Master thesis

Project 2:
Better understand the victims of GenAI-enabled fraud and the imitated organizations

Defending Against GenAI-Driven Fraud: The Role of Employee Awareness and Corporate Cybersecurity Training

Radboud University

Word count: 12.717

First examiner: Sidaoui, K
Second examiner: Weeterings, I.W.A.

11-06-2025

Nijmegen School of Management

Preface

I am pleased to present to you my master thesis, a project that marks the ending of my academic journey at Radboud University. Over the past four academic years, I have gained valuable knowledge, insights, and experiences in the field of Business Administration. These past few months have been a reflection of this growth along the way and just like the overall journey, this thesis process came with its challenges.

I would like to express my sincere gratitude to my supervisors, Dr. Karim Sidaoui and Ilona Weeterings, for their pleasant and supportive guidance. I always appreciated our meetings for their informal and comfortable atmosphere. You gave me the feedback and encouragement that I needed to stay on the right track.

I would also like to thank the financial institution involved in this research for generously making time to support me in my work. Your enthusiasm and willingness to help were instrumental in collecting valuable data in such an interesting domain that would otherwise have been difficult to obtain.

Finally, I would like to thank my family and friends for standing by me whenever I needed it. The distractions provided by my friends after a long day of work helped to ease the pressure. And my family, who's constant support gave me strength during the tougher moments. Whether it was letting me rant about my issues or providing feedback on my work, your help was really appreciated.

Abstract

The rise of generative AI (GenAI) is putting more pressure on the cybersecurity environment of organizations as practices such as advanced phishing, deepfake scams, and AI-generated malware are growing. This study explores how GenAI-driven fraud impacts employee cybersecurity awareness and the effectiveness of cybersecurity training in mitigating such threats. Through a qualitative case research approach with eleven semi-structured interviews from a major financial institution, this research identifies a gap in the perceived and actual awareness, revealing an "illusion of awareness", among employees. Although the organization prioritizes cybersecurity training, mostly static and generic, it fails to actively warn and incorporate the risks of GenAI-specific threats. Emotional vulnerability, overreliance on technology, and unstimulating training methods are factors influencing this issue. Findings suggest that cybersecurity training serves as a partial mediator to help bridge the gap between GenAI-related threats and employee awareness. But it falls short on preparing employees emotionally and behaviourally for sophisticated attacks. This study encourages a more dynamic and interactive training approach, strong leadership involvement, and clear communication channels. By connecting theory and practice, this research contributes on the most recent developments on GenAI-related fraud and current cybersecurity initiatives and employee awareness through a real-life case study.

Table of contents

1. Introduction

Artificial intelligence (AI) has been a hot topic in recent years as both usage and quality of the technology have increased dramatically. With the emergence of deep learning (DL), highly efficient models that can learn and make decisions autonomously based on fed data, AI is now capable of outperforming humans in most cognitive tasks, ranging from data interpretation and pattern recognition to content generation (Buxmann, Hess & Thatcher, 2021). AI has become increasingly integrated into everyday life, as seen in smart home systems, search machines, autonomous vehicles, phone software, or even farming equipment (European Parliament, 2020). Adoption of these tools are not just for personal use, as organizations across sectors invest in AI to gain competitive advantages and improve performance (Venkatesh, 2022). Primary functionalities include process automation, optimized decision-making, and personalized customer experiences (Schreiber & Schreiber, 2024). Falling behind in AI adoption may now even be a disadvantage, as firms implementing AI can achieve performance levels 3.8 times higher than the laggards (Lawler, D'Silva & Arora, 2025). Such companies build differentiated capabilities with compounding effects, ultimately increasing their performance advantage (Lawler et al., 2025). The McKinsey Global Institute predicts that AI's contribution to business processes will add $13 USD trillion in value by 2030 (Bughin, Seong, Manyika, Chui & Joshi, 2018).

Despite these advantages, concerns grow on ethics, data privacy, and malicious intentions. Especially the rise of generative AI (GenAI) has introduced new and complex cybersecurity risks (Schreiber & Schreiber, 2024). "GenAI is an unsupervised or partially supervised DL machine framework which generates manmade relics such as images, text, audio, or video by examining training examples" (Baidoo-anu & Ansah, 2023, p.53). DL technology is able to generate human-like text, deepfake audio and video, or create software code (Gupta, Akiri, Aryal, Parker & Praharaj, 2023; Schreiber & Schreiber, 2024). As a result, GenAI presents a double-edged sword, as both recreational users and fraudsters are able to benefit from its versatile applications. Besides the fun and harmless possibilities of GenAI, users are also able to create manipulative, deceiving, and harmful output for cyberattacks (Caldwell, Andrews, Tanay & Griffin, 2020). "Cyberattacks are digital malicious attempts to steal, damage, or intrude into the personal or organizational confidential data (Basit et al., 2021, p.140). These threats are becoming more advanced and frequent, and experts expect GenAI will lead to a significant rise in fraudulent behaviours (U.S. Department of the Treasury, 2024). Deloitte's Center for Financial Services (2024) estimates that GenAI related fraud losses in the

U.S. alone could reach $40 USD billion by 2027. Beyond financial losses, successful fraud can expose sensitive information and damage an organization's reputation (Hijji & Alam, 2022; Schreiber & Schreiber, 2024). This makes cybersecurity training programs more important than ever, as organizations look to protect their assets through employee education and secure digital networks. Cybersecurity programs are the essential pillars needed for the education of employees about digital threats and promoting a secure data network within the organization (Schreiber & Schreiber, 2024). Keeping the organization secure is dependent on the level of awareness and the sense of personal responsibility (Reegård, Blackett & Katta, 2019).

Although previous research has predominantly focused on the technical attributes of cybersecurity, the human factor remains undervalued (Huang & Pearlson, 2019; Kadel et al., 2022). Organizations are acknowledging the importance of cybersecurity education among employees as it only takes one incident to jeopardize a company's assets (Huang & Pearlson, 2019). Awareness initiatives are essential for equipping employees with the most recent knowledge on cyberattacks and attack strategies (Hijji & Alam, 2022). Yet, academic literature rarely addresses GenAI as a tool to commit fraud. While companies recognize the need to educate their workforce, the extent to which GenAI-specific threats are incorporated into cybersecurity programs varies widely (Schreiber & Schreiber, 2024). This study aims to bridge this gap by exploring how GenAI impacts employee awareness within organizations. Specifically, it explores how the role of cybersecurity training functions as a mediating role in this relationship through a case study on a major financial institution. It seeks to uncover the developments of such trainings and awareness among employees on GenAI-related risks. Adding on, rather than viewing GenAI-driven fraud as a static phenomenon, this study conceptualizes it as an evolving threat, growing in both sophistication and frequency as perceived by employees. This goal is transferred into the following research question:

How does evolving GenAI fraud influence corporate cybersecurity training developments and employee awareness, and how does corporate cybersecurity training mediate the relationship between GenAI fraud and employee awareness?

As cybercriminals increasingly deploy GenAI to create sophisticated phishing campaigns, deepfake scams, and AI-generated malware (Gupta et al., 2023; Salem, Azzam, Emam & Abohany, 2024), individuals and organizations face increasing risks of financial and reputational loss (Lalchand, Srinivas, Maggiore & Henderson, 2024). It is essential for organizations and its managers to be aware of GenAI threats and to ensure cybersecurity

training incorporates current developments. Unfortunately, research on the topic is scarce and lag behind on the matter. Despite the increasing frequency of GenAI-powered attacks, research indicates that many cybersecurity programs have yet to incorporate GenAI fraud awareness into their curricula (Schreiber & Schreiber, 2024). This research offers insights that can help managers understand employee thinking and behaviour related to GenAI threats in order to better protect company assets and shaping of cybersecurity trainings.

From an academic standpoint, this study contributes to the growing literature on cybersecurity awareness and training by incorporating the risks of GenAI supported fraud. As Schreiber and Schreiber (2024) mention, many of these threats remain poorly understood. By investigating the correlation between GenAI fraud, employee awareness, and cybersecurity training through a real-world case study, this research adds valuable information about the current understanding and measurements being taken in the private sector. Doing so it aims to connect both theory and practice, linking cybersecurity, GenAI fraud, and employee awareness behaviour, and ensuring extension of current academic literature.

2. Literature review

2.1 GenAI and fraud

AI has progressed significantly, moving from early rule-based systems to machine learning (ML), where computers learn from data rather than relying on predefined instructions (Aggarwal, Mijwil, Sonia, Al-Mistarehi & Alomari, 2022; Schreiber & Schreiber, 2024). ML enables pattern recognition and autonomous prediction, revolutionizing AI capabilities (Brynjolfsson, Li & Raymond, 2025). DL revitalized AI by mimicking the human brain through artificial neural networks with multiple layers (Samek, Montavon, Lapuschkin, Anders & Müller, 2021). Its efficiency in processing large datasets allows it to outperform humans in cognitive tasks such as image and speech recognition (Aggarwal et al., 2022). The latest AI advancement is GenAI, which differs from ML and DL by creating original content - text, images, music, and video - rather than making predictions (Schreiber & Schreiber, 2024). Using unsupervised or partially supervised learning, GenAI analyses data to generate human-like outputs without needing specific instructions (Chan & Lee, 2023; Goodfellow et al., 2020). GenAI is closely linked to large language models, which predict word sequences and are now increasingly handling multimodal inputs, allowing them to process audio and images alongside text (Brynjolfsson et al., 2025; Schreiber & Schreiber, 2024).

While GenAI can take on many support tools in different settings to aid users, there is an increasing trend in its use with ill-intended purposes (Lalchand et al., 2024). Specifically, the effect it has on corporate cybersecurity. AI has introduced a paradigm shift in both the capabilities of cybersecurity defence mechanisms and the sophistication of cyberattacks (Gupta et al., 2023). Especially the latter has grown in relevance as GenAI enables the mass creation of personalized, grammatically flawless messages, making fraud harder to detect (Schmitt & Flechais, 2024). The main purpose of such attacks are to spread misinformation, disrupt operations, steal data, or anything financial valuable (Uma & Padmavathi, 2013).

While AI-powered security tools can detect deviations, automate responses, and improve data protection, cybercriminals are now also leveraging GenAI to scale and refine their attacks (Familoni, 2024; Salem et al., 2024; Schreiber & Schreiber, 2024). Bypassing ethical boundaries of GenAI models through clever framing or using unregulated GenAI models enables cybercriminals to create convincing human-like text, voice, images, or video content for malevolent purposes (Baidoo-anu & Ansah, 2023). Deepfake technology, for example, has been used for impersonation scams, where attackers convincingly mimic the voice and/or appearance to manipulate others into transferring funds or sharing confidential data (Lalchand

et al., 2024). The well-known incident of a Hong-Kong banker transferring $25 million dollars to a scammer impersonating his chief financial officer in a video-call (Magramo, 2024) proves the effectiveness of a well-coordinated cyberattack. Moreover, GenAI-powered phishing campaigns have also become more effective, often bypassing traditional spam filters and exploiting psychological vulnerabilities (Gupta et al., 2023). These attacks predominantly employ social engineering tactics, where the weakest link is targeted, humans, due to their behavioural characteristics (Metalidou et al., 2014).

Indeed, research confirms that many cybersecurity incidents can be attributed to negligence, carelessness, or human error in organizational cybersecurity policies (Alshaikh, 2020; Alsharida, Al-rimy, Al-Emran & Zainal, 2023; Ansari, 2022; da Veiga, Astakhova, Botha & Herselman, 2020; Jeong, Mihelcic, Oliver & Rudolph, 2019; Metalidou et al., 2014). As a result, creating a secure organizational culture through awareness and individual responsibility is critical (Hijji & Alam, 2022; Reegård et al., 2019). Hence, organizations and its employees must stay informed about current threats and invest in training programs to help employees recognize and respond to modern cyberattack methods, especially those powered by GenAI (Hijji & Alam, 2022; Schreiber & Schreiber, 2024).

2.2 Employee cybersecurity awareness

Cybersecurity awareness is a critical component of an organization's defence strategy, ensuring employees can recognize and respond to cyber threats effectively. While technological defences like firewalls and encryption provide basic protection, the human factor remains a major vulnerability (Alshaikh, 2020). Research constantly shows how many cyber incidents result from human error, negligence, or lack of awareness rather than technological failures (Metalidou et al., 2014).

Although awareness lacks a single, universal definition due to its varied use across disciplines, cybersecurity literature typically frames it as an antecedent of cybersecurity-compliant behaviour (e.g. strong passwords), guidance on designing awareness programs, and identifying influential factors that influence the implementation of cybersecurity awareness (Tsohou, Karyda, Kokolakis & Kioutouzis, 2015). Since this study focuses on how GenAI-driven fraud affects individual employee awareness, a less technical and more behavioural approach is needed. Technology is often mistakenly treated as the immediate solution to cybersecurity issues (Reegård et al., 2019). Due to the constant changes and complexity of the concept, technological countermeasures alone are rarely enough to protect users from online threats (Zhang-Kennedy & Chiasson, 2022). Traditionally seen as an IT concern, cybersecurity

is increasingly recognized as an organization-wide responsibility that requires training and awareness at all levels (Reegård et al., 2019).

The human factor has shown to be the main cause of corporate cyber breaches. However, users engaging in online activities tend to share varying and unequal levels of cybersecurity awareness (Shaw, Chen, Harris & Huang, 2009). This has led to researchers adopting a more social-psychological approach to understand user behaviour. Kruger and Kearney (2006) followed this path and proposed that awareness has three components: affect (emotions), behaviour (intentions), and cognition (beliefs). These translate into three equivalent dimensions: the emotional response toward threats (attitude), understanding threats, risks, and best practices (knowledge), and the perception, and the ability and willingness to act in a security-conscious way (behaviour). Deriving from this, cybersecurity awareness can be defined "the degree of users' understanding about the importance of cybersecurity, and their responsibilities to exercise sufficient levels of information control to protect the organization's data and networks" (Rahim, Hamid, Kiah, Shamshirband & Furnell, 2015, p. 607). The following sections explore these three dimensions in greater detail.

2.2.1 Attitude in Cybersecurity Awareness

Attitude is a key factor in determining whether individuals take cybersecurity seriously and follow best practices. Employees who view cybersecurity measures as burdensome or unnecessary are significantly less likely to comply, increasing the organization's vulnerability, especially to social engineering attacks (Reegård et al., 2019; Shaw et al., 2009). In contrast, a positive attitude is a strong predictor for long-term secure behaviour (Thomson & von Solms, 1998). Employees must perceive security practices as important and personally relevant, rather than as an external IT requirement being pushed (Bulgurcu, Cavusoglu & Benbasat, 2010). Organizational strategies, such as incentive-based training, leadership reinforcement, and cultural integration, can help reshape cybersecurity attitudes, improving compliance and vigilance (Reeves et al., 2021). Beyond organizational influence, moral responsibility also shapes attitudes. Siponen (2000) argues that employees must internalize cybersecurity guidelines as ethically necessary actions, rather than seeing them as rules imposed by management. Without this intrinsic motivation, even informed employees may disregard security policies. Kannelønning and Katsikas (2023) state how in such a scenario it is important to consider why the situation exists and what can be done about it, indicating how this is often the repercussion of cybersecurity not fully being understood, accepted, or practiced. Similarly, Bulgurcu et al. (2010) discuss how employee cybersecurity policy adoption is shaped by threat

and coping appraisal processes, in which the employee evaluates these threats as a mean to cope with them. As appraisal requires a certain base frame of reference, it can be said that this relates back to the amount of knowledge someone possesses about cybersecurity threats.

2.2.2 Knowledge in Cybersecurity Awareness

Rahim et al. (2015) identify two major roles in cybersecurity awareness programmes: alerting individuals to potential threats and enhancing the understanding of cyber threats to encourage secure online behaviour. Chaudhary (2024) expands on this, stating how cybersecurity awareness is based on understanding this threat, understanding its consequences, and adopting the right attitude to translate knowledge into action. Knowledge is the foundation of cybersecurity awareness and includes an individual's understanding of threats, attack strategies, and preventive measures (Chaudhary, 2024; Rahim et al., 2015; Shaw et al., 2009). A certain level of understanding about the roots of the issue at hand is thus critical to incentivize desired behaviour on data protection. Without sufficient knowledge, employees are unable to recognize threats or take appropriate countermeasures. However, knowledge alone is insufficient, as without awareness of threats, employees are unlikely to behave accordingly (Shaw et al., 2009). For example, a low level of awareness behaviour includes not paying attention or ignoring security alerts. Such users are often careless when it comes to handling personal and confidential information and Shaw et al. (2009) state how this can be attributed to insufficient knowledge on technological factors (e.g. software, hardware, and network) and personal technical skills.

2.2.3 Behaviour in Cybersecurity Awareness

Behaviour in cybersecurity awareness refers to how employees translate their knowledge and attitudes into secure actions. While many employees may understand cybersecurity risks, research shows that awareness alone does not guarantee compliance (Gcaza & Von Solms, 2017). Secure behaviour includes practices such as using strong passwords, verifying sources, reporting suspicious activity, and following company security policies (Shaw et al., 2009). Behaviour represents the actual application of security practices (Kruger & Kearney, 2006). Employees who see security measures as inconvenient are less likely to adopt them, even if they are aware of their importance (Reegård et al., 2019). While awareness includes understanding risks, true cybersecurity effectiveness depends on whether individuals translate that awareness into consistent, security-conscious behaviour (Gcaza & Von Solms, 2017).

Cybersecurity awareness is a multifaceted concept consisting of attitude, behaviour, and knowledge. While attitude determines how employees perceive security measures, behaviour determines whether they act securely, and knowledge forms the foundation of informed decision-making. Research shows that awareness alone is not enough and that organizations must focus on behavioural reinforcement and cultural integration to ensure that cybersecurity practices become ingrained in workplace habits (Reegård et al., 2019; Shaw et al., 2009). With the rise of GenAI-powered fraud, awareness programs must evolve to address emerging threats. Despite this growing risk, many have yet to incorporate GenAI fraud awareness into their curricula (Schreiber & Schreiber, 2024).

2.3 Corporate cybersecurity training

Cybersecurity training has become an essential component of organizational risk management as businesses increasingly rely on digital infrastructure to store sensitive data, manage operations, and engage with customers (Alshaikh, 2020; Reegård et al., 2019). Traditional training methods have primarily focused on technical defences, such as firewalls, encryption, and recognizing suspicious links and emails (da Veiga et al., 2020). However, with the rise of social engineering tactics and GenAI-driven fraud, a shift toward human-centered training approaches has become necessary (Basit et al., 2021). Chief executive security officer at Liberty Mutual, a major insurance company, explains the essence of cybersecurity: “It only takes one mistake from an employee clicking a wrong link or email to erase all the good work done by our professionals” (Huang & Pearlson, 2019, p.6398).

Cybersecurity training refers to structured educational programs designed to improve employees' awareness, knowledge, and practices regarding digital threats (Alshaikh, Maynard, Ahmad & Chang, 2018; Huang & Pearlson, 2019). Rahim et al. (2015) note that cybersecurity training aims to (1) alert individuals to cybersecurity threats and (2) enhance their understanding to adopt secure behaviour. Training methods range from classroom-based learning and group discussions to gamified simulations, newsletters, poster campaigns, and computer-based modules (Stefaniuk, 2020; Zhang-Kennedy & Chiasson, 2022). Directing such initiatives towards appropriate recipients in a swift and effective way is essential to a proper raising of cybersecurity awareness (Stefaniuk, 2020).

Especially the computer-based training method has seen an uprise in popularity. Gamification, simulations, and video-based learning have proven effective in engaging employees and reinforcing practical understanding (Schreiber & Schreiber, 2024). Given the widespread success of phishing, pretexting, and baiting techniques, continuous education has

become essential (Basit et al., 2021). Organizations that invest in cybersecurity training not only enhance their overall cyber resilience but also create a workforce that is more vigilant and capable of identifying threats (Familoni, 2024). A higher level of cyber fraud threat resilience leads to noticeable improvements in ability, knowledge, attitude, and behaviour in (Zwilling et al., 2022).

The evolving nature of GenAI cyber threats demands a dynamic approach to corporate cybersecurity training. Static training formats such as e-learnings and periodic workshops may be insufficient for employees to combat AI-enhanced fraud (Ansari, 2022; Grover, Broll & Babb, 2023). The problem with static one-way methods is the absence to test somebody's understanding in practice (Furnell, Gennatou & Dowland, 2002). Testing and practising in a controlled setting is preferred as mistakes can be made and learned from without jeopardizing the organization's system (Furnell et al., 2002). Organizations must adopt adaptive learning models that integrate real-time threat simulations to ensure employees remain aware of emerging risks (Schreiber & Schreiber, 2024). Moreover, training programs should include real-world examples to enhance understanding and retention (Hijji & Alam, 2022). A shift towards interactive, scenario-based training is needed to improve employees' ability to recognize and respond to emerging threats (Ansari, 2022). Employees must be taught to identify phishing attempts, recognize deepfake scams, and understand how GenAI-driven fraud operates (Schreiber & Schreiber, 2024). Cybersecurity training research suggest that incorporating AI-driven simulations, where employees engage with AI-generated phishing emails for example, can significantly improve preparedness (Sarker, Furhad & Nowrozy, 2021). Furthermore, AI-powered threat detection tools can personalize training programs based on employees' risk profiles and behavioural patterns (Gupta et al., 2023). Training must also be tailored to sector-specific risks, as industries like finance face higher exposure to GenAI-enabled threats such as deep-fake scams and automated phishing (Lalchand et al., 2024).
To stay effective, training programs should be updated regularly in line the most recent fraud technique developments (Salem et al., 2024).

A strong cybersecurity culture is vital for the success of training programs. Organizations that foster a culture where employees feel personally responsible for security tend to experience fewer security breaches (Reegård et al., 2019). Cybersecurity culture is shaped by continuous training, leadership support, and an organizational commitment to security policies (Alshaikh, 2020). Studies indicate that employees are more likely to adhere to security protocols when

they observe management actively participating in cybersecurity initiatives (Familoni, 2024). Hence, cybersecurity training and awareness are closely interlinked. While awareness focuses on informing employee about risks, training equips them with the skills to respond. Chaudhary (2024) stresses how both need to be present to ensure behavioural change. In 2021, most of the digital fraud attempts were a result of a lack of awareness and training on such attacks has proven to be an effective strategy (Ansari, 2022). Employee awareness and cybersecurity training on fraud threats are thus of significant importance to a company's security. It is therefore of importance to examine the emerging effects and associated risks of GenAI on these elements.

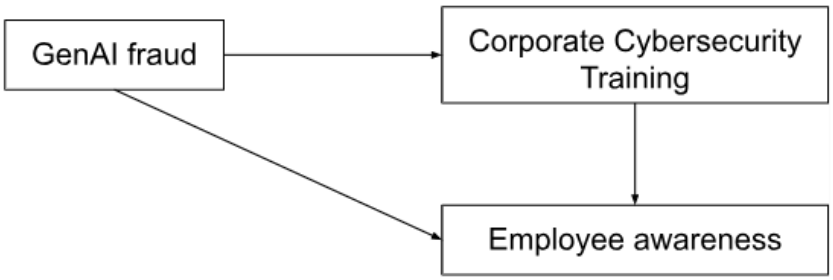

Figure 1: Conceptual model

3. Methodology

3.1 Research design

The goal of this study is to explore how the rise of GenAI fraud influences the development of corporate cybersecurity training and how this relates to employee awareness. To gain deep insight into individual perspectives on cybersecurity programs, a qualitative approach is employed, which is particularly suitable to capture personal experiences and meanings (Hammarberg, Krikman & de Lacey, 2016).

The study adopts an interpretivist paradigm, which focuses on understanding social phenomena through the subjective experience of individuals (Creswell & Poth, 2016). The research seeks to uncover how employees perceive and respond to GenAI-driven fraud and cybersecurity training in their specific organizational context. Continuing, this research has adopted a constructivist approach, which holds that knowledge is co-constructed between the researcher and participants (Creswell & Poth, 2016). Rather than seeking objective truths, this study explores how participants make sense of cybersecurity risks and incorporate training efforts in the context off emerging GenAI threats. Reality is viewed as subjective and shaped by the personal believes and language of the participant. An abductive reasoning approach

guides the research process, moving iteratively between theory and empirical data (Vennix, 2019). Initial theoretical frameworks on cybersecurity awareness and training informed the interviews design, while insights from the data helped refine these frameworks throughout the analysis later on.

Data has been collected through semi-structured interviews with employees of a major financial institution. Qualitative interviews attempt to gather comprehensive information about a participant's personal experience through open questions that aim to understand his/her opinions, motivation, and understanding of a certain phenomenon (Flick, 2018). Semi-structured interviews enable partial control through prepared questions and flexibility with participants being able to speak freely and ask follow-up questions if desired. This approach is suitable, compared to quantitative research, for capturing nuanced views and contextual insights (Lewis, 2015), aligning well with this research's aim to understand how employees experience GenAI threats and cybersecurity training methods.

3.2 Sampling

A major financial institution has served as a case study for this research on GenAI fraud and its impact on employee awareness and cybersecurity training. The company agreed to participate by allowing interviews with employees without imposing content restriction. However, complete access is subjective as it does not mean that every employee was reachable (e.g. too busy, unaware of their existence in the company, or unwilling to participate). The choice of language can affect the linguistical dynamics in interviews and cause issues in translation, interpretation, and even group ambience (Marschan-Piekkari & Reis, 2004). As all participants carry the Dutch nationality and were fluent, it was therefore decided to conduct all interviews in Dutch to ensure clarity and comfort.

This research is one of four under the overarching research on the effects of GenAI-related fraud, each with a distinct angle and research question. A collaborative approach was adopted in the data collection phase by designing and using a shared interview guideline that covered all relevant topics. This method allowed to reduce the preparatory workload, maintain interview quality, and expand the research on finding additional interviews. A shared interview guideline was constructed through multiple sessions in order to include all research topics. Such an approach enabled this research to gather data without having to be present at all interview moments.

In this case, the involved concepts of GenAI awareness and cybersecurity training did not require tight exclusion criteria for participants. Rather than seeking technical expertise, this

study aimed to capture a general understanding on how its effects impacts employees across various departments within the organization and experience levels. However, in order to receive meaningful data, participants have been selected according to the following criteria: the participant works at the financial institution, can elaborate on cybersecurity training experience, and has basic knowledge on (GenAI) fraud risks. Nevertheless, additional interviews with professionals in cybersecurity training and GenAI were conducted to incorporate expert insights and capture valuable perspectives that might otherwise have been overlooked.

A total of eleven semi-structured interviews were conducted and an overview of all participants details can be found in table 1. An expert lead fraud chain at the financial institution has been the first line of contact with employees. A snowballing technique has been used where existing interviewees were asked to recommend other suitable participants within the organization. Snowballing involves starting with a sample from a population, which is then extended by asking individuals to name other individuals to be included in the research, and repeating this process (Goodman, 1961).

Pseudonym	Gender	Management position	Place	Department	Interview type
Alpha	Female	Yes	Amsterdam	Fraud	Physically
Bravo	Female	Yes	Amsterdam	Fraud	Physically
Charlie	Male	Yes	Diemen	Fraud	Physically
Delta	Female	No	Amsterdam	Security	Physically
Echo	Male	Yes	Amsterdam	Awareness	Physically
Fox	Female	No	Amsterdam	Communication	Digitally
Golf	Male	No	Utrecht	Treasury	Digitally
India	Male	Yes	Utrecht	Treasury	Digitally
Juliet	Male	No	Amsterdam	Traineeship	Digitally
Kilo	Male	No	Amsterdam	Fraud	Digitally
Lima	Female	No	Amsterdam	Communication	Digitally

Table 1: Sample overview

3.3 Data collection

Interviews were conducted both physically and digitally, with a preference for physical conversations to enhance communication quality. Five interviews (Alpha to Echo) took place at the organization's headquarters and one at an office in Diemen. The remaining six interviews were performed digitally through Microsoft Teams due to tight working schedules, long travel

distances, and remote offices. Interviews lasted between 30 and 75 minutes, depending on the participant availability, engagement, and topic relevance. For example, participant Golf working in treasury, had limited knowledge of certain topics and therefore discussed fewer themes from the shared interview guideline.

Each interview began with a brief explanation on the subject of the research to ensure information symmetry in terms of content to be covered. What followed were a set of introduction questions, advancing with questions related to GenAI knowledge, continuing into questions about cybersecurity training, behaviour and awareness, and ending with questions concerning stakeholders and personal viewpoints.

In order to be able to retrieve information, two separate recordings were made through the dictate-app on a mobile phone per interview. The digital interviews were conducted through the online platform Teams, as this was the preference for all participants. Recordings were made and saved through the automated video and transcription option in the call. All interviews were transcribed in Dutch. The term transcription refers "to the word-for-word reproduction of verbal data, where the written words are an exact replication of the audio recorded words (Halcomb & Davidson, 2006, p.38). For the purpose of the results chapter, only relevant data was translated into English. This brings up the notion of loss of meaning. Translating verbal stimuli between two different languages in a way its stays identical is close to impossible according to Sechrest, Fay and Zaidi (1972). It is therefore to be assumed that a potential loss in data meaning is inevitable.

3.4 Ethical considerations

All participants have been informed about the intended use of data and have given consent to participate voluntarily. In line with institutional protocols, all participants were anonymized and assigned pseudonyms to preserve confidentiality. Every participant has been briefed in advance about the goal of this research and how data will be stored. Moreover, every participant in the research has been asked beforehand if he/she is willing to voluntarily participate and if he/she accepts recording of the conversation. Anonymity and privacy sensitive information has been made confidential by removing any information that can be traced back to the participant. Also, the participant was allowed to end the interview at any given point if that was desired. Finally, data has been processed and stored according to the master thesis guidelines of Radboud University.

3.5 Data analysis

The collected interviews were analysed using qualitative content analysis, more specifically, through thematic analysis. This type of analysis is often used in qualitative studies to understand motives and find patterns (Clarke & Braun, 2013). Unlike quantitative methods, which rely on standardised measures and statistical tools (Hammarberg et al., 2016), thematic analysis allows for in-depth exploration op personal opinions, attitudes, and experiences.

Transcripts of the interviews are analysed according to the thematic steps of open, axial, and selective coding. Codes make up the building block for themes, a pattern of meaning, which are then substantiated by a central connecting concept (Clarke & and Braun, 2017). Besides data summarization, thematic analysis aims to identify and interpret key features of related, but also less related features of the data (Clarke & and Braun, 2017). This helped to break down large amount of data and facilitated the process of finding patterns and data interpretation.

As mentioned, semi-structured interviews have been selected to obtain data as this method is particularly useful when trying to assess someone's understanding of a particular phenomena or service perspective (Adeoye-Olatunde & Olenik, 2021). Moreover, a semi-structured interview is neither completely open or closed, which allows the interviewer to provide a structure and focus on a natural flow of conversation with additional follow-up questions for deepening (Adeoye-Olatunde & Olenik, 2021). The process of data collection and analysis has been iterative as interviews will uncover thematic themes. When no new patterns or insights emerged from the data, it is decided that thematic saturation is reached.

4. Results

This chapter's purpose is introducing the key themes that have emerged from the semi-structured interviews that have been conducted with employees from a major financial institution. Each theme will be discussed alongside examples from the gathered data and connected to the theoretical background. Thematic data analysis initially resulted in thirteen final themes. However, only eight have been included in the results chapter due to their relevance and fit with the theoretical framework, research objective, and answering the research question. The themes are named (1) situational adaptiveness of GenAI (2) growing complexity of digital threat (3) Effectiveness of training methods (4) overestimating knowledge damages awareness (5) individual responsibility in cyberbehaviour (6) role of technology in behaviour (7) human emotion leads to mistakes (8) and knowledge on (future) GenAI possibilities. Each of these themes will be covered in the forthcoming sections.

4.1 Threat and perception of GenAI

GenAI driven fraud is a growing trend as its capabilities are being used to manipulate data and people on large scales. From the interviews it became clear that every employee has a basic understanding of GenAI's capabilities, but the true depth of this understanding, its capabilities, and risks varies strongly for each person. For many, GenAI is viewed as an aid tool that can support in terms of creativity and efficiency. The idea on how people can use GenAI in harmful ways was less understood, this is especially true for employees who are not directly involved with fraud in their work. India explains how *"GenAI is basically just a text generator. It's not going to come up with something for a link to click on or an email address. So, that's not where I see GenAI jump in directly".* As said, on the other hand, fraud experts from the financial institution have a better understanding of the most recent GenAI fraud developments. Fraud expert Alpha emphasizes the skilfulness of fraudsters and their speed: *"You can see, of course, that criminal or fraudsters are taking very clever advantage of this* [GenAI] *and they have been doing so for a while".* Fraud expert Bravo is able to further explain this advantage by saying how GenAI is improving the content of fraud messages: *"It all becomes much better these days, much higher quality and therefore a lot more realistic. They used to do it manually, having a lot spelling and grammar mistakes, that's much better these days"*. Especially the content of fraud attempts has been a popular concept as the growing complexity of digital threat appeared to be a much returning theme in the interviews with fraud experts of the financial institution.

4.1.1 Growing complexity of digital threat

First, GenAI enables somebody to scan the internet and collect personal information in order to tune the message to a specific individual. Fraud expert Echo, responsible for internal awareness programs, elaborates on this development by saying the following: *"What's happening is that fraudsters are having personalised phishing emails created based on GenAI through social media harvesting, and this not science fiction, because this can easily be done, yes, then detection becomes much more difficult".* Insights from real phishing message collected by the financial institution shows how personal data such as name, job title, and email are collected from digital platforms to give the message more power. People tend to react less hostile to messages that carry familiar information to the respondent. And such information is gathered without too much trouble, as Lima explains: *"Previously, someone would actually sit down and look at your LinkedIn profile and ask what's your name and position. And then they would type a fishing email to you with your salutation in it. Yes, all of that is now being pumped into one big prompt* [GenAI instruction] *and that goes out before you know it"*. The personalisation of phishing messages increases the risk of people believing that the sender of the message is legitimate. Such data collection methods are known within the financial institution and precautions are taken by pointing out the risks openly sharing your information online, especially when you are in this line of work, informs Bravo. *"We try to inform our employees about their behaviour on the socials. Of course, we are not allowed to tell them exactly how to behave, but we provide tips on how to do it in the safest way for them"*. Besides this increased rate in fraud success personalisation brings, there is another problem. Current IT cybersecurity measures are able to quarantine fraud attempts if flagged and reported by an employee, enabling the automatic blocking of similar messages. But Echo explains how GenAI jeopardizes this detection method: *"If everyone would receive its own personalised message, the mechanism would stop working. If I would send out 500 different emails internally, you would have to report all 500 emails to block each one. That is a clear effect of GenAI"*.

Second, interview respondents noted a rise in the volume of fraudulent messages detected by their systems in recent years. By sending phishing messages in bulk, fraudsters aim to scam as many people as possible, operating under the principle that the greater the output, the higher the likelihood someone will fall for it. *"Yes, and they just send it to a million victims. Then only one hundred have to click on it"* (Charlie). Bravo has also noticed this development by saying: *"It has become much more efficient in terms of volume"*. The sheer output these scammers generate should not be underestimated, as it places continuous pressure on the organization to respond effectively. Charlie talks about this pressure and the never-ending cycle

of fraud attempts: *"Detection keeps going. The scammer doesn't think: 'oh it's 21:30, lets stop'. If we don't detect, fraud will keep going and the phone will not stop ringing"*. Scammers are no longer confined by national borders, as GenAI now allows them to operate flawlessly in a foreign language. Alpha also expresses her concerns about this situation, stating: *"What I worry about when it comes fraud, is its global reach"*. The combination of GenAI and the ability to no longer distinguish between targets allows scammers to operate around the clock, anywhere in the world. Moreover, the COVID-19 pandemic triggered a significant shift towards working remotely. Fraudsters capitalised on this transition by targeting employees directly. Combined with the rise of GenAI, this led to a dramatic increase in fraud output. Charlie elaborates on this trend: *"So you were able to see a change in that* [COVID-19]*. (…) So I think that caused a really big change"*.

Third, GenAI has taken phishing to new levels in terms of quality. As briefly mentioned, GenAI enables a scammer to develop text that is free of any spelling and grammar mistakes. In addition, the structural content of the message improved similarly, matching a real firm's tone and professionalism. *"Yeah, there are no more mistakes, it's just like the real thing. I dare to say that many of my colleagues – including me – could fall for it"* (Charlie). Echo has a similar experience: *"One of the ways we used to inform people on recognizing phishing are through linguistical errors. You can forget about that now, that's of the table, anyone can now write flawlessly"*. Furthermore, GenAI is also used to enhance the visual design and layouts of phishing emails to match those of the companies impersonating them. *"I can see how the lay-outs of these messages are increasingly becoming more professional. (…) When I think back to the messages we were forwarded about four years ago, then often it all made no sense"* (Delta). Finally, scammers are able to closely mimic the domain names used by real firms to send out the messages, which further enhances their credibility, as victim often mistakenly associate them with the impersonated organization.

> "They are better aware of how to disguise original messages. There is spoofing now, which is a technique that works for phones and email where you send a message from a certain number or email address, but the recipient sees the name of the copied organization. However, if you click further, you can really see where it originally came from. As a fraudster you can very easily ask these kinds of questions to GenAI on how to take these actions" (Delta).

4.1.2 Situational adaptiveness of GenAI

While the content and quality of fraudulent messages are described as the most significant changes in recent years, another notable trend has emerged. Fraudsters cleverly capitalise on current events to give their message more persuasive power. Specific periods throughout the year tend to trigger surges in the volume of fraud-related messaging. For example, Charlie explains one of the recurring stories they notice: *"Now it's very interesting to send out emails on behalf of the Belastingdienst, because tax declarations are in this time-period. (…) In some way, they just have a calendar"*. However, familiar themes go beyond general trends, with highly specific events also being exploited. *"They respond to current events. Like now with NATO in The Hague, we really need to start warning people internally, because we just know that there's going to be phishing involved around NATO"* (Echo). Alpha even elaborates that much of the value of the attack is in its preparation: *"It's really more about the preparation of the attack, not so much in the execution. So people are more likely to be seduced (…) when it's specifically applied to a situation"*.

4.1.3 Knowledge on (future) GenAI possibilities

Both the growing complexity and situational adaptiveness of GenAI have impacted the overall quality of fraud attempts, but it seems that the recognition of dangerous effects of GenAI on fraud varies across the organization. This was confirmed by the respondent India who embraces GenAI as a text generator, which is just one of its core functionalities.

Another factor adding to the complexity of the technology is its continuously evolution, which ensures that there remains ambiguity on the subject in terms of opportunities and associated risks. In fact, Echo shared how he thinks this research is rather early as concrete data on the development of GenAI and its connection to fraud is still lacking. However, he does express concerns about future scenarios in which GenAI-driven fraud becomes widespread. Echo said the following: *"I think it* [GenAI fraud] *will explode, (…) but it will take longer than people might expect, the peak is yet to come"*. Although somewhat reluctant in expressing his opinion on the speed and scale of GenAI-driven fraud, he does acknowledge the troubling potential the technology brings.

> "We do fear at some point that stuff like deepfakes will be so good that it can also be done for the masses. Because if you can't trust what someone writes, someone says, and what they look like, then it gets complicated" (Echo).

Countering fraud is particularly challenging due to the lack of clear insights, which can partly be attributed to the secretive and constantly evolving tactics used by criminals: *"Look, the advantage they have is that they don't have to comply with laws and regulation"* (Alpha). The respondent Delta also addressed this issue: *"It is of course hard to say, because we have no insights into how the fraudster exactly arrives at a specific fraud method and by what means"*. While the organization is aware of GenAI's growing fraud related influence, it is unclear how prepared they are when the expected growth will take place. Respondent Lima also expressed this lack of clarity in her statement about internal GenAI-relate fraud communication: *"I think more information should be shared about it. Because it's still a fairly unknown area right know, even for us working on the subject"*.

4.2 Human behaviour in cybersecurity

4.2.1 Human emotion leads to mistakes

Several participants have highlighted how emotional dynamics make employees, but also clients, more susceptible to GenAI-supported fraud. Many cyberattacks exploit human instincts by creating a false sense of urgency, pressuring the victim to act quickly. Bravo illustrates how scammers simulate urgency to override rational thinking: *"Yes and especially the urgency, note if you have to respond now or the code will expire within 24 hours, those are things you should not trust"*. Echo adds that trust is also a crucial element that is exploited by attackers: *"To get someone to transfer all the money, including the four hour wait* [transfer window] *you need to be able to bridge it. In fact, that only works if you can keep someone on the line"*. These two quotes clearly illustrate how a sense of urgency and misplaced confidence can put pressure on people making mistakes.

In addition to these two principles, Delta also mentions that haste often leads to mistakes: *"There happened to be a colleague of mine who had clicked on that phishing mail* [dummy] *and said: 'Yeah I was so busy and had so many emails, it went so quick, and that's where it often goes wrong. Unintentionally"*. And she is not alone in this observation. Echo too notes these common situations: *"Well, colleagues at operation receive thirty a day (emails). So can I blame them if one slips through"?* Participants Delta, Lima, and Juliet all mentioned how getting caught up in the pressure of your work can lead to stupid mistakes that could lead to unpleasant outcomes. *"Well, I'm only human and the second to last phishing mail I got, there I very stupidly clicked on the link. Fortunately, it was only a test. But that just indicates, say like if you're busy with work and have deadlines…"* (Lima).

4.2.2 Role of technology in behaviour

As interview findings just revealed, employees acknowledge the human tendency to make mistakes and also recognize that a loss of focus can lead to cybersecurity incidents. Despite this awareness, as Alpha points out: *"Because it's pure emotion they're capitalizing on"* and Bravo: *"Fraudsters often rely heavily on social engineering techniques"*, the interviews reveal a recurring pattern of employees placing much confidence in the technological systems that detect or prevent fraud incidents at work. While this trust can be justified by the presence of reliable automated filters and security features, it can also lead to reduced personal vigilance from an employee perspective. A clear example is the following attitude of Fox:

> "Personally, I tend to rely heavily on the technology, we have such a good IT system. All kinds of things are blocked and alarm bells go off, I just trust the technical system. With that, I also feel less responsible for having to watch out for those kind of links or messages. I'm really not that suspicious".

In this example, the human factor and feeling of responsibility are minimized to a questionable level. Such reliance on the technological side may create a false sense of safety, especially with GenAI growing in sophistication. But such an attitude is not far from what Echo envisions as a potential future scenario driven by GenAI-drive fraud developments.

> "I think my profession might become impossible at some point. I think that when GenAI and AI become so good, we cannot expect from people to be able to tell the difference between real and fake and my function of educating them [employees] will disappear. We may eventually have to solve this with technology".

These statements suggest that while technical defences are crucial, putting too much trust in it may hurt individual responsibility. As GenAI-related fraud continues to evolve, undervaluing the human factor in cybersecurity is a worrying development.

4.2.3 Overestimating knowledge damages awareness

When asked about their overall attention to cybersecurity threats and practices, participants reported having a strong sense of awareness and a general positive attitude towards cybersecurity was observed. All acknowledge its importance and express confidence in wanting to keep the firm's data safe. Delta shares her vision on this: *"I feel my responsibility in this and I would genuinely feel bad if something I did caused a data leak"*.

Most participant reported that their knowledge of cybersecurity is at a sufficient level, giving them the sense that they can perform their work safely. Although this suggests that everyone is behaving correctly, in practice that is not always the case. As Echo noted: *"The knowledge level isn't the problem, it's acting accordingly, with all excuses that come with it"*. He further added: *"Yeah, so people are aware* [cybersecurity]*. That doesn't mean they always act accordingly"*.

In contrast Delta openly acknowledged that her limited IT knowledge poses a risk: *"I'm not very technically skilled and I think that there are many more risks I'm not aware of"*. With a background in customer service and currently working in a security-related role, she observed differences in how seriously employees take cybersecurity. When asked whether this has something to do with intrinsic motivation to talk about cybersecurity, she responded: *"Yes, it depends on the employee and how engaged they are. That engagement plays a bigger role in my current team. The culture here is very different – much more relaxed"*. Kilo shared a similar view: *"No, I think it really comes down to personalities, people who are driven by that motivation"*. After Delta's transfer to the security department, she reflected: *"I do think I'm more conscious of it now* [cybersecurity]*"*.

4.3 The evolving nature of training effectiveness

4.3.1 Effectiveness of training methods

A frequently recurring topic in the interviews was the variety of training methods provided by the organization to promote secure working practices. Two mandatory formats were identified that every employee across the organization is required to complete: SAFE (pseudonym) and a personal e-learning environment. The latter consists of periodic, generic modules covering topics such as online behaviour and integrity. SAFE, on the other hand, is a monthly returning interactive, digital tutorial including current topics, ranging from cybersecurity till terrorism, through brief lessons and multiple-choice questions. Although all participants recognized the necessity of SAFE, their views on its relevance, effectiveness, and interactivity varied considerably. Both SAFE and the e-learning environment are mandatory, but it was SAFE that generated the most extensive discussion among participants. As India noted: *"I find it a necessary evil"*, summarizing the mixed sentiment shared by several participants. As a result, this section will focus more closely on SAFE and its training in cybersecurity than on the e-learning modules.

First, there is the general content of SAFE. Multiple participants have voiced their concerns about the training being too generic, lacking specificity and relevance to their actual work context. Kilo criticized the latitude of SAFE's topics, stating: *"Completely useless. I can understand from a regulator perspective that some things are mandatory. But it obviously adds very little to make sure I know which transactions could be risky. That's something I'm not going to experience in my day-to-day work"*. Alpha looks at from a different perspective: *"Well, it forces you to think differently and I think that's a good thing. Otherwise we're all thinking in our own little bubble"*. Echo, responsible for SAFE, understands the content-related criticism, but sees the selection of training topics per department as a non-negotiable: *"The downside* [SAFE] *is answering pointless questions. However, the moment you start differentiating, endless discussions about it will start. Also, the law demands that everyone needs to follow certain training topics"*. When asked about GenAI training related to the risks it may pose to the company's cybersecurity, the responses were mixed. Many participants mentioned having received training on GenAI, but after further explanation, these sessions primarily focused on how to use the technology safely in their daily work, rather than directly connecting it to personal cybersecurity risks. Golf spoke about how SAFE addresses developments in the quality of fraud messages, for example by providing information on personalization and translation capabilities. However, this is not specifically attributed to GenAI technology. India shared a supporting insight from his SAFE training: *"As far as I can remember, it's not specifically: 'hey watch out, because GenAI does this'"*.

Second, there is the style in which the training method is presented: theoretical based lessons and multiple-choice questions. All participants criticised SAFE for its boring and passive delivery format of the trainings. Although the usefulness is recognised, the assignments feel like an obligation that is preferably completed as soon as possible. India mentions the following: *"The fact that it irritates says it all* [laughs]. *Everybody has to keep doing it and you can hate it, but it's the power of repetition. Doing the same thing over and over, at some point it will stick"*. Golf expressed a similar sentiment *"It's always the last week that you think: 'Oh yeah I still have to do SAFE'. Nobody really likes it, but I do think people see the point of it"*. Delta shares the same viewpoint but doubts the real effectiveness: *"It feels like a chore, that's what I think. And yeah, I don't know how much it helps, everybody thinks it's boring"*. These opinions about SAFE illustrate a broader trend among employees who view it as boring and delay it till the last minute. Golf elaborated on the training style by sharing a story from a friend at a similar financial institution who undergoes training through interactive games: *"(...) this sounds pretty fun and entertaining. An interactive style instead of multiple choice keeps it a bit*

more fun. Yeah, I would find something like this very interesting". Echo also acknowledges the need for a more interactive learning environment, but blames financial space for any new developments. However, he mentions how exploration for an interactive training method in the future is desired: *"(…) there's still a range of things I want to explore there".* Although, he adds how SAFE has reached its limits in terms of quantifying data: *"No, that's just the way it is and it has to stay that way. It has reached its limits for what is does"*.

Third, there is the dedicated place where people can go for cybersecurity related questions or to report incidents. While respondents indicated that they knew where to go if needed, further probing revealed that several people were unsure of the exact contact details, such as the appropriate phone number or email address. Different cybersecurity issues need to be reported to different reporting points. A phishing mail, for example, should be reported via the "flag-button" in Outlook, while a data breach requires a written report. As Fox put it: *"But I guess I don't know now who I should contact for what, what the team is called, what email address or whatever"*. Golf was able to confirm the existence of a reporting point but could not clarify what exactly falls under this point: *"Well, I know that there's SIM. I think a fraud reporting point and then there's also CISO"?* Echo, aware of this fact, suggested considering the implementation of a centralized 112-number to streamline the processing of cybersecurity-related incidents: *"There are too many places where somebody can go to with questions related to cybersecurity"*. In addition to where employees go with questions, an equally important question is whether the training leads to meaningful behavioural change.

Fourth, there is the behavioural impact of training. The e-learning environment and SAFE aim not only to inform, but also to influence behaviour. As Echo tried to make clear: *"Actually, I'm not interested in what people know, I'm interested in what people do. (…) What matters to me is why you click on it"*. The interviews make it clear that while the purpose of the trainings is understood, the experience is often described as unstimulating and more of a chore than an engaging activity. Views on the effectiveness of initiatives like SAFE, however, are mixed. India, for example, reported increased awareness of cybersecurity and a greater ability to recognize potential threats.

> "But because of those trainings, I have become more aware of things like: what are warning signs? How can I check whether something is phishing or not? And how do I recognize fake emails? So those trainings definitely contributed to that".

Several individuals have indicated that the training sessions have positively influenced their workplace behaviour, particularly due to the institution's internal awareness efforts. Initiatives such as the mandatory annual information sessions are well received and also well attended, according to Alpha. Nevertheless, not everyone is convinced of the value of cybersecurity initiatives. When Delta was asked whether the training had positively influenced her cybersecurity behaviour, she reported the following:

> "And training has had effect? No, I don't think so. No, it's really not that bad. I feel like I know enough because I'm invested in the topic. Like, I know I know all about it".

When the same question was asked to Fox, she responded: *"No, yeah, when I'm very honest, I'm kind of just reading through it quickly as possible, so not everything sticks. I just browse through it as quickly as possible and answer the questions"*. This illustrates the imbalance in employees' sense of effectiveness, particularly due to differences in the respondents' job backgrounds, which may raise doubts about the adequacy of the trainings.

4.3.2 Individual responsibility

Throughout the interviews, a recurring sentiment is the belief that cybersecurity is not the sole responsibility of the IT- or security-department, but something every employee must actively contribute to. While training and infrastructure can provide the tools and awareness, respondents emphasised the importance of individual accountability in day-to-day working behaviour. Echo expressed this most explicitly: *"So its actually everybody's responsibility"*. Such a statements reflects the underlying assumption that everyone in the organization must take ownership in their online behaviour. Yet, what became evident, the way this responsibility is perceived and acted upon varies between individuals. Alpha emphasised how training plays a role in reinforcing that sense of responsibility: *"Training just broadens your awareness"*.

Here, awareness is not viewed as an end in itself, but as a catalyst for responsible behaviour. Charlie highlighted this broader sense of responsibility, stating: *"it has to happen on all fonts, not just within our chain".* This underscores the idea that individual responsibility extends beyond small teams involved in cybersecurity, it must be part of the broader organizational mindset. Although many of the respondents confidently shared their personal involvement within the realm of cybersecurity, it is a comment by Delta that was interesting: *"I think from my two different jobs I have a diverse view of what it's like inside the organization, I think it* [feeling of responsibility] *very much depends on which department you work in"*.

Many respondents expressed a strong investment in the topic. However, according to Delta, this may be partly because they work in a more serious or high-risk area of the financial institution. In contrast, she noted that in lower-level, operational departments, cybersecurity tends to receive far less attention and is not as actively discussed.

Continuing, not everybody thinks this individual responsibility is this straightforward. Echo, who holds a managerial position, believes that leadership plays a crucial role: *"It's everybody's responsibility, but I think managers have a specific responsibility to make it discussable in their team"*. His view reflects on the notion that employees within a management position should lead by example and actively foster a culture of cyber awareness in their teams. Delta explains with a personal example how she is affected by this: "*I do think that your manager should be guiding in this or at least indicate something that you should watch out for and what the risks are. Now my manager is very enthusiastic and that's why we get dragged along in his vision".*

Juliet also shared the importance of cybersecurity within the organization by stating how neglecting cybersecurity behaviour can have grave consequences for the individual. *"So there was also a trainee before me. I don't know if it was ever told. So that one time he sent company data to himself and he got fired because of it. So that does just show the seriousness of cybersecurity".*

5. Conclusions

5.1 Conclusion

The goal of this study was to explore how the rise of GenAI fraud influences employee awareness and how this relates to the development of corporate cybersecurity training. This research underlines a critical paradox in the cybersecurity domain. Although employees express a strong sense of responsibility and acknowledge the importance of cybersecurity, their awareness does not directly translate into secure behaviour. With the rise of GenAI-related fraud, this is a problem as growing sophistication and personalization of fraud attacks jeopardize the effectiveness of current training and defence methods. In addition to the technological developments, it is equally important to consider the psychological tactics used by fraudsters.

The findings show an illusion of awareness, where employees believe that they are well-informed but fail to completely grasp the evolving risks. GenAI's ability to deceive is outpacing the content of current training methods. This suggests that providing knowledge through informing is insufficient. The organization must use continuous, interactive learning tools that go beyond finishing mandatory checklists.

A noteworthy theme emerging from the interviews is the emotional and behavioural vulnerability of employees. Respondents highlighted how stress and workload are often reasons for the happening of incidents, factors that GenAI-driven scams are known for targeting. More specifically, the concept of social engineering where fraudsters directly target individuals by manipulating their emotions. This pushes the notion of a need for more emotionally intelligent training methods where employees are trained to be more aware and act accordingly in specific situations. Another critical insight relates to leadership and cybersecurity culture. While individual responsibility is often emphasised, participants consistently pointed out that managers play a critical role in modelling secure behaviours, normalizing security discussions, and reinforcing training messages. Where managers show active interest in cybersecurity, employee engagement is higher.

The findings suggest that cybersecurity training acts as a partial mediator. While training informs and alerts the employees of specific risks and trends, its current design does not sufficiently enable the behavioural or emotional readiness needed to cope with GenAI threats. Overall, it can be said that with the evolving nature of GenAI and its related fraud, organizations must do so similarly to safeguard their assets.

5.2 Discussion

Through a qualitative study accompanied by eleven interviews with employees from a major financial institution, three core themes emerged: Threat and perception of GenAI, human behaviour in cybersecurity, and the evolving nature of training effectiveness.

The growing complexity and adaptability of GenAI-driven fraud (Gupta et al., 2023) was consistently remarked across the interviews. Especially experts in the security domain highlighted how phishing emails and fake messages are increasingly harder to distinguish from legitimate ones due to a growing quality in lay-out and language. This is logically attributed to the fact that these individuals are more engaged with the subject through their daily responsibilities. In contrast, employees without such a background lacked a clear understanding of GenAI threats. Instead, it was mostly viewed as a supportive tool for productivity and content generation, despite many indicating having a sufficient amount of awareness on GenAI-related fraud. This asymmetry between individuals knowledgeable about GenAI and the ones who are not pushes the concept “illusion of awareness”, an overestimation of someone’s competence. Such a concern is also called out upon by Shaw et al. (2009) who state awareness does not always result in secure behaviour. This notable growing complexity of fraud by the participants is also in line with conclusion from works like Schmitt and Flechais (2024) and Schreiber and Schreiber (2024) where a significant difference exists between trained and untrained people in GenAI associated risks.

Cybersecurity training is the needed behavioural reinforcement by organizations to ensure cybersecurity practices are transferred into workplace habits (Reegård et al., 2019; Schreiber & Schreiber, 2024; Shaw et al., 2009). While well-intended and mandatory across the organization, it appears to undermine the dynamic nature of GenAI-related threats. To promote secure behaviour, the financial institution uses static programs like SAFE and e-learning modules as a part of its cybersecurity training, which aims to alert individuals to threats and enhance their understanding to adopt secure behaviour (Rahim et al., 2015). However, respondents have repeatedly shared their discontent about the selected formats as they are boring, repetitive, and feel mostly contextual irrelevant. Although trainings include real-world examples, which enhance understanding and retention (Hijji & Alam, 2022), their static nature jeopardizes efficiency as such methods are increasingly seen as insufficient to safeguard employees (Ansari, 2022; Grover et al., 2023). This concern was also addressed by respondents, who desired a more interactive and dynamic learning environment, such as gamified methods or simulations (Furnell et al., 2002; Sarker et al., 2021; Zhang-Kennedy & Chiasson, 2022). This is indicating a gap between knowledge dissemination and adapting desired behaviour.

Moreover, it is putting pressure on the belief whether cybersecurity training is adequately affecting employee awareness. The vast majority of respondents indicated that they understood the purpose of the trainings and also reported gaining valuable insights into developments in cybersecurity. Despite this positive outcome, some acknowledged that they are still not always sufficiently alert or able to recognize threats, which was attributed to factors such as emotional responses, overconfidence in technology, and misjudgements. This aligns closely with the work by Kruger and Kearney (2006) where knowledge, attitude, and behaviour make up the concept of awareness in the cybersecurity domain. The data supports the claim by Shaw et al. (2009) that knowledge alone is insufficient to develop desired behaviour, particularly when under pressure, as became clear. Additionally, it was showed that for many there is a tendency to rely heavily on technological defence mechanisms, shifting responsibility towards the organization instead of the individual. Such a development is concerning as human error is a major cause for cybersecurity breaches (Huang & Pearlson, 2019). Although many respondents do agree on the individual responsibility someone has for cybersecurity, it was mentioned how leadership and management are strong initiators for cybersecurity engagement. As leadership capabilities vary per person, it is critical to encourage these qualities in any type of team setting.

For managers, this study offers several practical recommendations. It has become clear that knowledge of GenAI-related fraud risks and proper cybersecurity behaviour varies within the organization. Leadership was identified as a strong motivator for cybersecurity behaviour. Managers must be equipped and encouraged to lead cybersecurity conversations in their team, as their engagement directly influences employee behaviour. Additionally, for cybersecurity management, this indicates that the current approach to cybersecurity training may not be the most effective, given the negative responses related to its content and style. A critical review of these training programs is necessary to keep pace with GenAI fraud developments in future scenarios. Finally, multiple respondents expressed their confusion on how and where to rapport threats and fraud related incidents. A clear and concise communication channel must be prioritized to simplify the task of reporting for employees. The objective is to not just arm employees theoretically, but to equip them to stimulate desired behaviour. By highlighting the effectiveness of current cybersecurity training and awareness, this study urges organizations to take proactive action.

As this is a small qualitative sample research, there are of course several limitations. First, there is the amount of conducted interviews and its diversity. As this research focuses on cybersecurity and overall employee awareness, conducting only eleven interviews could be considered a limiting factor when the goal is to describe this awareness. Additionally, with more than half of the respondents having a background in security, this may lead to a skewed representation of the applicability of the results across the entire organization. Second, the reliance on self-reported data through interviews raises the concern of social desirability bias, especially since cybersecurity is a sensitive topic and there may be consequences to negligent behaviour. Adding on, the snowballing data collection method may have led to the situation where only individuals with an intrinsic motivation for cybersecurity agreed to participate, while employees with less interest in the topic, and their corresponding behaviour, were not represented. Finally, as GenAI capabilities and countermeasures evolve, the findings represent a temporal snapshot rather than a conclusive long-term outlook.

Due to these limitations, but also the results, several recommendations can be made for future research. First, this case study of a large financial institution considered its unique environment, which may limit the applicability to different settings. Exploring multiple, longer case studies would be interesting to provide a clearer understanding of the impact of GenAI on cybersecurity and employee awareness developments over time. A second recommendation would be to conduct more interviews with lower ranked functions and less connected to the cybersecurity domain employees, as a respondent shared how different departments are less interested in cybersecurity. Third, a comparative study across sectors would be interesting as it could highlight contextual variations in awareness, training, and its effectiveness. This could provide more clarity on the content of training programs, their effectiveness, employee attitudes, and general awareness of GenAI fraud developments. Finally, it would be a good initiative to conduct research about how GenAI is specifically used to commit fraud and how this effects the effectiveness of current cybersecurity training methods out there. Such research could inform the development of updated or new training approaches that directly address GenAI-related threats, thereby enhancing the protection of company assets.

Theoretically, this study extends the literature and knowledge on cybersecurity awareness by including the increased use of GenAI-related fraud by criminals. Much of existing literature on cybersecurity training treats AI either as a tool for defence mechanisms or as a vague threat without really considering its immediate risks. This study narrows in on GenAI as a specific powerful enabler of fraud, which is still a relatively unexplored area in empirical studies.

Moreover, it deepens the understanding on the human dimension of cybersecurity, particularly the emotional factors related to attitude and knowledge that influence behaviour. By performing a case study on a major financial institution, it provides empirical insights for a real-life situation where cybersecurity related issues can have serious consequences.

6. References

Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. *Journal of the American College of Clinical Pharmacy*, *4*(10), 1358–1367. https://doi.org/10.1002/jac5.1441

Aggarwal, K., Mijwil, M. M., Sonia, Al-Mistarehi, A.-H., Alomari, S., Gök, M., Allabdin, A. M. Z., & Abdulrhman, S. H. (2022). Has the future started? The current growth of artificial intelligence, machine learning, and deep learning. *Iraqi Journal for Computer Science and Mathematics*, 115–123. https://doi.org/10.52866/ijcsm.2022.01.01.013

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). *An exploratory study of current information security training and awareness practices in organizations*. Hawaii International Conference on System Sciences, Hawaii. https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/71f8c247-af73-4833-af80-b6721fdc8a12/content

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Ansari, M. F. (2022). A quantitative study of risk scores and the effectiveness of AI-based cybersecurity awareness training programs. *Interscience Research Network*, *3*, 9. https://doi.org/DOI: 10.47893/IJSSAN.2022.1212

Baidoo-anu, D., & Ansah, L. O. (2023). Education in the era of generative artificial intelligence (AI): Understanding the potential benefits of ChatGPT in promoting teaching and learning. *Journal of AI*, *7*(1), Article 1. https://doi.org/10.61969/jai.1337500

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), 139–154. https://doi.org/10.1007/s11235-020-00733-2

Brynjolfsson, E., Li, D., & Raymond, L. (2025). Generative AI at work. *The Quarterly Journal of Economics*, qjae044. https://doi.org/10.1093/qje/qjae044

Bughin, J., Seong, J., Manyika, J., Chui, M., & Joshi, R. (2018). *Notes from the AI frontier: Modeling the impact of AI on the world economy*. McKinsey & Company. https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

Buxmann, P., Hess, T., & Thatcher, J. B. (2021). AI-based information systems. *Business & Information Systems Engineering*, *63*(1), 1–4. https://doi.org/10.1007/s12599-020-00675-8

Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 14. https://doi.org/10.1186/s40163-020-00123-8

Chan, C. K. Y., & Lee, K. K. W. (2023). The AI generation gap: Are Gen Z students more interested in adopting generative AI such as ChatGPT in teaching and learning than their Gen X and millennial generation teachers? *Smart Learning Environments*, *10*(1), 60. https://doi.org/10.1186/s40561-023-00269-3

Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *Computers & Security*, *142*, 103858. https://doi.org/10.1016/j.cose.2024.103858

Clarke, V., & and Braun, V. (2017). Thematic analysis. *The Journal of Positive Psychology*, *12*(3), 297–298. https://doi.org/10.1080/17439760.2016.1262613

Clarke, V., & Braun, V. (2013). Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The Psychologist*, *26*(2), 13.

Creswell, J. W., & Poth, C. N. (2016). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. SAGE Publications.

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

Europian Parliament. (2020, September 4). *What is artificial intelligence and how is it used?* Topics | European Parliament. https://www.europarl.europa.eu/topics/en/article/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used

Familoni, B. T. (2024). 1. Cybersecurity challenges in the age of AI: Theoretical approaches and practical solutions. *Computer Science & IT Research Journal*, *5*(3), Article 3. https://doi.org/10.51594/csitrj.v5i3.930

Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*, *15*(5/6), 352–357. https://doi.org/10.1108/09576050210447037

Gcaza, N., & Von Solms, R. (2017). 1. Cybersecurity culture: An ill-defined problem. In M. Bishop, L. Futcher, N. Miloslavskaya, & M. Theocharidou (Eds.), *Information Security Education for a Global Digital Society* (Vol. 503, pp. 98–109). Springer International Publishing. https://doi.org/10.1007/978-3-319-58553-6_9

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2020). Generative adversarial networks. *Communications of the ACM*, *63*(11), 139–144. https://doi.org/10.1145/3422622

Goodman, L. A. (1961). Snowball Sampling. *The Annals of Mathematical Statistics*, *32*(1), 148–170.

Grover, S., Broll, B., & Babb, D. (2023). 1. Cybersecurity Education in the Age of AI: Integrating AI Learning into Cybersecurity High School Curricula. *Proceedings of the 54th ACM Technical*

Symposium on Computer Science Education V. 1, 980–986. https://doi.org/10.1145/3545945.3569750

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). 1. From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy. *IEEE Access*, *11*, 80218–80245. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3300381

Halcomb, E. J., & Davidson, P. M. (2006). Is verbatim transcription of interview data always necessary? *Applied Nursing Research*, *19*(1), 38–42. https://doi.org/10.1016/j.apnr.2005.06.001

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. *Human Repoduction*, *31*(3), 498–501. https://doi.org/10.1093/humrep/dev334

Hijji, M., & Alam, G. (2022). Cybersecurity awareness and training (CAT) framework for remote working employees. *SENSORS*, *22*(22), 8663. https://doi.org/10.3390/s22228663

Huang, K., & Pearlson, K. (2019). *For what technology can't fix: Building a model of organizational cybersecurity culture*. 10. https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/7083b12c-3069-42ec-ae0e-0ee6a3989437/content

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, 338–345. https://doi.org/10.1109/CIC48465.2019.00047

Kadel, R., Shrestha, H., Shrestha, A., Sharma, P., Shrestha, N., Bashyal, J., & Shrestha, S. (2022). Emergence of AI in cuber security. *International Research Journal of Modernization in Engineering Technology and Science*, *4*(12), 1820–1834. https://www.doi.org/10.56726/IRJMETS32643

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information & Computer Security*, *31*(4), 463–477. https://doi.org/10.1108/ICS-08-2022-0139

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Lalchand, S., Srinivas, V., Maggiore, B., & Henderson, J. (2024). *Generative AI is expected to magnify the risk of deepfakes and other fraud in banking*. Deloitte Insights. https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html

Lawler, B., D'Silva, V., & Arora, V. (2025, January 9). What companies succeeding with AI do differently. *Harvard Business Review*. https://hbr.org/2025/01/what-companies-succeeding-with-ai-do-differently

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, *16*(4), 473–475. https://doi.org/10.1177/1524839915580941

Magramo, H. C., Kathleen. (2024, February 4). *Finance worker pays out $25 million after video call with deepfake 'chief financial officer'*. CNN. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

Marschan-Piekkari, R., & Reis, C. (2004). *Language and languages in cross-cultural interviewing*. Edward Elgar Publishing. https://ru.on.worldcat.org/atoztitles/link?sid=google&auinit=R&aulast=Marschan-Piekkari&atitle=Language+and+languages+in+cross-cultural+interviewing&id=doi:10.4337/9781781954331.00027

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia - Social and Behavioral Sciences*, *147*, 424–428. https://doi.org/10.1016/j.sbspro.2014.07.133

Rahim, N. H. A., Hamid, S., Kiah, M. L. M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), 606–622. https://doi.org/10.1108/K-12-2014-0283

Reegård, K., Blackett, C., & Katta, V. (2019). *The concept of cybersecurity culture*. 8. https://doi.org/doi:10.3850/978-981-11-2724-3 0761-cd

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE Open*, *11*(1), 21582440211000049. https://doi.org/10.1177/21582440211000049

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1), 105. https://doi.org/10.1186/s40537-024-00957-y

Samek, W., Montavon, G., Lapuschkin, S., Anders, C. J., & Müller, K.-R. (2021). Explaining Deep Neural Networks and Beyond: A Review of Methods and Applications. *Proceedings of the IEEE*, *109*(3), 247–278. Proceedings of the IEEE. https://doi.org/10.1109/JPROC.2021.3060483

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), 173. https://doi.org/10.1007/s42979-021-00557-0

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12), 324. https://doi.org/10.1007/s10462-024-10973-2

Schreiber, A., & Schreiber, I. (2024). Bridging knowledge gap: The contribution of employees' awareness of AI cyber risks comprehensive program to reducing emerging AI digital threats. *Information & Computer Security*, *32*(5), 613–635. https://doi.org/10.1108/ICS-10-2023-0199

Sechrest, L., Fay, T. L., & Zaidi, S. M. H. (1972). Problems of Translation in Cross-Cultural Research. *Journal of Cross-Cultural Psychology*, *3*(1), 41–56. https://doi.org/10.1177/002202217200300103

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Stefaniuk, T. (2020). Training in shaping employee information security awareness. *Entrepreneurship and Sustainability Issues*, *7*(3), 1832–1846. https://doi.org/10.9770/jesi.2020.7.3(26)

Thomson, M. E., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, *6*(4), 167–173. https://doi.org/10.1108/09685229810227649

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*(1), 38–58. https://doi.org/10.1057/ejis.2013.27

Uma, M., & Padmavathi, G. (2013). A survey on various cyber attacks and their classification. *International Journal of Advances in Engineering and Management*, *15*(5), 733–741. https://doi.org/DOI: 10.35629/5252-0502733741

U.S. Department of the Treasury. (2024). *Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector* (p. 52). U.S. Government. https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf

Venkatesh, V. (2022). Adoption and use of AI tools: A research agenda grounded in UTAUT. *Annals of Operations Research*, *308*(1), 641–652. https://doi.org/10.1007/s10479-020-03918-9

Vennix, J. (2019). *An introduction to scientific thinking and practice* (6th ed.). Pearson Benelux B.V.

Zhang-Kennedy, L., & Chiasson, S. (2022). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys*, *54*(1), 1–39. https://doi.org/10.1145/3427920

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*. https://www.tandfonline.com/doi/abs/10.1080/08874417.2020.1712269

Appendices

Appendix 1: Interview guide

Topic	Interview Question	Provided by Student(s)
Introduction & Role	Could you briefly introduce yourself and explain your role within the organization?	Isa, Tiemen, Rick, Igor
	Could you describe your daily tasks?	Isa, Tiemen, Rick, Igor
	What does your position look like in practice, and how does your work relate to fraud prevention or AI developments?	Igor, Rick
	Can you describe your daily tasks and how they relate to digital security or communication?	Isa
Organizational Structure & Internal Communication	How is your organization (and your department) structured, and what has your experience been with collaboration between departments such as HR, IT, or communications?	Isa
	Which department do you collaborate with the most?	Isa
	How would you describe communication between teams within your department?	Isa
	What communication tools or channels do you use most often, and how do you find them in terms of collaboration?	Isa
	In your opinion, how do departments such as IT, communications, and compliance work together on cybersecurity or fraud prevention?	Isa
	How has your organization addressed GenAI related risks in its training or information efforts and what do you think those risks are?	Isa, Tiemen
AI Fraud & Realistic Phishing	What changes have you noticed in phishing messages since the rise of GenAI, for example in tone, style, or content?	Igor
	What are your experiences with phishing messages that contain personalized information, such as names or job titles?	Igor

	What are some recent examples of new types of phishing attacks you've encountered, and how did you recognize or respond to them?	Igor
	What are some key indicators, in your opinion, that can still reveal AI-generated phishing?	Igor
	How do you think AI affects the scalability and accessibility of phishing attacks?	Igor
Cybersecurity Awareness	How would you describe your awareness or knowledge of cybersecurity, and to what extent do you feel adequately equipped to identify/prevent/or respond to phishing threats in your daily work?	Isa, Tiemen
	What do you notice in your day-to-day work in terms of discussions or sharing of cybersecurity tips among colleagues?	Isa
	How strongly do you feel cybersecurity is embedded in your department's day-to-day work and overall mindset?	Tiemen
	What is your take on who should have responsibility in cyber-security and to what extent do you consider it to be a part of your own job?	Tiemen
	How do you view the role of managers or team leaders in promoting awareness of information security?	Isa, Tiemen?
	Does your organization have a point of contact or department where you can go with questions about cybersecurity or AI tools?	Isa
	Could you tell me about the cybersecurity training you received (if any) and how it has influenced your day-to-day work?	Tiemen
	If yes --> In what type of way has it helped you learn more about the subject?	Tiemen

Cybersecurity Training	How effective do you think the cybersecurity training was in preparing you for risks or situations you might realistically face in your role? Were there any parts that stood out as especially helpful or not applicable?	Tiemen
	To what extent have you received training or education on GenAI?	Isa
	To what extent do you think it's important that all employees receive GenAI training or education?	Isa
Use & Risks of GenAI	How is information about GenAI shared within your organization? Can you describe the process?	Isa
	Who do you think plays a key role in spreading knowledge about GenAI or cybersecurity within the organization?	Isa
Prevention Campaigns & Communication Strategies	In your opinion, what are the core messages your organization conveys in phishing prevention campaigns? Have these messages changed over time, for example with the rise of GenAI phishing content?	Igor
	What communication channels are currently used in your organization for phishing prevention campaigns? How are these channels selected, and have you noticed any changes in this approach in recent years, for example, since phishing techniques have become more sophisticated through GenAI?	Igor

	Have you noticed any differences of the campaigns before and after the rise of GenAI fraud? If yes --> How are differences among target groups, such as digital skills or roles, taken into account in campaigns? Have you seen changes in these choices across the years? (tone, style, frequency) If no --> continue	Igor
	How has the rise of GenAI influenced the tone, style, or frequency of your campaigns?	Igor
Collaboration & Stakeholder Coordination	With whom do you collaborate (internally or externally) in the area of fraud prevention, and what does that collaboration look like in practice?	Rick
	How did this collaboration look like? (E.g. face-to-face, online, direct/indirect contact)	
	Could you describe how you handle customers concerns/ questions, that have been frauded with the use of AI?	Rick
	Could you describe how you communicate/process/continue internally when a GenAI fraud related case happened?	Rick
	How do you learn/get know-ledge about GenAI fraud?	Rick, Tiemen
Reflection & Improvement	What do you see as the biggest challenges for the organization in identifying AI-generated fraud?	All
	What do you see as the biggest challenges for customers in identifying AI-generated fraud?	All
	What would you suggest as the biggest improvement that should be done for you personally in preventing GenAI fraud within the organization?	All
	What would you suggest as the biggest improvement personally in the coordination between stakeholders in preventing Gen-AI fraud?	Rick

Appendix 2: Coding scheme

Open	Axial	Selective
- Fraudsters used change of CEO as inspiration - Events such as NAVO-meeting increase fraud - Christmas holiday causes peak in webshop fraud	Fraudsters react on current affairs	Situational adaptiveness of fraud
- GenAI can collect personal information - Copied official writing style from firms - Fraudsters use your personal information to increase realism	Personalisation	Growing complexity of digital threat
- Very efficient these days and send out in bulk - Scammers operate 24/7, no 9 till 5 mentality - Scamming toolkits are being sold illegally in bulk	Volume	
- No errors in grammar and spelling - Generated output/visuals looks realistic - Victims sometimes don't even believe that they've been scammed as quality is that good - Fraudsters create complete scripts	Quality	
- Fraudsters want you to act quickly, we never do this	Urgence	Landmarks of fraud
- Fraudster want you to click in links, firms rarely ask for this	Links	
- Fraudsters closely mimic official domain names - You should check the page the link will bring you to, is it official?	Domain	
- Training tool SAFE to educate employees	Training methods	Conduct procedure of firm

- Training events for specific learning developments - Mock phishing messages to test employees - Training program admin can view test scores and determine level of awareness - Training content is evaluated weekly		
- Scores on phishing tests are shared - Acute threats are communicated quickly (intranet)	Interconnectedness departments	
- Insufficient test scores can jeopardize your employment -	Consequences on non-desired behaviour	
- Criticism on diverse topics that are irrelevant - Repetitive content is boring, but it works - I try to do it as quickly as I can to just finish it - Intranet covers the basics, for more extensive stuff you're on your own - No specific coverage on GenAI fraud risks/development	Content	Non-stimulating training methods
- Multiple choice methods is boring	Style	
- Too many hotlines for reporting of cyberincidents - Vision to develop 112-callcenter	Place	
- These training methods have not affected my way of acting	Behaviour	
- People's motivation is based in intrinsic motivation - Enough knowledge based on my personal experiences - Many are dependent on technology	Person-dependent	Overestimating knowledge damages awareness

- It should be everyone's job - Certain level of cyberbehaviour is expected - Undesired behaviour is known in some places	Shared responsibility	Individual responsibility in cyberbehaviour
- Management should take lead the way - Managers should promote desired behaviour	Leadership	
- IT has built great defences	Overconfidence in technology	Role of technology in behaviour
- Unclear where to go with what type of cyber-incident - Vision to develop 112-callcenter	Too many options	
- Privacy laws limit possibilities to act - Sharing data with competitors could help, but is restricted	Legal	External influence obstructs
- Busy schedules limit employee development choices - Management group decides what topics are covered - Time lost in addressing bottlenecks	Management	
- Busy with work lets your guard down - email intensive work lowers your guard - Fraudsters want you to act now	Urgence	Human emotion leads to mistakes
- Switch to fraudsters making you transfer money - Fraudsters try to mentions things that are familiar to you - GenAI can play your emotions better	Trust	
- Growing professionalism in fraud - GenAI fraud will explode - Fear that deepfake/spearfishing can be performed in bulk	Anticipated future	Knowledge on (future) GenAI possibilities

- No guarantee if certain fraud methods can be stopped - No insights in how fraudsters use GenAI - GenAI training methods mainly focused on internal use, not on external risks	Uncertainty	
- Fraud consultancy practices where needed - Clear communication channels for fraud reports	Integrated organizational responsibility and collaboration	Distinct cyberguidelines/-expectations
- Cybersecurity training content is adjusted weekly - National cybersecurity meetings and collaborations - Level of awareness differentiates across departments - Cybersecurity awareness program is useful	Continuous reinforcement	
- Many different contact points for reporting - Management receives internal GenAI training - Intranet for reporting of latest developments - Failing your cybertests can be disadvantageous	Procedures & Channels	
- NVB can steer cybersecurity initiatives	National association of banks (NVB)	External influence on cybersecurity policies
- Decision-making is slow - Many opinions on what is right or wrong	Bureaucracy	
- Fraud trends are investigated through experiences	Victims	