Research Article

Global Media Journal
ISSN 1550-7521

2025
Vol.23 No.78:521

Understanding Cybercrime and Its Effects on the Social Networking Site Usage Among Bahraini Youth

Kamel Gharbi*

Assistant Professor, University of Bahrain, Kingdom of Bahrain

***Corresponding author:**
Kamel Gharbi

kgharbi@uob.edu.bh

Assistant Professor, University of Bahrain, Kingdom of Bahrain

Citation: Gharbi, K. (2025). Understanding Cybercrime and Its Effects on the Social Networking Site Usage Among Bahraini Youth. Global Media Journal, 23:78.

Abstract

This study examines the awareness, perceptions, and lived experiences of cybercrime among Bahraini youth and their implications for the use of social networking sites. As digital engagement rises globally, young users are increasingly exposed to online threats, yet their awareness and protective behaviors vary significantly. Using a qualitative research design, this investigation conducted focus group discussions with 22 university students in Bahrain to explore their understanding of cyber risks, personal exposure to cybercrime, and resultant behavioral adaptations.

Findings reveal that while participants widely recognize the prevalence of cyber threats, including spam, phishing, and identity theft, their perceived vulnerability varies with factors such as parental supervision, digital literacy, and prior negative experiences. Thematic analysis identified two core themes: (1) Perceived Cybersecurity Knowledge and Awareness, highlighting divergent attitudes toward the necessity of formal cybersecurity education, and (2) Exposure to Cybercrime and Behavioral Responses, underscoring emotional and practical reactions to online victimization.

The study applies the Technology Acceptance Model (TAM) to interpret how perceived usefulness, ease of use, and emotional factors shape youths' adoption of protective online behaviors. Results indicate that cybersecurity practices are more likely to be adopted when they are viewed as both beneficial and manageable. The research concludes with practical recommendations for designing tailored, emotionally resonant, and context-aware cybersecurity education programs in Bahrain to foster proactive digital safety among youth.

Keywords: Cybercrime; Cybersecurity Awareness; Bahraini Youth; Social Networking Sites; Technology Acceptance Model (TAM); Qualitative Research

Received: 02-Dec-2025; Manuscript No. gmj-25-178054; **Editor assigned:** 04-Dec-2025; Pre QC No. gmj-25-178054; **Reviewed:** 18-Dec-2025; QC No. gmj-25-178054; **Revised:** 23-Dec-2025; Manuscript No. gmj-25-178054 (R); **Published:** 30-Dec-2025, DOI: 10.36648/1550-7521.23.78.521

Introduction

Currently, cybercrime is pervasive due to the multitude of internet-related activities. Cybercrime transcends temporal constraints and geographical limitations; it is perpetually accessible online from any location to everyone. Although the internet and cyberspace facilitate daily tasks, individuals do not consistently apply the same level of protection as they do in the physical world. Cyberspace has facilitated a new realm in which crime is increasingly prevalent, as cybercrime lacks specified locations or times and possesses no geographical limitations Ajayi, 2016. Corporations and governmental entities frequently experience cybercrime aimed at information leakage, data theft, and cyber espionage, while insufficient attention is given to the individuals impacted by these attacks. Although individuals are not necessarily the principal targets of cybercrime, they may become indirect victims Ayaz, 2018.

The advancement of information technology and the proliferation

of cybercrimes have recently heightened global interest in this phenomenon, as evidenced by conferences, conventions, research, and studies. This phenomenon has raised awareness in contemporary communities regarding the potential dangers, possible losses, and infringements on personal privacy it may entail Heinl, 2016.

This singular offense necessitates individuals successfully employing computer software and hardware to perpetrate crimes by forcefully accessing private networks and inflicting diverse harms upon them. Cybercrimes can impact individuals and perhaps escalate threaten national security, high authority, and sovereignty Bukart, 2017. Cybercrime encompasses any offenses related to computers and information technology, as well as any misconduct that may adversely impact individuals or groups with criminal intent or the aim to exploit, injure, or cause damage, whether directly or indirectly. Cybercrimes have garnered the attention of specialist organizations that recognize the significant harm they may inflict and the ease with which they can be perpetrated, prompting efforts to prioritize prevention and integrate it as a central concern within society Weijer, 2017.

Cybercrimes encompass several categories, which are classified into two areas. The first group pertains to communications, involving damage to devices, networks, and information, as well as scandals, hacking, defamation, fraud, the dissemination of viruses, and software destruction. The second group includes non-communication issues, such as stealing information, violating intellectual property laws, stealing money, illegally copying documents, attacking banks, spreading false information, and other crimes that harm society [1].

The proliferation of this problem, along with the availability of current information technology for criminal purposes, now jeopardizes national security by potentially undermining security measures. The situation is further complicated by the fact that cybercriminals do not need to be physically present to perpetrate these offenses; they merely require a computer and the skills to transmit harmful files and gather necessary information via private networks, rendering them difficult to trace and monitor [1].

Thus, it is vital to understand cybercrime and its software to identify its risks and potential losses, as well as the offenders' traits and motives. This understanding is essential for implementing appropriate measures to address the social, economic, and security implications of such crimes Jung, 2018.

These dangers pose a threat to societies and future generations, especially children and adolescents. Their unrestrained use of this technology and online networks, without oversight or regulation, renders them vulnerable to cybercrimes and harm. The lack of experience among most internet users exacerbates the situation, making them vulnerable to cyber victimization Ayaz, 2018.

Information technology and computerization represent some of the most significant accomplishments of contemporary science, as they have yielded numerous advantages in human development, alongside advancements in economic, educational, medical, and various other domains impacting humanity Alrasheedi, 2011. These accomplishments, however, were followed by adept criminals proficient in information technology software, capable of perpetrating cybercrimes using previously nonexistent creative tactics and strategies Lukatsky, 2003. Nations, companies, and powerful organizations must see cybercrime as a major issue that can harm society and create strong laws and rules to effectively handle and control these crimes.

Cybercrime results from inadequate cybersecurity, which is a perspective on digital security concerns that highlights the types of hazards that inflict substantial damage. These dangers may result in significant repercussions, including personal, societal, and financial harm Johnson, 2016. As ethical standards diminish in cultures, the incidence of cybercrimes has escalated throughout the years, adversely impacting our communities due to insufficient cybersecurity understanding Aiken, 2016. Organizations, governments, and esteemed authorities strongly advise enhancing cybercrime knowledge among youth, especially in high schools and colleges. Ossip, 2017. The primary objective of this research is to enhance knowledge of critical worldwide issues, including data privacy, among the youth, especially high school and university students in the Kingdom of Bahrain.

The Technology Acceptance Model (TAM), introduced by Davis in 1986, has become the preeminent framework for evaluating the acceptability and adoption of information and communication technologies (ICTs) Hsiao & Yang, 2011. This model seeks to predict and elucidate the adoption or non-adoption of an ICT by examining variables associated with perceptions (perceived utility [UP] and perceived ease of use [FUP]) and attitudes [A], which will influence behavioral intentions to use [IC].

According to TAM, technology acceptance is a three-stage process, whereby external factors (system design features) trigger cognitive responses (perceived ease of use and perceived usefulness), which, in turn, form an affective response (attitude toward using technology/intention), influencing use behaviour [2]. Perceived ease of use and perceived usefulness capture the expectations of positive behavioural outcomes and the belief that behaviour will not be labour-consuming [2].

Research Method

Research Design and Approach

This study employs a qualitative research method and uses focus group discussions as its primary data collection tool. Focus groups are considered a reliable qualitative technique to explore collective perceptions, shared meanings, and social attitudes [3,4]. In the current study, the qualitative technique enables a contextual analysis of Bahraini youth's awareness of cybercrime, their attitudes toward online safety, and the impact of these factors on their usage of social networking sites (SNS). The goal is to understand adolescents' rationale and conduct in the digital realm, rather than to measure these traits scientifically [5]. Focus groups allow participants to share their experiences and perspectives on social media use and the risks. Group talks encourage reflection and yield insights that might not emerge in solo interviews [5]. Given the rising participation of Bahraini youth on platforms such as Instagram, TikTok, and X (previously Twitter), focus group talks are ideal for examining peer influence, collective norms, and understanding of cybercrime, privacy, and

digital ethics.

We held three focus groups with 22 Bahraini undergraduate students from the Department of Media. The participants were all students at the same university, aged 18 to 21. Students were asked to participate on their own and were told they would not receive any rewards or course credits for doing so. The questions for the focus group were developed after reviewing the relevant literature and consulting experts in cybercrime. The students talked about how they characterized "cyber" and cybercrime, who they thought was most dangerous of cybercrime, and where they got most of their information about cybercrime and cybersecurity. The session lasted around 40 minutes and was filmed using both audio and video equipment. All recordings were subsequently transcribed verbatim. Inductive thematic analysis was used to analyze the data, following Braun and Clarke's (2006) steps: getting to know the data, developing initial codes, identifying and developing themes, reviewing themes, and refining and naming them [6]. This strategy, based on facts, ensured that any coding frameworks or assumptions the researchers previously had did not affect how themes were developed [7]. To protect their anonymity, participants are identified by their initials. The participants received detailed information sheets that explained their rights and how the study would be conducted. They got a debrief sheet and may ask questions when the focus group is over.

Population and Sampling

The target population comprises young Bahrainis aged 18 to 25 who are active users of social networking sites. A purposeful sample method is employed to choose participants from diverse genders, educational backgrounds, and social media usage frequencies. Participants are recruited through university networks. The research includes three focus groups, each with six to eight participants. This group size is excellent for fostering comprehensive discourse while being manageable for the researcher [8]. The total number of people who took part was 22. Sampling would have been continued until thematic saturation had been reached, signifying that no other themes emerge from subsequent discussions [9,10]. The focus groups each lasted about 60 to 90 minutes. The researcher led the sessions in Arabic and English, whichever the participant preferred.

Data Collection Procedures

The semi-structured discussion guide is designed with a focus on key themes, including participants' comprehension of cybercrime and online risks, prevalent risky behaviors or experiences on social media, awareness of online fraud, privacy issues, and the sharing of personal information, as well as the impact of cybercrime on trust in online interactions and social media usage patterns. The guide allowed participants to share their thoughts and experiences [11]. All focus group discussions were audio-recorded with participants' consent. Subsequently, Arabic recordings were translated into English for analytical purposes. Participant codes were employed to ensure the anonymity of the transcripts and protect individuals' privacy.

Data Analysis

Reflexive Thematic Analysis was used to analyze the data [12]. This process included getting to know the data, developing initial codes, identifying candidate themes, and then going over and improving these themes. The last steps were to come up with names for the final themes and write a coherent analytical story that showed how the meanings in the dataset fit together.

Analysis will be inductive, allowing themes to emerge from participants' narratives, while also being informed by cybercrime and social-media literacy frameworks.

Findings

The focus group data were examined through Reflexive Thematic Analysis. Two primary themes emerged from the discussions: (1) Perceived Cybersecurity Knowledge and Awareness and (2) Actual Exposure to Cybercrime and Corresponding Behavioral Responses. Other subthemes accompany the central theme. These include levels of awareness, exposure to cyber threat information, and the link between awareness and education. The second theme pertains to several subthemes, including pervasive perceptions of threat and vulnerability, familiarity with both standard and advanced cyber threats, the emotional repercussions of cybercrime experiences, and behavioral adaptations following exposure.

Perceived Cybersecurity Knowledge and Awareness

The respondents in the focus groups said they felt that they were at varying levels of risk when it came to cyber dangers, usually high, moderate, or low. Most of the people who took part claimed they do a lot of digital things every day. Many respondents reported that cyber threats were a routine part of their online lives, especially when using social media or playing games.

"You cannot really avoid cyber risks anymore because we are always online, especially on social media," said one of the people who took part. "I would not say it is extreme, but I do have a lot of cyber problems, like fake accounts or messages that make me suspicious," said another person.

The investigation revealed that a small subset of participants perceived their susceptibility to cyber threats as minimal. This point of view showed a clear trend in the data and was quite similar to parents who were rigorous about their kids' internet use and always watching them. People in this group knew that there were cyber hazards, but they said they felt safer because of rules that limited what they could do online.

One person remarked, "I think my exposure is limited because my parents' control how I use the internet and talk to people." This is an example of this point of view. These accounts were put into two groups: "parental supervision as a protective factor" and "regulated digital engagement." The primary point of the focus group conversations was that everyone agreed that cyber threats are widespread and pretty much difficult to avoid in today's digital world. Even though there was this sub-group. Most of the people who took part agreed that exposure levels can change, but they stressed that running into online dangers is now a normal part of using the internet.

The thematic analysis of focus group conversations underscored a pronounced, uniform emphasis on the importance of education and awareness regarding cyber risks. Most participants agreed that learning about cyber hazards is essential for using the internet safely and responsibly, but they disagreed on how important this education is.

Almost half of the participants said that knowing about cyber dangers is vital and should be a fundamental ability for students in today's digital world. These participants stressed that education helps people recognize hazards, avoid dangerous situations, and respond appropriately when they encounter threats online. One participant said, "If you don't know about cyber threats, you won't even know when something bad is happening. (Qassim, G1)" Another person said, "Learning helps you stay safe and not believe everything you see online. (Zahraa, G1)"

A significantly bigger percentage of people thought that learning about cyber threats was somewhat important, but not very important. These students agreed that cyber awareness was critical, but they saw it as beneficial background information rather than something they needed to learn right away. People typically thought this way because they were confident in their digital skills or trusted existing protections, such as parental advice or security features on the platform.

One person said, "It is important, but I feel like I already know the basics from experience. (Hawra, G2)" Someone else said, "It's good to learn about cyber threats, but I don't think about it all the time. (Qassim, G1)"

Perceived Necessity of Education on Cyberspace

The thematic analysis of the focus group conversations identified a prevailing theme regarding the perceived imperative to teach youth about cyberspace and its attendant threats. Some of the participants were firmly in favor of cyber education, while others were just somewhat in favor of it.

Many participants said they thought it was essential to understand the risks of cyberspace. They believe that cyber risks are continually evolving and that the internet is confusing; therefore, education needs to be ongoing and organized. They thought teaching people about the internet was vital because it would help them learn more, make better decisions, and avoid harmful online encounters. "We need to learn about the risks because the internet is not as easy as it used to be. (Hawra, G2)" Another participant stated, "It is easy to get into cyber problems without even knowing it if you do not get the proper education. We already know some things about cyber risks, but it would be good to learn more (Abdulaziz, G1).

Some participants claimed they did not think it was vital to understand cyberspace and the dangers it posed. School did not teach them how to be safe online. Instead, they thought about it based on their own experiences, gut sentiments, or the protection that technology offers. Their answers suggested that they were sure they could learn on their own. "I do not think we need lessons about it because we learn from using the internet every day," Qassim stated (G1).

The perceived danger of cybercrime

The focus group discussions revealed a predominant theme: students' perceived sense of threat associated with cybercrime. Some participants were apprehensive, while others felt very safe. However, the prevailing trend in the discussions suggested that many participants felt a degree of perceived threat when interacting in digital contexts.

The most common feeling among participants was a modest sensation of being threatened by cybercrime. Students in group 1 recognized the existence of cyber threats but did not express persistent worry or anxiety. Instead, they talked about being careful, since they had read online stories, heard warnings, or heard about things that had happened to their friends. One person said, "I'm not scared all the time, but I know cybercrime is real, so I try to be careful." Another person said, "It is not necessary for an individual to be tech-savvy or to be directly involved in digital industries to be aware of cybersecurity, as all ordinary people are conscious nowadays about all online precautions. (Abdulla, G3)"

Many in groups 2 and 3 said they felt very or very endangered by cybercrime. These students typically linked their anxiety to identity theft, hacking, internet scams, or the exploitation of their personal information. Their stories showed that they felt more vulnerable and had stronger emotional reactions in digital places. One person said, "Cybercrime is very scary because someone can steal your information without you knowing." Another person said, "I feel threatened because hackers are everywhere and you cannot trust anyone online." "If you ask me about my worst fear concerning the internet, I will say that I fear leakage of my personal pictures and personal information."

On the other hand, just a small number of participants said they did not feel threatened by cybercrime at all. These students commonly said that their confidence came from not spending much time online, good security habits, or trust in technology to keep them safe.

One respondent said, "I do not feel threatened because I do not share personal information online. (Hiba, G1)"

"I feel safe by following basic advice, always be aware of every action taken online, and change passwords occasionally. Furthermore, do not share any information on unsecured websites, and read and pay close attention to all "Terms and Conditions" documents online. And most importantly, the primary step a normal internet user can take is not to share personal details on unknown websites, to stay protected against cybercrime" (Malak, G2).

Types of Cybercrime Exposure and Emotional Responses

The focus group discussions uncovered two interconnected themes about students' experiences with cybercrime: (1) the categories of cybercrimes they faced and (2) the emotional repercussions of these incidents on them. Participants exhibited the same exposure patterns; however, they had diverse emotional responses to cyber incidents.

Participants frequently reported experiencing spam-related cyber threats, characterizing them as persistent, intrusive, and difficult to evade. Most of the time, these encounters involved

getting unwanted messages, ads, or links through email, text messages, or social media. "Spam messages are everywhere," someone said. "You keep getting rid of them, but they always come back."

The second most common type of cybercrime exposure was online phishing, which occurs when someone tries to get you to give them personal information or click on suspicious links. People who took part knew about phishing and discussed receiving fake accounts, emails, or messages that appeared to come from people they trusted. "Sometimes you get messages that look real, but later you find out they are trying to steal your information," one person said.

Some customers also reported experiencing denial-of-service attacks, which temporarily prevented them from accessing their accounts or internet services. People thought these things were incredibly annoying, even if they did not happen as often. People called these occurrences "frequent exposure to spam," "phishing encounters," and "service disruption experiences."

Most people felt terrible about what happened to them online. Many of the folks who took part said they were furious, hurt, and weak. Spam and other unwanted messages kept pouring in, upsetting people. People were angry when they thought someone was intruding on their personal space or privacy.

"It is annoying and frustrating because you did not ask for this to happen," someone said. Another person said, "It feels bad when someone tries to trick you or get into your account."

People felt quite vulnerable, especially regarding phishing and service outages. People were aware that their online identities and personal information could be in danger. A participant said, "You feel unsafe because someone is trying to get into your private information."

The answers were divided into three groups: "emotional annoyance," "perceived violation," and "digital vulnerability."

Most people did not like what happened, but a few said that their encounters with cybercrime made them feel better or were helpful. These kids said they were interested, motivated, or pushed to learn more about staying safe online. They did not think the experience was all bad; instead, they saw it as a chance to learn more about technology and not have those kinds of problems again.

"I thought it was weird at first, but then I wanted to know how it happened so I could avoid it next time," said one person.

Discussion

This study explored students' perceptions of cybersecurity awareness and their lived experiences of cybercrime through focus group discussions. The discussions included numerous questions about the participants' background knowledge, work environment, prior internet surfing experiences, and incidents involving cybersecurity and cybercrime. Having discussed the above has helped the researchers gain a broader understanding of individuals' perceptions of cybercrime and their behavior in the virtual world, as well as the extent to which they practice safe online behavior [13].

The Technology Acceptance Model (TAM) is a tool for understanding how students' beliefs, attitudes, feelings, and past experiences shape their online behavior and perceptions [14]. TAM was created to help people understand why they like and use technology. The basic ideas of the theory are still helpful for understanding behaviors related to cybersecurity, especially when people must choose between safe online activities and participating in educational interventions [15].

Perceived Cybersecurity Knowledge and TAM Constructs

The first central theme (Perceived Knowledge and Awareness of Cybersecurity) aligns with perceived usefulness in the TAM. People who recognize the importance of cybersecurity education view knowledge as a valuable tool for identifying threats and responding appropriately when necessary [16]. These students believed that being aware of cybersecurity would help them stay safer online and be less likely to be hacked. This seems to be in line with the theory: people are more likely to use systems or behaviors they think will help them perform better or achieve better results.

This perception might make people less likely to actively look for structured cybersecurity education, even if they know there are threats. From a TAM perspective, this indicates that awareness alone does not inherently lead to acceptance or adoption of protective behaviors unless individuals distinctly recognize additional value beyond their current practices [16].

Parental supervision and controlled digital interactions have been identified as protective factors, particularly among participants who considered themselves less vulnerable to cyber threats. These external controls can give people a sense of being at lower risk. However, they can also make people feel less capable of learning cybersecurity, as they partially delegate the responsibility for protection to others. This observation highlights a possible gap between individuals' perception of safety and their actual preparedness. This gap may become more apparent when external controls are removed [17].

The findings support the concept of perceived ease of use in the Technology Acceptance Model (TAM), particularly among participants who believed they could learn cybersecurity naturally through regular internet use. Students who expressed confidence in learning by doing stated that preventative behaviors did not require formal training and were intuitively simple to implement. This notion may encourage ongoing use of digital platforms, but it can also lead to overconfidence, particularly in the face of advanced or sophisticated cyber threats [18].

Participants who perceived the need for continuous and structured cybersecurity training implicitly acknowledged the complexity of the digital environment. For them, cybersecurity was not perceived as inherently easy to manage, reinforcing the need for formal learning to reduce cognitive effort and ambiguity. According to the Technology Acceptance Model (TAM), when systems or behaviors are perceived as complex, they are more likely to be accepted if support mechanisms, such as training and guidance, are put in place to facilitate their use.

The subject of Perceived Danger of Cybercrime serves as a crucial emotional element that amplifies the Technology Acceptance Model (TAM). While the Technology Acceptance Model (TAM) does not explicitly incorporate emotions, the participants' fear, anxiety, and vulnerability significantly influenced their perceptions of online behavior [19,20]. Students who perceived a significant threat from cybercrime, especially about identity theft, hacking, or the exposure of personal information, exhibited heightened alertness and vigilance. These emotional reactions seem to reinforce the perceived significance of cybersecurity knowledge and safe behaviors.

Conversely, participants who sensed a low threat typically adopted basic precautions or restricted their online engagement. These measures may reduce incidents, but they also risk diminishing stakeholders' willingness to adopt more comprehensive and sustainable preventive strategies [21]. Investigating the impact of cybersecurity awareness. Information & Management, 56(5), 754–766.). This distinction also demonstrates how risk perception influences various aspects of the technology acceptance model by altering individuals' attitudes toward cybersecurity training and procedures.

Exposure to Cybercrime and Behavioral Intentions

The second central theme, exposure to cybercrime and the corresponding behavioral reactions, sheds light on the central element of the TAM model, the behavioral intention. Participants who experienced attacks, spam, or phishing attempts often reported emotional reactions, including irritation, frustration, and a sense of vulnerability. For many, these experiences led to behavioral adaptations, particularly increased caution, password changes, and avoidance of suspicious links. These reactions indicate a desire to protect themselves online, confirming the TAM model's hypothesis that positive attitudes and perceived usefulness determine intention and behavior.

It is worth noting that a small group of participants viewed exposure to cybercrime as a learning opportunity rather than a negative experience. Their curiosity about the incidents they experienced suggests a proactive attitude toward cybersecurity learning. This finding reinforces the idea that experiential learning can improve perceived usefulness and strengthen commitment to safe digital practices [22].

Implications for Cybersecurity Education

Overall, the study results suggest that participants' willingness to learn more about cybersecurity and protective behaviors is influenced by a combination of factors: perceived usefulness, perceived ease of use, emotional responses, and lived experiences.

While many participants acknowledge that cyber threats are inevitable in the digital space, not all perceive formal education as necessary. From the perspective of the Technology Acceptance Model (TAM), it is essential to present cybersecurity education as both valuable and accessible, emphasizing its relevance to real-world experiences rather than presenting it as inaccessible technical knowledge [23,24]. Cybersecurity awareness, knowledge, and behavior. Journal of Computer Information Systems, 62(2), 207–217.

In conclusion, applying the Technology Acceptance Model to these results helped explain the variations in students' attitudes and behaviors toward cybersecurity. Perceived knowledge, emotional reactions to cybercrime, and prior exposure collectively influence students' likelihood of adopting safe online practices. Future interventions aim to enhance perceived usefulness, reduce perceived complexity, and address emotional concerns to encourage more consistent and proactive cybersecurity behaviors among young people.

References

1 Tawalba AH (2009) Cyber crime. Fakhrawi Studies and Publications.

2 Nowell LS, Norris JM, White DE, Moules NJ (Davis) Thematic analysis: Striving to meet the trustworthiness criteria. International Journal of Qualitative Methods 16(1): 1-13.

3 Morgan DL (2022) Basic and advanced focus groups. SAGE Publications.

4 Krueger RA, Casey MA (2021) Focus groups: A practical guide for applied research (6th ed.). SAGE Publications.

5 Nyumba TO, Wilson K, Derrick CJ, Mukherjee N (2018) The use of focus group discussion methodology: Insights from two decades of application in conservation. Methods in Ecology and Evolution, 9(1): 20-32.

6 Clarke V, Hayfield N, Moller N, Tischner I (2017) Once upon a time: Thematic analysis in qualitative research. Qualitative research in psychology (pp. 297-315).

7 Hayfield N, Moller N (2015) Analyzing digital communication using thematic analysis. Qualitative Research in Psychology 12(4): 343-356.

8 Hennink MM, Kaiser BN (2022) Sample sizes for saturation in qualitative research: A systematic review of empirical tests. Social Science & Medicine 292: 114523.

9 Guest G, Namey E, Chen M (2020) A simple method to assess and report thematic saturation in qualitative research. PLoS ONE 15(5): e0232076.

10 Hennink MM, Kaiser BN (2022) Sample sizes for saturation in qualitative research: A systematic review of empirical tests. Social Science & Medicine 292: 114523.

11 Braun V, Clarke V (2023) Supporting best practice in reflexive thematic analysis reporting. Qualitative Research in Psychology 20(2): 1-25.

12 Braun V, Clarke V (2021) One size fits all? What counts as quality practice in (reflexive) thematic analysis? Qualitative Research in Psychology 18(3): 328-352.

13 Ifinedo P (2021) Applying the technology acceptance model and protection motivation theory to investigate students' cybersecurity behaviors. Information & Computer Security 29(1): 1-18.

14 Alshaikh M. (2020) Developing cybersecurity culture to influence employee behavior. Computers & Security 98: 102003.

15 Venkatesh V, Thong JYL, Xu X (2021) Consumer acceptance and use of information technology: Extending the unified theory. MIS Quarterly 45(1): 187-230.

16 Parsons K, McCormac A, Butavicius M, Pattinson M et.al (2019) The human aspects of information security questionnaire (HAIS-Q). Computers & Security, 81: 1-17.

17 Hadlington L (2018) Employees' attitudes towards cyber security and risky online behaviours. Computers in Human Behavior 78: 105-113.

18 Cain AA, Edwards ME, Still JD (2018) An exploratory study of cyber hygiene behaviors and knowledge. Human Factors 60(2): 194–209.

19 Renaud K, Weir GRS (2020) Cybersecurity and the human factor. ACM Computing Surveys, 52(5): 1-35.

20 Boss SR, Galletta DF, Lowry PB, Moody GD, et.al (2015) What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly 39(4): 837-864.

21 Li L, He W, Xu L, Ash I, et.al (2019) Investigating the impact of cybersecurity awareness on employees' cybersecurity behavior. Information & Management 56(5): 754-766.

22 Furnell S, Clarke N (2021) Human aspects of cybersecurity. Computer Fraud & Security 2021(2): 5-11.

23 Katz FH (2020) Cybersecurity education: Challenges and strategies. IEEE Security & Privacy 18(2): 64-68.

24 Zwilling M, Klien G, Lesjak D, Wiechetek Ł, et.al (2022) Cybersecurity awareness, knowledge, and behavior. Journal of Computer Information Systems 62(2): 207-217.