

## Understanding Students' Security Intention and Protective Behaviour against Virus Threats in Higher Education BYOD Environments: A PMT Framework

### *Memahami Niat Keselamatan dan Tingkah Laku Perlindungan Pelajar terhadap Ancaman Virus dalam Persekitaran BYOD Pendidikan Tinggi: Satu Kerangka PMT*

Marwa Khalid Tahir<sup>1</sup>, Hanifah Abdul Hamid<sup>2</sup>

<sup>1, 2</sup> Faculty of Science and Technology, Universiti Sains Islam Malaysia

Email: <sup>1</sup> [3241303@raudah.usim.edu.my](mailto:3241303@raudah.usim.edu.my), <sup>2</sup> [hanifah@usim.edu.my](mailto:hanifah@usim.edu.my)

#### ABSTRACT

The adoption of Bring Your Own Device (BYOD) in educational institutions has enhanced learning flexibility but has also introduced cybersecurity vulnerabilities. Virus threats are a particular concern, as students' personal devices may lack consistent security controls and may be compromised through malicious files, links, and other online activities. This research applies Protection Motivation Theory (PMT) as the theoretical foundation for proposing a framework to explain students' Security Intention and Protective Behaviour toward virus threats in higher education BYOD environments. The proposed framework incorporates perceived severity, perceived vulnerability, response efficacy, self-efficacy, and response cost as factors influencing Security Intention, which subsequently influences Protective Behaviour. Security Intention is further positioned as a mediating mechanism between the PMT factors and Protective Behaviour. By integrating threat appraisal, coping appraisal, Security Intention, and Protective Behaviour, the framework provides a theoretical basis for understanding how students' evaluations of virus threats and protective measures may translate into protective action. The proposed framework provides a foundation for future empirical examination and may contribute to informing and strengthening cybersecurity practices in higher education BYOD environments.

*Keywords: BYOD, Virus Threats, Protection Motivation Theory, Security Intention, Protective Behaviour*

#### INTRODUCTION

Digital technologies have transformed the educational landscape by enabling students to access learning resources through their personal devices. The widespread adoption of Bring Your Own Device (BYOD) practices in higher education has further increased the use of personal devices for teaching and learning activities (Chilton et al., 2025). While BYOD offers flexibility and convenience, the increasing reliance on personal devices has introduced new cybersecurity challenges for both students and educational



institutions (Aljuaid et al., 2023). This challenge is particularly important because personally owned devices may operate beyond the direct security management of educational institutions, resulting in varying levels of security protection across devices (Ulven & Wangen, 2021; Ratchford et al., 2022). Among the various cybersecurity threats associated with personal device usage, virus infections continue to pose a significant concern. Viruses may spread through various channels and can compromise device security, affect system performance, and threaten institutional resources when infected devices are connected to shared networks (Alenezi et al., 2020; Felicia et al., 2022). As students increasingly depend on personal devices for academic activities, protecting these devices against virus threats has become increasingly important. Although technical measures such as antivirus software and security updates can help reduce the risk of virus infections, students in BYOD environments are largely responsible for ensuring the security of their personal devices through decisions regarding software installation, file downloads, and device security. This responsibility is particularly relevant because students may use the same personal devices for both academic and personal activities, potentially increasing their exposure to malicious websites, downloads, email attachments, and other online resources (Palanisamy et al., 2022). Consequently, effective protection against virus threats depends on both technical safeguards and students' security practices.

Human-related vulnerabilities continue to contribute to cybersecurity risks in higher education, particularly where personal devices are used for academic purposes (Ulven & Wangen, 2021). In BYOD environments, students are primarily responsible for securing their personal devices, making their security behaviour important in reducing cybersecurity risks (Sharfdeen et al., 2025). Therefore, technical safeguards alone may be insufficient if students do not recognise cybersecurity risks or are unwilling or unable to undertake recommended protective actions. Previous research has highlighted that the effectiveness of cybersecurity measures often depends on users' awareness and willingness to adopt recommended security practices (Alqahtani, 2022). Existing studies have also examined broader cybersecurity awareness and information security behaviour among university students (Alqahtani, 2022; Han et al., 2025; Alam et al., 2025). Nevertheless, the specific behavioural process through which students evaluate virus threats and translate these evaluations into protective action within BYOD environments remains insufficiently explained. This distinction is important because students exercise substantial control over their personal devices and make everyday decisions concerning downloads, software installation, security updates, and other practices that may increase or reduce their exposure to virus infection.

Protection Motivation Theory (PMT) provides an appropriate theoretical foundation for examining this behavioural process because it explains protective responses through two cognitive appraisal mechanisms: threat appraisal and coping appraisal (Siponen et al., 2024). Threat appraisal concerns individuals' evaluation of the seriousness and likelihood of a threat, whereas coping appraisal concerns their evaluation of the effectiveness, capability, and costs associated with undertaking protective actions. However, evaluating a threat and its possible protective responses does not necessarily mean that an individual will subsequently perform the corresponding protective behaviour. An important intermediate mechanism may therefore be Security Intention, which represents an individual's willingness and commitment to undertake protective actions. Behavioural intention provides an important link between cognitive evaluations and subsequent behaviour (Conner & Norman, 2022), while stronger cybersecurity-related intentions have been associated with greater engagement in protective security behaviour among university students (Han et al., 2025).

Accordingly, the proposed framework contributes to the existing literature in three related ways. First, it contextualises PMT specifically within students' responses to virus threats in higher education BYOD environments, where students assume considerable responsibility for securing their personal devices. Second, it distinguishes Security Intention from actual Protective Behaviour, recognising that the evaluation of cybersecurity threats and protective measures may not automatically translate into protective action. Third, by positioning Security Intention as a mediating mechanism, the framework seeks to explain how students' threat and coping appraisals may be translated into Protective Behaviour.

The framework therefore provides a theoretical foundation for subsequent empirical investigation of the behavioural mechanisms underlying virus protection in higher education BYOD environments.

## LITERATURE REVIEW

### Virus Threats in BYOD

Malware, including viruses, remains a persistent cybersecurity threat despite continuous advancements in information and communication technologies (Roseline & Geetha, 2021). Cyber threats continue to evolve, creating ongoing challenges associated with protecting digital systems from malicious activities (Perwej et al., 2021). Among these threats, viruses are a type of malicious software capable of replicating and spreading across devices, potentially compromising system functionality and information security. According to Zayyad (2023), virus infections may result in data loss, system disruption, and substantial recovery efforts. Although viruses constitute one category within the broader malware landscape, their relevance to BYOD extends beyond infection of an individual device. A compromised personally owned device may interact with institutional systems and networks, creating a potential security pathway between students' personal digital activities and university resources. This makes virus protection in BYOD not merely an individual device-security issue but also a concern for institutional cybersecurity.

The widespread adoption of BYOD has further increased exposure to virus threats because personal devices typically operate outside institutional security management (Downer & Bhattacharya, 2022). Unlike institution-managed devices, personal devices often vary in operating systems, installed security software, and software update practices, leading to inconsistent levels of protection among users (Jimshith & Mary Amala Bai, 2024). Ulven and Wangen (2021) reported that educational institutions face considerable challenges in enforcing consistent security controls across personally owned devices, while Ratchford et al. (2022) identified device diversity and inconsistent security configurations as key security challenges in BYOD environments. Collectively, these studies suggest that compromised personal devices may serve as entry points through which viruses and other forms of malware can infiltrate institutional networks.

Virus infections may also result from malicious downloads, infected files, email attachments, and compromised websites, through which malware can gain access to devices and spread across connected systems (Bahashwan & Al-Tuwairqi, 2021). Students' online activities may therefore increase their vulnerability to virus infections within BYOD environments. This risk may be amplified because students frequently use the same personal devices for both academic and personal activities, increasing their exposure to potentially malicious websites, downloads, email attachments, and other online resources (Palanisamy et al., 2022). Taken together, the literature indicates that virus risk in BYOD environments emerges from the interaction of technological and behavioural vulnerabilities. Device diversity and inconsistent security configurations create technical exposure, while students' everyday decisions concerning downloads, attachments, websites, updates, and security software may determine whether that exposure develops into an actual security incident. This interaction provides an important basis for examining students' protective responses rather than focusing exclusively on technical controls.

The consequences of virus infections may extend beyond individual devices, particularly when compromised personal devices are connected to institutional networks. Infected devices may contribute to unauthorised access, information compromise, and operational disruption within organisations (Aguboshim et al., 2023). Therefore, understanding virus risk in higher education BYOD environments requires attention not only to how devices become exposed but also to why students choose to adopt, postpone, or avoid protective security measures. This shifts the focus from the technological characteristics of the threat to the behavioural mechanisms underlying students' responses to that threat.

### **Human Factors in BYOD Security**

Human factors have become an important aspect of BYOD security because the use of personally owned devices places greater responsibility on users to maintain secure practices. Unlike organisation-managed devices, BYOD gives users greater control over device settings and security practices, making user awareness and behaviour important factors in maintaining information security (Aljuaid et al., 2023). The human dimension of BYOD security extends beyond users' technical knowledge and involves how individuals perceive, manage, and respond to security requirements. While Downer and Bhattacharya (2022) emphasised that users' awareness, attitudes, and responses to security measures influence the effectiveness of BYOD security practices, Ferdousi (2022) argued that human-related vulnerabilities primarily arise from lapses in user judgement that may allow malware to compromise devices or information. More importantly, awareness of a cybersecurity threat does not necessarily guarantee protective action. Users may recognise a security risk but still fail to respond when they perceive protective measures as ineffective, difficult to perform, inconvenient, or unnecessarily burdensome. The behavioural challenge in BYOD security therefore concerns not only whether students are aware of cybersecurity threats, but also how they evaluate those threats and the protective responses available to them.

In educational settings, these human factors are particularly important because students manage their own devices while accessing institutional resources. Sharfateen et al. (2025) reported that security awareness and policy compliance influence secure BYOD practices among users in Malaysian public universities. Tuah and Rahim (2023) further argued that successful BYOD adoption depends not only on technological infrastructure but also on human and contextual factors, including users' behaviours, institutional norms, and individual approaches to securing personal devices.

Beyond security awareness and individual behaviour, users' willingness to comply with BYOD security requirements may also be influenced by social and institutional factors. Social influence and perceived support have been identified as important predictors of users' intention to comply with BYOD security policies (Lee et al., 2024). These findings suggest an important distinction between providing cybersecurity protection and motivating students to use that protection. Universities may establish policies, provide security guidance, and recommend protective technologies, but students ultimately make many of the day-to-day security decisions on personally owned devices. Consequently, explaining Protective Behaviour requires consideration of the cognitive processes that motivate students to respond to perceived cybersecurity threats. This need provides the theoretical rationale for applying a behavioural framework such as Protection Motivation Theory, which explicitly considers both individuals' perceptions of threats and their evaluations of the actions available to manage those threats.

### **BYOD in Higher Education**

Bring Your Own Device (BYOD) refers to the practice where educational institutions allow students to use their personally owned devices, such as laptops, smartphones, and tablets, to access university systems, learning platforms, and educational resources (Sharfateen et al., 2025). The adoption of BYOD in education has been facilitated by advances in mobile technologies and wireless connectivity, enabling the integration of personal devices into teaching and learning (Li, 2022). Following the COVID-19 pandemic, universities increasingly relied on students' personal devices to support remote and hybrid learning, making BYOD an integral component of digital education (Calias et al., 2024).

BYOD enhances learning flexibility by enabling students to access educational resources anytime and anywhere using familiar devices. It also promotes student engagement and allows institutions to reduce investment in institution-owned hardware (Gundaboina, 2025). These benefits have contributed to the continued adoption of BYOD in higher education. Despite these advantages, the successful implementation of BYOD depends on both institutional readiness and students' ability to use and secure their personal devices effectively. While van As and Brits (2023) emphasised the importance of device quality, digital literacy, and infrastructure, Othman et al. (2020) highlighted the role of network capacity and institutional policies in supporting effective BYOD implementation. This combination of institutional dependence and individual responsibility creates a distinctive cybersecurity environment. Universities benefit from the accessibility and flexibility of student-owned devices but have less direct control over how those devices are configured, updated, protected, and used outside the institutional environment. As a result, the security of BYOD cannot be separated from the behaviour of the students who own and manage the devices.

The widespread use of personal devices also presents significant cybersecurity challenges. According to Ulven and Wangen (2021), personal devices operate outside the direct control of universities, making it difficult to enforce standardised security policies, software updates, and security configurations. Similarly, Ntwari et al. (2022) found that differences in operating systems, security software, and user practices create inconsistent levels of protection across devices, increasing institutional exposure to cybersecurity risks. The increasing reliance on personal devices has also heightened the risk of malware infections, unauthorised access, and data breaches in higher education (Alexei & Alexei, 2021; Rosman et al., 2022). Accordingly, higher education BYOD represents an appropriate setting for examining virus Protective Behaviour because responsibility for cybersecurity is shared between the institution and the individual user. While universities may provide technological infrastructure, policies, and security guidance, students retain considerable control over the protective actions performed on their own devices. Understanding the motivational processes underlying these actions is therefore important for explaining why students differ in their responses to the same or similar cybersecurity risks.

### **Protection Motivation Theory (PMT)**

Protection Motivation Theory (PMT) is widely used in cybersecurity research to explain individuals' adoption of protective security behaviours (Alrawhani et al., 2025). The theory focuses on how individuals assess potential threats and evaluate their ability to respond effectively. PMT consists of two key cognitive appraisal processes, namely threat appraisal and coping appraisal, which together influence an individual's protective behaviour (Siponen et al., 2024).

Threat appraisal refers to an individual's evaluation of a threat and its potential consequences. This process helps explain how individuals judge the seriousness of security risks and whether such risks require protective action (Khan et al., 2023). In cybersecurity contexts, threat appraisal plays an

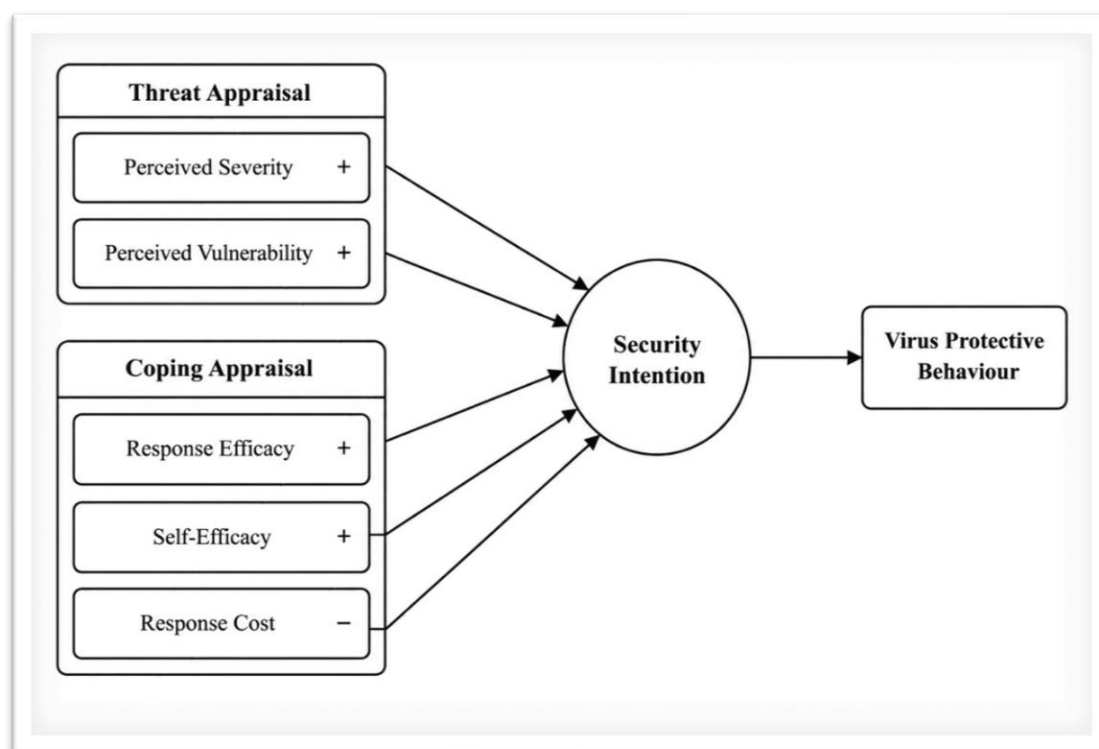
important role in shaping users' willingness to adopt security measures. Within the proposed framework, threat appraisal is represented by perceived severity and perceived vulnerability. Perceived severity captures the perceived seriousness of the consequences associated with a virus infection, whereas perceived vulnerability reflects the perceived likelihood of personally experiencing such an infection. Considering both dimensions is important because a student may recognise that a virus infection could have serious consequences while simultaneously believing that such an infection is unlikely to happen to them. This is particularly relevant in BYOD environments, where students increasingly depend on personal devices to access institutional systems and digital learning resources, potentially increasing their exposure to cyber threats and security vulnerabilities (Chilton et al., 2025). Previous research suggests that students' perceptions of security threats may influence their adoption of protective measures when using personal devices (Han et al., 2025).

Coping appraisal refers to an individual's evaluation of available protective actions and their ability to perform those actions effectively. This process involves assessing personal capability, available resources, and the effectiveness of recommended security measures in reducing potential threats (Sulaiman et al., 2022). In this study, coping appraisal is represented by response efficacy, self-efficacy, and response cost. Response efficacy concerns whether students believe that recommended security measures can effectively reduce virus threats; self-efficacy concerns whether students believe that they are capable of performing those measures; and response cost reflects the perceived time, effort, inconvenience, or other barriers associated with performing them. These constructs allow the framework to distinguish between recognising that protection is effective and believing that one is personally capable and willing to perform the required action.

By focusing on how individuals evaluate threats and protective actions, PMT has been widely applied to investigate various cybersecurity behaviours, including information security compliance, malware prevention, and threat avoidance (Siponen et al., 2024). However, the present framework goes beyond examining the direct motivational effects of PMT factors by distinguishing between the formation of Security Intention and the performance of Protective Behaviour. This distinction is theoretically important because individuals may evaluate a threat and a coping response positively without necessarily translating those evaluations immediately into action. Behavioural intention can therefore represent an intermediate motivational stage through which threat and coping appraisals are converted into subsequent behaviour (Conner & Norman, 2022). In the cybersecurity context, Han et al. (2025) similarly demonstrated the relevance of security-related intentions to students' information security behaviour. Collectively, the literature supports a sequential explanation in which students first evaluate the virus threat and available protective responses, subsequently develop an intention to undertake protective action, and ultimately translate that intention into Protective Behaviour. This theoretical sequence provides the foundation for the research framework developed in the following section.

### **Research Framework**

The research framework is based on Protection Motivation Theory (PMT) and illustrates how individuals evaluate potential threats and protective responses when addressing virus risks. Consistent with PMT and previous cybersecurity research, individuals assess both the characteristics of a threat and their ability to cope with it before engaging in protective actions (Sulaiman et al., 2022). More specifically, perceived severity and perceived vulnerability represent the threat-appraisal dimension of PMT, whereas response efficacy, self-efficacy, and response cost represent the coping-appraisal dimension. The framework proposes that these cognitive appraisals do not necessarily translate directly into Protective Behaviour; rather, they contribute to the formation of Security Intention, which represents students' motivation to undertake protective actions. Security Intention is subsequently expected to translate these evaluations into actual Protective Behaviour.



**Figure 1: Research Framework**

The framework outlines the proposed relationships among the research variables and provides the conceptual basis for this research. Importantly, the framework distinguishes between the cognitive appraisal of virus threats, the motivation to respond, and the performance of protective actions. This distinction enables the framework to explain not only which PMT factors may influence students' Protective Behaviour, but also the process through which these factors may lead to protective action in higher education BYOD environments.

### **Perceived Severity and Security Intention**

Perceived severity reflects students' assessment of the seriousness of consequences resulting from cyber threats, such as malware infection, data loss, and system compromise (Gwenhure, 2025). When students recognise that virus infections may disrupt academic activities and compromise personal information, they are more likely to regard protective actions as necessary. Students who perceive the consequences of cyber threats as serious may be more motivated to adopt preventive measures to reduce the likelihood of experiencing such outcomes. In an academic environment, concerns about losing important coursework, academic records, or personal information may further reinforce students' perceptions of the seriousness of virus threats. According to Khan et al. (2023), higher perceived severity strengthened students' motivation to comply with recommended cybersecurity practices. Similarly, Jones et al. (2022) reported that awareness of cyberattack consequences encouraged individuals to avoid unsafe digital behaviours. These findings indicate that perceived severity may function as an important motivational trigger: when the anticipated consequences of virus infection are considered sufficiently serious, students may perceive a stronger need to protect their devices. Conversely, when the consequences are regarded as minor or manageable, the motivation to undertake preventive security measures may be weaker.

### **Perceived Vulnerability and Security Intention**

Perceived vulnerability refers to an individual's belief regarding the likelihood of experiencing a threat (Vortia 2025). Students who frequently use personal devices for academic and online activities may perceive themselves as susceptible to malware infections and other cybersecurity threats. Gustara et al. (2025) observed that students who perceived themselves as more vulnerable demonstrated stronger

intentions to adopt secure online behaviours. Similarly, Saleh et al. (2025) found that perceived vulnerability was associated with increased cybersecurity intentions, suggesting that individuals who believe they are more susceptible to cyber threats are more likely to consider adopting protective measures. In the context of virus threats, students who perceive themselves as vulnerable to malware infection may be more motivated to adopt protective behaviours. Perceived vulnerability is conceptually distinct from perceived severity. A student may acknowledge that virus infection could produce serious consequences but still believe that such an event is unlikely to occur personally. Protective motivation may therefore depend not only on recognising the seriousness of the threat but also on perceiving oneself as susceptible to that threat.

### **Response Efficacy and Security Intention**

Response efficacy refers to students' beliefs that recommended protective measures, such as antivirus software, system updates, and cautious online behaviour, are effective in reducing cyber threats (Kiran et al., 2025). Individuals are generally more willing to adopt protective measures when they believe those measures can successfully prevent or reduce potential harm. Farooq et al. (2020) reported that perceived security positively influenced university students' intention to use e-learning systems, indicating that individuals who believe security measures are effective are more likely to adopt protective practices. Similarly, Jansen et al. (2020) found that response efficacy significantly influences users' intention to adopt cybersecurity protective behaviors, as individuals are more likely to comply with security measures when they believe those actions are effective in mitigating cyber threats. Thus, awareness of virus risk alone may not be sufficient to generate Security Intention. Students must also believe that the recommended response can meaningfully reduce the threat. If antivirus software, system updates, or cautious online practices are perceived as ineffective, students may have little motivation to invest effort in performing them even when the threat itself is considered serious.

### **Self-Efficacy and Security Intention**

Self-efficacy refers to students' confidence in their ability to successfully perform recommended cybersecurity practices. It reflects the extent to which individuals believe they possess the knowledge, skills, and capability required to implement protective actions against cyber threats (Sulaiman et al., 2022). Students who feel capable of identifying suspicious activities, updating software, and applying security measures are generally more confident in their ability to protect themselves from cyber risks. Zhou et al. (2020) found that individuals with higher levels of self-efficacy were more likely to engage in secure smartphone usage, indicating that confidence in one's ability to perform protective security behaviours promotes the adoption of recommended cybersecurity practices. In the context of higher education, Han et al. (2025) reported a positive relationship between self-efficacy and information security behaviour among university students. Similar findings were reported by Alam et al. (2025), who found that self-efficacy played an important role in influencing students' information security behaviour within the PMT framework. Likewise, Alhelaly et al. (2024) found that self-efficacy plays a significant role in enhancing individuals' motivation and intentions to engage in cybersecurity protection behaviours. The distinction between response efficacy and self-efficacy is particularly important. Students may believe that a particular security measure is effective but may still lack confidence in their own ability to implement it correctly. In such circumstances, the effectiveness of the security measure itself may not be sufficient to produce a strong intention to act.

### **Response Cost and Security Intention**

Response cost refers to perceived barriers associated with performing protective actions, including time, effort, inconvenience, or reduced usability (Han et al., 2025). Although individuals may recognise the benefits of cybersecurity measures, they may become reluctant to adopt them when implementation is perceived as burdensome. For example, installing security software, updating systems, or following security guidelines may be viewed as inconvenient or time-consuming by some students. Alqarni (2025) reported that higher perceived response costs discouraged students from adopting recommended cybersecurity measures, particularly when security practices were viewed as complex or time-consuming. Similarly, Dodge et al. (2023) found that response costs affected users' intentions to adopt recommended cybersecurity practices. Unlike response efficacy and self-efficacy, response cost

represents an inhibitory component of coping appraisal. Even when students believe that protective measures are effective and that they are capable of performing them, perceived inconvenience, time requirements, effort, or disruption may reduce their willingness to act. Security Intention may therefore reflect a cognitive trade-off between the perceived benefits of protection and the perceived burden associated with performing the protective response.

### **Security Intention and Protective Behaviour**

Security intention refers to an individual's willingness and commitment to engage in actions that reduce exposure to cybersecurity threats (Carter & McNealey, 2025). It represents the motivational factor that precedes actual behaviour and reflects the extent to which an individual plans to perform protective actions (Morwitz & Munz, 2021). Students who intend to protect their devices from virus threats are more likely to engage in activities such as updating software, using antivirus applications, avoiding suspicious downloads, and following safe online practices. Han et al. (2025) found that individuals who reported stronger cybersecurity intentions were more likely to engage in protective security behaviours. Ng et al. (2021) similarly demonstrated that users' security-related attitudes and intentions were significantly associated with compliance with recommended security practices. In addition, Conner and Norman (2022) noted that behavioural intentions are key determinants of subsequent behaviour, indicating that individuals with stronger intentions are more likely to carry out the intended actions. Security Intention is therefore conceptually important because it separates students' cognitive evaluations from the actual performance of security practices. A student may recognise a virus threat and evaluate a protective measure favourably, but Protective Behaviour is more likely when these evaluations have first developed into a sufficiently strong intention to act.

### **Mediating Role of Security Intention**

Security intention represents an individual's willingness to perform actions that reduce exposure to cybersecurity threats. Within PMT, security intention is considered a key motivational mechanism that links threat appraisal and coping appraisal to protective behaviour. PMT suggests that individuals first evaluate the severity and likelihood of a threat, as well as their ability to respond effectively, before forming intentions to adopt protective measures (Mou et al., 2022). These intentions subsequently influence whether protective behaviours are performed.

Previous studies have highlighted the key role of security intention in translating individuals' threat perceptions and coping evaluations into actual cybersecurity behaviours. According to Conner and Norman (2022), behavioural intention serves as the most immediate predictor of behaviour, linking cognitive evaluations to action. Similarly, Han et al. (2025) found that cybersecurity-related intentions significantly influenced protective security behaviour among university students. In the context of virus threats, students who perceive themselves as vulnerable to infection, consider protective measures to be effective, and feel capable of implementing them are more likely to develop stronger security intentions, which in turn encourage protective behaviour. The proposed mediation therefore represents more than an additional statistical relationship within the framework. It provides the explanatory mechanism connecting students' cognitive appraisal of virus threats and protective responses with their subsequent actions. In other words, the PMT factors are expected to shape whether students become motivated to act, while Security Intention represents the motivational pathway through which these appraisals may ultimately influence Protective Behaviour.

Accordingly, the proposed mediating role of Security Intention provides a process-oriented explanation of students' Protective Behaviour. Threat and coping appraisals may first influence whether students become motivated to protect their devices, while Security Intention represents the motivational stage preceding actual protective action. However, the framework does not imply that Security Intention will inevitably result in Protective Behaviour. Students may intend to update security software, avoid suspicious downloads, or adopt other recommended practices but may not consistently perform these actions. The proposed mediating role of Security Intention should therefore be regarded as a theoretical mechanism that warrants subsequent empirical examination rather than an empirically established relationship in the present conceptual paper.

Overall, the framework suggests that virus protection in higher education BYOD environments should not be understood solely as a technological issue or solely as a matter of cybersecurity awareness. Instead, Protective Behaviour may emerge from a sequence in which students evaluate the threat, assess their capacity and available responses, develop an intention to act, and subsequently translate that intention into protective practices. By integrating these stages, the framework provides a theoretical basis for understanding the behavioural processes underlying students' responses to virus threats in BYOD environments.

### **Discussion of Theoretical Framework**

The proposed framework provides a theoretical explanation of how students may develop Protective Behaviour against virus threats in higher education BYOD environments. Drawing on PMT, the framework suggests that students' responses to virus threats involve both threat appraisal and coping appraisal rather than being determined solely by their awareness of cybersecurity risks. Threat appraisal, represented by perceived severity and perceived vulnerability, reflects students' evaluation of the seriousness of virus threats and their susceptibility to such threats. Coping appraisal, represented by response efficacy, self-efficacy, and response cost, reflects students' evaluation of whether protective actions are effective, manageable, and worth performing. This distinction is consistent with the central appraisal processes of PMT in information security behaviour (Mou et al., 2022; Siponen et al., 2024). An important theoretical consideration arising from the framework is that recognising a virus threat may not, by itself, be sufficient to motivate Protective Behaviour. Students may perceive virus infection as serious and believe themselves to be vulnerable, but these perceptions may not result in protective action if they doubt the effectiveness of available security measures or lack confidence in their ability to perform them. Conversely, students who perceive protective measures as effective and believe themselves capable of implementing them may be more motivated to act when they also recognise the relevance of the threat. The framework therefore suggests that threat appraisal and coping appraisal perform complementary roles in explaining students' protective responses rather than representing independent explanations of security behaviour.

This interaction between threat and coping appraisals is particularly relevant within a BYOD environment because students exercise considerable control over the security of their personally owned devices. Unlike institution-managed devices, personal devices may differ in operating systems, security configurations, installed security software, and update practices (Jimshith & Mary Amala Bai, 2024; Ratchford et al., 2022). Educational institutions may therefore face difficulties in maintaining consistent security controls across these devices (Ulven & Wangen, 2021). In this context, students are not merely recipients of institutional cybersecurity measures; their individual decisions and security practices form part of the protective environment itself. The application of PMT to BYOD therefore provides a behavioural perspective for explaining why students exposed to similar cybersecurity risks may respond differently. The coping-appraisal component of the framework further highlights an important distinction between believing that a protective measure is effective and believing that one is personally capable of performing it. Response efficacy concerns confidence in the protective measure, whereas self-efficacy concerns confidence in one's own capability to perform the required action. A student may, for example, believe that antivirus software, regular system updates, and cautious downloading practices are effective but may lack the knowledge or confidence required to implement these measures appropriately. Previous studies have demonstrated the relevance of self-efficacy to secure technology use and students' information security behaviour (Zhou et al., 2020; Alam et al., 2025; Han et al., 2025). Response cost adds a further consideration

because even an effective and manageable security measure may be avoided if it is perceived as excessively inconvenient, time-consuming, or burdensome. Thus, coping appraisal provides a more nuanced explanation of why knowledge of an appropriate security response may not necessarily result in willingness to perform that response. A further theoretical feature of the framework is the distinction between Security Intention and Protective Behaviour. The framework does not assume that students' evaluations of virus threats and protective responses automatically produce protective action. Instead, Security Intention is conceptualised as an intervening motivational mechanism through which threat and coping appraisals may translate into Protective Behaviour. This distinction is important because behavioural intention represents a proximal predictor of behaviour, while an intention-behaviour gap may nevertheless occur (Conner & Norman, 2022). In the cybersecurity context, Han et al. (2025) similarly demonstrated the relevance of security-related intentions to information security behaviour among university students.

### **Theoretical implications**

The proposed conceptual framework extends the application of Protection Motivation Theory (PMT) to students' Protective Behaviour against virus threats in BYOD environments. PMT has been widely applied in information security research to explain how individuals evaluate threats and protective responses before engaging in security behaviour (Siponen et al., 2024). However, its application to students' Protective Behaviour against virus threats remains comparatively limited. By focusing specifically on virus-related Protective Behaviour within higher education BYOD environments, the framework provides a more context-specific application of PMT to a setting where security responsibility is distributed between institutional safeguards and individual users.

A key theoretical contribution of the framework is the positioning of Security Intention as a mediating mechanism between the PMT factors and Protective Behaviour. Behavioural intention represents an important link between individuals' evaluations and subsequent behaviour (Conner & Norman, 2022). Within cybersecurity, stronger security-related intentions have also been associated with greater engagement in protective security behaviour (Han et al., 2025). Building on this perspective, the framework proposes that students' threat and coping appraisals may influence Protective Behaviour through the formation of Security Intention. This positioning provides a process-oriented interpretation of PMT by distinguishing three conceptually related stages: appraisal of the threat and coping response, formation of motivation to act, and subsequent Protective Behaviour. In doing so, the framework avoids assuming that students' perceptions of cybersecurity risks necessarily translate directly into protective action.

The framework also applies both threat appraisal and coping appraisal to the higher education BYOD context. This is important because students are largely responsible for securing their own devices and making everyday security decisions (Ulven & Wangen, 2021). Rather than treating threat appraisal and coping appraisal as interchangeable sources of protective motivation, the framework preserves their distinct theoretical roles. Threat appraisal explains whether students perceive virus threats as sufficiently serious and personally relevant, whereas coping appraisal explains whether they perceive protective responses as effective, achievable, and acceptable in terms of their associated costs. Considering both appraisal processes may therefore provide a more comprehensive explanation of students' Protective Behaviour than focusing on threat awareness alone.

The framework further contributes by conceptually separating Security Intention from Protective Behaviour. This distinction is relevant because the formation of an intention does not guarantee that the intended behaviour will subsequently occur (Conner & Norman, 2022). Incorporating both constructs provides a theoretical basis for future research to examine not only how protective intentions are formed but also whether and under what conditions those intentions translate into actual cybersecurity practices. This may be particularly important in BYOD environments, where students retain considerable autonomy over day-to-day security decisions concerning their personally owned devices.

Overall, the theoretical value of the proposed framework lies not in introducing new PMT constructs, but in integrating established PMT mechanisms within the specific behavioural context of virus protection in higher education BYOD environments and in explicitly positioning Security Intention as the proposed motivational pathway between cognitive appraisal and Protective Behaviour. The framework therefore provides a basis for subsequent empirical examination of both the proposed relationships and the extent to which Security Intention translates into actual protective action.

### **Practical Implications**

The proposed framework may provide higher education institutions with a behavioural perspective for strengthening cybersecurity practices in BYOD environments. Universities often have limited control over the security configurations and practices applied to personally owned devices, making students' individual security behaviour an important component of BYOD security (Ulven & Wangen, 2021). Previous research has also identified security awareness and policy compliance as important considerations for secure BYOD practices within university environments (Sharfdeen et al., 2025). The framework suggests that cybersecurity initiatives should consider both students' perceptions of virus threats and their evaluations of available protective measures. Awareness programmes may address the potential consequences and likelihood of virus infections while also helping students understand the effectiveness of recommended security practices.

Practical training may help strengthen students' confidence in performing actions such as maintaining security software, applying updates, and responding appropriately to suspicious files or downloads. Self-efficacy has been identified as an important factor in students' information security behaviour (Alam et al., 2025), supporting the importance of developing students' confidence alongside cybersecurity knowledge. Universities may also consider barriers that make protective practices appear inconvenient, difficult, or time-consuming. Reducing unnecessary complexity and providing accessible cybersecurity guidance could make recommended practices easier for students to adopt. These practical implications illustrate how the proposed framework may inform the design of cybersecurity initiatives in higher education BYOD environments, although their effectiveness requires subsequent empirical examination.

### **Future Research**

Future research should empirically validate the proposed framework to determine whether the proposed relationships are supported within higher education BYOD environments. In particular, research should examine the influence of the PMT factors on Security Intention and determine whether Security Intention subsequently contributes to Protective Behaviour. The proposed mediating role of Security Intention also warrants examination because behavioural intention can provide an important link between individuals' evaluations and subsequent behaviour (Conner & Norman, 2022). Such empirical examination would help determine whether Security Intention functions as the proposed motivational mechanism through which threat and coping appraisals are translated into Protective Behaviour.

The framework could also be examined across different universities and student populations. Differences in cybersecurity policies, technological environments, and institutional support may influence how students respond to virus threats. Comparative studies may also help determine whether the relationships proposed in the framework remain consistent across different institutional and student contexts. Longitudinal research would be particularly useful for examining whether Security Intention is subsequently translated into Protective Behaviour and for identifying a possible intention-behaviour gap (Conner & Norman, 2022). In addition, combining self-reported measures with behavioural observations or cybersecurity simulations could provide a more comprehensive assessment of students' actual protective practices. This would help reduce reliance on students' reported intentions and provide a clearer distinction between what students intend to do and the protective actions they actually perform.

### **CONCLUSION**

This conceptual paper addresses the behavioural dimension of virus protection in higher education BYOD environments through the application of Protection Motivation Theory. As students increasingly use personally owned devices for academic activities, their decisions and security practices play an important role in managing the risks associated with virus threats. Understanding the motivational processes underlying these behaviours is therefore important for strengthening cybersecurity in BYOD environments. By incorporating threat appraisal, coping appraisal, Security Intention, and Protective Behaviour within a unified framework, the paper provides a theoretical basis for understanding how students may progress from evaluating cybersecurity risks and protective measures to forming intentions and adopting protective actions. In particular, the framework emphasises that awareness or perception of virus threats alone may not be sufficient to produce Protective Behaviour. Students must also evaluate whether protective responses are effective, whether they are capable of performing them, and whether the associated costs are acceptable.

The framework further conceptualises Security Intention as an intervening motivational mechanism between these cognitive appraisals and Protective Behaviour. This distinction recognises that forming an intention to act and actually performing protective actions are related but conceptually distinct stages of the protective process. Overall, the proposed framework provides a foundation for advancing research on students' responses to virus threats and for informing cybersecurity initiatives within higher education. Its primary contribution lies in providing a process-oriented explanation of how threat and coping appraisals may be translated into Protective Behaviour through Security Intention within the specific context of higher education BYOD. Future empirical examination can further establish its applicability and determine whether the proposed relationships, particularly the mediating role of Security Intention, are supported in practice.

## REFERENCES

- Aguboshim, F. C., Udobi, J. I., & Otuu, O. O. (2023). Security issues associated with Bring Your Own Device (BYOD): A narrative review. *Research Highlights in Science and Technology*, 2, 167–186. <https://doi.org/10.9734/bpi/rhst/v2/19215D>
- Alam, S. S., Ahsan, N., Kokash, H. A., Alam, S., & Ahmed, S. (2025). Students' behaviors in information security: Extension of Protection Motivation Theory (PMT). *Information Security Journal: A Global Perspective*, 34(3), 191–213. <https://doi.org/10.1080/19393555.2024.2408264>
- Alenezi, M. N., Alabdulrazzaq, H., Alshaher, A. A., & Alkharang, M. M. (2020). Evolution of malware threats and techniques: A review. *International Journal of Communication Networks and Information Security*, 12(3), 326–337.
- Alhelaly, Y., Dhillon, G., & Oliveira, T. (2024). Mobile identity protection: The moderation role of self-efficacy. *Australasian Journal of Information Systems*, 28. <https://doi.org/10.3127/ajis.v28.4397>
- Aljuaid, T. A., Abdul Wahab, A. W., & Idris, M. Y. (2023). Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment: State of the art and future directions. *Applied Sciences*, 13(14), 8048. <https://doi.org/10.3390/app13148048>
- Alqahtani, M. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, 12(5), 2589. <https://doi.org/10.3390/app12052589>
- Alqarni, S. (2025). Humans as a weak link to malware distribution. *International Journal of Computer Applications*, 187, 94–99. <https://doi.org/10.5120/ijca2025925564>
- Alrawhani, E. M., Romli, A., & Al-Sharafi, M. A. (2025). Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. *Journal of Open Innovation: Technology, Market, and Complexity*, 11(1), 100463.

- Alexei, A. L., & Alexei, A. (2021). Cyber security threat analysis in higher education institutions as a result of distance learning. *International Journal of Scientific & Technology Research*, 10(3), 128–133.
- Bahashwan, W. S., & Al-Tuwairqi, S. M. (2021). Modeling the effect of external computers and removable devices on a computer network with heterogeneous immunity. *International Journal of Differential Equations*, 2021, Article 6694098. <https://doi.org/10.1155/2021/6694098>
- Calias, S. E., Caoli, B., Padilla, R., Tum-en, J., Bacilio, K. C., Lyn, I., & Guaki, G. S. (2024). The impact of BYOD on network security: A literature review. *Southeast Asian Journal of Science and Technology*, 9(1), 1–8.
- Carter, T., & McNealey, R. L. (2025). Protection motivation and cybersecurity intentions: A visual conjoint experiment. *Journal of Experimental Criminology*. Advance online publication. <https://doi.org/10.1007/s11292-025-09717-1>
- Chilton, D., Wilson, K., & Dutton, J. (2025). A case study of students' and teachers' attitudes towards BYOD and its use within their history classrooms. *Education and Information Technologies*, 30(4), 4795–4824. <https://doi.org/10.1007/s10639-024-13006-1>
- Conner, M., & Norman, P. (2022). Understanding the intention-behavior gap: The role of intention strength. *Frontiers in Psychology*, 13, 923464. <https://doi.org/10.3389/fpsyg.2022.923464>
- Dodge, H. R., Burruss, G. W., Holt, T. J., & Bossler, A. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy*, 22(4), 777–806. <https://doi.org/10.1111/1745-9133.12641>
- Downer, K., & Bhattacharya, M. (2022). BYOD security: A study of human dimensions. *Informatics*, 9(1), 16. <https://doi.org/10.3390/informatics9010016>
- Farooq, A., Ahmad, F., Khadam, N., Lorenz, B., & Isoaho, J. (2020). The impact of perceived security on intention to use e-learning among students. In 2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT) (pp. 360–364). IEEE. <https://doi.org/10.1109/ICALT49669.2020.00115>
- Felicia, F., Noraini, M. Y., & Nurul, H. A. (2022). Worm-based malware threats in network environments. *Research in Management of Technology and Business*, 3(2), 85–86.
- Ferdousi, B. (2022). Cyber security risks of BYOD practice. *International Journal of Research Publication and Reviews*, 3(12), 4554–4558.
- Gundaboina, A. K. (2025). Securing BYOD in education. *Journal of Engineering and Applied Sciences Technology*, 7(4), 1–6.
- Gustara, M., Cahyadi, E. R., & Sartono, B. (2025). Cybersecurity awareness and behavior using PMT. *Indonesian Interdisciplinary Journal of Sharia Economics*, 8(3), 13552–13565.
- Gwenhure, A. K. (2025). University students' security behavior against phishing attacks. *Journal of Cybersecurity*, 11(1).
- Han, M., Zhao, H., Ma, X., & Shi, R. (2025). Influencing factors of information security behavior among college students based on protection motivation theory: Evidence from China. *Frontiers in Public Health*, 13, 1677024. <https://doi.org/10.3389/fpubh.2025.1677024>

- Jansen, J., Van Schaik, P., & Thompson, M. (2020). Protection motivation and cybersecurity behavior: The role of coping appraisal in security compliance intentions. *Computers in Human Behavior*, 105, 106229. <https://doi.org/10.1016/j.chb.2019.106229>
- Jimshith, V. T., & Mary Amala Bai, V. (2024). Evaluation of security framework for BYOD device in cloud environment. *Automatika*, 65(3), 803–814. <https://doi.org/10.1080/00051144.2024.2310458>
- Jones, K. S., Lodinger, N. R., Widlus, B. P., Namin, A. S., Maw, E., & Armstrong, M. (2022). Perceived severity of cyber-attack consequences. *Journal on Multimodal User Interfaces*, 16(4), 399–412.
- Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). PMT-based cybersecurity awareness training. *Computers & Security*, 125, 103049.
- Kiran, U., Khan, N. F., Murtaza, H., Farooq, A., & Pirkkalainen, H. (2025). Modeling cybersecurity behaviors using PMT. *Computers & Security*, 149, 104204.
- Lee, C. G., Yoo, J. W., Park, J. S., Cho, Y., Yoo, J. Y., Kim, S., & Park, H. J. (2024). A study on the effect of social cognitive factors on employees' intention to comply with BYOD security policy. *Journal of Korean Society for Quality Management*, 52(4), 657–674. <https://doi.org/10.7469/JKSQM.2024.52.4.657>
- Li, B. (2022). The application trend and advantages of mobile technology in higher education. *Mobile Information Systems*, 2022, 3874673. <https://doi.org/10.1155/2022/3874673>
- Morwitz, V. G., & Munz, K. P. (2021). Intentions. *Consumer Psychology Review*, 4(1), 26–41. <https://doi.org/10.1002/arc.1061>
- Mou, J., Cohen, J. F., Bhattacharjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems*, 23(1), 196–236. <https://doi.org/10.17705/1jais.00723>
- Ng, K. C., Zhang, X., Thong, J. Y., & Tam, K. Y. (2021). Threats to information security. *Journal of Management Information Systems*, 38(3), 732–764.
- Ntwari, R., Habinka, A. E., & Kagawa, F. (2022). Enhancing BYOD security in education. *Journal of Science & Technology*, 2(4), 1–18.
- Othman, Z., Sepli, M., Mokhtar, U., & Yeop, Y. (2020). BYOD implementation model. *International Journal of Advanced and Applied Sciences*, 7(6), 57–68. <https://doi.org/10.21833/ijaas.2020.06.008>
- Palanisamy, R., Norman, A. A., & Kiah, M. L. M. (2022). BYOD security risks and mitigation strategies: Insights from IT security experts. *Journal of Organizational Computing and Electronic Commerce*.
- Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on cyber security. *International Journal of Scientific Research and Management*, 9(12), 669–710. <https://doi.org/10.18535/ijssrm/v9i12.ec04>
- Ratchford, M., El-Gayar, O. F., Noteboom, C., & Wang, Y. (2022). BYOD security issues: A systematic literature review. *Information Security Journal: A Global Perspective*, 31(3), 253–273. <https://doi.org/10.1080/19393555.2021.1923873>

- Roseline, S. A., & Geetha, S. (2021). A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks. *Computers & Electrical Engineering*, 92, 107143. <https://doi.org/10.1016/j.compeleceng.2021.107143>
- Rosman, M. R. M., Baharuddin, N. S., Alimin, N. A., Rosli, N. N. I. N., Shukry, A. I. M., & Razlan, N. M. (2022). Bring-Your-Own-Device (BYOD) and productivity: A conceptual framework. *Proceedings*, 82(1), Article 10. <https://doi.org/10.3390/proceedings2022082010>
- Saleh, T., Kanaan, R., Alzubaidi, A., Kanaan, S., & Nino, M. (2025). Factors affecting cybersecurity awareness: A qualitative study in Saudi Arabia. *Uncertain Supply Chain Management*, 13(1), 230–238. <https://doi.org/10.5267/j.uscm.2024.12.005>
- Sharfadeen, O. A. A., Norman, A. A., & Ghani, N. A. (2025). BYOD security policy compliance in Malaysian public universities: An integrated PMT–TPB–GDT model with ISA moderation. *Malaysian Journal of Computer Science*, 38(3), 262–286. <https://doi.org/10.22452/mjcs.vol38no3.4>
- Siponen, M., Rönkkö, M., Fufan, L., Haag, S., & Laatikainen, G. (2024). Protection motivation theory in information security behavior research: Reconsidering the fundamentals. *Communications of the Association for Information Systems*, 53, 1136–1165. <https://doi.org/10.17705/1CAIS.05348>
- Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees. *Information*, 13(9), 413.
- Tuah, F. F., & Abd Rahim, N. A. A. (2023). The implementation of Bring Your Own Device (BYOD) at school through Actor-Network Theory (ANT). *International Journal of Academic Research in Progressive Education and Development*, 12(2), 2192–2205. <https://doi.org/10.6007/IJARPED/v12-i2/17434>
- Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), Article 39. <https://doi.org/10.3390/fi13020039>
- van As, J., & Brits, E. K. (2023). Student experiences using BYOD. *MedEdPublish*, 13, 212.
- Vortia, W. (2025). Modelling cybersecurity awareness, perceived threats and secure online behavioral intentions among Ghanaian university students: A PLS-SEM approach. *Magna Scientia Advanced Research and Reviews*, 14(2), 96–111. <https://doi.org/10.30574/msarr.2025.14.2.0094>
- Zayyad, M. A. (2023). Systematic study of computer virus using virus definition and scanning techniques. *Asian Journal of Research in Computer Science*, 16(4), 230–238. <https://doi.org/10.9734/AJRCOS/2023/v16i4385>
- Zhou, G., Gou, M., Gan, Y., & Schwarzer, R. (2020). Risk awareness, self-efficacy, and social support predict secure smartphone usage. *Frontiers in Psychology*, 11, Article 1066. <https://doi.org/10.3389/fpsyg.2020.01066>