Journal of Cyber Security

Tech Science Press

Doi:10.32604/jcs.2025.059712

ARTICLE

A Conceptual Framework for Cybersecurity Awareness

Kagiso Komane[1,*], **Lucas Khoza**[2] **and Fani Radebe**[1]

[1]Department of Applied Information Systems, College of Business Economics, University of Johannesburg, Johannesburg, 2092, South Africa

[2]School of Computing, College of Science, Engineering & Technology, University of South Africa, Pretoria, 0002, South Africa

*Corresponding Author: Kagiso Komane. Email: kagiso.komane67@gmail.com

Received: 15 October 2024; Accepted: 21 April 2025; Published: 20 May 2025

ABSTRACT: Financial support, government support, cyber hygiene, and ongoing education and training as well as parental guidance and supervision are all essential components of cybersecurity awareness (CSA) identified in this study among the youth. It's critical to realize that adequate funding is needed to effectively increase CSA, particularly among South African youth. Previous studies have demonstrated several ways to address inadequate CSA by utilizing various cybersecurity frameworks, ideas, and models. To increase CSA, this literature review seeks to emphasize the significance of integrating cybersecurity education throughout the entire school curriculum. This paper identified ethical issues, protection of digital assets and unskilled personnel as some of the cybersecurity challenges faced by the youth. Some of the challenges facing domestic cybersecurity education include social integration, structural capabilities, cybersecurity skills, financial resources, and governance ability. In addition, the goal of the literature study is to assess the necessary components including cybersecurity theories, independent variables, methodologies, participants, data analysis, and recommendations for the proposed conceptual framework for CSA. Only 193 of the roughly 1000 journal articles that were gathered were used in the literature review. The primary findings showed that the two most prevalent hypotheses in the reviewed literature were the Theory of Reasoned Action and the Theory of Planned Behavior. Most of the data was gathered from Gauteng-based university or college students between the ages of 18 and 23. Data were gathered using a mixed technique approach that included interviews and a questionnaire. The target variables in the research that were analyzed were behavioral intention and the current state of CSA. The review and analysis provided various research issues that might be looked at in future studies, as well as practical consequences.

KEYWORDS: Cybersecurity; cyberbullying; conceptual framework; social media; phishing; awareness; cyber hygiene; financial support; government support

1 Introduction

Cybersecurity has become increasingly popular because of technology's rapid growth, particularly on the internet. In our advanced technological world, most youth use the Internet through their mobile devices. Our use of the Internet now takes up a large amount of time and has become an essential component of our lives [1]. Security experts from all around the world are debating the need to improve cybersecurity in the wake of reports of a significant cyber compromise [2]. According to Vishwanath et al. [2] and colleagues, "cyber hygiene" is the term used to describe cybersecurity practices that online users should adhere to protect the security and integrity of their personal information stored on their Internet-connected devices from being compromised in a cyber-attack.

To increase online safety, interpersonal and intrapersonal factors that affect human behavior must be taken into consideration to be aware [3]. This is in line with the social work approach, which acknowledges that a person's conduct can be influenced by their health, attitudes, and social status [3]. These unique, psychological, and cultural characteristics of people have a significant impact on whether they will adopt and maintain secure internet behaviors like choosing strong passwords, ensuring the privacy of their online communications, and purchasing security-related software [3].

According to Seok and DaCosta [4], gamers are prone to bad online behavior and are unconcerned about the potential repercussions of disregarding cybersecurity best practices. To compromise a larger system or an entire corporation, new tactics like social engineering and phishing are used to reveal individual users' vulnerability to attacks [5]. The concept of cyber hygiene is becoming more and more important to address the risk associated with a person's cybersecurity actions because user knowledge and behavior have become crucial variables in preventing, reducing, and effectively responding to unfavorable occurrences [5].

Using cybersecurity knowledge to drive behavior change is one of the more recent methods for raising awareness of cybersecurity [6]. The limited definition and comprehension of CSA is one of the main reasons why most CSA initiatives fail. Contrary to popular belief, CSA should encompass much more than merely the dissemination of knowledge [6]. It involves influencing people to change their current behavior while also encouraging them to adopt new behavior [6].

One's capacity to practice effective CSA may be impacted by a variety of cybersecurity knowledge, perceived security, and competence perception aspects [7]. More systematic knowledge of how people choose to engage (or not) in good CSA practices may lead to the development of clearer communication materials or strategies to spread them further [7].

Cybersecurity incidents like cyberattacks and even warfare have not only been observed by specialists but have frequently made headlines and attracted the public's attention [8]. It is vital to keep a global perspective because cybersecurity is a major concern for foreign authorities [8]. The United States of America (US) is implementing its cybersecurity policy in response to China's adoption of its cybersecurity law in 2017 [8], which prompted responses from the European Union (EU) and other nations. During the COVID-19 outbreak, cybercriminals used people's worries to steal personal information, install malicious software, conduct ransomware attacks, and use other social engineering techniques [9].

Skilled professionals are required to handle cyber issues to detect and respond to cyber threats and secure critical infrastructure [10]. Students who are not enrolled in cybersecurity will not learn how to be cyber-resilient because CSA is only taught at the university level and is only available to students registered in cybersecurity modules [11]. South African women are more vulnerable to cyberattacks because of the gender gap in computer security degrees, which suggests that the country's approach to developing CSA is failing to produce a citizenry that is cyber-resilient [11].

2 Literature Review

2.1 Cybersecurity

In academic and popular literature, the term "cybersecurity" has been the focus of a lot of viewpoints on the subject. According to Oxford University Press, cybersecurity refers to the ability to secure electronic data against misuse by criminals or others as well as the steps taken to do so. Information and communications systems, as well as the data held inside them, are protected from and/or defended against damage, unauthorized use or alteration, or exploitation, according to McBride et al. [12] definition of cybersecurity. The field of information and communication technology (ICT) is wide and includes all the technological tools needed to handle and transfer data. Online communication is increasingly taking the place of face-to-face

interactions in daily life. The benefit of this communication taking place in cyberspace is that it gives people the freedom to interact from anywhere at any time, but it can also have undesirable impacts [13]. Nowadays, practically everyone lives in two worlds—the actual and the virtual—thanks to advancements in computer technology and the expansion of the Internet [14]. The virtual and physical worlds are intertwined; just as the virtual world provides diverse Internet representations of actual persons and imposes social and legal obligations, so does the physical world [14].

In the age of global communication, the Internet has made life easier for users and given them access to added information, education, and entertainment. However, improper or excessive Internet use can have several negative effects [15]. Teenagers spend a sizable amount of time online for amusement or education even though more and more of their lives are being digitally documented, potentially having long-term repercussions on their privacy [15]. Children struggle to weigh the advantages and risks of utilizing the Internet and other digital systems because of their age [16].

Pons-Salvador et al. [17] claim that children start using smart gadgets to access the Internet at an early age, frequently unsupervised or with no time limits from parents. Teenagers can benefit from the Internet because it is a fantastic informational resource [1,17]. Teenagers today use the Internet frequently and own more online devices than ever before. Because of their quick learning curves with technology, this age group is becoming more and more reliant on the Internet and social media [16].

The development of the internet and the subsequent rise of digital media have had a significant impact on learning, information access, and knowledge generation. For example, the internet has made it simpler for people to interact and communicate. Because of the rising connection to high technology, people use the internet more frequently for social networking in both personal and professional contexts, including daily conversation, work-related activities, and online services like banking, education, and virtual healthcare.

Data is often referred to as "the new oil," which makes sense given why ransomware poses such a serious threat. The 2022 SOES survey indicates that this knowledge is finally becoming more widespread, even though organizations and enterprises still struggle to guard their digital capital with the same vigilance as their physical assets.

2.2 Effects of Social Media on Youth

Social media addiction is a behavioral condition that affects adolescents and youth who become fascinated by the platform and are unable to reduce or stop using it despite its clear negative consequences and significant drawbacks [18]. Teen social media addiction is characterized by a combination of excessive media consumption, a growing reliance on social media as a way to feel good, and an inability to stop or curb this behavior despite suffering friendship loss, a decline in physical social engagement, and a negative impact on academic performance [18].

Although a large number of the youth regularly use online media (such as Facebook, Instagram, Twitter/X, YouTube, Vine, Snapchat, and video games), teen social media addiction is characterized by a mix of excessive media consumption [18]. Understanding and monitoring people's online behavior is important, especially their preferences for how they present themselves [19]. The widespread usage of digital applications made possible by the steady rise in computing power has accelerated the fusion of people's online and offline lives. The bulk of social networking site (SNS) users today are "digital natives" because they were raised with digital technology [19]. The internet is being used by society to date, host conferences, and conduct business meetings; all of these interactions take place in contexts where online personas are necessary [19].

Online drug purchases are a growing problem habit that could be especially dangerous given how difficult it is to regulate online activity, according to a 2021 study by Oksanen and colleagues on more than

2400 youth in the USA and Spain between the ages of 15 and 25. Drug users who already battle with self-control and mental health may find that things get worse if they purchase drugs online [20]. Because it is so easy to make hasty decisions on social media, more attention has to be devoted to how the youth act on well-known social media platforms [20]. The implications for policy and practice underline the necessity to deal with kids' social media use because youth spend a lot of time online [20].

Cyberbullying is one of the issues that youth encounter online. Cyberbullying, often referred to as cyber harassment, is the deliberate and persistent infliction of harm using computers, mobile phones, and other electronic devices, according to [21]. While cyberbullying involves behavior that is similar to traditional bullying in terms of aim, violence, power disparity, and the repetition of abusive behavior, these components may not be the same in the digital realm [22]. Because a single image or video can generate a lot of views and reactions on social media, cyberbullying, for instance, might not repeat its aggressiveness. However, views, shares, saves, comments, and "likes" could be used to revive the victim's bullying experience and start a cycle of violent repetition [22].

To begin with, the internet enables a single offender to be hostile to multiple victims at once. They can send insulting comments or statements to others and simply post them on multiple homepages or chat rooms [23]. Second, bullying can be more easily committed online by both younger and older offenders, as well as peers in the same age range [23]. Since most bullying in schools occurs between students in the same grade, the internet makes it simple for people of different ages to harass you.

Another problem that impacts adults as well as teenagers and adults is online dating. As one of the technologies used to create interpersonal connections, online dating websites, and programs use the function of matching people to form romantic relationships [24]. According to demographic identifiers including gender and sexual orientation as well as personality-based characteristics, Sumter and VandenBosch looked at the relationship between youth's use of dating apps and the motivations for doing so [25]. Over half of the sample regularly used the most well-known dating app, Tinder, and non-users were more likely to be heterosexual, to have high levels of dating anxiety, and to have lower levels of sexual permissiveness than users of dating apps [25].

Men are more likely to focus on the physical aspect of relationships, whereas women often have a variety of demands [24]. The meta-findings reviews recommended both a focus on the quantity of partners for men and a focus on the caliber of partners for women [24]. Men are expected to show traits that put them on a superiority scale and initiate contact, whereas women focus on finding inventive ways to expose themselves and use more photos than men because they think success is correlated with appearance [24]. The traditional and stereotypical depictions of people were also discussed. Users' identity characteristics were significantly correlated with their motivations for using dating apps, including relational goals like love and casual sex, intrapersonal goals like self-worth validation and communication ease, and entertainment goals like the thrill of excitement and trendiness [25].

One in five young youth experience improper internet exposure to sexually explicit content, and one in nine youths experience unwanted online sexual solicitation [26]. This overview underscores the ongoing need for awareness-raising campaigns to draw attention to Internet dangers, as well as the demand for more research on the psychological impacts of sexual encounters made possible by the Internet [26].

Phishing is another issue that is growing in prominence online. It entails sending emails or messages that encourage the recipient to click on links that lead to websites that contain malicious code, download malware, or any of these things. The elderly and younger generations are the "lowest hanging fruit," hence previous research suggests that cybercriminals would likely target them [27]. To obtain the victim's sensitive data and credentials, such as their social security number and bank account information, or to launch malicious code,

Zhuo and colleagues define phishing as a type of cyberattack that tries to trick the victim into taking specific actions, like clicking on embedded links or downloading or running attached files [28]. To deceive recipients into performing the attackers' intended actions, usually clicking an embedded link, the most common sort of phishing involves replicating a valid email's visual presentation and content [29]. Digital tools and techniques are used by online predators to lure their victims.

These users need to understand how online predators think to prevent becoming just another statistic in an attack [27].

2.3 Feature Merits and Demerits of Existing Work

The development of innovative security awareness training techniques is necessary due to the complexity and sophistication of cybersecurity threats in the present day [30]. Various state-of-the-art cybersecurity awareness models have been examined in numerous studies to educate and teach individuals about the latest threats and how to protect themselves from them [30]. Innovative cybersecurity awareness models provide unique and effective means of educating and training individuals on the latest threats and how to protect themselves from them [30]. These techniques can help reduce risks in the present digital environment and increase public awareness of cybersecurity issues.

Information security experts must be able to express their value in monetary terms because it has never been easy to measure an organization's information security costs in a thorough and comparative manner [31]. When the decision-makers do not provide enough financial support, this could become a financial problem. The necessity and significance of financial assistance in increasing CSA among young people have been emphasized in this study. To help an organization address information security management, the assessment of information security risk features aids in the evaluation and comprehension of the existing information security landscape, the risks that the firm faces, and the critical success elements [31].

According to a study by Khader and colleagues those entrusted with critical data, like banking data, made significant investments in cybersecurity by employing security experts, creating comprehensive security policies, integrating cutting-edge security technologies, and regularly training their security professionals to protect data and help lower the number of potential cybercrimes that stem from illicit online activities [32]. Although this significant investment in cybersecurity has made networks, operating systems, and applications safer and more secure, comparatively less money has been invested in raising security awareness among these industries' consumers or users, making them the weakest link [32]. In an attempt to steal their data, organized cybercriminals have therefore turned their focus to human factors by making great efforts to study and create sophisticated hacking techniques that take advantage of clients' trust and propensity to assist [32].

Because criminals target sectors entrusted with critical data such as banks to take advantage of their weaknesses, sectors such as banks must work with the government and invest in their clients' continuous CSA education and training in addition to providing financial support. People will be less likely to become are online fraud victims when equipped with CSA knowledge. Young people may not have a lot of money invested in banks, but if they are empowered with knowledge earlier on, they will be able to help the elderly people in their immediate vicinity in addition to protecting themselves.

2.4 Similar Studies

In their study, Govender, Kritzinger, and Loock investigated information security data breaches and discovered that, to better support information security management, the emphasis should be on lowering the costs of goods, services, and organizational structures while also fostering the right attitudes and behaviors

in IT personnel and enhancing their capacity to improve the organization's information security assessment capabilities [31]. However, Govender, Kritzinger, and Loock seemed to be limited by only considering IT personnel and enhancing their information security awareness. The model that they proposed had several technical factors that also included parental monitoring, which is also a construct in the current study, however, their model did not include financial and government support. Therefore, this current study proposes financial and government support to address youth access to CSA. Furthermore, this study aims to raise CSA for all the youth, not only those who aspire to work in the IT field but everyone who has access to the internet.

A list of crucial cybersecurity controls specific to school districts in the United States is provided by the non-traditional K12 SIX Essential Cybersecurity Protections framework [33], as a baseline cybersecurity standard. This baseline cybersecurity standard, which was created by K12 IT professionals, aids educational institutions in prioritizing the protection of vital infrastructure and coordinating with industry best practices for managing cybersecurity risks [33]. Cyber hygiene, which the current study suggests as one of the primary constructs for the conceptual framework, is in line with the K12 Six framework's criteria. In their study, Warnekar and colleagues proposed a conceptual framework to address the lack of knowledge through effective governance and continuous student learning to shape responsible online citizens [33]. These observations indicated the importance of cyber hygiene and continuous learning among the youth. The digital world continues to evolve, it is therefore essential for continuous CSA training and education to be implemented and maintained.

Regulations that protect student data privacy include the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Children's Internet Protection Act (CIPA) [34]. These laws offer particular security control recommendations to make sure that educational institutions, including schools, protect student data from breaches and unauthorized access [34]. In their study, Radway and colleagues showed that students feel more at ease when they are aware of the data being shared and, more importantly, with whom [34]. Students should be aware if universities are only sharing within their institution or with required third parties, as this will make them feel more at ease. The negative misalliance between how students perceive the world and how they share their personal information is probably present in several schools that currently take precautions by not disclosing information to outside parties but fail to tell students about this misalliance [34]. This suggestion that students feel comfortable because they know with whom their information is being shared demonstrates unequivocally that US university students who took part in the survey are aware of their information security, demonstrating that they practice adequate cyber hygiene and are not ignorant of it.

2.5 Proposed Conceptual Framework for CSA for the Youth

The suggested conceptual framework for youth CSA was developed based on a literature review, and the constructs were guided by the findings of both qualitative and quantitative data analysis. Fig. 1 below illustrates the proposed conceptual framework for CSA. The constructs of cyber hygiene, education, continuing training, and parental advice and supervision were all informed by qualitative data. The quantitative data influenced the financial and government support constructs.

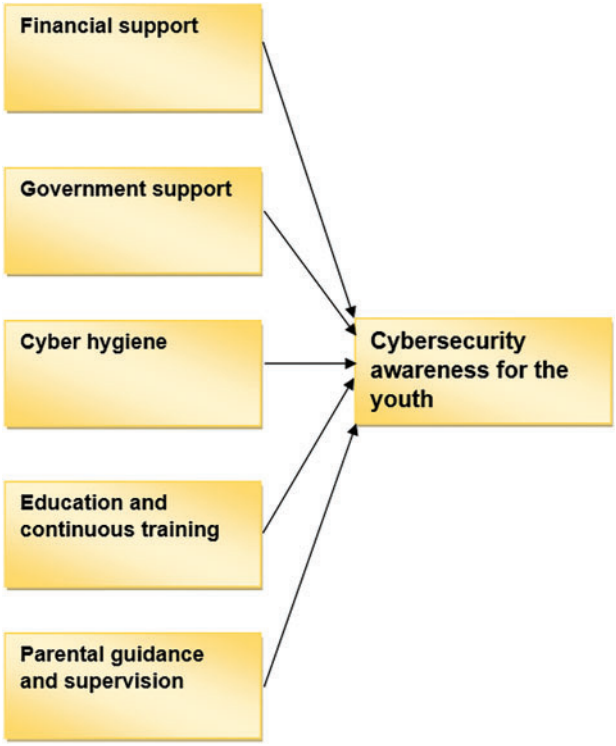

Figure 1: Proposed conceptual framework for CSA for the youth

2.5.1 Financial Support

The fundamental construct towards addressing CSA is to identify the need for and importance of financial support. After assessing the literature review three aspects are determined that demonstrate the significance of financial support in CSA. These aspects include a lack of CSA knowledge which can lead to data loss and damage, vital infrastructure that can prevent cyberattacks, and the availability of a skilled workforce. These aspects are systematically retrieved from the literature, and they are required to raise CSA. The COVID-19 pandemic has profoundly altered the educational landscape, resulting in a rise in online teaching and learning methods, and consequently, heightened Internet usage among students [35]. The heightened Internet usage conditions have fostered an environment that renders the youth susceptible to cybercrime due to insufficient cybersecurity awareness [35]. When people lack CSA knowledge, they will not know how to avoid or prevent data loss and damage as they can fall victim to cybercrimes [36]. Data loss and damage can result in huge financial implications [36]. The researchers in this paper emphasize the necessity of securing financial support from both public and private stakeholders, necessitating their collaboration to address the three aspects. However, with the increasing digitization and interdependence of critical infrastructure, cybersecurity threats have emerged as significant concerns, posing risks to the reliability, safety, and resilience of these essential systems [37]. The cybersecurity of critical infrastructure is paramount, as cyberattacks targeting these systems can have far-reaching consequences, including disruption of services, loss of life, and economic damage [37].

Vital infrastructure that can prevent cyberattacks is the second aspect retrieved from the literature review, in the contemporary interconnected world, vital infrastructure is essential for the operation of modern communities and economies [37].

2.5.2 Government Support

To help communities and citizens better understand the ongoing threats posed by cyberthreats and cyberattacks, as well as the inadvertent creation of skills gaps, governments should take the lead in implementing cybersecurity education, training, and awareness initiatives [12]. One of the few African countries with national cybersecurity policy frameworks in South Africa [38]. Understanding the factors that affect the development and delivery of information and cybersecurity curricula in South African higher education institutions is crucial because there is currently a dearth of knowledge regarding cybersecurity specialization and information [38].

Governments must work with experts who can see possible vulnerabilities and, as a result, develop cost-effective risk-reduction strategies so that they may make well-informed decisions when directing scarce public and private resources toward cyber protection and security [10].

Engaging professionals is required because before developing effective action plans, a comprehensive awareness of cybersecurity resource restrictions must be established [39]. Protecting these systems is a current scholarly concern, especially in light of the ongoing and ever-emerging cybersecurity vulnerabilities [38]. For example, as vital national infrastructure includes, among other things, healthcare, energy distribution, transportation, governmental operations, and financial services, it becomes imperative to protect the data utilized, processed, and controlled by governmental organizations [40].

2.5.3 Cyber Hygiene

Online users should follow cybersecurity precautions, also referred to as cyber hygiene, to safeguard the security and integrity of personal data kept on devices connected to the Internet from assaults [2]. The concept of cyber hygiene is becoming increasingly important to manage the risk associated with an individual's cybersecurity behaviors, as user behavior and awareness have emerged as critical factors in effectively preventing, reducing, and responding to unfavorable events [5].

Although students were aware of online security, most were unfamiliar with the phrase cybersecurity and thought it was the same thing as cybersecurity rather than a subset of it [41]. The study suggests creating a conceptual framework that tackles youth cybersecurity awareness issues and promotes cyber hygiene and procedures for dealing with cybersecurity breach incidents and crimes like cyberbullying (reporting, information sharing, alert management, and collaboration between the police and judiciary).

According to the quantitative data gathered for this study, 24% of the participants stated that they included their addresses, phone numbers, photos, real names, and last names on their internet profiles so that others could quickly identify them, while 54% disagreed. This finding is concerning since it suggests that almost half of the participants did not practice any kind of cyber hygiene, making young people more vulnerable to cyberattacks.

Cyber hygiene, which outlines the necessity of safe online practices and sufficient protection of young people's data and gadgets, became one of the main themes during the qualitative data collection for this study. In general, the participants believed that young people should use complicated passwords and avoid sharing their devices and login information to practice good cyber hygiene.

2.5.4 Education and Continuous Training

One significant and rapidly growing area of information technology is cybersecurity. Therefore, despite the development, researchers have raised concerns about the availability of cybersecurity expertise [42]. Cybersecurity educators and trainers have been urged to address several issues, including the lack of young

people entering the field, the lack of information and cybersecurity concepts exposure, the lack of established career and training pathways into the field, and the lack of appropriately qualified teachers [43].

The need for cybersecurity experts has increased because of the surge in cyberattacks and cybercrimes. Businesses that advertised cybersecurity analyst openings also revealed an 82% likelihood of facing a cyberattack, according to a global survey that found that at least 59% of cybersecurity analyst roles in the US were vacant [44].

Hart et al. discovered similar findings, showing a strong relationship between the number of cybersecurity professionals available to combat cyberattacks and their frequency and complexity [45]. In general, people, companies, and educational institutions are more vulnerable to hackers when there are insufficient cybersecurity specialists [46].

The National Initiative for Cybersecurity Education (NICE), a comprehensive resource for knowledge and skill sets relating to the legal, managerial, and social elements of information and cybersecurity, forms the basis of most cybersecurity curricula. Consequently, when developing such a curriculum, "optional courses, within and outside the traditional computer science, computer engineering, information systems management, or information assurance topic areas," must be taken into account [46].

The interdisciplinary nature of cybersecurity work, information sharing regarding cybersecurity work, and the skills required to do tasks that can improve an organization's cybersecurity posture are all described by the NICE Framework, a reference structure [47]. Early cybersecurity education for students is necessary to address the current shortage of cybersecurity specialists since technology and cybersecurity have become more important in the employment market [48].

Many female youth are discouraged from pursuing professions in cybersecurity due to the lack of mentors and counselors, which exacerbates the persistent talent gap [49]. The findings of Hodhod and colleagues [50], who found that women were more likely to discontinue information technology and security courses when they had fewer peer mentors, are supported by Pinchot and colleagues' qualitative study, which involved 25 students [51]. According to Burrell, young people are discouraged from pursuing jobs in cybersecurity due to the lack of professionals and experts in the industry, as they lack role models or mentors [52].

Due to a lack of experts, schools are unable to keep up with the quickly changing cybersecurity world, even with efforts to update the information security curricula [53]. Cybersecurity education needs to be improved or added to school curricula while still giving young girls the support they require. This will close the skills gap for cybersecurity specialists.

2.5.5 Parental Guidance and Supervision

It is crucial to remember that parental supervision and guidance are essential in the field of cybersecurity. In this instance, parents are supposed to be aware of the people their kids are connecting with on the internet. Parents need to make sure that their children's online and offline lives are in harmony with one another. This can be accomplished by investigating and correcting any observable anomalous behavior.

Since the majority of young people now own smart electronic devices, they utilize social media and the Internet more regularly [54]. As a result, parents must monitor and participate in their children's internet activities.

Because of "glamorous" lifestyles, airbrushed body pictures, unattainable beauty standards, and cyberbullying, online platforms encourage the notion that young people's ideas and social behavior are simple and unambiguous rather than nuanced and multifaceted [22]. Most significantly, a new consensus that is founded on "likes" and "favorites" rather than discussion and well-reasoned arguments also influences the

aforementioned behavior [22]. This self-perception may have an impact on one's self-esteem, leading to self-harm and harm to others.

3 Methods

The researchers used the "variation theory," which states that everyone has a unique perspective on the world and experiences it in different ways Orgill [55], and "practical epistemologies," a pragmatist-based strategy [56]. The research methodology selected for this study was Design Science Research Methodology (DSRM). The researchers adopted the DSRM to guide the development of the proposed conceptual framework for increasing CSA among South African youth. Although it is commonly forgotten, design research was first recognized as a field of study in 1966, when the "Design Research Society" was founded [57].

The first section of the study highlighted the problem, and the second section included a literature review that helped develop a conceptual model for raising CSA among the youth. The third component of the study covered the methodologies, data gathering, and analysis. Data was collected using a mixed-method technique. Mixed approaches combine both qualitative and quantitative components to address research questions [58]. Joshi et al. [59] argue that additional qualitative and quantitative studies on youth technology use are required. Mixed methods research can provide a more thorough picture than either quantitative or qualitative research alone since it combines the benefits of both [60]. The researchers adopted [61]'s approach to guide the application of the DSRM in this study and this approach recommends the following steps:

- **Awareness of the problem:** An awareness of a compelling research problem may arise from various sources, including recent advancements in industry or the recognition of problems within an associated discipline; the researchers evaluate criteria for assessing the outcome of the research endeavor. The result of this phase is a proposal, either official or informal, for a new research initiative.
- **Suggestion of a preliminary framework:** The suggestion is directly tied to the problem's awareness. The recommendation is frequently included as an output in the final proposal as a rough design. If a potential answer is not immediately apparent, the proposal may offer a method to create a recommendation.
- **Design and development of the actual framework:** This step involves implementing the tentative design, with varying implementation techniques based on the artifact.
- **Demonstration and evaluation of the framework:** Following development, the artifact must be evaluated, often per the specifications and standards laid out at the proposal stage. The evaluation's outcome needs to be properly documented and explained. In this step, awareness, a suggestion, or a development may be refined, especially if the evaluation's outcome is unsatisfactory.
- **Conclusion of the framework:** The identification of the research findings and contributions occurs in this last stage. This covers not just the artifact but also all extra information learned about its creation, assessment, and handling. This phase's outcome represents a respectable research contribution.

3.1 Sampling Technique

The study used the convenient sampling technique, which selects sample members based on their proximity to the researcher, especially when the target population is rather small [62]. Since the researcher currently resides in the Gauteng province, it was easier for the researcher to reach out to the target population for sampling participants based in Gauteng. The target population for this study included the Gauteng province youth who are between 18–23 years old and have Internet access. Studies that describe the age-related census data from numerous nations show that the accuracy of age information obtained from door-to-door surveys differs depending on a variety of different circumstances and settings [63]. According to Stats's census 2022 statistics, youth of this age are passionate internet users, and it has become a fundamental part of their everyday life [64]. As a result, the researcher in this study requested youth in

the Gauteng province with internet connections to engage in this survey to evaluate the level of awareness of cybersecurity among the youth and highlight youth's perceptions of improving cybersecurity.

3.2 Data Collection

The researcher initiated the data collection process after receiving ethical clearance. Using a mixed-method data-gathering strategy to collect qualitative and quantitative data. The researcher used these data collection methods to empirically address the research objectives of this study. Any study whose conclusions are based only on concrete, verifiable facts is referred to as empirical research [65]. The following subsections briefly discuss the data collection methods employed in this study.

3.2.1 Quantitative Data

In this study, an online and printed questionnaire was administered to participants. The researchers adopted this strategy primarily to encourage participants to answer the questions honestly because they were anonymous [66]. The questionnaire had 33 question items based on a five-point Likert scale created by the researchers. Likert-scale questionnaires are the most often used instruments for evaluating affective variables like motivation and self-efficacy, allowing researchers to easily collect large amounts of data [67]. Structured, closed-ended question items were used to collect pertinent information. The questionnaire has five sections. The first section of the data collected focused on participants' demographics using five question items. The second section of the questionnaire consisted of seven question items, assisting the study in better understanding the need for financial support for CSA. The third section included seven questions, which were designed to better understand the government's support in raising CSA among youth. The fourth section included five questions to help the study better understand the need for education and ongoing cybersecurity training. The final and fifth sections of the questionnaire included nine questions to help better understand the youth's cybersecurity perceptions.

3.2.2 Qualitative Data

Researchers also collected qualitative data using interviews to supplement the collected quantitative data. Participants' involvement in this kind of research supports a methodology that emphasizes personal meaning, applies an inductive method, and stresses the importance of communicating the complexity of a situation [68].

A total of 10 participants who are between 18 and 23 years old and are based in Gauteng (Tshwane) were interviewed. Participants were requested for permission to record conversations, and they were also assured that confidentiality, and their anonymity would be always maintained. Table 1 presents nine questions that were used as the discussion guides for the interviews.

Table 1: Interview questions

	Interview questions
1.	Do you consent to the recording of this interview?
2.	What is your name?
3.	What is your age?
4.	What is your gender?
5.	What is your race?
6.	What is your municipal area?
7.	Do you know CSA?
8.	Are you aware of it (cybersecurity)?
9.	What is your perception of how CSA can be enhanced among the youth in Gauteng?

3.3 Data Analysis

If a study uses actual data to support its conclusion, it is deemed empirical [65]. The questionnaire consisted of 33 items x of which sought to discover participants' demographics. Other question items sought participants' insight about knowledge of cybersecurity and awareness thereof, their perception of cybersecurity and how it can be enhanced as well as cybersecurity education and continuous training. Using the Statistical Package for the Social Sciences (SPSS) software, Version 29, the quantitative data were analyzed and transformed into information. The analysis of the quantitative data comprised one-way Analysis of Variance (ANOVA), Exploratory Factor Analysis (EFA), descriptive variance analysis of responses, and reliability analysis. Before doing EFA, two statistical measures were used to assess the data's factorability, namely the Kaiser-Meyer-Olkin (KMO) measure of sample adequacy and Bartlett's Test of Sphericity (BTS). The KMO measure of sampling adequacy demonstrates how much of the variance in the variables could be related to underlying causes [69]. Table 2 presents KMO and BTS measures. High values of around 1.0 usually indicate that factor analysis can be beneficial for the data [69]. The factor analysis results are unlikely to be very useful if the value is less than 0.50 [69]. The measures in Table 2 are moderate according to the KMO sample measure of 0,759 [70]. However, the dataset is appropriate for the data reduction technique because the BTS sampling significance value is less than 0,001 [71].

Table 2: KMO and Bartlett's test

KMO adequacy		EFA
KMO measure of sampling adequacy.		0.759
BTS	Approx. Chi-Square	1170.803
	df	105
	Sig.	<0.001

To ascertain the level of CSA among South African youth descriptive analysis was conducted. Researchers use descriptive analysis to better understand the collected data [72] by computing frequencies, mean, and standard deviation.

Thematic analysis which is one of Amin [73] five techniques for data analysis were applied to assist the researcher in interpreting the information gathered through interviews. The interview responses were transcribed. To find themes, researchers sort through the data set in search of patterns and significance, as employed in the thematic data analysis approach [74]. The main purpose of collecting qualitative data was to supplement the quantitative data collected through the questionnaire. Thematic data analysis was performed using qualitative data obtained during interviews with ten participants, all of whom gave consent for their comments to be audio-recorded. The participants consisted of four males and six females aged 19 to 21, all of whom were Africans living in the Tshwane municipal region.

Three of the participants were 21 years old, four were 20, and two were 19. Nine of the participants, who were all living in university dormitories, were enrolled in cybersecurity and information technology courses, while one resided off campus and was studying education. After carefully going over the qualitative data, the researcher looked for any patterns or reoccurring themes in the responses. Subsequently, the researcher employed an inductive approach to implement the six-step Dovetail Editorial [75] process, which includes familiarization, coding, theme generation, theme review, theme definition and labeling, and writing up. Sections and numbers were assigned to the transcripts based on their respective contents.

3.4 Ethical Issues

Before gathering the data, the researcher received ethical clearance from the university of study. The first section of the questionnaire provided information on the researcher's project and participants' eligibility to take the survey. The participants were also made aware that the study was voluntary and that they would only be included if they granted their consent. The participants were informed that they may stop filling out the questionnaire at any time without having negative effects. There were no questions on the questionnaire that might be used to identify a specific respondent, making it anonymous.

The participants were informed by the researcher that the questionnaire would be treated confidentially and that the responses would be kept in a secure cloud for five years before being deleted. The datasets will be entirely anonymized, and saved indefinitely on a password-protected computer, and only the researcher will have access to the raw data. The researcher provided her with contact information in case anyone had any questions about the study in general or the items on the questionnaire. The participant consent section of the questionnaire asked respondents to confirm that they had received information about the questionnaire and what was required of them. The participants could then choose to continue with the questionnaire or disregard and quit the questionnaire.

4 Results

4.1 Rotated Component Matrix

The results for the rotated component matrix in Table 3 show that continuous training and education, financial support, government support, and cybersecurity awareness constructs of the proposed conceptual framework were very significant, as their factor loadings were above the standard benchmark of 0.5. The continuous education and training themes in component 1 have a factor loading between 0.783 and 0.909. Financial support themes under component 2 had factor loading values between 0.609 and 0.807. In component 3, government support themes have a factor loading that ranges between 0.792 and 0.884. Finally, in component 4, the cybersecurity awareness themes have factor loading between 0.641 and 0.729. This analysis clearly shows the suitability of these four constructs of the questionnaire categories to evaluate the proposed conceptual model shown in Fig. 1.

Table 3: Rotated component matrix

Rotated component matrix				
	Component			
	1	2	3	4
ECT1	0.909	−0.125	−0.067	−0.036
ECT2	0.899	−0.161	−0.106	0.007
ECT3	0.814	−0.155	0.017	−0.125
ECT4	0.783	−0.231	0.030	0.046
FS5	−0.029	0.807	0.096	−0.034
FS6	−0.268	0.734	0.080	−0.098
FS4	−0.079	0.696	0.185	0.090
FS3	−0.151	0.621	0.074	0.095
FS7	−0.215	0.609	−0.025	0.213
GS2	0.007	0.107	0.884	−0.023
GS3	−0.085	0.058	0.798	0.146
GS1	−0.015	0.176	0.792	−0.139
CAY5	−0.071	0.102	0.176	0.729
CAY8	0.042	−0.026	−0.033	0.690
CAY4	−0.048	0.104	−0.114	0.641

Note: Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalizationa. Rotation converged in 5 iterations. a. Rotation converged in 5 iterations. Education and Continuous Training (ECT); Financial Support (FS); Government Support (GS); Cybersecurity Awareness for the Youth (CAY).

4.2 Quantitative Results

Table 4 displays the age distribution. Out of 260 questionnaires sent out 225 were returned, resulting in an overall response rate of 87%. The actual response rate was 77% since only 200 of the 225 returned surveys were completed correctly, making them valid for this study. Of the participants who completed the questionnaire, 40% were between the ages of 22% and 23%, 37.5% were between the ages of 20% and 21%, and 22.5% were between the ages of 18 and 19 years.

Table 4: Age distribution

Age group	Frequency
18–19	45 (22.5%)
20–21	75 (37.5%)
22–23	80 (40.0%)

Table 5 shows the gender distribution. The male participation in this study was slightly higher than that of females. Of 200 participants, 50.8% of respondents were men, 44.7% were women, and only 4.5% did not disclose their gender.

The results of participants' age distribution make it abundantly evident that older individuals were more inclined to take part than younger ones. Probably, because they may have taken part in related studies, therefore the older volunteers were better equipped to comprehend and respond to the survey of this study.

Table 5: Gender distribution

Gender distribution	Frequency
Male	101 (50.5%)
Female	89 (44.5%)
Undisclosed	10 (5.0%)

The researchers made the study anonymous and did not gather any personal information that could identify the participants because these results are in line with earlier research showing that students are more likely to participate in studies when they feel comfortable sharing their data.

Table 6 displays the race distribution. Of the 200 participants, 67% were African, with 12% White, 8.5% Colored, 9.5% Indian, and 3% from other racial groups.

Table 6: Race distribution

Race distribution	Frequency
African	134 (67.0%)
White	24 (12.0%)
Colored	17 (8.5%)
Indian	19 (9.5%)
Other	6 (3.0%)

With a population of 62 million, South Africa is a developing nation where the majority of people are under 34 [76]. This means that the youth population in South Africa, which consists of 8.80 million women and 9.04 million men, makes up about a third of the country's total population [76]. The results for gender distribution are in line with South Africa's youth population as more males responded than females.

The results of participants' demarcation within the Gauteng province of South Africa are shown in Table 7. Out of 200 respondents, 56% lived in Johannesburg, 26.5% in Tshwane, and 11% in the municipal areas of Ekurhuleni. Another area with a lesser representation of participants is shown in Table 7.

Table 7: Municipal area distribution

Municipal area	Frequency
Ekurhuleni	22 (11.0%)
Johannesburg	112 (56.0%)
Sedibeng	6 (3.0%)
Tshwane	53 (26.5%)
West rand	7 (3.5%)

With 45.7 million people or 80.8% of the overall population, Black South Africans make up the majority [77]. Five million South Africans of color (8.7%), 1.4 million Indian or Asian South Africans (2.6%), and 4.5 million white South Africans (7.9%) make up the remaining population [77]. The results from the

race distribution align with the overall South African population statistics. This affirms that the questionnaire was distributed accordingly.

The devices owned by the respondents are displayed in Table 8. Regarding devices owned by the respondents, the results show that 99% of respondents possessed smartphones, 78% laptops, 26% tablets, and 19.5% shared a laptop or a personal computer.

Table 8: Devices owned by respondents

Type of device	No	Yes
Smartphone	2 (1.0%)	198 (99.0%)
Tablet	148 (74.0%)	52 (26.0%)
Own laptop	44 (22.0%)	156 (78.0%)
Shared laptop/computer	161 (80.5%)	39 (19.5%)

The results for the participants' municipal areas are not surprising, as most of the universities in Gauteng are in Johannesburg and Tshwane regions, these results also affirm that the questionnaire was distributed accordingly within the province of Gauteng.

This study also considered financial support aspects regarding CSA among youth, as an essential construct in the proposed conceptual framework in this study. According to 48% of respondents, as shown in Table 9, they felt that there were not enough financial support options for cybersecurity training, and 70% of respondents indicated that they did not receive financial assistance for cybersecurity training. Shillair et al. outlined several issues facing cybersecurity education which this study aims to verify [78].

Table 9: Financial support

Financial support	SD[1]	N[2]	SA[3]
Received financial assistance to obtain cybersecurity training.	140 (70.0%)	28 (14.0%)	32 (16.0%)
Many financial support options are available for cybersecurity training.	96 (48.0%)	63 (31.5%)	41 (20.5%)
Financial support for proper cybersecurity infrastructure in Gauteng high schools.	118 (59.0%)	50 (25.0%)	32 (16.0%)
Financial support for cybersecurity training and infrastructure in schools.	105 (52.5%)	46 (23.0%)	49 (24.5%)
The government is doing enough to help schools implement proper cybersecurity.	111 (55.5%)	32 (16.0%)	57 (28.5%)
Teachers are receiving financial support for acquiring cybersecurity skills.	111 (55.5%)	52 (26.0%)	37 (18.5%)
Private sector companies are providing financial support for CSA programs in schools.	73 (36.5%)	72 (36.0%)	55 (27.5%)

Note: [1]Strongly Disagree/Disagree (SD), [2]Neither Disagree nor Agree (N), [3]Strongly Agree/Agree (SA).

Furthermore, 59% of respondents indicated that Gauteng schools lacked the funding to establish a strong cybersecurity infrastructure. Also, 55.5% of respondents felt that instructors did not receive adequate

financial help to develop basic cybersecurity abilities. However, respondents' views on the private sector's financial support for CSA campaigns in schools differed slightly, as 31.5% of respondents believed that the government opposed including cybersecurity instruction in the school curriculum, while 52.5% were undecided on the issue. These observations necessitate the need for the can be improved if governments to improve CSA access by implementing cybersecurity education, training, and awareness programs, as proposed by McBride et al. [12].

The results for the types of devices owned by the participants were a little bit surprising as younger children tend to own tablets more than youth. With 99% of the participants owning smartphones, and 78% owning laptops, this observation may serve as a confirmation that the researchers selected the right target of participants as they use these devices for connecting to the internet. Therefore, this information allowed the researcher to determine the status of CSA among the youth participants as presented in this section.

In terms of receiving support from the government, Table 10 shows that 40.5% of the respondents were neutral, while 42.5% believed that the government did not promote CSA among youth in their respective municipal regions. These findings support Mogoane and Kabanda [38] statements that South Africa is one of the few African countries having a robust national cybersecurity policy framework. Compared to 22% who disagreed, 46% of respondents were neutral on the government's support for anti-cyberbullying measures and the development of rigorous legislation for doing so.

Table 10: Government support

Government support	SD[1]	N[2]	SA[3]
The government supports cybersecurity education inclusion in the school curriculum.	66 (31.5%)	105 (52.5%)	32 (16.0%)
The government supports CSA among the youth in my municipal area.	85 (42.5%)	81 (40.5%)	34 (17.0%)
The government supports anti-cyberbullying and has established strict rules to combat cyberbullying.	64 (32.0%)	92 (46.0%)	44 (22.0%)
The government needs to improve the current legal regulations to enable proper integration of social media.	10 (5.0%)	24 (12.0%)	166 (83.0%)
The government needs to enforce increased social media platform accountability in South Africa.	21 (10.5%)	53 (26.5%)	126 (64.0%)
The government is maintaining a global cybersecurity perspective about related laws and policies.	97 (48.5%)	54 (27.0%)	49 (24.5%)
Law enforcement agencies consider cybercrime as a serious offense.	52 (26.0%)	71 (35.5%)	77 (38.5%)

Note: [1]Strongly Disagree/Disagree (SD), [2]Neither Disagree nor Agree (N), [3]Strongly Agree/Agree (SA).

The results for financial support demonstrate the need for financial support in raising the CSA as 70% of the participants strongly disagreed with receiving financial assistance to receive cybersecurity training. This study has repeatedly mentioned the need for financial support when it comes to raising CSA among the

youth, other studies have also demonstrated that financial support is one of the main themes of raising CSA as it can be a challenge to motivate for obtaining financial support.

Only 20.5% of the participants agreed that many financial support options were available for cybersecurity training. This finding further affirms the dire need for financial support in raising CSA among the youth. Also, surprisingly 55.5% of the participants strongly disagreed that the government is doing enough to help schools implement proper cybersecurity. According to 83% of survey respondents, the government must improve the current legislative framework to allow for the integration of social media.

Table 11 below shows that according to 79% of the respondents, cybersecurity teaching should begin in elementary school. This finding is consistent with Gabra et al. [48], who discovered that early cybersecurity education for students is required to address the existing scarcity of cybersecurity specialists. 82% of respondents believe there is a lack of sufficient cybersecurity training resources. Coleman and Reeder [49] reinforce this conclusion, claiming that few educational institutions have the resources necessary to handle security events and raise teachers' and students' knowledge of cybersecurity crises. While 26.5% of respondents disagreed, 33% believed the government was not doing enough to promote continuing cybersecurity education and training. This data supports Armstrong et al. [79] assertion that the cybersecurity teaching or training obtained by students did not match the capabilities desired by businesses.

Table 11: Education and continuous training

Education and continuous training	SD[1]	N[2]	SA[3]
Cybersecurity education should begin in primary schools.	21 (10.5%)	21 (10.5%)	158 (79.0%)
Continuous cybersecurity training should be provided to educators.	17 (8.5%	22 (11.0%)	161 (80.5%)
Continuous cybersecurity training for both the youth and the old should align to global standards.	17 (8.5%)	19 (9.5%)	164 (82.0%)
Lack of proper cybersecurity training resources is a challenge.	10 (5.0%)	27 (13.5%)	163 (81.5%)
The government is not doing enough to foster cybersecurity education and continuous training for the youth.	53 (26.5%)	81 (40.5%)	66 (33.0%)

Note: [1]Strongly Disagree/Disagree (SD), [2]Neither Disagree nor Agree (N), [3]Strongly Agree/Agree (SA).

The results for government support suggest that the youth are unaware of the support from the government to include cybersecurity education in the school curriculum as 52.5% of the participants were neutral. However, 83% of the participants strongly agreed that the government needs to improve the current legal regulations to enable proper integration of social media, clearly demonstrates that the youth yearn for cyber hygiene, and want to feel safe online. Furthermore 64% of the participants also strongly agreed that the government needs to enforce increased social media platform accountability in South Africa. This clearly illustrates the need for government support and to consider the opinions of the youth when it comes to CSA among the youth.

Table 12 below displays that 20% of respondents stated they could not recognize social engineering and phishing emails, while 56% indicated they could. This finding is consistent with the findings of Zhuo

et al. [28], who discovered that phishing victims faced primarily design challenges for phishing emails or websites, as well as anxiety, a lack of education and understanding, and envy of their more affluent counterparts. To prevent the spread of false information, 41% of respondents said they checked news before sharing it on social media, while 35% said they did not. This conclusion supports Dongre [80] admonition that people should be cautious when posting anything online.

Table 12: CSA for the youth

CSA for the youth	SD[1]	N[2]	SA[3]
Recognize social engineering and phishing emails	40 (20.0%)	48 (24.0%)	112 (56.0%)
Check news before sharing it on social media to prevent spreading false information	70 (35.0%)	48 (24.0%)	82 (41.0%)
Use simple passwords that are easy to remember	110 (55.0%)	34 (17.0%)	56 (28,0%)
Genuine name, surname, address, phone number, and pictures are all listed on my web profiles so that anyone can quickly recognize me.	108 (54.0%)	44 (22.0%)	48 (24.0%)
Instead of clicking a hyperlink, I would rather type a URL into a new browser tab.	96 (43.0%)	57 (28.5%)	57 (28.5%)
Feel safer using public Wi-Fi that prompts for password login	75 (37.5%)	45 (22.5%)	80 (40.0%)
Multifactor authentication reduces identity theft.	46 (23.0%)	54 (27.0%)	100 (50.0%)
All location tracking is stopped by turning off GPS location on a smart device.	53 (26.5%)	55 (27.5%)	92 (46.0%)
Aware of the latest phishing techniques	69 (34.5%)	54 (27.0%)	77 (38.5%)

Note: [1]Strongly Disagree/Disagree (SD), [2]Neither Disagree nor Agree (N), [3]Strongly Agree/Agree (SA)

Although 28% of respondents claimed to use simple, easy-to-remember passwords, 55% said they did not. Furthermore, 54% of respondents stated that their personal information, such as their names, surnames, addresses, phone numbers, or photos, were not included in their online accounts, but 24% stated that they were included so that others could readily recognize them. This conclusion is concerning since the level of violence increases when audio-visual shocks, such as voice recordings, photos, and videos, are used as a form of cyberattack [13].

43% of respondents said they would rather click on a hyperlink than enter a URL into a new browser tab, compared to 28.5% who said the same. This supports Das et al. [81] findings that most users simply looked at the first legitimate component of a URL and concluded the website was secure, whereas attackers would have changed the links by adding external ones that direct users to phishing websites. 40% of respondents said they felt safer using public Wi-Fi that required a password login, while 37.5% said they were not comfortable with it at all. 23% of respondents disagreed with the idea that multifactor authentication protects against identity theft, while 50% agreed. These two findings support Mutunhu et al. [82] study, which concluded that universities rarely put online safety principles into practice, and neither staff nor students were aware of the fundamentals of cybersecurity or the best practices for protecting themselves against various forms of assault. 46% of respondents believed that turning off location on a smart device would prevent all location tracking, while 27% disagreed. This conclusion is backed by McAfee [83], who warns that even when location services are disabled, mobile devices can still be tracked. Finally, 38.5% of respondents claimed to be familiar with the most recent phishing methods, while 35% said they were not. This evidence supports Vann [27] the

conclusion that, because they represent the lowest-hanging fruit, hackers will most likely target the old and younger generations.

Results that are shown in Table 12 regarding CSA for the youth indicate that the continuous education and training construct is in line with what the researchers in this current study aim to emphasize. That is, the need for continuous CSA education and training should be aligned to global standards. Proper resources for implementing CSA need to be put in place, which require financial support from both the public and private sectors, as they can be economically costly. Therefore, financial and government support must be achieved through collaboration from both private and public sectors.

According to 56% of the respondents, they can recognize phishing emails. Also, 41% of the respondents said that they verify news on social media before they share it, 55% of the respondents said that they use strong passwords and 54% said they do not use their real names, addresses, and pictures that can identify them.

The results for cybersecurity awareness clearly show the need for cyber hygiene to be enhanced since almost half of the participants are unable to identify phishing emails. A lot of people have lost money due to phishing scams; it is therefore crucial to ensure that CSA is enhanced among the youth, especially the concept of cyber hygiene which can allow them to practice good conduct that is safe online.

4.3 Qualitative Results

Table 13 shows samples of participants' responses and themes together with their subthemes that emerged from the transcribed data. The main themes that emerged include cyber hygiene, cyberattack forms, CSA enhancement, and the cybersecurity introduction stage.

Table 13: Thematic data analysis—sample of themes and responses

Theme	Responses
Cyber hygiene	"They shouldn't use their date of birth [as a password] because most of the time hackers start with that" (Respondent 4).
Complex passwords	"Their passwords should be more complex" (Respondent 4).
Sharing device and online credentials	"I think they [the youth] should be more educated on them [the youth] having to not share their [youth's] personal login details with other persons" (Respondent 4).
Parental supervision	"I think it [CSA] can be enhanced through more parental supervision" (Respondent 3).
	"I can say that parents need to be more involved in their children's online things [profiles and activities] and monitor their [children's] phones" (Respondent 3).
Cyberattack forms	"For example, in a manner where you're [a young person] being cyber-bullied and in instances where people are being hacked and know how to deal with it [cyberattack] when it comes in a bad manner" (Respondent 5).
Cyberbullying	
Hacking	

(Continued)

Table 13 (continued)

Theme	Responses
CSA enhancement Expos Reporting Cybersecurity readiness Cybersecurity as a school subject (Cybersecurity in curriculum)	"The second point that I'd like to mention is that if they [youth] get threatening messages they [youth] should at least try and report it [threatening message] at the nearest police station if they [perpetrators] are trying to access their [the youth's] things [online profiles] without their [the youth's] consent" (Respondent 5). "I think it [CSA] must start at grassroots development level" (Respondent 1). "They [the schools] should give younger people a deeper and more foundation education on Cybersecurity" (Respondent 5). "For me, it is only now that I'm learning about Cybersecurity and how to protect my data" (Respondent 1). "So yes, if they [the schools] can get education on how to kind of prevent or be ready for it [cybersecurity attack]" (Respondent 5). "I believe I as much as electricity education is included from primary school, Cybersecurity should also be included in the school curriculum from grassroots or primary to high school. It [cybersecurity education] must keep on increasing" (Respondent 10). "I think people should be taught how to be aware of their [the youth] passwords" (Respondent 10). "Growing up, if I was exposed to Cybersecurity then, I would know how to protect myself now" (Respondent 1). "In my opinion computer applications technology should be introduced as a compulsory subject in secondary schools because most of the learners in secondary schools do not have the technology knowledge and we are [the youth] moving into 4th industrial revolution" (Respondent 10).
Cybersecurity introduction stages Primary and high school pupils	"Growing up, if I were exposed to Cybersecurity then, I would know how to protect myself [respondent 1] now" (Respondent 1). "They [the government] must take Cybersecurity to primary and high schools so that the learners can know more about it [CSA] earlier" (Respondent 6). "It [CSA] must be included in the curriculum" (Respondents 1 & 6). "I [Respondent 8] think they [the youth] can be taught about it [CSA] in school, starting from primary level of school to high school, so that when they [the youth] go to varsity, they [the youth] know more about it [CSA]" (Respondent 8).

(Continued)

Table 13 (continued)

Theme	Responses
	"More expos can be held in primary and high schools, depending on the outcome, maybe have assignments and such" (Respondent 9).

Participants' responses indicate that cybersecurity should be taught in schools at younger ages, such as primary and secondary schools, as an attempt to "*enhance cybersecurity awareness*." As shown in respondent 5's response, "*They should give younger people a deeper and more foundational education on Cybersecurity*." Also, respondent 6's view supported the need for early-stage education on cybersecurity, stating that "*they must take cybersecurity to primary and high schools so that the learners can know more about it earlier. It must be included in the curriculum*." These views confirm Rahman et al. [84] views that "one of the vital measures to be taken is to cultivate knowledge and awareness among Internet users from their early age, i.e., young children." One of the main themes, "*cybersecurity introduction stages*," emerged from the data indicating the need for youth to be made aware of cybersecurity at an early age, in primary and high schools. As shown in respondent 10's statement, "*In my opinion, computer applications technology should be introduced as a compulsory subject in secondary schools because most of the learners in secondary schools do not know about technology, and we are moving into the 4th industrial revolution*." This observation confirms Omodan and Ige's view that "the cyber insecurities in South Africa became more precarious as schools do not teach cybersecurity as a subject in South Africa at present" [85]. The "cyber hygiene" theme also emerged, which lays out the need for safe online practices and adequate protection of personal data and devices for youth. As shown in respondent 4's statement "*I think people should be taught how to be aware of their passwords. They should not use their date of birth because most of the time hackers start with that. Their passwords should be more complex*." This view confirms Mohammad et al. [3] suggestion that "human factors, including personal, psychological, and cultural factors, play a vital role in determining if an individual will engage in and maintain online safety behaviors such as choosing strong passwords, ensuring that online interactions are secure, and purchasing security-related software to protect their overall privacy."

Following the thematic analysis, researchers conducted content analysis to quantify participants' opinions as shown in Table 14. The quantitative study found that the Department of Education does not have fully integrated cybersecurity instruction in school curricula. Also, according to 79% of interview participants, cybersecurity education and training should be ongoing and start at the elementary school level. Furthermore, 81% of respondents agreed that instructors should receive ongoing cybersecurity training, with 82% believing that it should adhere to global criteria for both adults and youth. One issue raised by 82% of respondents was a lack of appropriate cybersecurity training materials. 33% of respondents thought that the government was not doing enough to encourage youth to continue their cybersecurity education and training, while 27% disagreed. Similar sentiments were also observed in the quantitative results, as 46% of participants felt neutral about the government's support for anti-cyberbullying measures and the adoption of strong legislation, while 22% disagreed. Also, 53% of respondents were unsure about the level of government support for CSA education in schools, while 32% believed that the government was opposed to including cybersecurity education in school curricula. Also, 41% of the questionnaire respondents had a neutral opinion, while 43% disagreed that their local governments effectively promoted CSA among youth. While 56% of respondents said they could identify phishing and social engineering emails, 20% said they could not.

Table 14: Interview responses

Awareness trait	Percentage of responses
Education and continuous training should be ongoing and start at the elementary level	79%
Educators should receive ongoing cybersecurity training	81%
Cybersecurity training should adhere to global standards	82%
There is a lack of appropriate cybersecurity training material	82%
The government not doing enough to foster cybersecurity training and education and continuous training in youth	33%
Able to identify phishing and social engineering emails	56%
Verify news before sharing on social media	41%
Use simple easy-to-remember passwords	28%
Include true full names, photos, addresses, and contact details on online accounts	24%

To prevent the spread of misleading information, 41% of respondents said they examined the news before sharing it on social media, compared to 35% who did not. While 28% of respondents claimed to use simple, easy-to-remember passwords, 55% said they did not. Furthermore, 24% of respondents stated that they included their photos, phone numbers, addresses, true names, and surnames on their internet accounts so that others might easily recognize them, whereas 54% did not.

5 Discussion

The age distribution of the questionnaire and interview participants demonstrates that they were still young enough to understand the issues that the youth face with cybersecurity [86]. The age relevance of 18 to 23 years improved the data collection approach. The quantitative results clearly show that we live in a technologically advanced world, with 99% of participants owning a smartphone. Furthermore, quantitative data highlighted a need for government and financial support to develop CSA among the youth from an early age throughout their school curriculum since most organizations readily give CSA to their employees. During thematic data analysis, cyber hygiene emerged as an essential theme, emphasizing the importance of safe online activities and proper security of youth's data and gadgets. The participants generally agreed that the youth should practice good cyber hygiene by using complex passwords and not sharing their login credentials or devices.

According to Jerman Blažič and Jerman Blažič [87], school curricula should cover topics such as password creation, social media safety, and identifying fake accounts. Cyber hygiene is a critical component that should be integrated into mainstream education and CSA programs. Parental supervision was also emphasized by interview participants, which supports Baldry et al. [88] the argument that parental online monitoring protects the youth from cyberbullying and cyber victimization, but this is dependent on how much the youth trust adults to oversee their lives and help them rather than snooping around, controlling them, or taking away their gadgets. Most respondents agreed that cybersecurity should be taught in both primary and secondary schools to increase CSA. This viewpoint is supported by Rahman et al. (2020:378), who argues that "one of the vital measures to be taken is to cultivate knowledge and awareness among Internet

users from their early age, i.e., young children". A lack of cyber safety education in schools makes students vulnerable to cyberattacks, hence it should be included in both primary and secondary school curricula [89].

5.1 Limitations

There were several limitations that this study encountered. Firstly, only data from the Gauteng province was gathered by the researchers. Gauteng is the most densely inhabited province in South Africa, despite being the smallest. Together, the cities, towns, and urban hubs that comprise the Gauteng city region form South Africa's economic core. The researcher gathered data from Gauteng-based first and second-year university students, who were perfect study participants because they were above the age of eighteen and enrolled in school classes a year or two before this study. Gauteng province is home to many universities, and most university students have access to the internet. For these reasons, the researchers gathered information from Gauteng-based volunteers.

Secondly, in some parts of the questionnaire, participants were required to provide their opinions regarding CSA aspects in schools, while they were no longer in the school context. However, the researchers believe that the sampling was adequate given that until recently (within the last three years) these participants have been in the schools. Therefore, the results obtained, and the evaluation of the proposed conceptual framework were limited in this study.

There were many difficulties in gathering the data using an online link for the questionnaire, particularly because the participants did not know the researcher personally. Another difficulty was the target audience's lack of participation, they typically made empty promises to take the survey and spread the link among their friends but never followed through. Most of the concerns were from people who believed the researcher was trying to con them or was conducting the questionnaire for financial gain, as a result, they chose not to participate. Interviews had to be conducted to supplement the responses obtained from the questionnaire, as a result, this required more data collection.

5.2 Recommendations

To produce a generation of digital natives who can also secure themselves online, school curricula must include cybersecurity education. This study, therefore, recommends the following constructs to help develop and implement youth's cybersecurity awareness Educating the youth on cybersecurity dangers and best practices can foster a sense of responsibility and empower them to make informed decisions to protect themselves and others.

- Early exposure to cybersecurity classes can help students gain a rudimentary understanding of the risks associated with technology.
- Collaboration among educational institutions, parents, and corporate leaders is crucial for educating the youth about cybersecurity.
- Encouraging the youth to participate in cybersecurity and ethical hacking contests increases their interest in technology and provides valuable practical experience.
- Mentorship programs and career pathways provide guidance and assistance for the youth interested in cybersecurity careers.
- CSA efforts should integrate social media and other digital platforms for today's youth, given their familiarity with technology

6 Conclusion

Following the design science research methodology, this study developed a conceptual framework from the literature review. The purpose of this study was to provide a conceptual framework to promote youth CSA. This framework was designed using constructs from literature review, as well as qualitative and quantitative data analysis. The conceptual framework's purpose was to promote cybersecurity education throughout the educational curriculum. The results showed that the proposed conceptual framework constructs, including financial support, government support, cyber hygiene, education and continuous training, and parental guidance and supervision, are suitable for CSA. Results also showed a need for government and financial support to develop CSA for the youth from an early age throughout the school curriculum, preferably starting in both primary and secondary schools. Also, parental supervision and cyber hygiene were emphasized as essential to enable safe activities and adequate security practice online for youth as well as protecting personal data, and gadgets using complex passwords, and avoiding sharing their login credentials or devices.

The study focused on incorporating cybersecurity instruction across the entire school curriculum. Future studies should incorporate perspectives from a wider sample, including parents and the youth. Additionally, future studies need to evaluate the proposed framework from the application perspective. Overall, this study provides comprehensive guidelines as a start for policies that the government can use to enhance cybersecurity awareness for youth, especially in school curricula.

Acknowledgement: The authors wish to firstly thank God Almighty for the opportunity and strength to complete the study. Secondly, the authors thank the supervisor, Professor Lucas Khoza, and the co-supervisor Dr. Fani Radebe for reviewing and providing support and guidance throughout the study. Thirdly, the authors thank Dr. Anesu for assisting with data analysis. Finally, the authors thank Rodwell Chindomu for providing language editing services.

Funding Statement: The authors were partially supported by the FIC during the first year of study. The University of Johannesburg supported the authors by providing financial support for language editing services. The rest of the funding was covered by the authors.

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Kagiso Komane, Lucas Khoza and Fani Radebe; methodology, Kagiso Komane and Fani Radebe; software, Kagiso Komane; validation, Kagiso Komane; formal analysis, Kagiso Komane; investigation, Kagiso Komane; resources, Kagiso Komane and Lucas Khoza; data curation, Kagiso Komane; writing—original draft preparation, Kagiso Komane; writing—review and editing, Kagiso Komane and Fani Radebe; visualization, Kagiso Komane; supervision, Lucas Khoza and Fani Radebe; project administration, Lucas Khoza and Fani Radebe; funding acquisition, Kagiso Komane and Lucas Khoza. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data available on request from the authors.

Ethics Approval: Ethics committee approval has been granted from University of Johannesburg's CBE Research Ethics Committee (Approval No. 2023SCiiS004, Date: 13 March 2023) This study was planned in accordance with the Declaration of Helsinki. Prior to gathering the data, the researcher received ethical clearance from the university of study. The first section of the questionnaire provided information on the researcher's project and participants' eligibility to take the survey. The participants were also made aware that the study was voluntary and that they would only be included if they granted their consent. The participants were informed that they may stop filling out the questionnaire at any time without having negative effects. There were no questions on the questionnaire that might be used to identify a specific respondent, making it anonymous. The participants were informed by the researcher that the questionnaire would be treated confidentially and that the responses would be kept in a secure cloud for five years before being deleted. The datasets will be entirely anonymized, saved indefinitely on a password-protected computer, and only the researcher will have access to the raw data. The researcher provided her contact information in case anyone had any questions about the study in general or the items on the questionnaire. The participant consent section of the questionnaire asked

respondents to confirm that they had received information about the questionnaire and what was required of them. The participants could then choose to continue with the questionnaire or disregard and quit the questionnaire.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Abbreviations

CSA	Cybersecurity awareness
ICT	Information and communication technology
IT	Information technology
SOES	State of email security
DSRM	Design science research methodology
KMO	Kaiser-Meyer-Olkin
BTS	Bartlett's test of sphericity
EU	European Union
ANOVA	Analysis of variance
URL	Uniform resource locator

References

1. Al Shamsi AA. Effectiveness of cyber security awareness program for young children: a case study in UAE. Int J Inf Technol Lang Stud. 2019;3(2):8–29.
2. Vishwanath A, Neo LS, Goh P, Lee S, Khader M, Ong G, et al. Cyber hygiene: the concept, its measure, and its initial tests. Decis Support Syst. 2020;128(1):113160. doi:10.1016/j.dss.2019.113160.
3. Mohammad T, Mohamed Hussin NA, Husin MH. Online safety awareness and human factors: an application of the theory of human ecology. Technol Soc. 2022;68(2):101823. doi:10.1016/j.techsoc.2021.101823.
4. Seok S, DaCosta B. The cyber awareness of online video game players. Int J Cyber Res Educ. 2019;1(1):69–77. doi:10.4018/IJCRE.
5. Esparza J, Caporusso N, Walters A. Addressing human factors in the design of cyber hygiene self-assessment tools. In: Advances in human factors in cybersecurity. Cham, Switzerland: Springer International Publishing; 2020. p. 88–94. doi:10.1007/978-3-030-52581-1_12.
6. Chaudhary S. Driving behaviour change with cybersecurity awareness. Comput Secur. 2024;142(12):103858. doi:10.1016/j.cose.2024.103858.
7. Ahamed B, Polas MRH, Kabir AI, Sohel-Uz-Zaman ASM, Al Fahad A, Chowdhury S, et al. Empowering students for cybersecurity awareness management in the emerging digital era: the role of cybersecurity attitude in the 4.0 industrial revolution era. Sage Open. 2024;14(1):21582440241228920. doi:10.1177/21582440241228920.
8. Markopoulou D, Papakonstantinou V, de Hert P. The new EU cybersecurity framework: the NIS Directive, ENISA's role and the general data protection regulation. Comput Law Secur Rev. 2019;35(6):105336. doi:10.1016/j.clsr.2019.06.007.
9. Alzahrani A. Coronavirus social engineering attacks: issues and recommendations. Int J Adv Comput Sci Appl. 2020;11(5):154–61. doi:10.14569/issn.2156-5570.
10. Catota FE, Morgan MG, Sicker DC. Cybersecurity education in a developing nation: the Ecuadorian environment. J Cybersecur. 2019;5(1):tyz001. doi:10.1093/cybsec/tyz001.
11. Venter IM, Blignaut RJ, Renaud K, Venter MA. Cyber security education is as essential as "the three R's". Heliyon. 2019;5(12):e02855. doi:10.1016/j.heliyon.2019.e02855.
12. McBride M, Carter L, Warkentin M. "Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies 2012 report", RTI International–Institute of Homeland Security Solutions [Internet]. 2012 [cited 2024 May 3]. Available from: https://www.academia.edu/57232522/Exploring_the_Role_of_Individual_Employee_Characteristics_and_Personality_on_Employee_Compliance_with_Cybersecurity_Policies.

13. Jun W. A study on the cause analysis of cyberbullying in Korean adolescents. Int J Environ Res Public Health. 2020;17(13):4648. doi:10.3390/ijerph17134648.
14. Erokhina EV, Letuta TV. Juvenile cybersecurity and artificial intelligence system. In: 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020); Yekaterinburg, Russia; 2020. p. 607–11.
15. Mathew P, Dr RK. Impact of problematic internet use on the self-esteem of adolescents in the selected school, Kerala, India. Arch Psychiatr Nurs. 2020;34(3):122–8. doi:10.1016/j.apnu.2020.02.008.
16. Quayyum F, Cruzes DS, Jaccheri L. Cybersecurity awareness for children: a systematic literature review. Int J Child Comput Interact. 2021;30(2):100343. doi:10.1016/j.ijcci.2021.100343.
17. Pons-Salvador G, Zubieta-Méndez X, Frias-Navarro D. Parents' digital competence in guiding and supervising young children's use of the Internet. Eur J Commun. 2022;37(4):443–59. doi:10.1177/02673231211072669.
18. Social media addiction treatment. Paradigm treatment [Internet]. [cited 2024 May 3]. Available from: https://paradigmtreatment.com/mental-health-treatment-for-teens/social-media-addiction-treatment/.
19. Strimbu N, O'Connell M, Nearchou F, Ó'Sé C. Adaption and psychometric evaluation of the presentation of online self scale in adults. Comput Hum Behav Rep. 2021;3(5):100073. doi:10.1016/j.chbr.2021.100073.
20. Oksanen A, Miller BL, Savolainen I, Sirola A, Demant J, Kaakinen M, et al. Social media and access to drugs online: a nationwide study in the United States and Spain among adolescents and young adults. Eur J Psychol Appl Leg Context. 2020;13(1):29–36. doi:10.5093/ejpalc2021a5.
21. Hasse A, Cortesi S, Lombana-Bermudez A, Gasser U. Youth and cyberbullying: another look. Cambridge, MA, USA: Berkman Klein Center Research Publication; 2019.
22. Alsawalqa RO. Cyberbullying, social stigma, and self-esteem: the impact of COVID-19 on students from east and Southeast Asia at the university of Jordan. Heliyon. 2021;7(4):e06711. doi:10.1016/j.heliyon.2021.e06711.
23. Bergmann M, Baier D. Prevalence and correlates of cyberbullying perpetration. Findings from a German representative student survey. Int J Environ Res Public Health. 2018;15(2):274. doi:10.3390/ijerph15020274.
24. Stoicescu M. The globalized online dating culture: reframing the dating process through online dating. J Comp Res Anthropol Sociol. 2019;10(1):21–32.
25. Sumter SR, Vandenbosch L. Dating gone mobile: demographic and personality-based correlates of using smartphone-based dating applications among emerging adults. New Med Soc. 2019;21(3):655–73. doi:10.1177/1461444818804773.
26. Madigan S, Villani V, Azzopardi C, Laut D, Smith T, Temple JR, et al. The prevalence of unwanted online sexual exposure and solicitation among youth: a meta-analysis. J Adolesc Health. 2018;63(2):133–41. doi:10.1016/j.jadohealth.2018.03.012.
27. Vann R. Phishing for all ages [master's thesis]. San Bernadino, CA, USA: California State University; 2021.
28. Zhuo S, Biddle R, Koh YS, Lottridge D, Russello G. SoK: human-centered phishing susceptibility. ACM Trans Priv Secur. 2023;26(3):1–27. doi:10.1145/3575797.
29. Chaudhry JA, Ahmad Chaudhry S, Rittenhouse RG. Phishing attacks and defenses. Int J Secur Appl. 2016;10(1):247–56. doi:10.14257/ijsia.2016.10.1.23.
30. Taherdoost H. A Critical review on cybersecurity awareness frameworks and training models. Procedia Comput Sci. 2024;235(3):1649–63. doi:10.1016/j.procs.2024.04.156.
31. Govender S, Kritzinger E, Loock M. A framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture. Pers Ubiquitous Comput. 2021;25(5):927–40. doi:10.1007/s00779-021-01549-w.
32. Khader M, Karam M, Fares H. Cybersecurity awareness framework for academia. Information. 2021;12(10):417. doi:10.3390/info12100417.
33. Warnekar SS, Khandhadia R, Balakrishnan V, Gathani S. Integrating sustainability in K-12 schools: the GSF schools model. Glob J Educ Thoughts. 2024;1(1):82–93.
34. Radway S, Ludden C, Quintanilla K, Votipka D. An investigation of US universities' implementation of FERPA student directory policies and student privacy preferences. In: CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems; 2024 May 11–16; Honolulu, HI, USA. p. 1–35.

35. Jalil M, Ali NH, Yunus F, Zaki FAM, Hsiung LH, Almaayah MA. Cybersecurity awareness among secondary school students post COVID-19 pandemic. J Adv Res Appl Sci Eng Technol. 2024;37(1):115–27. doi:10.37934/araset.37.1.115127.
36. Sadiku MNO, Chukwu UC, Sadiku JO. Cybersecurity for education. EJINE. 2023;3(6):182–8.
37. Vegesna VV. Cybersecurity of critical infrastructure. Int Machine Learn J Comput Eng. 2024;7(7):1–17.
38. Mogoane SN, Kabanda S. Challenges in information and cybersecurity program offering at higher education institutions. In: Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems; Johannesburg, South Africa; 2019. p. 202–12.
39. O'Brien C. Teachers' perceptions about use of digital games and online resources for cybersecurity basics education: a case study [dissertation]. Ann Arbor, MI, USA: Capella University; 2019.
40. Sreedevi AG, Nitya Harshitha T, Sugumaran V, Shankar P. Application of cognitive computing in healthcare, cybersecurity, big data and IoT: a literature review. Inf Process Manag. 2022;59(2):102888. doi:10.1016/j.ipm.2022.102888.
41. Pencheva D, Hallett J, Rashid A. Bringing cyber to school: integrating cybersecurity into secondary school education. IEEE Secur Priv. 2020;18(2):68–74. doi:10.1109/MSEC.2020.2969409.
42. Dunn M, Merkle L. Overview of software security issues in direct-recording electronic voting machines. In: Proceedings of the 13th International Conference on Cyber Warfare and Security; Washington, DC, USA; 2018. p. 201–9.
43. HM Government. National cyber security strategy 2016–2021 [Internet]. 2016 [cited 2024 Sep 30]. Available from: https://assets.publishing.service.gov.uk/media/5a81914de5274a2e8ab54ae9/national_cyber_security_strategy_2016.pdf.
44. Mountrouidou X, Vosen D, Kari C, Azhar M, Bhatia S, Gagne G, et al. Securing the human: a review of literature on broadening diversity in cybersecurity education. In: ITiCSE 19. Aberdeen, UK: Innovation and Technology in Computer Science Education; 2019. p. 157–76.
45. Hart S, Margheri A, Paci F, Sassone V. Riskio: a serious game for cyber security awareness and education. Comput Secur. 2020;95(2):101827. doi:10.1016/j.cose.2020.101827.
46. Triplett WJ. Addressing cybersecurity challenges in education. Int J STEM Educ Sustain. 2023;3(1):47–67. doi:10.53889/ijses.v3i1.132.
47. Petersen R, Santos D, Smith MC, Wetzel KA, Witte G. Workforce framework for cybersecurity (NICE Framework). Gaithersburg, MD, USA: National Initiative for Cybersecurity Careers and Studies; 2020.
48. Garba A, Sirat MB, Hajar S, Dauda IB. Cyber security awareness among university students: a case study. Sci Prcd Ser. 2020;2(1):82–6. doi:10.31580/sps.v2i1.1320.
49. Coleman CD, Reeder E. Three reasons for improving cybersecurity instruction and practice in schools. In: 29th Proceedings of the Society for Information Technology and Teacher Education International Conference (SITE 2018); 2018 Mar 26–30; Washington, DC, USA. p. 1020–5.
50. Hodhod R, Khan S, Wang S. CyberMaster: an expert system to guide the development of cybersecurity curricula. Int J Onl Eng. 2019;15(3):70–81. doi:10.3991/ijoe.v15i03.9890.
51. Pinchot J, Cellante D, Mishra S, Paullet K. Student perceptions of challenges and role of mentorship in cybersecurity careers: addressing the gender gap. Inf Syst Educ J. 2020;18(3):44–53.
52. Burrell DN. An exploration of the cybersecurity workforce shortage. In: Cyber warfare and terrorism: concepts, methodologies, tools, and applications. Hershey, PA, USA: IGI Global; 2020. p. 1072–81. doi:10.4018/978-1-7998-2466-4.ch063.
53. Sanzo KL, Paredes Scribner J, Wu H. Designing a K-16 cybersecurity collaborative: cipher. IEEE Secur Priv. 2021;19(2):56–9. doi:10.1109/MSEC.2021.3050246.
54. Quayyum F, Bueie J, Cruzes DS, Jaccheri L, Vidal JCT. Understanding parents' perceptions of children's cybersecurity awareness in Norway. In: Proceedings of the Conference on Information Technology for Social Good; Roma, Italy; 2021. p. 236–41. doi:10.1145/3462203.3475900.
55. Orgill M. Variation theory. In: Encyclopedia of the sciences of learning. Boston, MA, USA: Springer; 2012. p. 3391–3. doi:10.1007/978-1-4419-1428-6_272.

56. Wickman PO. The practical epistemologies of the classroom: a study of laboratory work. Sci Educ. 2004;88(3):325–44. doi:10.1002/sce.10129.
57. Roworth-Stokes S. The design research society and emerging themes in design research. J Product Innov Manag. 2011;28(3):419–24. doi:10.1111/j.1540-5885.2011.00815.x.
58. George T. Mixed methods research: definition, guide & examples. Scribbr. [Internet]. 2025 [cited 2025 Jan 20]. Available from: https://www.scribbr.com/methodology/mixed-methods-research/.
59. Joshi SV, Stubbe D, Li ST, Hilty DM. The use of technology by youth: implications for psychiatric educators. Acad Psychiatry. 2019;43(1):101–9. doi:10.1007/s40596-018-1007-2.
60. Ivankova NV, Creswell JW, Stick SL. Using mixed-methods sequential explanatory design: from theory to practice. Field Meth. 2006;18(1):3–20. doi:10.1177/1525822x05282260.
61. Vaishnavi V, Kuechler B, Petter S. Design science research in information systems [Internet]. Computer Information Systems Department, Georgia State University; 2004 [cited 2024 May 23]. Available from: http://www.dphu.org/uploads/attachements/books/books_3407_0.pdf.
62. Obilor EI. Convenience and purposive sampling techniques: are they the same? Int J Innov Soc Sci Educ Res. 2023;11(1):1–7.
63. Pardeshi GS. Age heaping and accuracy of age data collected during a community survey in the yavatmal district. Maharashtra Indian J Community Med. 2010;35(3):391–5. doi:10.4103/0970-0218.69256.
64. Statistics South Africa. Census 2022: statistical release P0301.4 [Internet]. Pretoria: Statistics South Africa; 2023 [cited 2024 May 23]. Available from: https://census.statssa.gov.za/assets/documents/2022/P03014_Census_2022_Statistical_Release.pdf.
65. Bouchrika I. What is empirical research? Definition, types & samples in 2024 [Internet]. [cited 2024 May 23]. Available from: https://research.com/research/what-is-empirical-research.
66. Barlett CP, Heath JB, Madison CS, DeWitt CC, Kirkpatrick SM. You're not anonymous online: the development and validation of a new cyberbullying intervention curriculum. Psychol Pop Medium. 2020;9(2):135–44. doi:10.1037/ppm0000226.
67. Nemoto T, Beglar D. Developing likert-scale questionnaires. In: JALT2013 Conference Proceedings; Tokyo, Japan; 2014. p. 1–8.
68. Creswell J. Research design: qualitative, quantitative, and mixed methods approaches; 2009.
69. Li N, Huang J, Feng Y. Construction and confirmatory factor analysis of the core cognitive ability index system of ship C2 system operators. PLoS One. 2020;15(8):e0237339. doi:10.1371/journal.pone.0237339.
70. Glen S. Kaiser-Meyer-Olkin (KMO) test for sampling adequacy. Statistics How To [Internet]. 2023 [cited 2024 Sep 30]. Available from: https://www.statisticshowto.com/kaiser-meyer-olkin/.
71. Zach B. A guide to Bartlett's test of sphericity. Arab Psychology. [Internet]. 2019 [cited 2024 Sep 30]. Available from: https://stats.arabpsychology.com/a-guide-to-bartletts-test-of-sphericity/.
72. Runeson P, Höst M. Guidelines for conducting and reporting case study research in software engineering. Empir Software Eng. 2009;14(2):131–64. doi:10.1007/s10664-008-9102-8.
73. Amin H. 5 qualitative data analysis methods. Verywell Mind [Internet]. 2023 [cited 2024 Sep 30]. Available from: https://www.verywellmind.com/5-qualitative-data-analysis-methods-5196973.
74. Naeem M, Ozuem W, Howell K, Ranfagni S. A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. Int J Qual Meth. 2023;22(11):16094069231205789. doi:10.1177/16094069231205789.
75. Dovetail Editorial Team. How to do thematic analysis. Dovetail [Internet]. 2023 [cited 2024 Sep 30]. Available from: https://dovetail.com/research/thematic-analysis.
76. Selala C. The government roll out of the 2024 youth month by committing to acceleration of opportunities for youth empowerment and skills development [Internet]. 2024 [cited 2025 Apr 20]. Available from: https://www.dsac.gov.za/Thegovernmentcommittingtoaccelerationofopportunitiesforyouthempowermentandskillsdevelopment#:.
77. Gateway SA. South Africa's population [Internet]. 2023 [cited 2025 Apr 20]. Available from: https://southafrica-info.com/people/south-africa-population/#:.

78. Shillair R, Esteve-González P, Dutton WH, Creese S, Nagyfejeo E, von Solms B. Cybersecurity education, awareness raising, and training initiatives: national level evidence-based results, challenges, and promise. Comput Secur. 2022;119(3):102756. doi:10.1016/j.cose.2022.102756.
79. Armstrong ME, Jones KS, Namin AS, Newton DC. The knowledge, skills, and abilities used by penetration testers: results of interviews with cybersecurity professionals in vulnerability assessment and management. Proc Hum Factors Ergon Soc Annu Meet. 2018;62(1):709–13. doi:10.1177/1541931218621161.
80. Dongre P. Social media use patterns: some observations. Amoghvarta. 2023;3(4):67–70.
81. Das S, Nippert-Eng C, Camp LJ. Evaluating user susceptibility to phishing attacks. Inf Comput Secur. 2022;30(1):1–18. doi:10.1108/ICS-12-2020-0204.
82. Mutunhu B, Dube S, Ncube N, Sibanda S. Cyber security awareness and education framework for zimbabwe universities: a case of national university of science and technology. In: Proceedings of the International Conference on Industrial Engineering and Operations Management; 2022 Apr 5–7; Nsukka, Nigeria.
83. McAfee E. Can my phone be tracked if location services are off? McAfee [Internet]. 2023 [cited 2025 Apr 20]. Available from: https://www.mcafee.com/learn/can-my-phone-be-tracked-if-location-services-are-off/.
84. Rahman NAA, Sairi IH, Zizi NAM, Khalid F. The importance of cybersecurity education in school. Int J Inf Educ Technol. 2020;10(5):378–82. doi:10.18178/ijiet.2020.10.5.1393.
85. Omodan BI, Ige OA. University students' perceptions of curriculum content delivery during COVID-19 new normal in South Africa. Qual Res Educ. 2021;10(2):204. doi:10.17583/qre.2021.7446.
86. Chang V, Golightly L, Xu QA, Boonmee T, Liu BS. Cybersecurity for children: an investigation into the application of social media. Enterp Inf Syst. 2023;17(11):2188122. doi:10.1080/17517575.2023.2188122.
87. Jerman Blažič B, Jerman Blažič A. Cybersecurity skills among European high-school students: a new approach in the design of sustainable educational development in cybersecurity. Sustainability. 2022;14(8):4763. doi:10.3390/su14084763.
88. Baldry AC, Sorrentino A, Farrington DP. Cyberbullying and cybervictimization versus parental supervision, monitoring and control of adolescents' online activities. Child Youth Serv Rev. 2019;96(3):302–7. doi:10.1016/j.childyouth.2018.11.058.
89. Kritzinger E, Bada M, Nurse JRC. A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In: Information security education for a global digital society. Cham, Switzerland: Springer International Publishing; 2017. p. 110–20. doi:10.1007/978-3-319-58553-6_10.