

https://dspace.org/

# Gamification to educate consumers about cybercrime in South Africa

**Maselo, Kehilwe Venacia**

**2024**
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/43778
Maselo, Kehilwe Venacia. (2024). Gamification to educate consumers about cybercrime in South Africa [Master's dissertation, University of the Witwatersrand, Johannesburg]. WireDSpace.

Downloaded from a DSpace repository. https://dspace.org/

# Gamification to educate consumers about cybercrime in South Africa


**Kehilwe Venacia Maselo**

**Student number: 2406422**

**Student email: 2406422@students.wits.ac.za**

**Supervisor: Professor Gregory Lee**





**Johannesburg, 2024**

**Table of Contents**

Table of Contents....ii
List of Tables....vi
List of Figures....vi
**Chapter 1: Gamification use to educate consumers on cybercrime.1**
1.1 Introduction....1
1.2 Background of the study....2
1.3 Context of the Study....3
1.4 Research Problem....5
1.5 Research objectives....6
1.5.1 Primary research objective....6
1.5.2 Secondary research objectives....**Error! Bookmark not defined.**
1.6 Research questions....6
1.6.1 Primary research question....6
1.6.2 Secondary research questions....6
1.7 Justification/Rationale of the Study....6
1.8 Limitations of the Study....7
1.9 Operational Definitions....8
1.10 Structure of the dissertation....9
1.11 Conclusion....10
**Chapter 2: Literature Review....11**
2.1 Introduction....11
2.2 Exploring the role consumers play in cybersecurity....11
2.3 Cybercrime definition and origins....12
2.3.1 Cyber Crime Education....13

2.3.2 The main influence of cybercrime ..... 14
2.3.3 Overview of cybercrime in SA ..... 15
2.3.4 Importance of cybercrime education in SA ..... 16
2.3.5 Different types of cybercrime ..... 17
2.4 Definition of the Gamification Concept ..... 17
2.4.1 Origins of Gamification ..... 18
2.4.2 Gamification Techniques and the education process ..... 19
2.4.3 Gamification techniques and applications ..... 20
2.4.4 Elements of Gamification for Effective Cybersecurity Skills Training ..... 21
2.4.5 Effectiveness of gamification as a medium for educating ..... 21
2.5 Existing Gamification Training Solutions ..... 23
2.6 Successful implementation of gamification ..... 23
2.7 Shortcomings of using gamification to educate consumers on cybercrime 25
2.8 Gamification for educating about cybercrime in other contexts ..... 26
2.9 Research gaps ..... 27
2.10 Theoretical Frameworks ..... 33
2.10.1 Self-determination Theory (SDT) ..... 33
2.10.2 The concept of behavioural science ..... 36
2.10.3 Conceptual framework ..... 37
2.11 Chapter conclusion ..... 41
**Chapter 3: Research Methodology ..... 43**
3.1 Introduction ..... 43
3.2 Research approach ..... 43
3.3 Research Design and Philosophy ..... 44
Figure 3.1: Targeted groups to test the effectiveness of gamification (*Author's compilation)* ..... 45

3.4 Data collection ..... 45
3.5 Population and Sample ..... 46
3.5.1 Inclusion and exclusion criteria ..... 47
3.6 Sample size and sampling method ..... 47
3.7 Research Instrument and data collection procedures ..... 49
3.8 Data analysis ..... 49
3.8.1 Definition of variables ..... 51
3.8.2 Independent variable: Gamification ..... 51
3.8.3 Dependant variable 1: Consumer knowledge of cybercrime ..... 52
3.8.4 Dependent Variable 2: Consumer attitude towards cyber crime ..... 52
3.8.5 Outcome variable ..... 52
3.9 Ethical consideration ..... 52
3.10 Privacy and anonymity ..... 53
3.11 Chapter conclusion ..... 53
**Chapter 4: Data analysis and interpretation .....54**
4.1 Introduction ..... 54
4.2 Data screening ..... 54
4.3 Sample characteristics / Demographic ..... 54
4.3.1 Gender ..... 54
4.3.2 Level of education ..... 55
4.3.3 Income ..... 55
4.3.4 Have a bank account in SA ..... 56
4.4 Hypothesis testing ..... 58
4.5 Concluding comments ..... 64
**Chapter 5: Findings and recommendations .....65**
5.1 Introduction ..... 65
5.2 Effectiveness of gamification on knowledge enhancement ..... 66

5.3 Customised content for improved engagement ..... 67
5.4 Learning preferences in educational games ..... 69
5.5 Gamification: Perception vs. Effectiveness ..... 70
5.6 Attitudinal and behavioural change ..... 71
5.7 Efficacy of gamification as a tool to educate consumers ..... 72
5.8 Limitations and recommendations ..... 73
5.8.1 Linguistic landscape ..... 73
5.8.2 Financial institutions to collaborate with third parties ..... 76
5.9 Future research ..... 76
**References ..... 80**
Appendices ..... 99
List of tables ..... 99
Research instrument ..... 107
List of Figures ..... 111
Figure 3.1: Effectiveness of gamification (*Author's compilation)* ..... 112

## List of Tables

Table 2.1: Identified research gaps .....

Table 2.2: Relationship between constructs .....

Table 4.1: Chi-square p-values for sample characteristics/demographics .....

Table 4.2: Comparing results by whether a respondent played the game.....

## List of Figures

Figure 2.1: Proposed conceptual framework.....

Figure 3.1: Effectiveness of gamification.....

Figure 4.1: Respondent gender.....

Figure 4.2: Highest level of education completed.....

Figure 4.3: Respondent income .....

Figure 4.4: Have a bank account in SA.....

Figure 5.1: South African linguistic landscape.....

## Abstract

This study examines the impact of gamification on South African consumers attitudes and understanding of cybercrime. Given the increasing reliance on the Internet activities such as social media, digital banking, and e-commerce, there is a critical need for consumers to adopt basic security measures to protect themselves against threats such as privacy breaches, identity theft, cyberbullying, and exposure to harmful content.

However, many individuals lack the necessary knowledge and expertise to ensure their online security. The research explores the challenges associated with enhancing security awareness and assesses the potential of gamification techniques to overcome these obstacles. By integrating game mechanics and elements into online security awareness activities, the study aims to make learning about cybersecurity engaging and enjoyable, leading to better understanding and adoption of safe online practices.

The findings indicate that gamification significantly enhances consumer engagement, knowledge retention, and proactive cybersecurity behaviours. Additionally, the research contributes to the theoretical framework of Self-Determination Theory (SDT) and behavioural science by providing empirical evidence that intrinsic motivation, fostered through gamification, enhances learning outcomes and behaviour change in cybercrime education. These insights offer valuable implications for businesses and organisations seeking to improve their cybersecurity training and consumer awareness campaigns. Ultimately, this research highlights gamification's potential to transform cybersecurity education and to promote a more cyber-aware and proactive consumer base in South Africa.



**Keywords:** Cybercrime, gamification, knowledge, attitudes, behavioural change, cybersecurity.

# Chapter 1: Gamification use to educate consumers on cybercrime

## 1.1 Introduction

The research examines the impact of gamification on South African consumers' attitudes and understanding of cybercrime. The Internet is essential to our daily life, offering an array of web services including social media, digital banking, and e-commerce websites (Naeem & Ozuem, 2021). As more consumers engage in online activities, it is crucial to acquire and apply basic security measures to protect their security and well-being, which can be impacted by various factors such as privacy breaches, identity theft, cyberbullying, and exposure to harmful content. However, many individuals lack the necessary knowledge and expertise to ensure their online security. The research recognises the challenges associated with enhancing security awareness and assesses the potential of gamification techniques to overcome these obstacles. It also considers the growing popularity of digital platforms and concerns about escalating digital banking fraud (Cavaliere et al., 2021).

Therefore, this study seeks to enhance online security awareness programmes by integrating game mechanics and elements. This integration not only aims to enhance the overall learning experience but also makes learning exciting and enjoyable. Ultimately, learning leads to a better understanding and the adoption of safe online practices.

Chen et al. (2023) believes that the use of gamification in the banking industry has yielded encouraging outcomes in terms of strengthening the consumer engagement, satisfaction, and brand loyalty which contributes to the detection and prevention of cybercriminal activities. Studies have shown a clear and robust connection between the use of gamification techniques and an increased inclination to engage with mobile banking services, highlighting that the concept of gamification has the potential to make banking interactions more compelling and pleasurable for consumers (Rahi & Ghani, 2019; Bitrián et al., 2021). The increase in engagement may result in a better understanding of consumer activity which in turn can aid in recognising inconsistencies that may be indicate of fraudulent behaviour.

Gamification enhances cybercrime awareness by providing interactive experiences with game-like elements that educate consumers on how to identify and respond to cyber threats in a safe environment (Alqahtani & Kavali-Thorne, 2020). Engaging with these elements increases investment in learning and information retention, encouraging the application of secure banking practices. Immediate feedback in gamified training helps consumers to understand the impact of their actions and adjust their behaviours, leading to improved online security. These findings may have important implications for the banking services industry and may establish a foundation for future studies on the implementation of gamification in cybersecurity education and awareness.

## 1.2 Background of the study

Technological innovation has brought many benefits to society, including easier communication, better access to information, and new opportunities for online banking. Bokang and Mapimele (2019) reports that the incidence of cybercrime in South Africa (SA) has risen in the past few years. This can be attributed to the country's status as a prominent financial and technological hub in Africa. Incidents include online banking fraud, phishing, identity theft, and ransomware attacks. Bokang and Mapimele (2019) further highlighted in their analysis that the legislative and regulatory framework for cybersecurity in South Africa is still in the process of development, even though cybercrime poses a significant threat to national security and the economy. It is a pressing issue that requires immediate attention.

The country has a significant rate of Internet penetration but lower levels of cybersecurity awareness and preparedness, and this contributes to the country's cybercrime epidemic (Kshetri 2019; Stats SA 2022). Olofinbiyi (2022) confirms that cybercrime is a major issue, and it is projected to continue expanding as the country becomes more interconnected. Addressing this issue will require a multifaceted strategy, which includes enhanced cybersecurity education, strengthened legal and regulatory frameworks, and more investment in cybersecurity infrastructure (Olukayode 2021). However, the primary objective of this study is to enhance cybersecurity education.

The increasing popularity of digital channels has led to a rise in the use of mobile banking apps and web-based banking platforms for conducting financial transactions (Rahi & Ghani, 2019). Although the use of digital technology has brought about many benefits, it has also contributed to a rise in cybercrime. Cybercrime can have severe consequences, including economic and reputational harm, theft of personal information and in some cases physical damage (Olukayode 2021).

Efforts to tackle cybercrime in SA have led to the establishment of institutions such as The Cybersecurity Hub and the South African Banking Risk Information Centre, which continue to work with partners from government, businesses, and the broader community to address these challenges. However, among the obstacles in this regard are insufficient knowledge and skills among consumers, as they often do not fully comprehend the risks and consequences of cybercrime or know how to safeguard themselves from online threats. This conclusion is supported by a study by Garba et al., (2020) who discovered that university students lacked understanding of cybercrime. While several studies have demonstrated the effectiveness of gamification in various fields such as education, health, and marketing (Deeleman and Van Steen, 2021), this research sought to explore gamification as a communication medium in addressing cybersecurity training.

Hassan and Hamari (2019) investigated opportunities and barriers to gamification in cybersecurity education and found that gamification can boost motivation and engagement, but only when well-designed and thought out beforehand. The absence of clear learning objectives, inadequate game mechanics design, and excessive dependence on gamification have all been identified as barriers to effective outcomes (Almeida et al., 2023). Nevertheless, the effectiveness of gamification for cybersecurity awareness and the prevention of cyber threats has not been fully explored in the South African context.

## 1.3 Context of the Study

The growing use of digital platforms has amplified the risks associated with digital banking fraud. In the South African financial sector, cybercrime has risen at an unprecedented rate in recent years (Bokang & Mapimele, 2019). The COVID-19

pandemic has led to a surge in technological vulnerabilities associated with consumer adoption of digital banking channels, as they were unable to visit an actual branch. Consumers therefore started to embrace online shopping platforms more, leaving them more susceptible to fraud (Chen et al., 2023).

For instance, standard online banking transactions entail the transmission of personal data, including home addresses and bank card information such as credit card details. Fraudsters have found easy ways to target individuals by soliciting their banking details, including their personal identification number (PIN), in order to defraud them. The fraudsters' *modus operandi* consistently changes as they continue to find innovative ways to trick consumers into sharing their PINs or clicking on malware-encrypted links, with the intention of taking over their accounts (Li & Liu, 2021). According to Chen et al. (2023), this type of technology affects the way consumers behave in the digital banking era. Consumers are concerned about data breaches, which can undermine trust in the digital banking platforms and ultimately lead to a reduction in the adoption and use of such services.

Salahdine and Kaabouch (2019) further explained that biometric authentication systems, such as fingerprint scans, have become more prevalent, while passwords continue to be the primary means of gaining access to online services. Therefore, banks must ensure consumer security when it comes to the use of passwords online. For the sake of consumer safety, it is essential to develop strategies that promote password security, such as the implementation of stringent verification protocols and two-factor authentication. Durrani et al. (2022) found using gamification challenges and rewarding consumers, the intention of this study is to increase security awareness regarding the hygiene factors the consumer will need to consider when transacting on their online banking platforms.

It is unfortunate that consumers continue to divulge their personal information to fraudsters and compromise their security despite the bank's efforts to educate consumers on fraud prevention methods (SABRIC, 2020). Although numerous initiatives have been taken to heighten public awareness and educate them about cybercrime, consumers still find themselves ill-equipped to deal with the ever-evolving online threats (SABRIC, 2020). This lack of awareness and skills can have severe consequences, not only for individuals, but also for businesses and the economy

(Koivisto 2022). Therefore, it is necessary to develop more efficient strategies to educate and engage South African consumers in cybercrime. Consumers are usually the easiest targets in the cybersecurity chain and teaching them to protect their personal data can improve the security of businesses and the entire country (Xiao et al., 2022).

Gamification promotes autonomous and self-directed learning by providing consumers with control over their learning experience. It creates a sense of connection and relevance between the user and the learning content, making the education process more engaging and personal, thus enhancing both the learning experience and the retention of cybersecurity knowledge (Lachner et al., 2022). The research proposed to help assess the potential of gamification as a communication medium to educate consumers regarding cybercrime in SA.

## 1.4 Research Problem

Prior research has identified several research gaps, including a lack of comprehension of the factors that influence the effectiveness of gamification in the context of cyber security education (Lachner et al. 2022).

Koivisto (2019) notes that empirical evidence has shown the effectiveness of gamification in various fields including education, health, and marketing. However, its potential for enhancing cybercrime awareness and prevention has not been fully investigated. Gamification increases user engagement, knowledge retention, and encourages changes in consumers' behaviour towards safer cybersecurity practices. However, the factors determining its effectiveness in cybersecurity education are not well understood (Salah and Alzaghal 2022). The gamification system's design, level of interactivity, user motivation, and learning style are all factors that could be relevant (Khan et al., 2022). However, there has been a lack of research on the impact of gamification on the consumer attitudes and knowledge of cybercrime in SA.

This study might add new knowledge on cybercrime and how gamification can enable cybercriminal activity detection and prevention in the banking industry. This is a critical knowledge development that could contribute to the existing body of knowledge, as

the assessment of gamification as an educational and awareness tool is most likely to alleviate the occurrence of cybercrime.

## 1.5 Research objectives

### 1.5.1 Primary research objective

- Understanding the effectiveness of gamification as an educational medium for educating consumers regarding cybercrime in SA.

### 1.5.2 Secondary research objectives

- Assessing the effectiveness of gamification in increasing consumers' cybercrime knowledge
- Assessing the impact of gamification on consumer attitudes towards cybercrime

## 1.6 Research questions

### 1.6.1 Primary research question

- How effective is gamification as an educational tool to combat cybercrime in SA?

### 1.6.2 Secondary research questions

- How effective is gamification in increasing consumers' knowledge of cybercrime?
- What is the impact of gamification on consumer attitudes towards cybercrime?

## 1.7 Justification/Rationale of the Study

The aim of this research was to explore the impact of gamification on consumer's knowledge of and attitudes towards cybercrime in SA. The findings could potentially contribute to the existing literature and provide valuable insights to numerous

stakeholders and policymakers on how to strengthen education policies and build efficient cybercrime education programmes and campaigns in SA. These findings can be used by industry professionals, such as marketers in the retail banking sector, to create cutting-edge, useful, and interesting cybercrime education campaigns, as there is a need to explore effective ways of educating consumers regarding cybercrime-associated risks and protection against cybercriminals.

The study also highlights the need for innovative and effective strategies that businesses can use to engage with the public, which may benefit them significantly because the use of gamification may lead to enhanced customer trust and confidence, resulting in increased customer loyalty and sales. From a consumer perspective, adopting best practices may reduce the risk of falling prey to cybercrime, improve overall online security, and enable them to transact online more safely and with greater peace of mind (Dlamini & Mbambo, 2019).

The outcomes of the present investigation should enhance our understanding of the frequency and structure of cybercrime and provide insight into potential measures to reduce cybercrime occurrence and patterns. This can be accomplished by educating consumers through gamification designs and programmes.

## 1.8 Limitations of the Study

The study has several limitations, including factors such as geographical scope. Specifically, the research is mainly focused on consumers in South Africa, which may limit the generalisability of the findings to other countries or regions with different social, economic, and political contexts. In addition, the sample size may be limited by practical considerations such as time and budget constraints. This could reduce the sample representativeness and the knowledge development process of the study.

In addition, self-report measures will be utilised to evaluate changes in participants' knowledge, attitudes, and behaviours regarding cybersecurity. While these measures are widely used, they may not always be accurate in reflecting the actual knowledge, attitudes, and behaviours of the participants as they are subject to bias.

## 1.9 Operational Definitions

**Cybercrime** is defined as any illegal or unethical activity committed by utilising digital mediums, such as computers, the Internet, and mobile phones. It includes phishing, hacking, malware attacks, and identity theft, as well as cyberbullying (Phillips et al., 2022).

The concept of **cybersecurity awareness** encompasses the knowledge and comprehension of potential cybersecurity risks, threats as well as the measures taken to prevent them (Zwilling et al., 2022).

A **consumer** is to an individual who utilises digital technologies for personal reasons such as accessing social media or engaging in online banking, and purchases goods or services for their own consumption (OECD, 2020).

**Effectiveness of Gamification** is the extent to which gamification intervention is successful in achieving its intended outcomes, such as increasing cybersecurity awareness and preventing the success of cybercrime among consumers. The efficacy of the intervention will be assessed by changes in the participants' knowledge, attitudes, and behaviours related to cybersecurity (Alqahtani & Kavakli-Thorne 2020).

**Knowledge** refers to an understanding of the different types of cyberthreats, as well as the methods employed by fraudsters. It includes being aware of potential vulnerabilities and implementing effective strategies for safeguarding personal information (Zwilling et al., 2022).

**Attitude** refers to an individual's viewpoint, emotional response, and inclination towards cybersecurity which can influence their readiness to practice safe online behaviours encouraged by the engaging and motivational aspects of gamified learning (Ferrer et al., 2022).

**Gamification** is the process of incorporating aspects of game design, such as points, challenges, and rewards, into non-game settings such as training to enhance engagement, motivation, and learning (Deterding et al., 2011; Barreto and França 2021). Studies have demonstrated that gamification can be a highly effective method for disseminating information and fostering behavioural change (Deeleman and Van Steen 2021). In the context of cybersecurity education, gamification can help to

improve user engagement and knowledge retention. However, it is important to design relevant, meaningful, and effective gamification experiences (Khan et al., 2022).

**Cybersecurity prevention** - Cybersecurity prevention is the adoption of behaviours and practices that reduce the risk of cybercrime, such as creating strong passwords, maintaining software updates, and exercising caution when divulging personal information online (Alkhalil et al., 2021).

**Cyber-attacks are** malicious acts that employ digital technologies to damage, steal information from, or disrupt computer systems and networks (Li & Liu, 2021).

## 1.10 Structure of the dissertation

The research examined the effectiveness of gamification as a communication medium to educate SA consumers regarding cybercrime. It assesses the impact of gamification on consumer comprehension and awareness of cybercrime in the country by conducting a comprehensive literature review and analysis. The study also considers the ramifications of gamification as a strategy and its potential to effect positive consumer behaviour change.

This report is divided into five chapters, each addressing a distinct research topic. The study's background and context are presented in Chapter 1, along with the primary research questions, objectives, and limitations. The chapter also highlights the problem statement, which emphasises the need for effective communication strategies to raise cybercrime awareness among SA consumers.

Chapter 2 explores the function of gamification through a comprehensive literature review and analysis, investigates the use of gamification technology as a means of communication and analyses previous research, which includes identifying and addressing research gaps regarding the incorporation of game elements in educational settings.

The research methods and techniques used to evaluate the theoretical foundations of gamification technology as a communication medium for consumer cybercrime education are elaborated upon in Chapter 3. The study adopted an interpretivist

methodology and used surveys as the primary method of data collection. The following chapters present the results of the thematic analysis conducted on the data.

Chapter 4 provides an analysis and interpretation of the data that has been obtained. This is where the findings of the study will be discussed, highlighting the advantages and disadvantages of using gamification technology as a communication medium for cybercrime education for consumers in SA.

The evidence-based conclusions and recommendations will be presented in Chapter 5, based on the scientific research procedure. This chapter draws on the study findings to make recommendations at the management and policy levels to enhance the efficacy of communication strategies aimed at educating South African consumers on cybercrime.

## 1.11 Conclusion

The goal of this research was to contribute to the existing literature with regard to the use of gamification technology as a communication tool for cybercrime education among consumers. By conducting a thorough literature review (Chapter 2), research methodology (Chapter 3), and data collection and analysis (Chapter 4), in addition to providing recommendations, this study offers valuable insights for policymakers and other stakeholders (Chapter 5). Furthermore, it can assist in informing the creation of effective communication programmes that can increase South African consumers' awareness of cybercrime.

# Chapter 2: Literature Review

## 2.1 Introduction

The section critically examines and evaluates the literature with a focus on addressing the research gaps identified in the research questions. The concepts of gamification and cybercrime are used to illuminate the factors that enable gamification to be used as a communication medium to educate South African consumers regarding cybercrime.

## 2.2 Exploring the role consumers play in cybersecurity

In the context of cybersecurity, the human element has been identified as the weakest link because of human error, poor practices, and lack of awareness. According to Amorosa and Yankson (2023), 95 percent of cybersecurity breaches are attributable to human error. In contrast to technical vulnerabilities or system flaws, the human element of cybersecurity refers to security risks and privacy concerns from the actions or conduct of individuals, such as employees or customers (Zoto et al., 2018).

Sociotechnical systems are composed of social, psychological, technical, and environmental elements that rely on the interactions between people and technology to function cohesively (Zimmermann & Renaud, 2019; Ali, 2019). Deeleman and Van Steen (2021) believe that effective cybersecurity calls for the effective management and application of human factors to mitigate cybersecurity threats and risks.

Despite the vast amount of personal data available to anyone to access human behaviour, consumer decisions remain unpredictable and irrational. This can lead to a considerable vulnerability to cybersecurity risks (Nguyen & Pham, 2020). Human beings are often considered to be the most vulnerable aspect of cybersecurity systems for several reasons, such as poor cybersecurity practices, lack of awareness, shared responsibility, motivation to implement cybersecurity practices, and inconvenient cybersecurity protocols (Zimmermann and Renaud 2019). Therefore, Nguyen and Pham (2020) further emphasised that cybersecurity socio-technical systems should prioritise security awareness to educate users on the significance of data and potential

risks, thereby reducing human error. On the contrary Zimmermann & Renaud (2019) posited that humans could be regarded as a solution to cybersecurity issues, rather than a hindrance. However, it is crucial to prioritise the management and education of individuals to ensure that they can positively contribute to cybersecurity efforts.

## 2.3 Cybercrime definition and origins

Norbert Wiener, a prominent mathematician, created the term "cyber" to describe the study of information exchange between living things and artificial devices, thereby giving rise to the concept of "cybernetics" (Wiener 2019). The cyber realm encompasses a wide range of components, from individuals who use the networks to the software and services that run on devices. With the networks linked to the software and services, the processes and information circulated between the applications and systems that store them are all connected, creating a constantly evolving and changing virtual environment. The concept of "cyberspace" encompasses the interconnected systems and services that are accessible through the Internet and telecommunications, as explained by Ning et al. (2018).

Cybercrime refers to the unlawful use of digital technologies which includes computers and computer networks to commit offenses, such as hacking, phishing, identity theft, and virus attacks, in addition to online fraud ( (Li & Liu , 2021). This expanding global problem has severe repercussions for individuals, businesses, and governments, including financial losses, reputational harm, and data breaches, which undermine public confidence in digital technologies.

Cybercrime dates to the earliest days of computer networking, when hackers broke into systems for fun or to test their skills (Chigada & Madzinga, 2021). However, it has evolved into an organised and sophisticated criminal enterprise, with cybercriminals employing sophisticated techniques to steal sensitive information and extort money from victims. Due to the emergence of new technologies and attack vectors on a regular basis, cybercrime must be combated using a multifaceted strategy that incorporates increased awareness, collaboration, and investment in cybersecurity measures (Cascavilla et al., 2021).

Governments, businesses, and consumers must therefore collaborate to implement effective cybersecurity strategies and practices that can help minimise the threats posed by cybercrime. This necessitates constant learning and adaptation to stay ahead of cybercriminals and to reduce the risk of cyberthreats.

### 2.3.1 Cyber Crime Education

Cybercrime education has become a vital reaction to the escalating number of cyber-intrusions and cyberattacks (Khader, et al., 2021). Despite this, attackers exploit weaknesses that can be attributed to human error; however, cyber education security has primarily focused on the information technology aspect while ignoring the human factor (Zimmermann and Renaud 2019). Human vulnerabilities include negligence, inadequate skills, misinformation, insider malice, and unauthorised third-party Internet access. To address the issue of cybercrime, it is necessary to equip consumers with cybersecurity capabilities and heighten cybersecurity knowledge in the workplace, management, and academic institutions (Zoto et al., 2018).

Hatzivasilis et al. (2020), and McIlwraith (2021) determined that traditional cybersecurity education programs are sometimes limited to IT personnel and that awareness campaigns potentially target only those employees. This is insufficient for combating cybercrime and does not reduce the number of organisational attacks (Bossler & Berenblum, 2019). Ineffective instructional methods include online information dissemination strategies, classroom training sessions, and extensive instructional programs that produce passive, overwhelming, and disconnected learning environments (Almeida et al., 2023).

In order to enhance cybersecurity training, a robust and inclusive participatory approach is necessary (Borrás-Gené et al., 2019). The gamification strategy, which employs entrepreneurial perspectives and rewards, can be utilised to improve cybersecurity skills training programs. This strategy promotes crime prevention through skill training for consumers, as well as hands-on, immersive, and interactive training, as well as the differentiation between cyber security skills training and cyber security awareness training. Newsletters and web-based classrooms, teleconferencing, instructor-led training, and cyber security-themed events are all examples of educational programs (Kimpe et al., 2021). However, gamification may

be more effective in increasing user engagement and motivation, which is necessary to reduce human vulnerabilities and fight cybercrime.

### 2.3.2 The main influence of cybercrime

The rapid evolution of technology, which provides cybercriminals with new opportunities to exploit vulnerabilities in digital systems, has had the greatest impact on cybercrime. According to Alkhalil et al. (2021), the advancements in technology have elevated the level of sophistication in cyberattacks which in turn has made it harder for both individuals and organisations to defend themselves against such attacks. In addition, Anderson et al. (2021) noted that recent advancements in artificial intelligence and machine learning have made it simpler for cybercriminals to conduct large-scale attacks.

The most prevalent types of cybercrime are phishing scams, social engineering, and other attacks that rely on human error or manipulation. Consequently, combating cybercrime requires not only technical measures but also education and awareness-raising activities to strengthen cybersecurity practices (Salahdine and Kaabouch 2019). It must be emphasised that cybercrime has far-reaching repercussions including financial loss, reputational harm, and the compromise of sensitive data. Moreover, cybercrime prevalence significantly threatens the global economy and security. Thus, it is crucial to develop effective strategies and technologies to combat cybercrime and protect digital systems from unauthorised access and malicious activities.

Alkhalil et al. (2021) established that ransomware attacks are becoming increasingly sophisticated, incorporating advanced techniques such as encryption and anti-analysis capabilities. This trend has made it more difficult for organisations to detect and prevent such attacks, and this has resulted in substantial financial and operational losses. In addition, the increasing prevalence of cybercrime in the COVID-19 pandemic setting was highlighted in a study by Kshetri (2019), since more individuals and organisations relied on digital systems to conduct their daily business, with the author further noting that the pandemic created new opportunities for cybercriminals. The research highlighted the importance of implementing robust cybersecurity

measures to tackle the distinct challenges arising from the pandemic and to avert the undermining of global pandemic control efforts by cybercrime.

The literature suggests that the rapid evolution of technology and the increasing sophistication of cyberattacks pose significant challenges for organisations and consumers attempting to defend themselves against cybercrime (Salahdine & Kaabouch, 2019). Effective cybersecurity strategies must include both technical and nontechnical measures to address the complexity of the problem.

### 2.3.3 Overview of cybercrime in SA

Cybercrime has emerged as a major threat to SA, as it has worldwide (Jung et al., 2021). The country has witnessed an increase in various types of cybercrime owing to the expanding use of technology and the Internet (Dlamini & Mbambo, 2019). These crimes have significantly impacted both consumers and businesses, causing widespread concern. According to Kshetri (2019), a thorough examination of the relevant literature suggests that there has been a concerning rise in online fraud and other forms of cyberattack in SA over the years, which indicates a significant increase in cybercrime. Moreover, the increased sophistication of cybercriminal methods makes it more difficult for consumers and organisations to protect themselves.

SA has emerged as the main hub for cybercrime in Africa, according to an Interpol report providing key insights into cybercrime on the continent that emphasised the rising cyber-threats (Jung et al., 2021). SA ranks third globally, leading the African continent, where the number of victims affected by cybercrime is concerned, losing R2.2 billion a year (Mcanyana et al., 2020). The Accenture Research Report further points out that 230 million threats were detected in SA in 2022, with email being the most common method; however, the country is also said to have the highest targeted ransomware and attempts to compromise business email. Therefore, it is impossible to overstate the impact of cybercrime on businesses, with financial loss and reputational harm being the most common outcomes (Mcanyana et al., 2020). SMEs have suffered significantly from cyberattacks, particularly in terms of financial losses, and some have been unable to recover (Bokang & Mapimele, 2019). Insufficient awareness and investment in cybersecurity measures further exacerbate the situation (SABRIC, 2020).

Therefore, the challenges posed by cybercrime necessitate a multifaceted strategy (Cascavilla et al., 2021; Olukayode, 2021). First, it is crucial to raise awareness about cybercrime and its consequences. Education and training initiatives aimed at both individuals and businesses can accomplish this. The significance of fostering collaboration among key stakeholders, including law enforcement agencies, industry organisations and cybersecurity specialists, lies in their ability to recognise developing threats and devise efficient mitigation measures. To prevent cybercrime, it is essential to invest in cybersecurity measures, including the implementation of cutting-edge cybersecurity tools and technologies.

### 2.3.4 Importance of cybercrime education in SA

According to Jung et al. (2021), cybercrime is a growing global concern, and SA is no exception. Cybercrime significantly impacts individuals and businesses in SA, causing monetary losses, reputational harm, data breaches, and operational disruptions. Olukayode (2021) found that cybercrime victims in SA, as elsewhere, experienced negative emotional, social, and financial repercussions, leading to losses in productivity and income. In this regard, consumer education can play a crucial role in increasing cyber risk awareness, promoting responsible technology use, and supporting the protection of sensitive personal data.

According to Salahdine and Kaabouch (2019), raising public awareness about cyberthreats including their identification and prevention can decrease the probability of individuals becoming victims of cyberattacks. However, Dlamini and Mbambo (2019) indicate that many South Africans have limited comprehension of the potential hazards of digital technology and the significance of protecting their personal information. Consequently, SA requires more inclusive and accessible cybercrime educational initiatives.

According to Stats SA (2022), SA is a culturally and linguistically diverse nation, and cybercrime education initiatives must take these differences into account to ensure that everyone has access to cybercrime education and understand its significance. In addition, including under-represented groups in cybercrime education initiatives, such as women and marginalised communities, can help bridge the gender and digital divide, empower these groups, and improve SA's overall cybersecurity. In order to

achieve the desired outcomes, educational programmes should be customised to meet the unique requirements of SA communities.

### 2.3.5 Different types of cybercrime

This study focuses on some of the most prevalent cybercrime types, as discussed more fully below. By gaining an understanding of these kinds of online and digital criminal activities, individuals can take precautions against becoming victims (Cascavilla et al., 2021).

**Phishing** occurs when criminals use social engineering to obtain personal information from individuals via phone calls, text messages, and emails. The data is then employed to gain unauthorised access to bank accounts for the purpose of committing identity theft.

**Vishing** is similar to phishing, except that criminals use voice calls to obtain personal information about individuals.

**Smishing** occur when criminals use SMS messages to obtain unsuspecting individuals' personal information.

Malicious software, commonly known as **malware**, is designed to infiltrate computer systems without authorisation and steal confidential information. Emails, downloads, and malicious websites can all be used to spread malware.

The act of **identity theft** involves the use of personal information which includes social security numbers and bank account details to perpetrate fraud or misappropriate funds.

**Online banking fraud** occurs when criminals use phishing or malware attacks to access unsuspecting consumers' online banking accounts and defraud them.

## 2.4 Definition of the Gamification Concept

The digital media industry has popularised the idea of gamification, which involves incorporating game design aspects into non-game situations. According to Torres-Toukoumidis et al. (2021), gamification mechanics are based on human desires,

including rewards, status, competition, self-expression, accomplishment, and altruism. Despite extensive research on gamification, few studies have focused on its application in crime prevention (Welbers, et al., 2019). Gamification is a technique used to improve a service by integrating game-like components, such as progress tracking, player engagement, rewards, and narrative structures, into non-game contexts (Fitz-Walter et al., 2017; Deterding, 2019). This approach also involves fostering collaborative problem-solving, and by aligning motivation with objectives, gamification can be an effective technique for influencing and encouraging individuals' desired behaviours (Alqahtani & Kavakli-Thorne, 2020). Gamification is an effective method for enhancing employee engagement and motivation by incorporating elements of play and competition both within and across the various teams. By doing so, routine tasks can be transformed into enjoyable activities (Borrás-Gené et al., 2019; Bitrián et al., 2021).

As explained by Alqahtani and Kavakli-Thorne (2020), gamification involves the use of game elements to solve problems through a series of activities and procedures. This definition is essential for comprehending the precise meaning of gamification because it emphasises its systematic approach to problem solving. It also underscores the significance of intentionally utilising game mechanics such as badges and points, as opposed to relying solely on them (Deterding, 2019).

Gamification is a dynamic approach to information security awareness that can provide consumers with substantial benefits beyond conventional training. In addition, gamification can help students retain information and apply it in real-world contexts by making learning more interactive and engaging (Ali 2019). Moreover, gamification can foster a sense of competition and accomplishment among individuals to improve motivation and performance and can be an effective tool for promoting cyber security awareness education.

### 2.4.1 Origins of Gamification

The literature review shows that gamification originated in the Soviet Union, where motivational techniques were utilised to boost factory productivity during the early-to mid-20th century (Nelson 2012). Subsequently, gamification was integrated into various settings such as sales, education, production, and health, along with

sustainability, with the goal of engaging clients, consumers, learners, and employees, as well as the public (Ferrer et al., 2022; Yamani, 2021; Z ennaro & Erdődi, 2023).

In recent years gamification has also been implemented in the workplace utilising components of a game such as competition, badges, and points of achievement (Boudadi et al., 2020; Christians 2018). Burke (2021) has observed that gamification utilises psychological concepts such as competition and the desire to succeed. According to Nguyen and Pham (2020), game elements have been employed to induce specific behaviours in various contexts, including business management, advertising, and marketing activities.

In the workplace, gamification has expanded to include competitive activities between individuals and groups, points as a measurement of progress, and achievement badges as gaming elements. As Alqahtani and Kavakli-Thorne (2020) and Vesa (2021) assert, gamification can motivate a desire for competition and achievement by exploiting the human spirit, making serious activities enjoyable by transforming them into games. Borrás-Gené et al. (2019) noted that one major benefit of gamification is that it strengthens the connections between institutions, their employees, and their customers.

However, Almeida et al. (2023) point out that some of the concerns regarding the propensity to manipulate and influence behaviour excessively have prompted criticism of gamification. Nevertheless, gamification may impact the consumer behaviour when used responsibly to increase participation in diverse disciplines such as education and information dissemination. Scholefield and Shepherd (2019) emphasise that it needs to be critically and methodically presented to be effective and advantageous as an instructional strategy. Such methodical approaches in gamification can improve the content of games and contribute to the programme's personalisation for resource optimisation.

### 2.4.2 Gamification Techniques and the education process

Marczewski (2020) uncovered several gamification techniques to create engaging learning experiences. In addition to offering physical incentives and clear instructions these methods also involve posing challenges to users. Zichermann and Cunningham (2021) have revolutionised gamification with the Status, Access, Power, and Stuff

(SAPS) rewards system, which integrates the distribution of rewards, authority, and power. For example, users can acquire status by performing well or competing against their peers on leaderboards, and access can be granted via loyalty programs. Users can be granted authority through moderator duties and given free rewards as incentives for the continued use of an application. These gamification strategies have been successfully integrated in educational platforms like Duolingo or ClassDojo to improve learning outcomes and increase user engagement (Burke, 2021; Scholefield & Sheperd, 2019). Overall, gamification can be a powerful instrument for creating immersive and engaging learning experiences, but it requires careful consideration and implementation of effective gamification techniques to be truly effective.

### 2.4.3 Gamification techniques and applications

In 2017, Marczewski's research catalogued various gamification mechanics used to create learning solutions that maintain user engagement. The mechanisms employed involve presenting users with obstacles and offering tangible incentives, while also utilising signposting to prevent users from becoming lost within an application. Zichermann and Cunningham (2021) investigated several gamification techniques that can be implemented in various contexts, including SAPS. Scholefield and Shepherd (2019) and Thompson et al. (2022) believed that these techniques involve employing gamification to motivate users with rewards. Users can earn status by comparing their performance with that of their peers. Access can be implemented through loyalty programs to maintain user engagement whereas power can be attained by assigning moderator duties to users. To encourage users to keep using the platform, the "stuff" category offers free rewards as an incentive.

Educational games such as Duolingo and ClassDojo have successfully implemented gamification mechanics to improve their learning experiences. For example, Duolingo offers incentives, such as points, streaks, and virtual currencies, to encourage users to continue learning new languages (Loewen et al. 2019). ClassDojo provides teachers and parents with a platform for monitoring and rewarding student progress, thereby encouraging them to acquire new skills. By utilising gamification mechanisms such as SAPS and offering rewards and incentives, applications can keep users engaged and motivated, resulting in enhanced learning outcomes.

### 2.4.4 Elements of Gamification for Effective Cybersecurity Skills Training

It is essential to clearly define training objectives when designing effective games for training and education (Deeleman and Van Steen 2021). In order to create games that are relevant and effective for the desired training approach, it is crucial to select the correct gamification elements. The research investigated four gamification components for enhancing cybersecurity skills training. These components include tools that motivate players by offering solutions to monitor their progress (Tobon et al., 2020). Examples of such tools include **progress mechanics** such as badges, points, and leaderboards.

An important component of gamification is the use of avatars or characters to control the players. According to research, behavioural patterns can be influenced by avatars. The use of avatars or characters for **player control** is important to gamification. Furthermore, Vesa (2021) discovered that the employment of avatars may have an impact on individuals' attitude.

Collaboration and identification of shared goals are essential to the development of **problem-solving** skills. This is particularly important in gamification, when new data must be comprehended and applied outside the training environment. Using a narrative can foster a connection amongst the student and their avatar but also between the avatars participating in the gamified programme. Additionally, a story can entice the learners to continue participating in order to discover the outcome of a narrative (Bitrián et al., 2021).

### 2.4.5 Effectiveness of gamification as a medium for educating

Gamification has gained prominence in recent times as a highly effective and captivating educational approach. Numerous studies have demonstrated that incorporating elements of fun and competition into learning can make it more engaging and enjoyable, leading to improved outcomes (Alomair & Hammami, 2020; Scholefield and Shepherd 2019). In today’s world, where cybercrime is on the rise, it is essential to educate and prepare consumers to face cyber threats.

Additionally, gamification can be utilised for consumer training, as demonstrated by Nippon Telegraph and Telephone Corporation (NTT) Data's "Ignite Leadership Game" (Burke, 2021).The design rooted in gaming principles serves to assess the knowledge

of employees and streamlines the cultivation of essential skills. Lampropoulos et al. (2023) explored how the fusion of gamification with augmented reality can enhance disciplines like advertising and marketing campaigns which can invigorate workplace incentive methods. Gamification will undoubtedly play a larger role in education and training, as technology continues to advance. Moreover, it is a highly effective method for enhancing learning by incorporating competitive and enjoyable elements into a learning platform thereby making it more enjoyable and fostering the desire to learn.

Numerous research efforts, such as those by Friedrich et al. (2017), Scholefield and Shepherd (2019), and Deeleman and Van Steen (2021), have investigated the effects of gamification integration. These studies collectively indicate that, with proper execution, gamification can successfully meet its intended objectives. Capture The Flag (CTF) is a game-based learning tool that has proven valuable for fostering cybersecurity awareness, a necessity in today's society. Zennaro and Erdődi (2023) have expanded on the idea that CTF fosters an engaging learning environment. By weaving gamification elements into educational frameworks, CTF enhances participant involvement and facilitates the acquisition of essential skills for cybersecurity defense.

Incorporating gamification goes beyond bolstering user interaction; it plays a crucial role in enhancing participant competencies. According to Burke (2019) analysis underscores the effectiveness of gamification in workforce education, exemplified by NTT Data’s "Ignite Leadership Game." This innovative game assesses the knowledge base of employees to identify their potential and areas for improvement, facilitating targeted skill development. Gamification strategies in skill development foster an engaging work atmosphere, tackle problems, boost employees' drive for superior performance, and enhance the educational experience through cooperative settings (Mitchell et al., 2020). Furthermore, Martínez-Jiménez et al. (2021) highlights the importance of blending augmented reality with gamification techniques, showing its multifaceted objectives.

## 2.5 Existing Gamification Training Solutions

As technological development and its dependence on digital platforms have increased, the risk of cyberattacks has also intensified (Salahdine & Kaabouch, 2019). For this purpose, numerous cybersecurity training and awareness initiatives have adopted gamification techniques to improve consumer skills, knowledge, and preparedness ( Barreto & França, 2021). These programmes involve teaching the consumer how to identify security weaknesses and provide a fundamental comprehension of how to recognise and deflect malicious cyber penetrations (**awareness**).

The following are the most employed cybersecurity training and awareness strategies, according to Huang and Zhu (2020):

- **Defensive strategies require** necessitate a deep understanding among defenders, equipping them with the critical tools and methods required for an effective cyber defense
- **Offensive strategies** position consumers in the role of adversaries to gain insight into their tactics and mindset

- **Attacker centricity** involves leveraging the identified characteristics of cyber attackers and training consumers to anticipate the intentions and actions of adversaries during the specific cyber incursions. Such foresight is vital in aiding the development as well as the implementation of the attack which includes the defensive strategies in combating cybercrime.

Employing gamification for educational purposes equips participants with hands-on knowledge and skills to address real-life cyber challenges in an innovative and captivating way. With the progression of technology and the dynamic nature of cyber threats, the incorporation of gamification in cyber defense education is expected to become more prevalent, as proposed by (Deeleman & Van Steen, 2021).

## 2.6 Successful implementation of gamification

Numerous countries and sectors such as education, healthcare, and marketing have seen successful adoption of gamification practices (Alomair & Hammami, 2020; Kalogiannakis et al., 2021; Ofosu-Ampong, 2020). Shah and Agarwal (2020) and

Burke (2021) further highlighted several advantages of gamification which included the enhancement of engagement and motivation, intrinsic motivations such as accomplishment, competition, and social interaction as the key drivers. Gamification can promote learning by providing a safe and simulated environment for consumers to practice and experiment and facilitate behaviour change by encouraging the adoption of new habits and reinforcing positive ones (Martínez-Jiménez et al., 2021). Furthermore, it can increase the effectiveness of feedback by providing immediate and personalised responses to consumers. These benefits make gamification a promising tool for promoting behaviour modification, enhancing learning outcomes, and enhancing engagement, with some instances listed below in which gamification has been successfully implemented in other nations.

The fitness app "Keep" has garnered significant attention in China with a monthly active user count of 13.54 million (Thomala, 2023). This application incorporates game-like features, including points, badges, and elements of social competition to incentivise consistent physical exercise among its users. A study by Mazeas et al. (2022) found that the use of these gamified elements notably improved not only the regularity and length of workouts but also the user’s overall enjoyment of the physical activities.

The city of Helsinki in Finland has used gamification to encourage sustainable transportation practices among residents. The "CitiCAP" initiative rewards users for choosing eco-friendly transport options like cycling, walking, or utilising public transportation by allowing them to accumulate points and receive incentives. Research carried out by Yen et al. (2019) concluded that gamification significantly boosts the frequency of participant engagement in sustainable travel behaviours.

In **Australia**, the Commonwealth Bank of Australia has implemented gamification to improve the financial literacy and engagement of its consumers. The "Dollarmites" program uses gamification elements, such as badges and rewards to encourage juvenile customers to develop healthy financial habits and save money. Mistry (2020) found that the programme substantially increased children's financial knowledge and interest.

The "EcoAgents" program in **Brazil** teaches children and their families regarding environmental sustainability using video games. The program, developed by the Brazilian government and implemented in schools across the country, uses gamification elements such as challenges, badges, and rewards, as encouragement for participants to adopt sustainable behaviours such as recycling, reducing energy consumption, and water conservation. Brandão and Costa (2021) found that gamification significantly increased participant knowledge and the adoption of sustainable behaviours.

Gamification can foster a sense of self-efficacy and empowerment in consumers enabling them to exercise greater control over their online safety and security. In the long run, it can equip them with the necessary expertise and abilities to practice safe online practices (Welbers, et al., 2019).

## 2.7 Shortcomings of using gamification to educate consumers on cybercrime

Although gamification may have benefits and does not conform to traditional educational methods, it is important to highlight some of its drawbacks because they impact the study objectives. When consumers are not invested in the designer's goals, the game's player experiences are poorly developed, and the message is ineffective. The possibility of not creating captivating player experiences is an inherent hazard to the development of serious games (Almeida et al., 2023).

Ferrara (2013) and Chung (2017) dismisses gamification as an effective strategy for educating the public, with quite a scathing critique. The author suggests there is no exact meaning for the term "gamification," as it is widely used for a variety of activities, ranging from the online game “Farmville” to the profile completion bar in LinkedIn. Gamification is therefore described as a useless term because it cannot distinguish between meaningfully dissimilar things. Depending on the speaker, the term "gamification" may refer to the extreme ends of a spectrum, which serves to institutionalise the fallacy that games can be stripped of their "useful" components, while ignoring the remainder of what constitutes a game (Almeida et al., 2023). Ferrara (2013) further argues that game elements, touted as magical in their efficacy, can

supposedly be grafted onto things that are not games, causing people to react similarly to how they react to video games.

The greatest flaw of gamification is its failure to recognise games are significantly more than mere rewards. While acknowledging rewards, such as the awarding of points, leader boards, and badges, can be beneficial, Ferrara (2013) argues that these are only a small portion of the player experience, residing solely on the motivational plane. When using gamification for cybercrime education, ethical considerations must also be considered (Kim and Werbach, 2016).

Rapp et al. (2019) discussed the potential for gamification to reinforce stereotypes and biases, as well as the need to consider the potential for gamification to have unintended consequences, such as encouraging risky behaviour or promoting a culture of competition, as opposed to collaboration. Additionally, it is essential to consider the privacy implications of gamified approaches, particularly in terms of personal information collection and use.

## 2.8 Gamification for educating about cybercrime in other contexts

Studies across various settings have explored gamification as a viable tool for cybercrime education (Barreto & França, 2021; Yen et al., 2019; Schmidt-Kraepelin et al., 2019). For instance, Ali (2019) found that gamification boosts engagement and motivation among students studying cybersecurity ultimately leading to better knowledge retention and application. Likewise, Hart et al. (2020) illustrated how a cybersecurity game could promote better awareness and behaviours amongst employees. Alqahtani and Kavakli-Thorne (2020) further observed that gamified approaches enhance cybercrime knowledge and security practices more effectively than traditional training. Participants in gamified learning showed a higher level of cybersecurity knowledge and better practices. In agreement with Hatzivasilis et al. (2020), the study confirmed that gamified cybersecurity training programs significantly improve awareness among employees in large organisations.

To further support the existing studies, Gjertsen (2016) found that while a gamified cybersecurity training program improved user knowledge and confidence in detecting cyber threats, it did not necessarily result in improved behaviour.

In a separate study, conducted by Deeleman and Van Steen (2021) it was determined a gamified cybersecurity education program had no effect on participant intent to adopt secure behaviour. Almeida et al. (2023) revealed that traditional training methods outperformed the training program in question when it came to improving participants' understanding and application of cybersecurity when they investigated the application of gamification in education software. As suggested by the authors the complexity of the gamification design may have contributed to participant confusion and disinterest. These contradictory findings suggest that the efficacy of gamification in cybercrime education may depend on several variables including game design, intended audience and the context in which it is used (Thompson et al., 2022). When designing and implementing gamification for cybercrime education it is important to carefully consider the aforementioned factors.

## 2.9 Research gaps

Cybersecurity awareness and preparedness are more important than ever because of the growing frequency and complexity of cyberthreats. Researchers have identified several gaps in current cybersecurity training and awareness programmes, including the need to extend training to banking industry clients, the efficacy of gamification in promoting cybersecurity awareness, and factors influencing gamification efficacy. As shown in Table 2.1, it is essential to comprehend these research gaps if we are to develop effective strategies to combat cyberthreats.

**Table 2.1: Identified research gaps**

| Author name and year | Conceptual discussion | Research gap | Research question |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Loewen et al., (2019) | The study aimed to evaluate nine Turkish-learning students on Duolingo for a semester, their language skills and the relationship between app use and improvement. It also sought participants' opinions on their experiences with the app. It also aimed to address research gaps by examining widely used language apps like Duolingo for second language acquisition. | The research underscores the lack of independent studies assessing the efficacy of mobile-assisted language learning platforms, notably with respect to widely used commercial apps for second language acquisition like Duolingo. | To investigate the effectiveness of Duolingo for second language (L2) acquisition. |

| | | | |
|---|---|---|---|
| Salahdine and Kaabouch (2019) | The paper discusses the diverse social engineering strategies including but not limited to baiting, phishing, pretexting and quid pro quo, and explores the strategies for detecting and averting such attacks. It also highlights the limitations of existing social engineering detection methods and its countermeasures for such attacks. | The lack of effective strategies to cope with the ever-growing number of social engineering attacks. | The study focused on the following research questions:<br>-What are social engineering attacks & how can they be classified?<br>-What current detection strategies exist for social engineering attacks?<br>-What are the limitations of the current detection methods and countermeasures for social engineering attacks?<br>- Which measures should be implemented to safeguard against social engineering attacks? |

| | | | |
|---|---|---|---|
| Zimmermann and Renaud (2019) | The way cybersecurity is currently conceptualised and the need for a mindset change | There is no explicit mention of a research gap in the paper, however, the paper proposes a new mindset called "Cybersecurity, differently", acknowledging the constructive role humans can play as "part of the solution" rather than "the problem" in organisational cybersecurity. | What constitutes the core challenges in cybersecurity and how does the prevalent mindset affect personal reactions to cybersecurity issues? |

| | | | |
|---|---|---|---|
| Scholefield and Shepherd (2019) | The implementation of gamification strategies aimed to enhance user awareness of password security and boost overall security consciousness while simultaneously incorporating diligent planning and feedback to guarantee the effectiveness of these techniques in an educational setting. | - No assessment was performed regarding the long-term retention of knowledge about password security and only a limited sample size was utilised.<br>-Gender differences were not investigated; demographic participant questionnaire was not factored. Prior research indicates that males generally favour game-based learning over females. This implies that the application of password security may need to be adapted to increase its appeal to a broader audience. | What is the efficacy of using gamification approaches in enhancing password security behaviours among everyday users to boost their cybersecurity awareness? |
| Deeleman and Van Steen (2021) | Whether video game, designed based on prior research and expert advice, can improve participant performance on the Theory of Planned Behaviour (TPB) components? | Investigation into the effectiveness of gaming on different target groups to address cybersecurity. | Does the Theory of Planned Behaviour model, which includes personal attitudes, subjective norms, and behavioural intentions, apply to understanding how gamification influences cybersecurity behaviour? |

| | | | |
|---|---|---|---|
| Scholefield and Shepherd (2019); Thompson et al., (2022) | The paper discusses the RAD-SIM framework, which integrates behavioural and psychological principles as well as learning theories to enhance game-based cybersecurity education. | Evaluate the effectiveness of gamified approaches versus traditional methods in improving educational results across different fields. | What are the most effective methods for leveraging gamification to train individuals in recognising and mitigating socially engineered cyber threats? |
| Scholefield and Shepherd (2019); Rieb et al., (2017) | Factors influencing gamification in promoting cybersecurity awareness. | | What are the factors influencing gamification effectiveness in promoting awareness among consumers of cybersecurity and the prevention of cybercrime? |

*Source: Research gaps (Author's compilation)*

Cybersecurity is a discipline comprised of numerous interconnected elements (Pacheco et al., 2020). In order to effectively address the security challenges posed by cyber threats, research needs to be conducted from a comprehensive and interdisciplinary perspective. This should encompass a thorough examination of its many aspects such as the technological risks and defences, economic and societal consequences, current solutions, and tactics & the potential that gamification has to enhance the effectiveness of education and training efforts in cybersecurity. By conducting sufficient research on these topics, a deeper understanding of the challenges posed by cyber threats can be developed, more effective training and awareness programs can be created, and ultimately, the impact of cybercrime on society can be reduced. Creating a strong cybersecurity education and awareness initiatives is crucial as it equips consumers to deal with the ever-changing threats in the digital space underscoring the importance of bridging the gaps in current research.

Cybercrime represents an expanding and pervasive hazard to South African society (Kshetri 2019). To effectively combat this problem, all stakeholders such as the public sector, academia, government, and more must improve their collaboration to increase cybersecurity awareness and investment.

## 2.10 Theoretical Frameworks

The surge in technological advancements has undeniably provided numerous benefits, such as enhanced communication, improved availability of information, and broadened opportunities for conducting banking online. However, as noted by Bokang and Mapimele (2019), South Africa has experienced a rise in cybercrime incidents in recent times, attributed to the country's position as a significant financial and technological centre in Africa. This underscores the need for consumers to be technologically literate. Nonetheless, few studies have assessed the cybersecurity or cybercrime awareness literacy levels of consumers in South Africa (Dlamini & Mbambo, 2019). This present study interrogates a few theoretical frameworks or models to answer the research questions. Among the potential theories, Self-Determination Theory (SDT) and behavioural science have been identified as the most relevant frameworks within which to investigate the problem of enhancing user motivation to adopt safe cybersecurity practices.

### 2.10.1 Self-determination Theory (SDT)

The Self-Determination Theory (SDT) is particularly appropriate for this study as it provides a comprehensive framework for understanding the human motivation and personality. SDT highlights the critical roles of autonomy, competence, and relatedness in fostering intrinsic motivation (Kam & Umar, 2018). As explained by Mitchell et al. (2020), autonomy refers to the extent to which an individual perceives they have control over their actions and the results of those actions. Competence refers to a person’s belief in their own capability to successfully complete tasks, which can be fostered by gamification features that offer a blend of challenge that is neither too easy nor too difficult to achieve (Kim et al., 2018). Relatedness represents an individual’s need to connect with others and can be fostered through gamification

features that encourage communication, collaboration, and comparison, such as multiplayer and teamwork options (Featherstone & Habgood, 2019). When these requirements are satisfied, consumers tend to be more inclined to participate in activities that contribute to their personal growth, educational advancement, and self-improvement. These elements are crucial in designing gamified educational interventions that can effectively engage users and encourage sustained behaviour change in cybersecurity practices. Traditional gamification approaches often fail to consider different consumer needs such as their capabilities and preferences, leading to unpredictable results (Tobon et al., 2020). Adaptive gamification, rooted in SDT, offers a more personalised approach by considering these individual differences (Alqahtani & Kavakli-Thorne, 2020). This theory helps to understand how gamification can promote consumer behaviour change, retention of cybercrime best practices, knowledge, and learning (Zwilling et al., 2022).

While other theories such as the Theory of Planned Behaviour (TPB) or the Technology Acceptance Model (TAM) provide insights into user intentions and technology acceptance, they lack the depth in addressing intrinsic motivation (Cheng, 2019). TPB focuses on intention and perceived behavioural control but does not delve into the intrinsic motivational aspects that SDT covers. TAM is useful for understanding acceptance and usage of technology but does not provide a framework for sustained engagement and intrinsic motivation.

Studies have shown that incorporating SDT into educational game design significantly enhances user engagement and learning outcomes (Kim et al., 2018). SDT's focus on autonomy, competence, and relatedness aligns well with the goals of cybersecurity education, making it a robust framework for this study.

The gamification framework consists of a collection of building elements designed to create an engaging gamified environment (Yamani, 2021). Effectively integrating these building blocks is essential for a seamless and engaging experience, accomplished by using various game elements (Zichermann & Linder, 2021). However, earlier models of gamification, like the frameworks put forth by Dignan (2011), have been criticised for omitting intrinsic motivational items such as relatedness, autonomy, and competence (Morschheuser et al., 2018), which, according to SDT, are essential for engagement. Incorporating intrinsic motivators is

crucial for avoiding the negative effects of extrinsic rewards, which can demotivate participants when intrinsic motivators are already present (Manzano-León et al., 2021).

Mora et al. (2017) emphasise that the gamification framework created by Werbach (2012), which is the most referenced and widely used, extends the model proposed by Dignan (2011) by incorporating intrinsic motivators, persuasive technologies, and design-thinking methodologies to devise a comprehensive and engaging approach to gamification. Unlike the approach taken by Bockle et al. (2018), current models do not explicitly utilise game elements to steer the design of gamification systems in a way that strategically influences long-term impact. As a result, many gamification initiatives have lacked a formal design process, leading to a plethora of disorganised experiences and game elements (Mora et al., 2017). Warmelink et al. (2020) conducted an extensive analysis of the current literature on gamification, highlighting deficiencies such as the lack of detailed design frameworks that clarify the selection of game elements and motivational affordances. The researchers also pointed out the lack of clarity in the current models and noted that the limited application of game elements fails to effectively address long-term strategic effects, despite attempts to establish a robust design structure (Azouz & Lefdaoui, 2018).

The solution may be found in adaptive gamification, a promising approach to improve traditional gamification by transforming it into user-centred and personalised experiences. SDT and the Gamification User Types Hexad framework, developed by Tondello et al. (2018), are considered useful tools to help designers achieve this goal. By applying these tools, this study can individualise gamification concepts that consider the specific characteristics and needs of users and contexts, promote engagement, and encourage users to behave in the intended way.

For the research goal to be met, it is necessary to assess the consumer's attributes and demands, enabling the customisation of gamification techniques that foster involvement and stimulate the targeted behaviour (Kim et al., 2018). When gamification elements are designed to meet psychological needs, such as receiving feedback, challenges, and experiencing social interaction, they have the potential to heighten consumer engagement and incentivise motivation within cybercrime education.

### 2.10.2 The concept of behavioural science

Behavioural science examines human behaviour and decision-making by drawing on insights from psychology, sociology, economics, and neuroscience (Privitera, 2020). This interdisciplinary approach is essential for designing effective gamification strategies that can influence consumer behaviour in cybersecurity education.

Behavioural science offers a broad understanding of how people make decisions and how these decisions can be influenced. This is particularly relevant in cybersecurity education, where changing user behaviour is a key objective. By applying principles from behavioural science, such as clear feedback, rewards, and social norms, designers can create more effective and engaging gamified experiences (Burke, 2021)

Unlike cognitive theories that focus primarily on mental processes (Schunk & DiBenedetto, 2020), behavioural science provides a more comprehensive view by incorporating social and environmental factors. This makes it more suitable for designing interventions that require behaviour change in a complex and dynamic field like cybersecurity.

Research has demonstrated the effectiveness of behavioural science in various fields, including education and health, for promoting behaviour change (Salah & Alzaghal, 2022). Its principles are highly applicable to the gamification of cybercrime education, providing a solid foundation for developing strategies that can effectively change user behaviour.

Behavioural science examines human behaviours and decision-making by drawing on insights from psychology, sociology, economics, and neuroscience to comprehend and shape behaviours (Privitera, 2020). This research, through a review of existing literature seeks to refine the design and implementation of gamification strategies aimed at achieving educational objectives while closely considering behavioural change principles (Burke, 2021). However, behavioural science-based interventions may impact consumer actions but often do not comprehensively address systemic problems like poverty or entrenched inequality that shape those behaviours (Deeleman & Van Steen, 2021). Moreover, behavioural science might not adequately account for the role that emotions play in behaviour, nor address the emotional and affective issues that contribute to behaviours (Privitera, 2020).

The concepts of behavioural science and Self-Determination Theory (SDT) provides a valuable framework for understanding and influencing human behaviour. These principles can be used to design gamification interventions where designers can create engaging, motivating, and behaviourally effective experiences (Zwilling et al., 2022). For example, by providing clear feedback and rewards using social norms to encourage desirable behaviours, and tailoring interventions to individual preferences, designers can optimise the effectiveness of gamification interventions for educating consumers about cybercrime (Alqahtani et al., 2020).

### 2.10.3 Conceptual framework

The conceptual framework (Fig. 2.1) aims to determine the effectiveness of gamification as a communication tool to change consumer behaviours towards cybercrime in South Africa. This framework integrates elements of behavioural science, self-determination theory, education, and gamification interventions to achieve this goal and is aligned with the research questions, hypotheses, and sub-problems identified in the literature.

**Behavioural science** provides the foundation for understanding human behaviours and decision-making processes. This study leverages principles from behavioural science to uncover the psychological mechanisms that drive consumer behaviour. By understanding how consumers process information, make decisions, and alter their behaviour, the study aims to design effective educational interventions that can influence behaviour change.

**Self-determination theory** (SDT) is employed to focus on the internal sources of motivation that drive behaviours. According to Mitchell et al. (2020), SDT enhances engagement and retention of educational content through intrinsic motivation. In this context, SDT supports the educational content by enhancing participants' knowledge and shaping their attitudes towards cybercrime. This theory is linked to education, which ultimately leads to improved knowledge and attitudes. Education is a critical component of the conceptual framework and is interlinked with self-determination theory. The educational content aims to increase consumers' knowledge and improve their attitudes towards cybercrime, addressing the following sub-problems:

- Increased knowledge providing comprehensive information on various cyber threats and safe online practices to equip consumers with the necessary understanding
- Shaping attitudes to encourage a proactive and positive attitude towards cybersecurity to make consumers more vigilant and responsible online

The **gamification interventions** in this study include challenges and interactive content designed to educate consumers about cybercrime. These interventions aim to engage and motivate participants by:

- Presenting tasks and scenarios in the form of challenges that require applying knowledge of cybercrime, thereby reinforcing learning through problem-solving
- Using interactive content such as simulations, quizzes, and other interactive elements to keep participants engaged and involved in the learning process, making the educational experience more dynamic and enjoyable

The goal of the study is to achieve **behaviour change** among, South African consumers by enhancing their knowledge and shaping their attitudes through engaging and motivating gamification interventions, the study aims to foster a proactive approach to cybercrime education (Burke, 2021). This involves evaluating how well gamification works as a tool when it comes to communicating important cybercrime information and influencing consumer behaviour. This aligns with the primary research question of assessing the overall effectiveness of gamification in educating consumers about cybercrime. The study also addresses secondary research questions by comparing knowledge and attitudes between those who have and have not participated in the gamified educational interventions.

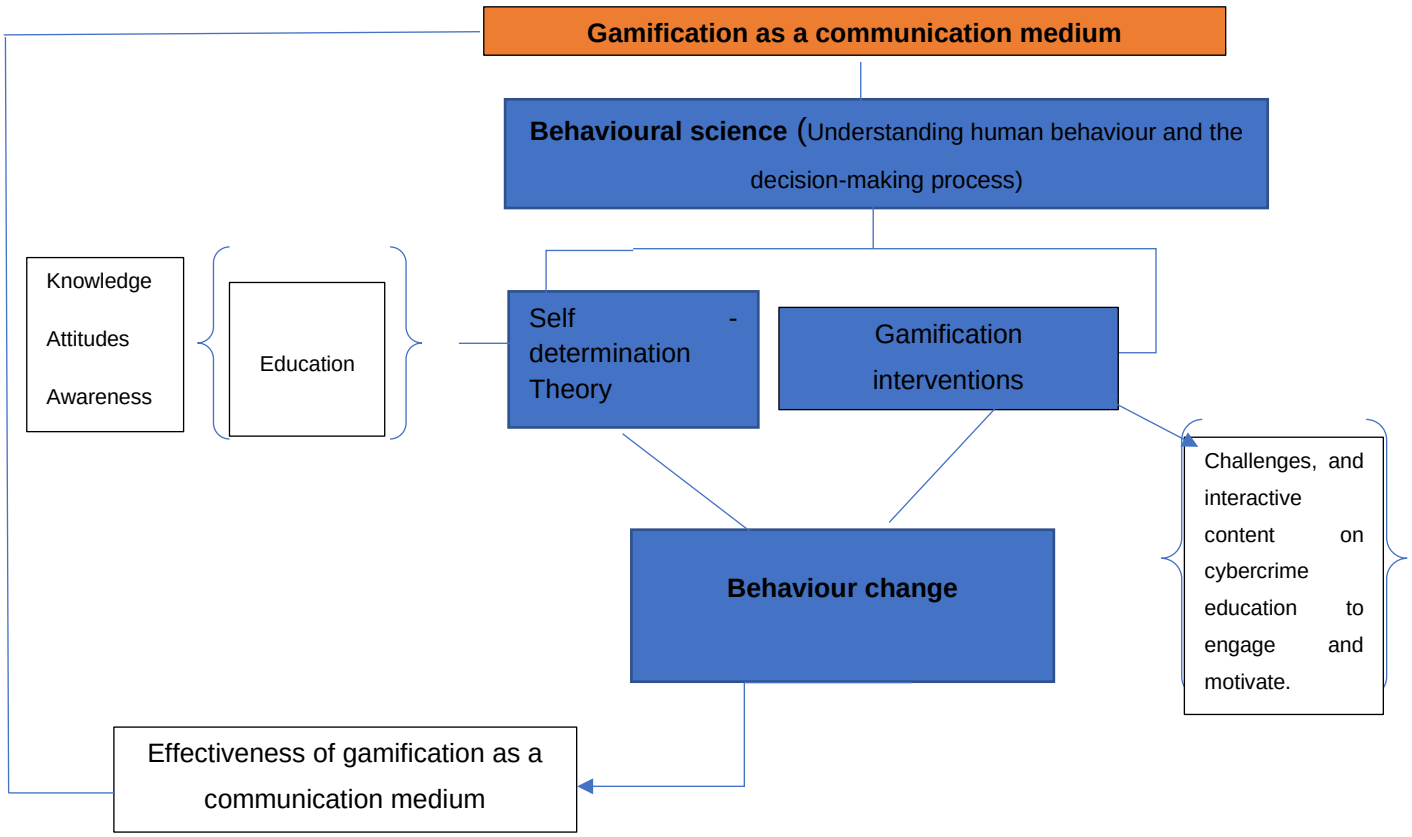



**Figure 2.1: Proposed conceptual framework of *determining the effectiveness of gamification in boosting knowledge, shifting attitudes, and adjusting behaviours* (*Author's compilation)***

SDT and behavioural science offer thorough insights into human behaviour, aiding the research in investigating ways to cultivate a feeling of ownership and involvement in the learning journey. Morschheuser et al. (2018) further emphasised that this may consequently improve the likelihood of retaining knowledge and achieving behaviour modification.

**Table 2.2: Relationship between constructs**

| Construct | Interpretation | Measure | References |
|---|---|---|---|
| Autonomy | The extent to which consumers feel they possess autonomy and influence within their learning experience facilitated by gamified elements. | Duration of the user engagement on the game, average test scores of users, number of users who reported improving their knowledge or skill and number of users who felt | Cheong and Park (2020 |

| | | | |
|---|---|---|---|
| | | motivated, a percentage of users who were able to complete and answer questions correctly | |
| Competence | The level at which consumers believe they are equipped with the appropriate knowledge and skills to interact with the gamified content on cybercrime education | Ability to identify and respond to cybersecurity threats, the consumer's success in completing the gamified content, knowledge retention. | Kankanhalli et al., (2020) |
| Relatedness | The degree to which consumers perceive they related to others and are receiving support and feedback through the gamified cybercrime education content | How well is the user retaining the information, how enjoyable was the game, and how relevant is the content? | Sailer and Sailer (2020) |
| Perceived usefulness | The degree to which consumers perceive that the gamified cybercrime education content is useful in improving their knowledge and awareness of cybercrime. | Knowledge & awareness (pre- and post-game testing), engagement (number of participants in and duration of the game), how useful are the gamified content and customer feedback? | Oluwajana et al., (2019) |
| Behavioural intention | The degree to which consumers intend to engage in safe cybersecurity behaviours due to participation in gamified cybercrime education. | Perception of cybercrime, adoption of cybersecurity prevention measures, level of trust in online digital banking platforms. | Kimpe et al., (2021) |

The following hypotheses or propositions were generated from these relationships (Table 2.2):

**H1: Consumers' knowledge of cybercrime improves after they play games designed to improve such knowledge.**

**H2: Consumers' attitude towards cybercrime improves after playing a game meant to educate them about cybercrime.**

By integrating behavioural science, self-determination theory, and gamification interventions, this conceptual model specifically addresses the unique context of educating South African consumers about cybercrime. It combines these elements to create engaging, motivating, and effective educational interventions that improve knowledge, attitudes, and ultimately lead to behaviour change. This model not only evaluates the effectiveness of gamification as a communication medium but also provides a comprehensive framework to develop broader educational strategies to combat cybercrime.

The present chapter emphasises the importance of using theoretical frameworks when designing gamification elements for cybercrime education (Kam and Umar, 2018). It allows for a comprehensive analysis of the underlying mechanisms and processes, through which gamification can achieve the objectives highlighted in the study, while also considering the motivational factors, social dynamics, and behavioural change techniques.

The literature offers a broadened perspective on gamification and its relevance to consumer behaviour in cybercrime and security, illuminating how gamification can serve as an educational tool for the prevention of cybercrime (Hart, Beale, & Carmichael, 2020). This chapter presents the hypotheses along with the theoretical and conceptual underpinnings that guide the research. This study contributes to Self-Determination Theory (SDT) by empirically demonstrating how the integration of autonomy, competence, and relatedness within gamified educational interventions can enhance intrinsic motivation among consumers. Specifically, the research provides evidence that gamification elements designed to foster these three psychological needs which leads to improved engagement, knowledge retention, and positive attitudes towards cybersecurity practices. This aligns with SDT's assertion that intrinsic motivation is crucial for sustained behavioural change and deep learning

(Mitchell, Petherick, & Ziegler, 2020). Additionally, the study advances the application of behavioural science in educational contexts by showing how principles such as immediate feedback, social norms, and interactive content can effectively influence consumer behaviour towards safer online practices (Alqahtani & Kavakli-Thorne, 2020; Burke, 2021). By combining SDT and behavioural science, the research presents a comprehensive framework for understanding and enhancing the effectiveness of gamification in cybersecurity education. This dual-theoretical approach not only validates the constructs of SDT in a new context but also enriches behavioural science by highlighting practical strategies for behaviour changes in the digital environments. Subsequently, the following chapter will detail the research methodology utilised in this study and describe the techniques used for analysing the data collected.

## 2.11 Chapter conclusion

The literature offers a broadened perspective on gamification and its relevance to consumer play in cybercrime and security, illuminating how gamification can serve as educational tool for the prevention of cybercrime (Hart et al., 2020). The chapter further presents the hypotheses along with theoretical and conceptual underpinnings that guide the research. Subsequently, the following chapter will detail the research methodology utilised in this study and describe the techniques used for analysing the data gathered.

# Chapter 3: Research Methodology

## 3.1 Introduction

In this chapter a detailed research methodology is presented which correlates directly with the research questions and objectives, as well as building on the critical analysis of literature from the preceding chapter. This section is important as it illuminates the strategic underpinnings of the study which includes the design and scope which involves the population, sampling methods, as well as the techniques for data collection and analysis. Ethical considerations are also addressed ensuring a high standard of research integrity. Additionally, the logistical aspects of data management will be discussed along with a description of the anticipated role of statistical analysis and other analytical frameworks in interpreting the research outcomes.

## 3.2 Research approach

The primary goal of this study was to assess the effectiveness of gamification in enhancing consumer knowledge and attitudes towards cybercrime in South Africa. A quantitative research method was used for its advantage in allowing findings to be generalisable to a broader audience. The approach was grounded in an empiricist paradigm, emphasising that knowledge primarily comes from observable experience.

Consistent with the works of scholars such as (Sileyew, 2019) the research commenced with a clear problem statement and hypothesis creation. The methodology involved administering surveys to gather data from a wide-ranging consumer base which enables a comprehensive analysis of patterns and relationships between variables. This method is well suited for confirming hypotheses and establishing factual relationships in a study. Quantitative research offers the benefit of drawing objective and meaningful conclusions that can be relevant for future predictive or explanatory studies.

## 3.3 Research Design and Philosophy

In scientific research inquiry, according to Sileyew (2019) the research design is defined as the underlying research philosophy that informs the methodological framework and procedures which offer the baseline of the knowledge development process. The research design serves two primary functions which involves identifying and developing the necessary procedures and logistical arrangements for a study. It also highlights the critical need to uphold the integrity of these methods to ensure precision, impartiality, and authenticity (Kumar, 2018).

An online questionnaire (survey) incorporating both open-ended and multiple-choice items was utilized to gather information from a targeted group of consumers in South Africa. Surveys are a helpful tool for gauging opinions, attitudes, and perceptions (Krosnick, Judd, & Wittenbrink, 2018). Participants had the opportunity to complete this during their own time, using a computer or any form of electronic device allowing the researcher to access several individuals whereby a face-to-face interview might have been difficult to access or reach, saving on costs and time.

On the one hand, the benefits of adopting a survey format for this research includes the potential to garnering more specific and all-encompassing feedback as open-ended questions enable respondents to provide in-depth accounts of their experiences and perspectives (Krosnick 2018; Casula et al., 2021). Furthermore, open-ended questions can also allow for unexpected results and useful for exploratory research in generating hypotheses and ideas for future research (Casula et al., 2021). Conversely, the drawbacks of employing a survey design could consist of the challenges in interpreting responses to open-ended questions, which can differ greatly in substance and extent, and the possibility of receiving responses that are either incomplete or lacking in clarity (Nayak and Narayan, 2019).

This research design was chosen for its potential to provide detailed and elaborate responses, allowing for the possibility of unexpected findings, and being useful for exploratory research (Casula et al., 2021). However, there are some disadvantages to this approach, such as the complexity of analysing open-ended questions and the potential for incomplete or vague responses.

This research approach was selected for its ability to generate rich, descriptive data and foster the emergence of unforeseen insights, a characteristic pertinent to exploratory research.

The process of assessing the effectiveness of gamification on consumer knowledge and attitudes towards cybercrime, as detailed by the researcher, is illustrated below (Fig 3.1).

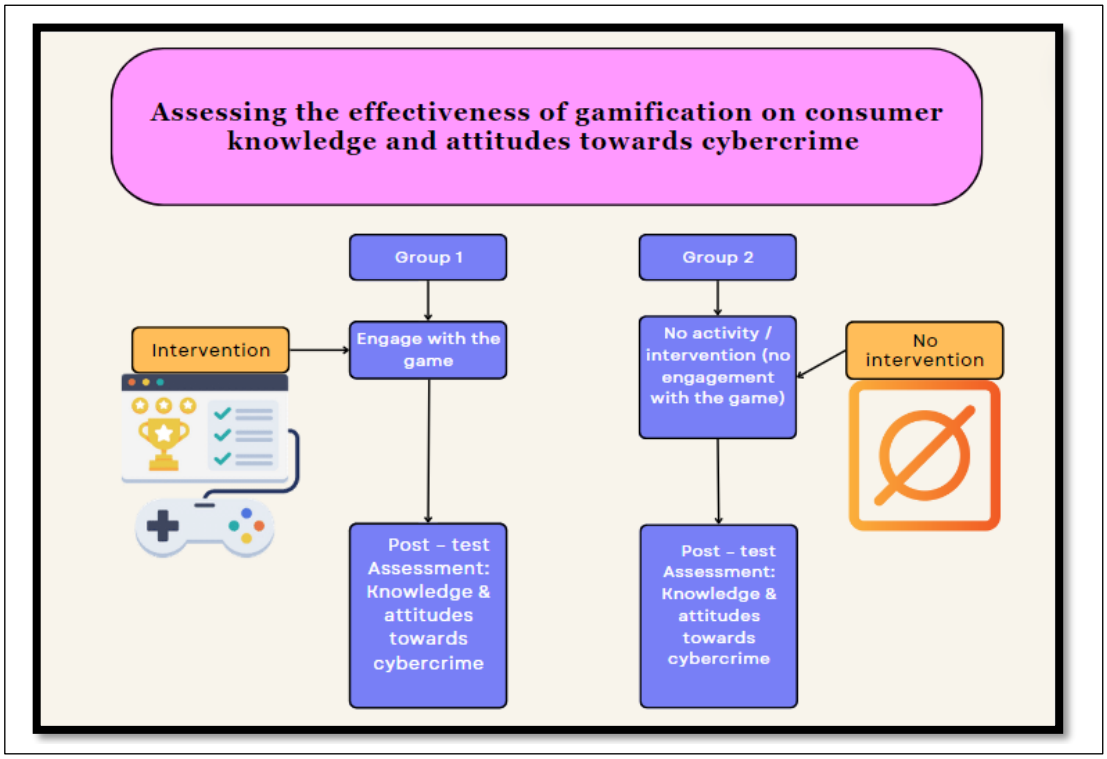



**Figure 3.1: Targeted groups to test the effectiveness of gamification (*Author's compilation)***

## 3.4 Data collection

Figure 3.1 shows that the study embarked on an investigative approach to examine how gamification influences consumer understanding and viewpoints on cybercrime. This was done to gain a full grasp of how gamification serves as a tool for educating South African consumers about cybercrime.

Primary data was gathered using a survey comprising both open ended and closed questions. The data collection was a vital step in achieving the research aim to answer

the research question. In order to acquire relevant data, careful consideration was provided to the selection of the information gathering process method for this research.

Dörnyei and Dewaele (2022) suggest a questionnaire is a useful means of obtaining a large amount of data for quantitative research, which is necessary for the present study. Furthermore, Nayak & Narayan (2019) claims questionnaires are advantageous for data accuracy, as the information is already set out in a spreadsheet, leaving less room for mistakes. Other benefits of this data collection method include cost-efficiency, the ability to reach people quickly, scalability and the anonymity of the respondent (Mazikana et al., 2023).

## 3.5 Population and Sample

Following a series of studies, the population for this study is constituted by the aggregate of the research respondents that the scientific enquiry seeks to cover aiming to facilitate the progression of knowledge (Saunders et al., 2019). In the context of this study the population relates to consumers comprising of banked persons in in SA. The focus is on retail banking customers, these are customers with a valid bank account at any bank in SA, who engage in banking activities, and primarily use digital banking platforms such as internet, mobile banking, and ATM services.

The selected population includes individuals who are 18 years old and beyond. This group was targeted, because members are more likely to be active users of the banking digital platforms, have a part- or full-time job, or run their own businesses. These individuals are directly impacted by cybercrime risks and can benefit from the intervention, as they are active participants in the South African economy and represent a significant portion of the workforce, which makes them susceptible to cybercrime due to their financial commitments and digital engagement. According to Aluwani (2020), the value of ecommerce transactions is expected to reach R225bn by the year 2025, with these numbers attributed to the working class and small businesses, and the change in consumer behaviour.

The group examined in this research plays a role in the rise of e-commerce engagement (Thenga, 2020). Some participants should, therefore, have experience in playing games in order to educate themselves regarding cybercrime. This would

facilitate data collection on the role and impact of gamification to educate consumers regarding cybercrime in SA.

### 3.5.1 Inclusion and exclusion criteria

According to Saunders (2012), inclusion and exclusion criteria dictate who can participate in the study. On the one hand, inclusion thus refers to the relevant participant attributes that allow study participation. This includes aspects such as knowledge of the research topic and whether they have been involved or are experienced in the area of study. Exclusion criteria, on the other hand, denote those matters that disallow someone from participating, such as not being knowledgeable on the study topic.

Eligibility for the study was restricted to individuals over 18 years with an active South African bank account and some level of awareness and education about cybercrime, particularly regarding gamification. Participants were required to have the ability to read and comprehend English and possess access to a smartphone or laptop.

## 3.6 Sample size and sampling method

The participants were divided into two categories, one group consisted of individuals who had played an educational game designed to create knowledge and awareness of cybercrime, and the other group included individuals who had never played such a game. This division aimed to test and compare each group's knowledge and attitudes towards cybercrime, thus addressing the main question of the effectiveness of gamification. The goal was to determine whether gamification influenced the participants' knowledge and attitudes towards cybercrime.

A minimum of 250 participants was targeted based on the researcher's social media reach. Using various social media channels, such as Facebook, Instagram, and LinkedIn, the researcher invited individuals to join the study by distributing a consent letter explaining the research goals. Quantitative data was collected using a secure online questionnaire designed with Qualtrics, a specialised experience management application. The survey included structured questions covering demographics, cybercrime knowledge, attitudes towards cybersecurity, and preferences for gamified

learning. It was designed to gather information on participants' cybercrime knowledge and awareness, experience and engagement with gamified education, and their attitudes and preferences towards gamification as an educational tool.

Selecting an appropriate sample size is essential for ensuring the validity and reliability of research findings. For this study, a sample size of 248 respondents was determined based on statistical principles and practical considerations. Given the vast population of South Africa, surveying the entire population is impractical. Instead, a representative sample of 248 respondents provides a statistically significant and manageable sample size. The chosen sample size was calculated to achieve a 95% confidence level with a margin of error of approximately 6%, assuming a population proportion of 50%. This margin of error is acceptable in social science research and ensures that the results are statistically reliable and can be generalised to the broader South African consumer population (Lakens, 2022).

A power analysis determined the minimum sample size required to detect a significant effect of gamification on consumer knowledge and attitudes towards cybercrime with a desired power of 0.80, an alpha level of 0.05, and assuming a medium effect size, the required sample size was determined to be approximately 248 respondents. This ensures that the study has sufficient power to detect statistically significant differences or relationships.

In addition to statistical considerations, practical constraints such as time, resources, and accessibility to respondents were also considered. The sample size of 248 respondents is both manageable and feasible within the scope of this study, allowing for efficient data collection and analysis while still providing robust and meaningful insights into the effectiveness of gamification as an educational tool for cybercrime awareness.

Efforts were made to ensure that the sample is representative of the diverse demographic characteristics of South African consumers, including considerations of age, gender, socioeconomic status, and geographic distribution. A representative sample enhances the generalisability of the findings, ensuring that the conclusions drawn from the study are applicable to the broader population. The sample size of 248 respondents is justified based on statistical principles, power analysis, practical constraints, and efforts to ensure representation (Landers & Armstrong, 2017).

## 3.7 Research Instrument and data collection procedures

The Qualtrics survey tool was utilised using a quantitative data collection approach. Quantitative data collection instruments are valuable tools for capturing numeric data in a systematic and organised manner, allowing the researcher to test hypotheses and obtain objective responses to their queries, as emphasised by Clark et al. (2021). Quantitative data are often gathered using tools such as structured questionnaires, surveys, formal interviews, and observational checklists. These methods generally have set questions, choices for answers, or distinct categories for gathering data, which are designed to ensure consistency and comparability in responses, prompting clear and structured feedback from participants (Fanning, 2019).

Using the Qualtrics research platform, we deployed a mix of Likert scale items, multiple-choice questions, and open-ended queries to gather data that was both quantifiable and qualitative. In order to minimise potential biases, the survey was designed to offer a concise array of answer choices. Clark et al. (2021) highlights that tools for collecting quantitative data afford a systematic and structured approach to acquiring data that lends itself to statistical analysis. Notably, qualitative feedback was solicited through open-ended survey questions, providing participants with the opportunity to detail their personal experiences, views, and recommendations about gamification.

## 3.8 Data analysis

Quantitative research often encompasses of statistical analysis to determine ‘the connection between what is known and what can be learned by research’ (Flinton & Malamateniou, 2020). Therefore, data analysis through quantitative strategies requires either descriptive or inferential statistics to understand the relationships among variables of the study. Flinton & Malamateniou (2020) further explain that inferences about populations are drawn using descriptive statistics, which help to

estimate parameters and enable assumptions that generalises the population from the selected sample. The study employed descriptive analysis and inferential statistics, specifically using the Statistical Package for the Social Sciences (SPSS) software.

Each participant's responses were subject to descriptive statistical evaluation to understand response patterns. Descriptive statistics synthesise individual data into concise metrics, revealing profiles, tendencies, and relationships within the data, as mentioned by Cooksey (2020). Moreover, inferential statistics scrutinise the authenticity of observed patterns within the broader population by analysing the sample data. This analysis included the computation of frequency distributions, average scores, range, and standard deviation to assess the commonality and dispersion of the survey responses.

The research utilised the exploratory factor analysis to detect possible correlations among the variables being studied. Responses to open-ended questions were systematically coded and categorised into themes, enabling the identification of patterns and recurring topics related to participant experiences with gamified cybercrime education.

In order to ensure the validity and reliability of this study, several measures were implemented throughout the research process. The use of a standardised online questionnaire incorporating both open-ended and multiple-choice items allowed for a comprehensive collection of data, enhancing content validity by covering various aspects of cybercrime awareness and gamification. The questionnaire was pilot tested to identify and correct any ambiguities, thereby improving its reliability and ensuring consistent responses.

Although internal consistency could not be assessed using Cronbach’s alpha due to the mixed-method nature of the survey, researchers have supported the reliability of mixed surveys by using other methods such as test-retest reliability, inter-rater reliability, and triangulation to ensure robustness (Buil-Gil, Miró-Llinares, & Moneva, 2020; Koivisto & Hamari, 2019; Denden, Tlili, Essalmi, & Jemni, 2020). For instance, Koivisto and Hamari (2019) highlight that mixed-method surveys can provide a rich and nuanced understanding of the research problem by combining quantitative and qualitative data, which enhances the overall reliability of the findings. Additionally, Denden et al. (2020) emphasised the importance of using diverse data collection tools

to capture the multifaceted nature of engagement and learning outcomes, thereby ensuring robust and reliable results. In order to ensure construct validity, the survey items were grounded from the established theoretical frameworks such as Self-Determination Theory (SDT) and behavioural science principles, aligning with previous research in the field (Zimmermann & Renaud, 2019; Sailer et al., 2021).

Furthermore, external validity was addressed by selecting a diverse sample of 248 respondents from various demographic backgrounds, reflecting the broader population of South African consumers. The use of Chi-square tests and independent samples t-tests to analyse the data helped to control the potential biases and confirm the robustness of the findings. These statistical methods ensured that the observed differences in knowledge and attitudes towards cybersecurity were not due to random chance, thereby reinforcing the reliability of the results.

### 3.8.1 Definition of variables

According to Pokhariyal (2019) an independent variable is a variable manipulated or controlled in a scientific experiment to determine its effect on a dependent variable. It's the component that the researcher manipulates to see how it impacts the results of the experiment, essentially the presumed cause of variation in the dependent variable. The dependent variable, on the other hand is the aspect that is measured or noted during the experiment and is believed to be affected by the independent variable's alterations. It's the element under examination and it is anticipated to vary in response to the independent variable's modifications (Andrade, 2021).

### 3.8.2 Independent variable: Gamification

Gamification involves incorporating elements and concepts from game design into non-gaming environments in order to boost user involvement, motivation, and activity. It includes the use of gaming components such as scoring points, earning badges, ranking on leaderboards undertaking challenges, and receiving rewards within platforms or activities that typically do not feature gameplay (Deterding, 2019). The purpose of gamification is to create a more engaging, absorbing, and interactive experience, aiming to encourage specific behaviours and achieve targeted results. This strategy seeks to make tasks that might normally seem mundane feel more like

play, therefore increasing the likelihood of participation and engagement (Brandão and Costa, 2021; Zennaro & Erdődi, 2023).

### 3.8.3 Dependant variable 1: Consumer knowledge of cybercrime

In the context of this study, consumer knowledge of cybercrime means awareness and recognition of what cybercrime is, how it works, its objective and effect on consumers.

### 3.8.4 Dependent Variable 2: Consumer attitude towards cyber crime

Consumer attitudes on cybercrime refers to how consumers perceive cybercrime, how they relate to it and what their believes are.

### 3.8.5 Outcome variable

The effectiveness of gamification on reducing the impact of cybercrime on consumers.

## 3.9 Ethical consideration

Adhering strictly to established protocols for conducting scientific research is of utmost importance to adhere to the pursuit of advancing knowledge. These guidelines are essential for directing the evolution of learning and discovery in the realm of research. Therefore, in compliance with the protocol, an application for ethical research approval was submitted to the Ethical Committee of Witwatersrand University.

The Qualtrics online survey platform facilitated the electronic distribution of detailed study information and informed consent forms. Participants were provided with electronic consent prior to engaging in the survey, informing them on how the researcher would adhere to the scientific process protocols, ensuring an ethical and informed research process. In order to maintain participant confidentiality, all data were anonymised during analysis.

For instance, the letter of consent clarified the following issues,

- Ensuring no harm to participants, the letter of consent informed the participants no harm would come to them, considering the interviews were conducted through a survey and they were given the option to exit the study at any point without any repercussions.

- Ensuring safekeeping of data and information drawn from the scientific process would be achieved through password encryption of all the data and the information used in this research.

Furthermore, the data collected was kept confidential by strictly following the Protection of Personal Information Act 4 of 2013 (POPI Act), by refraining from any sharing with external parties.

### 3.10 Privacy and anonymity

According to Skelton et al. (2020), a common method for ensuring research participant confidentiality is to make use of passwords protected files. This approach is covered in research planning, including obtaining necessary ethical approval from a research study committee and implementing strict protocols throughout data collection, analysis, and reporting of research findings (Stommel and Rijk, 2021). In order to safeguard privacy and maintain anonymity the researcher followed the established ethical clearance process, provided informed consent forms to participants, and emphasised the protection of participant information throughout data collection, analysis, presentation, and storage.

### 3.11 Chapter conclusion

In summary the chapter presents a comprehensive research plan aimed at enriching the examination and integration of the previously discussed scholarly works. The plan outlines the research design, population, as well as the techniques employed in analysing and collecting the data. The adherence to these established methods is geared towards a thorough and effective investigation of the research questions and aims set forth at the outset. Furthermore, it underscores the commitment to ethical research practices and the safeguarding of participants' privacy which are essential for upholding the integrity of the research outcomes.

# Chapter 4: Data analysis and interpretation

## 4.1 Introduction

Following the survey methodology described in the previous chapter, this section offers an analysis and interpretation of of findings obtained from the survey regarding the use of gamification to educate consumers on cybercrime in SA. Data processing was executed through IBM SPSS version 25 beginning with the coding and inputting of data onto spreadsheets. Descriptive statistics formed the basis of the analytical process. To identify correlations between different variables, a Chi-square test was applied, contrasting observed outcomes with expected results. A p-value of less than 0.05 was interpreted as an indicator of being statistical relevant highlighting the important discoveries within the investigation (Di Leo and Sardanelli, 2020).

## 4.2 Data screening

A total of 304 respondent surveys were returned; of these, 52 were removed from the sample as they were incomplete, while four were excluded because they did not consent to take part in the study. Thus, a sample of 248 responses were analysed for this study.

## 4.3 Sample characteristics / Demographic

### 4.3.1 Gender

The results presented (Fig 4.1 and Table 4.1) show that the majority respondents identified as female (58 percent), followed by male (39 percent). A small percentage identified as non-binary or third gender (one percent), while an additional two percent chose not to disclose their gender preference.

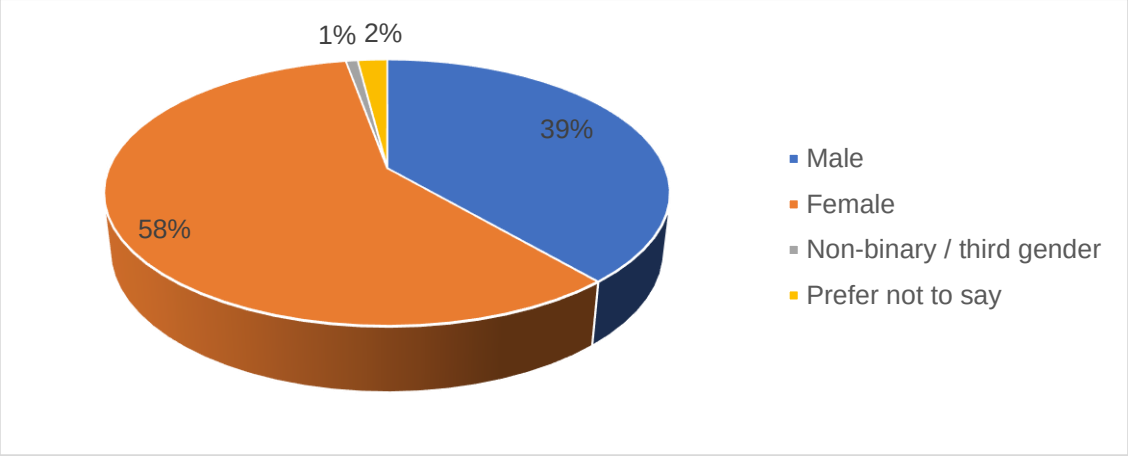



**Figure 4.1: Respondent gender**

### 4.3.2 Level of education

The sample's educational attainment is diverse, reflecting a range of academic achievements (Fig 4.2 and Table 4.1). A small portion of the sample (9%) has completed their high school education. A notable percentage (27%) holds a diploma, while a significant portion of the sample (49%) has attained at least an undergraduate university degree.

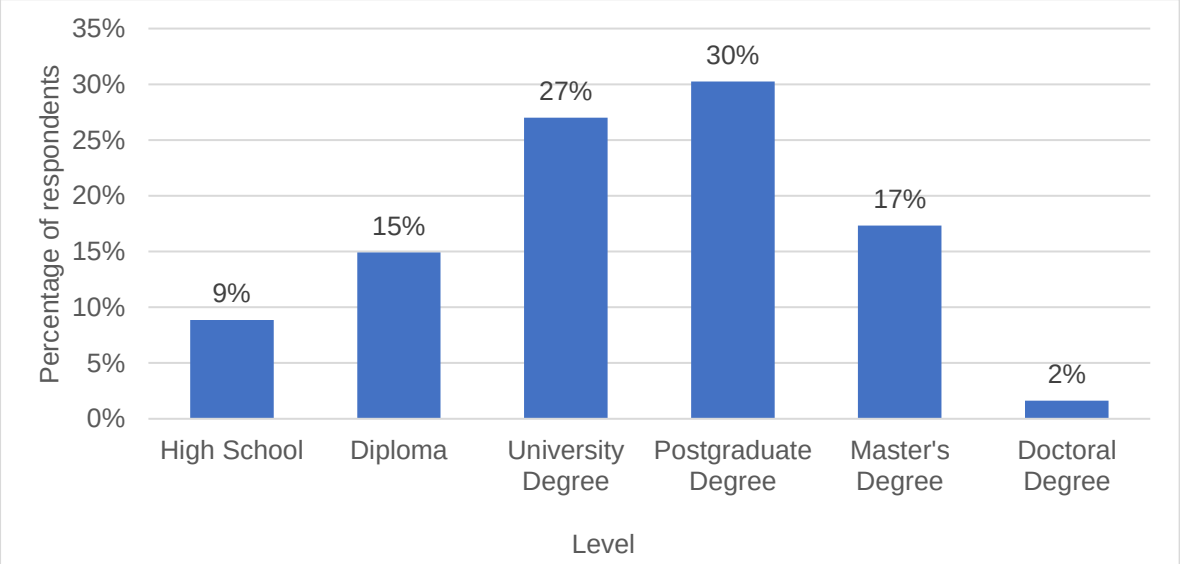



**Figure 4.2: Highest level of education completed**

### 4.3.3 Income

The results (Fig 4.3 and Table 4.1) showed that respondents with incomes less than R14 999 make up 12 percent of the sample, those with incomes ranging between R15 000 and R25 999 account for 11 percent, and those with incomes ranging

between R26 000 and R39 999 account for 12 percent, while eight percent earned an income falling within the R40 000 to R59 999 range. The highest income bracket, R60 000 and above, has the largest share at 36 percent, while 11 percent of the sample did not disclose their income information.

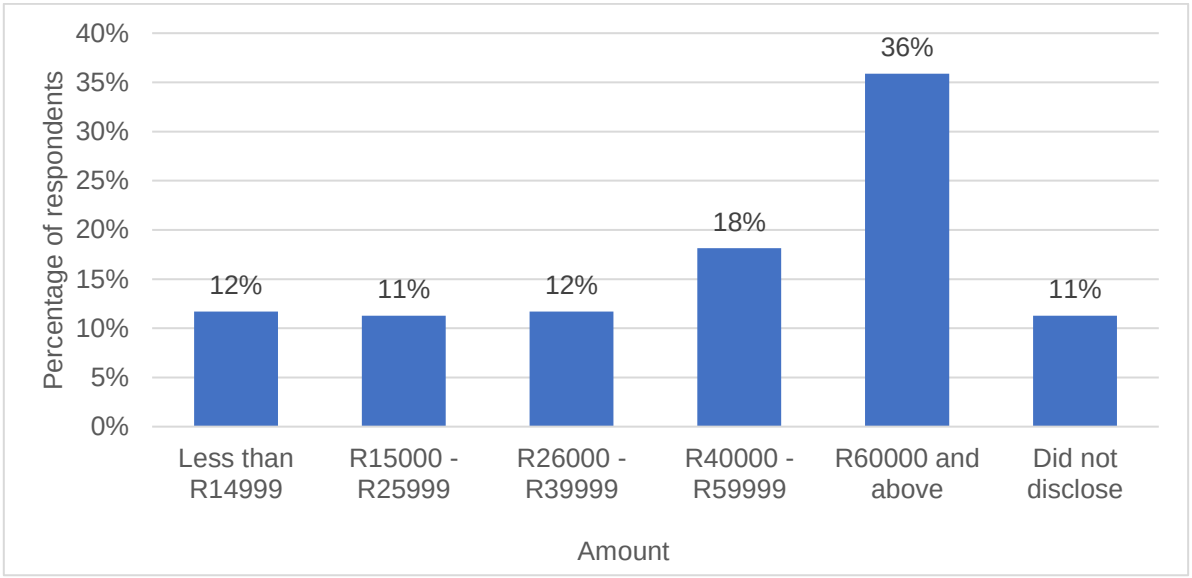



**Figure 4.3: Respondent income**

### 4.3.4 Have a bank account in SA

The results (Fig 4.4 and Table 4.1) show that the majority of respondents (70 percent) had a personal bank account in SA. A small percentage (one percent) indicated they have a business bank account only, while 27 percent had both business and personal bank accounts (27 percent). A small minority (two percent) indicated they did not have a bank account in SA.

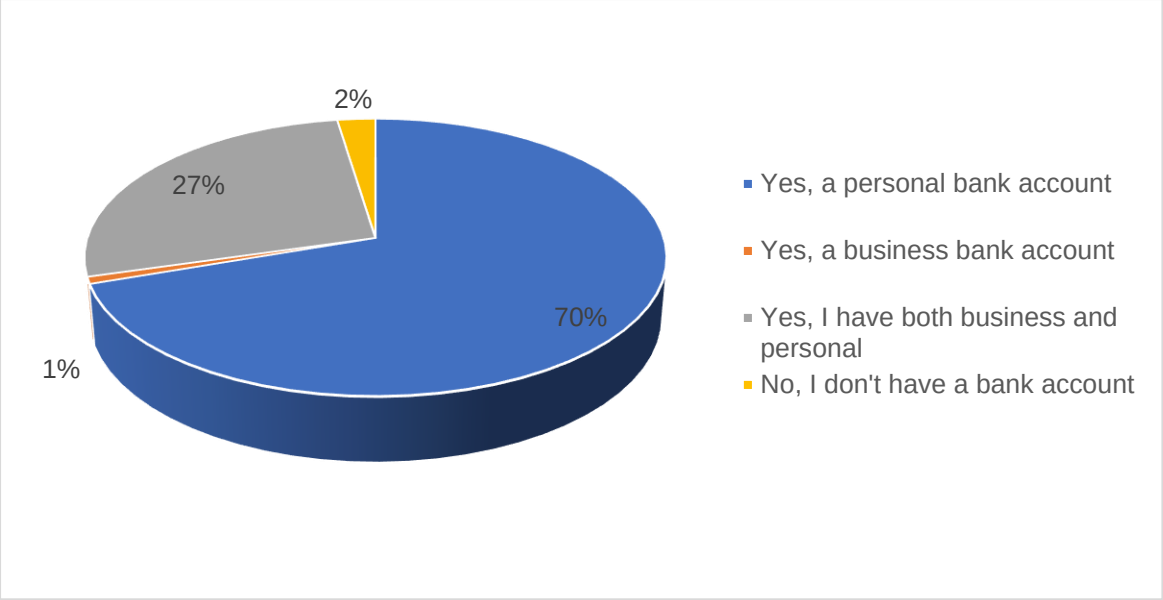



**Figure 4.4: Have a bank account in SA**

**Table 4.1: Chi-square p-values for sample characteristics/demographics**

| | | Played an educational game | | Total (n=248) | P-value |
|---|---|---|---|---|---|
| **Variable** | **Options** | **Yes (n=77)** | **No (n=171)** | | |
| Q1. Most often used way to conduct banking needs | Mobile application | 77.9% | 75.4% | 76.2% | .426 |
| | Internet banking | 5.2% | 9.9% | 8.5% | |
| | Branch | 0.0% | 1.2% | 0.8% | |
| | Cellphone banking | 16.9% | 13.5% | 14.5% | |
| Q13. Gender | Male | 36.4% | 40.0% | 38.9% | .462 |
| | Female | 62.3% | 57.1% | 58.7% | |
| | Non-binary / third gender | 1.3% | 0.6% | 0.8% | |
| | Prefer not to say | 0.0% | 2.4% | 1.6% | |
| Q15. Highest level of education | Completed high school | 6.5% | 9.9% | 8.9% | .775 |
| | Completed a diploma | 11.7% | 16.4% | 14.9% | |
| | Completed a university degree | 27.3% | 26.9% | 27.0% | |

| | | | | | |
|---|---|---|---|---|---|
| | Completed a postgraduate degree | 32.5% | 29.2% | 30.2% | |
| | Completed a master's degree | 20.8% | 15.8% | 17.3% | |
| | Completed a doctoral degree | 1.3% | 1.8% | 1.6% | |
| Q16. Income | Less than R14 999 | 4.0% | 15.3% | 11.8% | .049 |
| | R15 000 – R25 999 | 8.0% | 12.9% | 11.4% | |
| | R26 000 – R39 999 | 10.7% | 12.4% | 11.8% | |
| | R40 000 – R59 999 | 17.3% | 18.8% | 18.4% | |
| | R60 000 and above | 46.7% | 31.8% | 36.3% | |
| | Do not wish to disclose | 13.3% | 8.8% | 10.2% | |
| Q17. I have a South African bank account? | Yes, a personal bank account | 72.7% | 68.4% | 69.8% | .644 |
| | Yes, a business bank account | 0.0% | 1.2% | 0.8% | |
| | Yes, I have both business and personal | 26.0% | 27.5% | 27.0% | |
| | No, I don't have a bank account | 1.3% | 2.9% | 2.4% | |

The results (Table 4.1) showed the most frequent way respondents indicated they conduct banking needs, which showed use did not depend on whether one would have played a game or not. This was because the chi-square p-value was greater than 0.05.

## 4.4 Hypothesis testing

The Chi-square test of association was carried out on all variables, excluding the mean score regarding "Your knowledge on cybercrime." For the latter, to compare the mean scores of individuals who had engaged with the game against those who hadn't, the study employed an independent samples t-test. The choice of the Chi-square test for the remaining variables was considered appropriate, due to the categorical nature of both the independent variable—playing an educational game or not—and the dependent variables. The findings can be found in Table 4.2.

**Table 4.2: Comparing results by whether a respondent played the game**

| | | Played an educational game | | Total (n=248) | P-value |
|---|---|---|---|---|---|
| **Variable** | **Options** | **Yes (n=77)** | **No (n=171)** | | |
| Q2. Your knowledge on cybercrime? | Mean score | 8.22 | 6.56 | 7.07 | .000 |
| Q7. Which online safety topics would interest you in a game? Choose two. | Using strong passwords, updating software, and being cautious when sharing personal information online | 61.0% | 52.6% | 55.2% | .270 |
| | Vishing: criminals impersonate legitimate companies via phone calls to obtain personal information from unaware consumers | 57.1% | 52.6% | 54.0% | .582 |
| | Phishing: a technique used by cyber criminals to deceive individuals into unknowingly installing malicious software by clicking on hyperlinks | 51.9% | 37.4% | 41.9% | .037 |
| | Safe online banking hygiene factors | 24.7% | 25.1% | 25.0% | 1.000 |
| Q8. If you had or have played a game to increase your understanding of cybersecurity threats, which aspect of the game would be most important? | Quizzes | 40.3% | 36.8% | 37.9% | .672 |
| | Simulation of real-world examples | 79.2% | 70.2% | 73.0% | .165 |
| | Tips or educational content | 50.6% | 33.3% | 38.7% | .011 |
| | Dangers of using public Wi-Fi | 33.8% | 35.7% | 35.1% | .886 |

**H1: Consumers' knowledge of cybercrime improves after play games designed to improve such knowledge.**

The study examined the impact of playing a game on cybercrime knowledge by utilising an independent samples t-test. These results (Table 4.2) revealed a significant difference in knowledge between participants who played a game (mean = 8.22 out of 10) and those who did not play a game (mean = 6.56), with a p-value of 0.000. This indicates that the Consumers' knowledge of cybercrime improves after playing games designed to improve such knowledge.

A statistical analysis, utilising a chi-square test, was conducted to assess the preferences for online safety topics in an educational game among participants who played and those who did not play. The results indicate no significant difference in interest between the two groups for the topics "Using strong passwords, updating software, and being cautious when sharing personal information online" (p = 0.270) and "Vishing: criminals impersonate legitimate companies via phone calls to obtain personal information from unaware consumers" (p = 0.582). However, a significant difference was observed for the topic "Phishing: a technique used by cyber criminals to deceive individuals into unknowingly installing malicious software by clicking on hyperlinks" (p = .037), with a higher interest among participants who played the game (57.1%) compared to 37.4% among those that did not play the game. No significant differences were found for "Safe online banking hygiene factors" (p = 1.000).

A statistical analysis was performed using a chi-square test to examine the significance of preferences regarding aspects of an educational game for increasing understanding of cybersecurity threats among participants who played and those who did not play. The results indicate no significant difference in preference amongst the two groups for "Quizzes" (p = 0.672) "Simulation of real-world examples" (p = 0.165), and "Dangers of using public Wi-Fi" (p = 0.886). There was, however, a significant difference observed for "Tips or educational content" (p = .011), with a higher preference among participants who played the game.

The above results (Table 4.2) reveal that consumer's knowledge of cybercrime improves after playing games designed to improve such knowledge with those that would have played the games preferring to learn more about phishing and those that

would have played games preferring to get tips or educational content (Sailer et al., 2017).

**Table 4.2: Comparing results by whether a respondent played the game**

| | | Played an educational game | | Total (n=248) | P-value |
|---|---|---|---|---|---|
| **Variable** | **Options** | **Yes (n=77)** | **No (n=171)** | | |
| Q4. Most effective way for learning while playing a game | I learn more if I score points or get rewards | 31.2% | 42.4% | 38.9% | .279 |
| | I learn more from tips | 14.3% | 11.8% | 12.6% | |
| | I learn equally from both | 39.0% | 36.5% | 37.2% | |
| | I learn more from failing | 15.6% | 9.4% | 11.3% | |
| Q5. Please choose a statement(s) that resonate(s) with you. | Playing a game improves my cyber hygiene knowledge and habits | 37.7% | 14.6% | 21.8% | .000 |
| | I have a cautious attitude | 48.1% | 50.3% | 49.6% | .785 |
| | I am confident in advising others about cybercrime education such as scams and tricks | 44.2% | 27.5% | 32.7% | .013 |
| | My bank has equipped me with the necessary information to avoid falling victim to scams | 51.9% | 51.5% | 51.6% | 1.000 |
| Q6. To what extent would online safety game effectively teach people about cybercrimes, including avoiding scams and tricks? | Definitely effective | 64.5% | 48.0% | 53.0% | .016 |
| | Might or might not | 35.5% | 46.8% | 43.3% | |
| | Not effective | 0.0% | 5.3% | 3.6% | |
| Q9. If an online safety game made you aware of | Extremely unlikely | 7.8% | 7.6% | 7.7% | .755 |
| | Neither likely nor unlikely | 6.5% | 9.4% | 8.5% | |

| | | | | | |
|---|---|---|---|---|---|
| risks, how likely are you to change your behaviour? | Extremely likely | 85.7% | 83.0% | 83.9% | |
| Q10. Have you ever been a victim of online banking fraud, such as scams or tricks, after being exposed to the game? | Yes | 13.0% | 12.9% | 12.9% | 1.000 |
| | No | 87.0% | 87.1% | 87.1% | |
| Q11. What would make you want to play a game about online safety to change your online banking behaviour? | Playing with friends | 26.0% | 20.5% | 22.2% | .409 |
| | Nice designs and pictures | 31.2% | 23.4% | 25.8% | .212 |
| | Competing for points, rewards or having a leader board | 68.8% | 65.5% | 66.5% | .664 |
| | Duration of the game | 41.6% | 36.8% | 38.3% | .484 |
| | Other | 6.5% | 5.8% | 6.0% | .782 |

**H2: Consumers' attitude toward cybercrime improves after they played a game meant to educate them about cybercrime**

To evaluate the perceived effectiveness of an educational game on learning, a chi-square test was performed comparing responses from participants who played the game to those who did not. The results showed no significant difference in preferences amongst the two groups across all options as all the p-values were more than 0.05.

A chi-square test was also conducted to assess the statements that resonate with participants who played an educational game compared to those who did not play. The results revealed significant differences in responses for the statements: "Playing a game improves my cyber hygiene knowledge and habits" ($p = 0.000$), with a higher agreement among participants who played the game, and "I am confident in advising others about cybercrime education such as scams & tricks" $p = 0.013$), with a higher agreement among participants who played the game.

There were no significant differences for statements "I have a cautious attitude" ($p = 0.785$), and "My bank has equipped me with the necessary information to avoid falling victim to scams" ($p = 1.000$), indicating no significant difference between the two groups.

A chi-square test was conducted to analyse the participants' opinions on the effectiveness of online safety games in teaching about cyber-crimes, including avoiding scams and tricks, among those who played and those who did not. The results indicate that 64.5% of those that who played the game were of the view that the games were Definitely effective, compared to 48.0% among those that did not play the game (Mitchell et al., 2021).

There were no significance differences on the likelihood to change behaviours if an online safety game one aware of risks (p-value = 0.755), being a victim of online fraud (p-value = 1.000) and reasons for wanting to play a game about online safety to change online banking behaviour (p-values > 0.05).

The results (Table 4.3) showed that the most often way to conduct banking needs used did not dependent on whether one would have played a game or not. This was because the chi-square p-value was greater than 0.05.

| | | **Played an educational game** | | **Total (n=248)** | **P-value** |
|---|---|---|---|---|---|
| **Variable** | **Options** | **Yes (n=77)** | **No (n=171)** | | |
| Q1. Most often used way to conduct banking needs | Mobile application | 77.9% | 75.4% | 76.2% | .426 |
| | Internet banking | 5.2% | 9.9% | 8.5% | |
| | Branch | 0.0% | 1.2% | 0.8% | |
| | Cellphone banking | 16.9% | 13.5% | 14.5% | |
| Q13. Gender | Male | 36.4% | 40.0% | 38.9% | .462 |
| | Female | 62.3% | 57.1% | 58.7% | |
| | Non-binary / third gender | 1.3% | 0.6% | 0.8% | |
| | Prefer not to say | 0.0% | 2.4% | 1.6% | |
| Q15. Highest level of education | Completed high school | 6.5% | 9.9% | 8.9% | .775 |
| | Completed a diploma | 11.7% | 16.4% | 14.9% | |
| | Completed a university degree | 27.3% | 26.9% | 27.0% | |
| | Completed a postgraduate degree | 32.5% | 29.2% | 30.2% | |

| | | | | | |
|---|---|---|---|---|---|
| | Completed a master's degree | 20.8% | 15.8% | 17.3% | |
| | Completed a doctoral degree | 1.3% | 1.8% | 1.6% | |
| Q16. Income | Less than R14 999 | 4.0% | 15.3% | 11.8% | .049 |
| | R15 000 – R25 999 | 8.0% | 12.9% | 11.4% | |
| | R26 000 – R39 999 | 10.7% | 12.4% | 11.8% | |
| | R40 000 – R59 999 | 17.3% | 18.8% | 18.4% | |
| | R60 000 and above | 46.7% | 31.8% | 36.3% | |
| | Do not wish to disclose | 13.3% | 8.8% | 10.2% | |
| Q17. I have a South African bank account? | Yes, a personal bank account | 72.7% | 68.4% | 69.8% | .644 |
| | Yes, a business bank account | 0.0% | 1.2% | 0.8% | |
| | Yes, I have both business and personal | 26.0% | 27.5% | 27.0% | |
| | No, I don't have a bank account | 1.3% | 2.9% | 2.4% | |

## 4.5 Concluding comments

This section provided a summary of the feedback obtained from survey respondents, detailing the categorisation of responses and the data processing methods employed. The data was organised by several demographic factors such as gender, education level, income, and the possession of a bank account in South Africa, along with the presence of cybercrime awareness education. The next and final chapter provides a comprehensive discussion of these findings, proposing recommendations derived from the outcomes, and suggestions for future research.

## Chapter 5: Findings and recommendations

The results of the quantitative study conducted in this research are presented in this chapter, displaying the data in a concise and structured manner. The study highlights patterns and trends that emerged from the data, enhancing the understanding of gamification as an educational tool for increasing consumer awareness of cybercrime in South Africa. These findings will be valuable for future studies in this area. The objective was to investigate the effect of gamification on South African consumers' knowledge and attitudes to educate them about the risks of cybercrime. Gamification requires the coordination of numerous stakeholders and resources, making it essential to evaluate its effectiveness and identify the most effective design elements in various contexts.

### 5.1 Introduction

This study makes significant contributions to the literature on gamification, cybercrime education, and consumer behaviour. Previous research, such as Hart, Beale, and Carmichael (2020), has highlighted the effectiveness of gamified interventions in increasing cybersecurity awareness. This study extends those findings by empirically demonstrating that integrating elements of Self-Determination Theory (SDT) autonomy, competence, and relatedness within gamified educational tools enhances intrinsic motivation, engagement, and knowledge retention among consumers. These findings align with the work of Mitchell, Petherick, and Ziegler (2020), who emphasised the importance of these psychological needs in educational contexts.

Furthermore, while Alqahtani and Kavakli-Thorne (2020) identified the potential of gamification in cybersecurity education, this study uniquely combines SDT and behavioural science principles, providing a comprehensive framework for influencing consumer behaviour. The results shows that immediate feedback, social norms, and interactive content effectively promote safer online practices, supporting and expanding on the findings of Burke (2021) regarding behavioural interventions.

By positioning these findings within the broader context of existing literature, the study not only validates established theories but also offers new insights into designing

effective gamification strategies for cybersecurity education. This dual-theoretical approach enhances understanding and highlights practical strategies for behaviour modification in digital environments, contributing significantly to both academic knowledge and practical applications. The next chapter will detail the research methodology and describe the techniques used for data analysis.

## 5.2 Effectiveness of gamification on knowledge enhancement

The independent samples t-test conducted emphasises the effectiveness of gamified approaches in improving consumer understanding of cybercrime. It is evident from the results, by incorporating educational games, they can greatly enhance cybersecurity awareness campaigns proving how effective gamification can be as an educational tool. The statement suggests engaging in interactive and participatory activities, such as gaming, can lead to a greater acquisition of knowledge, when compared to traditional educational methods (Riopel, et al., 2019).

Participants furthermore emphasised the need for a comprehensive strategy to promote cybersecurity awareness. They recommended financial institutions to offer concise tutorials for non-app users and use relatable personas and real-life examples to improve understanding. Additionally, they stressed the importance of providing educational content on popular platforms such as YouTube and TikTok, identifying the limitations of relying solely on email notifications.

When designing a campaign to increase customer awareness it is important to take into account different elements, including the prompts that can be employed (Charandura, 2022). Examples of such prompts include urging users to establish a passcode or alter default passwords when first setting up their devices or systems on their various banking platforms (internet banking, mobile application, and cell phone banking). Additionally, when consumers access the bank’s platforms, it is important that they are reminded of the most recent scams, in order to encourage digital identity safeguards and creating robust passwords. This evidence supports H1. The importance of educating consumers on security measures and nurturing a strong security culture within financial institutions cannot be overstated (Akinbowale, Klingelhöfer, & Zerihun, 2021). It is a continuous process rather than a one-time occurrence. The participants who had previously played games on educating themselves about cybercrime indicate that they are comfortable to advise others on

the topics. There has been substantial research conducted on the effectiveness of gamification in acquiring knowledge making it easier for decision makers to consider investing in the tool (Alqahtani and Kavakli-Thorne 2020).

### 5.3 Customised content for improved engagement

An interesting finding emerged from a Chi-square test regarding consumers' preferences for online safety topics in educational games. While both groups displayed a similar level of interest in specific online safety topics, such as password security and software updates, there was a clear distinction in the heightened interest in phishing among gamers versus non-gamers (Q7), (Bossler & Berenblum, 2019). This unexpected result indicates a possible opportunity for focused educational interventions on phishing in gamified platforms, suggesting customised content delivery could enhance learning results and increase player engagement in educational games (Li and Liu 2021).

When examining these results in relation to previous research, it becomes clear gamification is consistently proven effective in improving knowledge (Borrás-Gené et al., 2019). This supports research findings that highlight the success of interactive and engaging learning approaches (Q2), (Fitz-Walter 2015; Friedrich et al., 2020). Research carried out by Smith et al., (2021), Monteith et al. (2021), and Kim et al., (2018) have all found that participating in cybersecurity-themed games can enhance individual's comprehension of various concepts related to online safety. These concepts include identifying potential cyber threats, understanding different types of threats, and implementing best practices for staying safe on the internet (Rahi & Ghani, 2019). Nacke and Deterding (2021) suggests that educational games can enhance participant understanding of cybersecurity issues, resulting in an overall improvement in their comprehension of these matters.

Cybercrime in SA has become a major cause for concern, particularly due to its potential to disrupt financial stability and compromise security (Dlamini & Mbambo, 2019). Extensive research has highlighted the need for strong cybersecurity measures and educational programmes to help consumers mitigate the financial risks associated with cyber threats (Akinbowale, Klingelhöfer, and Zerihun 2021). The findings

underscore the importance of implementing targeted educational interventions to address different cybersecurity challenges, with a special focus on raising awareness with regards to phishing and social engineering tactics (McIlwraith, 2021). In addition, the interest in topics such as phishing amongst individuals who played games, suggests educational games can effectively address specific cybersecurity issues, providing tailored learning opportunities to meet user needs (Riopel, et al., 2019).

Educational game interventions can be customised to address cybersecurity challenges and provide participants with practical knowledge and skills to effectively counter cyber threats (Alqahtani and Kavak-Thorne 2020). In addition, studies have demonstrated the significant psychological and financial impact cybercrime can have on individuals, highlighting the need to recognise and deal with these outcomes (Monteith et al. 2021).

Caution should, however, be exercised when interpreting the results. It is clear from the diverse range of user preferences for online safety topics that tailored gamification strategies are essential to cater to individual interests and concerns (Q8). This makes it crucial to recognise the importance of understanding the target audience pain points, these are some of the factors which are often overlooked in the literature on successful educational interventions (Kalogiannakis et al., 2021).

Evidently, certain participants expressed scepticism regarding the use of gamification in financial institutions, which brings the credibility of institutions that employ gamification into question, especially when the gaming experiences fail to meet consumer product or service requirements. It is also important to highlight the respondent's feedback whereby they encouraged financial institutions to provide incentives as a reward to be used for continuous learning process however it must be implemented clear objectives should it be applied (Hernández-Fernández et al., 2020).

**Participant's feedback**

"*It's vital to know who you are targeting; I find many companies/banks are leaning into gamification and playing games when money is involved makes me question the legitimacy of the institution. Especially if the gamification do not speak to my product need*s."

*“Incentives are definitely a good idea for millennials and younger generations. Making it mandatory to read a popup (with tips to avoid being a cybercrime victim) in order to continue using the banking app or online site might be very effective. Seminars, printed material in branches and newsletters with this content might work for older clients. Having short, sharp tips and warnings in adverts on radio, TV and even YouTube and social media is another idea”.*

*“Gamification is good. However, acted out case scenarios in a short video (s) could be effective. Reward users who have completed the video: stickers, points, recognition etc…Some people might not be interested in games.”*

*“A monthly focus topic - for example if FNB focuses on Phishing...they can reward those who complete the game with a few eBucks or a percentage off voucher”*

Prior studies have emphasised how gamification can successfully impart cybersecurity principles and highlighted the importance of tailoring the cybercrime content to the target audience (Fitz-Walter 2015; Tobon et al., 2020; Mitchell et al., 2021).

### 5.4 Learning preferences in educational games

Research findings indicated participants had varying preferences on the learning strategies employed in educational games (Marinescu 2017). Individuals who participated in the game showed a greater interest in receiving tips or educational content, indicating a preference for practical and actionable information within the gaming environment. The use of impersonation techniques, such as vishing and phishing, was emphasised, along with a suggestion to incorporate AI cybersecurity awareness into current training programmes, considering SA's lack of AI regulations (Sampene et al., 2022). Additionally, the research stressed the importance of implementing two-step authentication and providing prompt customer notifications (Fitz-Walter 2015; Tobon et al., 2020; Mitchell et al., 2021).

The findings showed interactive and participatory learning approaches, such as short quizzes and simulations that incorporate game-like elements, for instance, challenges, rewards, and scenarios, are preferred by respondents (Friedrich et al., 2020). These methods are effective in capturing the attention and engagement of users of all ages

and digital literacy levels and is adaptable to meet the specific requirements and preferences of the intended audience (Sailer and Homner, 2020).

## 5.5 Gamification: Perception vs. Effectiveness

Both groups were found to hold similar views on the effectiveness of learning through educational games. Nevertheless, a greater number of participants who engaged in the game were convinced the games were unquestionably successful in educating them about cybercrimes. It seems there is a favourable view regarding the efficacy of gamification in teaching about cybersecurity (Hart et al., 2020).

The most compelling finding is that gamified cybersecurity education can be improved by incorporating AI-driven technologies, such as personalised learning experiences, content recommendation algorithms, and real-time threat detection (Sampene et al., 2022). The platform can offer tailored guidance and support based on individual needs and learning progress, which can lead to positive behavioural changes and long-term adherence to best practices, by fostering a sense of agency and self-efficacy (Lopez & Tucker, 2019).

The increasing dependence on online banking and transactions heightens the financial hazards linked to cyberattacks (Buil-Gil et al., 2020; Cavaliere et al., 2021). Consumers can make better choices when educated regarding cybercrime awareness, online transactions, and security precautions (Akinbowale et al. 2021). Gamification could provide numerous benefits for financial institutions when it comes to instructing consumers on the safety of using online banking services, which aligns with the author's primary argument. These benefits can be seen in the value it creates, which is reflected in a positive public image and a favourable reputation, and the economic value resulting from increased brand recognition that attracts and retains consumers (Huotari & Hamari, 2012). The financial institutions may use the SABRIC and the South African Banking Ombudsman fraud reports as a benchmark to assess how they’re competing against their competitors when it comes to customer and bank fraud losses. Additionally, gamification provides functional value by providing feedback from consumers, which helps the corporation to improve its products and services (Deeleman & Van Steen, 2021).

## 5.6 Attitudinal and behavioural change

The overall findings indicated that engaging in educational games could potentially foster a more favourable mindset towards embracing safer online practices. Individuals who participated in these games demonstrated a stronger alignment with statements pertaining to enhanced understanding of cyber-hygiene and increased confidence in educating others regarding cybercrime. There seems to be a change in how people think and act whereby staying safe online is concerned (McIlwraith, 2021). It highlights the importance of educational games in encouraging proactive cybersecurity habits.

Surprisingly, it is worth highlighting when participants were specifically asked regarding their likelihood of changing behaviours after playing an online safety game that made them aware of risks (Q9) and the factors that would motivate them to play such a game to alter their online banking behaviour (Q11), no significant differences were observed in their willingness to change behaviours in response to awareness of online safety risks (p-value = 0.755), falling victim to online fraud (p-value = 1.000), or the reasons for wanting to engage in a game about online safety to modify online banking behaviour (p-values > 0.05). These results indicate gamification should be combined with other approaches to achieve behavioural change.

The results align with earlier studies on gamification in educational settings, demonstrating the beneficial effects of educational games on both motivation and learning outcomes (Alqahtani and Kavakli 2020; Burke, 2021; Zhang et al., 2020). Gamification can foster a setting that stimulates creativity and diverse thought processes, which in turn facilitates a rich exchange of varying perspectives among consumers (Krosnick et al., 2018). This exchange can contribute to collective learning and cooperation whereby individuals are motivated to participate and engage with the material, leading to a more dynamic and interactive learning experience (Koivisto and Hamari, 2019). Additionally, it can help to break down barriers and to encourage collaboration as individuals work together to achieve a common goal (Featherstone & Habgood, 2019).

This enhances the intrinsic motivation as consumers are more likely to be invested in their learning journey when they feel a sense of belonging and purpose (Fitz-Walter et al., 2017; Sailer et al., 2017; Thompson et al., 2022). Moreover, using game elements in contexts where they are applicable can act as a motivational factor inspiring consumers to participate in learning activities and experience a sense of accomplishment and progress (Manzano-León et al., 2021). This discovery becomes even more important, considering the increasing occurrence of cybercrime and the pressing necessity for efficient ways to educate consumers with regards to safeguarding themselves from the risks (Riopel, et al., 2019).

Gamification is a process that entails analysing player behaviour and expenses to optimise the design of games (Tobon et al., 2020). This involves implementing various measures to effectively gamify activities, which is an ongoing process. Marketing professionals must take diverse player types and their behaviour into account, and it is widely acknowledged different types of players require distinct games and game elements. Nevertheless, player profiling is often not performed, or when it is done, it focuses on sociodemographic rather than psychographic parameters (Kam & Umar, 2018).

Theories on motivation have played a crucial role in shaping the gamification framework. Within the scope of numerous motivational theories, gamification draws upon extrinsic and intrinsic motivators. However, it is the intrinsic motivators that drive consumer participation in gamified experiences. Implementing game components effectively can engage both extrinsic and intrinsic motivators (Manzano-León et al., 2021).

### 5.7 Efficacy of gamification as a tool to educate consumers

The importance of gathering user input and continuously improving educational interventions is highlighted by the positive feedback received from participants regarding online safety games. According to Alqahtani and Kavakli-Thorne (2020), it is possible to improve the relevance, effectiveness, and engagement of educational games and as a result their capacity to encourage cybercrime awareness and behaviour adjustment by incorporating user feedback into the iterative design process (Huang & Zhu, 2020). Individuals who actively participated in playing games showed notably elevated levels of understanding in the field of cybercrime, in contrast to those

who did not engage in such activities. This demonstrates how online safety games can help consumers to learn about the dangers of cybersecurity and the precautions to become more conscious of them (Hart et al., 2020).

Lee and Johnson (2020) further supported the evidence on how gamification can enhance consumer comprehension of cybercrime. The study demonstrated that those who participated in educational games exhibited greater knowledge and competence in cybersecurity ideas. Consequently, individuals who engaged in these activities were more capable of recognising and addressing potential cyber threats than those who did not. The research highlights the effectiveness of gamification as a powerful method for teaching consumers about cybersecurity, enabling them to gain an enhanced comprehension of and effectively manage online threats. These outcomes are encouraging as they offer innovative strategies that have been previously applied successfully across different fields. The investigation revealed a beneficial link between game elements and participant involvement in gamified activities, an insight that could be valuable for enterprises considering the adoption of gamification tactics to engage their consumer base (Bitrián et al., 2021).

## 5.8 Limitations and recommendations

SA is a developing country faced with certain constraints, particularly in the realm of digital literacy, due to its rich linguistic and cultural diversity. The country has eleven official languages and famously known “the rainbow nation”, in reference to its cultural diversity. As a result, the design and implementation of gamification initiatives present challenges making it crucial to consider local context and tailor games to cater to the specific requirements and inclinations of diverse communities in order to embrace their varied characteristics.

### 5.8.1 Linguistic landscape

The diverse linguistic (Fig 5.1) and cultural landscape of South Africa poses challenges for designing and implementing gamification initiatives. It is essential to consider the local context and tailor games to meet the specific interests and demands of various communities (Liebrecht et al., 2021). According to (Stats SA, 2022), isiZulu is the most widely spoken language in South African households, with approximately 24.4 percent (15.13 million) of the population fluent in the language, while isiXhosa is spoken by 16.3 percent of the population (Fig 5).

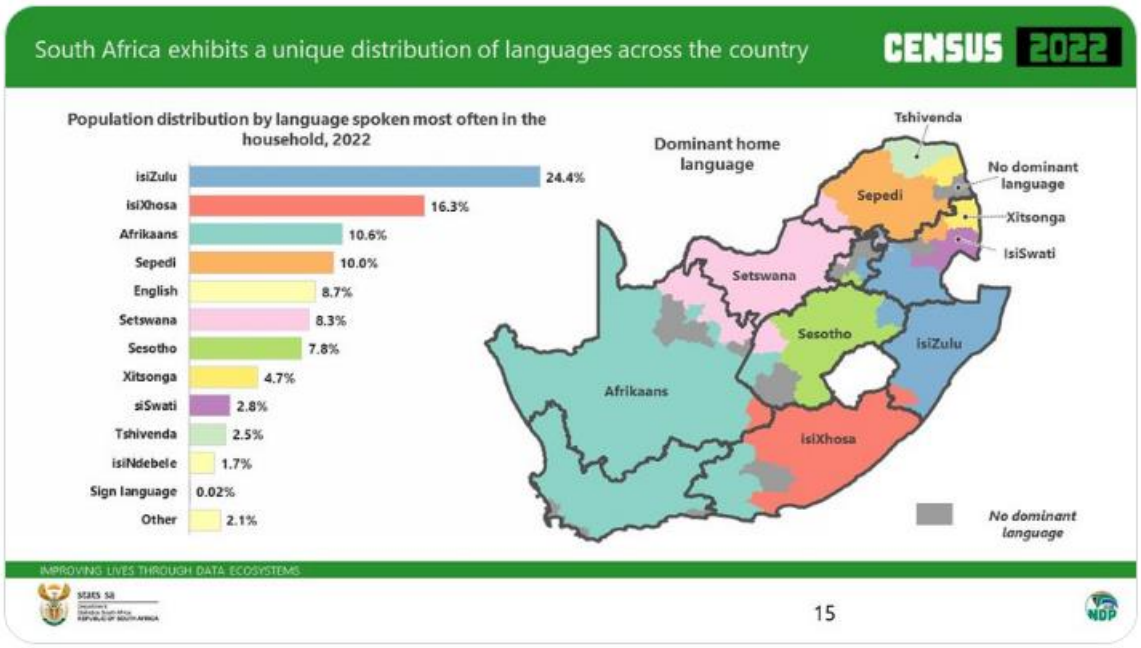



**Figure 5.1: South African linguistic landscape**

This shows the need for communication by financial institutions, to move away from being heavily focused on English as the preferred language in their communication but rather to initiate promoting cybercrime awareness, through tailored content by applying it to other South African languages, such as isiZulu, isiXhosa, Afrikaans, and Sepedi; the most widely spoken languages in the country (Stats SA, 2022). However, the most used language for disseminating cybercrime content is English, which raises concerns whether it is well understood and received by the intended audience.

This approach presents opportunities for financial institutions, policy makers and marketing professionals to tailor their campaigns to the consumer's preferred languages and understand the provincial nuances (Kim et al. 2018). Additionally, partnerships with stakeholders familiar with the local context can further facilitate the implementation of gamification initiatives. Moreover, cybercrime should be a topic introduced from primary school with the aim of using gamification to encourage learning and training at schools, ultimately impacting behaviour and attitude. Below is the feedback received from the respondents which highlights the importance of understanding the target audience when building the cybersecurity awareness strategies.

**Participants feedback**

*“Usage of other languages other than English and Afrikaans”*

*“Awareness should always be in the moment, consider the context of the transaction And importantly be personalized to suit the audience and engagement channel”*

*“Definitely. I think banks should find more ways to educate the older generation. With Gen Z, we’re more aware of cybercrimes but older consumers are not. Especially consumers that may not be as educated on the matter. It’s one thing to have pop up messages on the app that say “don’t share your pin” etc. There needs to be more effective ways the older age groups are educated. From what I have seen and read, this group is more likely to be scammed online by phishing and other online attacks.”*

*“Segment the players by age group and level of education to be more effective”.*

*“Make the content available in the languages reflecting the different demographics of their customer base.”*

Leveraging digital platforms and social media channels can, in addition, help banks reach a wider audience, including rural and underserved communities. Partnering with government agencies and non-profit organisations can also provide additional support and resources for language localisation initiatives. Partners such as the Banking Association of South Africa (BASA) are critical to these types of programmes to help and enforce such on the banks. Employing gamification can enhance user experience and engagement, particularly in service marketing. Ultimately, this approach can be effective in influencing customer behaviour, promoting innovation, and improving marketing effectiveness.

Furthermore, Belanche et al. (2021) discusses how influencer marketing is a successful strategy that involves collaborating with prominent individuals who share the same values and effectively represent the brand and, thus, a means to implement the above recommendations. This method of marketing enables financial institutions to produce engaging content that stimulates emotions, captures people's attention, and educates them in an enjoyable way. It is crucial to translate training materials into local languages for those not proficient in English as a medium of instruction to ensure inclusivity. Doing so can help SA overcome the legacy of its unbalanced education system (Stat SA 2022).

However, it is worth highlighting that the **research limitations** include a limited perspective on South African demographics with participants selected based on the researcher's social media reach which does not fully provide a representative sample of the average South African's experiences which includes those who are living in the rural areas. This is particularly evident in the income and education levels (SASSA, 2023).

### 5.8.2 Financial institutions to collaborate with third parties

Banks can collaborate with mobile network operators such as MTN, Vodacom, and Cell C to launch co-branded and promotional campaigns aimed at raising awareness concerning mobile cybersecurity best practices. This also creates an opportunity for financial institutions to negotiate with the mobile network operators to provide discounts or offer a zero-rate fee for consumers to access the educational games, where they don't require data to access the content, this is achievable by zero rating the applications identified. By doing so, they can encourage users to adopt safe hygiene cybersecurity practices (Amorosa & Yankson, 2023). To enhance user engagement, banks can incorporate gamification elements into their mobile applications, such as rewards systems, quizzes, and challenges. Furthermore, they can utilise mobile messaging platforms such as WhatsApp and Unstructured Supplementary Service Data (USSD) to provide real-time communication and support for customers seeking cybersecurity assistance or reporting suspicious activities. According to Stats SA (2022), 69.9 percent of households in SA have access to the internet through mobile technology which makes it easier to adopt the channels. These suggestions can help bridge the gap between the high cost of data, reach marginalised communities, and ensure an inclusive communication approach is adopted to reach millions of South Africans. While higher-income earners can access digital technologies and have better work and economic opportunities, low-income earners face challenges with basic digital literacy (Stats SA 2022).

## 5.9 Future research

The main objective for this research was to explore secondary questions in understanding how gamification can promote changes in consumer behaviour, retention, knowledge acquisition, and learning, as well as motivation, and engagement

in cybersecurity education. Although gamification has been widely used in various domains (Ofosu-Ampong, 2020; Alomair & Hammami, 2020; Barreto & França, 2021; Kalogiannakis et al., 2021), it is crucial to explore the connection between the consumer engagement behaviours and the development of a long-term relationship between banks which extend beyond mere transactions.

Future research could delve deeper into this area, analysing the dynamic interaction between player engagement behaviour in gamification-based consumer engagement. By examining this relationship researchers can gain valuable insights into how gamification can assist consumers in achieving their goals, thus providing value through engagement. The study also assessed how gamification impacts consumer perceptions and understanding when it comes to cybercrime education, however, it did not delve into the role various types of players have in enhancing the overall appeal and efficacy of gamification techniques (Burke, 2021). Further investigation could be conducted to investigate the connection between player segmentation and consumer behaviour, with the goal of gaining a better understanding of how to customise gamified experiences for distinct player types and enhance consumer engagement.

The quantitative study which had a majority of female participants in its sample size offers a stimulus to examine the connection between gender and consumer engagement in value creation, through gamification-based approaches. Previous studies on gamification have mainly centred on categorising players according to their psychological profiles and gaming behaviours (Alomair & Hammami, 2020). However, there is potential for new scientific and practical insights into gamification by exploring the socio-demographic traits of consumers and how they align with various player categories.

Gamification has been gaining traction and is projected to make a considerable impact in the years to come. However, at present it is primarily used to engage consumers in virtual markets, as opposed to traditional markets. In many cases, businesses use individual game elements, instead of a complete system of gamified activities, due to the high cost of implementation. Most often the gamification strategies are created with anticipated consumer actions in mind rather than being founded on an in-depth examination of the intended audience. To guarantee the success of these gamified

initiatives it is crucial to persistently refine and advance them (Alqahtani & Kavakli-Thorne , 2020).

In conclusion, gamification serves as a tool for financial institutions to engage customers mainly driven by economical goals which include increasing revenue, enhancing brand recognition, and collecting customer data to form and refine consumer databases. Moreover, gamification is effective in drawing new customers and reinforcing the loyalty of current ones. Additionally, it has various applications such as promoting communication by soliciting feedback, involving customers in product enhancement by encouraging them to propose ideas for packaging or product feature improvements, and offering rewards or feedback, whether as standalone incentives or integrated within sales functions (Riopel, et al., 2019).

Upon review, games can generally be categorised into two principal types based on their core dynamic features which are, those geared towards challenges, teamwork, and rivalry, and those designed for exploration and solitary self-improvement (Mitchell., 2020).The analysis indicated a player preference for games where scoring points is a central component however, the relevance of other elements like feedback, achievement badges, and ranking on leaderboards was also clear. There was a noticeable positive relationship between the motivation of consumers and the constituent elements of gamification (Welbers, et al., 2019).

The hypothesis can be confirmed that consumer knowledge of cybercrime improves after playing games designed to enhance such knowledge. The findings demonstrate that gamification is essential and effective for not only engaging consumers but also improving communication strategies (Scholefield & Shepherd, 2019). However, in the context of SDT, gamification should be used to explore how it can promote behaviour change, retention, knowledge acquisition, and learning motivation, as well as engagement, in cybersecurity education (Kam & Umar, 2018). According to this theory, different types of players may have varying roles in gamified activities, which can impact their engagement behaviour. Overall, the study found that gamification can boost motivation and engagement, but only when well-designed and thought-out beforehand (Deterding, 2019). Clear learning objectives, designing appropriate game mechanics, and avoiding over-reliance on gamification are important considerations in the use of gamification for cybersecurity education (Krath et al., 2021).

In conclusion, this research contributes to the theoretical framework regarding the use of gamification in the educational process shedding light on its influence on the consumer attitudes and knowledge acquisition.

## References


Barreto , C. F., & França, C. (2021). Gamification in Software Engineering: A literature Review. *International Workshop on Cooperative and Human Aspects of Software Engineering*, 85-89. doi:https://doi.org/10.1145/3510454.3516862

Boudadi, N., & Gutiérrez-Colón, M. (2020, March). Effect of Gamification on students' motivation and learning achievement in Second Language Acquisition within higher education: a literature review 2011 - 2019. *The EUROCALL Review*, 13. Retrieved from https://files.eric.ed.gov/fulltext/EJ1257523.pdf

Jung, W., Lim, R., Kabera, E., Isah, M., Cross, S., Sin, J., . . . Watkinson, D. (2021). *African Cyberthreat Assessment Report.* INTERPOL. INTERPOL. Retrieved from https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

Lachner, A., Hoogerheide, V., van Gog, T., & Renkl , A. (2022). Learning-by-Teaching Without Audience Presence or Interaction: When and Why Does it Work? *Educational Psychology Review*, 575–607. doi:https://link.springer.com/article/10.1007%2Fs10648-021-09643-4

Lee, C., & Johnson, A. (2020). Effectiveness of Educational Games in Improving Cybercrime Knowledge: A Longitudinal Study. *Cybersecurity Research Quarterly, 3*(8), 112-125.

Marinescu, D. (2017). *Complex Systems and Clouds: A Self-Organization and Self-Management.* doi:https://doi.org/10.1016/C2015-0-00979-0

Sileyew, K. J. (2019). Research Design and Methodology. doi:10.5772/intechopen.85731

Singleton, C., Hammond, C., & Eitan, A. (2022). *X-Force Threat Intelligence.* IBM. IMB Security. Retrieved from https://www.ibm.com/downloads/cas/ADLMYLAZ

Tobon, S., Ruiz-Alba, J., & García-Madariaga , J. (2020, January). Gamification and online consumer decisions: Is the game over? *Decision Support Systems, 128*. doi:https://doi.org/10.1016/j.dss.2019.113167

Adams, M., & Makramalla, M. (2015). *Cybersecurity Skills Training: An Attacker-Centric Gamified Approach.* doi:http://dx.doi.org/10.22215/timreview/861

Adams, M., & Makramalla, M. (2015). *Cybersecurity skills training: An attacker-centric gamified approach. Technology Innovation Management Review.*

Akinbowale, O., Klingelhöfer, H., & Zerihun, M. (2021). Analytical hierarchy processes and pareto analysis for mitigating cybercrime in the financial sector. *Journal of Financial Crime, 3*(29), 984-1008. doi:https://doi.org/10.1108/jfc-04-2021-0086

Akram, U., Fülöp, M., Tiron-Tudor, A., Topor, D., & Căpușneanu, S. (2021). Impact of Digitalization on Customers' Well-Being in the Pandemic Period: Challenges and Opportunities for the Retail Industry. *International Journal of Environmental Research and Public Health*. doi:https://doi.org/10.3390/ijerph18147533

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *5*(2). doi:https://doi.org/10.3390/bdcc5020023

Ali, F. (2019). In Quest of information security in higher education institutions : security awareness, concerns and behaviour of students. Retrieved from http://urn.fi/URN:ISBN:978-952-12-3879-6

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021, March 9). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Security*. doi:https://doi.org/10.3389/fcomp.2021.563060

Almeida, C., Kalinowski, M., Uchôa, A., & Feijó , B. (2023). Negative effects of gamification in education software: Systematic mapping and practitioner perceptions. *Information and Software Technology*. Retrieved from https://doi.org/10.1016/j.infsof.2022.107142

Alomair , Y., & Hammami, S. (2020). A review of methods for adaptive gamified learning environments. *International Conference on Computer Applications & Information Security*, 1-6. doi:10.1109/ICCAIS48893.2020.9096871

Alqahtani , H., & Kavakli-Thorne , M. (2020). Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR). *Information, 11*(2). doi:https://doi.org/10.3390/info11020121

Alqahtani , H., & Kavakli-Thorne, M. (2020, February 21). Gamification has emerged as a useful technique for increasing education and communication on themes like cybercrime. *Information, 2*(11). doi:https://doi.org/10.3390/info11020121

Alqahtani, H., & Kavakli, M. (2020). Exploring Factors Affecting User's Cybersecurity Behaviour by Using Mobile Augmented Reality App (CybAR). *International Conference on Computer and Automation Engineering*, 129-135. doi:10.1145/3384613.3384629

Amorim, J., Hendrix, M., Andler, S., & Gustavsson, P. (2013). *Gamified training for cyber defence: Methods and automated tools for situation and threat assessment. In NATO Modelling and Simulation Group (MSG).*

Amorosa, K., & Yankson, B. (2023). Human Error-A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education. *HOLISTICA–Journal of Business and Public Administration, 14*(1), 110-132. doi:DOI:10.2478/hjbpa-2023-0007

Anderson, J., Rainie , L., & Vogels, E. (2021). Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges. Retrieved from https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/02/PI_2021.02.18_New-Normal-2025_FINAL.pdf

Andrade, C. (2021). A Student's Guide to the Classification and Operationalization of Variables in the Conceptualization and Design of a Clinical Study: Part 1. *Indian Journal of Psychological Medicine, 43*(2), 177-179. doi:https://doi.org/10.1177/0253717621994334

Armstrong, G., Adam, S., Denize, S., & Kotler , P. (2014). *Principles of marketing.* Australia: Pearson Australia.

Azouz, O., & Lefdaoui, Y. (2018). Gamification design frameworks: a systematic mapping study. *In 2018 6th International Conference on Multimedia Computing and Systems (ICMCS)* (pp. 1-9). IEEE.

Barreto, C. F., & França, C. (2021). Gamification in Software Engineering: A literature Review. *Cooperative and Human Aspect of Software Engineering*.

Belanche , D., Casaló , L. V., & Flavián, M. (2021). Understanding influencer marketing: The role of congruence between influencers, products and consumers. *Journal of Business Research, 132*, 186-195. doi:https://doi.org/10.1016/j.jbusres.2021.03.067

Bitrián, P., Buil , I., & Catalán , S. (2021). Enhancing user engagement: The role of gamification in mobile apps. *Journal of Business Research, 132*, 170-185. doi:https://doi.org/10.1016/j.jbusres.2021.04.028

Bittner, J., & Schipper, J. (2014). Motivational effects and age differences of gamification in product advertising. *Journal of Consumer Marketing, 5*(31), 391-400. doi:https://doi.org/10.1108/jcm-04-2014-0945

Böckle, M., Micheel, I., Bick, M., & Novak, J. (2018). A Design Framework for Adaptive Gamification Applications. *Proceedings of the 51st Hawaii International Conference on System Sciences.* Retrieved from http://hdl.handle.net/10125/50038

Bokang, C. M., & Mapimele, F. (2019). *The cybercrime combating platform.* Pretoria: CSIR.

Borrás-Gené, O., Martínez-Núñez , M., & Martín-Fernández, L. (2019, July 26). Enhancing Fun through Gamification to Improve Engagement in MOOC. *Informatics*. Retrieved from https://scholar.google.co.za/scholar_url?url=https://www.mdpi.com/2227-9709/6/3/28/pdf&hl=en&sa=X&ei=SiADZLqMI5n0yAT_xK_ADg&scisig=AAGBfm2HxmRc-LOmCfj-TGeLsjfErCj1sA&oi=scholarr

Bossler, A., & Berenblum, T. (2019, November). Introduction: new directions in cybercrime research. *Journal of Crime and Justice, 42*, 495-499. doi:https://doi.org/10.1080/0735648X.2019.1692426

Boyce , M., Duma, K., Hettinger, L., Malone , T., Wilson , D., & Lockett-Reynolds , J. (2011, September). Human Performance in Cybersecurity: A Research Agenda. *SAGE JOURNALS, 55*, 1115-1119. doi:https://doi.org/10.1177/1541931213571086

Brandão, A., & Costa, A. (2021). Extending the theory of planned behaviour to understand the effects of barriers towards sustainable fashion consumption. *European Business Review*. doi:https://doi.org/10.1108/ebr-11-2020-0306

Buil-Gil, , D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during covid-19: a preliminary analysis in the uk. *European Societies*, S47-S59. doi:https://doi.org/10.1080/14616696.2020.1804973

Burke, B. (2021). *Gamify: How gamification motivates people to do extraordinary things.* Routledge.

Caldwell , M., Andrews, J., Tanay , T., & Griffin, L. (2020, August 5). AI-enabled future crime. *Crime Science*. doi:https://doi.org/10.1186/s40163-020-00123-8

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404821000821

Casula, M., Rangarajan, N., & Shields, P. (2021). The potential of working hypotheses for deductive exploratory research. *Quality & Quantity*, 1703-1725.

Charandura, K. (2022, May 13). *Cybersecurity in the Education Industry.* Retrieved from SNG Grant Thornton: https://www.grantthornton.co.za/Newsroom/cybersecurity-in-the-education-industry/

Chen, L., Jia, J., & Wu, C. (2023). Factors influencing the behavioral intention to use contactless financial services in the banking industry: An application and extension of UTAUT model. *Frontiers in Psychology, 13*. doi:https://doi.org/10.3389/fpsyg.2023.1096709

Cheong, C., & Park, M. (2020). The impact of gamification on consumer autonomy in learning experiences. *Journal of Consumer Behaviour, 4*(19), 345-362. doi:doi:10.1287/isre.2019.0899

Chigada, J., & Madzinga, R. (2021, February). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal Of Information Management*. doi:https://doi.org/10.4102/sajim.v23i1.1277

Chudasama, D., Patel, D., Shah , A., & Shaikh, N. (2021). Research on Cybercrime and its Policing. *American Journal of Computer Science and Engineering Survey, 8*. Retrieved from https://www.primescholars.com/articles/research-on-cybercrime-and-its-policing.pdf

Chung, A. (2017). A Critique and Defense of Gamification. *Journal of interactive online learning, 15*, 57-72. Retrieved from https://api.semanticscholar.org/CorpusID:64992003

Clark, T., Foster, L., Bryman, A., & Sloan, L. (2021). *Bryman's social research methods.* Oxford university press.

Cooksey, R. W. (2020). Descriptive Statistics for Summarising Data. Illustrating Statistical Procedures: Finding Meaning in Quantitative Data. 61–139. doi:doi: 10.1007/978-981-15-2537-7_5

Creswell, J. (2003). Research design: Qualitative, quantitative and mixed methods approaches.

Creswell, J. W. (2011). Controversies in mixed methods research. *The Sage handbook of qualitative research*, 269-284.

Deci, E., & Ryan, R. (2012). Handbook of theories of social psychology. (A. Van Lange, A. Kruglanski, & E. Higgins, Eds.) *American Psychology Association*, 416–436. doi:https://psycnet.apa.org/doi/10.4135/9781446249215.n21

Deeleman, J., & Van Steen, T. (2021). Successful Gamification of Cybersecurity Training. *Cyberpsychology, Behavior, and Social Networking*.

Deterding, S. (2019). Gamification in management: Between choice architecture and humanistic design. *Journal of Management Inquiry, 28*(2), 131-136.

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining" gamification". Retrieved from https://dl.acm.org/doi/abs/10.1145/2181037.2181040

Deterding, S., Khaled, R., Nacke, L., & Dixon, D. (2011). Gamification : Toward a Definition. 4. Retrieved from http://gamification-research.org/wp-content/uploads/2011/04/02-Deterding-Khaled-Nacke-Dixon.pdf

Di Leo, G., & Sardanelli, F. (2020). Statistical significance: p value, 0.05 threshold, and applications to radiomics—reasons for a conservative approach. *European Radiology Experimental*. doi:https://doi.org/10.1186/s41747-020-0145-y

Dignan, A. (2011). *Game frame: Using games as a strategy for success.* Free Press.

Dlamini, S., & Mbambo, C. (2019, October). Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. (W. Ma, Ed.) *Cogent Social Sciences, 5*(1). doi:https://doi.org/10.1080/23311886.2019.1675404

Durrani, U., Naymat, G., Ayoubi, R., Kamal, M., & Hussain, H. (2022). Gamified flipped classroom versus traditional classroom learning: Which approach is more efficient in business education? *The International Journal of Management Education, 20*(1). doi:https://doi.org/10.1016/j.ijme.2021.100595

Ezeh, P., Nzeakor, O., & Nwokeoma, B. (2020). Pattern of Cybercrime Awareness in Imo State, Nigeria: An Empirical Assessmen. *International Journal of Cyber Criminology*. Retrieved from https://www.proquest.com/docview/2404396076?pq-origsite=gscholar&fromopenview=true

Fanning, E. (2019). Formatting a paper-based survey questionnaire: Best practices. *Practical Assessment, Research, and Evaluation, 10*(1), 12.

Featherstone, M., & Habgood, J. (2019, July). UniCraft: Exploring the impact of asynchronous multiplayer game elements in gamification. *International Journal of Human-Computer Studies, 127*, 150-168. doi:https://doi.org/10.1016/j.ijhcs.2018.05.006

Ferrara, J. (2013). Games for persuasion: Argumentation, procedurality, and the lie of gamification. *Games and Culture, 8*(4), 289-304.

Ferrer, J., Ringer, A., Saville, K. A., & Parris, M. (2022). Students' motivation and engagement in higher education: The importance of attitude to online learning. *Higher Education, 83*(2), 317-338.

Fitz-Walter , Z. (2015). Achievement unlocked: Investigating the design of effective gamification experiences for mobile applications and devices. Retrieved from https://eprints.qut.edu.au/83675/1/Zac%20Fitz-Walter%20Thesis.pdf

Fitz-Walter, Z., Johnson, D., Wyeth, P., Tjondronegoro, D., & Scott-Parker, B. (2017). Driven to drive?Investigating the effect of gamification on learner driver behavior, perceived motivation and user experience. *Computers in Human Behavior, 71*, 586-595. doi:doi:10.1016/j.chb.2016.08.050

Flinton, D. M., & Malamateniou, C. (2020). Quantitative methods and analysis. *Medical Imaging and Radiotherapy Research: Skills and Strategies*, 273-322.

Flinton, D., & Malamateniou, C. (2020). Quantitative Methods and Analysis. doi:https://doi.org/10.1007/978-3-030-37944-5_15

Friedrich, J., Becker, M., Kramer, F., Wirth, M., & Schneider, M. (2020, January). Incentive design and gamification for knowledge management. *Journal of Business Research*, 341-352. doi:https://doi.org/10.1016/j.jbusres.2019.02.009

Garba, A., Maheyzah , B., Siti, H., & Dauda, I. (2020). Cyber Security Awareness Among University Students: A Case Study. 82–86.

Gary, R. (2016). Methodology of Research. *Indian Journal of Anaesthesia*, 642. doi:10.4103/0019-5049.190619

Gjertsen, E. G. (2016). Use of Gamification in Security Awareness and Training Programs.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security, 95*, 101827.

Hassan, L., & Hamari, J. (2019). *Gamification of e-participation: A literature review.*

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Goeke, L., Hildebrandt, T., Tsakirakis, G., . . . Koshutanski, H. (2020). Modern Aspects of Cyber-Security Training and

Continuous Adaptation of Programmes to Trainees. *Applied Sciences, 10*(16). doi:https://doi.org/10.3390/app10165702

Hernández-Fernández, A., Olmedo-Torre, N., & Peña, M. (2020). Is classroom gamification opposed to performance? *Sustainability, 12*, 9958.

Huang, L., & Zhu, Q. (2020). A dynamic games approach to proactive defense strategies against Advanced Persistent Threats in cyber-physical systems. *Computers & Security, 89*. doi:https://doi.org/10.1016/j.cose.2019.101660

Huotari, K., & Hamari, J. (2012). Defining Gamification: A Service Marketing Perspective. *In Proceeding of the 16th International Academic MindTrek Conference*, (pp. 17-22). New York.

Kaiser , K. (2009). Protecting Respondent Confidentiality in Qualitative Research. *Qualitative Health Research, 19*(11), 1632-1641. doi:10.1177/1049732309350879

Kalogiannakis , M., Papadakis, S., & Zourmpakis, A.-I. (2021). Gamification in Science Education. A Systematic Review of the Literature. *Education Sciences*, 36. Retrieved from https://files.eric.ed.gov/fulltext/EJ1283113.pdf

Kam, A. H., & Umar, I. N. (2018). Fostering authentic learning motivations through gamification: A self-determination theory (SDT) approach. *Journal of Engineering Science and Technology*.

Kankanhalli, G., Campello, M., & Muthukrishnan, P. (2020). *Corporate hiring under COVID-19: Labor market concentration, downskilling, and income inequality (No. w27208).* National Bureau of economic research.

Keating, X. D., Zhou, K., Liu, X., Hodges, M., Liu, J., Guan, J., & Castro-Piñero, J. (2019). Reliability and concurrent validity of global physical activity questionnaire (GPAQ): a systematic review. *International journal of environmental research and public health, 16*(21), 4128.

Khader , M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. Information. *10*(417). doi:https://doi.org/10.3390/info12100417

Khan, I., Melro, A., Carla Amaro, A., & Oliveira, L. (2022). Systematic Review on Gamification and Cultural Heritage Dissemination. *Journal of Digital Media &*

*Interaction*, 23. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4092507

Kim, T. W., & Werbach, K. (2016). More than just a game: ethical issues in gamification. *Ethics and Information Technology, 18*(2), 157-173.

Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour &Amp; Information Technology, 8*(41), 1796-1808. doi:https://doi.org/10.1080/0144929x.2021.1905066

Koivisto , J., & Hamari , J. (2019). The rise of motivational information systems: a review of gamification research. *International Journal of Information Management, 45*, 191-210. doi:10.1016/j.ijinfomgt.2018.10.013

Krath, J., Schürmann, L., & von Korflesch, H. (2021, December). Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning. *Computers in Human Behavior, 125*. doi:https://doi.org/10.1016/j.chb.2021.106963

Krosnick, J. A., Judd, C. M., & Wittenbrink, B. (2018). The measurement of attitudes. *In The handbook of attitudes, Volume 1: Basic principles*, 45-105.

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*.

Kumar, R. (2018). Research methodology: a step-by-step guide for beginners. *SAGE*.

Lampropoulos, G., Keramopoulos, E., & Diamantaras, K. (2023). Augmented reality and gamification in education: A systematic literature review of research, applications, and empirical studies. *Applied Sciences, 13*(12), 6809.

Leonardo Cavaliere, L. P., Subhash, N., Durga Rao, P. V., Koti , K., Chakravarthi, M. K., & Regin, R. (n.d.). The Impact of Internet Fraud on Financial Performance of Banks. *Turkish Online Journal of Qualitative Inquiry, 12*(6).

Li, Y., & Liu , Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Science Direct, 7*, 8176-8186. doi:https://doi.org/10.1016/j.egyr.2021.08.126

Liebrecht , C., Tsaousi , C., & van Hooijdonk, C. (n.d.). Linguistic elements of conversational human voice in online brand communication: Manipulations and perceptions. *Journal of Business Research, 132*, 124-135. doi:https://doi.org/10.1016/j.jbusres.2021.03.050

Loewen, S., Crowther, D., Isbell, D., Kim, K., Maloney, J., Miller, Z., & Rawal, H. (2019). *Mobile-assisted language learning: A Duolingo case study.* doi:https://doi.org/10.1017/S0958344019000065

Lopez, C. E., & Tucker, C. S. (2019). The effects of player type on performance: a gamification case study. *Computers in Human Behavior, 91*, 333–345. doi:https://doi.org/10.1016/j.chb.2018.10.005

Manzano-León , A., Camacho-Lazarraga, P., Guerrero, M. A., Guerrero-Puerta, L., Aguilar-Parra, J. M., Trigueros, R., & Alias, A. (2021). Between Level Up and Game Over: A Systematic Literature Review of Gamification in Education. *Sustainability, 13*(4), 2247. doi:https://doi.org/10.3390/su13042247

Marczewski, A. (2017). *Gamified UK*. Retrieved from Gamified UK: https://www.gamified.uk/2017/04/03/periodic-table-gamification-elements/

Martínez-Jiménez , R., Pedrosa-Ortega , C., Licerán-Gutiérrez, A., Ruiz-Jiménez MC, M., & García-Martí , E. (2021). Kahoot! as a Tool to Improve Student Academic Performance in Business Management Subjects. *Sustainability, 13*(5), 2969. doi:https://doi.org/10.3390/su13052969

Mathoosoothenen, V. N., Sundaram, J. S., Palanichamy, R. A., & Brohi, S. N. (2017). An integrated real-time simulated ethical hacking toolkit with interactive gamification capabilities and cyber security educational platform., (pp. 199-202). doi:https://doi.org/10.1145/3168390.3168397

Mazeas, A., Duclos, M., & Chalabaev, A. (2022). Evaluating the effectiveness of gamification on physical activity: systematic review and meta-analysis of randomized controlled trials. *Journal of medical Internet research, 24*(1), e26779.

Mcanyana , W., Brindley , C., & Seedat, Y. (2020). *Insight into the Cyberthreat landscape in South Africa, Accenture.* Accenture. Retrieved from https://wwww.accenture.com/za-en/insights/security/cyberthreat-south-africa

Mcanyana, W., Brindley, C., & Seedat, Y. (2020, June 10). *Insight into the cyberthreat landscape in South Africa.* Accenture. Accenture.

McIlwraith, A. (2021). *Information security and employee behaviour: how to reduce risk through employee education, training and awareness.* Routledge.

Mistry, D. (2020, September 18). *Kids are banking's future NOW*. Retrieved from Fintechfutures.com: https://www.fintechfutures.com/2020/09/kids-are-bankings-future-now/

Mitchell, G., Leonard, L., Carter, G., Santin, O., & Wilson, C. (2021). Evaluation of a 'serious game' on nursing student knowledge and uptake of influenza vaccination. *Plus One*. doi:https://doi.org/10.1371/journal.pone.0245389

Mitchell, R., Schuster, L., & Seung Jin, H. (2020). Gamification and the impact of extrinsic motivation on needs satisfaction: Making work fun? *Journal of Business Research, 106*. doi:https://doi.org/10.1016/j.jbusres.2018.11.022

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P., & Glenn, T. (n.d.). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Psychiatry in the Digital Age*. doi:https://doi.org/10.1007/s11920-021-01228-w

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P., & Glenn, T. (2021). ncreasing cybercrime since the pandemic: concerns for psychiatry. *Current Psychiatry Reports*. doi:https://doi.org/10.1007/s11920-021-01228-w

Mora, A., Riera, D., González, C., & Arnedo-Moreno, J. (2017). Gamification: a systematic review of design frameworks. *Journal of Computing in Higher Education, 29*, 516-548.

Morschheuser, B., Hassan, L., Werder, K., & Hamari, J. (2018). How to design gamification? A method for engineering gamified software. *Information and Software Technology*(95), 219-237.

Nacke, L. E., & Deterding, S. (2017). The maturing of gamification research. *Computers in Human Behavior, 71*, 450--454. doi:doi:10.1016/j.chb.2016.11.062

Naeem, M., & Ozuem, W. (2021). The role of social media in internet banking transition during COVID-19 pandemic: Using multiple methods and sources in qualitative research. *Journal of Retailing and Consumer Services, 60*, 102483.

Nayak, M. S., & Narayan, K. A. (2019). Strengths and weaknesses of online surveys. *Technology*.

Nelson, M. (2012). *Soviet and American Precursors to the Gamification of Work.* Retrieved from https://www.kmjn.org/publications/Gamification_MT12.pdf

Nelson, M. J. (2012). Soviet and American precursors to the gamification of work. *Proceeding of the 16th International Academic MindTrek Conference*, 23-26. doi:https://doi.org/10.1145/2393132.2393138

Nguyen, T., & Pham, H. (2020, October). A Design Theory-Based Gamification Approach for Information Security Training. In 2020 RIVF International Conference on Computing and Communication Technologies. *International*, 1 - 4.

Ning, H., Ye, X., Bouras , M., Dawei , W., & Mahmoud , D. (2018, March 13). General Cyberspace: Cyberspace and Cyber-Enabled Spaces. *Internet of Things Journal, 5*(3), 1843 - 1856. doi:10.1109/JIOT.2018.2815535

Nu Mai, N., Takahashi, Y., & Mon Oo, M. (2020). *Testing the Effectiveness of Transfer Interventions Using Solomon Four-Group Designs.* doi:https://doi.org/10.3390/educsci10040092

OECD. (2020). Tax Challenges Arising from Digitalisation – Report on Pillar One Blueprint: Inclusive Framework on BEPS. *OECD/G20 Base Erosion and Profit Shifting Project*. doi:https://doi.org/10.1787/beba0634-en

Ofosu-Ampong, K. (2020, April). The Shift to Gamification in Education: A Review on Dominant Issues. *Journal of Educational Technology Systems, 9*. Retrieved from https://journals.sagepub.com/doi/full/10.1177/0047239520917629

Olofinbiyi, S. (2022, June 28). A reassessment of public awareness and legislative framework on cybersecurity in South Africa. *ScienceRise: Juridical Science*. doi:https://doi.org/10.15587/2523-4153.2022.259764

Olukayode, O. (2021). An Appraisal of the Legal Framework for Online Banking in Nigeria and South Africa. *Journal of Commercial and Property Law*.

Oluwajana, D., Idowu, A., Nat, M., & Vanduhe, V. (2019). The adoption of students' hedonic motivation system model to gamified learning environment. *Journal of Theoretical and Applied Electronic Commerce Research, 3*(14), 156-167. doi:https://doi.org/10.4067/s0718-18762019000300109

Pacheco, J., Benítez, V., Félix-Herrán, L., & Satam, P. (2020). Artificial neural networks-based intrusion detection system for internet of things fog nodes. *8*, 73907-73918. doi:https://doi.org/10.1109/access.2020.2988055

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences, 2*(2). doi:https://doi.org/10.3390/forensicsci2020028

Pokhariyal, G. P. (2019). Pokhariyal, G.P. (2019). Importance of moderating and intervening variables on the relationship between independent and dependent variables.

Privitera, G. (2020). *Research Methods for the Behavioral Sciences.* Retrieved from https://toc.library.ethz.ch/objects/pdf03/e01_978-1-5063-2657-3_01.pdf

Rahi, S., & Ghani, M. (2019). Does gamified elements influence on user's intention to adopt and intention to recommend internet banking? *International Journal of Information and Learning Technology, 36*(1), 2-20. doi:https://doi.org/10.1108/ijilt-05-2018-0045

Rapp, A., Hopfgartner, F., Hamari, J., & Linehan, C. (2019). Strengthening gamification studies: Current trends and future opportunities of gamification research. *International Journal of Human-Computer Studies, 127*, 1-6. doi:https://doi.org/10.1016/J.IJHCS.2018.11.007

Rieb, A., Gurschler, T., & Lechner, U. (June 7-8, 2017). A gamified approach to explore techniques of neutralization of threat actors in cybercrime. . *In Privacy*

*Technologies and Policy: 5th Annual Privacy Forum, APF, Revised Sel.* Vienna, Austria,.

Riopel, M., Nenciovici, L., Potvin, P., Chastenay , P., Charland, P., Sarrasin, J., & Masson, S. (2019). Impact of serious games on science learning achievement compared with more conventional instruction: an overview and a meta-analysis. . *Studies in Science Education*, 169-214. doi:https://doi.org/10.1080/03057267.2019.1722420

Ryan, R., & Deci, E. (2005). Handbook of theories of social psychology. *American Psychological Association*, pp. 416 - 436.

SABRIC. (2020). SABRIC ANNUAL CRIME STATS 2020. Gauteng, South Africa. Retrieved from https://www.fic.gov.za/Documents/SABRIC%20Media%20Statement%20-%20Annual%20Crime%20Stats%202020.pdf

Sailer , M., & Homner , L. (2020). The Gamification of Learning: a Meta-analysis. *Educational Psychology Review*, 77–112. doi:10.1007/s10648-019-09498-w

Sailer , M., Hense, J., Mayr, S., & Mandl, H. (2017, April). How gamification motivates: An experimental study of the effects of specific game design elements on psychological need satisfaction. *Computers in Human Behavior*, 371-380. doi:https://doi.org/10.1016/j.chb.2016.12.033

Sailer, M., & Sailer, M. (2020). Gamification of in-class activities in flipped classroom lectures. *British Journal of Educational Technology, 1*(57), 75-90. doi:https://doi.org/10.1111/bjet.12948

Salahdine , F., & Kaabouch, N. (2019, April 2). Social Engineering Attacks: A Survey. *Future Internet, 11*(4). doi:https://doi.org/10.3390/fi11040089

Salahdine , F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet, 4*(11), 89. doi:https://doi.org/10.3390/fi11040089

SASSA. (2023). *Annual Performance Plan.* SOUTH AFRICAN SECURITY AGENCY. Retrieved from https://static.pmg.org.za/SASSA_2022-23_Annual_Performance_Plan.pdf#page=9

Saunders, M. N. (2012). Choosing research participants. Qualitative organizational research: Core methods and current challenges. 35-52.

Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students eight edition. *QualitativeMarket Research: An International Journal*.

Schmidt-Kraepelin, M., Thiebes, S., Stepanovic, S., Mettler, T., & Sunyaev, A. (2019). Gamification in Health Behavior Change Support Systems - A Synthesis of Unintended Side Effects. 15. Retrieved from https://serval.unil.ch/resource/serval:BIB_4B8751E9C432.P001/REF.pdf

Scholefield, S., & Shepherd, L. ( 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, Proceedings 21* (pp. 191 -203). Orlando, FL, USA,: Springer Inernational Publishing.

Shah, P., & Agarwal, A. (2020). Cybersecurity behaviour of smartphone users in india: an empirical analysis. *Information and Computer Security, 2*(28), 293-318. doi:https://doi.org/10.1108/ics-04-2019-0041

Skelton, E., Drey, N., Rutherford, M., Ayers, S., & Malamateniou, C. (2020). Electronic consenting for conducting research remotely: A review of current practice and key recommendations for using e-consenting. *International journal of medical informatics, 143*, 104271.

Smith, J., Johnson, A., & Lee, C. (2021). The Impact of Educational Games on Cybercrime Knowledge: A Comparative Study. *Journal of Cybersecurity Education, 2*(15), 45-58.

Stats SA. (2022). Statistic South Africa. Retrieved from https://census.statssa.gov.za/assets/documents/2022/Census_2022_SG_Presentation_10102023.pdf

Stommel, W., & Rijk, L. D. (2021). Ethical approval: none sought. How discourse analysts report ethical issues around publicly available online data. *Research Ethics, 17*(3), 275-297.

Taherdoost, H. (2013). Sampling Method in Research Methodology; How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management, 5*(2), 18 -27. doi:10.2139/ssrn.3205035.

Thenga, Aluwani. (2020, September 10). *Rand Merchant Bank*. Retrieved from RMB: https://www.rmb.co.za/news/ecommerce-to-be-worth-r225bn-in-sa-in-5-years

Thomala, L. L. (2023). *fitness industry in China 2023.* Statista. Statista. Retrieved from https://www.statista.com/study/63475/fitness-industry-in-china/

Thompson, L. A., Melendez, N., Hempson-Jones, J., & Salvi, F. (2022). Gamification in Cybersecurity Education: The RAD-SIM Framework for Effective Learning. Retrieved from https://papers.academic-conferences.org/index.php/ecgbl/article/view/504

Tondello, G. F., Mora, A., & Marczew, A. (2019). Empirical validation of the Gamification User Types Hexad scale in English and Spanish. *International Journal of Human-Computer Studies, 127*, 95-111. doi:https://doi.org/10.1016/j.ijhcs.2018.10.002

Tondello, G. F., Mora, A., Marczewski, A., & Nacke, L. E. (2018). Empirical validation of the Gamification User Types Hexad Scale. *International Journal of Human-Computer Studies, 127*(95), 95-111. doi:https://doi.org/10.1016/j.ijhcs.2018.10.002

Torres-Toukoumidis, A., Carrera, P., & Balcázar, I. (2021). Descriptive Study of Motivation in Gamification Experiences from Higher Education: Systematic Review of Scientific Literature. *Universal Journal of Educational Research*. doi:https://doi.org/10.13189/UJER.2021.090403

Vesa, M. (2021). Organizational Gamification: Theories and Practices of Ludified Work in Late Modernity. Routledge. Retrieved from https://books.google.co.za/books?id=WnwSEAAAQBAJ&pg=PA121&lpg=PA121&dq=research+on+%22negative+consequences+of+gamification%22&source=bl&ots=Nv4ik3aG9i&sig=ACfU3U0XTt1aW_IC0d7tTxoypYFNNmcqUA&hl=en&sa=X&ved=2ahUKEwimye3cj8L9AhUKB8AKHSPGANc4FBDoAXoECCEQAw

Warmelink, H., Koivisto, J., Mayer, I., & Vesa, M. (2020). Gamification of production and logistics operations: Status quo and future directions. *Journal of business research, 106*, 331-340.

Welbers, K., Konijn, E. A., Burgers, C., de Vaate, A. B., Eden, A., & Brugman, B. C. (2019). Gamification as a tool for engaging student learning: A field experiment with a gamified app. *E-Learning and Digital Media, 16*(2), 92-109. doi:https://doi.org/10.1177/2042753018818342

Wiener, N. (2019). *Cybernetics or Control and Communication in the Animal and the Machine.* Th MIT Press.

Yamani, H. A. (2021). A Conceptual Framework for Integrating Gamificationin eLearning Systems Based on Instructional. *International Journal of Emerging Technologies in Learning (iJET), 16*(4), 14-33. doi:https://doi.org/10.3991/ijet.v16i04.15693

Yen, B. T., Mulley, C., & Burke, M. (2019). Gamification in transport interventions: Another way to improve travel behavioural change. *Cities, 85*, 140-149.

Yoo, C., Kwon, S., Na, H., & Chang, B. (2017). Factors Affecting the Adoption of Gamified Smart Tourism Applications: An Integrative Approach. *Mobile Technology and Smart Tourism Development, 9*(12). doi:https://doi.org/10.3390/su9122162

Zennaro, F. M., & Erdődi, L. (2023). ). Modelling penetration testing with reinforcement learning using capture-the-flag challenges: Trade-offs between model-free learning and a priori knowledge. *IET Information Security, 17*(3), 441-457.

Zhang, T., Jahromi, M., Hua, N., & Lu, L. (2020). Engaging customers with hospitality brandsin social commerce activities. *Journal of Hospitality and Tourism Technology*. doi:https://doi.org/10.1108/jhtt-04-2019-0056

Zichermann , G., & Linder, J. (2021). *Gamification.*

Zichermann, G., & Cunningham, C. (2011). *Gamification by design: Implementing game mechanics in web and mobile apps.* O'Reilly. Retrieved from https://books.google.co.za/books?hl=en&lr=&id=zZcpuMRpAB8C&oi=fnd&pg=PR7&dq=Zichermann+G.,+Cunningham+C.+(2011).+Gamification+by+desig

n:+Implementing+game+mechanics+in+web+and+mobile+apps.+O%E2%80%99Reilly+Media.&ots=UvRc-Zza6f&sig=Wn737RLWvDbQ2zV9CieJBte

Zimmermann , V., & Renaud , K. (2019, November). Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. *International Journal of Human-Computer Studies*(131), 169-187. doi:https://doi.org/10.1016/j.ijhcs.2019.05.005

Zoto, E., Kowalski, S., Lopez-Rojas, E., & Kianpour, M. (2018). Using a socio-technical systems approach to design and support systems thinking in cyber security education. *CEUR Workshop Proceedings*, 6.

Zwilling, M., Klien, G., Lesjakb , D., Wiechetekc , L., Cetin, F., & Nejat Basim, H. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82-97. doi:https://doi.org/10.1080/08874417.2020.1712269

## Appendices

- List of tables
- Survey instrument
- List of figures

## List of tables

### Table 2.1: Identified research gaps

| Author name and year | Conceptual discussion | Research gap | Research question |
|---|---|---|---|
| Loewen et al. (2019) | The study aimed to evaluate nine Turkish-learning students on Duolingo for a semester, their language skills and the relationship between app use and improvement. It also sought participants' opinions on their experiences with the app. It also aimed to address research gaps by examining widely used language apps like Duolingo for second language acquisition. | The research underscores the lack of independent studies assessing the efficacy of mobile-assisted language learning platforms, notably with respect to widely used commercial apps for second language acquisition like Duolingo. | To investigate the effectiveness of Duolingo for second language (L2) acquisition. |

| | | | |
|---|---|---|---|
| Salahdine and Kaabouch (2019) | The paper discusses the diverse social engineering strategies including but not limited to baiting, phishing, pretexting and quid pro quo, and explores the strategies for detecting and averting such attacks. It also highlights the limitations of existing social engineering detection methods and its countermeasures for such attacks. | The lack of effective strategies to cope with the ever-growing number of social engineering attacks. | The study focused on the following research questions:<br>-What are social engineering attacks & how can they be classified?<br>-What current detection strategies exist for social engineering attacks?<br>-What are the limitations of the current detection methods and countermeasures for social engineering attacks?<br>- Which measures should be implemented to safeguard against social engineering attacks? |

| | | | |
|---|---|---|---|
| Zimmermann and Renaud (2019) | The way cybersecurity is currently conceptualised and the need for a mindset change | There is no explicit mention of a research gap in the paper, however, the paper proposes a new mindset called "Cybersecurity, differently", acknowledging the constructive role humans can play as "part of the solution" rather than "the problem" in organisational cybersecurity. | What constitutes the core challenges in cybersecurity and how does the prevalent mindset affect personal reactions to cybersecurity issues? |

| | | | |
|---|---|---|---|
| Scholefield and Shepherd (2019) | The implementation of gamification strategies aimed to enhance user awareness of password security and boost overall security consciousness while simultaneously incorporating diligent planning and feedback to guarantee the effectiveness of these techniques in an educational setting. | - No assessment was performed regarding the long-term retention of knowledge about password security and only a limited sample size was utilised.<br>-Gender differences were not investigated; demographic participant questionnaire was not factored. Prior research indicates that males generally favour game-based learning over females. This implies that the application of password security may need to be adapted to increase its appeal to a broader audience. | What is the efficacy of using gamification approaches in enhancing password security behaviours among everyday users to boost their cybersecurity awareness? |
| Deeleman and Van Steen (2021) | Whether video game, designed based on prior research and expert advice, can improve participant performance on the Theory of Planned Behaviour (TPB) components? | Investigation into the effectiveness of gaming on different target groups to address cybersecurity. | Does the Theory of Planned Behaviour model, which includes personal attitudes, subjective norms, and behavioural intentions, apply to understanding how gamification influences cybersecurity behaviour? |

| | | | |
|---|---|---|---|
| Scholefield and Shepherd (2019); Thompson et al. (2022) | The paper discusses the RAD-SIM framework, which integrates behavioural and psychological principles as well as learning theories to enhance game-based cybersecurity education. | Evaluate the effectiveness of gamified approaches versus traditional methods in improving educational results across different fields. | What are the most effective methods for leveraging gamification to train individuals in recognising and mitigating socially engineered cyber threats? |
| Scholefield and Shepherd (2019); Rieb et al., (2017) | Factors influencing gamification in promoting cybersecurity awareness. | | What are the factors influencing gamification effectiveness in promoting awareness among consumers of cybersecurity and the prevention of cybercrime? |

## Table 2.2: Relationship between constructs

| Construct | Interpretation | Measure | References |
|---|---|---|---|
| Autonomy | The extent to which consumers feel they possess autonomy and influence within their learning experience facilitated by gamified elements. | Duration of the user engagement on the game, average test scores of users, number of users who reported improving their knowledge or skill and number of users who felt motivated, a percentage of users who were able to complete and answer questions correctly | Cheong and Park (2020 |
| Competence | The level at which consumers believe they are equipped with | Ability to identify and respond to cybersecurity threats, the consumer's | Kankanhalli et al. (2020) |

| | | | |
|---|---|---|---|
| | the appropriate knowledge and skills to interact with the gamified content on cybercrime education | success in completing the gamified content, knowledge retention. | |
| Relatedness | The degree to which consumers perceive they related to others and are receiving support and feedback through the gamified cybercrime education content | How well is the user retaining the information, how enjoyable was the game, and how relevant is the content? | Sailer and Sailer (2020) |
| Perceived usefulness | The degree to which consumers perceive that the gamified cybercrime education content is useful in improving their knowledge and awareness of cybercrime. | Knowledge & awareness (pre- and post-game testing), engagement (number of participants in and duration of the game), how useful are the gamified content and customer feedback? | Oluwajana et al. (2019) |
| Behavioural intention | The degree to which consumers intend to engage in safe cybersecurity behaviours due to participation in gamified cybercrime education. | Perception of cybercrime, adoption of cybersecurity prevention measures, level of trust in online digital banking platforms. | Kimpe et al. (2021) |

**Table 4.1: Chi-square p-values for sample characteristics/demographics**

| | | Played an educational game | | Total (n=248) | P-value |
|---|---|---|---|---|---|
| **Variable** | **Options** | **Yes (n=77)** | **No (n=171)** | | |
| | Mobile Application | 77.9% | 75.4% | 76.2% | .426 |

| | | | | | |
|---|---|---|---|---|---|
| Q1. Most often used way to conduct banking needs | Internet Banking | 5.2% | 9.9% | 8.5% | |
| | Branch | 0.0% | 1.2% | 0.8% | |
| | Cellphone banking | 16.9% | 13.5% | 14.5% | |
| Q13. Gender | Male | 36.4% | 40.0% | 38.9% | .462 |
| | Female | 62.3% | 57.1% | 58.7% | |
| | Non-binary / third gender | 1.3% | 0.6% | 0.8% | |
| | Prefer not to say | 0.0% | 2.4% | 1.6% | |
| Q15. Highest level of education | Completed high school | 6.5% | 9.9% | 8.9% | .775 |
| | Completed a diploma | 11.7% | 16.4% | 14.9% | |
| | Completed university degree | 27.3% | 26.9% | 27.0% | |
| | Completed postgraduate degree | 32.5% | 29.2% | 30.2% | |
| | Completed master's degree | 20.8% | 15.8% | 17.3% | |
| | Completed a doctoral degree | 1.3% | 1.8% | 1.6% | |
| Q16. Income | Less than R14999 | 4.0% | 15.3% | 11.8% | .049 |
| | R15000 - R25999 | 8.0% | 12.9% | 11.4% | |
| | R26000 - R39999 | 10.7% | 12.4% | 11.8% | |
| | R40000 - R59999 | 17.3% | 18.8% | 18.4% | |
| | R60000 and above | 46.7% | 31.8% | 36.3% | |
| | Do not wish to disclose | 13.3% | 8.8% | 10.2% | |
| Q17. I have a South African bank account? | Yes, a personal bank account | 72.7% | 68.4% | 69.8% | .644 |
| | Yes, a business bank account | 0.0% | 1.2% | 0.8% | |
| | Yes, I have both business and personal | 26.0% | 27.5% | 27.0% | |
| | No, I don't have a bank account | 1.3% | 2.9% | 2.4% | |

**Table 4.2: Comparing results by whether a respondent played the game**

| | | Played an educational game | | Total (n=248) | P-value |
|---|---|---|---|---|---|
| **Variable** | **Options** | **Yes (n=77)** | **No (n=171)** | | |
| Q2. Your knowledge on cybercrime? | Mean score | 8.22 | 6.56 | 7.07 | .000 |
| Q7. Which online safety topics would interest you in a game? Choose two. | Using strong passwords, updating software, and being cautious when sharing personal information online | 61.0% | 52.6% | 55.2% | .270 |
| | Vishing: criminals impersonate legitimate companies via phone calls to obtain personal information from unaware consumers | 57.1% | 52.6% | 54.0% | .582 |
| | Phishing: a technique used by cyber criminals to deceive individuals into unknowingly installing malicious software by clicking on hyperlinks | 51.9% | 37.4% | 41.9% | .037 |
| | Safe online banking hygiene factors | 24.7% | 25.1% | 25.0% | 1.000 |
| Q8. If you had or have played a game to increase your understanding of cybersecurity threats, which aspect of the game would be most important? | Quizzes | 40.3% | 36.8% | 37.9% | .672 |
| | Simulation of real-world examples | 79.2% | 70.2% | 73.0% | .165 |
| | Tips or educational content | 50.6% | 33.3% | 38.7% | .011 |
| | Dangers of using public Wi-Fi | 33.8% | 35.7% | 35.1% | .886 |

**Research instrument**

**Gamification to educate consumers about cybercrime in South Africa**

Hello, my name is **Kehilwe** "**Kelly" Maselo**, and I am a Master of Business Administration (MBA) student at Wits Business School. Under the supervision of Professor Gregory John Lee, I am conducting a research study titled "Gamification to educate consumers about cybercrime in South Africa". The aim of the study is to explore the impact of gamification on consumer knowledge and attitudes towards cybercrime in South Africa. The rising adoption of digital platforms has heightened the danger associated with digital banking fraud. Consumers face challenges due to their lack of knowledge and skills, and their limited understanding of the risks and consequences of cybercrime or how to protect themselves from online threats.

I would greatly appreciate your participation in the survey, which should take 5–10 minutes of your time. Your involvement in this survey is entirely voluntary and comes with no personal costs or direct benefits. Your responses are anonymous and confidential. You have the right to withdraw at any time without providing a reason, and your decision to participate or not will not affect your relationship with Wits Business School or any affiliated organizations. Your data will only be used for research purposes.

**Important to note:**

Your demographic data does not allow for anyone to be identified, it's strictly anonymous.

*__Gamification__ uses game examples, components, and concepts in a non-game context to stimulate motivation, engagement, and user behaviour. *__Cybercrime__ refers to the use of a computer as a tool to advance unlawful activities, including engaging in fraudulent activities, perpetrating identity theft, or infringing upon an individual's privacy.

Thank you for your participation.

**Do you consent to participating in this study and having your answers used for research purposes?**

1. Yes
2. No

**Q1 - In order to understand your banking behaviour better, which of the following do you use most often to conduct your banking needs?**

- Mobile Application
- Internet Banking
- Branch
- Cellphone banking

**Q2 - On a scale of 1 to 10, with 1 being very low and 10 being very high, how would you rate your knowledge on cybercrime?**

**Q3 - Have you played an educational game meant or designed to teach you about cybercrime education?**

- Yes
- No

**Q4 - What have you found to be the most effective way for you to learn while playing a game?**

- I learn more if I score points or get rewards.
- I learn more from tips.
- I learn equally from both.
- I learn more from failing.

**Q5 - Please choose a statement(s) that resonates with you.**

- Playing a game improves my cyber hygiene knowledge and habits
- I have a cautious attitude
- I am confident in advising others about cybercrime education such as scams & tricks
- My bank has equipped me with the necessary information to avoid falling victim to scams

**Q6 - In your opinion, to what extent would online safety game effectively teach people about cyber-crimes, including avoiding scams and tricks?**

- Definitely effective

- Might or might not
- Not effective

**Q7 - Which online safety topics would interest you in a game? Choose two.**

- Using strong passwords, updating software, and being cautious when sharing personal information online
- Vishing: criminals impersonate legitimate companies via phone calls to obtain personal information from unaware consumers
- Phishing: a technique used by cybercriminals to deceive individuals into unknowingly installing malicious software by clicking on hyperlinks
- Safe online banking hygiene factors

**Q8 - If you had or have played a game to increase your understanding of cybersecurity threats, which aspect of the game would be most important?**

- Quizzes
- Simulation of real-world examples
- Tips or educational content
- Dangers of using public WiFi

**Q9 - If an online safety game made you aware of risks, how likely are you to change your behaviour?**

- Extremely unlikely
- Neither likely nor unlikely
- Extremely likely

**Q10 - Have you ever been a victim of online banking fraud, such as scams or tricks, after being exposed to the game?**

- Yes
- No

**Q11 - What would make you want to play a game about online safety to change your online banking behaviour?**

- Playing with friends

- Nice designs and pictures
- Competing for points, rewards or having a leader board
- Duration of the game
- Other

**Q12 - Do you have any suggestions or ideas for banks to improve their online safety programmes or educational initiatives?**

**Q13 - In order to assist with the analysis of the results, please complete the following demographic analysis: Gender**

- Male
- Female
- Non-binary/third gender
- Prefer not to say

**Q14 – Age group (please indicate the year you were born)**

**Q15 – Highest level of education**

Completed high school

Completed a diploma

Completed university degree

Completed postgraduate degree

Completed master's degree

Completed a doctoral degree

**Q16 - Income range**

- Less than R14 999
- R15 000 – R25 999
- R26 000 – R39 999
- R40 000 – R59 999
- R60 000 and above
- Do not wish to disclose

**Q17 – Do you have a South African bank account?**

- Yes, a personal bank account
- Yes, a business bank account
- Yes, I have both business and personal
- No, I don't have a bank account

## List of Figures

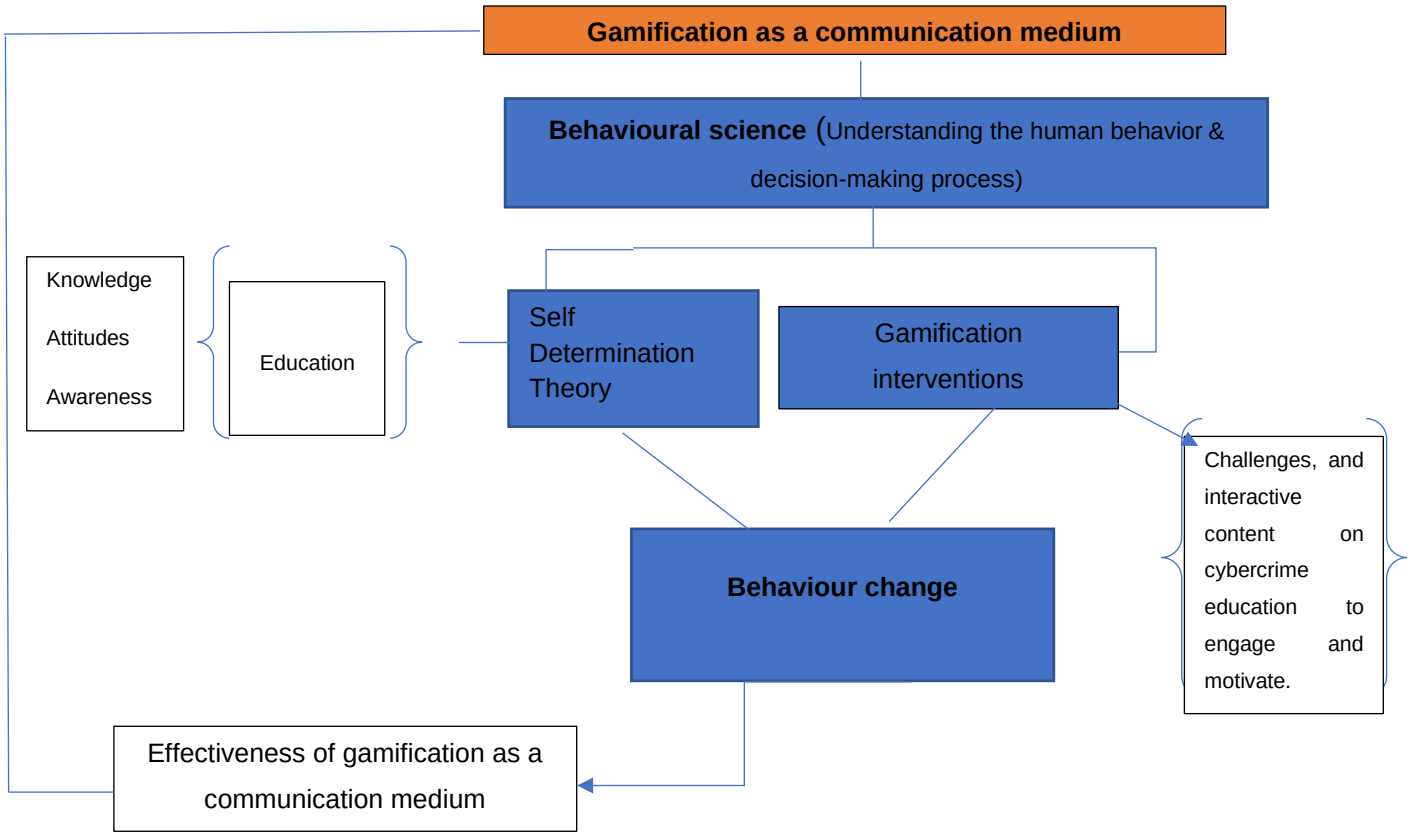



**Figure 2.1: Proposed conceptual framework of *determining the effectiveness of gamification in boosting knowledge, shifting attitudes, and adjusting behaviours* (*Author's compilation*)**

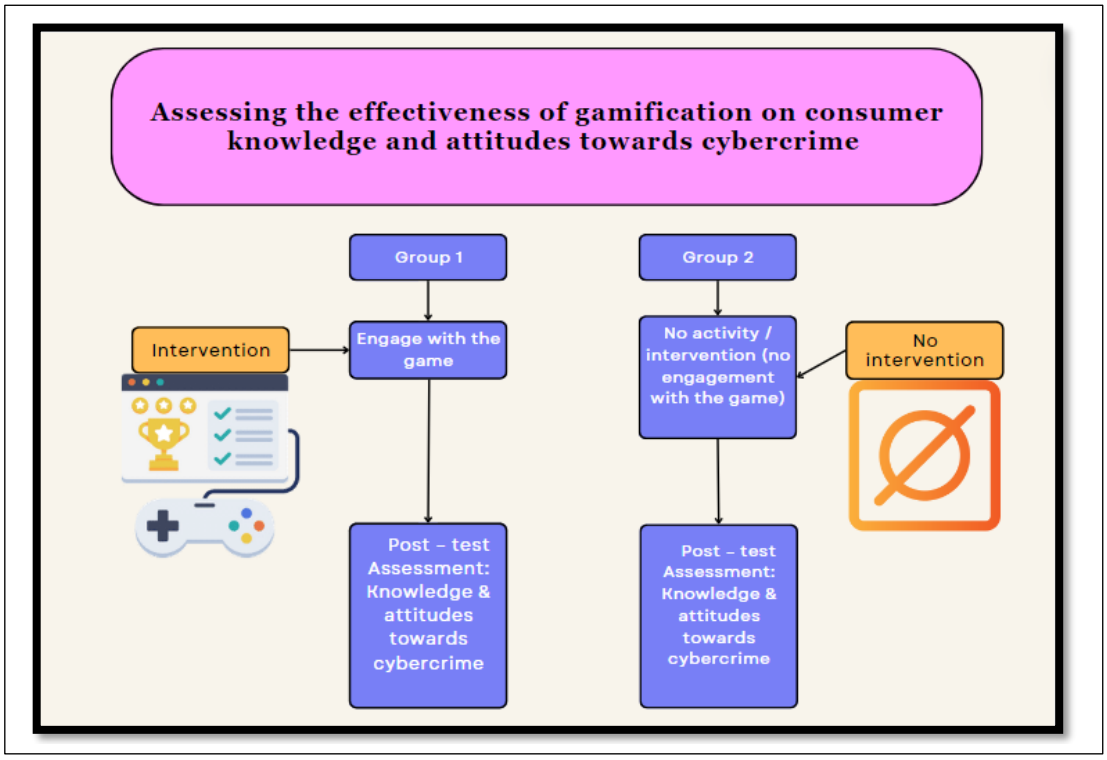



**Figure 3.1: Effectiveness of gamification (*Author's compilation)***

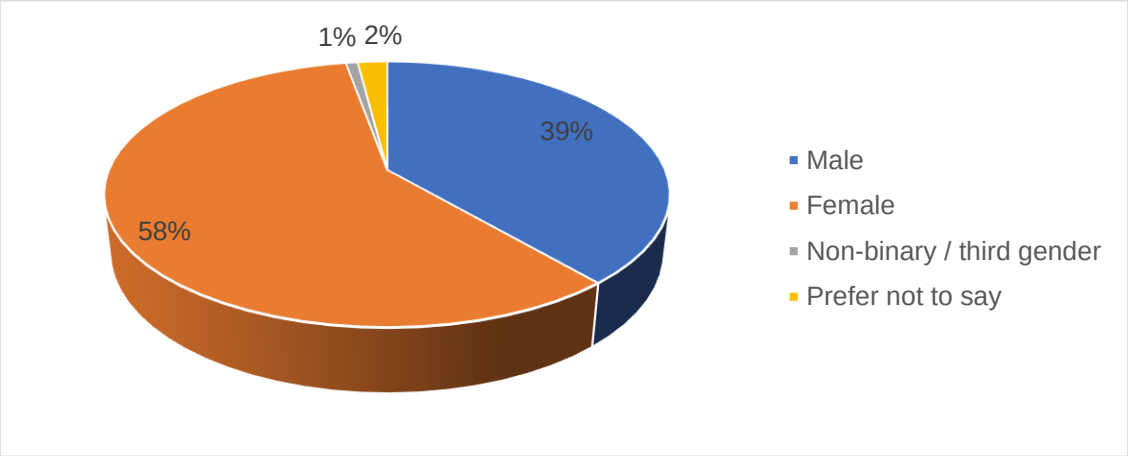



**Figure 4.3: Respondent gender**

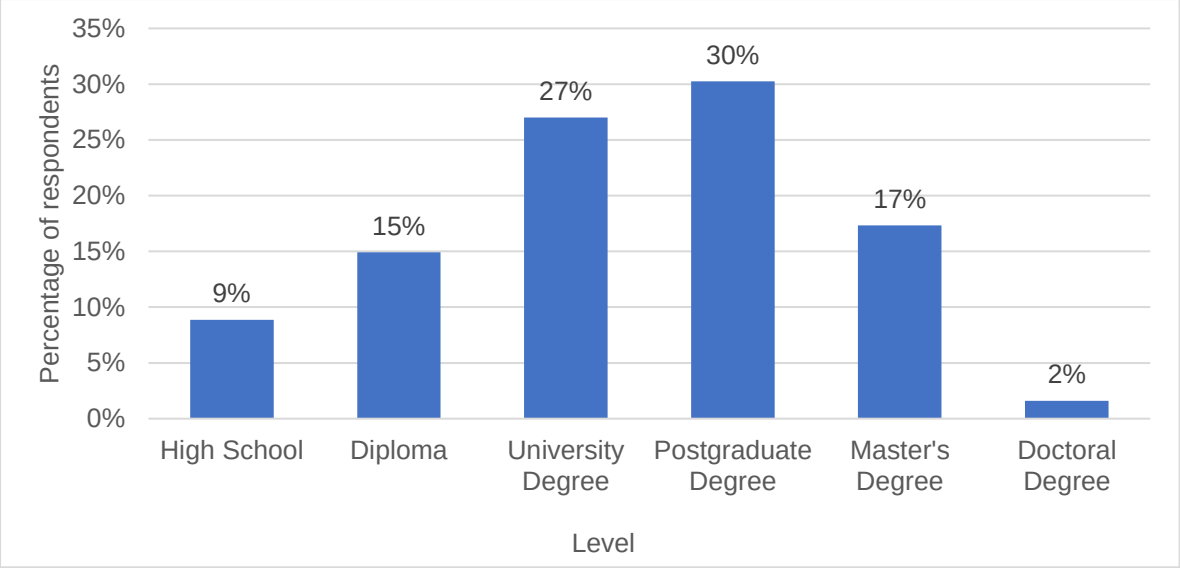



**Figure 4.4: Highest level of education completed.**

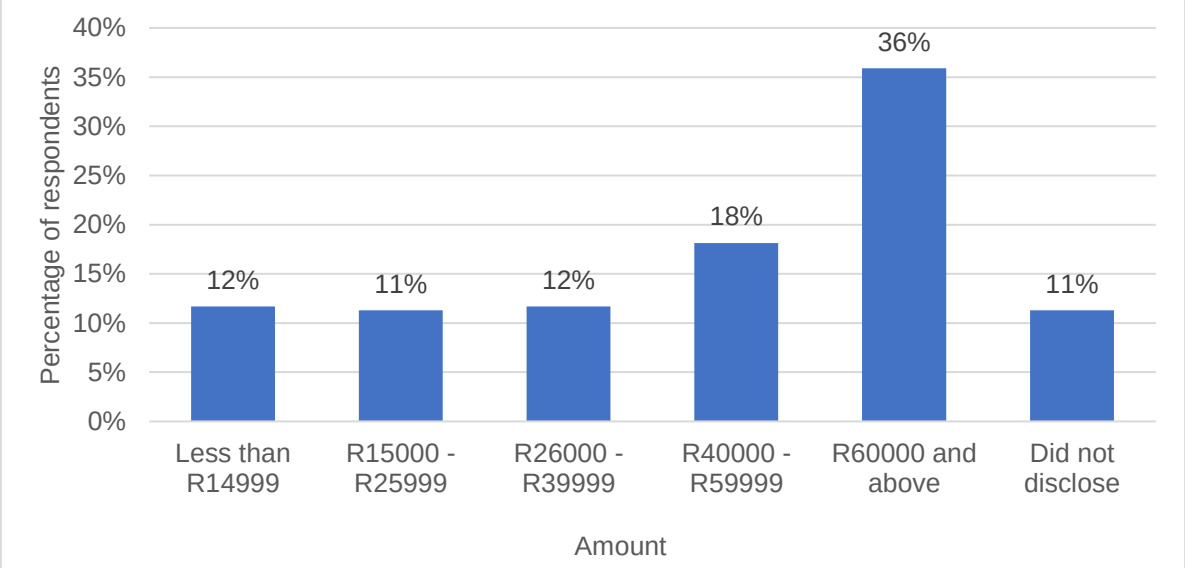



**Figure 4.3: Respondent income**

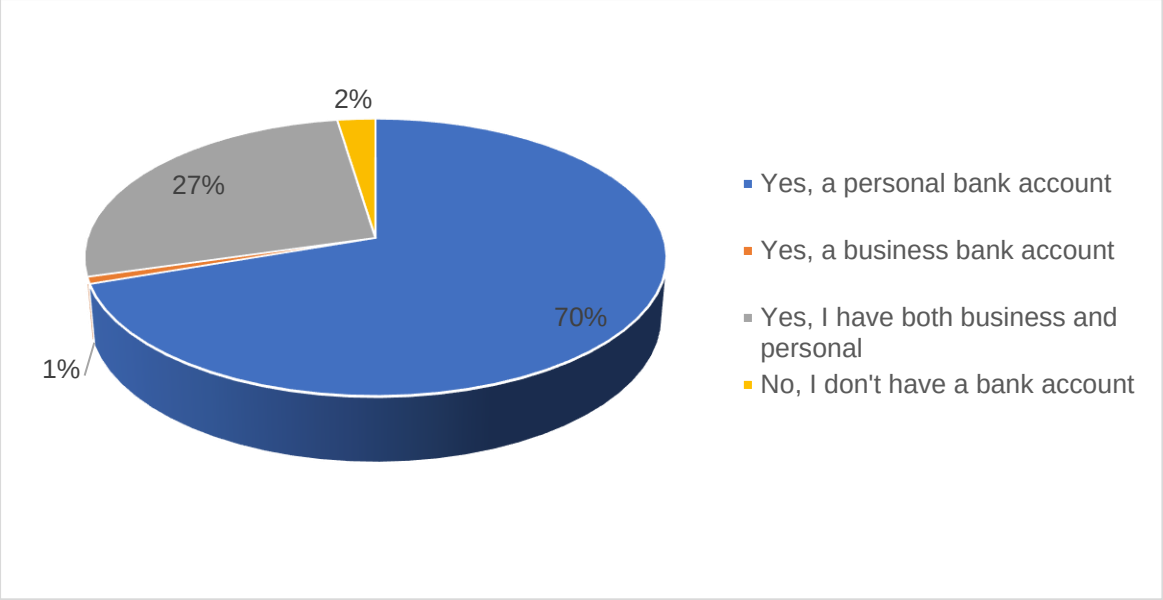



**Figure 4.4: Owing a bank account in SA.**

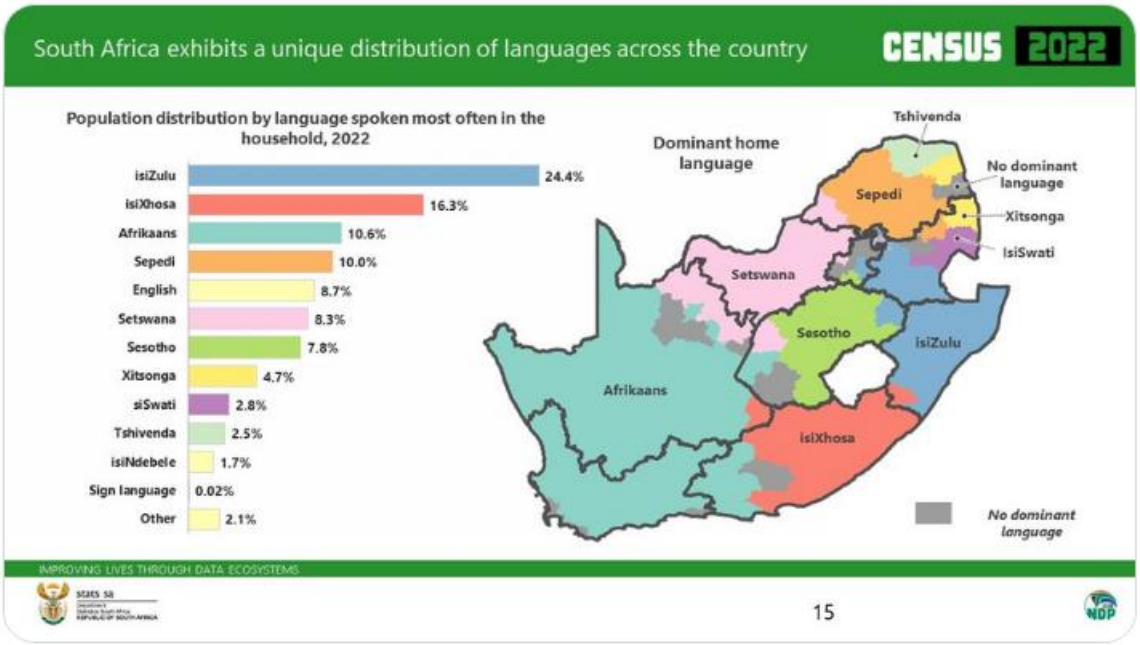



**Figure 5.1: South African linguistic landscape**