lure, it tailored the attack scenario considering another routine operation performed by the Procurement department. Specifically, it considered operations such as "*handling and processing invoices related to the purchase of materials and services*" and crafted a relevant email subject "*Immediate Attention Required: Invoice Discrepancy for Recent Order*". The tool suggested creating an email claiming either an overpayment or underpayment by maritime-FLE and stress out the urgency of resolving this issue to maintain a smooth business relationship and avoid any legal complications. This scenario can be particularly effective for the Procurement department as it directly ties into their daily responsibilities and challenges, making the attack relevant and engaging.

Observation 4. Attack scenarios involved different internal and external stakeholders, ranging from trusted suppliers, service providers, customs, shipping agencies, freight forwarder, technology partners, and research organizations. The diversity of stakeholders demonstrates the dimensions of the attack surface and the importance to communicate this aspect to the workforce; the aim is to empower the workforce to understand the plausibility to become a target, and that cybercriminals will try to leverage the business relationships of the company with external stakeholders.

Observation 5. A variety of attack scenarios are suggested that create a sense of urgency and fear, conveying that if the employee does not act, that could significantly impact the company's operations. Some other scenarios appear to be from maritime authorities creating a sense of responsibility to act quickly.

As it was observed, the use of email was considered across all proposed phishing scenarios. Moving on with the investigations, efforts focused on examining whether the tool can suggest more advanced scenarios. A prompt was crafted instructing the tool to "*consider the scenario related to Shipping & Logistics department and amend it so the phone is also used as part of the attack*" (prompt #21). In this case, the tool considered that the Shipping & Logistics department handles the intricate process of shipping and customs clearance and proposed an attack scenario that was broken into two phases. Phase 1 involved the use of email to deliver an urgent message with the subject "*Urgent Customs Clearance Action Needed for Shipment ID #12345*". The tool suggested to state that there is an issue with customs clearance for a specific shipment, possibly due to missing or incorrect documentation. As part of the attack scenario, a link was provided, allegedly to the customs portal for preliminary information entry, also mentioning that a representative will call shortly to assist with resolving the issue. Phase 2 involved the use of phone and suggested that the attack could involve a call to the department from an individual claiming to be a representative of the customs agency. The scenario assumes that this person references the email and shipment ID, creating a sense of continuity and legitimacy; the person calling urges the employee to follow the email's instructions immediately to avoid shipment delays. This revised scenario addresses a more sophisticated social engineering tactic, adding credibility to the request and enhancing the realism of the attack scenario for the Shipping & Logistics department. This is achieved by incorporating a phone call into the phishing attempt, in combination with the caller's knowledge of the email and specific shipment details.

The ability of the tool to create more sophisticated attacks was further investigated to identify the level of creativity that the tool could demonstrate to suggest scenarios that were realistic and linked to typical operations performed by the targeted department(s). The tool was prompt to "*create a more complicate plausible phishing scenario that involves different departments. The use of email and/or phone can be utilized.*" (prompt #22). The proposed phishing scenario involved multiple departments at maritime-FLE, including Procurement, Shipping & Logistics, and IT & Web Development, exploiting the interconnected nature of their operations. The attack scenario was broken into three phases. The first phase assumed infiltration through the Procurement department. Initially, the scenario describes that the Procurement department receives an email that appears to be from a trusted supplier, announcing a new online ordering system. The email includes a link to register on this new platform. Then a subsequent phone call from someone claiming to be from the supplier's customer service team is made to the Procurement department, referencing the email and offering assistance with the registration process. The tool assumes that phase 1 is successful and the attack is expanded to the

Shipping & Logistics department. Once the Procurement department's credentials are compromised, attackers can gain access to upcoming shipment schedules. They can then send an email to the Shipping & Logistics department, masquerading as the Procurement department, informing them of a change in shipment details and providing a link to view the updated information. A phone call from the 'Procurement Department' is made to Shipping & Logistics, urging them to check the email as it contains critical information about urgent shipment changes. Phase 3 targets the IT & Web Development department. Using information from the previous breaches, attackers send an email to the IT & Web Development department, posing as a senior executive from Shipping & Logistics. They claim there is an issue with the internal tracking system affecting shipments and urge the IT team to install a software patch, provided in the email link, to resolve the issue immediately. Overall, this scenario highlights the complexity of phishing attacks in a large organization and the importance of vigilance across all departments. By demonstrating how attackers can maneuver through different layers of the company, it underscores the need for comprehensive security practices and protocols.

Further examination of the last scenario revealed a weak point in phase 3. The IT & Web development department is handling technological and cybersecurity issues. Thus, it is reasonable to assume that the respective employees are typically more aware of common phishing tactics. Any phishing scenario crafted for them needs to be sophisticated and highly believable; the suggested scenario (phase 3) lacks these attributes. A new prompt was created to request the tool to "*create a phishing scenario for the Information Technology and Web Development department of maritime-FLE. Consider that employees in this department have more advanced knowledge and will not fall easily for typical phishing lures.*" (prompt #23). The tool suggested a new scenario that involved the IT & Web Development department. As per the tool's suggestion, department members receive an email that appears to be from a reputable cybersecurity firm or a well-known software vendor. The email discusses a newly discovered and critical vulnerability affecting a specific software or system that maritime-FLE uses. Considering the employees' expertise, the email is technically detailed, mentioning specific code libraries, platforms, or software versions used by maritime-FLE. It offers an immediate solution to this vulnerability – a patch or an update, which can be accessed by clicking on a link. The email is crafted to mimic the vendor's usual communication style and includes technical jargon to make it more convincing. This scenario acknowledges the advanced technical knowledge of the IT & Web Development department and suggested a sophisticated, technically plausible phishing attempt, which can be utilized in activities to ensuring that the training is engaging and effective.

6 Discussion

Designing tailored social engineering attack scenarios to inform awareness raising and training initiatives requires good understanding of the business environment, its operations, structure and relevant job roles and responsibilities of personnel across the different departments. Also, it requires a lot of effort and a great level of creativity from the educators and trainers to design diverse attack scenarios and expose the workforce to different situations to enhance their skills and knowledge and empower them to become resilient when they have been targeted. The explorations performed in this study have indicated that generative AI tools have the potential to assist educators and trainers by suggesting tailored attack scenarios based on a business environment. Having assistance from a generative AI tool can prove to be invaluable for upskilling initiatives as it can accelerate the process of creating learning content and contribute to designing engaging and effective learning activities. Below we discuss the aspects that demonstrate ChatGPT's ability to assist in the creation of tailored social engineering attack scenarios.

Relevance to Different Departments/Operations. The suggested phishing attack scenarios are customized based on the typical operations delivered by the respective departments. The tool expanded upon the brief information that was initially provided about the business environment and considered routine operations that are reasonable to be performed by the departments that have been profiled. This means that the suggested scenarios should be validated by trainers to confirm that the attack context would be relevant to the business environment in which learning activities will be delivered. Having the attack training scenarios tailored to daily operations can engage people and assist them to easily relate with the attack storyline and understand how attacks can be implemented in the context of their daily routine.

Realism and Plausibility. The tool demonstrated that it could suggest attack scenarios that are realistic and plausible. This is achieved by creating attack scenarios that are tailored to exploit the routine operations and potential concerns of different departments. Also, the combination of different attack vectors (phone, email) and the caller's knowledge of prior (email) communication can create a sense of authenticity and add credibility to the presented (malicious) requests. Another element that adds to the realism of the suggested attack scenarios is that they consider the cooperation with a range of stakeholders (e.g. suppliers, customs, shipping agencies, freight forwarders, technology partners, etc.) that the victim organization is possible to have established a trusted collaboration with. Utilizing realistic and plausible attack training scenarios is crucial to effectively upskill employees and enhance their resilience to diverse phishing attacks that are tailored to the business environment.

Psychological Manipulation. Social engineers manipulate people's feelings to achieve their objectives. Thus, the attack training scenarios should demonstrate how a social engineer can take benefit of human nature and manipulate different psychological attributes. The suggested phishing attack scenarios considered daily responsibilities and concerns that employees might have in the context of their work role to convince them to act, e.g., open a malicious attachment, click on a link, enter sensitive information on a fake website, etc. Influence tactics demonstrated through the suggested scenarios include creating a sense of urgency, fear, authority, and responsibility. These are tactics that have proved to be a driving factor for victims to act and allow the attackers to gain unauthorized access. Depending on an employee's job role, individuals might be more susceptible to responding to a request made by a social engineer. Therefore, it is imperative to demonstrate how a social engineer could take advantage of the business structure and collaborations to create the conditions to convey a sense of urgency, fear, authority, etc. Empowering the workforce to enhance its situational awareness could increase their resilience against sophisticated phishing attacks that might not be expected to happen.

Sophistication. Social engineers are creative in terms of the lures they use. Training scenarios should demonstrate similar creativity so that employees realize the extent that attackers might take to achieve their objectives. This is an aspect that was demonstrated by the tool; initially, phishing attack scenarios primarily utilized email communication. When prompted, the tool adjusted the scenarios and created more sophisticated attacks. For example, it combined the use of email and phone to create a multilayered sense of urgency and authenticity. In another case, it demonstrated that it could suggest attack scenarios aligned with the skill level and experience of the targeted department. Specifically, it considered the IT & Web development department in which employees have technical expertise and suggested more sophisticated attack scenarios. Such scenarios are vital to train more experienced personnel to identify more complex social engineering attempts.

This study presented an initial set of investigations performed in the context of the maritime domain. Authors considered that the study findings provide the ground to extend the investigations to include other forms of social engineering attacks; also, to consider other domains and investigate the level of creativity and adaptability demonstrated by generative AI tools. Future investigations will focus on extensively assessing how generative AI tools can assist educators and trainers design tailored attack scenarios that could be utilized to effectively educate and train the workforce; the aim should be the workforce to realize the extent a social engineer would operate to manipulate people and compromise a business. Moreover, another future direction is to upskill cybersecurity educators and trainers; future investigations should focus on investigating the skills educators and trainers should develop so they can leverage generative AI in the context of their activities.

7 Conclusions

Generative AI has transformed the cyber threat landscape and provided the means to cybercriminals to thrive with tailored social engineering attacks. This is an aspect that could not be evident to the workforce who may not easily realize how a social engineering attack can be transformed depending on the domain the victim organization is operating. This lack of understanding may explain why employees often fall for the phish even if they attended a training. Upskilling initiatives should leverage generative AI to accelerate the process of learning content creation by creating tailored and sophisticated social engineering attack scenarios that could be delivered in a specific domain. Exposing the workforce to advanced attack scenarios, which can resemble generative-AI attack strategies that cybercriminals could be leveraging, can promote a better understanding of how social engineering attacks could be delivered in their working environment, can be engaging in terms of learning and retaining knowledge, and can enhance the workforce's cyber situational awareness. Cyber situational awareness is pivotal for the workforce to become cyber resilient when it becomes a target of a social engineering attack. Future awareness raising and training endeavors should investigate how generative AI can be leveraged to improve the workforce's cyber situational awareness and contribute to a cyber-resilient society.

Acknowledgments. This paper has received funding from the Digital Europe Programme (DIGITAL) under grant agreement project no. 101128049 - SecAwarenessTruss. The work reflects only the authors' view, and the Agency is not responsible for any use that may be made of the information it contains.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Venkatesha, S., Reddy, K., Chandavarkar, B.: Social engineering attacks during the COVID-19 pandemic. SN Comput. Sci. (2021)
2. ENISA: ENISA Threat Landscape 2023 (2023). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
3. SlashNext: The State of Phishing 2023 (2024). https://slashnext.com/wp-content/uploads/2023/10/SlashNext-The-State-of-Phishing-Report-2023.pdf
4. cybersecuritymonth.eu: European Cyber Security Month (2023). https://cybersecuritymonth.eu/
5. Piki, A., Stavrou, E., Procopiou, A., Demosthenous, A.: Fostering cybersecurity awareness and skills development through digital game-based learning. In: 10th International Conference on Behavioural and Social Computing (BESC), Larnaca (2023)
6. Smith, A., Papadaki, M., Furnell, S.M.: Improving awareness of social engineering attacks. In: Dodge, R.C., Futcher, L. (eds.) Information Assurance and Security Education and Training. IAICT, vol. 406, pp. 249–256. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39377-8_29
7. Aldawood, H., Skinner, G.: Reviewing cyber security social engineering training and awareness programs - pitfalls and ongoing issues. Future Internet (2019)
8. Stavrou, E.: Back to basics: towards building societal resilience against a cyber pandemic. J. Syst. Cybern. Inf. (JSCI), 73–80 (2020)
9. Microsoft: Microsoft Digital Defense Report - Building and improving cyber resilience (2023). https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
10. Nah, F.F.-H., Zheng, R., Cai, J., Siau, K., Chen, L.: Generative AI and ChatGPT: applications, challenges, and AI-human collaboration. J. Inf. Technol. Case Appl. Res., 277–304 (2023)
11. Charalambous, A., Stavrou, E.: Building societal resilience against social engineering attacks: unleashing the power of instructional design and microtargeting. In: 16th Annual International Conference of Education, Research and Innovation (ICERI), Seville (2023)
12. Aldawood, H.: A policy framework to prevent social engineering. In: 3rd International Conference Middle East and North Africa Conference of Information System, Casablanca (2020)
13. WEF: The Cyber Resilience Index: Advancing Organizational Cyber Resilience (2022). https://www3.weforum.org/docs/WEF_Cyber_Resilience_Index_2022.pdf
14. Hulatt, D., Stavrou, E.: The development of a multidisciplinary cybersecurity workforce: an investigation. In: 17th International Symposium on Human Aspects of Information Security & Assurance (HAISA), Kent (2021)
15. Potamos, G., Theodoulou, S., Stavrou, E., Stavrou, S.: Maritime cyber threats detection framework: building capabilities. In: Drevin, L., Miloslavskaya, N., Leung, W.S., von Solms, S. (eds.) WISE 2022. IFIP Advances in Information and Communication Technology, vol. 650, pp. 107–129. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-08172-9_8

16. Potamos, G., Theodoulou, S., Stavrou, E., Stavrou, S.: Building maritime cybersecurity capacity against ransomware attacks. In: Onwubiko, C., et al. (eds.) International Conference on Cybersecurity, Situational Awareness and Social Media, pp. 87–101. Springer, Singapore (2023). https://doi.org/10.1007/978-981-19-6414-5_6
17. Kallonas, C., Piki, A., Stavrou, E.: Empowering professionals: a generative AI approach to personalized cybersecurity learning. In: IEEE Global Engineering Education Conference 2024, Kos (2024)
18. NIST: NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments (2012). https://csrc.nist.gov/pubs/sp/800/30/r1/final
19. Gutterman, A.S.: Designing the organizational structure. In: SSRN (2023)
20. CompassAir: Part 2 – Stakeholders (2024). https://mycompassair.com/part-2-stakeholders/. Accessed 10 Feb 2024