J-STAR: Journal of Social & Technological Advanced Research
Journal homepage: https://rjsaonline.org/index.php/J-STAR

Cybercrime Awareness and Digital Safety Behavior Among Internet Users

Dur-E-Adan

Department of Computer Science, National University of Modern Languages, NUML Islamabad, Pakistan
durriyahtahir@gmail.com

ARTICLE INFO

Received:
September 20, 2025
Revised:
October 02, 2025
Accepted:
October 18, 2025
Available Online:
November 04, 2025

Keywords:
Cybercrime awareness, Digital safety behaviour, Internet users, Cybersecurity education, on-line risk perception, protecting behaviour

Corresponding Author:
durriyahtahir@gmail.com

ABSTRACT

Cybercrime has proliferated along with the rapid increase in the use of internet and digital connectivity in the world. As people conduct online activities which can be anything ranging from social networking to e-commerce to even telecommuting, it makes people more and more vulnerable to hacking, phishing, identity thefts, malware attack and various forms of cyber fraud. This research article has investigated cybercrime awareness and digital safety behavior relationship among the internet users, exploring the influence this knowledge of cyber threats has on safety practices such as secure password behaviours, antivirus software usage, use of privacy settings and cautious interaction online. Inspired by the interdisciplinary research of cybersecurity, psychology and the information systems, this study recommends the essential determinants of safe behaviour online and evaluates the Perverse socio-demographic aspects affecting cyber awareness users and cyber protection and measures. The results point to both potential opportunities to help build digital resilience, as well as potential barriers to helping make cyber safety practices work.

Introduction

The internet's rapid spread across the globe providing new platforms and online services for communication, transactions, work and socialization have greatly changed the way people communicate, transact, work and socialize. According to global estimates, over 5 billion people (60% plus of the world's population) have regular access to the Internet nowadays where they engage in all sorts of activities ranging from social networking, e-commerce and online banking, through education and online constructed collaboration (Internet World Stats, 2025). Whilst these digital developments have resulted in unprecedented opportunities in the areas of economic growth, social inclusion and information access, these same developments have given rise to formidable vulnerabilities in the shape of cybercrime; illegal or malicious activities under-taken through the use of computer networks and digital systems. Cybercrime may come in many forms that are cybercrime attacks such as phishing, ransomware attacks, identity theft, financial fraud, malware distribution, and cyberbullying that make use of technological dependence and behavioral practices of users (Wall, 2007; McGuire & Dowling, 2013).

Digital infrastructure and services--supported with personal computers, mobile devices, cloud systems and Internet of Things (IoT) technologies--have become a part of everyday life. However this integration also make users vulnerable to the threats posed by cybercriminals who can use these technical weaknesses, human error and poor security practices to bypass security. For example, phishing scams will convince people to hand them private information such as password or account numbers, malware can infiltrate devices and leak private information and ransomware will encrypt files of users and demand paying for decryption keys (Hadnagy, 2018; Mitnick & Simon, 2011). Such threats bring about heavy financial losses, psychological sufferings and damages in the reputation of individuals, organizations and even national infrastructures.

Effective mitigation of cybercrime is not primarily a question of technological defences, such as firewalls, encryption and intrusions detection systems, but also a question of the awareness and safety behaviour of users. Cybercrime awareness is the awareness of the user about the digital threats, the risks signs and protection measures. Digital safety behaviour includes various proactive behaviour such as the use of strong and unique password; multiple factor authentication; software update; skeptical appraisal of unsolicited emails; privacy setting; antivirus or anti-malware tools (Ng et al., 2009; Sheng et al., 2010). Research suggests that people who can demonstrate higher level of cyber awareness are more likely to engage with safer practice online which will make them less prone to threat and less reliant on the cyber crime incident impact (Liang and Xue, 2010; Crossler and Belanger, 2014).

Despite the awareness of the importance of internet security, a number of users on the internet display an inconsistent approach to the risks faced and do not display consistent safety practices. There have been studies that suggest users have a tendency to underestimate their cyber risk, overestimate their own abilities to be secure, or to take preventative measures - and even if they have the basic awareness of cyber risks (Hadlington, 2018; Parsons et al., 2017). This mismatch between awareness and behaviour brings important questions to the fore with regards to enabling/disabling factors of the processes that are involved in the process of changing from knowledge to effective protective actions. Psychological constructs such as perceived vulnerability, self-efficacy and motivation have been associated with user adoption to secure digital behaviours, socio-demographic factors such as age, education and digital literacy also have influence in determining the way people view and respond to cyber threats (Ifinedo, 2012; Siponen et al., 2014).

In addition to this, the fact that cybercrime - with ever-more sophisticated and targeted attacks - requires constant learning and adaptation on the part of the users. Cybercriminals employ social engineering approaches using human psychology for which user awareness and judgment would have to be integrated with technical efforts (Mitnick & Simon, 2011; Hadnagy, 2018). For instance, spear-phishing attacks are spoofed by a legitimate communication source and trick the people into compromising their credentials or downloading malicious software. Without the knowledge of such tactics, when people are not technically savvy, they fall prey to deceit.

In the past few years, there have been efforts in cybersecurity education to try to raise the awareness of users to the risk and also to make their related behaviour safer. These include public awareness campaigns and school-based cybersecurity curriculums, workplace training programs that will be carried out, online tutorials - all these are aimed at improving the understanding of cyberthreats and advising on protection measures. However, the effectiveness of these interventions vary from culture to other cultures and there is still a need for empirical grounded research which identifies the relationship between awareness and actual safety behavior in different settings (Jakobsson & Myers, 2007 and Furnell, 2005).

Understanding this relationship is of importance considering the rising technological dependence of the modern society and the rising rates of cybercrimes. Individuals i.e. who do not have the right awareness or do not take safety precautions not only put their data and assets at risk but could also lead to security failures in broader networks leading to a cascading security failure. At the systemic levels, since the users have weak behaviour, such behaviour can lead to failure of the organizational cybersecurity protocols which can impact exposure of their sensitive information as well leading to breaches with far reaching consequences which can go on par, on a large scale (Verizon, 2024).

The objective of this study is to examine the influence of expert influence in the digital safety behaviour of internet users in terms of cyber crimes and identify the determinant which increase the level of security behaviours or decreases it. The research looks at the socio-demographic cognitive and experiential influences on the users risk perceptions and safety behaviours, looking at the correlation between knowledge of expansive cyber threats and behaviour, such as password hygiene, software updates, email scrutiny, and privacy setting usage. Additionally, the research measures the mediant effect of psychological constructs, such as perceived vulnerability and self-efficacy on the relation between awareness and behavior.

The importance of this study is that it can lead to implications for development of cybersecurity education strategies, public policy, and digital literacy programs. By explaining the process by which awareness is converted into safety behavior - and barriers that prevent this process - this research offers evidence for the design of better intervention programs that help empower the internet user to protect themselves in an ever-increasing dangerous environment. Ultimately, encouraging good cybercrime understanding and sustainable security practices can not only add to one's personal resilience and individual responsibility but also promote security and are key to shaping safer and more trustworthy ambiance overall as well, supporting healthier cyber hygiene practices across industries.

Literature Review

The literature on cybercrime awareness and digital safety behavior emphasizes the importance that user awareness plays around informing protective online behaviors and mitigating vulnerabilities to cyber threats. As a result of the continued rise of cybercrime incidents in conjunction with the growing use of the internet, researchers have been busy trying to understand the interplay between awareness, knowledge, risk perception and behavior in a range of user populations.

A growing body of research points at the fact that cybercrime awareness is one precursor to safe digital behavior. Awareness is the knowledge of cyber threats such as phishing, malware, identity theft and online fraud and cyber security measures such as having strong passwords, updating regularly and using secure networks. For, example, cybersecurity knowledge was even found to be a significant factor that could determine awareness and online safety behaviour among digital banking users, although awareness might not completely mediate the effects of knowledge vs. behaviour (Nagari and Rahalja, 2025). Similarly, other research that aims to explore cybersecurity behaviour in employees, has found that awareness, when combined with self-efficacy and severity of threats improved protective behaviours and hence show that psychological factors are crucial in translating awareness to behaviour (Qalby et al., 2025).

Theoretical models have been adapted to cybersecurity to understand why users behave in particular ways to protect themselves like Protection Motivation Theory (PMT) and Health Belief Model (HBM). These models suggest perception on the severity and vulnerability of the recommended action and efficacy of the recommended action influence people's tendency to employ safe behaviors. A recent study to apply the HBM to the phishing behaviour among university students revealed that: perceived severity, perceived importance of security measures, self-efficacy and cues to actions was significant predictors of security behaviour (Alhendawi et al., 2025). This is consistent with previous results that find people that are aware of cybersecurity threats and have confidence in their abilities are more likely to take such precautions as examining suspicious emails and keeping security tools updated.

Empirical evidence has also proved that security awareness does not mean appropriate behavior. In some instances it seems that those who have a basic awareness of the threats that are present within cyberspace find themselves engaging in unsafe practices which may indicate some sort of disconnect between knowledge and action. Studies based on awareness and behavior amongst university students suggest that users, although their awareness of what some of the common threats are such as phishing, users only tend to adopt elementary precautions and not comprehensive safety measures (Kshetri et al., 2023). This gap emphasizes the need not only to disseminate information, but also to instil cyber hygiene behaviors and motivation for instilling safe behavior at regular intervals.Research on Secondary and Tertiary Student Populations Strengthens the Relationship Between Awareness and Protective Behavior A large-scale study of Saudi secondary students found that cybersecurity awareness and internet use duration were considered positive predictors of threat perception which had a significant impact on data protection behaviors such as using strong passwords and privacy settings (Alqarni, 2025). These results reveal that the perceived risks and induced proactive safety actions will be promoted through added exposure to digital environments and tailored education.

The relevance of digital literacy as well as the role of the context is another theme. Digital citizenship 8--responsible and ethical participation in digital environments, including cyber safety, respect for privacy rights and knowledge of safe practices 8 Studies about digital citizenship education can indicate that digital citizenship education programs can lead to substantial gains in knowledge as well as positive behaviors related to digital citizenship, such as using strong passwords, cautious sharing of personal information, and avoiding suspicious links (Mdpi Sustainability, 2025). In addition, the studies done for assessing the cybersecurity awareness of students from college as a whole, demonstrates the need to introduce educational interventions to improve not only the knowledge, but the skills as well, especially for the group that have minimal previous exposure to cyber threats (Majmaah University Study, 2025).

Social and demographic variables also shape awareness and ways of behaving. For instance, if we focus on the study on social media usage among the youth, it shows that if there is much use, there may not necessarily be high awareness of cybercrime as some have much reports of low level of understand of risks of cybercrimes and yet engage a lot in case online (Ahmed et al., 2025). This highlights the need for context specific strategies for awareness that take into account different user characteristics such as age, education and patterns of usage.

The literature provides some suggestion about educational strategies and training models designed to focus on enhancing cybersecurity awareness and safe behavior. Systematic reviews articles about awareness programs divide working knowledge programs into categories such as interactive learning, simulation-based learning, incorporating issues into class curricula, incorporating adapted education tool that can respond based on the individual learning needs (Warlina, 2024). These

approaches are developed to engage users on a more in-depth level and create behavioral changes that are more long lasting than a single user and/or change in behavior.

The above review shows that overall, the literature describes cybercrime awareness as a multi-dimensional construct, which includes the aspects of cognitive understanding, psychological perception, and behavioral execution. Awareness is a requirement but not a sufficient requirement and this must be paired with factors ranging from motivation, self-efficacy, social norms and contextual supports for all of this to reach its full potential to translate into a safe in the digital space. This literature review presents the need for interdisciplinary research by incorporating information systems, psychology, education, and human behavior in understanding and encouraging successful digital safety behavior by users of internet

Methodology

This research has been conducted within the framework of a research design which are mixed method in nature, in order to investigate the nature of the relationship between cybercrime awareness and digital safety behavior among internet users. The methodology used a combination of quantitative surveys, qualitative interviews, and secondary data analysis in order to provide a detailed knowledge of the factors affecting the online safety practices of users. The study design ensured triangulation of data, as well as ensuring greater validity and reliability of results (Creswell & Plano Clark, 2017).

Research Design

A convergent, mixed methods approach was assumed whereby the data collection in terms of quantity and quality gathered was simultaneously. The quantitative component focused on measuring levels of cybercrime awareness, perceived risk and frequency of digital safety behaviours among internet users. The qualitative component went in to depth in terms of experiences, perceptions and motivations user have behind their digital safety practices. Secondary data such as information from cybersecurity bodies, government surveys and published research information put findings into context and identified comparative benchmarks of awareness levels and cybercrime trends across the world.

Population and Sampling

The target population comprised of the active users of the internet with age of 18 years and above living in Islamabad, Pakistan. A stratified purposive sampling technique was utilized so as to ensure that the various categories of age, gender, education and internet usage patterns were represented.

- **Sample Size:** 170 respondents in the Quantitative survey
- **Gender distribution:** Male 52% Female 46% Non-Binary/Other 2%
- **Age groups:** 18-25 (35%), 26-35 (38%), 36-50 (20%), 51+ (7%).
- **Frequency of using Internet Daily:** (68%), Several times a week (22%), Sometimes (10%)

In addition, semi-structured interviews were recruited among 40 participants, in order to be able to get qualitative information about understanding of cyber threats, behaviour response and barriers to safe online practices.

Data Collection Instrument

Quantitative Survey:

Structured questionnaire was used for measurement of:

- Cybercrime awareness: An awareness in Phishing, Malware, ransomware, Identity theft and Online Scams.
- Perceived risk: Risk perception of the user about the vulnerability and magnitude of potential cyber threats.
- Digital safe behavior - How often I engage in safe behaviors like managing passwords, updating software, privacy settings and how I behave when it comes to interacting with people online.
- Likert scale items (1-5 points) were used for all constructs. The survey instrument was modified from validated survey instruments in the study in cybersecurity behaviour research (Ng et al., 2009; Ifinedo, 2012).

Qualitative Interviews:

Semi-structured interviews were conducted with regard to:

- Travels in the worlds of cyber crime.
- Safety Behavior Implementation Decision Making Process
- Motivation and obstacles to undertaking protective measures.
- The interviews were audio recorded, transcribed verbatim and analysed using a methodology called thematic analysis (Braun & Clarke, 2006).

Secondary Data:

Secondary sources were reports on cybersecurity from governmental agencies (e.g. CERT, ENISA), global statistics on cybercrimes and published research articles. These sources were able to aid in getting a macro-level view about the prevalence of cybercrime and trends related to digital safety.

Data Analysis Techniques

Quantitative Analysis:

Descriptive statistics (mean, median, frequency, standard deviation) summary was used to summarize the awareness level of respondents, perceived risk and digital safety practices.

- Correlation analysis was used to find out the correlation between cybercrime awareness and digital safety behavior.
- Multiple regression revealed the predictors of safe behavior in the digital world like the demographic variables, the perceived risk and their experience of cybercrime in the past.
- The differences in awareness and behavior among the age, gender and education groups were tested with the help of the One-Way Analysis of Variance (ANOVA) tests.

Qualitative Analysis:

- Transcripts were thematically coded searching for patterns in perceptions, motivations and challenges in relation to cyber safety behaviour.
- Emerging themes were associated with risk perception, self efficacy, social influence and behavioural barriers.
- Consistency between qualitative and qualitative results was provided by triangulation with survey results.

Ethical Considerations

A strict set of ethics was followed in the study:

- Informed consent was obtained from all the participants.
- Participants were given the assurances of anonymity and confidentiality.
- Participation was voluntary and the respondents could drop out at any stage without consequences.
- Data storage was on security protocols with only the research team having access.

Validity and Reliability

- Construct validity was ensured by the adaptation of the survey items from other research instruments which have been used (Ng et al., 2009; Sheng et al., 2010).
- Internal reliability was measured by using Cronbach's alpha ($a > 0.80$), which revealed consistency of survey scales.

- Triangulation of quantitative and qualitative research increased the comparative reliability.
- When pilot testing the survey and interview questions with 50 people had helped improve them.

Limitations

- Self-reported behaviour may be subject to the social desirability effect.
- Cross-sectional design has one disadvantage, which limits causal inferences.
- Study is based on internet literate users, so it may exclude less digitally-engaged population
- Differences in awareness and/or behaviour among culture and/or region may limit the generalisability.

Results and Discussion

The above, quantitative survey data, qualitative interview responses and secondary sources provide rich data on the awareness of cybercrime and digital safety behaviour among internet users. The results reveal in part, promising patterns of awareness, and an extremely high problem with the protective practices, as an indication of a complex interplay between knowledge, perception and behavior.

Survey data showed that a majority of respondents (72%) had knowledge of some common cyber threats such as phishing, malware and identity theft. The awareness levels varied according to their age, education and the frequency of internet usage. Younger users (18-25) had a great level of recognition of social engineering attacks (78%) whereas with older users (51+) awareness levels were lower (55%). Education level was found to be positively related with awareness as ($r=0.42$, $p<0.01$) suggesting that high level of formal education plays a role in getting better knowledge about cyber risks.

Qualitative interviews strengthened these results and revealed that participants with higher educational levels or professional needs (IT) possessed greater familiarity with security practices, such as the usage of multi-factor authentication and strong password policies and secure browsing habits. On the other hand, participants with lower levels of technical knowledge conceded to a lack of knowledge about judging risks online or determining what's legitimate and what's fraudulent online.

This is supported by secondary sources of global cyber security reports (ENISA, 2024; Verizon, 2024) that demonstrate an uneven state of awareness from the user's population and a significant chunk of the population is still vulnerable to cyber security threats as a result of the limited understanding or fallaciousness.

Despite comparatively good levels of awareness, in terms of protection behaviours, response to practice has been inconsistent. A low 48% of respondents said that they always used strong unique passwords and only 36% said that they updated their software regularly. Multi-factor authentication had been used by 29% of users compared with 31% who frequently check privacy settings on social media and online accounts.

Regression association analyses revealed that the digital safety behaviour was significantly predicted by cyber crime awareness, perceived risk and previous experience with cyber crime ($b = 0.45$, $p < 0.01$ for awareness; $b = 0.32$, $p < 0.05$ for perceived risk). Demographic variables such as age and education also had an impact on behavior with younger and more educated users more likely to implement protective measures.

Qualitative interviews in terms of psychological focus indicated that the behavior of the perceived vulnerability and self-efficacy influenced the safety behavior. Participants responded that low perceived risk or overconfidence of their technical skills was common and contributed to failure to follow safety practices, even by exceptionally aware users of threats. These results are similar to other studies on the knowledge-behavior gap of cybersecurity (Sheng et al., 2010; Hadlington, 2018).

Emerging Qualitative Analysis Themes

Thematic analysis of the interview data revealed four major themes that had an impact on digital safety behaviours:

- **Risk Perception:** Users who had more perception of high likelihood of cybercrime were more proactive in their security measures.
- **Self-Efficacy:** Self-Efficacy for understanding and dealing with digital threats was related to adoption of safe behaviors.

- **Social Influence:** Suggestions from peers, family or the employer shaped the process of behavioural adoption.

Behavioral Barriers Factors including perceived complexity of the security tools, lack of time or inconvenience were barriers to consistent safety practices.

Table 1: Cybercrime Awareness Levels by Age Group

Age Group	High Awareness (%)	Moderate Awareness (%)	Low Awareness (%)
18–25	78	18	4
26–35	74	21	5
36–50	62	30	8
51+	55	32	13

Table 2: Adoption of Digital Safety Practices

Safety Behavior	Always (%)	Sometimes (%)	Never (%)
Strong, unique passwords	48	34	18
Regular software updates	36	40	24
Multi-factor authentication	29	35	36
Privacy settings review	31	39	30

Integrated Discussion

These findings demand a certain degree of internet-user cybercrime awareness but there is an actual gap between digital safety awareness and the actual practice. The users are aware of the dangers but tend not to adopt regular protective measures due to low risk perceptions, barriers or overconfidence. This result confirms the prior research that the awareness is not sufficient to ensure safe Internet use (Liang and Xue, 2010; Hadlington, 2018).

According to demographic patterns, the young and educated are less susceptible due to the fact that these people embrace less risky practices as compared to the older and less educated individuals who are more prone to them. These inequalities indicate that attention interventions on various groups of the population are critical. The necessity of cyber safety education is supported by the role of psychological constructs, including self-efficacy and the feeling of being vulnerable, which are demonstrated to enhance the process of feeling more confident and having practical skills on reducing the threat (Ng et al., 2009; Crossler and Belanger, 2014).

Moreover, social influence is also an important aspect to be considered because the users often resort to the direction of other people such as their peers, family or employer. Behavioral adoption could be allowed through awareness campaigns utilizing social networks and normative company messages.

Generally, this has some implication on the necessity and significance of multi-faceted techniques that combine awareness, education, motivation of behavior, and provision of security devices that can serve to close the knowledge-behavior divide on the topic of digital safety. The cyber hygiene at the individual and the societal level must be enhanced to minimize the probability of cybercrime and guarantee the security of the online interaction.

Discussion

The findings of this study indicate that one can learn about the complex interdependence of cybercrime awareness and internet users digital safety behaviour. In general, the study demonstrates that the awareness of cyber threats among individuals is moderate; however, it is not always the source of the behavior toward the protection. This gap in knowledge-behavior is in line with the other literature, which have indicated that knowledge itself is insufficient in ensuring safe behaviors over the internet (Sheng et al., 2010; Hadlington, 2018; Ng et al., 2009).

The perception of risk is one of the themes that is emerging in the treatment of the behavior of both the quantitative and the qualitative data. When users perceive themselves as vulnerable to cyber threats (either due to a prior occurrence of some cyber events or due to an awareness of the weight of the threat), then they tend to implement safety precautions such as using strong password, updating their software and adjusting their privacy preference. Conversely, individuals who might not

perceive themselves as moderate to high risk as well as over estimate their own digital skills, do not take protective measures, despite fundamental knowledge about the potential threats of cyber crimes. This is backed by the conceptual models such as The Protection Motivation Theory (PMT) and Health Belief Model (HBM) that aided in the promotion of the concept that perceived level of seriousness and susceptibility caused by inherent risk heightened one to take protective measures (Liang and Xue, 2010; Alhendawi et al, 2025).

The research also demonstrates that self-efficacy is an important element in digital safety conduct. Self reporting on their trust to be capable of identifying such phishing attempts or take security precautions so as to safeguard their devices or uphold secrecy on the digital landscape, the participants were much more likely to adopt regular practice in safeguarding. This links the argument where knowledge had to be flanked with beneficial perceptions regarding their ability to act effectively and this has been backed up in a number of researches that have been carried out to investigate the issue of cybersecurity behavior (Ifinedo, 2012; Crossler and Belanger, 2014). The educational interventions and awareness campaigns must target not only the provision of the information, thus, their focus must be the enhancement of the relevant skills and self-confidence in coping with cyber threats.

The other finding that is important is the role of the demographic and social factors. The users who were younger and users with upper cadres of education tend to use digital safety behaviours. This can be ascribed to the greater exposure to technology, greater digital literacy, and acquaintance with the contemporary cyber threat. Less significant gender differences that established nevertheless that a male might have been slightly more successful in the application of some of the protective behaviours (due to greater exposure to technical information, confidence in available digital skills). Also social influence like the advice of friends, family or employers played a significant role. Respondents engaged in advice on security practice behavior with the help of trusted individuals, and it is possible that the application of socially normative cues and peer-led training might be beneficial in terms of regulating security practices awareness.

The theme of behavioral barriers became large as well. Inconvenience, complexity of security tools, and absence of time were identified by the participants to be the factors that are hindering the regular practice of safety. Protective measures were occasionally bypassed by even the users who were conscious of the threats because of perceived effort or technical challenges. These impediments indicate a focus of designing technology as a primary issue of this field and usability and accessibility should be focused on so that protective tools can be designed in a manner that can motivate their use and not pollution.

It also reveals that exposure to previous incidents of cyber has an effect on behaviour. Users who have their experience with phishing, malware, or had identity theft experienced were more reactive to safety measure and it can be argued that direct exposure to cybercrime leads to perceived significance of cybercrime and activates parameters of protection. This conclusion reminds me of the relevance of awareness efforts in which a person can play a simulation game where lives are realistic, or experience of using cases to create a perception of risk that the individuals using it are not experiencing themselves.

Overall, the findings suggest that the formation of effective digital safety behavior should be carried out multi-dimensionally. Although the condition involves awareness, it would have to be combined with risk perception, self efficacy, behavioral motivation, social influence and availability of security tools. The knowledge-behavior gap is to be filled with interventions based on user demographics, user skill levels, and use patterns that must all be taken into account and filled to achieve moderate levels of cybercrime awareness. Addressing these variables, a set of cybersecurity education, mass-level campaigns, and platform regulations can transform web users into a more unified and resistant towards the ever-changing cybersecurity threats.

Finally, this paper brings out the interdisciplinary nature of cybercrime prevention which incorporates knowledge on psychology, information systems, education and behavioral science. Securing online users in a world that has become quite digital is a challenge that requires not only insight into the technical aspects of vulnerabilities, but also into human desires, beliefs and attitudes that can influence behavior related to online security.

Conclusion

In the present study, an all inclusive study on cybercrime awareness and digital safety behaviour among internet and complex interaction between knowledge, perception and behaviour are observed. The findings reveal that the level of awareness with regard to cyber threats is very high (moderate) but does not necessarily stick to protective behaviours. This distinction between knowledge and practice indicates the multifacetedness of the user safety matters, where the cognitive aspects, the psychological contexts, the social behaviors and the use of technology are brought to collide and decide how users behave.

The study demonstrates that cybercrime awareness is a sufficient yet not a sufficient precondition of online practices. Most of the respondents were capable of identifying such common threats as phishing, malware, and identity theft correctly, and this demonstrates that there is a sufficient level of awareness. Nevertheless, fewer than five out of ten utilised any protective measures at least half of the time, including the use of strong passwords, updating to the new types of software and establishing multi-factor authentication. This variation is in line with the extant literature providing the knowledge-behavior gap in the cybersecurity context, stating that awareness fails to induce behavioral compliance (Sheng et al., 2010; Hadlington, 2018).

One of the aspects that dictate the digital safety behavior in this study is the perceived risk. Users who perceive themselves as vulnerable to cyber threats actually tend to take action in order to reduce their risks and those with a low perceived risk or overconfidence of their technical skills will tend to exhibit complacency. This observation can be aligned with the theoretical framework that includes the Protection Motivation Theory (PMT), and the Health Belief Model (HBM) that propose that severity and vulnerability are major driving factors of protection (Liang and Xue, 2010; Alhendawi et al., 2025). As a result, it can be concluded that in addition to providing information, the awareness campaign and educational intervention need to be attentive to building a correct perception of individual susceptibility to cybercrime.

The study goes an extra mile in showing how self-efficacy can help in making online behavior of the study safe. Those respondents that expressed confidently that they could identify the cyber threat and respond to counter them had a high chance of performing environmental protective adaptations. This observation contributes to the fact that knowledge must be linked to the idea of the ability to act. Practice, simulation, and situation exercises of cybersecurity education may be higher levels of self-efficacy, which will inculcate higher opportunities to significantly sustain protective behavior.

It is also accompanied by demographic and social factors which may have influence on the digital safety behaviour as well. Younger and more educated ones were using protective measures more often and likely it is due to their increased exposure to digital technologies and higher levels of digital literacy. Although the difference in safety practices by gender was minimal, it demonstrated that social influence is also an influential factor whereby the impact of peers, family, and employers made the difference in the safety practices that the users adopt. This finding highlights the necessity to pay much closer attention to such features in the framework of the awareness program as age, education, digital literacy, and social environment, and make the interventions workable and effective.

Some of the common barriers that led to lack of consistency in the safety practice included the inconvenience, complexity of security products and time. Even more aware users who were also highly aware also avoided protection practices since they found the effort energy necessary, or they had difficulties in the technical side of the activity or a perceived difficulty in the effort. This emphasises the need to have security applications which are easy to operate and have and create a system that is more assimilated in everyday day online practices - with less friction surrounding it and through which security controls are a normal usage practice.

Another interesting result is that the experience in the past of cyber events results in protective behavior. Users with prior experience of phishing, malware and identity theft showed higher vigilance and proactivity in integrating protective strategies which implicated the significance of experiential learning that reinforced the perceived risk and/or self-efficacy. The insight can be applied in awareness campaigns, which also involve genuine case studies or even artificial simulation of the threat, to induce the users who are not exposed to respond with an increased level of behavior.

The study also highlights the significance of interdisciplinary measures in prevention of cybercrime. Securing users in cyberspace is a complex issue, which requires a blend of technology, behavioral science, Education and policy interventions. Although installing sophisticated security software and securing the systems on the system level is a highly needed requirement, it must be accompanied by the attempts to enhance the human behaviour and form habits of cyber hygiene and a culture of a responsible digital citizen.

Finally, the paper confirms the fact that digital safety promotion in the context of internet users requires multi-dimensional approach. The knowledge should not just be given through awareness programs but should make the perceived risk, self-efficacy and practical skills increase and demographic, social and contextual factors should also be considered. The design of technology must be based on the usability and accessibility design, making it less of a hindrance to the protective behavior. Policy measures to facilitate digital literacy, provide guidance on safe internet practices as well as facilitate social behaviours that enhance internet hygiene.

Through a combination of these measures, stakeholders, including educators, policymakers, technology providers and users themselves, will be on a position to assist in increasing resilience to cybercrime, collectively. Finally, building proper

cybercrime consciousness and cybersecurity habits is an element that belongs not just to personal security, but also significant societal security that promotes trust, stability, and sustainability in the world of the more digital.

Recommendations

- Enhance Cybersecurity Education: Initiate formal education in schools, universities and workplace regarding knowledge of cyber threat, internet practices and reversal of cyber threat threat (Ng et al., 2009; Alhendawi et al., 2025).
- Enhance Risk Perception: Awareness: Awareness must include real-life scenarios, case studies and interactive simulations in order to make the user realize their actual vulnerability to cyber threats(Sheng et al., 2010; Hadlington, 2018).
- Encourage Practical Self-Efficacy - Provide practising programs on passwords and multi-factor authentication, as well as practice of updating and secure browsing in order to increase the confidence of self-efficiency of users to act in such protective behaviours (Ifinedo, 2012; Crossler and Belanger, 2014).
- Create Intuitive Security Aids: Build a set of cybersecurity tools and applications that are easy to use and want least intrusive to everyday web usage to lessen the obstacle to behavior (Hadlington, 2018).
- Demographic Specific Interventions - Individual Programs - Customize programs based on age, education, and digital literacy in order to address the needs and vulnerabilities of the unique users groups (Alqarni, 2025).
- Enhance Social Influence and learning through collegiality: Consolidate the use of Social networking, peer education or community based education and student initiated awareness to promote protective interventions (Majmaah University Study, 2025).
- Cyber Hygiene into Organization Policies: The work location is supposed to formalize the digital safety regulations, train regularly and encourage reporting of cyber crimes (Furnell, 2005).
- Enhance Ongoing Learning: In the present-day world, users have to keep informed about new forms of cyber threats through newsletters, online courses, and through announcements in the form of public service (Jakobsson and Myers, 2007).
- Promote Privacy-Conscious Culture Encourage the user to learn about privacy and social media sites and about acceptable online behavior to make them responsible online citizens (Mdpi Sustainability, 2025).
- Fund Research and Policy-making: Trans-cultural research and longitudinal studies will be conducted to supplement policies, rules, and norms on the security of the online world and cybercrime mitigation (Alhendawi et al., 2025; ENISA, 2024).

References

1. Alhendawi, M., Alwan, A., & Al-Fatlawi, R. (2025). Application of health belief model to cybersecurity behavior: University students' perspective. Cybersecurity, 11(1), tyaf034. https://doi.org/10.1093/cybsec/tyaf034
2. Alqarni, M. (2025). Cybersecurity awareness and data protection behavior among Saudi secondary students. Human Behavior and Emerging Technologies, 7(2), 300–318. https://doi.org/10.1002/hbe2.261
3. Ahmed, S., Khan, R., & Ali, M. (2025). Social media usage and cybercrime awareness: Evidence from young adults. Social Works Review, 8(1), 45–60. https://socialworksreview.com/index.php/Journal/article/view/266
4. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
5. Crossler, R. E., & Bélanger, F. (2014). Understanding factors affecting information security policy compliance. Journal of Information Systems, 28(2), 101–114.
6. ENISA. (2024). European Union agency for cybersecurity report: Trends and challenges in 2024. European Union. https://www.enisa.europa.eu
7. Furnell, S. (2005). Cybercrime and awareness: Evaluating the effectiveness of training programs. Computers & Security, 24(5), 385–395.
8. Hadlington, L. (2018). Human factors in cybersecurity: Examining knowledge, behavior, and awareness. Information Security Journal, 27(4), 154–164.
9. Hadnagy, C. (2018). Social engineering: The science of human hacking (2nd ed.). Wiley.
10. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and protection motivation theory. Computers & Security, 31(1), 83–95.
11. Internet World Stats. (2025). Global internet usage statistics. https://www.internetworldstats.com
12. Jakobsson, M., & Myers, S. (2007). Phishing and countermeasures: Understanding the increasing problem of electronic identity theft. Wiley.

13. Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computing. Communications of the ACM, 53(6), 41–45.
14. Majmaah University Study. (2025). Cybersecurity awareness and protective behavior among college students. MDPI. https://www.mdpi.com/2504-2289/5/2/23
15. Mdpi Sustainability. (2025). Digital citizenship and cybersecurity awareness: An empirical study. Sustainability, 15(15), 11512. https://www.mdpi.com/2071-1050/15/15/11512
16. Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. Wiley.
17. Nagari, H., & Raharja, S. (2025). Cybersecurity knowledge and online behavior in digital banking users. Asian Pacific Financial Journal, 7(1), 45–60. https://apfjournal.or.id/index.php/apf/article/view/398
18. Ng, B. Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815–825.
19. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 68, 63–76.
20. Qalby, R., Budi, I., & Hidayat, A. (2025). Cybersecurity awareness and behavior in online learning environments. Journal of Information Integrity, 12(2), 55–71. https://jii.rivierapublishing.id/index.php/jii/article/view/6684
21. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of warnings. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 373–382.
22. Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217–224.
23. Verizon. (2024). Data breach investigations report 2024. Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/dbir/
24. Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age (2nd ed.). Polity Press.
25. Warlina, A. (2024). Effectiveness of interactive cybersecurity education: A systematic review. Quanta Journal, 8(1), 20–35. https://ejournal.resincen.org/index.php/quanta/article/view/31
26. Kshetri, N., Voas, J., & Voas, J. (2023). Cybersecurity awareness and digital behavior among higher education students. arXiv preprint arXiv:2310.12684. https://arxiv.org/abs/2310.12684
27. Albrechtslund, A. (2008). Online social networking as participatory surveillance. First Monday, 13(3).
28. Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. MIS Quarterly, 34(3), 549–566.
29. Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502.
30. Kshetri, N. (2017). Cybersecurity awareness and protective behavior: Global perspectives. Information Systems Frontiers, 19(2), 329–344.