Gamifying cyber security training for improved employee engagement in the South African banking industry

Aashika Bava

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2023

ABSTRACT

Based on the South African banking cyber threat landscape, cybercriminals have exploited the Covid-19 pandemic to carry out malicious activities and fulfil their nefarious intentions. Contrary to popular belief, cyber criminals primarily target humans because humans are the weakest targets and the first barrier to breakthrough to extract confidential data or bypass systems. Consequently, human error emerges as the primary cause of cyber-attacks, underscoring the critical role of cyber security training in mitigating such risks. Therefore, cyber security training becomes the foremost line of defence in safeguarding employees and organisations against the loss of personal information, financial loss, and reputational damage.

For cyber security training to be effective, employee engagement with the training content is of utmost importance. Equipping employees with recommended cyber security tools to protect themselves and their organisations assumes a crucial role within the training framework. In the South African banking industry, organisations must prioritise creating cyber security awareness by identifying the most interactive training methodology to enhance employee engagement.

This study focuses on investigating the level of training engagement among South African bank employees concerning critical cyber threats, considering both traditional and modern cyber security training programmes. Additionally, the research explores modern cyber security training tools and techniques, with a specific emphasis on gamification, to empower employees. Adopting a quantitative research methodology, the study employs a questionnaire to analyse employee training engagement in critical cyber threat scenario games, encompassing threats such as phishing and malware. The findings of this research highlight that modern training methods, compared to traditional methodologies, incorporate positive reinforcement techniques that significantly improve cyber security training engagement across the South African banking industry.

KEYWORDS

Cyber security, awareness, modern training methods, traditional training methods, gamification, gamification methodologies, phishing, malware, training programme

DECLARATION

I, Aashika Bava, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: Aashika Bava Signature: A.Bava

Signed at ……Sandton……

On the ……31…….. day of ……May…… 2023

Table of contents

ABSTRACT ..... **II**

DECLARATION ..... **III**

LIST OF TABLES ..... **VII**

LIST OF FIGURES ..... **VIII**

LIST OF ACRONYMS ..... **IX**

CHAPTER 1. INTRODUCTION **10**

1.1 STATEMENT OF PURPOSE 10
1.2 BACKGROUND OF THE STUDY 10
1.3 RESEARCH PROBLEM 14
1.4 RESEARCH OBJECTIVES 15
1.4.1 Research objective 1 ..... *16*
1.4.2 Research objective 2 ..... *16*
1.4.3 Research objective 3 ..... *16*
1.4.4 Research objective 4 ..... *17*
1.5 RATIONALE 17
1.6 DELIMITATIONS OF THE STUDY 18
1.7 DEFINITION OF TERMS 19
1.8 ASSUMPTIONS 20
1.9 SUMMARY 21

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK **22**

2.1 INTRODUCTION 22
2.2 CYBER SECURITY TRAINING 22
2.3 TO ANALYSE THE CYBER THREAT LANDSCAPE OF THE SOUTH AFRICAN BANKING INDUSTRY, IDENTIFYING TWO MAJOR CYBER THREATS 23
2.3.1 Cyber threat *23*
2.3.2 Cyber attack *24*
2.3.3 Cyber security threat landscape *24*
2.3.4 Phishing *25*
2.3.5 Malware *26*
2.4 TO DESIGN A TRADITIONAL CYBER SECURITY TRAINING PROGRAMME FOR TWO MAJOR SOUTH AFRICAN BANKING INDUSTRY CYBER THREATS 26
2.4.1 Traditional training methodologies *27*
2.4.2 Traditional phishing and malware cyber security training programme *27*
2.5 TO GAMIFY THE TRADITIONAL CYBER SECURITY TRAINING PROGRAMME FOR TWO MAJOR SOUTH AFRICAN BANKING INDUSTRY CYBER THREATS 28
2.5.1 Gamification *28*

2.5.2 Gamification methodologies *30*
2.5.3 Gamification implementation process *32*
2.5.4 Gamified phishing and malware cyber security training programme *32*
2.6 TO COMPARE EMPLOYEES' EXPERIENCE WITH THE TRADITIONAL AND GAMIFIED CYBER SECURITY TRAINING PROGRAMMES QUANTITATIVELY 33
2.6.1 Employee training experience and engagement *33*
2.7 THEORETICAL FRAMEWORK 34
2.8 SUMMARY 38

CHAPTER 3. RESEARCH METHODOLOGY 40

3.1 RESEARCH APPROACH 40
3.2 RESEARCH DESIGN 40
3.3 DATA COLLECTION METHODS 40
3.4 POPULATION AND SAMPLE 41
3.4.1 Population *41*
3.4.2 Sample and sampling method *41*
3.5 THE RESEARCH INSTRUMENT 41
3.6 PROCEDURE FOR DATA COLLECTION 42
3.7 DATA ANALYSIS STRATEGIES AND INTERPRETATION 43
3.8 POSSIBLE LIMITATIONS AND CHALLENGES OF THE STUDY 43
3.9 QUALITY ASSURANCE 43
3.9.1 External validity *43*
3.9.2 Internal validity *44*
3.9.3 Reliability *44*
3.10 ETHICAL CONSIDERATIONS 44
3.11 PROPOSED SCHEDULE AND TIMELINES 45

CHAPTER 4. PRESENTATION AND DISCUSSION OF RESULTS 47

4.1 INTRODUCTION 47
4.2 RESULTS AT A BUSINESS AREA LEVEL 48
4.3 RESULTS PERTAINING TO THE HYPOTHESIS 56
4.4 SUMMARY 68

CHAPTER 5. CONCLUSIONS & RECOMMENDATIONS 69

5.1 INTRODUCTION 69
5.2 CONCLUSIONS REGARDING THE CYBER THREAT LANDSCAPE OF THE SOUTH AFRICAN BANKING INDUSTRY, IDENTIFYING TWO MAJOR CYBER THREATS 69
5.3 CONCLUSIONS REGARDING THE DESIGN OF A TRADITIONAL CYBER SECURITY TRAINING PROGRAMME FOR TWO MAJOR SOUTH AFRICAN BANKING INDUSTRY CYBER THREATS 70
5.4 CONCLUSIONS REGARDING GAMIFYING A TRADITIONAL CYBER SECURITY TRAINING PROGRAMME FOR TWO MAJOR SOUTH AFRICAN BANKING INDUSTRY CYBER THREATS 70

5.5 CONCLUSIONS REGARDING THE COMPARISON OF EMPLOYEES' EXPERIENCE WITH THE TRADITIONAL AND GAMIFIED CYBER SECURITY TRAINING PROGRAMMES QUANTITATIVELY 71
5.6 RECOMMENDATIONS 72
5.6.1 Organisations in the South African banking industry 72
5.7 CONCLUSION AND SUGGESTIONS FOR FURTHER RESEARCH 75
REFERENCES 78
APPENDIX A - RESEARCH INSTRUMENT, CONSENT & INFORMATION SHEET 87

LIST OF TABLES

Table 1: Key phishing attacks 25

Table 2: Examples of malware and related attributes (NIST, 2022) 26

Table 3: Proposed research project schedule and timeline 45

Table 4: Consistency table showing research objectives, hypothesis, data collection and data analysis 46

Table 5: Showing the cyber security training experience statements statistics across different departments/business areas 55

Table 6: One-sample test for the gamified training experience statements 65

Table 7: One-sample test for the traditional training experience statements 66

LIST OF FIGURES

Figure 1: First gamification methodology for cyber security training, adapted from Qusa & Tarazi (2021, p. 680) 34

Figure 2: Third gamification methodology for cyber security training, adapted from Silic & Lowry (2020, p. 132-139) 36

Figure 3: Pie charts depicting gamified cyber security training experience responses 59

Figure 4: Pie charts depicting traditional cyber security training experience responses 62

LIST OF ACRONYMS

AR – Augmented Reality

ENISA – The European Union Agency for Cybersecurity

Hyp – Hypothesis

NIST – National Institute of Standards and Technology

N/A – Not Applicable

HR – Human Resources

IT – Information Technology

LMS – Learning Management System

RO – Research Objective

SDT – Self-Determination Theory

SPSS – Statistical Software Package for Social Science

VR – Virtual Reality

CHAPTER 1. INTRODUCTION

1.1 Statement of purpose

The aim of the study is to examine the traditional cyber security awareness and training programmes in the South African banking industry using modern methodologies (specifically gamification) in order to assess employee training engagement. The literature related to user awareness, user engagement, user behaviour, cyber security culture, cyber threats, and training engagement methods is considered in this study. Consequently, when comparing literature on the traditional training methods, the modern or gamified methods are analysed to gain an understanding of the improvements in employee training engagement. The focus is also on literature and theories that guide the research objectives and identify critical models for enhancing cyber security training engagement.

1.2 Background of the study

The human element is acknowledged to be the weakest link and the easiest target within the organisation, forming the foundation for attack vectors. Consequently, cyber security training is employed as a preventative measure to create awareness and strengthen the weakest element in the chain.

There are regular patterns of new and advanced technological changes in the banking industry, which give rise to the need for human behavioural changes in order to combat the introduced cyber challenges (Holdsworth & Apeh, 2017, p. 113); Mai & Tick, 2021, p. 84). These cyber challenges are addressed through the implementation of cyber security training programmes (herein referred to as training programmes) for bank employees.

Training programmes are implemented within banks to augment employees' cyber security knowledge and safeguard both them and the organisation from potential cyber threats (Hu, Hsu & Zhou, 2021, p. 1). The training programmes are tailored to address current cyber security issues in the economy, and to promote awareness among bank employees (Hu et al., 2021, p. 4). The training programmes are proven to be a

fundamental and central strategy employed to govern the security posture of the organisations (Hu et al., 2021, p. 6). As per the National Institute of Standards and Technology (NIST), organisations that do not integrate training programmes would face a higher likelihood of experiencing more cyber-attacks through the human element (Wilson & Hash, 2003). Several academic literature sources indicate that employees often succumb to cyber-attacks due to their lack of security knowledge (Hu et al., 2021, p. 4). Therefore, establishing and integrating a robust training programme should enhance employees' comprehension of current cyber security issues, tools, and other preventive measures against cyber security incidents within the organisation (Hu et al., 2021, p. 3).

While training programmes bolster the security posture, including security governance, within the organisation, the economics of cyber security play a vital role in determining the required methods to enhance employee training engagement and minimise cyber security damage (Wirth, 2017). These methods may encompass scenario-based engagement on prevailing cyber security issues in the banking industry, where employees are trained to serve as the first line of defence. Conversely, multiple training methods that may leverage key capabilities to attract and engage with employees; however, there is limited investment in this initiative. The economics of cyber security revolves around the decision of whether to invest in targeting the human element through effective training engagement, or investing in technological capabilities to prevent cyber threats (Wirth, 2017).

An alignment exists between the economics of cyber security and a focus on investment in technological capabilities. The continuous increase in security and technological complexities needs to be emphasised (Wirth, 2017). Consequently, additional investment in technical capabilities could address short-term challenges. Therefore, the investment in modernising traditional methods of cyber security training for employees may offer long-term preventive solutions through the human element for organisations. Moreover, the transformation of traditional methods can bring forth new tools and technologies to enhance the synergy between technology and humans, facilitating effective decision-making (Wirth, 2017). For instance, this can involve improving an organisation's incident response processes or procedures.

As mentioned, it is essential to consider the role of technology and its impact on instructional methods, when evaluating different methods to cyber security training. It is important to understand the conceptual levels of traditional and modern cyber security training methods and determine where gamification fits into this framework.

To set the context, traditional training methods typically encompasses conventional instructional methods that have been used for years, which include communicating with employees through general modes such as pamphlets, posters, newsletters, articles on the intranet, in-person and online training talks, discussion forums, blogs, videos, centralised training modules, lectures, textbooks, and slide-based presentations (Sharif & Ameen, 2020, p. 152; Haney, & Lutters, 2020, p. 3; Angafor, Yevseyeva, & He, 2020, p. 2). These methods often rely on a linear approach, with instructors delivering information to learners in a one-way manner.

On the other hand, modern cyber security training leverages technology and innovative approaches to enhance the learning experience. This can involve interactive and immersive techniques that actively engage learners and simulate real-world scenarios. Additionally, modern training methods often utilise a variety of tools, such as virtual reality (VR), augmented reality (AR), simulations, and gamification (Wang et al., 2018). These modern method alternatives will be further discussed in this research paper.

Gamification introduces interactive elements to engage learners and motivate their active participation. It incorporates game mechanics, such as challenges, rewards, leader boards, and progress tracking, to make the learning experience more interactive and enjoyable. By leveraging gamification, employees are inspired, motivated, and encouraged to actively participate in cyber security training (Robson, Plangger, Kietzmann, McCarthy & Pitt, 2015; Sharif & Ameen, 2020, p. 154). Positive reinforcement techniques, such as badges, a point system, leader boards, avatars, target goals, and rewards, are employed to enhance training engagement (Sharif & Ameen, 2020, p. 154).

Hence, adoption of gamification in cyber security training offers several advantages over traditional methods. Firstly, it captures employees' attention and fosters a sense of enjoyment, transforming training from a perceived task to an engaging experience (Sharif & Ameen, 2020, p. 153). This increases the likelihood of employees willingly

participating in the training and retaining the knowledge imparted. Secondly, gamification allows for personalised learning experiences by tailoring the training content to employee roles and responsibilities (Sharif & Ameen, 2020, p. 154). This ensures that employees receive training relevant to their specific cyber security needs, enhancing their understanding and application of best practices.

Furthermore, modern methods of cyber security training leverage technology and applications to deliver gamified content (Robson et al., 2015). This enables organisations to reach a wider audience and provide training that is accessible anytime and anywhere. The use of digital platforms also facilitates the tracking of training progress, allowing organisations to assess employee engagement, comprehension, and compliance. Therefore, transforming traditional cyber security training into a game-like format, gamification aims to increase learner engagement, retention, and application of knowledge.

Considering the conceptual levels of traditional and modern cyber security training methods addressed, it is evident that gamification falls under the modern training methods. While traditional training methods, including PowerPoint presentations, can incorporate multimedia elements, they do not inherently include the interactive and game-like aspects that define gamified training (Haney, & Lutters, 2020, p. 3). Therefore, gamification should be considered as a distinct approach within the broader modern cyber security training landscape.

Hence, the context provides clear notable distinctions in terms of strategy, engagement, and effectiveness when comparing traditional and modern methodologies to cyber security training. These methods aim to disseminate information and raise awareness about cyber security practices. However, some methods often lack personalisation and fail to target specific employee roles and responsibilities within the organisation (Sharif & Ameen, 2020, p. 155).

For future studies, the application of gamification can be considered, utilising different human behaviour or psychology frameworks to categorise and assign employees to risk groups (Alshaikh, Naseer, Ahmad, & Maynard, 2019). These risk groups should be the target of cyber security training that specifically addresses their deficiencies in knowledge and application of particular cyber security topics. For instance, a scale for

risk groups can be incorporated into the capability of a rewards mechanism within the Learning Management System (LMS), thereby enhancing training engagement. In addition to risk groups, studying the effects of age classification on responses to gamification is an intriguing future research area that can shed light on the preferences and effectiveness of gamified experiences across different age groups. Understanding how age influences employees' responses to gamification can help design more engaging and effective experiences tailored to specific age groups.

1.3 Research problem

The threat landscape is comprised of numerous cyber threats that impact organisations in the South African banking industry. These cyber threats are continuously advancing and emerging. According to Mcanyana, Brindley & Seedat (2020, p. 7), an overview of the cyber threat landscape in South Africa reveals that organisations are more likely to face significant cyber-attacks due to the insufficient investment in cyber security prevention mechanisms. For example, South Africa lacks stringent cybercrime regulations and legislation pertaining to cybercrime (Mcanyana, Brindley & Seedat, 2020, p. 7), and most notably, there is a lack of adequate cyber security awareness or knowledge among employees (Mcanyana, Brindley & Seedat, 2020, p. 7).

There is a growing recognition of the human element as the primary target for cyber-attacks, highlighting the need to address this aspect rather than solely focusing on technology and infrastructure. Although technological infrastructure and capabilities are in place to address and remediate cyber threats, "hacking the human" is the easiest target for cybercriminals. Cybercriminals often exploit the vulnerabilities of employees through social engineering and manipulation techniques. To combat this issue, many banks in South Africa are taking proactive measures by implementing cyber security training programmes. In the past, traditional training methods have been employed to educate employees about cyber security best practices (Angafor, Yevseyeva, & He, 2020, p. 2). However, with the evolving threat landscape and the need for engaging and effective training methodologies, some banks are embracing modern methodologies, including gamification.

Although gamified training in cyber security is relatively new, limited literature exists on the methodologies and effectiveness of these approaches (Angafor, Yevseyeva, & He, 2020, p. 3). This research gap underscores the need for further exploration and investigation into the gamification of cyber security training. By conducting rigorous studies and sharing findings, organisations can gain valuable insights into the efficacy of gamification and refine their training strategies accordingly.

Hence, considering the focus of the economics of cyber security within organisations in the South African banking industry, an examination is conducted on gamification methodologies to determine the most suitable method for enhancing engagement in cyber security training. Numerous studies demonstrate that gamified training methods are more effective in terms of training engagement (Sharif & Ameen, 2020, p. 152). However, there is limited literature available on the gamification methodologies that can be applied to specific cyber threats in order to improve the engagement in cyber security training within the South African banking industry.

Therefore, this research investigates gamification methodologies that can be applied to two prevailing major cyber threats: phishing and malware. Phishing and malware have been selected to cover different methods of attack delivery. For example, phishing attacks are carried out through phone calls, emails, or messaging, while malware attack manifest as viruses that can lead to ransomware attacks. Furthermore, these two cyber threats are chosen to ensure consistency in knowledge and experience from a training content standpoint.

1.4 Research objectives

The aim of this research is to investigate the gamification methodologies utilised in cyber security training to improve the rate of engagement within the South African banking industry. The study encompasses interconnected themes of cyber threats, threat landscape, training, awareness, and gamification methodologies. As mentioned previously, a comprehensive discussion is formulated to present findings and implications based on these cyber security themes. The following research objectives lay the groundwork for a thorough analysis of literature and investigation in this research:

1.4.1 *Research objective 1*

To analyse the cyber threat landscape of the South African banking industry, identifying two major cyber threats.

The first research objective focuses on the review of literature that establishes a contextual foundation for comprehending the existing cyber security threat landscape. The cyber security threat landscape indicates and illustrates the prevailing cyber security issues and challenges encountered within the South African economy. While the cyber threat landscape encompasses numerous threats, this research selects two major cyber threats, phishing and malware, for examination and testing within a cyber security training programme.

Phishing and malware are chosen to cover distinct methods of attack delivery. For example, phishing attacks are carried out through phone calls, emails, or messaging. Conversely, malware attacks manifest in a form of viruses that can initiate ransomware attacks. Additionally, the selection of these two cyber threats ensures consistency in knowledge and experience from a training content perspective.

1.4.2 *Research objective 2*

To design a traditional cyber security training programme for two major South African banking industry cyber threats.

The second research objective involves mapping the two chosen major cyber threats from the cyber threat landscape into the design of a traditional cyber security training programme. The components and approach of the programme in addressing the cyber threat content were formulated.

1.4.3 *Research objective 3*

To gamify the traditional cyber security training programme for two major South African banking industry cyber threats.

The third research objective involves synthesising the design of a traditional cyber security training programme with gamification methodologies. It is crucial to

understand the gamification ecosystem, examine gamification features, and apply gamification methodologies to the two selected major cyber threats in this research. Building upon the first research objective, this study will explore and apply gamification methodologies to the two chosen major cyber threats, phishing and malware. For future research, additional cyber threats may be incorporated into the gamification methodologies used for cyber security training.

1.4.4 *Research objective 4*

To compare employees' experience with the traditional and gamified cyber security training programmes quantitatively.

The fourth research objective involves evaluating both the traditional and gamified training programmes by comparing the experiences of employees. This research objective aims to highlight the advantages of adopting a gamified approach to cyber security training. It also seeks to provide bank management with insights into the use of gamification methodologies for phishing and malware, and to gather feedback from employees that can be incorporated into current cyber security training programmes.

The null hypothesis of this research assumes that traditional cyber security training enhances employees' knowledge, awareness, and engagement in the banking industry. The research objectives for this study test the null hypothesis against the alternative hypothesis, which state that "gamification methodologies embedded into training programmes improve employee engagement."

1.5 Rationale

This research contributes to the existing literature on cyber security training by implementing and utilising gamification methodologies. South African banks, for example, can explore new methods to foster a cyber security training culture within their environments. Establishing a robust cyber security training programme with positive reinforcement mechanisms can help organisations in reducing potential cyber threats. Additionally, the research findings may reveal gamification application strategies that South African banks can easily incorporate into their environments. Gamification proves to be an effective alternative to traditional methodologies for cyber

security training (Abawajy, 2014, p. 242). By utilising gamification methodologies, employee experience and engagement with the training content can be enhanced, avoiding a mere “compliance tick-box exercise” (Abawajy, 2014, p. 242; Angafor, Yevseyeva, & He, 2020, p. 2). The interactive nature of gamification is a key advantage when compared to traditional methods. Furthermore, the voluntary aspect of engaging with game-based scenarios can stimulate employees’ curiosity and attention, resulting in improved training engagement. In contrast, content-driven methods alone (traditional methods) may leave gaps where employees can become unfocused on the learning (Abawajy, 2014, p. 242; Bada, Sasse, & Nurse, 2019, p. 2).

According to ENISA (2022) and Tanner & Preiksaitis (2023, p. 6), opportunities for cybercrime have reached their peak during the Covid-19 pandemic. Cybercriminals employ various methods to exploit humans’ vulnerabilities, such as Covid-19 vaccination-related scams, phishing emails containing false information about new Covid-19 variants, and malware attacks tailored to the remote working situation. Additionally, the proliferation of misinformation and knowledge transfer has underscored the importance of cyber security training. Employees in the South African banking industry must be aware of current cyber threats in order to prevent falling victim to them and causing severe consequences for the organisation.

There is limited academic literature that specifically focuses on gamification frameworks (Qusa & Tarazi, 2021, p. 678), cyber security training methodologies to enhance awareness (Sharif & Ameen, 2020, p. 152), and the application of gamification to cyber security training (Rieff, 2018). However, this research aims to integrate literature on training programmes applied to gamification methodologies in order to improve engagement and awareness.

1.6 Delimitations of the study

During the analysis process, limitations are encountered in this research. Firstly, the data collection process was restricted to employees employed in any bank in South Africa. The training engagement was tested and evaluated in the results, rather than the knowledge of the topics.

Additionally, in this research, the banks and the respondents are anonymised. Consequently, the respondents are required to provide the generic department in which they work. This information will aid in the classification of respondents into different groups and can be utilised for future studies. Lastly, the Likert scale will be employed in the questionnaire to gather insights on comparisons of traditional or modern cyber security training methodologies for the purpose of improving training engagements.

These limitations are duly considered and should be considered when interpreting the findings of this research. Future studies can build upon these limitations and address them to further enhance the understanding of cyber security training in the banking industry.

1.7 Definition of terms

The following terms are defined in this research for the purpose of understanding and clarification:

Cyber threats: A cyber threat is an unauthorised intrusion into an organisation with the intention of maliciously impacting technology, people, and organisation itself (NIST, 2022). According to NIST (2022), a cyber threat is an event that could occur through a system or human element, which affects the modification of data, denial-of-service, unauthorised access, and disclosure and destruction of assets and information.

Cybercriminals: Cybercriminals are individuals who engage in illegal activities using people and technology as their tools (Sammons & Cross, 2017).

Cryptojacking: Cryptojacking is a cyber threat involves authorising devices for cryptocurrency mining (Carlin et al., 2019, p. 3; Kaspersky, 2022d).

Disinformation: Disinformation refers to the fabrication of content or information that is disseminated over digital platforms and through word-of-mouth (Shu et al., 2020). An example of disinformation is fake news shared on social media.

Gamification: According to Robson et al. (2015), gamification transforms information or context into a game design application. Gamification inspires, motivates, and

encourages employees to engage with the training content (Robson et al., 2015; Sharif & Ameen, 2020, p. 151).

Malware: Malware is an unauthorised program that is loaded onto a person's device to compromise and carry out harmful actions that target the confidentiality, integrity, and availability of their information, applications, and operating system (NIST, 2022).

Phishing: Phishing is a social engineering technique used by cybercriminals to trick employees into providing sensitive information through a link in a fake email or website (NIST, 2022). According to NIST (2022), cybercriminals attempt to obtain sensitive data such as bank account information, passwords, identity numbers, and credentials.

Social engineering: Social engineering is a cyber threat and can be used as a technique to execute a phishing attack. Cybercriminals employ this technique to trick individuals into divulging information that can be used to compromise a network or system (NIST, 2022). According to NIST (2022), information such as passwords or credentials can us used to compromise a network or system.

Threat landscape: The threat landscape encompasses the entire range of cyber threats that have the potential to harm or cause damage to organisations and employees (Babate et al., 2015, p. 114; Kaspersky, 2022a). According to Babate et al. (2015, p. 114) and Kaspersky (2022d), cyber threats include a group of dangerous techniques such as phishing and malware.

1.8 Assumptions

In the research design process, certain assumptions are considered, including the respondents' solid understanding of phishing and malware concepts. Furthermore, it is assumed that the feedback provided by the respondents is reliable. Lastly, it can be assumed that if majority of respondents from the same department achieve similar quantitative results, this will serve as justification for the effectiveness of the gamification methodologies in improving training engagement.

1.9 Summary

This chapter serves as an introduction to the research components that will be discussed in the upcoming chapters. The salient points summarised in this chapter are as follows:

- This research focuses on the application of gamification methodologies to two major cyber threats, namely phishing and malware within the South African banking industry.
- The research objectives include analysing the cyber threat landscape of the South African banking industry, designing traditional and gamified cyber security training programme for the identified threats, and quantitatively comparing the experiences of employees with both training programmes
- Quantitative data is collected through a questionnaire that includes both traditional and gamified training elements to assess the training engagement of bank employees.

The literature review will provide the necessary context to understand the implementation and findings of gamification methodologies in relation to training engagement.

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

This research chapter aims to extend and build upon the existing literature on cyber security training and awareness. According to Petrenko (2019), human error is responsible for ninety percent (90%) of cyber-attacks. Therefore, it is crucial to understand the current cyber security threats and trends that organisations can utilise to proactively assess risks and develop mitigation strategies (Wilding, 2016). Additionally, the training engagement has become even more critical due to the opportunities that the Covid-19 pandemic has presented for cybercriminals to exploit employees.

The research objectives and hypothesis are thoroughly analysed, incorporating the design and implementation methodologies derived from relevant literature. The hypothesis is examined in relation to the applicable research objectives: “Gamification methodologies embedded into cyber security training programmes improve employee engagement.”

2.2 Cyber security training

In this research context, cyber security training can be defined as the provision of security best practices knowledge and training to employees in the South African banking industry (Abawajy, 2014, p. 237). Furthermore, the levels of knowledge that employees possess regarding cyber security best practices are considered. For example, Abawajy (2014, p. 239) states that cyber security training significantly reduces cyber damage and costs following a cyber-attack.

A robust cyber security training programme is developed with the aim of enhancing employees’ ability to recognise and report malicious or suspicious activities, thereby safeguarding the organisation from cyber threats and attacks (Abawajy, 2014, p. 237). The training programmes are implemented on an ongoing basis to ensure that all employees remain informed about current cyber threats and trends, along with the

relevant mitigation measures to defend and protect themselves and the organisation (Abawajy, 2014, p. 237).

It is crucial to highlight that, just like organisations invest in cyber security technology, the human component in driving training serves as the first line of defence (Abawajy, 2014, p. 237).

According to Al-Daeef, Basir, & Saudi (2017), numerous studies have tested the efficiency and effectiveness of cyber security training. Additionally, well-designed methodologies can enhance engagement in cyber security training (Al-Daeef et al., 2017).

2.3 To analyse the cyber threat landscape of the South African banking industry, identifying two major cyber threats

This section aims to conduct an analysis of the current cyber threats in South Africa within the broader cyber threat landscape and identify two major cyber threats that significantly impact the banking industry. Phishing and malware have been specifically selected to encompass distinct attack delivery methods. For example, phishing attacks are executed through various channels such as phone calls, emails, or messaging platforms. On the other hand, malware attacks involve the deployment of malicious software, such as viruses, which can lead to ransomware attacks. Additionally, the choice of these two cyber threats serves to ensure the consistency in knowledge and experience within the training content perspective.

2.3.1 *Cyber threat*

An unauthorised intrusion into an organisation with the intent of maliciously impacting any technology, people, and organisation is referred to as a cyber threat (NIST, 2022). According to NIST (2022), a cyber threat is an event that could occur through a system or human element, resulting in the modification of data, denial-of-service, unauthorised access, as well as the disclosure and destruction of assets and information.

Current prime cyber threats, as stated by ENISA (2022), include ransomware, malware, phishing, disinformation, non-malicious threats caused by human error, crypto jacking, and data breaches.

2.3.2 *Cyber attack*

A malicious attack conducted through cyberspace that targets people and an organisation by damaging and disrupting the environment, including the confidentiality, integrity, and availability of data and assets, is referred to as a cyber-attack (NIST, 2022).

According to Mcanyana et al. (2020), recent central banking South African cyber-attacks are related to banking malware, cryptocurrency mobile device crimes, credit card fraud (through phishing), and banking application fraud (through phishing).

2.3.3 *Cyber security threat landscape*

An overview of the most recent cyber threats based on public data and cyber threat intelligence resources is depicted by the cyber security threat landscape (Pieterse, 2021). Additionally, according to Pieterse (2021), emerging threat trends are also included in the cyber threat landscape. The threat trends are related to current threats that are trending in the economy, such as remote working security risks, ransomware attacks due to more ingenious social engineering techniques, cloud security threats due to more employees and organisations migrating to the cloud, and device security threats (Babate et al., 2015, p. 114; Kaspersky, 2022b).

In the South African banking industry, organisations invest in the cyber threat landscape to discover critical cyber threats that emerge through the evolution and adaptation of new economic technologies (Petrenko, 2019). The cyber threat landscape is used by organisations to accelerate various scenario mitigation plans and formulate strategic decision-making regarding the organisation’s security as cyber-attacks advance.

2.3.4 *Phishing*

Social engineering techniques are used by cybercriminals to carry out phishing, wherein someone is tricked into obtaining sensitive information through a link in a fake email or website (NIST, 2022). It is stated by NIST (2022) that sensitive data such as bank account information, passwords, identity numbers, and credentials are targeted by cybercriminals. The following table illustrates the critical types of phishing attacks:

Phishing attack	Description
Email phishing	Cybercriminals use an attack to trick someone into obtaining sensitive information through a link in a fake email (NIST, 2022).
Vishing	Vishing is when a person is scammed into giving personal information through misdirected, automated or impersonated phone calls (Fakieh, & Akremi, 2022, p. 1; Jones et al., 2021, p. 2; Kaspersky, 2022b).
Smishing	Smishing involves automated or impersonated text messages that scam employees into giving personal information using a provided contact number or a fake link (Jain et al., 2022, p. 2; Kaspersky, 2022b; Rahman et al., 2023, p. 1).
Spear phishing	Cybercriminals track a specific employee or organisation to obtain sensitive information through a link in a fake customised email (NIST, 2022).
Whaling	Whaling targets executives, senior personnel, or key employees in organisations to obtain sensitive information through a link in a fake customised email (NIST, 2022).

Table 1: Key phishing attacks

2.3.5 *Malware*

A form of an unauthorised program known as malware is loaded onto a person's device with the aim of compromising and undertaking harmful actions towards the confidentiality, integrity, and availability of the person's information, applications, and operating system (NIST, 2022). According to NIST (2022), the following table includes some examples and attributes of malware:

Malware	Attribute
Spyware	Software that violates a person's privacy and us secretly installed.
Viruses	A malicious software, reliant on activation that spreads as it attaches to files to infect a device.
Worms	Like a virus but is independently run and self-replicates to infect a device.
Trojan horses	Embedded into valuable programs, processing a hidden malicious capability to destroy, alter, and collect confidential information.
Adware	Advertisements or pop-ups generated online that, when clicked on, can download malicious software.

Table 2: Examples of malware and related attributes (NIST, 2022)

2.4 To design a traditional cyber security training programme for two major South African banking industry cyber threats

According to Abawajy (2014, p. 240), various cyber security training delivery methodologies exist. However, with an emphasis on traditional methodologies, the design of the cyber security training programme on phishing and malware in the context of a bank in South Africa is covered in this section.

2.4.1 *Traditional training methodologies*

The traditional training programmes follow conventional methodologies, which can be presented in either electronic or paper formats (Abawajy, 2014, p. 240; Aldawood & Skinner, 2019, p. 7). In the paper format, the training material is disseminated to employees through pamphlets, posters, and newsletters (Abawajy, 2014; Aldawood & Skinner, 2019, p. 7; Angafor, Yevseyeva, & He, 2020, p. 2). These materials typically contain general cyber security best practices and are not tailored to specific employee groups within the organisation (Abawajy, 2014; Angafor, Yevseyeva, & He, 2020, p. 3). They often serve as basic reminders of cyber security tips and address topical issues relevant to that particular period (Abawajy, 2014, p. 242).

Alternatively, these training materials can also be translated into an electronic format (Abawajy, 2014, p. 242). Once in electronic form, the content can be made available on various channels, including the organisation's intranet, websites, and internal communication applications.

However, one limitation of these traditional delivery methods is that they do not provide statistical information regarding the number of employees who have read, understood, and implemented the training (Aldawood & Skinner, 2019, p. 7). In other words, it is difficult to gauge the effectiveness of the training or assess employee compliance.

Overall, traditional training programmes encompass methodologies that involve the use of either paper-based or electronic materials to educate employees on generic cyber security best practices. These materials are often distributed through pamphlets, posters, newsletters, or electronic channels such as intranets and websites (Abawajy, 2014, p. 240; Aldawood & Skinner, 2019, p. 7; Angafor, Yevseyeva, & He, 2020, p. 2). However, these methods lack the ability to track and measure employee engagement, understanding, and application of the training content.

2.4.2 *Traditional phishing and malware cyber security training programme*

When designing a traditional cyber security training programme for phishing, there are essential components that employees need to be educated on, such as tools for identifying and reporting the phishing email or malware incidents (Miranda, 2018, p. 7).

These key components are embedded into the cyber security training programme, which is rolled out to all employees on an ongoing basis.

The curating of phishing and malware content based on relevant resources or current banking scenarios is the first activity in the cyber security training programme. Following this, reviews, amendments, and approvals take place. The second activity involves the evaluation of a delivery method to be used for presenting the developed training content to employees. Lastly, the training is distributed to employees using traditional methodologies (Miranda, 2018, p. 7).

The concerns surrounding traditional methodology training content being perceived as mundane due to the low attention span of employees during training have been highlighted by Aldawood & Skinner (2019, p. 7), taking into consideration the above-mentioned activities.

2.5 To gamify the traditional cyber security training programme for two major South African banking industry cyber threats

According to Holdsworth & Apeh (2017, p. 113), the attention and engagement of employees can be enhanced through gamified cyber security training. When compared to the traditional cyber security training programme, minimal statistical information on the training's success is provided by the traditional delivery methods (Holdsworth & Apeh, 2017, p. 113). While this may suffice for some organisations, the cyber threat landscape reveals numerous targeted cyber-attacks on organisations in the banking industry. Therefore, cyber security training plays a crucial role in creating awareness among banking employees.

As a result, the role of gamification becomes essential in attracting employees to cyber security training. This research section will specifically focus on the gamification of a traditional cyber security training programme for phishing and malware.

2.5.1 *Gamification*

In the context of this research, gamification refers to applying or embedding gaming mechanisms into training to empower employees with the security tools and knowledge

and ultimately improving training engagement (Holdsworth & Apeh, 2017, p. 113; Scholefield & Shepherd, 2019, p. 4; Silic & Lowry, 2020, p. 131). Gamification aims to capture employees' attention with design techniques that are not mundane (Holdsworth & Apeh, 2017, p. 113). The gamification process simulates goal achievement through engaging and motivational means (Hanus, & Wu, 2016; Holdsworth & Apeh, 2017, p. 113; Scholefield & Shepherd, 2019, p. 5).

In addition to gamification, several alternative methods can be utilised for cyber security training, offering a range of approaches to engage employees and enhance their understanding of cyber security best practices (Holdsworth & Apeh, 2017, p. 113; Scholefield & Shepherd, 2019, p. 5). The following alternative methods warrant consideration:

- Microlearning modules: The delivery of training content in bite-sized modules characterises microlearning. These modules focus on specific topics or concepts, facilitating employees' absorption and retention of information. Microlearning can employ various formats such as short videos, quizzes, infographics, or interactive content, enabling employees to easily consume the material (Thomas, Baral, & Crocco, 2022, p. 19; Orwoll et al., 2018, p. 7).
- Serious games: Purposefully designed for training purposes, serious games combine educational content with engaging gameplay. These games simulate cyber security scenarios, challenges, and decision-making processes, allowing employees to learn and practice their skills within a gamified environment. By providing a realistic and interactive experience, serious games foster active learning and skill development (Alqahtani, & Kavakli-Thorne, 2020, p. 4; Caserman et al., 2020, p. 3-9; Švábenský et al., 2018, p. 5; Wu et al., 2021, p. 3).
- Virtual Reality (VR) and Augmented Reality (AR): VR and AR technologies offer immersive experiences where employees can interact with virtual environments relevant to cyber security. These technologies provide realistic simulations, hands-on training opportunities, and a controlled setting for practicing skills. By immersing employees in simulated scenarios, VR and AR enhance their understanding and preparedness for real-world cyber security incidents (Alqahtani, & Kavakli-Thorne, 2020, p. 4; Wang et al., 2018).

- Phishing simulations: Phishing simulations involve the distribution of mock phishing emails to employees, assessing their ability to detect and respond to phishing attacks. Such simulations raise awareness about the risks associated with phishing and educate employees on how to identify and report suspicious emails (Al-Daeef et al., 2017; Miranda, 2018, p. 10).

When selecting cyber security training methods, businesses should carefully consider their specific training goals, available resources, and the characteristics of their employee population. Evaluating the effectiveness of these alternative methods through assessments, feedback, and metrics can contribute to refining cyber security training strategies and improving overall training outcomes. By adopting a tailored approach to cyber security training, organisations can maximise employee engagement, knowledge retention, and the practical application of cyber security best practices.

2.5.2 *Gamification methodologies*

Gamification methodologies have gained significant attention and recognition in the context of cyber security training. By infusing game-like elements into the training process, these methodologies aim to enhance engagement, motivation, and knowledge retention among employees. This discussion will delve into the benefits and considerations associated with gamification methodologies in cyber security training.

One key advantage of gamification methodologies is their ability to make training more enjoyable and interactive. By incorporating challenges, rewards, leader boards, and progress tracking, employees are encouraged to actively participate in the learning process (Abawajy, 2014, p. 242; Scholefield & Shepherd, 2019, p. 4). This active engagement can foster a sense of excitement and curiosity, transforming training from a mundane task into an engaging experience. Consequently, employees are more likely to willingly participate and retain the knowledge imparted during the training.

Furthermore, gamification methodologies offer personalised learning experiences tailored to employee roles and responsibilities (Abawajy, 2014, p. 242; Scholefield & Shepherd, 2019, p. 4). This customisation ensures that employees receive training relevant to their specific cyber security needs, improving their understanding and

application of best practices. By addressing employee skill gaps and focusing on targeted learning objectives, gamification methodologies can have a direct impact on improving an organisation's security posture.

Gamification methodologies also have the potential to reinforce positive behaviours and encourage continuous learning (Wu et al., 2021, p. 13). Through the use of badges, points systems, leader boards, and rewards, employees are motivated to actively engage with the training content and strive for improvement (Abawajy, 2014, p. 242). This intrinsic motivation fosters a culture of ongoing learning and development, encouraging employees to stay up-to-date with evolving cyber security threats and best practices (Hanus, & Wu, 2016, p. 3).

While the benefits of gamification methodologies in cyber security training are evident, several considerations should be kept in mind. First and foremost, the design of gamified elements should align with the organisation's strategic objectives related to security posture (Abawajy, 2014, p. 242). The gamification should not solely focus on entertainment value but should be designed to effectively impart knowledge and skills that are relevant to the organisation's specific security challenges.

Another consideration is the need for proper implementation and integration of gamification methodologies into the existing training framework. This includes selecting appropriate technologies, platforms, and tools to deliver gamified content effectively (Abawajy, 2014, p. 242; Scholefield & Shepherd, 2019, p. 5). Organisations should also ensure that the gamified elements are intuitive, user-friendly, and aligned with the target audience's preferences and learning styles.

Lastly, it is crucial to regularly evaluate the effectiveness of gamification methodologies in achieving desired learning outcomes (Scholefield & Shepherd, 2019, p. 4). This can be done through the assessment of engagement levels, knowledge retention, and practical application of skills learned (Abawajy, 2014, p. 242). By gathering feedback from employees and monitoring their progress, organisations can identify areas for improvement and make necessary adjustments to optimise the effectiveness of the gamified training approach.

2.5.3 *Gamification implementation process*

In order to gamify training, a complex process must be followed (Sharif & Ameen, 2020, p. 151). The implementation process of gamification follows a lifecycle, encompassing the phases of analysis, design, testing, development or implementation, and monitoring. Further elaborating on the gamification implementation process, the first step involves mapping the objectives of the cyber security training. In the second step, employee groups within respective departments in the organisation, such as human resources (HR), finance, information technology (IT), procurement, marketing and others, are analysed. The third step focuses on examining the design elements and components of gamification. Lastly, the fourth step entails identifying the platforms for disseminating the training and the embedded features, including leader boards, avatars, points systems, reward systems, and game levels. Subsequently, the implemented gamified training is tested and monitored to identify any areas for improvement (Sharif & Ameen, 2020, p. 154).

According to (Sharif & Ameen, 2020, p. 154), the individuals involved in the end-to-end implementation process of the system are the designers. The designers have the responsibility of ensuring that the system workflow of the gamified training fulfils all the functional and operational requirements (Sharif & Ameen, 2020, p. 154). The functions are designed to enhance employees' engagement with the game. Therefore, the designers monitor the level of employee engagement through the technical operations or functionalities incorporated into the system (Sharif & Ameen, 2020, p. 154).

2.5.4 *Gamified phishing and malware cyber security training programme*

According to Miranda (2018, p. 5), conducting phishing simulations in an organisation is regarded as a form of training that aims to better prepare for potential cyber-attacks that an organisation may face. Several phishing tools are available for creating phishing simulations (Miranda, 2018). These tools operate by generating email templates and landing pages, and they provide feedback on the number of employees who respond, click, and enter credentials on the phishing email (Miranda, 2018, p. 8).

Hence, a gamified phishing and malware cyber security training programme can be devised by an organisation. The programme can employ a customised gamification

methodology, such as the development of scenario-based phishing simulations using an approved tool. The phishing simulation is then tested with a pilot group, and any amendments are made before implementing the simulation with all employees. The results of the simulation should be automatically recorded and communicated to employees who have failed the simulation (Miranda, 2018, p. 7). The process is repeated with randomised scenarios to ensure that employees attain a significant level of training.

2.6 To compare employees' experience with the traditional and gamified cyber security training programmes quantitatively

The experience that employees have with training plays a crucial role in determining their level of engagement with the cyber security content. Therefore, this section aims to compare the most effective and efficient cyber security training methodology based on employees' experiences.

2.6.1 *Employee training experience and engagement*

According to He and Zhang (2019, p. 250), as technology and digital transformation continue to evolve in the banking industry, employees are frequently alerted of cyber threats and cyber-attacks through traditional channels such as news, social media, and word-of-mouth. This frequent exposure to cyber security awareness can be overwhelming (He & Zhang, 2019, p. 255).

As the number of cyber threats increases, staff members are constantly informed about the best practices cyber security, including what they should do and how to do it (He & Zhang, 2019, p. 255). However, these overwhelming experiences can lead to negligence in protecting themselves and the organisation, resulting in "security fatigue" (He & Zhang, 2019, p. 255).

Therefore, it is crucial to follow gamification methodologies to enhance engagement and motivation, thereby reducing security fatigue. Additionally, delivering gamified phishing and malware training to employees can help alleviate security fatigue.

2.7 THEORETICAL FRAMEWORK

The theoretical framework forms the basis for this research, supporting the research objectives and hypothesis. Furthermore, there is an acknowledgement of the limited number of gamification theories and frameworks developed in the literature, thus highlighting the contribution for thus research in examining gamification methodologies to enhance engagement.

Several training methodologies identified in the literature have demonstrated that promoting gamification improves training engagement (Alcivar & Abad, 2016; Cechella et al., 2021, p. 7; Filsecker & Hickey, 2014; Hamari et al., 2016, p. 171-172; Ibanez et al., 2014). These methodologies facilitate better learning of cyber security concepts, long term knowledge retention, and practical application of knowledge in various cyber security contexts (Cechella et al., 2021, p. 2). The positive outcomes are based on the employees' experience with the gamified training (Wu et al., 2021, p. 13).

According to Cechella et al. (2021, p. 2), the application of gamification in cyber security training can be designed using two methods. The first method involves a partially designed gaming training experience, while the second method applies to a fully designed gaming experience. Both methods incorporate gamification elements in their design.

By integrating gamification methodologies with traditional training methods, a positive training engagement and user experience can be achieved (Buckley & Doyle, 2017, p. 44; De-Marcos et al., 2016; Wu et al., 2021, p. 13). Based on the literature reviewed, the first gamification methodology for cyber security training engagement is presented in Figure 1 below:

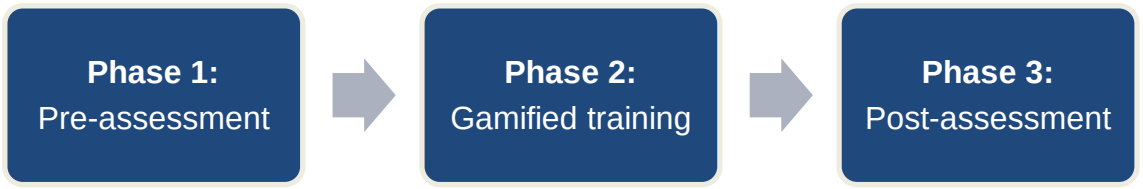


Figure 1: First gamification methodology for cyber security training, adapted from Qusa & Tarazi (2021, p. 680)

The first phase involves assessing cyber security awareness or knowledge through a set of pre-assessment questions on cyber threats such as phishing and malware (Qusa & Tarazi, 2021, p. 680). These questions are presented in a randomised multiple-choice format for each employee and can be retried (Qusa & Tarazi, 2021, p. 680). The difficulty level of the assessment questions varies, but the results are not displayed to maintain engagement for the subsequent gamified training phase (Qusa & Tarazi, 2021, p. 680).

In the second phase, cyber security awareness or knowledge is assessed through cyber threat scenarios (Qusa & Tarazi, 2021, p. 680). The employee starts the training by engaging with gamified components, such as navigating a maze format that presents cyber security tips to reach the end of the maze (Qusa & Tarazi, 2021, p. 680). The maze interface can simulate a workstation or area within the bank. Additionally, an optional timeframe element can be included in the gamified training, and the retry function can enhance the retention of cyber security knowledge. Therefore, scenario-based training in a gamified format improves the retention and engagement with the cyber security training content.

The final phase assesses cyber security awareness or knowledge through a set of post-assessment questions across on the cyber threats covered in the scenario-based game training (Qusa & Tarazi, 2021, p. 680). The results are displayed to the employee, demonstrating the effectiveness of knowledge retention based on the scenario tips provided in the game-based training (Qusa & Tarazi, 2021, p. 680). This framework stores both the pre-assessment and post-assessment results and encourages employees to retake the training with changes in the interface for each iteration (Qusa & Tarazi, 2021, p. 680).

The second gamification methodology for cyber security training utilises a model specific to cyber threats such as phishing or malware to create awareness (Safonov et al., 2020). This model, adapted from Safonov et al. (2020), incorporates scenario-based actions that a cybercriminal could take executing a cyber threat like phishing. The game is designed with tasks that teach employees how to prevent the cybercriminal from infiltrating the organisation (Safonov et al., 2020). The game analytics capture the employee’s phishing knowledge and assign them to a risk group.

Similar to the adapted framework by Qusa & Tarazi (2021, p. 680), the game's interfaces change with each retry and differ based on the employee group.

The third gamification methodology incorporates a theoretical framework for enhancing the efficacy of employee cyber security training. It is well-established that gamification methodologies have a positive impact on employee training engagement (Silic & Lowry, 2020, p. 154; Wu et al., 2021, p. 13). Silic & Lowry (2020, p. 132-139) propose a framework, depicted in Figure 2 below, that aims to improve cyber security training engagement.

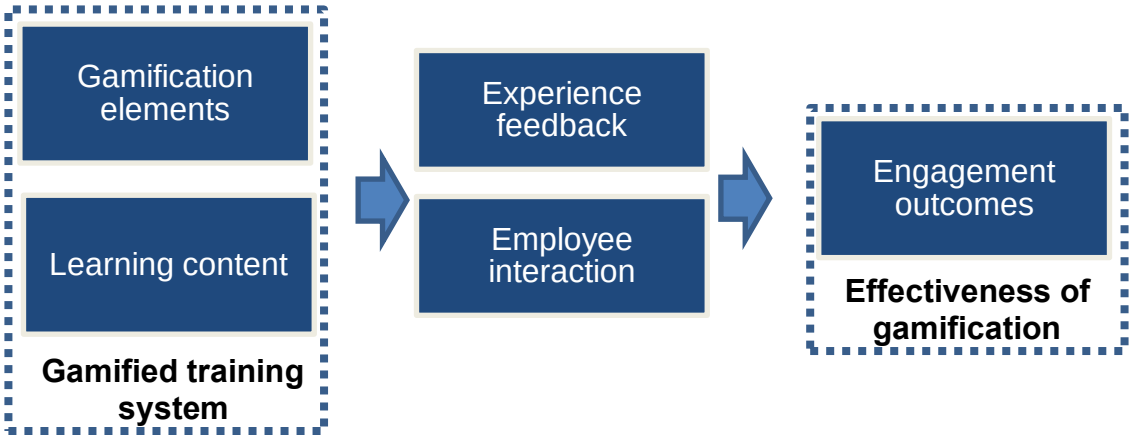


Figure 2: Third gamification methodology for cyber security training, adapted from Silic & Lowry (2020, p. 132-139)

To ensure a comprehensive understanding of gamification, it is important to examine various theories that pertain to shaping behaviour. In this context, the self-determination theory (SDT) and social cognitive theories will be discussed. These theories provide valuable insights into the motivational factors and social influences that impact employees' engagement and behaviour in gamified environments.

The self-determination theory (SDT) is a psychological framework that emphasises intrinsic motivation and personal autonomy as key drivers of human behaviour (Iacono, Vallarino, & Vercelli, 2020, p. 73; Thornton, & Francia, 2014, p. 17; Tobon, Ruiz-Alba, & García-Madariaga, 2020, p. 13). When applied to gamification methods used for cyber security training, SDT can provide valuable insights into the effectiveness and sustainability of these approaches. SDT argues that employees have three basic psychological needs: autonomy, competence, and relatedness. Gamification can tap

into these needs and enhance the training experience by offering choices, challenges, and opportunities for social interaction (Iacono, Vallarino, & Vercelli, 2020, p. 73-74; Thornton, & Francia, 2014, p. 17).

One of the main strengths of SDT in the context of cyber security training is its focus on intrinsic motivation (Iacono, Vallarino, & Vercelli, 2020, p. 73-74). By designing gamified training programmes that align with the employees' inherent interests and values, trainers can foster a sense of autonomy and ownership over the learning process. This can lead to increased engagement, persistence, and enjoyment, as employees feel a sense of personal agency and control. For example, incorporating narrative elements or allowing learners to customise their avatars can create a more immersive and personally relevant experience (Iacono, Vallarino, & Vercelli, 2020, p. 73-74).

Furthermore, SDT highlights the importance of competence development (Iacono, Vallarino, & Vercelli, 2020, p. 73; Thornton, & Francia, 2014, p. 17; Tobon, Ruiz-Alba, & García-Madariaga, 2020, p. 13). Gamification methods can provide employees with clear goals, feedback mechanisms, and progressive challenges, allowing them to acquire and refine the necessary skills in a controlled environment. As employees experience a sense of mastery and achievement, their self-efficacy and confidence in handling cyber security threats can increase, leading to better performance and adherence to secure practices (Iacono, Vallarino, & Vercelli, 2020, p. 73-74; Silic, & Lowry, 2020, p. 15).

In terms of relatedness, SDT emphasises the social nature of human beings. Gamification methods can leverage this aspect by fostering collaboration, competition, or both. By incorporating multiplayer features, leader boards, or team-based challenges, employees can connect with others, share experiences, and develop a sense of community. This social element can enhance motivation, accountability, and the exchange of knowledge and best practices among employees (Iacono, Vallarino, & Vercelli, 2020, p. 73-74; Hanus, & Wu, 2016, p. 5).

Comparatively, social cognitive theories, such as Bandura's social learning theory, offer complementary perspectives on gamification for cyber security training (Banfield, & Wilkerson, 2014, p. 292; Baral, & Arachchilage, 2019, p. 7; Thompson et al., 2022,

p. 565; Silic, & Lowry, 2020, p. 15; Skinner, 2018, p. 4). Social cognitive theories emphasise the role of observational learning, modelling, and reinforcement in shaping behaviour. In the context of gamified training, this means that employees can learn by observing and imitating cyber security experts or successful peers (Banfield, & Wilkerson, 2014, p. 292). Gamification methods can provide opportunities for role-playing, simulations, or virtual mentors, allowing learners to observe and practice effective cyber security behaviours in a safe environment.

While SDT focuses more on intrinsic motivation and the fulfilment of psychological needs, social cognitive theories highlight the importance of external factors, such as social influences and rewards (Banfield, & Wilkerson, 2014, p. 292; Baral, & Arachchilage, 2019, p. 7; Buckley & Doyle, 2017, p. 47; Thompson et al., 2022, p. 565; Silic, & Lowry, 2020, p. 15; Skinner, 2018, p. 4). Both theories can inform the design of gamified training programmes that effectively engage learners, promote skill development, and reinforce secure behaviours.

Several theories support the effectiveness of gamification methods in enhancing engagement in cyber security training. For the purposes of this research, a specific gamification methodology, adapted from Silic & Lowry (2020, p. 132-139), has been employed to guide the design and implementation of the study. The focus of this research is to obtain quantitative results that demonstrate the efficacy of the training engagement, and it should be noted that theories related to behaviour shaping are beyond the scope of this study and have not been included.

2.8 Summary

In the context of the Covid-19 pandemic, which has created new opportunities for cybercriminals to exploit vulnerabilities in human behaviour, a robust cyber security training programme becomes crucial in minimising cyber damage. As cyber-attacks continue to evolve, organisations rely on the cyber threat landscape to expedite scenario mitigation plans and make strategic decisions regarding their security measures. However, the existing literature offers limited insights into the application of gamification methodologies specifically targeting cyber threats. Traditional training delivery methodologies often fail to provide measurable metrics that demonstrate an

improvement in engagement, whereas gamification methodologies utilise metrics that effectively monitor different aspects of engagement.

In conclusion, SDT presents a valuable framework for understanding and enhancing the effectiveness of gamification methods used for cyber security training. By incorporating elements that support autonomy, competence, and relatedness, trainers can create engaging and motivating experiences that foster intrinsic motivation, skill development, and social interaction (Iacono, Vallarino, & Vercelli, 2020, p. 73; Thornton, & Francia, 2014, p. 17; Tobon, Ruiz-Alba, & García-Madariaga, 2020, p. 13). Additionally, social cognitive theories complement SDT by emphasising the role of observation, modelling, and reinforcement in shaping behaviour. By considering these theories in conjunction, trainers can design comprehensive and effective gamified training programmes that promote cyber security awareness and competence (Banfield, & Wilkerson, 2014, p. 292; Baral, & Arachchilage, 2019, p. 7; Thompson et al., 2022, p. 565; Silic, & Lowry, 2020, p. 15; Skinner, 2018, p. 4).

CHAPTER 3. RESEARCH METHODOLOGY

This chapter of the research will discuss the methodology used to conduct this cross-sectional research. The research design is analysed through a questionnaire. The quantitative approach is chosen as the methodological preference for this research. Lastly, a positivist philosophy is adhered to in the conduct of the research.

3.1 Research approach

This quantitative research aims to describe and statistically examine the data to test the hypothesis. In addition, this research focuses on examining gamification methodologies for improved cyber security training engagement in the South African banking industry.

A quantitative research approach is selected to obtain an unbiased understanding through questionnaires. This approach provides numerical results for comparing traditional and gamified methodologies. Organisations in the South African banking industry can utilise these results to make informed decisions regarding training value creation.

3.2 Research design

The questionnaire research design is employed to assess the effectiveness of traditional and gamified training methodologies applied to phishing and malware content in the South African banking industry. Questionnaires are conducted to gather data indicating improvements in cyber security training engagement. Closed questions in the questionnaire determine which training method, traditional or gamified, is more effective in terms of training engagement.

3.3 Data collection methods

Primary data based on knowledge and experiences is collected through questionnaires. Primary data refers to the original data captured or obtained from respondents. This data is collected specifically for this research, where questions are

aligned to the research objectives. The questionnaire questions are related to a customised cyber security training programme aligned with the research objectives. Primary data collection has been selected to collect specific information from respondents to test the hypothesis for this research.

3.4 Population and sample

3.4.1 *Population*

Cyber security is everyone's responsibility. Hence, all employees in an organisation can be targeted by cyber-attacks, signifying the importance of training engagement. The population of this research includes all employees with and without technical knowledge of cyber security concepts in the South African banking industry. It encompasses various departments such as HR, Finance, IT, Procurement, Marketing, and others. All banks are considered for this research to align with the observations based on the South African cyber security threat landscape for the banking industry.

3.4.2 *Sample and sampling method*

A nonprobability convenience sampling method is chosen to determine the sample size for this research. Due to the time horizon of this cross-sectional study, convenience sampling is selected for easy accessibility of respondents. The intended sample size for this study is between 60 and 100 respondents.

Respondents are invited to participate through a shared link to an anonymous questionnaire distributed via instant messaging, social media, and email.

3.5 The research instrument

To ensure the collection of data from a large sample size and assess the effectiveness of data collection, a questionnaire is selected as the instrument for this study (Kyriazos & Stalikas, 2018; Nicewander, 2017). The questionnaire is developed and implemented using the Qualtrics tool. Prior to data collection, a pre-testing phase is

conducted to identify and address any faults or complexities, ensuring the reliability of the question scales (Nicewander, 2017).

The questionnaire comprises various sections and constructs aligned with the research objectives. It begins with three pre-screening questions to determine respondents' eligibility, categorise them into specific groups, and assess their level of cyber training maturity.

For the first and second constructs, knowledge questions are included in a basic multiple-choice format to gather statistical data on employees' understanding of major cyber threats. The research instrument includes four gamified training questions in the first construct and four traditional training questions in the second construct.

Finally, the experience construct, which is directly related to the research hypothesis, consists of 15 statements. These statements are designed to elicit responses measured on a seven-point Likert interval scale (Li et al., 2015). The Likert interval scale is selected for its ability to capture a wide range of experiences in a user-friendly manner. The scale provides seven response options: strongly disagree, disagree, somewhat disagree, neither agree nor disagree, somewhat agree, agree, and strongly agree (Tan, 2006).

By employing these comprehensive measures in questionnaire design and utilising validated scales, the study aims to gather accurate and reliable data to support its research objectives.

3.6 Procedure for data collection

Primary data is gathered using a questionnaire where respondents have an opportunity to participate through a shared link distributed through channels such as instant messaging, social media, and email (Nardi, 2018, p. 13). The procedure begins once this research is approved. The questionnaire has been piloted before roll-out to ensure validity and reliability. The respondents are informed about the purpose of the study, their freedom of choice, and data collection anonymity. In addition, respondents are able to answer the questionnaire on their own time and ask any questions.

Furthermore, respondents are given a deadline for submission, where the responses are collated and compiled, ready to be analysed.

3.7 Data analysis strategies and interpretation

This research utilises descriptive statistics to analyse the data collected from respondents. In addition, descriptive statistics for this research provide valuable insights based on employees' knowledge and experiences on cyber security training engagement (Antonius, 2013). Finally, the descriptive analysis draws outcomes and interpretations of the data collected.

The Statistical Software Package for Social Science (SPSS) tool is utilised to represent the descriptive analysis. SPSS ensures validity for findings and results that can be utilised for future studies and can be amended if required (Antonius, 2013).

3.8 Possible limitations and challenges of the study

Any uncontrollable event or restriction placed on this research is considered a possible limitation (Shipman, 2014). Therefore, a fundamental limitation of this research is the inability to conduct a mixed methods research to obtain valuable insight through interviews and questionnaires for enhancing gamification training to improve training engagement.

Other challenges of the study relate to designing, implementing, and testing a gamified cyber security training programme using a platform to deliver it to respondents. Instead, a questionnaire is used. Time constraints for cross-sectional research contribute to this limitation. However, this limitation also provides an opportunity for future research.

3.9 Quality assurance

3.9.1 *External validity*

This research uses probability sampling to void any bias from the population and ensure compliance with external validity (Andrade, 2018). Furthermore, as part of the

exclusion and inclusion criteria, respondents are requested to confirm if they work in a bank in South Africa before continuing with the questionnaire (Heale & Twycross, 2015). Additionally, a reasonable timeframe is provided for respondents to complete the questionnaire. Contact information is also provided to respondents in case they encounter any technical or non-technical difficulties while completing the questionnaire.

3.9.2 *Internal validity*

This research meets internal validity by ensuring that the relevant literature guides the data collection procedure, avoiding any random selection of respondents (Andrade, 2018). All captured responses have been analysed and contribute to the findings of this research.

3.9.3 *Reliability*

The questionnaire utilised is reliable based on the Qualtrics and SPSS procedure used to collect and analyse the data. The questionnaire has been tested before distribution to maintain validation and quality checks, as well as to test the controls for saving and resuming the questionnaire later (Andrade, 2018). Furthermore, the Qualtrics and SPSS tools are trustworthy, compliant, and align with all ethical principles.

3.10 Ethical considerations

The ethical considerations for this research are highlighted on the introduction page of the questionnaire, ensuring that respondents will not experience any physical harm, discomfort, pain, loss of personal information, and embarrassment as a result of their participation in this research (Zimbardo, 2017).

Moreover, the ethical standards pertaining to the purpose of the research, its benefits, its risks, and consequences are communicated to respondents. Consent is obtained by proceeding with the questionnaire after the introduction, signifying that respondents are participating willingly.

3.11 Schedule and timelines

The activities across the timeline between April 2022 to February 2023 for this research project are mapped in Table 3.

Activity		Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May
1	Proposal development & submission														
2	Panel presentation & outcome (including Ethics Clearance)														
3	Data collection & analysis														
4	Report preparation														
5	Research report first submission														
6	Research report final submission														

Table 3: Proposed research project schedule and timeline

As depicted in Table 4, the summary of the research objectives, hypothesis, data collection, and data analysis is presented in the contingency table. The details for data collection adhere to the standard procedure for the research instrument (questionnaire) to be distributed in order to address the research objectives. The data analysis methods employed include the utilisation of multiple-choice questions and the seven-point Likert scale.

RO #	Research objective (RO)	Hyp #	Hypothesis (Hyp)	Data collection detail	Data analysis method
1	To analyse the cyber threat landscape of the South African banking industry, identifying two major cyber threats	Not applicable (N/A)	N/A	Questionnaire	Multiple choice
2	To design a traditional cyber security training programme for two major South African banking industry cyber threats	N/A	N/A	Questionnaire	Multiple choice
3	To gamify the traditional cyber security training programme for two major South African banking industry cyber threats	N/A	N/A	Questionnaire	Multiple choice
4	To compare employee's experience with the traditional and gamified cyber security training programmes quantitatively	1	Gamification methodologies embedded into cyber security training programmes improve employee engagement	Questionnaire	Seven-point Likert Scale

Table 4: Consistency table showing research objectives, hypothesis, data collection and data analysis

CHAPTER 4. PRESENTATION AND DISCUSSION OF RESULTS

4.1 Introduction

The research results are analysed, presented, and discussed in accordance with the research objectives outlined as part of the study. Data analysis was performed to evaluate the effectiveness of gamified cyber security training in improving employee engagement in the South African banking industry. Data were collected through a research questionnaire completed by 100 (n = 100) employees in the South African banking industry. A total of 142 questionnaire responses were received. However, the target was to collect 100 responses, therefore, based on the data collected, only 100 useable responses met the inclusion criteria for respondents working in the South African banking industry. Hence, the response rate for the study was 100%.

A descriptive statistical analysis was employed to present and discuss the research results. This method involved evaluating percentages and the frequencies across the questionnaire questions. In addition to the inclusion criteria, 100 respondents answered all questions in the questionnaire. The inclusion criteria depended on the initial questions, and the percentages reported in the experience section will reflect the responses of all the respondents who answered those questions.

The questionnaire was structured into three sections, from which the data collection is presented as follows:

- The questionnaire commenced with pre-screening questions, including confirmation of the respondent's employment in a South African bank, their department, and the type of cyber security training they had received.
- Following the pre-screening questions, the gamified and traditional training content questions were presented. If respondents indicated exposure to gamified training in the pre-screening, they would receive the traditional training content, and vice versa for those who selected traditional training. Respondents who indicated no prior cyber security training were required to experience both gamified and traditional training content. If respondents had experienced both

gamified and traditional training, they would proceed to the last section of the questionnaire.

- The third or final section of the questionnaire consisted of training experience questions that all respondents were required to answer before submission.

4.2 Results at a business area level

As part of the pre-screening questions, it is noteworthy that, out of the 100 responses received, the respondents are distributed across various departments/areas in the South African banking industry as follows:

- Audit – 10%
- Fraud – 2%
- Sales – 2%
- Procurement – 3%
- Digital and Technology – 41%
- Finance – 15%
- Human Resources – 7%
- Other (Information Security, Risk, Sustainability, Learning and Development, Operations, Compliance, Vendor Management, Trainees, and Credit) – 20%

Understanding the level of experience and preferences at the departmental level is crucial for determining and delivering cyber security training in a manner that ensures maximum employee engagement. Therefore, Table 5 presents the statistics for the data collected at the departmental/business area level.

Audit (n = 10)	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
1. Gamified training is more effective than traditional training	0%	0%	0%	10%	20%	60%	10%
2. The gamified training is interesting and intriguing	0%	0%	10%	0%	10%	70%	10%
3. Traditional training is interesting and intriguing	0%	20%	30%	0%	30%	20%	0%
4. Gamified training teaches me something new that I will remember for longer	0%	0%	0%	10%	10%	50%	30%
5. Traditional training is more effective	0%	20%	40%	30%	10%	0%	0%
6. The gamified training made me want to complete all my training in that format	0%	10%	0%	10%	20%	50%	10%
7. Any incentive or reward would catch my attention to complete the training	0%	10%	0%	0%	10%	50%	30%
8. Pictures and videos of the cyber threat demonstrations would help me understand the content better	0%	0%	0%	0%	10%	70%	20%
9. I prefer to receive a phishing email as part of a simulation than to read about an example online	0%	10%	10%	0%	10%	50%	20%
10. I prefer story-telling of real-life phishing and malware attacks through a game	0%	0%	0%	0%	20%	60%	20%
11. I prefer 10 minutes on cyber security training compared to 1+ hours of training	0%	0%	0%	0%	0%	60%	40%
12. I prefer having a few hours of someone training me on phishing and malware	50%	20%	20%	0%	10%	0%	0%
13. A leader board or top achievers rank for completing the training would motivate me to complete my cyber security training	10%	20%	0%	30%	10%	30%	0%
14. I regularly read my companies newsletters or cyber security content on the intranet	0%	30%	0%	10%	20%	40%	0%
15. Customised training to my role would be beneficial	0%	10%	0%	0%	20%	60%	10%

Fraud (n = 2)	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
1. Gamified training is more effective than traditional training	0%	0%	0%	100%	0%	0%	0%
2. The gamified training is interesting and intriguing	0%	0%	0%	0%	50%	50%	0%
3. Traditional training is interesting and intriguing	0%	0%	0%	50%	0%	50%	0%
4. Gamified training teaches me something new that I will remember for longer	0%	0%	0%	50%	0%	50%	0%
5. Traditional training is more effective	0%	0%	0%	100%	0%	0%	0%
6. The gamified training made me want to complete all my training in that format	0%	0%	0%	0%	0%	100%	0%
7. Any incentive or reward would catch my attention to complete the training	0%	0%	50%	0%	50%	0%	0%
8. Pictures and videos of the cyber threat demonstrations would help me understand the content better	0%	0%	0%	0%	0%	50%	50%
9. I prefer to receive a phishing email as part of a simulation than to read about an example online	0%	0%	0%	0%	0%	100%	0%
10. I prefer story-telling of real-life phishing and malware attacks through a game	0%	0%	0%	0%	0%	100%	0%
11. I prefer 10 minutes on cyber security training compared to 1+ hours of training	0%	0%	50%	0%	0%	0%	50%
12. I prefer having a few hours of someone training me on phishing and malware	50%	0%	0%	0%	0%	50%	0%
13. A leader board or top achievers rank for completing the training would motivate me to complete my cyber security training	0%	0%	50%	50%	0%	0%	0%
14. I regularly read my companies newsletters or cyber security content on the intranet	0%	0%	0%	0%	50%	0%	50%
15. Customised training to my role would be beneficial	0%	0%	0%	0%	0%	50%	50%

Sales (n = 2)	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
1. Gamified training is more effective than traditional training	50%	0%	0%	0%	0%	0%	50%
2. The gamified training is interesting and intriguing	0%	0%	0%	50%	0%	0%	50%
3. Traditional training is interesting and intriguing	0%	50%	0%	0%	50%	0%	0%
4. Gamified training teaches me something new that I will remember for longer	0%	0%	0%	0%	50%	0%	50%
5. Traditional training is more effective	0%	50%	0%	0%	50%	0%	0%
6. The gamified training made me want to complete all my training in that format	0%	0%	0%	0%	50%	50%	0%
7. Any incentive or reward would catch my attention to complete the training	0%	0%	0%	50%	0%	0%	50%
8. Pictures and videos of the cyber threat demonstrations would help me understand the content better	0%	0%	0%	0%	50%	0%	50%
9. I prefer to receive a phishing email as part of a simulation than to read about an example online	0%	0%	50%	0%	0%	0%	50%
10. I prefer story-telling of real-life phishing and malware attacks through a game	0%	0%	0%	0%	50%	0%	50%
11. I prefer 10 minutes on cyber security training compared to 1+ hours of training	0%	0%	0%	50%	0%	0%	50%
12. I prefer having a few hours of someone training me on phishing and malware	0%	100%	0%	0%	0%	0%	0%
13. A leader board or top achievers rank for completing the training would motivate me to complete my cyber security training	0%	0%	0%	50%	0%	50%	0%
14. I regularly read my companies newsletters or cyber security content on the intranet	0%	0%	50%	50%	0%	0%	0%
15. Customised training to my role would be beneficial	0%	0%	0%	50%	0%	0%	50%

Procurement (n = 3)	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
1. Gamified training is more effective than traditional training	67%	0%	33%	0%	0%	0%	0%
2. The gamified training is interesting and intriguing	67%	0%	33%	0%	0%	0%	0%
3. Traditional training is interesting and intriguing	67%	0%	33%	0%	0%	0%	0%
4. Gamified training teaches me something new that I will remember for longer	67%	0%	33%	0%	0%	0%	0%
5. Traditional training is more effective	67%	0%	33%	0%	0%	0%	0%
6. The gamified training made me want to complete all my training in that format	67%	0%	33%	0%	0%	0%	0%
7. Any incentive or reward would catch my attention to complete the training	67%	0%	33%	0%	0%	0%	0%
8. Pictures and videos of the cyber threat demonstrations would help me understand the content better	67%	0%	33%	0%	0%	0%	0%
9. I prefer to receive a phishing email as part of a simulation than to read about an example online	67%	0%	33%	0%	0%	0%	0%
10. I prefer story-telling of real-life phishing and malware attacks through a game	67%	0%	33%	0%	0%	0%	0%
11. I prefer 10 minutes on cyber security training compared to 1+ hours of training	67%	0%	33%	0%	0%	0%	0%
12. I prefer having a few hours of someone training me on phishing and malware	67%	0%	33%	0%	0%	0%	0%
13. A leader board or top achievers rank for completing the training would motivate me to complete my cyber security training	67%	0%	33%	0%	0%	0%	0%
14. I regularly read my companies newsletters or cyber security content on the intranet	67%	0%	33%	0%	0%	0%	0%
15. Customised training to my role would be beneficial	67%	0%	33%	0%	0%	0%	0%

Digital and Technology (n = 41)	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
1. Gamified training is more effective than traditional training	7%	0%	7%	7%	24%	41%	12%
2. The gamified training is interesting and intriguing	7%	2%	0%	5%	29%	34%	22%
3. Traditional training is interesting and intriguing	17%	12%	27%	15%	20%	5%	5%
4. Gamified training teaches me something new that I will remember for longer	5%	5%	5%	5%	27%	34%	20%
5. Traditional training is more effective	12%	15%	32%	27%	2%	7%	5%
6. The gamified training made me want to complete all my training in that format	5%	5%	5%	17%	24%	29%	15%
7. Any incentive or reward would catch my attention to complete the training	7%	10%	2%	5%	17%	29%	29%
8. Pictures and videos of the cyber threat demonstrations would help me understand the content better	5%	2%	0%	5%	15%	41%	32%
9. I prefer to receive a phishing email as part of a simulation than to read about an example online	12%	7%	2%	15%	10%	32%	22%
10. I prefer story-telling of real-life phishing and malware attacks through a game	5%	2%	5%	7%	20%	37%	24%
11. I prefer 10 minutes on cyber security training compared to 1+ hours of training	5%	0%	0%	10%	12%	22%	51%
12. I prefer having a few hours of someone training me on phishing and malware	32%	24%	15%	5%	10%	12%	2%
13. A leader board or top achievers rank for completing the training would motivate me to complete my cyber security training	10%	15%	5%	17%	20%	20%	15%
14. I regularly read my companies newsletters or cyber security content on the intranet	17%	12%	15%	17%	20%	15%	5%
15. Customised training to my role would be beneficial	5%	2%	2%	12%	15%	27%	37%

Finance (n = 15)	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
1. Gamified training is more effective than traditional training	7%	7%	0%	13%	0%	40%	33%
2. The gamified training is interesting and intriguing	7%	0%	0%	7%	13%	47%	27%
3. Traditional training is interesting and intriguing	7%	20%	13%	27%	7%	27%	0%
4. Gamified training teaches me something new that I will remember for longer	7%	0%	0%	7%	7%	53%	27%
5. Traditional training is more effective	13%	27%	7%	33%	13%	7%	0%
6. The gamified training made me want to complete all my training in that format	7%	7%	0%	20%	20%	27%	20%
7. Any incentive or reward would catch my attention to complete the training	0%	7%	0%	0%	27%	40%	27%
8. Pictures and videos of the cyber threat demonstrations would help me understand the content better	0%	0%	7%	0%	13%	33%	47%
9. I prefer to receive a phishing email as part of a simulation than to read about an example online	0%	20%	0%	0%	7%	33%	40%
10. I prefer story-telling of real-life phishing and malware attacks through a game	0%	7%	0%	7%	7%	40%	40%
11. I prefer 10 minutes on cyber security training compared to 1+ hours of training	0%	0%	0%	0%	0%	40%	60%
12. I prefer having a few hours of someone training me on phishing and malware	27%	33%	13%	0%	7%	7%	13%
13. A leader board or top achievers rank for completing the training would motivate me to complete my cyber security training	7%	27%	13%	0%	7%	20%	27%
14. I regularly read my companies newsletters or cyber security content on the intranet	7%	13%	13%	27%	13%	13%	13%
15. Customised training to my role would be beneficial	0%	7%	0%	0%	13%	53%	27%

Human Resources (n = 7)	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
1. Gamified training is more effective than traditional training	0%	0%	0%	0%	29%	14%	57%
2. The gamified training is interesting and intriguing	0%	0%	0%	0%	14%	29%	57%
3. Traditional training is interesting and intriguing	43%	14%	0%	14%	29%	0%	0%
4. Gamified training teaches me something new that I will remember for longer	0%	0%	14%	14%	0%	14%	57%
5. Traditional training is more effective	43%	14%	14%	29%	0%	0%	0%
6. The gamified training made me want to complete all my training in that format	0%	14%	0%	14%	14%	14%	43%
7. Any incentive or reward would catch my attention to complete the training	0%	14%	0%	29%	14%	0%	43%
8. Pictures and videos of the cyber threat demonstrations would help me understand the content better	0%	0%	0%	0%	29%	14%	57%
9. I prefer to receive a phishing email as part of a simulation than to read about an example online	0%	0%	0%	14%	14%	14%	57%
10. I prefer story-telling of real-life phishing and malware attacks through a game	0%	0%	0%	0%	14%	29%	57%
11. I prefer 10 minutes on cyber security training compared to 1+ hours of training	0%	0%	0%	0%	0%	14%	86%
12. I prefer having a few hours of someone training me on phishing and malware	57%	29%	14%	0%	0%	0%	0%
13. A leader board or top achievers rank for completing the training would motivate me to complete my cyber security training	0%	14%	0%	14%	14%	14%	43%
14. I regularly read my companies newsletters or cyber security content on the intranet	43%	0%	14%	14%	0%	0%	29%
15. Customised training to my role would be beneficial	0%	14%	0%	0%	14%	0%	71%

Table 5: Showing the cyber security training experience statements statistics across different departments/business areas

The results discussion reveals that certain departments within the South African banking industry show a preference for gamified cyber security training based on the highest scores in Table 5. These departments include Audit, Fraud, Sales, Digital and Technology, Finance, and Human Resources. These findings suggest that employees in these areas find gamified training more effective, interesting, and intriguing, and believe that it teaches them something new that they will remember for longer. They also express a desire to complete all their training in a gamified format and show a strong inclination towards incentives or rewards as motivators for completing the training.

On the other hand, the Procurement department indicates a preference for traditional cyber security training. It is important to note that further research should be conducted across a larger population within the Procurement department to validate this finding. The small sample size of respondents from areas other than Digital and Technology also calls for expanding data collection to obtain more accurate insights into the preferences of those areas. This expansion of data collection can be part of a needs analysis aimed at understanding the training maturity levels across each department or business area.

The results suggest the potential for targeted training customisation at both the business level and individual role level to enhance employee engagement. By considering the preferences and needs of different departments, organisations can tailor their training programmes to optimise effectiveness and maximise employee participation. This approach can help create a more engaging and impactful training experience, leading to improved cyber security awareness and practices within the South African banking industry.

4.3 Results pertaining to the hypothesis

The hypothesis for this study is “gamification methodologies embedded into cyber security training programmes improve employee engagement.”

The measurement component to assess respondent’s experiences utilised the seven-point Likert interval scale (Li et al., 2015; Tan , 2006). The Likert interval scale varying from, 1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 = neither agree

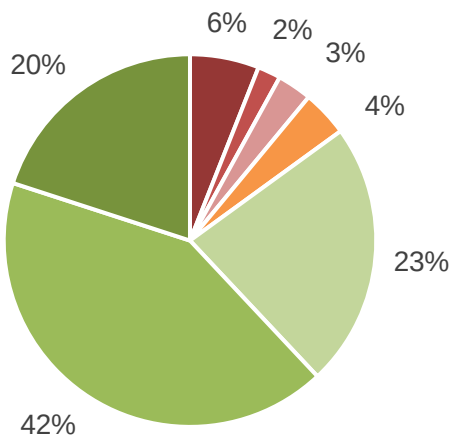
nor disagree, 5 = somewhat agree, 6 = agree, and 7 = strongly agree (Li et al., 2015; Tan, 2006), is employed to evaluate the degree of agreement or disagreement with the statements regarding the training experience. The use of this scale allowed for the capturing of varying levels of agreement or disagreement and enabled a more nuanced analysis of the data. The justification for employing the Likert interval scale in this study stemmed from the positive outcomes of employees' experiences with gamified training, as indicated in the literature (Alcivar & Abad, 2016; Cechella et al., 2021, p. 7; Filsecker & Hickey, 2014; Hamari et al., 2016, p. 171-172; Ibanez et al., 2014; Wu et al., 2021, p. 13). These outcomes encompassed improved learning of cyber security concepts, better retention of knowledge in the long term, and the practical application of knowledge in various cyber security contexts within their job functions. By utilising this scale, the study aimed to explore whether these positive outcomes were reflected in the experiences of employees in the South African banking industry.

Two purposes were served by the questions and statements included in the questionnaire. Firstly, the respondents' level of knowledge and understanding between gamified and traditional training was measured. In this way, a basic understanding of the concepts was ensured to be obtained and served as the basis for further analysis. Secondly, the respondents' experiences with gamified and traditional cyber security training were measured. This was done to determine which training method would be more effective in improving employee engagement within the South African banking industry.

The results obtained from the respondents are represented in Figures 3 and 4, which illustrate the gamified and traditional cyber security training experiences section of the questionnaire. All respondents were given an opportunity to partake in both gamified and traditional training content, depending on their experience, before providing their responses in the training experience section.

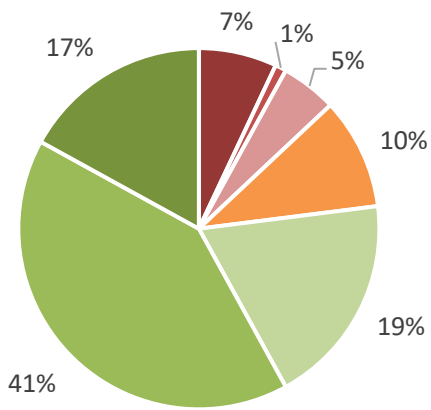
A

The gamified training is interesting and intriguing



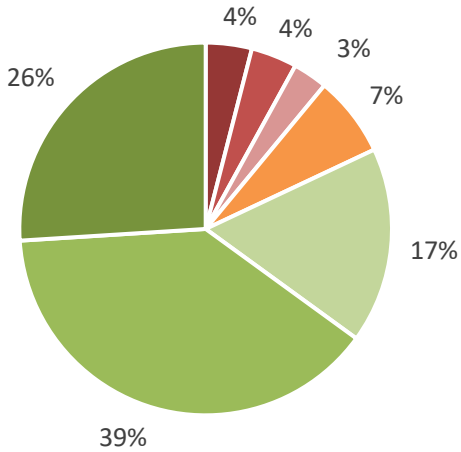
B

Gamified training is more effective than traditional training



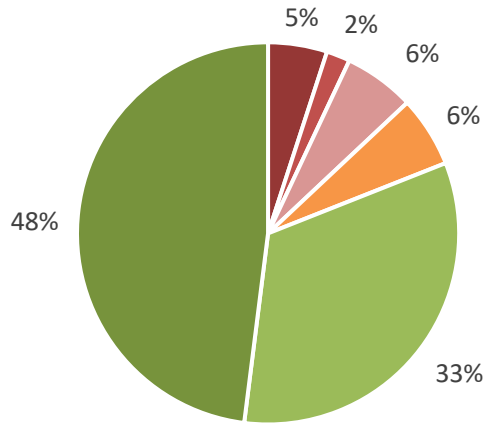
C

I prefer story-telling of real-life phishing and malware attacks through a game



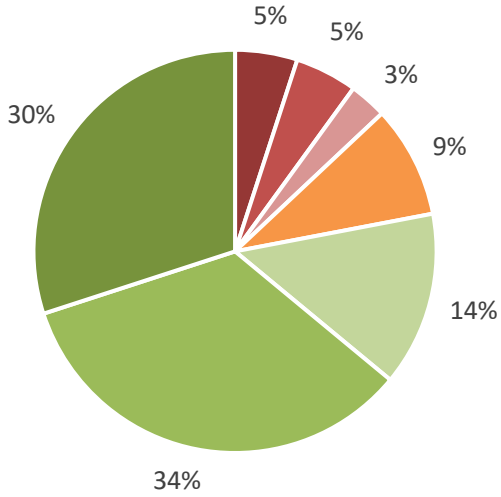
D

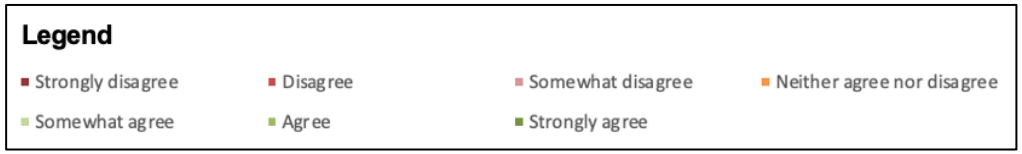
I prefer 10 minutes on cyber security training compared to 1+ hours of training



E

Customised training to my role would be beneficial





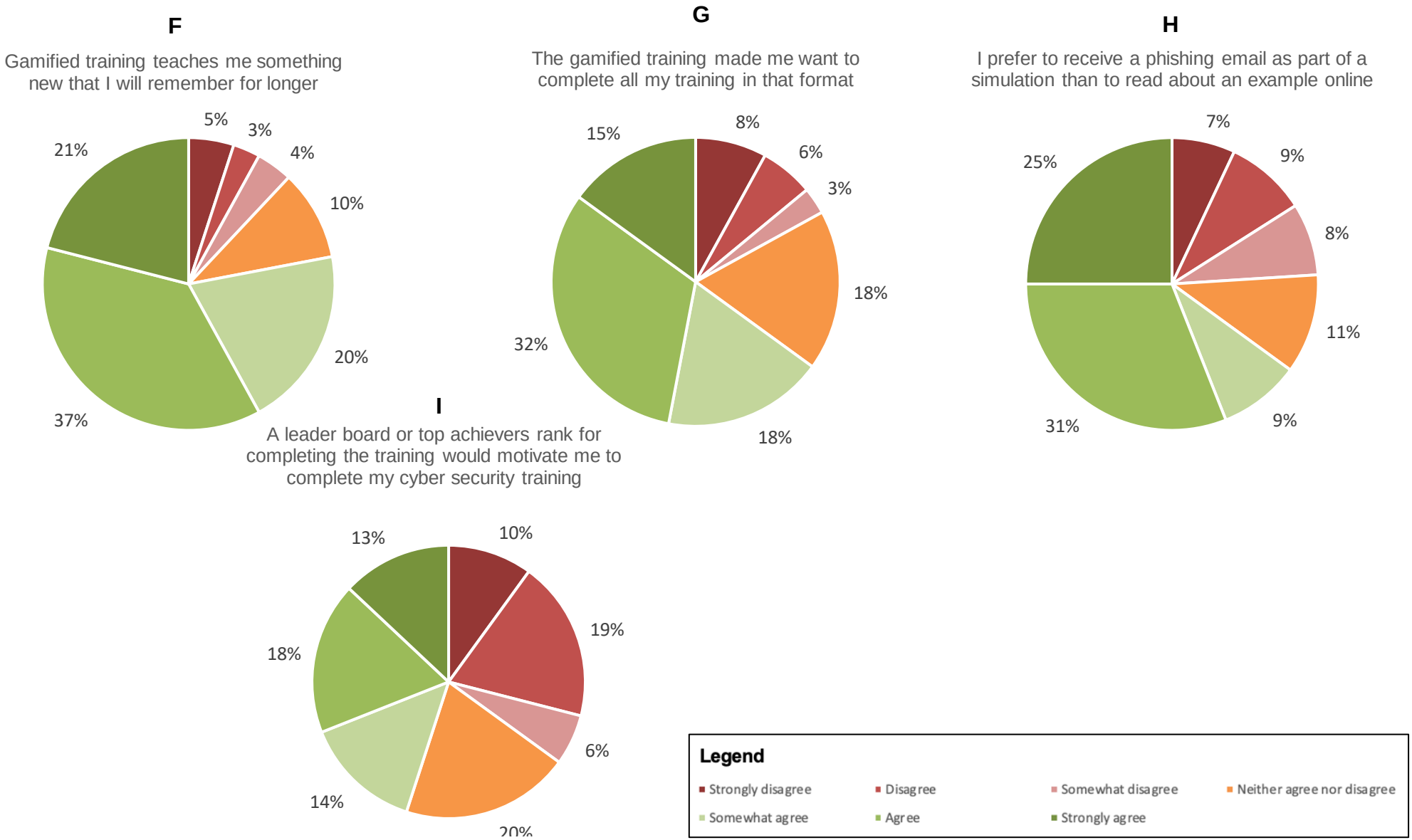


Figure 3: Pie charts depicting gamified cyber security training experience responses

The data presented in Figure 3 offers compelling evidence to support the alternative hypothesis regarding gamified training statements in the context of cyber security. The statistics indicate a clear trend among the respondents, as discussed below.

In Figure 3 (A), it is observed that 85% of the respondents agree that gamified cyber security training is both interesting and intriguing. This suggests that the gamified method successfully captures the attention and curiosity of the trainees.

Figure 3 (B) reveals that 78% of the respondents agree that gamified cyber security training is more effective compared to traditional training methods. This finding implies that the gamified method has a greater impact on learning outcomes and knowledge retention.

The preference for story-telling of real-life phishing and malware attacks through a game is highlighted in Figure 3 (C), with 82% of the respondents expressing their preference for this method. This indicates that incorporating real-life scenarios into the gamified training enhances its appeal and relevance.

Figure 3 (D) demonstrates that 81% of the respondents prefer shorter training sessions. This finding suggests that shorter and more focused training sessions align better with the respondents' preferences and engagement levels.

Furthermore, Figure 3 (E) indicates that 78% of the respondents agree that role-based cyber security training is beneficial. This result suggests that tailoring the training content to specific job roles and responsibilities enhances its perceived value and effectiveness.

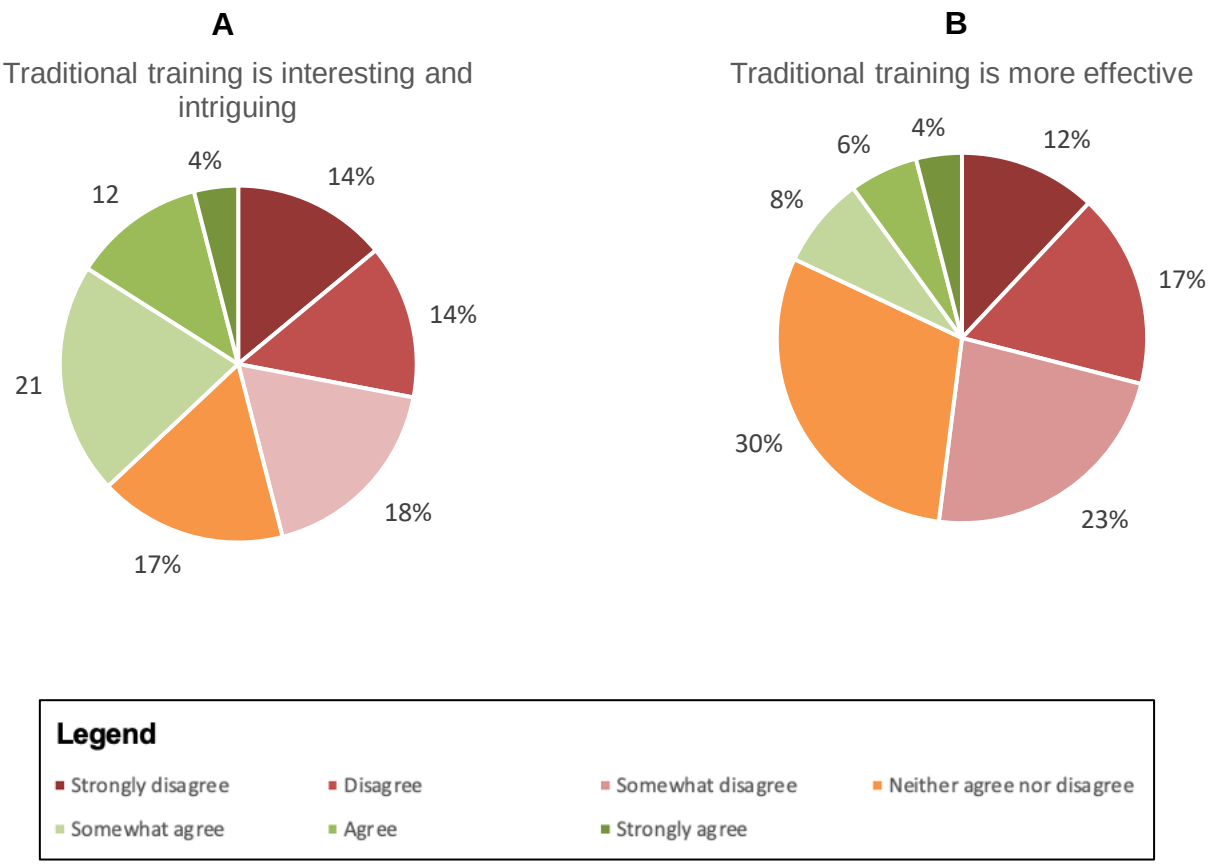
Figure 3 (F) reveals that 78% of the respondents agree that they would remember key messages for a longer period through gamified training. This implies that the gamified method facilitates better retention and recall of important information.

Motivation to complete gamified cyber security training is explored in Figure 3 (G), where 65% of the respondents agree that they are motivated to complete such training. This finding indicates that gamification elements have a positive impact on respondents' motivation levels, driving them to engage with the training content (Wu et al., 2021, p. 13).

In Figure 3 (H), 65% of the respondents express a preference for receiving a phishing email as part of a simulation rather than reading about an example online. This suggests that interactive simulations, even when involving potentially harmful content, are more appealing to respondents than passive learning methods.

Contrarily, the null hypothesis is supported by the data presented in Figure 3 (I), where only 45% of the respondents agree that a leader board or top achievers rank for completing the training would motivate them to complete the cyber security training. This finding indicates that the use of leader boards as a motivational tool may not be as effective as initially hypothesised.

The responses depicted in Figure 3 provide valuable insights into the experiences of gamified cyber security training in the banking industry. Overall, the findings demonstrate positive responses towards gamified training, aligning with the study's hypotheses. Additionally, the theoretical framework for employee cyber security training efficacy supports the notion that gamified training positively influences employee engagement in training activities (Silic & Lowry, 2020, p. 132-139).



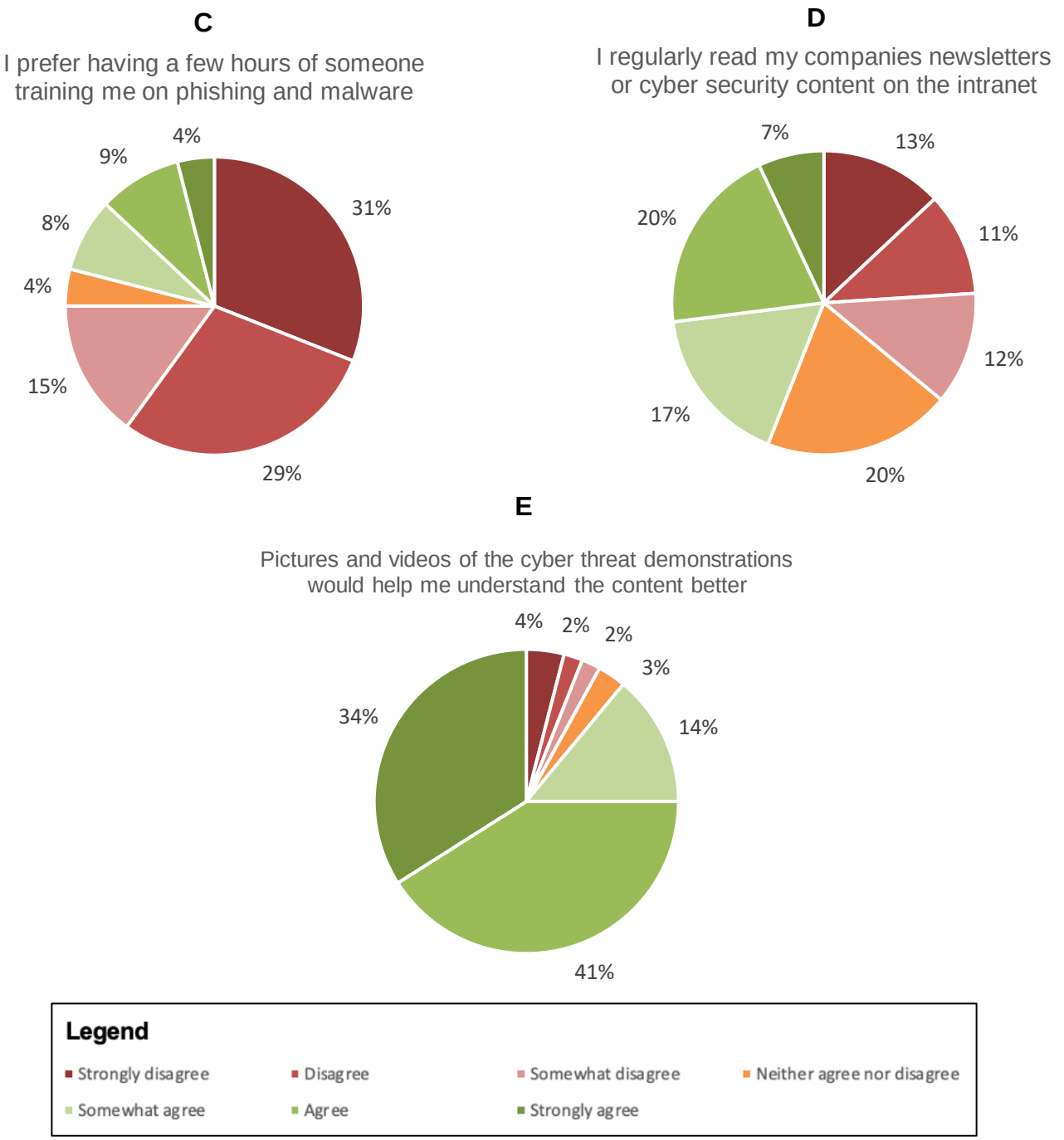


Figure 4: Pie charts depicting traditional cyber security training experience responses

The data presented in Figure 4 provides evidence to support the alternative hypothesis regarding traditional training in the field of cyber security. The statistics presented indicate a notable trend among the respondents, as outlined below.

Figure 4 (A) reveals that only 37% of the respondents agree that traditional cyber security training is interesting and intriguing. This finding suggests that the traditional training method fails to generate a high level of interest or engagement among the respondents.

In Figure 4 (B), it is observed that a mere 18% of the respondents agree that traditional cyber security training is more effective than gamified training. This result indicates that the traditional method is perceived as less impactful in terms of learning outcomes and knowledge retention compared to the gamified training method.

Figure 4 (C) demonstrates that 21% of the respondents prefer longer training sessions on key cyber threats. This finding implies that a subset of the respondents finds value in extended training sessions, suggesting a desire for in-depth knowledge and comprehensive coverage of cyber threats.

The reading habits of the respondents are explored in Figure 4 (D), where 44% of them indicate that they read content on the company's intranet or newsletters. This result suggests that company-provided written materials are utilised by a significant portion of the respondents as a source of information on cyber security.

Furthermore, Figure 4 (E) indicates that a substantial 89% of the respondents believe that picture and video content depicting cyber threat demonstrations improve their understanding. This finding suggests that visual aids, such as pictures and videos, play a crucial role in enhancing the respondents' comprehension of cyber threats.

Overall, the data presented in Figure 4 provides valuable insights into the perceptions and preferences regarding traditional cyber security training. The findings indicate a relatively low level of interest and effectiveness associated with the traditional method. Additionally, the preference for longer training sessions and the value placed on visual content for improved understanding highlight important considerations for designing and delivering effective training programmes.

It is worth noting that the statistical evidence supports the alternative hypothesis, and suggests that traditional cyber security training may be less engaging and effective compared to alternative methodologies. These findings have implications for the development and implementation of training strategies in the field of cyber security,

emphasising the importance of incorporating interactive and visually appealing elements to enhance engagement and knowledge acquisition among trainees.

The results pertaining to the hypothesis indicate that traditional cyber security training methods often suffer from several concerns, leading to a low attention span among employees during training (Abawajy, 2014, p. 242). These concerns align with the negative responses received regarding traditional training experiences in the study.

As shown in Figure 4, the majority of respondents did not find traditional training to be interesting, intriguing, or effective. Additionally, most respondents expressed a preference for shorter training sessions, indicating a potential issue with the duration of traditional training methods. Moreover, a significant number of respondents claimed uncertainty about reading cyber security content in newsletters and on the intranet, suggesting a lack of engagement with the provided materials.

To address these concerns, the research aims to test the null hypothesis that traditional cyber security training enhances knowledge, awareness, and engagement for employees in the banking industry. In contrast, the alternative hypothesis suggests that gamification methodologies embedded into training programmes improve employee engagement.

The following table presents the one-sample test and statistics for the questions related to the gamified training experience, which will be used to evaluate the null hypothesis against the alternative hypothesis. This analysis will provide insights into the effectiveness of gamification in improving employee engagement during cyber security training.

Gamified training experience statements	N (df = 99)	Mean	Std. Deviation	Std. Error Mean	t	Significance		Mean Difference	95% Confidence Interval of the Difference	
						One-Sided p	Two-Sided p		Lower	Upper
1. Gamified training is more effective than traditional training	100	5.24	1.603	.160	-4.743	<.001	<.001	-.760	-1.08	-.44
2. The gamified training is interesting and intriguing	100	5.42	1.539	.154	-3.770	<.001	<.001	-.580	-.89	-.27
3. Gamified training teaches me something new that I will remember for longer	100	5.32	1.569	.157	-4.334	<.001	<.001	-.680	-.99	-.37
4. The gamified training made me want to complete all my training in that format	100	4.88	1.748	.175	-6.407	<.001	<.001	-1.120	-1.47	-.77
5. Any incentive or reward would catch my attention to complete the training	100	5.07	1.844	.184	-5.044	<.001	<.001	-.930	-1.30	-.56
6. I prefer to receive a phishing email as part of a simulation than to read about an example online	100	4.99	1.925	.193	-5.246	<.001	<.001	-1.010	-1.39	-.63
7. I prefer story-telling of real-life phishing and malware attacks through a game	100	5.50	1.547	.155	-3.232	<.001	.002	-.500	-.81	-.19
8. A leader board or top achievers rank for completing the training would motivate me to complete my cyber security training	100	4.15	1.940	.194	-9.534	<.001	<.001	-1.850	-2.24	-1.46
9. Customised training to my role would be beneficial	100	5.44	1.684	.168	-3.326	<.001	.001	-.560	-.89	-.23
10. I prefer 10 minutes on cyber security training compared to 1+ hours of training	100	5.99	1.494	.149	-6.760	<.001	<.001	-1.010	-1.31	-.71
11. Pictures and videos of the cyber threat demonstrations would help me understand the content better	100	5.80	1.443	.144	5.546	<.001	<.001	.800	.51	1.09

Table 6: One-sample test for the gamified training experience statements

Traditional training experience statements	N (df = 99)	Mean	Std. Deviation	Std. Error Mean	t	Significance		Mean Difference	95% Confidence Interval of the Difference	
						One-Sided p	Two-Sided p		Lower	Upper
1. Traditional training is interesting and intriguing	100	3.69	1.727	.173	9.784	<.001	<.001	1.690	1.35	2.03
2. Traditional training is more effective	100	3.39	1.524	.152	9.124	<.001	<.001	1.390	1.09	1.69
3. I prefer having a few hours of someone training me on phishing and malware	100	2.72	1.815	.182	3.967	<.001	<.001	.720	.36	1.08
4. I regularly read my companies newsletters or cyber security content on the intranet	100	4.05	1.833	.183	11.182	<.001	<.001	2.050	1.69	2.41

Table 7: One-sample test for the traditional training experience statements

Table 6 and 7 present the mean, standard deviation, standard error mean, t values, the significance levels, the mean difference, and the confidence levels.

In Table 6, the gamified training experience statements received responses indicating higher engagement among employees. The eleven gamified training experience statements yielded a total mean of 5.25, a standard deviation of 1.66, and a standard error mean of 0.16.

In Table 7, traditional training experience statements received responses indicating lower engagement among employees. The four traditional training experience statements yielded an average mean of 3.46, an average standard deviation of 1.72, and an average standard error mean of 0.17.

The higher mean for the gamified training experience statements suggests that majority of respondents agree that gamified cyber security training improves their engagement. The lower standard deviation for gamified cyber security training statements indicates greater agreement and stability in perceptions regarding gamifying training. The standard error mean values across Table 6 and 7, being closer to zero, suggest a more accurate representation of the true mean value of the population.

As observed in Table 6 and 7, the significance (alpha) is divided into one-sided and two-sided p-values. The p-values for the 95% confidence interval of the difference in gamified cyber security training are lower than the alpha, indicating higher significance. Conversely, the p-values for the 95% confidence interval of the difference for traditional cyber security training are higher than the alpha, indicating that there is lower significance. Based on these finding, if all p-values for the 95% confidence interval in the tables are less than 0.05 ($p \leq 0.05$), it can be concluded that the results are statistically significant. These results support the use of gamification methodologies in the design and implementation of cyber security training programmes, particularly in the South African banking industry. Thus, according to the statistics, the alternative hypothesis is accepted.

4.4 Summary

The pie charts and table presented in this chapter demonstrate a statistically significant improvement in employee training engagement through the use of gamified training content. A preference for gamified training was expressed by the majority of respondents, who found it more interesting, intriguing, engaging, and effective in retaining knowledge in the long term compared to traditional training. It was also revealed that most respondents preferred shorter training sessions, indicating the effectiveness of gamification elements such as phishing simulations, visual demonstrations, leader boards, and storytelling in enhancing training engagement.

Furthermore, a majority of respondents indicated that tailored cyber training aligned with their specific roles in the business would be more beneficial than a generic "one-size-fits-all" approach. This finding reinforces the importance of tailored training experiences in improving employee engagement.

These findings hold significant implications for the South African banking industry, suggesting that the incorporation of gamified training methods can lead to enhanced employee engagement in cyber security training. By utilising gamification techniques and customising training content to align with employee roles, organisations can improve the effectiveness and efficiency of their training programmes.

It is important to note that this study focuses on a specific population within the South African banking industry. Future research should aim to replicate these findings in a larger and more diverse sample to ensure generalisability. Additionally, qualitative research methods such as interviews or focus groups, as demonstrated in Francia et al. (2014), could provide further insights into the specific aspects of gamified training that contribute to its effectiveness in engaging employees.

Based on the observed positive relationship between gamified cyber security training experience and traditional methods, it can be concluded that gamified training has a significant positive impact on improving employee training engagement. All gamified cyber security training experience questions yielded lower p-values, indicating a strong statistical significance. Therefore, the alternative hypothesis, suggesting a positive relationship between gamified training and employee engagement, is accepted.

CHAPTER 5. CONCLUSIONS & RECOMMENDATIONS

5.1 Introduction

A summary of the study's recommendations will be provided in this chapter, aligning with the research findings and results that were analysed in the previous chapter. Each research objective has been addressed through hypothesis testing and a synopsis of the literature. The results of the study will be reviewed in the conclusion, highlighting areas for further research that have been identified.

5.2 Conclusions regarding the cyber threat landscape of the South African banking industry, identifying two major cyber threats

The understanding of current cyber security threats and trends, which can be utilised to improve employee training engagement, has been assisted by this research objective, as it is fundamental to the study (Wilding, 2016). Risk assessments and the development of mitigation actions by organisations can be guided by this understanding, enabling them to remain proactive and vigilant.

The conclusions drawn in this study are based on the current South African cyber threats within the cyber threat landscape. Phishing and malware were selected as they represent different attack delivery methods (Pieterse, 2021). Additionally, these two cyber threats were chosen to validate employees' experience from a training content perspective.

The research findings confirm that respondents' preference for the training method enhances training engagement, thereby positively influencing the assimilation of information and the improvement of their cyber knowledge. It can be highlighted that, an average of 85% of respondents believe gamified cyber security training is interesting and intriguing, indicating the empowering nature of the gamification methodology in terms of knowledge and experience.

5.3 Conclusions regarding the design of a traditional cyber security training programme for two major South African banking industry cyber threats

The impact on employee training engagement is influenced by the cyber security training methodologies implemented by organisations. In this study, two key methodologies were explored: gamified cyber security training methodology and traditional cyber security training methodology. In the context of the South African banking industry, a traditional cyber security training programme focusing on phishing and malware training content was implemented as part of the research instrument.

In accordance with the literature by Abawajy (2014), the traditional questions in the research instrument were formulated to encompass generic cyber security best practices, without targeting specific employee groups within the organisation. It was found that an average of 18% of respondents perceive traditional training as effective.

The concerns raised by Abawajy (2014, p. 240) regarding the mundane nature of traditional training content due to employees' low attention span during the training were confirmed by the research findings presented in chapter 4.

Additionally, this study did not previously mention that traditional newsletter delivery can be partially effective. Approximately 44% of respondents reported reading newsletters, which presents an opportunity to enhance content delivery through digital newsletters using modern approaches such as podcasts, short leadership-focused messages, and other forms of positive reinforcement messaging to improve engagement (Koehler et al., 2021).

5.4 Conclusions regarding gamifying a traditional cyber security training programme for two major South African banking industry cyber threats

It has been indicated by the study that gamified cyber security training is capable of enhancing the attention and engagement of employees in comparison to the traditional cyber security training programme (Holdsworth & Apeh, 2017, p. 113). The results

presented in chapter 4, provide evidence that majority of respondents preferred engaging with gamified training techniques based on their experiences.

The importance of cyber security training for the banking employees is emphasised (Holdsworth & Apeh, 2017, p. 113), highlighting the crucial role that gamification plays in attracting employees to participate in cyber security training. Abawajy, (2014, p. 242) referred to a game-based training course aimed at educating employees on identifying phishing emails, which was implemented as part of the research instrument.

Furthermore, streamlining the gamification process within a single platform is a complex task that should be addressed (Sharif & Ameen, 2020, p. 154). For instance, according to Miranda (2018, p. 7), phishing simulations can effectively prepare employees in an organisation to recognise potential external cyber threats. The research findings indicate that an average of 56% of respondents believe that phishing simulations would be effective in identifying what constitutes a phishing email.

The research results also suggest that modernising traditional training methods may still be effective, especially considering the virtual fatigue experienced after the Covid-19 pandemic (Wicks, 2021). Therefore, there are various opportunities to incorporate into the design of the traditional cyber security training programme for addressing phishing and malware threats.

5.5 Conclusions regarding the comparison of employees' experience with the traditional and gamified cyber security training programmes quantitatively

An important aspect of the study, as well as the testing of the hypothesis, involves comparing training methodologies and their associated experiences. Therefore, the results of employees' experiences with cyber security training are crucial as they impact the level of engagement with the cyber security content.

As stated by He and Zhang (2019, p. 255), traditional cyber security training that inundates employees with a large amount of content leads to "security fatigue". Based on the responses, the majority of respondents preferred the gamified methodology, which promotes engagement and helps alleviate security fatigue. Additionally, as part

of the research instrument, gamified phishing and malware training were provided to employees to mitigate security fatigue.

5.6 Recommendations

During the Covid-19 pandemic, the South African banking industry encountered various challenges, leading to an increase in opportunities for cybercriminals to exploit humans. To mitigate these risks, the implementation of a robust cyber security training programme can help minimise the potential damage caused by cyber threats.

Based on the industry benchmarks, discoveries, and analysis of the research results, this study will contribute to the following recommendations. The key stakeholders identified in this context are the organisations operating within the banking industry.

5.6.1 *Organisations in the South African banking industry*

Recommendation 1: Continuous analysis and monitoring of the threat landscape

The continuous evolution of cyber security defence mechanisms is usually accompanied by the advancement of cyber threats and cyber-attacks, which stay ahead of the game (Carter, 2017). Strategies should be developed by organisations in the South African banking industry to effectively analyse the threat landscape and improve the content of cyber security training. The level of knowledge demonstrated by the respondents in the study on two major cyber threats, phishing and malware, within the current threat landscape was variable. Hence, training can be improved by analysing employee attitudes or the way training content is consumed.

Furthermore, the assessment of the threat landscape can be utilised to enhance security tools and measures, enabling organisations to identify new cyber threats more effectively. Evaluating employee security behaviour across each identified cyber threat within the threat landscape is crucial. For instance, simulations for smishing, phishing, and social engineering can be implemented.

As mentioned earlier, identifying new cyber threats is a key competent when curating training content. However, continuous monitoring is equally significant. Monitoring the

threat landscape and incorporating threat intelligence into a cyber security training programme will enhance the security posture of the organisation.

To stay ahead of the game, organisations in the banking industry need to determine and develop new approaches for building cyber security training (Carter, 2017). This involves integrating security defence mechanisms with human defence, considering that humans are often perceived as the weakest security link within an organisation. Developing a cyber security-savvy culture will support a broader ecosystem (Carter, 2017). As long as organisations in the banking industry exist, cybercriminals will continue to launch attacks. Therefore, it is important for security defence mechanisms to integrate with human security training to mitigate security risks (Carter, 2017).

Recommendation 2: Establish and implement a gamified cyber security training programme for internal and external audiences

In recent years, gamified training has been steadily emerging within organisations (Katsantonis et al., 2017). Various methodologies and literature on cyber security training have been explored in this paper.

Organisations in the South African banking industry should consider implementing gamification methodologies and techniques in their cyber security training programmes. Gamified training programmes motivate and promote positive employee training engagement, which reduces security errors and enhances the organisation's security posture. These positive effects enhance employee knowledge and potentially facilitate behavioural change analysis (Sharif & Ameen, 2020, p. 154). According to Schieltz et al. (2017), gamified reinforcement techniques such as rewards or leader boards encourage positive employee behaviour.

Additionally, gamified cyber security training overcomes the limitations of traditional learning approaches by providing an enhanced learner experience (Nguyen & Pham, 2020). Real-life scenarios are easier to understand, creating a visually simulated environment that facilitates maximum knowledge absorption (Nguyen & Pham, 2020). As mentioned, employees would be enthusiastic about learning, bridging the gap between learning and practical application (Nguyen & Pham, 2020).

A comprehensive cyber security training programme should be developed for employees and external audiences, including clients, to cover all aspects of cyber security. This will enable an immediate response to any volume of cyber-attacks across all environments (Modina, 2015).

There are numerous cyber security training models that can be adapted to focus on gamification and drive effective and efficient learning (Birajdar & Nisha, 2022). Organisations should consider defining a customised cyber security training framework based on the business culture (Birajdar & Nisha, 2022). Integrating this framework into other learning functions within the organisation can provide additional value (Birajdar & Nisha, 2022).

Recommendation 3: Source a security behavioural and human risk intelligence tool for data analytics

Sourcing security behavioural tools is not an easy acquisition, and the budget and time spent on research are crucial. All requirements should be scoped by organisations in the banking industry once a mature level of cyber security training has been achieved in the environment. For example, once a foundation has been built on a customised cyber security training programme, instead of adopting a tick-box exercise or one-size fits all approach (Angafor, Yevseyeva, & He, 2020, p. 2).

The requirements should be mapped back to the objectives and frameworks that have been embedded. Subsequently, all security tools should be mapped to gain an understanding of data flow analysis, security behaviour, and employee risk levels. By focusing on human risk intelligence and training employees based on their behaviour, it becomes easier to determine individual cyber security scores. Ultimately, improved employee training engagement will enhance the security culture within the organisation. This will enable organisations to easily adapt and counter new cyber threats entering the cyber threat landscape.

Recommendation 4: Obtain continuous feedback from employees based on their training experience

To stay ahead of cybercriminals and continuously monitor the cyber threat landscape, organisations in the banking industry need to consider feedback from employees

regarding their training. Just as security tools and integrations are crucial for organisations, the training content should be maintained and kept up to date with the ever-changing cyber threat landscape. Additionally, it is important to ensure that employees are engaged with the training content.

The effectiveness of cyber security training relies on the training experience of employees. Therefore, obtaining feedback allows an organisation to adapt and adopt new methods of delivery for their employees. Moreover, creating a positive cyber security culture, where employees are curious and eager to learn more, rather than disengaged, is essential.

Feedback can be obtained through various channels, such as questionnaires after a training session, at events, online polls, word of mouth, or other alternative modes. The method of obtaining feedback largely depends on the organisation's environment and may vary from one organisation to another. Another way to gather feedback is by embedding the feedback questions into the gamified experience. For example, gamifying the feedback questionnaire and ensuring its inclusion in a training course.

5.7 Conclusion and suggestions for further research

The engagement of South African bank employees on critical cyber threats across both traditional and modern methods of cyber security training programmes was examined in this study. Furthermore, modern cyber security training tools and techniques to empower employees, with a focus on gamification, were investigated. The effectiveness of training engagement was tested based on the adopted training methodology. Hence, the research objectives were addressed, and efficient recommendations based on literature and research discoveries are provided to stakeholders.

Change management, psychological, and behavioural analytic models that improve employee training should be assessed in future research (Alshaikh, Naseer, Ahmad, & Maynard, 2019). For example, cyber security training could be delivered at a risk level by individually profiling each employee's risk profile. Risk groups or levels can be classified to limit the number of groups to a manageable level.

Expanding the scope to include employees in the banking industry globally may yield valuable insights into improving training engagement, particularly from countries with well-established cyber security training programmes.

Furthermore, future research should utilise the insights gained from this study to gamify a cyber security training course and analyse behavioural changes in employee training engagement. This would establish a strong foundation for organisations to incorporate gamification methodologies into their cyber security training programmes.

Investigating the effects of age classification on responses to gamification is an intriguing area for future research, as it can provide insights into preferences and effectiveness of gamified experiences across different age groups. Understanding how age influences employees' responses to gamification can help design engaging and effective experiences tailored to specific age groups.

The cognitive and developmental factors associated with different age groups could have been considered in this study (Thomas, Baral, & Crocco, 2022). For instance, younger employees may exhibit higher levels of cognitive flexibility and be more receptive to novel game mechanics, while older adults may prefer familiar and intuitive designs. Examining how different age groups perceive and interact with various game elements, such as badges, leader boards, rewards, or progress tracking, can provide valuable insights for designing age-appropriate gamified interventions.

Furthermore, studying the impact of age on motivation and engagement in gamified experiences is essential. Different age groups may have distinct intrinsic and extrinsic motivations that influence their preference for gamification. For example, younger employees might be more motivated by competition and social interaction, while older adults may prioritise personal growth and enjoyment. Examining how age influences the perceived enjoyment, motivation, and sustained engagement in gamified activities can help tailor gamification strategies to effectively engage different age groups.

The influence of age-related factors, such as digital literacy and technological proficiency, on the preference for gamification is another aspect to explore. Older adults may have varying levels of experience and comfort with technology, which can impact their acceptance and adoption of gamified systems. Investigating how age-related factors intersect with preferences for gamification can guide the development

of user-friendly and inclusive gamified designs that cater to the needs and abilities of different age groups.

Lastly, considering the potential implications of gamification for different age groups is crucial. Gamified interventions aimed at promoting healthy behaviours or learning outcomes may have varying effectiveness and acceptability across different age groups. Assessing the impact of gamification on behavioural change, skill acquisition, or knowledge retention among different age groups can provide insights into the appropriateness and effectiveness of gamified methodologies for specific age ranges.

For this research, a minor critique is that it would have been beneficial to distribute the questionnaire to a specific organisation in the South African banking industry. This would have allowed for the separation of the population, ensuring a similar number of responses across selected (or high-risk) departments or business areas. This approach would have addressed the controversy surrounding the current data collected, which primarily consisted of employees based in the digital and technology business area. Furthermore, it would have provided the opportunity to identify specific gaps and make recommendations for cyber security training within these groups, offering high value to organisations in the banking industry.

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour and Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Alcivar, I., & Abad, A.G. (2016). Design and evaluation of a gamified system for ERP training. *Computers in Human Behavior*, *58*, 109–118. https://doi.org/10.1016/j.chb.2015.12.018

Al-Daeef, M.M., Basir, N., & Saudi, M.M. (2017). *Security Awareness Training: A Review* (Vol. 1).

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3), 73.

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). Information, 11(2), 121.

Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S.B. (2019). Toward sustainable behaviour change: an approach for cyber security education training and awareness.

Andrade, C. (2018). Internal, external, and ecological validity in research design, conduct, and evaluation. *Indian Journal of Psychological Medicine*, *40*(5), 498–499. https://doi.org/10.4103/IJPSYM.IJPSYM_334_18

Angafor, G.N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. Security and privacy, 3(6), e126.

Antonius, R. (2013). *Interpreting Quantitative Data with IBM SPSS Statistics*. Sage. https://books.google.co.za/books?hl=en&lr=&id=EM9saeSNjLQC&oi=fnd&pg=PP2&dq=Interpreting+Quantitative+Data+with+IBM+SPSS+Statistics&ots=DqiKV4OKyV&sig=ZXVIjJIDUNvqCo60sOnRvBaUUoU&redir_esc=y#v=onepage&q=Interpreting%20Quantitative%20Data%20with%20IBM%20SPSS%20Statistics&f=false

Babate, A., Musa, M., Kida, A., & Saidu, M. (2015). State of cyber security: emerging threats landscape. International Journal of Advanced Research in Computer Science & Technology, 3(1), 113-119.

Bada, M., Sasse, A.M., & Nurse, J.R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.

Banfield, J., & Wilkerson, B. (2014). Increasing student intrinsic motivation and self-efficacy through gamification pedagogy. Contemporary Issues in Education Research (CIER), 7(4), 291-298.

Baral, G., & Arachchilage, N.A.G. (2019). Building confidence not to be phished through a gamified approach: conceptualising user's self-efficacy in phishing threat avoidance behaviour. In 2019 cybersecurity and cyberforensics conference (CCC) (pp. 102-110). IEEE.

Birajdar, A., & Nisha, T.N. (2022). APPEARS Framework for evaluating Gamified Cyber Security Awareness Training. In 2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS) (pp. 1-8). IEEE.

Buckley, P., & Doyle, E. (2017). Individualising gamification: An investigation of the impact of learning styles and personality traits on the efficacy of gamification using a prediction market. *Computers and Education*, *106*, 43–55. https://doi.org/10.1016/j.compedu.2016.11.009

Carter, W. (2017). Forces shaping the cyber threat landscape for financial institutions.

Carlin, D., Burgess, J., O'Kane, P., & Sezer, S. (2019). You could be mine (d): the rise of cryptojacking. IEEE Security & Privacy, 18(2), 16-22.

Cechella, F., Abbad, G., & Wagner, R. (2021). Leveraging learning with gamification: An experimental case study with bank managers. *Computers in Human Behavior Reports*, *3*. https://doi.org/10.1016/j.chbr.2020.100044

De-Marcos, L., Garcia-Lopez, E., & Garcia-Cabot, A. (2016). On the effectiveness of game-like and social approaches in learning: Comparing educational gaming, gamification &

social networking. *Computers and Education*, *95*, 99–113. https://doi.org/10.1016/j.compedu.2015.12.008

ENISA. (2022). *Threat Landscape*. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

Filsecker, M., & Hickey, D.T. (2014). A multilevel analysis of the effects of external rewards on elementary students' motivation, engagement and learning in an educational game. *Computers and Education*, *75*, 136–148. https://doi.org/10.1016/j.compedu.2014.02.008

Francia III, G., Thornton, D., Trifas, M., & Bowden, T. (2014). Gamification of information security awareness training. In Emerging trends in ICT security (pp. 85-97). Morgan Kaufmann.

Hamari, J., Shernoff, D.J., Rowe, E., Coller, B., Asbell-Clarke, J., & Edwards, T. (2016). Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. *Computers in Human Behavior*, *54*, 170–179. https://doi.org/10.1016/j.chb.2015.07.045

Haney, J., & Lutters, W. (2020). Security awareness training for the workforce: moving beyond "check-the-box" compliance. Computer, 53(10).

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528

Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. In *Evidence-Based Nursing* (Vol. 18, Issue 3, pp. 66–67). BMJ Publishing Group. https://doi.org/10.1136/eb-2015-102129

Holdsworth, J., & Apeh, E. (2017). An effective immersive cyber security awareness learning platform for businesses in the hospitality sector. *Proceedings – 2017 IEEE 25th International Requirements Engineering Conference Workshops, REW 2017*, 111–117. https://doi.org/10.1109/REW.2017.47

Hu, S., Hsu, C., & Zhou, Z. (2021). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2021.1913671

Iacono, S., Vallarino, M., & Vercelli, G. (2020). Gamification in corporate training to enhance engagement: An approach. International Journal of Emerging Technologies in Learning (iJET), 15(17), 69-84.

Ibanez, M.B., Di-Serio, A., & Delgado-Kloos, C. (2014). Gamification for engaging computer science students in learning activities: A case study. *IEEE Transactions on Learning Technologies*, *7*(3), 291–301. https://doi.org/10.1109/TLT.2014.2329293

Jain, A.K., Gupta, B.B., Kaur, K., Bhutani, P., Alhalabi, W., & Almomani, A. (2022). A content and URL analysis-based efficient approach to detect smishing SMS in intelligent systems. International Journal of Intelligent Systems, 37(12), 11117-11141.

Kaspersky. (2022a). *Phishing Scams & Attacks – How to Protect Yourself*. https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips

Kaspersky. (2022b). *Top Ten Cybersecurity Trends*. https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends

Kaspersky. (2022c). *What is Crypto jacking & How does it work?* https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking

Kaspersky. (2022d). *What is the threat landscape? | Kaspersky IT Encyclopedia*. https://encyclopedia.kaspersky.com/glossary/threat-landscape/

Katsantonis, M.N., Fouliras, P., & Mavridis, I. (2017). Conceptualization of game based approaches for learning and training on cyber security. In *Proceedings of the 21st Pan-Hellenic conference on informatics* (pp. 1-2).

Koehler, D., Serth, S., & Meinel, C. (2021). Consuming Security: Evaluating Podcasts to Promote Online Learning Integrated with Everyday Life. In 2021 World Engineering Education Forum/Global Engineering Deans Council (WEEF/GEDC) (pp. 476-481). IEEE.

Kyriazos, T.A., & Stalikas, A. (2018). Applied Psychometrics: The Steps of Scale Development and Standardization Process. *Psychology*, *09*(11), 2531–2560. https://doi.org/10.4236/psych.2018.911145

Li, T., Vedula, S.S., Hadar, N., Parkin, C., Lau, J., & Dickersin, K. (2015). Innovations in Data Collection, Management, and Archiving for Systematic Reviews. *Https://Doi.Org/10.7326/M14-1603*, *162*(4), 287–294. https://doi.org/10.7326/M14-1603

Mai, P.T., & Tick, A. (2021). Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in hungary and Vietnam. *Acta Polytechnica Hungarica*, *18*(8), 67–89. https://doi.org/10.12700/APH.18.8.2021.8.4

Mcanyana, W., Brindley, C., & Seedat, Y. (2020). *Insight into the cyberthreat landscape in South Africa*.

Miranda, M.J.A. (2018). Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach. In *International Management Review* (Vol. 14, Issue 2). https://help.salesforce.com/articleView?id=admin_loginrestrict.htm&type=5,

Modina, M. (2015). Internal Rating Systems: A Critical Vision. In Credit Rating and Bank-Firm Relationships (pp. 48-70). Palgrave Macmillan, London.

Nardi, P.M. (2018). Doing survey research: A guide to quantitative methods. Routledge.

Nguyen, T.A. & Pham, H. (2020). A Design Theory-Based Gamification Approach for Information Security Training. RIVF International Conference on Computing and Communication Technologies (RIVF), pp. 1-4, doi:10.1109/RIVF48685.2020.9140730.

Nicewander, W.A. (2017). Conditional reliability coefficients for test scores. *Psychological Methods*, *23*(2), 351. https://doi.org/10.1037/MET0000132

NIST. (2022). *Cyber Threat – Glossary | CSRC*. https://csrc.nist.gov/glossary/term/cyber_threat

Orwoll, B., Diane, S., Henry, D., Tsang, L., Chu, K., Meer, C., Hartman, K., & Roy-Burman, A. (2018). Gamification and microlearning for engagement with quality improvement

(GAMEQI): A bundled digital intervention for the prevention of central line–associated bloodstream infection. American Journal of Medical Quality, 33(1), 21-29.

Petrenko, S. (2019). Cyber resilience. In *Cyber Resilience*. River Publishers. https://doi.org/10.1177/0266382116650299

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. The African Journal of Information and Communication, 28, 1-21.

Qusa, H., & Tarazi, J. (2021). Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, 677–682. https://doi.org/10.1109/CCWC51732.2021.9375847

Rahman, M. L., Timko, D., Wali, H., & Neupane, A. (2023). Users Really Do Respond To Smishing. In Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy (pp. 49-60).

Rieff, I. (2018). *Systematically Applying Gamification to Cyber Security Awareness Trainings A framework and case study approach*.

Robson, K., Plangger, K., Kietzmann, J.H., McCarthy, I., & Pitt, L. (2015). Is it all a game? Understanding the principles of gamification. *Business Horizons*, *58*(4), 411–420. https://doi.org/10.1016/j.bushor.2015.03.006

Safonov, K.v., Zolotarev, V.v., & Derben, A.M. (2020). Analysis and forecasting strategies of attacks on game resources for distributed cybersecurity training games. *IOP Conference Series: Materials Science and Engineering*, *822*(1). https://doi.org/10.1088/1757-899X/822/1/012027

Sammons, J., & Cross, M. (2017). *The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy*. Elsevier. https://books.google.co.za/books?hl=en&lr=&id=vLNZAwAAQBAJ&oi=fnd&pg=PP1&dq=Sammons,+J.,+%26+Cross,+M.+(2017)+Cybercrime&ots=2dxos5yiA2&sig=0tz3bwc1UliqeZiuB2BpLIP-Acc&redir_esc=y#v=onepage&q&f=false

Schieltz, K.M., Wacker, D.P., & Romani, P.W. (2017). Effects of signaled positive reinforcement on problem behavior maintained by negative reinforcement. Journal of Behavioral Education, 26(2), 137-150.

Scholefield, S., & Shepherd, L.A. (2019). Gamification techniques for raising cyber security awareness. In HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21 (pp. 191-203). Springer International Publishing.

Sharif, K.H., & Ameen, S.Y. (2020). A Review of Security Awareness Approaches with Special Emphasis on Gamification. *3rd International Conference on Advanced Science and Engineering, ICOASE 2020*, 151–156. https://doi.org/10.1109/ICOASE51841.2020.9436595

Shipman, M. (2014). The limitations of social research. *The Limitations of Social Research*, 1–174. https://doi.org/10.4324/9781315840727/LIMITATIONS-SOCIAL-RESEARCH-SHIPMAN

Shu, K., Bhattacharjee, A., Alatawi, F., Nazer, T., Ding, K., Karami, M., & Liu, H. (2020). *Combating Disinformation in a Social Media Age*. http://arxiv.org/abs/2007.07388

Silic, M., & Lowry, P.B. (2020). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. *Journal of Management Information Systems*, *37*(1), 129–161. https://doi.org/10.1080/07421222.2019.1705512

Skinner, T., Taylor, J., Dale, J., & McAlaney, J. (2018). The development of intervention e-learning materials and implementation techniques for cyber-security behaviour change. ACM SIG CHI.

Švábenský, V., Vykopal, J., Cermak, M., & Laštovička, M. (2018). Enhancing cybersecurity skills by creating serious games. In Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (pp. 194-199).

Tan, C.C. (2006). The Theory and Practice of Change Management. *Asian Business & Management*, *5*(1), 153–155. https://doi.org/10.1057/palgrave.abm.9200152

Tanner, A., & Preiksaitis, M. (2023). Perspectives of Learning and Training Practitioners on Gamification. CORALS'Journal of Applied Research, 1(1).

Thornton, D., & Francia, G. (2014). Gamification of information systems and security training: Issues and case studies. Information Security Education Journal, 1(1), 16-24.

Thomas, N.J., Baral, R., & Crocco, O.S. (2022). Gamification for HRD: Systematic review and future research directions. Human Resource Development Review, 21(2), 198-224.

Thompson, L., Melendez, N., Hempson-Jones, J., & Salvi, F. (2022). Gamification in Cybersecurity Education: The RAD-SIM Framework for Effective Learning. In European Conference on Games Based Learning (Vol. 16, No. 1, pp. 562-569).

Tobon, S., Ruiz-Alba, J.L., & García-Madariaga, J. (2020). Gamification and online consumer decisions: Is the game over?. Decision Support Systems, 128, 113167.

Wang, P., Wu, P., Wang, J., Chi, H.L., & Wang, X. (2018). A critical review of the use of virtual reality in construction engineering education and training. International journal of environmental research and public health, 15(6), 1204.

Wicks, D.A. (2021). Minimizing zoom fatigue and other strategies for a successful synchronous class experience. Tackling online education: Implications of responses to COVID-19 in higher education globally, 2-24.

Wilson, M., Hash, J., Evans, D.L., Bond, P.J., & Bement, A. L. (2003). *Building an Information Technology Security Awareness and Training Program Technology Administration*.

Wirth, A. (2017). The economics of cybersecurity. Biomedical Instrumentation & Technology, 51(1), 52-59.

Wu, T., Tien, K.Y., Hsu, W. C., & Wen, F.H. (2021). Assessing the effects of gamification on enhancing information security awareness knowledge. Applied Sciences, 11(19), 9266.

Zimbardo, P.G. (2017). *On the ethics of intervention in human psychological research: With special reference to the Stanford prison experiment*.

APPENDIX A - RESEARCH INSTRUMENT, CONSENT & INFORMATION SHEET

Good day

You are invited to participate in an anonymous **Cyber Security Training Questionnaire** as part of my research project, as required to fulfil my Master of Management in Digital Business (MMDB) qualification at WITS Business School.

The questionnaire consists of short multiple choice questions only, and should take you approximately **10 to 15 minutes** to complete.

Title of the study: Gamifying cyber security training for improved employee engagement in the South African banking industry
Purpose of the study: To examine the traditional and gamified cyber security awareness and training content to compare employee training engagement in the South African banking industry.
Author of study: Aashika Bava
Supervisor: Prof. Turgay Celik

The information that you will share will remain strictly confidential and will be used for the purposes of this study. The only people who will have access to the research data is the author of the study, the supervisor of the study and Wits Business School. Your answers to all questions may be used verbatim in presentations and publications, but neither you nor your organisation will be identified. Results will be published in pooled (aggregate) format. **Anonymity is guaranteed** since you are not being asked to provide your name or any personal identification. You will not receive any incentives or benefits for participating in this study. There are no penalties if you choose not to participate or if you withdraw from the study.

If you have any questions or concerns about this questionnaire or the study, please feel free to contact Aashika via email 804403@students.wits.ac.za and/or Prof. Turgay Celik on turgay.celik@wits.ac.za

By completing this survey, you are consenting to participate in this study.

Next

PRE-SCREENING

Do you work for a bank in South Africa?

- ○ No
- ○ Yes

Next

Which department/area do you work in?

- ○ Sales
- ○ Marketing
- ○ Finance
- ○ Human Resources
- ○ Digital/Technology
- ○ Procurement
- ○ Other

Next

DEFINITIONS

Gamified cyber security training definition:
Transforms information or context into a game design application and is topical based on economic events.
Examples: Fake emails sent by your company to test if you can spot a phishing email; games or quizzes; story-telling through a game; badges; a point system; a leader board; avatars, target goals; rewards for training; anything outside of the traditional examples

Traditional cyber security training definition:
Generic cyber security training that delivered through traditional modes and is not specific to a persons' role.
Examples: Pamphlets; posters; newsletters; articles on the intranet; in-person and online training / talks; discussion forums; blogs; basic definition videos and training modules

Which type of cyber security training have you received or experienced in your current or previous company?

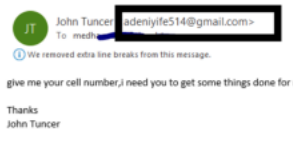
- ○ Both - Traditional and gamified cyber security training
- ○ Gamified cyber security training
- ○ Traditional cyber security training
- ○ None

Next

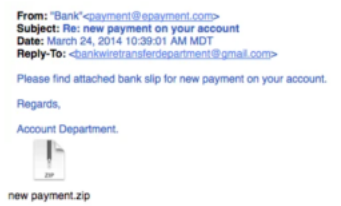
GAMIFIED TRAINING

Please answer the following questions to experience **gamified cyber security training content.**

QUESTION 1:
If you had to design a phishing email, which of the following would you select as examples of phishing warning signs to inform people about?

- [ ] 

- [ ] 

- [ ] 

- [ ] 

QUESTION 2:
In a game-based scenario you are shown how an employee at a bank opened a malicious Microsoft Word file attachment in an email, which released malware onto their computer. The malware created a backdoor into the company's systems, allowing cybercriminals to gain access and deploy a ransomware attack.

Based on this scenario, select all the **malware warning signs** you would pick-up if this happened to you:

- [ ] Blue screen
- [ ] Unwanted program pop-ups
- [ ] Auto opening and/or closing of programmes
- [ ] Sent emails or messages without your involvement

QUESTION 3:
As part of a cyber security game-based training course, you are requested to spin a virtual wheel that contains various cyber categories. You land on the phishing topic, and are prompted to confirm how you would respond to a phishing email related to the organisation that you work for. Select the most applicable solution:

- ◯ Do nothing
- ◯ Report it to the team or individual that will investigate the incident
- ◯ Ignore and delete the email
- ◯ Share it with colleagues to confirm if it's a phishing email

QUESTION 4:
As part of a virtual escape room, you are faced with a challenge to create a malware attack to unlock the door. Choose the option/s that malware attacks begin with:

- ◯ USB with a virus on it
- ◯ Unsafe downloadable software planted on a fake website
- ◯ A fake advert on Facebook, that will prompt someone to click on it and take them to a fake website
- ◯ A fake app in the Play Store or App store
- ◯ All of the above

Next

TRADITIONAL TRAINING

Please answer the following questions to experience **traditional cyber security training content.**

QUESTION 1:
You get a text message from someone who asks you to click on a link to change your password so that you can log in to its website. Select the option/s of what you would do:

- [ ] Reply to the sender and confirm why you need to change your password
- [ ] Report the email
- [ ] Click on the link to change your password immediately

QUESTION 2:
Malware is

- ◯ Software used or created to disrupt computer operations, gather sensitive information, or gain access to systems
- ◯ A form of code, script, active content, and other software
- ◯ A general term used to refer to a variety of forms of hostile, intrusive, or annoying software
- ◯ All of the above

QUESTION 3:
Phishing is

- ◯ Not sure - never heard of this
- ◯ An attack used to obtain sensitive data
- ◯ An attack caused in person by a hacker
- ◯ An attack that can only take place over email

QUESTION 4:
True or false.
If you enable your biometrics, like your fingerprint or facial ID (Identification) on your phone or personal device, or anti-virus software (paid for license) this would help to reduce the risk on a malware attack

- ◯ True
- ◯ False

Next

TRAINING EXPERIENCE

You have experienced both gamified and traditional cyber security training content. Based on your experiences, please provide a rating for each of the following statements:

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
1. Gamified training is more effective than traditional training	○	○	○	○	○	○	○
2. The gamified training is interesting and intriguing	○	○	○	○	○	○	○
3. Traditional training is interesting and intriguing	○	○	○	○	○	○	○
4. Gamified training teaches me something new that I will remember for longer	○	○	○	○	○	○	○
5. Traditional training is more effective	○	○	○	○	○	○	○
6. The gamified training made me want to complete all my training in that format	○	○	○	○	○	○	○
7. Any incentive or reward would catch my attention to complete the training	○	○	○	○	○	○	○
8. Pictures and videos of the cyber threat demonstrations would help me understand the content better	○	○	○	○	○	○	○
9. I prefer to receive a phishing email as part of a simulation than to read about an example online	○	○	○	○	○	○	○
10. I prefer story-telling of real-life phishing and malware attacks through a game	○	○	○	○	○	○	○
11. I prefer 10 minutes on cyber security training compared to 1+ hours of training	○	○	○	○	○	○	○
12. I prefer having a few hours of someone training me on phishing and malware	○	○	○	○	○	○	○
13. A leader board or top achievers rank for completing the training would motivate me to complete my cyber security training	○	○	○	○	○	○	○
14. I regularly read my companies newsletters or cyber security content on the intranet	○	○	○	○	○	○	○
15. Customised training to my role would be beneficial	○	○	○	○	○	○	○

Next