Volume: 5 Issue: 5 Pages: 13-22

Stay Smart, Stay Safe: Exploring Cyber Hygiene and Digital Awareness

[*1] Dr. Bindu VV, [2]Pournami CP, [3]Abhirami O and [4]Arunima M

[*1] Associate Professor, Department of Economics, S.N. College, Kannur, Kerala, India.
2,3,4 BA Economics S.N. College, Kannur, Kerala, India.

Article Info.
E-ISSN: 2583-6528
Impact Factor (QJIF): 8.4
Peer Reviewed Journal
Available online:
www.alladvancejournal.com

Received: 03/April/2026
Accepted: 04/May/2026

***Corresponding Author**
Dr. Bindu VV
Associate Professor, Department of Economics, S.N. College, Kannur, Kerala, India.

Abstract
The rapid growth of internet usage and digital technology has significantly transformed communication, education, business, and social interaction. However, along with these advancements, cyber threats and cyber-crimes have also increased at an alarming rate. Many internet users rely heavily on personal computers and digital devices for daily activities, yet not all individuals possess adequate knowledge or awareness of safe online practices. A lack of proper cyber hygiene and insufficient awareness of cyber security measures can make users vulnerable to cyber-crimes such as phishing, hacking, identity theft, online fraud, and malware attacks. Therefore, the problem addressed in this study is the need to assess and analyse the level of awareness about cyber hygiene practices among different age groups and genders, and to evaluate the level of awareness regarding safety while using personal computers and the internet in relation to cyber- crimes. The objectives of the study are identifying the level of awareness about cyber hygiene practices among internet users and also to find out the depth of understanding among internet users regarding cybercrime risks and safety practices while using the internet. Identifying variations and gaps in awareness is essential to develop effective educational strategies, awareness programs, and preventive measures aimed at promoting safer digital behaviour and reducing vulnerability to cyber threats.

Keywords: Hacking, phishing, malware attacks, cyber threats, cyber hygiene, digital engagement.

Introduction

In today's digital age, the use of internet and connected devices has become an essential part of our daily life. The rapid expansion of digital technology and internet usage has transformed the way people communicate, learn, work and conduct financial transactions. The twenty first century has witnessed an unprecedented growth in digital technology and internet connectivity. The integration of digital devices into everyday life has revolutionized communication, education, commerce, healthcare, banking, governance, and entertainment.

From online banking and education to communication and business operations, digital platforms play a crucial role in modern society. Computers, smart phones and online platforms have become deeply integrated into everyday life across all age groups. While the digital growth offers convenience and efficiency, it also exposes users to various cyber risks such as hacking, phishing, identity theft, date leakage, malware attacks, and online fraud. As cyber threats continue to increase in frequency and sophistication, the importance of safe online behavior has become more critical than ever. In this context, cyber hygiene practices have emerged as a necessary preventive approach to ensure safe and secure digital behavior.

One of the most important preventive approaches to cyber threats is the practice of cyber hygiene. Cyber hygiene refers to the set of regular practices and preventive measures that individuals follow to maintain the security and health of their digital devices, networks, and personal data. These practices include using strong and unique passwords, updating software and antivirus programs, recognizing suspicious emails and links, securing personal information, enabling privacy settings, and practicing safe browsing habits. Just as personal hygiene prevents digital threats and reduces vulnerability to cybercrimes.

Awareness plays a key role in the effectiveness of cyber hygiene practices. Awareness includes understanding different types of cybercrimes, recognizing early warning signs of digital threats, knowing preventive measures, and being informed about reporting mechanisms. The level of

awareness significantly influences online behavior and risk exposure. Individuals with higher awareness are more likely to adopt safe browsing habits, verify website authenticity, use security tool, and protect, sensitive data.

Different age groups and genders may show varying levels of knowledge, attitudes, and behavior toward cyber security measures. Younger uses may be more technologically active but not always cautious, while older users may lack technological awareness. Similarly, usage patterns and safety awareness can differ across gender groups due to differences in exposure, training, and digital engagement. Understanding these variations is important for designing targeted awareness programs and preventive strategies. Despite increasing awareness campaigns and technological safeguards, many internet users still demonstrate inadequate knowledge and inconsistent implementation of cyber hygiene measures.

In addition, many internet users are not fully aware of the safety measures required while using personal computers and online services. Unsafe practices such as using weak passwords, sharing personal data, ignoring security updates, and clicking unknown links increase the risk of cybercrime. Therefore, assessing user awareness about safe computer and internet usage is essential for strengthening cyber security culture. The rapid expansion of digital services such as online banking, e-commerce, cloud storage, and remote work environments has increased the need for personal accountability in maintaining cyber security. As cyber threats continue to evolve in complexity and frequency, individual users represent the first line of defense against cybercrime. Therefore, understanding the current level of awareness among internet users becomes essential in developing effective preventive measures.

By collecting and analyzing data from internet users, this project aims to evaluate their knowledge, attitudes, and behavioral practices related to cyber security. It aims to examine the concept of cyber hygiene, its importance, key practices, and its role in reducing cyber risks. It also highlights how awareness, education, and responsible online behavior can significantly improve cyber security at both individual and organizational levels. By understanding and adopting proper cyber hygiene practices, users can create a safer digital environment and reduce vulnerability to cyber-attacks.

The findings of this project are expected to reveal strength and gaps in awareness levels and provide insights into demographic differences. The findings may help the educational institutions, policymakers, and community organizations develop effective awareness campaigns and training programs. Strengthening cyber hygiene practices and promoting responsible internet usage are essential steps toward building a safer digital environment for all users. As society becomes increasingly dependent on digital technology, enhancing cyber security awareness is not only a personal responsibility but also a collective necessity.

Materials and Methods

Review of Literature

O'Connell (2012) challenges the prevailing trend of militarizing cybersecurity, emphasizing instead the importance of regulating cyber activity under international law governing economic and communication activity. The article highlights key historical events, including the 2007 cyber-attacks on Estonia, the 2008 Russia–Georgia conflict, and the deployment of the Stuxnet worm against Iran, to illustrate the shift toward a military response to cyber threats. O'Connell warns that these responses often ignore international legal frameworks and instead rely on outdated Cold War deterrence logic. Instead, O'Connell proposes that cyberspace should be governed through existing principles of international law, including rules on non-intervention, economic law, and communication rights, rather than those on the use of force.

Von Solms and Van Niekerk (2013) provided distinction between information security and cyber security. They argue that although both terms are often used interchangeably, cyber security encompasses a broader scope. Cyber security addresses the protection of not only digital information but also the physical and societal aspects that may be affected through cyberspace (Von Solms & van Niekerk, 2013). The authors illustrate this distinction through several scenarios such as cyberbullying, home automation attacks, digital media piracy, and cyber terrorism. The paper concludes by advocating for the recognition of cyber security as a distinct and expanded field of study.

Budu, Yinping, and Mireku (2018) investigated how behavioural intention influences the adoption and usage of e-learning systems among students in Ghanaian tertiary institutions. Prior research by Venkatesh *et al*. (2003) established that factors such as performance expectancy, effort expectancy, and social influence significantly affect users' intentions to adopt digital tools. Budu *et al*. (2018) confirmed these relationships within the African educational context, highlighting that students' perceptions of e-learning benefits, ease of use, and peer influence directly impact their willingness to engage with such platforms. Furthermore, the study underlines the importance of institutional support and user confidence in fostering effective digital learning environments. These findings support global research on e-learning adoption while adding a contextual dimension specific to the challenges and opportunities in Ghana's higher education system.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018) investigates the knowledge and behaviours related to cyber hygiene among end users, emphasizing the critical role users play in maintaining cybersecurity. The authors identify that despite the widespread awareness of cybersecurity threats, many users still exhibit poor cyber hygiene practices such as password reuse, lack of regular software updates, and susceptibility to phishing scams. The literature review explores previous studies that show discrepancies in the reported usage of antivirus software, firewall configurations, and security behaviours across different demographics. For example, one study cited found that 67% of users lacked antivirus protection, while another found that 97% had it-highlighting inconsistencies in past research. The authors further detail how individual characteristics such as age, gender, training, and perceived expertise influence security practices. Notably, older users were found to engage in more secure behaviours.

Mughal (2019**)** examined the importance of cyber security hygiene in the era of the Internet of Things (IoT), focusing on both best practices and the challenges organizations face. The research highlighted that as IoT devices become more integrated into critical infrastructure and personal environments, the aftermath of security incidents becomes increasingly severe. Mughal emphasized that maintaining cyber security hygiene is essential to prevent vulnerabilities and manage threats in complex IoT ecosystems. Key recommendations included routine updates, strong authentication protocols, network segmentation, and user

awareness training. The findings concluded that without consistent cyber security hygiene practices, IoT networks remain highly susceptible to exploitation.

Fatokun, Hamid, Norman, and Fatokun (2019) conducted an empirical investigation to analyze how demographic variables-specifically age, gender, and educational level-affect cybersecurity behaviours among students in Malaysian tertiary institutions. Their findings align with existing literature suggesting that demographic factors play a significant role in shaping online security practices. Previous studies have established that older students often exhibit more cautious digital behaviour due to increased awareness and life experience (Nguyen *et al*., 2017). Gender differences also emerge in cyber behaviour, with females generally demonstrating more risk-averse practices compared to males (Tian & Zhang, 2018). Furthermore, educational level correlates with cybersecurity awareness; postgraduate students are typically more informed and proactive than undergraduates, possibly due to increased academic exposure and digital responsibilities (Alotaibi & Alfehaid, 2016). The research by Fatokun *et al*. (2019) supports and extends these observations within the Malaysian university context, highlighting the need for tailored cyber security awareness programs that consider these demographic variables.

Vishwanath, Neo, Goh, Lee, and Khader (2020) addressed the conceptual gap in the understanding of cyber hygiene by defining the term, developing a measurement scale, and conducting initial empirical tests. Their study proposed a structured framework that views cyber hygiene as a set of habitual, proactive security behaviours individuals perform to protect digital environments. Using surveys and empirical validation, the researchers tested their measurement instrument and found it to be both valid and reliable. The results supported the existence of distinct behavioural dimensions of cyber hygiene, including routine updates, password practices, and cautious online behaviour. This work significantly contributes to the literature by offering a standardized way to measure cyber hygiene, enabling more accurate future assessments and interventions aimed at enhancing individual cybersecurity behaviours.

Panda *et al*. (2020) highlight the limitations of generic cybersecurity recommendations in healthcare, where user roles and risks vary greatly. The authors introduce the Optimal Safeguards Tool (OST), which uses game theory and combinatorial optimization to select the most effective cyber hygiene measures for different user groups. Building on Fielder *et al*.'s (2016) hybrid cybersecurity investment model, OST considers the likelihood of attacks, asset value, training costs, and user-specific safeguard effectiveness.

Bognár and Bottyán (2021) addressed a significant gap in cyber security research by developing and validating a personal cyber security awareness scale tailored specifically for university students. Their work highlights the increasing demand for reliable tools to measure online security behaviour within the academic context. Prior studies have emphasized that while students are digitally active, they often lack consistent and informed cyber security practices (Hadlington, 2017).

Ugwu, Ani, Ezema, and Asogwa (2022) conducted an online study to examine the influence of age and educational level on cyber hygiene among students and employees. The study aimed to understand how demographic factors affect cyber hygiene culture and behaviour. The authors found that both age and educational attainment significantly influence cyber hygiene practices. The research revealed that many participants-especially younger individuals and those with lower levels of education-exhibited low cyber hygiene culture, such as weak password practices and limited awareness of security protocols. Conversely, participants with higher educational backgrounds and older age groups demonstrated better cyber hygiene behaviours.

Ghelani (2022) reviews cybersecurity strategies in the context of Industry 4.0, emphasizing a shift from purely technical defences to more integrated approaches. The study highlights that most organizations rely on prevention tools like firewalls and encryption but often overlook broader strategies like deterrence, surveillance, and detection. The author stresses the need for proactive security planning and integrating cybersecurity into organizational strategy. Emerging technologies such as IoT and AI introduce new threats, especially in manufacturing and healthcare, where digital and physical systems interact. Ghelani concludes that future cybersecurity must combine technology, people, and processes to build resilient and adaptive defences.

Barakovic and Barakovic Husic (2023) explored the concept of cyber hygiene practices by investigating the knowledge, awareness, and behavioural practices of university students in Bosnia and Herzegovina. Their study is grounded in the increasing need for cyber security due to the growing cyber-attacks, especially in the post COVID-19 digital environment. The authors emphasized that while technical solutions exist, human behavior remains a critical factor in cyber security. Knowledge involves technical skills like password management (Cain *et al*., 2018), awareness reflects threat sensitivity (Zwilling *et al*., 2020) and behaviour includes practices like backups and software updates (Ovelgonne *et al*., 2017). The study found that demographic factors (including gender and education level) influence cyber hygiene and revealed knowledge gaps despite moderate awareness and behaviour.

Fikry, Hamzah, and Hussein (2023) conducted a study on cyber hygiene practices among professional youth in Malaysia, focusing on how cyber security knowledge influences online safety behaviour. The research assessed practices such as using strong passwords, updating software, safe browsing, and recognizing cyber threats.

Mtambeka, Mtegha, and Chigona (2023) investigated the factors that influence university students' compliance with cyber security measures in South Africa, recognizing the rising threat of cyber-attacks in higher education due to increased ICT usage. The study aimed to understand why some students fail to adopt safe cyber practices despite awareness efforts. Using a mixed-methods approach, the researchers identified several significant factors influencing compliance: perceived vulnerability, awareness, institutional support, and self-efficacy. The findings showed that students with higher levels of cyber security awareness and confidence in their ability to protect themselves were more likely to comply with security protocols. The study concluded that improving compliance among students requires a holistic approach that enhances awareness, builds technical confidence, and reinforces institutional support through consistent cyber security education and enforcement.

Oliveira *et al*. (2023) conducted a cross-national study that evaluates cybersecurity awareness levels among first-year computer science students in Portugal and Poland. Their work fills a vital gap in the literature, which has often been limited to single-country or single-institution analyses. Prior research has extensively explored cyber security awareness within local contexts. For example, Alharbi and Tassaddiq (2021)

evaluated cyber security understanding among students in Saudi Arabia, identifying gaps in practical security behaviour. Chandarman and van Niekerk (2017) found discrepancies between self-perceived and actual cyber security skills among South African students, suggesting the need for targeted education. Similarly, Garba *et al*. (2020) studied Nigerian students, concluding that while awareness existed, data protection practices remained weak, especially among female students.

Podlinyayeva and Sytnyk (2023) present a comprehensive examination of cyber hygiene practices, emphasizing the need for educational interventions to promote safe and responsible digital behaviour, particularly among school-aged children. The article begins by contextualizing the urgency of cybersecurity awareness within the backdrop of the COVID-19 pandemic and ongoing geopolitical instability, which accelerated the digital transformation of educational and public services. Central to the authors' discussion is the concept of cyber hygiene, defined as a set of practices aimed at maintaining digital security and minimizing cyber threats. These include using strong passwords, regularly updating software, being cautious with digital communications, and employing antivirus protection. The article extensively details age-appropriate strategies for instilling cyber hygiene habits in children, ranging from simple concepts like avoiding personal information sharing for pre-schoolers to complex topics such as phishing awareness and digital footprints for adolescents.

Basholli *et al*. (2023) explore the critical role of education in promoting cyber hygiene amidst rapid digitalization, particularly in Albania. As cyber threats such as malware, phishing, and data breaches become increasingly prevalent, the authors argue that mere technological defence are insufficient without an informed and aware user base. The study highlights that human error remains the primary cause of security breaches, making education a key pillar in cybersecurity frameworks. The authors advocate for collaborative strategies, including government involvement, NGO-led awareness programs, and private sector partnerships to strengthen educational efforts.

Ugwu *et al*. (2023) explored the multifaceted relationship between cyber hygiene practices and demographic variables such as gender, employment status, and academic discipline among university students. The study was grounded in the increasing concern over cyber security threats in educational environments, especially as students' online presence continues to grow. Prior research highlights that cyber hygiene awareness varies widely among students based on personal and academic characteristics (Akhter & Sultana, 2020). For instance, male students are often perceived to engage in riskier online behaviours compared to their female counterparts, though some studies argue this gap is narrowing with increased digital literacy (Kumar & Singh, 2021). Employment status may also influence cyber hygiene, as working students might develop stronger digital security habits due to workplace exposure (Cheng *et al*., 2019). Additionally, students in technology-oriented disciplines tend to exhibit more proactive cyber hygiene behaviours than those in the humanities (Aliyu & Bello, 2022). The current study by Ugwu *et al*. (2023) contributes to this evolving discourse by offering empirical data from a Nigerian university context, emphasizing the urgent need for targeted cyber hygiene education policies.

Berdi, Niyazova, and Bayterekova (2024) conducted a study exploring the relationship between digital hygiene skills and the reduction of cyberbullying among teenagers in Kazakhstan. Their research found that when adolescents received education on digital hygiene practices, there was a notable decrease in both experiencing and perpetrating cyberbullying behaviours. These findings suggest that enhancing digital literacy and awareness can serve as a proactive method to combat online harassment. This approach not only reduces the likelihood of cyberbullying but also strengthens young people's understanding of cybersecurity and ethical digital behaviour (Berdi *et al*., 2024). Howell, Maimon, Muniz, and Kamar (2024) conducted a study exploring the impact of thoughtful decision-making and informational interventions on individuals' engagement in cyber hygiene practices. The research emphasized that the adoption of proper cyber hygiene is not solely a technical matter but also strongly influenced by individual-level decision-making and access to informational resources. Results of the study revealed that informational nudges and structured awareness programs significantly improved individuals' proactive cyber security behaviors, including password management, software updates, and threat recognition.

Bhandari, Sree, and Kakar (2024) explored the consequences of neglecting digital hygiene among youth and its relationship to online behaviour. The researchers applied a behavioural framework to assess how attitudes, perceived behavioural control, and subjective norms affect the intentions of youth to engage in cyber aggression. The findings indicated that attitudes and perceived behavioural control were significant predictors of youth's intentions to commit cyber aggression, whereas subjective norms had no significant impact.

Fikry, Hamzah, and Hussein (2024) offer a comprehensive conceptual review of cyber hygiene, focusing on its theoretical underpinnings and practical dimensions. The research results highlight that cyber hygiene encompasses four key dimensions: practices, knowledge, behaviour, and attitude. These components collectively influence how individuals interact with digital systems and defend against cyber threats. The study also underscores the need for a clearer definition of cyber hygiene to support education, policy-making, and behaviour change.

Shah *et al*. (2024) investigate the relationship between cyber hygiene practices and the growing phenomenon of IPTV (Internet Protocol Television) piracy, exploring whether security behaviour can serve as an effective deterrent to online copyright infringement. The authors begin by discussing risk perception, highlighting that previous research finds it to be a key predictor of digital piracy behaviour (Liao *et al*., 2010; Yoon, 2011; Pham *et al*., 2020). Next, the role of cyber hygiene is emphasized, framed as a form of security behaviour influenced by awareness and knowledge (Neigel *et al*., 2020; Shaw *et al*., 2009). Studies show that better cyber hygiene correlates with more cautious online behaviour and can mitigate risks such as malware infections, which are often associated with illegal IPTV sites (Watson *et al*., 2014; Bosco & Shalaginov, 2018). However, research directly linking security behaviour to digital piracy has been limited until now. Personality traits, particularly the "dark triad" (Machiavellianism, narcissism, and psychopathy), are also investigated as predictors of IPTV piracy. Past studies (Satchell *et al*., 2022; Al-Rafee & Cronan, 2006) indicate that these traits are positively correlated with risk-taking and IP infringement. Shah *et al*. (2024) support this by finding a negative relationship between dark triad traits and perceived risk of IPTV usage, suggesting individuals with these traits

underestimate potential threats. This study significantly contributes to the existing literature by proposing a structural equation model integrating these factors and demonstrating that cyber hygiene mediates the effect of problematic internet use on IPTV risk behaviour. Grepcka, Basholli, & Daberdini (2024) explores the critical role of cyber hygiene in today's increasingly digital world. The article offers a comprehensive overview of cybersecurity, defining it as a multifaceted discipline involving the protection of information systems, networks, and data from unauthorized access and malicious threats. A core focus of the article is the categorization of cybersecurity domains, which include network security, information security, application security, and cloud security, among others. The authors detail how these areas work collectively to form a defence-in-depth strategy against various threat actors. They also highlight the importance of user education, noting that end-users often represent the weakest link in the security chain and require training to adopt secure online behaviour importantly, the article underscores the economic and social consequences of cyberattacks.

Importance of the Study

In the present digital age, the use of personal computers, smart phones, and the internet has become an essential part of everyday life. Individuals of all age groups depend on digital technologies for communication, education, banking, shopping, entertainment, and professional work. However, the increasing reliance on online platforms has also resulted in a rise in cyber threats and cyber- crimes. In this context, understanding the level of awareness regarding cyber hygiene and online safety is highly important.

This study is significant because it helps to assess how well internet users understand and practice cyber hygiene measures such as using strong passwords, updating software, managing privacy settings, and protecting personal information. By identifying awareness levels among different age groups and genders, the study highlights whether certain groups are more vulnerable to cyber risks due to limited knowledge or unsafe practices. The importance of this study also lies in its focus on safety while using personal computers and the internet. The study also promotes responsible digital citizenship by encouraging individuals to adopt safe online behaviors. Enhancing awareness about cyber hygiene not only protects personal data and financial information but also reduces the overall impact of cyber- crimes in the community.

Objectives

The overall objective of this study is to examine cyber hygiene awareness among persons having different educational level and occupation. The specific objectives are:

- To identify the level of awareness about cyber hygiene practices among internet users.
- To find out the depth of understanding among internet users regarding cybercrime risks and safety practices while using the internet.

Methodology

The study utilizes both primary and secondary sources of data to achieve its research objectives. Primary data has been collected using a well-structured questionnaire designed to address the key aspects of the study. The questionnaire includes both closed-ended and open-ended questions to gather quantitative and qualitative insights. The study adopts a convenience sampling method, selecting respondents based on accessibility and willingness to participate. A total of 61 respondents were chosen for the study. The sample includes students, professionals and housewives, having different educational level. Online survey and self-administered questionnaires were used to collect responses from the participants.

Secondary data has been collected from various published and online sources including: Research articles and academic journals. To ensure meaningful interpretation the collected data has been analyzed using various statistical and graphical techniques, including:

- **Percentage Analysis:** Used to interpret demographic characteristics and key study variables.
- **Graphs and Charts:** Pie charts are used to visually represent trends and patterns in the collected data.
- **Tabulation:** Data is categorized and presented in tabular format for easy understanding and comparison.
- **Likert Scale:** The Likert scale is widely used survey tool that gauges the level of agreement or disagreement with a series of statement on a graded scale, typically ranking from "strongly disagree" to "strongly agree". Respondents were asked to rate each statement on a five-point scale, where each point was assigned a numerical value from 1 (strongly disagree) to 5 (strongly agree). The responses were then quantified, and the resulting data were analyzed to determine the mean score.

Limitations

One of the primary constraints is the limited time available for an in-depth and extensive analysis which may restrict the scope of the study.

- Some respondents may be hesitant to disclose complete or accurate information due to personal concerns or social stigma, leading to potential data gaps.
- The sample size is limited to 61 respondents, which may not fully capture the diversity of experiences across the entire unorganized sector.
- Convenience sampling may introduce bias as participants are selected based on accessibility rather than random selection.

Results and Discussions

The present section provides the analysis and interpretation of data collected from persons of different age groups, having different educational qualification and occupation. The study is based on primary data, aims to understand the level of awareness about cyber hygiene practices among different age groups. The study also aims to understand the level of awareness on safety while browsing online. Primary data was gathered through a structured questionnaire using a convenience sampling method with 61 respondents. The collected data has been analysed using percentages, graphs and tables to provide a comprehensive understanding of cyber hygiene practices among ages and gender. This analysis will help to identify level of cyber safety awareness and provide insights into cyber well-being of the population.

The table 1 shows the occupational distribution is almost evenly balanced. Students form the largest group with 34.42% of the respondents. Housewives and professionals each represent 32.78%. This balanced distribution strengthens the reliability of occupational comparison in the study. Students are typically more active on digital platforms for educational and social purposes. Professionals use digital tools for work-related activities. Housewives may use the internet for communication, shopping, entertainment, and information access.

Table 1: Occupational Distribution

Occupation	No of respondents	Percentage of respondents
Students	21	34.42
House wife	20	32.78
Professionals	20	32.78
Total	61	100

Source: Primary data

Since all three occupational groups are nearly equally represented, the study can effectively compare cyber hygiene awareness levels across different occupational backgrounds. This also indicates that cyber hygiene awareness is relevant across different social and professional categories.

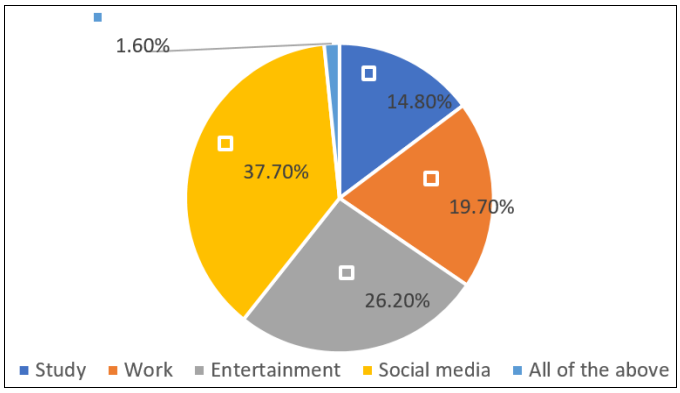
Table 2: Average hours of online spending

Hours	No. of respondents	Percentage of respondents (%)
Below 8 hours	46	75.4
8 hours	9	14.8
Above 8 hours	6	9.8
Total	61	100

Source: Primary data

The table 2 presents the distribution of respondents based on the number of hours they spend, showing that the majority spend below 8 hours, i.e., 46 respondents representing 75.4% of the total sample. This indicates that most of the individuals fall within a moderate time range and do not exceed 8 hours. A smaller group of 9 respondents, accounting for 14.8%, reported spending exactly 8 hours. Meanwhile, only 6 respondents, representing 9.8%, spend above 8 hours, making this the smallest category.

The figure 1 shows that 37.7% of internet users are interested in social media. This indicates that a significant proportion of individuals primarily access the internet for communication, networking, and social interaction.



Source: Primary data

Fig 1: Type of Internet Use

Entertainment (Figure 1) follows as the second most common purpose at 26.2%, suggesting that activities such as streaming videos, gaming, and other leisure-related uses also play a major role in internet consumption. Work-related use represents 19.7%, demonstrating that nearly one-fifth of the respondents rely on the internet for professional tasks. Study purposes account for 14.8%, which is comparatively lower, implying that academic use is not the main priority for most of the respondents. Only 1.6% selected "all of the above," indicating that very few individuals use the internet equally for study, work, entertainment, and social media.

The table 3 shows respondents' understanding of the concept of cyber hygiene. For familiarity with the concept, 31.1% agreed and 9.8% strongly agreed, while 42.6% were neutral, giving a point value of 3.28, which indicates moderate familiarity. Regarding practices that maintain online security, 47.5% agreed and 9.8% strongly agreed, with 39.3% neutral, resulting in a point value of 3.64, showing a good level of understanding. The statement on regular software updates, strong passwords, and safe browsing had the highest agreement, with 47.5% agreeing and 21.3% strongly agreeing, producing the highest point value of 3.82. For the idea that cyber hygiene (Table 3) is similar to personal hygiene but applied to digital devices and data security, 32.7% agreed and 13.1% strongly agreed, with 37.7% neutral, giving a point value of 3.40. Lastly, 45.9% agreed and 13.1% strongly agreed that checking privacy settings and protecting personal information is part of cyber hygiene, resulting in a point value of 3.62. Overall, the results indicate a moderate to good understanding of cyber hygiene among respondents.

Table 3: Understanding the Term Cyber Hygiene

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Point Value
Familiar with the concept of cyber hygiene	4 (6.5%)	6 (9.8%)	26 (42.6%)	19 (31.1%)	6 (9.8%)	3.28
Practices that maintain online security	0 (0%)	2 (3.3%)	24 (39.3%)	29 (47.5%)	6 (9.8%)	3.64
Regular software updates, strong password, safe browsing	0 (0%)	5 (8.2%)	14 (22.9%)	29 (47.5%)	13 (21.3%)	3.82
Similar to personal hygiene but applied to digital devices and data security	1 (1.6%)	9 (14.7%)	23 (37.7%)	20 (32.7%)	8 (13.1%)	3.4
Checking privacy settings and protecting personal information online	0 (0%)	6 (9.8%)	19 (31.1%)	28 (45.9%)	8 (13.1%)	3.62

Source: Primary data (Strongly Disagree-1, Disagree-2, Neutral-3, Agree-4, Strongly Agree-5)

The table 4 presents respondents' views on protection of devices. For regularly updating device software, 49.1% agreed and 16.4% strongly agreed, while 22.9% were neutral, resulting in a point value of 3.7, indicating a good practice among respondents. Regarding the use of strong and unique passwords, 55.7% agreed and 22.9% strongly agreed, with only 11.5% neutral, giving the highest point value of 3.87, which shows strong awareness of password security. For enabling two-factor authentication, 40.9% agreed and 19.7% strongly agreed, while 27.9% remained neutral, producing a point value of 3.7.

Table 4: Protection of Devices

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Point Value
Regularly update device software	1 (1.6%)	6 (9.8%)	14 (22.9%)	30 (49.1%)	10 (16.4%)	3.7
Use strong and unique passwords for the accounts	3 (4.9%)	3 (4.9%)	7 (11.5%)	34 (55.7%)	14 (22.9%)	3.87
Enable two factor authentication whenever possible	2 (3.3%)	5 (8.2%)	17 (27.9%)	25 (40.9%)	12 (19.7%)	3.7
Regular backup the data plan to a secure location	3 (4.9%)	7 (11.5%)	19 (31.1%)	26 (42.6%)	6 (9.8%)	3.4
Avoid connecting to unsecured public or Wi-Fi networks	1 (1.6%)	4 (6.5%)	16 (26.2%)	26 (42.6%)	14 (22.9%)	3.8

Source: Primary data (Strongly Disagree-1, Disagree-2, Neutral-3, Agree-4, Strongly Agree-5)

In terms of regularly (Table 4) backing up data to a secure location, 42.6% agreed and 9.8% strongly agreed, with 31.1% neutral, resulting in a point value of 3.4, indicating a moderate practice level. Lastly, for avoiding connection to unsecured public Wi-Fi networks, 42.6% agreed and 22.9% strongly agreed, while 26.2% were neutral, giving a point value of 3.8. Overall, the results suggest that respondents generally demonstrate good device protection practices, particularly in using strong passwords and avoiding unsecured networks.

The table 5 shows respondents' perceptions of the usefulness of cyber awareness programs. For the statement that cyber safety awareness programs are important for all internet users, 39.3% agreed and 37.7% strongly agreed, while 19.7% were neutral, resulting in the highest point value of 4.08, indicating strong agreement. Regarding improving understanding of online threats, 47.5% agreed and 24.6% strongly agreed, with 19.7% neutral, giving a point value of 3.86.

Table 5: Usefulness of Cyber Awareness Program

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Point Value
Cyber safety awareness programs are important for all internet users	2 (3.3%)	0 (0%)	12 (19.7%)	24 (39.3%)	23 (37.7%)	4.08
Improved the understanding of online threats	1 (1.6%)	4 (6.6%)	12 (19.7%)	29 (47.5%)	15 (24.6%)	3.86
Help to practice safer online behavior	1 (1.6%)	2 (3.3%)	12 (19.7%)	30 (49.2%)	16 (26.2%)	3.95
Willing to attend cyber safety awareness sessions in the future	3 (4.9%)	1 (1.6%)	12 (19.7%)	24 (39.3%)	21 (34.4%)	3.96
Stay informed about current cyber threats and online risks	1 (1.6%)	3 (4.9%)	13 (21.3%)	27 (34.4%)	17 (27.9%)	3.91

Source: Primary data (Strongly Disagree-1, Disagree-2, Neutral-3, Agree-4, Strongly Agree-5)

In terms (Table 5) of helping to practice safer online behavior, 49.2% agreed and 26.2% strongly agreed, while 19.7% were neutral, producing a point value of 3.95. For willingness to attend cyber safety awareness sessions in the future, 39.3% agreed and 34.4% strongly agreed, with 19.7% neutral, resulting in a point value of 3.96. Lastly, regarding staying informed about current cyber threats and online risks, 34.4% agreed and 27.9% strongly agreed, while 21.3% were neutral, giving a point value of 3.91. Overall, the results indicate that respondents generally recognize the importance and usefulness of cyber awareness programs, with all point values close to 4.0, reflecting positive perceptions.

Table 6: Response to Suspicious Behavior of Devices

Statement	No. of respondents	Percentage of respondents (%)
Run a virus scan	12	19.7
Restart the device	23	37.7
Ask a tech expert	10	16.4
Search online for solutions	10	16.4
Ignore it	6	9.8
Total	61	100

Source: Primary data

The table 6 indicates that when faced with suspicious device behavior, respondents show mixed but generally proactive responses. The most common action is restarting the device (23 respondents, 37.7%), which may resolve minor issues but does not always address security threats. A significant portion (12 respondents, 19.7%) run a virus scan, reflecting appropriate security awareness. Others seek assistance either by asking a tech expert (10 respondents, 16.4%) or searching online for solutions (10 respondents, 16.4%), indicating willingness to address the issue. However, 6 respondents (9.8%) ignore suspicious behavior, which could worsen potential security problems. Overall, while many respondents take action, reliance on simple restarts and occasional inaction suggests a need for improved understanding of proper incident response.

The table 7 presents the different safety practices adopted by the respondents while browsing the internet, along with their number and percentage. The data reveal that the largest proportion of respondents, 28 (45.9%), follow all of these practices, which include avoiding unknown links, using secured websites only, and avoiding sharing personal information. This indicates a high level of awareness and comprehensive adoption of safe browsing habits among nearly half of the respondents. Individually, 14 respondents (23%) reported that they specifically avoid unknown links, highlighting caution against phishing and malicious content. Additionally, 10 respondents (16.4%) stated that they avoid sharing personal information, while 6 respondents (9.8%) use secured websites only, reflecting selective but important protective measures.

Table 7: Approach to online browsing

Statement	No. of respondents	Percentage of respondents (%)
Avoid unknown links	14	23
Use secured websites only	6	9.8
Avoid sharing personal info	10	16.4
All of these	28	45.9
Prefer none	3	4.9
Total	61	100

Source: primary data

However, a small minority of 3 respondents (4.9%) (Table 7) preferred none of these practices, indicating minimal concern for online safety. Overall, the findings suggest that most of the respondents demonstrate responsible and proactive behavior toward safe online browsing, though a small group still lacks adequate cyber safety practices.

Table 8: Method Used to Secure Online Accounts

Statement	No. of respondents	Percentage of respondents (%)
Two factor authentication	22	36.1
Strong password only	24	39.3
Password manager	10	16.4
No specific method	3	4.9
Not aware of the security options	2	3.3
Total	61	100

Source: primary data

The data in the table 8 shows that most commonly used method to secure online accounts among the respondents is using a strong password only, selected by 39.3%. This indicates that many users depend mainly on password strength without adding extra security layers. While strong passwords are important, relying only on them may not provide full protection against modern cyber threats.

Table 9: Viewpoint on Factor Influencing Cyber Hygiene Behavior

Statement	No. of respondents	Percentage of respondents (%)
Education/ training	24	39.3
Peer influence	3	4.9
Personal experiences	10	16.4
Fear of cyber crime	12	19.7
No influence	12	19.7
Total	61	100

Source: primary data

The table 9 shows that education and training is the most important factor influencing cyber hygiene behavior among respondents. A large share, 39.3%, selected education/training, indicating that awareness programs, formal instruction, and learning about cyber safety practices play the biggest role in shaping secure online behavior. This suggests that knowledge-based interventions are highly effective in improving cyber hygiene. The next strongest influences are fear of cybercrime and no specific influence, each at 19.7%. This indicates that for many respondents, concern about cyber threats motivates safer behavior, while an equal proportion feels their behavior is not driven by any one major factor. This split shows that both emotional drivers (fear/risk perception) and personal habits independent of influence are significant. Personal experiences account for 16.4%, meaning that past incidents such as scams, hacking attempts, or data loss also encourage people to adopt safer digital practices. Direct experience appears to be a meaningful but secondary motivator compared to formal education. Peer influence has the smallest share (4.9%), showing that friends or colleagues have relatively little effect on respondents' cyber hygiene behavior compared to training, fear of threats, or personal experience.

The data in the table 10 shows that most regularly followed cyber hygiene practice among respondents is privacy settings management, selected by 32.8% of participants. This indicates that many users actively adjust and monitor their account privacy controls, showing awareness about protecting personal information on digital platforms. The next most common practice is device updates, chosen by 23% of the respondents. This suggests that a good portion of users regularly update their devices and software, which is an important step in preventing security vulnerabilities and cyber-attacks.

Table 10: Regularly Following Cyber Hygiene Practices

Statement	No. of respondents	Percentage of respondents (%)
Password protection	11	18
Privacy settings	20	32.8
Safe browsing	10	16.4
Device updates	14	23
None regularly	6	9.8
Total	61	100

Source: primary data

Password protection is followed most regularly by 18% (Table 10) of respondents, while safe browsing practices are selected by 16.4%. These results show moderate attention to creating strong passwords and browsing carefully, but they are not the top priority practices for most users compared to privacy settings and updates. However, 9.8% report that they follow no cyber hygiene practice regularly. This is a concern, as it indicates that nearly one in ten respondents may not consistently apply basic cyber safety measures.

Table 11 shows respondents' views on the government's role in practicing and promoting cyber hygiene. For the statement that the government provides adequate information on cyber hygiene practices, 34.4% agreed and 29.5% strongly agreed, while 21.3% were neutral, 8.2% disagreed, and 6.6% strongly disagreed, with a point value of 3.7. Regarding government agencies conducting effective cyber safety awareness programs, 36.06% agreed and 31.1% strongly agreed, while 26.2% were neutral and 6.6% disagreed, giving a point value of 3.9. Similarly, 32.8% agreed and 34.4% strongly agreed that government laws and policies help protect citizens from cyber threats, while 19.7% were neutral, 9.8% disagreed, and 3.3% strongly disagreed, with a point value of 3.9. Lastly, 39.3% agreed and 32.8% strongly agreed that government websites and platforms provide clear guidelines on safe online practices, while 18.03% were neutral, 8.2% disagreed, and 1.6% strongly disagreed, also recording a point value of 3.9. Overall, the results indicate a general agreement on the perception of the government's role in promoting cyber hygiene.

Table 11: Government's Role in Practicing and Promoting Cyber Hygiene

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Pont Value
Provides adequate information on cyber hygiene practices	4 (6.6%)	5 (8.2%)	13 (21.3%)	21 (34.4%)	18 (29.5%)	3.7
Govt. agencies conduct effective cyber safety awareness programs	0 (0%)	4 (6.6%)	16 (26.2%)	22 (36.06%)	19 (31.1%)	3.9
Govt. laws and policies help protect citizens from cyber threats	2 (3.3%)	6 (9.8%)	12 (19.7%)	20 (32.8%)	21 (34.4%)	3.9
Govt. websites and platforms provide clear guide lines on safe online practices	1 (1.6%)	5 (8.2%)	11 (18.03%)	24 (39.3%)	20 (32.8%)	3.9

Source: primary data (Strongly Disagree-1, Disagree-2, Neutral-3, Agree-4, Strongly Agree-5)

Findings

- The study shows a strong representation from both younger and older individuals with 41% of the respondents aged below 25 and 41% aged above 35.
- Out of 61 respondents the middle age group (25 to 35) is comparatively under represented, making up only 18% of the sample.
- A significant majority of the respondents are highly educated, with 55.73% holding a degree and 9.83% holding post-graduate qualifications. Only a small fraction (6.56% combined) has lower educational qualifications like SSLC or Plus One.
- The sample is almost perfectly balanced across students (34.42%), housewives (32.78%) and professionals (32.78%). This balance allows a meaningful comparison of cyber hygiene across different social and professional backgrounds.
- Device usage and online time smartphones are the primary digital gateway, used by an overwhelming 93.40% of respondents. 75.4% maintained a moderate internet usage, spending less than 8 hours online per day.
- Internet usage is primarily driven by social media (37.7%) and entertainment (26.2%). professional work (19.7%) and academic study (14.8%) account for a smaller portion of digital activity.
- The conceptual understanding of the term "Cyber Hygiene" itself is moderate while the respondents show a high practical engagement in safety measures like strong passwords and software updates.
- Strong and unique passwords are the most widely adopted security measure with a mean score 3.87. Regular data backup is the least consistently practiced habit, receiving the lowest mean score in this category (3.4).
- Respondents are most cautious about where they get their apps, with downloading from trusted sources scoring a high 3.9 mean value.
- While most avoid apps with unnecessary permissions (3.8), the actual habit of carefully reviewing permissions before installation is slightly lower (3.5).
- There is a near-universal agreement that cyber safety programs are important for all users, receiving the highest mean value in the entire study (4.08).
- Respondents expressed a high willingness to attend future awareness sessions (mean score 3.96).
- Respondents are least confident in their knowledge of what steps to take once a device is already compromised (mean score 3.34). While is highest regarding where to report cybercrimes (mean score 3.6)
- 49.2% of the respondents practice safe habits by ignoring and deleting unknown messages.
- 37.7% of the respondents use secured tools are browser warnings, while 27.9% look for https or lock icon while browsing internet.
- Over half of the respondents (54.1%) avoid public Wi-Fi entirely to mitigate risks. 31.1% of respondents control their profile visibility to protect privacy. 23% of the respondents restrict location sharing, demonstrating the awareness of location based privacy risks. However 16.4% of the respondents do not manage privacy settings, indicating weak cyber hygiene practice. 37.7% of the respondents restart device is when it acts suspiciously, which may not address actual security threats.
- A strong majority of the respondents (60.7%) ensure safety in online shopping by using only trusted websites. 42.6% adopts a cautious approach by checking the authenticity of websites while browsing.
- Approximately 39.3% of the respondents regularly clear their browser history, showing a proactive stance toward privacy.
- A small group of the respondents (16.4%) never clear their browser history, which represents a potential privacy risk.
- A majority of 39.3% of the respondents use strong passwords, while 36.1% of the respondents use two factor authentication method (2FA) to protect online accounts.
- Most respondents check their financial activity at least weekly (32.80%) or daily (23%), showing responsible behavior to financial monitoring.
- A majority of 52.5% of respondents shows strong general awareness that cyber threats can occur in any online environment.
- A majority of 60.7% respondents follow cyber hygiene practices to maintain personal safety, indicating that protecting their own data and privacy is the primary concern.
- 39.3% respondents believes that structured education and awareness effort are the strongest drivers of good cyber hygiene.
- A clear majority of 52.5% show a strong awareness that cyber hygiene should be universal across platforms, with special concern toward social media and banking applications.
- Most respondents (41%) recognized that multiple online activities can lead to cybercrime, indicating good general awareness of cyber risks.
- Over one-third of respondents (34.4%) are not confident in managing personal data, privacy settings and information sharing practices.
- The most regularly followed cyber hygiene practice among respondents is privacy settings management, selected by 32.8% of respondents.
- Only 24.6% of respondent's report that they always logout from accounts on shared devices, while for majority (32.8%) logout behavior is not consistent.
- Most respondents adopt proactive measures such as strict privacy control (36.1%) and limited sharing (27.9%), while very few neglect monitoring their online activities.

- Most respondents (50.8%) recognize cyber hygiene as a multidimensional concept requiring balanced awareness of knowledge, behavior, technical measures, and legal aspects rather than relying on a single factor.
- 36.1% respondents believe that different age groups adopt different levels of online safety practices.
- Many respondents (29.5%) believe that gender itself does not create differences.
- About three-fourth (77%) of respondents believe parents play a very important role in promoting cyber hygiene and guiding children about online safety.
- Most respondents (around 65-72%) think the government plays a good role in promoting cyber hygiene, but some people are still unsure.

Conclusion

This study aimed to examine the level of awareness about cyber hygiene practices among different age groups and genders, and to assess the awareness of safe practices while using personal computers and the internet among users in the context of cyber- crimes. The findings of the study reveal that, overall, respondents possess a moderate to high level of awareness regarding cyber hygiene and online safety practices. A majority of participants demonstrate good knowledge about basic security measures such as using strong passwords, avoiding suspicious links, downloading applications from trusted sources, and practicing safe online shopping. This indicates a positive trend in the general understanding of cyber security among internet users.

However, the study also highlights certain gaps in practical knowledge and consistent behavior. While many respondents are aware of cyber hygiene in theory, some lack confidence in handling situations such as responding to cyber-attacks, managing privacy settings effectively, and taking appropriate action when a device is compromised. Additionally, practices such as regular data backup, careful review of app permissions, and consistent logout from shared devices are not uniformly followed by all users, indicating areas where awareness needs to be strengthened.

With respect to age and gender, the study suggests that awareness levels are relatively similar across genders, indicating that cyber hygiene knowledge is not significantly influenced by gender differences. However, variations in awareness and practices are observed across different age groups, with younger users being more active online but not always more cautious, while older users tend to be more careful but less technically confident. This highlights the need for age-specific awareness and training programs.

Overall, the study concludes that while the foundation of cyber hygiene awareness among users is reasonably strong, there is a clear need for continuous education, practical training, and awareness initiatives to bridge the gap between knowledge and practice. Strengthening cyber safety education through institutions, community programs, and government initiatives will help individuals to adopt safer digital behaviors and reduce vulnerability to cyber-crimes. By promoting responsible digital habits and empowering users with the right knowledge and tools, a more secure and resilient online environment can be achieved.

References

1. Barakovic S, Barakovic Husic J. Cyber hygiene practices among university students in Bosnia and Herzegovina: Knowledge, awareness, and behavioural practices, 2023.
2. Basholli A *et al*. The role of education in promoting cyber hygiene amidst rapid digitalization, 2023.
3. Berdi A, Niyazova G, Bayterekova A. Digital hygiene skills and cyberbullying reduction among teenagers in Kazakhstan. International Journal of Evaluation and Research in Education, 2024.
4. Bhandari R, Sree P, Kakar S. Digital hygiene awareness and cyber aggression among youth. Annual Research Journal, 2024.
5. Bognár F, Bottyán T. Development and validation of a personal cybersecurity awareness scale for university students, 2021.
6. Bosco F, Shalaginov A. Malware risks associated with illegal IPTV streaming sites, 2018.
7. Budu KW, Yinping L, Mireku KK. Behavioral intention and adoption of e-learning systems in Ghanaian tertiary institutions, 2018.
8. Cain AA, Edwards ME, Still JD. An exploratory study of cyber hygiene knowledge and behaviors among end users, 2018.
9. Fatokun F, Hamid S, Norman A, Fatokun J. Influence of demographic variables on cybersecurity behaviors among Malaysian tertiary students, 2019.
10. Fielder A, *et al*. A hybrid cybersecurity investment model, 2016.
11. Fikry MA, Hamzah A, Hussein N. Cyber hygiene practices among professional youth in Malaysia, 2023.
12. Fikry MA, Hamzah A, Hussein N. Cyber hygiene: A conceptual and theoretical review, 2024.
13. Garba A *et al*. Cybersecurity awareness and data protection practices among Nigerian students, 2020.
14. Ghelani N. Cybersecurity strategies in Industry 4.0., 2022.
15. Grepcka E, Basholli A, Daberdini L. The critical role of cyber hygiene in an increasingly digital world, 2024.
16. Hadlington L. Human factors in cybersecurity, 2017.
17. Howell CJ, Maimon D, Muniz C, Kamar E. Informational interventions and thoughtful decision-making in cyber hygiene adoption, 2024.
18. Mughal M. Cybersecurity hygiene in the era of the Internet of Things. Applied Research in Artificial Intelligence and Cloud Computing, 2019.
19. Mtambeka P, Mtegha H, Chigona W. Factors influencing university students' compliance with cybersecurity measures in South Africa, 2023.
20. O'Connell ME. Cyber security without cyber war. Journal of Conflict and Security Law. 2012; 17(2):187-209.
21. Oliveira T *et al*. Cross-national comparison of cybersecurity awareness among first-year computer science students in Portugal and Poland, 2023.
22. Panda A *et al*. Optimal Safeguards Tool (OST): A game-theoretic approach to cybersecurity investment in healthcare, 2020.
23. Podlinyayeva O, Sytnyk O. Cyber hygiene education strategies for school-aged children, 2023.
24. Shah S *et al*. Cyber hygiene, risk perception, and IPTV piracy: A structural equation modeling approach, 2024.
25. Ugwu C, Ani O, Ezema I, Asogwa B. Age and educational level as predictors of cyber hygiene culture, 2022.
26. Ugwu C *et al*. Demographic variables and cyber hygiene practices among university students, 2023.
27. Vishwanath A, Neo LS, Goh PS, Lee J, Khader M. Development and validation of a cyber-hygiene scale, 2020.