Computers in Human Behavior Reports 10 (2023) 100289

Contents lists available at ScienceDirect

Computers in Human Behavior Reports

journal homepage: www.sciencedirect.com/journal/computers-in-human-behavior-reports

# Is the digital security act 2018 sufficient to avoid cyberbullying in Bangladesh? A quantitative study on young women from generation-z of Dhaka city

Arif Mahmud [a], Jannatul Bakia Sweety [b,e], Aftab Hossain [c,f,*], Mohd Heikal Husin [d]

[a] Department of Computer Science and Engineering, Daffodil International University, Bangladesh
[b] School of Humanities, Univerisiti Sains Malaysia, Malaysia
[c] Department of Journalism, Media and Communication, School of Communication, Daffodil International University, Bangladesh
[d] School of Computer Sciences, Universiti Sains Malaysia, Malaysia
[e] Global Research and Marketing, Bangladesh
[f] School of Communication, Universiti Sains Malaysia, Malaysia

ARTICLE INFO

*Keywords:*
Social Media
Cyberbullying
Digital security act 2018
Generation-z
Social networking
TTAT

ABSTRACT

*Purpose:* Cyberbullying has yet to be thoroughly investigated from the perspective of Gen-Z women, and it is vital to determine how this law influences these young women to avoid cyberbullying. Consequently, the purpose of this study is to fill a knowledge vacuum by confirming the technology threat avoidance theory utilizing both adaptive (avoidance motivation) and maladaptive (wishful thinking) approaches.
*Design/methodology/approach:* To gather data from Gen-Z women in Dhaka, we employed a purposive sampling strategy, which yielded 252 valid replies. After that, there were three steps to the evaluation: a measuring model, a structural model, and a mediation analysis.
*Findings:* Seven out of ten hypotheses were found to be significant, with variances of 73.4% and 10.5% for avoidance motivation and wishful thinking, respectively. Furthermore, rather than having a direct influence on coping approaches, the perceived threat had an indirect effect through the mediation effect of perceived avoidability.
*Practical implications:* This study takes into account Gen-Z women's motivation to be protected from cyberbullying, paving the way for the passage of the digital security act 2018. The data also reveal how to teach these young ladies about the threats of cyberbullying and how to defend themselves.
*Originality/value:* This is one of the first studies to look at the factors that influence Gen-Z women's motivation to use the digital security act 2018 to address cyberbullying. In addition, wishful thinking has been newly included as an emotional coping strategy in this context, along with the present avoidance motivation of TTAT.

## 1. Introduction

The massive rise of social networking sites (i.e. Facebook, Whatsapp, Twitter, Messenger, etc.) has altered a range of human interaction sectors in today's society (Jain & Agrawal, 2020). Such socialization also creates an environment that is favorable to unpleasant behaviors, one of which is cyberbullying or cyber harassment. This cyberbullying is becoming increasingly prevalent throughout the world. On the other side, distress, melancholy, social anxiety, phobic anxiety, paranoia, low self-esteem, and suicidal thoughts are identified as negative consequences of cyberbullying (Uddin et al., 2019). Due to the growing use of social media, cyberbullying is more widespread among school-aged children and teenagers. Notably, the cyberbullying victimization among this age group varies from 4.8% to 55.3% in different countries (Mallik, 2020). In addition, the percentages of parents who consider their child to be a victim of cyberbullying from 2011 to 2018 in various countries are shown in Table 1.

In Bangladesh, people of all ages are using the internet on their cell phones and other communication devices. In 2021, the total number of internet subscribers reached 126.60 million ("Internet Subscribers," 2021). Social media, such as Facebook, has grown in popularity in Bangladesh in the previous decade. According to a recent survey, Dhaka,

* Corresponding author. Department of Journalism, Media and Communication, School of Communication, Daffodil International University, Bangladesh.
*E-mail address:* aftab.hossain@gmail.com (A. Hossain).

https://doi.org/10.1016/j.chbr.2023.100289
Received 10 July 2022; Received in revised form 1 April 2023; Accepted 15 April 2023
Available online 3 May 2023

**Table 1**
Reported cases of cyberbullying (Dhiraj, 2018).

| No | Country | 2018 | 2016 | 2011 |
|---|---|---|---|---|
| 1 | India | 37 | 32 | 32 |
| 2 | Brazil | 29 | 19 | 20 |
| 3 | United States | 26 | 34 | 15 |
| 4 | Belgium | 25 | 13 | 12 |
| 5 | South Africa | 26 | 25 | 10 |
| 6 | Sweden | 23 | 20 | 14 |
| 7 | Canada | 20 | 17 | 18 |
| 8 | Turkey | 20 | 14 | 5 |
| 9 | Saudi Arabia | 19 | 17 | 18 |
| 10 | Australia | 19 | 20 | 13 |

the capital, has more than 22 million active Facebook users in 2017, placing it second among cities globally ("Star online report, " 2017). Besides, Bangladesh's social network is made up of friendship connections, neighboring ties, coworkers, group members, and other forms of relationships. Furthermore, as per Sarker and Shahid (2018), young people use the internet in most cases. Hence, young people's online safety has become a major worry in this country.

Teenagers' bullying experiences are evolving globally as well in Bangladesh. Initially, bullying events were restricted to the schoolyard and concluded at the end of the school day. However, face-to-face bullying has developed a new online form (Betts et al., 2017). Most importantly, young women are more likely to report this issue than young boys worldwide (Cénat et al., 2014). Similarly, Bangladesh has a high prevalence of cyberbullying, with 80% of victims being women between the ages of 14 and 22, commonly known as Generation Z (Gen-Z). This generation resembles youth born after 1997 in particular (Cheung et al., 2020). On the other hand, youth should be between the ages of 15 and 24 ("Youth and the 2030 Agenda," 2018). They are an easy target for crooks, as reported by Wachs et al. (2016). These ladies are usually targeted by stealing their personal information when they get engaged in an uncomfortable relationship, or sometimes for no other justification than the bully's motives. This conduct is extremely dangerous for the victim's psychological well-being, and it can even lead to commiting suicide (Mansbach-Kleinfeld et al., 2015). Simona et al. (2016) further added that these victims experience psychological and social dysfunction as a result of cyberbullying. We were therefore really motivated to assess this Bangladeshi Gen-Z woman's (who were 15–24 years of age) use of the Digital Security Act 2018 to combat cyberbullying.

The policy for cyberbullying varies by country's legislation and comes in a variety of legal packages. Even so, it appears that in some nations, a legal process is a generic approach, while in others; it is categorical in terms of age. In Bangladesh, the policy is applied uniformly regardless of age or employment. Despite the growing global acknowledgment of cyberbullying, Bangladesh's lack of proper legislation has remained a significant obstacle (Hossain et al., 2022) Furthermore, cyberbullying is seen as a form of cybercrime rather than a particular offense. Some aspects of cyberbullying are covered by the ICT Act 2006, the Pornography Control Act 2012, and the Digital Security Act 2018, but not all. The government of Bangladesh enacted the Digital Security Act 2018 after amending the ICT Act 2006; section 57 (Sohel, 2018). Bangladesh's parliament passed the Digital Security Act in late 2018 in response to sectarian violence sparked by Facebook postings (Sabera, 2021). Those, who break the law, face steep fines and lengthy jail terms. Moreover, this legislation allows for arrests without a warrant (Frontline Defenders, 2020). Our decision to analyze this law against cyberbullying was therefore driven by the trade-off between usefulness and controversy.

The acts were criticized by civil societies and media experts since the law was less concerned about the violation of the security of the citizens rather than protecting the image of the government and its related institutions (Babu & Ullah, 2021; Riaz & Zaman, 2022). If someone posts anything that harms the image of the government, can be sent to jail for up to 14 years with/without BDT 1 crore (10 million) fine (Bangladesh Computer Council, 2019). The legislation was initiated with less support for the citizens and their rights. However, there were several cases found where people reported online harassment and abuse (Mogumder, 2022; The Business Standard, 2022). On the other hand, according to Bari and Dey (2019), some misuse of this law was also found. But, as the women and young people of Bangladesh are at a higher risk zone of getting cyberbullied, the uses and actions of these laws came into action on several occasions. In essence, two factors motivated us to conduct this research. First off, the young women of Dhaka will gain a lot and be better equipped to use social media. Finally, young women's evaluation of the Digital Security Act 2018 can assist the government in taking the appropriate action to lessen the dispute.

Cyberbullying has not been well studied in Bangladesh. Nonetheless, 49% of Bangladeshi schoolchildren report experiencing cyberbullying, with women being the majority of victims. Moreover, these bullying events resulted in the deaths of some teenage girls (Chowdhury, 2020; Fakir, 2023; Smriti & Nahar, 2019). Therefore, this study is essential for educating young women against cyberbullying when they use online social media. In addition, Gen-Z women can understand the effects of cyberbullying and how to protect themselves rather than ignoring the problem. Moreover, the study reports the negative effects of cyberbullying and offers an analysis of Bangladesh's legal system for preventing such disasters. Besides, this study expands the behavioral intents of young users to defend themselves against online bullying, enabling the application of the digital security act 2018. The findings provide practitioners with information on how to warn social networking users about the risks of cyberbullying and how to defend themselves against it. Hence, it is anticipated that this study will have a significant impact on reducing the cyberbullying phenomenon in the Dhaka city and that young women would greatly benefit from the ability to utilize social media in a positive way.

Moreover, it is crucial to choose the right theory to comprehend how systems are adopted and used (Monni & Sultana, 2016). Thereby, the technology threat avoidance theory (TTAT), presented by Liang and Xue (2009), was chosen since it is comparable to the protection motivation theory but more suited to IT-related fields (Boysen et al., 2019). Individuals' IT threat avoidance motivation is driven by a perceived threat and perceived avoidability, as per TTAT (Liang & Xue, 2009). The perceived threat, on the contrary, is determined by perceived severity and susceptibility, whereas avoidability is impacted by safeguard effectiveness, safeguard cost, and self-efficacy (Arachchilage & Love, 2014). Importantly, because many users depend extensively on wishful thinking to decrease the emotional impact of the threat, it also can be integrated into the model. Furthermore, perceived avoidability might act as a mediator between the relationship between perceived threat and coping strategies. Thereupon, the following are the research objectives (RO) of this research.

- RO1: To test the impact of the perceived threat and perceived avoidability on the coping approaches (avoidance motivation and wishful thinking)
- RO2: To test the impact of perceived susceptibility and perceived severity on the perceived threat
- RO3: To test the impact of perceived effectiveness, perceived cost, self-efficacy, and perceived threat on the perceived avoidability
- RO4: To test the mediation impact of the perceived avoidability between the relationship of the perceived threat and coping approaches (avoidance motivation and wishful thinking)

The following is how the rest of the paper is organized: The second section would provide a quick overview of TTAT's key information and contributions to its domain. Following the establishment of hypotheses, section 3 would present a conceptual model. The methodology of the investigation will be discussed in Section 4. Section 5 would

subsequently be devoted to the outcomes analysis. The discussion, conclusion, contribution, limitations as well as the study's recommendations for further research, would be included in the last sections (6, 7, 8, and 9).

## 2. Background

Liang and Xue (2010) introduced the TTAT to describe people's security actions in terms of incentives to avoid threats. Besides, vulnerability and severity of technological risks influence their desire and action to avoid them, according to (TTAT) (see Fig. 1). TTAT may also be used to look into how people employ preventive methods to keep themselves safe. The core idea behind TTAT is that users can only be motivated to actively avoid danger after going through two cognitive processes, namely threat appraisal and coping appraisal (Liang & Xue, 2009). Users will evaluate the threat appraisal (perceived threat) and determine their level of preparedness for the threat while making a choice (perceived avoidability). Users will utilize problem-focused coping (avoidance motivation) when they believe a threat is preventable and will take precautions to do so. Users will engage in emotional-focused coping (wishful thinking) if they believe that a threat cannot be avoided by using a precaution (Butler & Butler, 2021). It is impossible to explore all forms of emotion-focused coping in a single research due to their multidimensional and complex character. Wishful thinking should be taken into consideration as an emotion-focused coping strategy while examining a particular coping strategy, according to Chen and Liang (2019). On the other hand, wishful thinking is seen as maladaptive behavior according to Marett et al. (2019), expressing feelings of powerlessness and continuing to act in a harmful manner. To the best of our knowledge, this is one of the first studies to take into account wishful thinking as a form of coping in the context of cyberbullying.

The degree to which a user interprets a threat as harmful is known as a "perceived threat" (Zheng et al., 2022). Within the cyberbullying context, it is defined as the degree to which an individual considers cyberbullying to be hazardous (Liang & Xue, 2009). Two factors, namely perceived susceptibility and perceived severity, influence this perception (Liang & Xue, 2010). Perceived susceptibility refers to the probability that cyberbullying will result in unfavorable effects for the individual (Liang & Xue, 2009). This is the estimation of the likelihood of a security breach (Wynn et al., 2013). On the other hand, perceived severity is the amount of harm caused by cyberbullying to the individual (Liang & Xue, 2009). This evaluation of unfavorable effects is connected to a certain incident. This evaluation considers potential psychological, social, economic and technological effects (Wynn et al., 2013).

However, Liang and Xue (2010) discovered that the interaction between severity and susceptibility was not relevant in the threat-appraisal process. They observed that both severity and susceptibility were significant in shaping threat perceptions. Manzano (2012) and Young et al. (2016) provide support for this finding. On the flip side, as per Young et al. (2016), while severity was strongly associated with threat, neither susceptibility nor the interaction of severity and susceptibility to the threat was significant. However, as followed by Chen and Liang (2019), this study considered perceived threat and safeguard effectiveness as a part of two different cognitive procedures named threat and coping appraisal. Therefore, the interaction between these variables was not considered in this study. Finally, due to the non-significant contribution, in several studies the interaction between severity-susceptibility and threat-effectiveness was not included (Boysen et al., 2019; Butler & Butler, 2021; Chen & Liang, 2019). On the other hand, Carpenter et al. (2019) redefined TTAT where interaction term has been excluded. Due to above mentioned reasons, this study has considered the following TTAT model as proposed by Hewitt et al. (2017) that measured the security behavior of the students. Interestingly, Hewitt et al. (2017) only took into account the significant connections in their suggested model while adapting the TTAT from Liang and Xue (2010).

Copying appraisal, which is also known as perceived avoidability, is determined by three constructs such as safeguard effectiveness, safeguard cost, and self-efficacy (Liang & Xue, 2010). First, safeguard effectiveness is described as an individual's belief that the digital security act 2018 will genuinely safeguard the individual (Liang & Xue, 2009). This is the individual assessment regarding how effectively the digital security act 2018 can be applied to avoid cyberbullying. Second, safeguard cost is defined as the financial and time repercussions of enacting the digital security act 2018 on individuals. This variable also relates to mental and physical exertion, including the time, expense, annoyance, and awareness needed to use the safety precaution (Choi et al., 2022). Finally, self-efficacy is described as an individual's belief in their ability to use the digital security act 2018 (Liang & Xue, 2009).

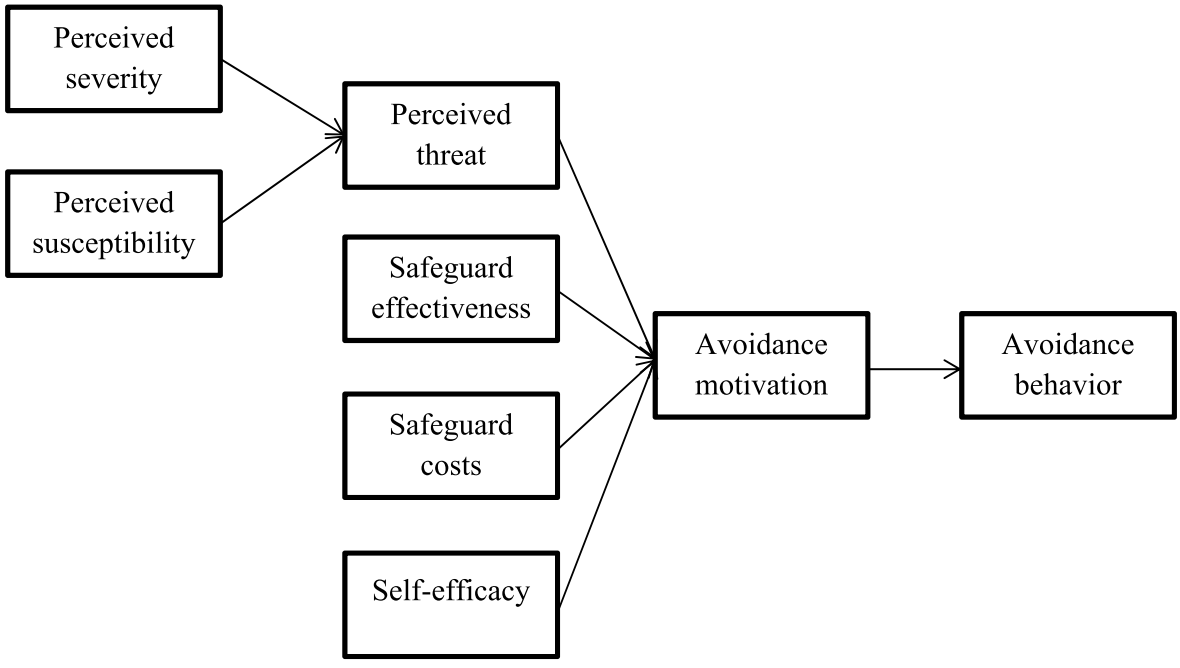


**Fig. 1.** TTAT model (Hewitt et al., 2017).

In most cases, users select the procedure to avoid the threat by engaging in problem- and emotion-focused coping because of the perceived threat and perceived avoidability (Liang & Xue, 2009). An adaptive behavior that employs a problem-solving strategy in an effort to alter the objective reality is referred to as problem-focused coping. By employing protective measures, it deals with the threat at its root. Emotion-focused coping, on the other hand, aims to distort the environment's reality (Chen & Liang, 2019). In any case, avoidance motivation is a form of problem-based coping. The result of this evaluation process can affect the person's decision to take actions that are specially designed to assist them to avoid cyberbullying (Butler & Butler, 2021). Avoidance motivation is defined as the degree to which individuals are driven to follow the digital security act 2018. The behavioral intention to employ the safeguard can be used to express this variable in essence. According to our argument, users are more likely to utilize the safeguard as a preventative measure if their avoidance motivation is higher, which is consistent with earlier studies (Liang & Xue, 2010).

In addition, due to the following reasons, avoidance behavior was not taken into account in this study. First of all, the digital security act 2018 is one of the newest legislation, and the majority of the individuals have not yet begun using it. Second, Chen and Liang (2019) recommended employing wishful thinking and avoidance motivation as coping mechanisms. Lastly, the use of the digital security act 2018 is entirely voluntary. Consequently, rather than focusing on avoidance behavior, it is feasible to evaluate avoidance motivation and wishful thinking. Users are permitted to utilize wishful thinking in the context of cyberbullying than they are in the mandated setting when problem-focused safeguarding is necessary. In order to obtain a holistic picture of users' coping behavior, Chen and Liang (2019) contend that it is crucial to take into account both problem and emotion-focused strategies while using TTAT.

Emotion-focused coping aims to alleviate or manage the emotional suffering in a dangerous circumstance (Nabi et al., 2022). This approach, on the other side, does not modify the issue itself; rather, it modifies one's experience of the situation (Beaudry & Pinsonneault, 2005). Wishful thinking, an example of emotion-based coping, is a technique of escaping a stressful circumstance by dreaming that some intervening act or force would turn things around in the desired manner (Folkman et al., 1986; Mogaji, 2022). It may also be defined as the formation of views based on what is pleasurable to envision rather than what is supported by facts or reality (Chen & Liang, 2019). Anyhow, Hunter et al. (2007) found that victims reported more wishful thinking than peers who were not bullied. Moreover, wishful thinking, denial, acceptance, self-blame, and self-isolation, are the common types of emotion-focused coping (Carver et al., 1989; Folkman & Lazarus, 1985). Importantly, wishful thinking is considered one of the most prevalent kinds of emotion-focused coping when compared to other types (Folkman & Lazarus, 1985; Križan & Windschitl, 2007). This strategy is the most popular justification for consumers to ignore an IT danger which was also validated by Microsoft Security Intelligence (Chen & Liang, 2019). The Gen-Z women of Dhaka city are projected to be too optimistic and wishfully believe that they are protected from cyberbullying on online social media, which is similar to the scenario as stated by Liang et al. (2019). Wishful thinking is a significant type of emotion-focused coping behavior that is understudied, according to Chen and Liang (2019). Wishful thinking can therefore bring important knowledge to the body of knowledge. As a result, the current study looks at users' wishful thinking as an example of emotion-focused coping.

Pursuant to Liang and Xue (2010), both susceptibility and severity had a direct effect on avoidance motivation. Nevertheless, when we looked at other studies, the correlations between susceptibility, severity, and threat perceptions appeared to be non-consistent (Vance et al., 2014; Manzano, 2012). As stated by Chen and Liang (2019), the perceived threat was influenced by severity, susceptibility, and perceived avoidability by effectiveness and self-efficacy but not by perceived cost. Finally, as per Young et al. (2016), while severity was strongly associated with threat, neither susceptibility nor the interaction of severity and susceptibility to the threat was significant. Hence, it would be interesting to evaluate the behavior of these variables from the context of our study. Some of the recent quantitative studies that have used TTAT have been listed in Table 2.

This study adds to the body of knowledge by filling up the following critical gaps. First, cyberbullying has not yet been properly studied from Bangladesh's perspective. Besides, the digital security act 2018 has just been enacted in order to defend such an approach. That's why it's easy to see why there hasn't been much done to defend cyberbullying concerns under this provision. Furthermore, Gen-Z women are the most vulnerable to internet harassment (Hossen, 2021). Regrettably, research on this group has been lacking. On the other hand, the TTAT model was primarily utilized to build adaptive techniques. As a consequence, it may be necessary to investigate a new study route that incorporates negative (maladaptive) techniques, such as wishful thinking. Therefore, there are certain research gaps in this area that we must address.

## 3. Hypotheses and model development

### 3.1. Perceived susceptibility to the perceived threat

As stated by Arachchilage et al. (2016), susceptibility to phishing grew through the mobile game prototype, where participants saw phishing as a dangerous threat. Similarly, being vulnerable to malicious IT attacks had a positive influence on the perception of malware threats. Indeed, two antecedents, vulnerability and severity combine to create the appearance of a threat (Young et al., 2016). Importantly, this threat was positively influenced by perceived susceptibility in several studies like phishing avoidance (Arachchilage & Love, 2014), mobile operating systems (Butler & Butler, 2021), and healthcare (Samhan, 2017). So, we can form the following hypothesis based on the foregoing discussion.

**H1**. Perceived susceptibility has a positive impact on the perceived threat.

### 3.2. Perceived severity to the perceived threat

As claimed by Boysen et al. (2019), an individual must measure the severity of threat perceptions from the outset because the potential threat might grow afterward. Mwagwabi et al. (2014) came to the same result where password-related threats were judged to be significant. This threat was affected favorably by severity in numerous studies like phishing avoidance (Arachchilage & Love, 2014), threat calculus (Boysen et al., 2019), and malware avoidance (Young et al., 2016). As a result, we may project the following hypothesis.

**H2**. Perceived severity has a positive impact on the perceived threat

### 3.3. Perceived effectiveness to perceived avoidability

The individual's belief in the effectiveness of safety protection is a significant factor in choosing the avoidability method to deal with the threat (Arachchilage & Love, 2014). Carpenter et al. (2019) found that safeguarding effectiveness had the most favorable effect on the incentive for avoidability. Furthermore, it is unlikely to be applied if consumers do not consider avoidability as a useful defense against computer viruses (Boysen et al., 2019). It's worth noting that when an effective safeguards solution was established, avoidability might lead to avoidance motivation (Liang & Xue, 2009). With the help of the above discussion, the following hypothesis can be expected.

**H3**. Perceived effectiveness has a positive impact on perceived avoidability

**Table 2**
Some recent applications of TTAT.

| SL | References | Year | Journal/Conference Name | Country | Sample | Sample size | #of citation | Application |
|---|---|---|---|---|---|---|---|---|
| 1 | Aribake and Aji (2020) | 2020 | Journal of Computer Engineering and Technology | Nigeria | Nigerian Internet Banking users | 280 | 5 | Phishing avoidance behavior |
| 2 | Gillam and Foster (2020) | 2020 | Computers in Human Behavior | US | Working adults | 184 | 7 | Cyber security behaviors |
| 3 | Chen and Liang (2019) | 2019 | IEEE transactions on engineering management | US | Business students | 207 | 7 | IT Threat Avoidance |
| 4 | Dodel and Mesch (2019). | 2019 | Computers & Security | Israel and Uruguay | Israeli Internet users | 1850 | 14 | Cyber-safety behaviors |
| 5 | Liu et al. (2020) | 2020 | International Journal of Information Management | China | Chinese government employees | 235 | 18 | Information security policy |
| 6 | Alomar et al. (2019) | 2019 | Computers & Security | Saudi Arabia | Crowd workers | 882 | 4 | Unsafe computing behaviors |
| 7 | Cho and Ip (2018) | 2018 | Enterprise Information Systems | Hong Kong | Employees | 450 | 19 | BYOD adoption security policy |
| 8 | Samhan (2017) | 2017 | 8th International Conference on Information and Communication Systems | US | Healthcare Providers | 1224 | 9 | Security Behaviors |
| 9 | Cao et al. (2021) | 2021 | Technovation | UK and UAE | UK business managers | 269 | 8 | AI in decision making |
| 10 | Jain and Agrawal (2020) | 2020 | Indian Growth and Development Review | India | Social media users | 365 | 4 | Cyberbullying |
| 11 | Kim et al. (2018) | 2018 | National Cyber Summit Research Track | US | Undergraduate and graduate students | 224 | 1 | Secure Intention |

### *3.4. Perceived cost to perceived avoidability*

Individuals must evaluate the financial or intellectual costs which have an influence on their productivity. Users may be less likely to pursue avoidability approaches that require an inordinate amount of time, effort, or money (Boysen et al., 2019). A previous IT security study discovered that network security costs significantly reduced the likelihood of customers adopting home wireless network security (Arachchilage et al., 2016). In the case of an IT threat, the perceived cost might have a negative impact on perceived avoidability (Chen & Liang, 2019; Liang & Xue, 2009). Accordingly, the following hypothesis can be put forth.

**H4**. Perceived cost has a negative impact on perceived avoidability.

### *3.5. Self-efficacy to perceived avoidability*

Users must assess their efficacy in order to determine their motivation for avoiding detrimental IT risks (Boysen et al., 2019). Individuals with greater efficacies were more motivated to perform IT-related acts favorably, according to Arachchilage and Love (2014). Furthermore, in order to reduce phishing threats, Arachchilage et al. (2016) added self-efficacy to the framework for game design. In essence, self-efficacy was found to have a positive impact on the perceived avoidability of IT threats (Chen & Liang, 2019; Liang & Xue, 2009). As a consequence, we may form the following hypothesis.

**H5**. Self-efficacy has a positive impact on perceived avoidability

Perceived threat to perceived avoidability:

The belief that a security risk may be efficiently avoided by a person is seen as avoidable (Liang & Xue, 2009). When individuals understand that malware poses a threat to their personal and professional lives, they rely on a combination of cognitive and behavioral approaches to address possible problems (Liang & Xue, 2009). In view of this, the degree of threat must be increased to improve avoidability. Furthermore, both of these characteristics were connected where threats occurred before avoidability (Chen & Liang, 2019). In that case, the following hypothesis can be proposed.

**H6**. Perceived threat has a positive impact on perceived avoidability.

### *3.6. Perceived threat to avoidance motivation*

The perceived threat is a determinant of avoidance motivation as per TTAT. When perceived threats rise, end-users take a certain degree of security (Chen & Liang, 2019). Therefore, avoidance motivation increases with the escalation of the threat. Many studies had empirically examined the correlation between perceived threat and avoidance motivation. We can take threat calculus (Boysen et al., 2019), phishing threats (Arachchilage et al., 2016), and mobile operating systems (Butler & Butler, 2021) for example. As a consequence, the following hypothesis may be formed.

**H7**. Perceived threat has a positive impact on avoidance motivation

### *3.7. Perceived threat to wishful thinking*

If computer users perceive a high level of IT threat, they might become more emotionally worried. In these circumstances, people are more likely to take a firm stance in favor of wishful thinking (Beaudry & Pinsonneault, 2005). Individuals, who considered malevolent IT as a danger, were driven to apply emotional coping strategies (Liang & Xue, 2009). Furthermore, the bigger the perceived malware threat, the greater the desire to be protected. On that ground, people were more inclined to engage in wishful thinking under such circumstances (Chen & Liang, 2019). Based on the above discussion, we may construct the following hypothesis.

**H8**. Perceived threat has a positive impact on wishful thinking.

### *3.8. Perceived avoidability to avoidance motivation*

The perception of avoidability increases the desire to take preventative security measures (Wynn et al., 2013). Indeed, the combination of perceived avoidability and perceived threat had an impact on avoidance motivation (Liang et al., 2019). Furthermore, since avoidability offers a sense of control, users are more likely to apply avoidance motivation, and these two are positively related (Chen & Liang, 2019). As such, we may make the following prediction.

**H9**. Perceived avoidability has a positive impact on avoidance motivation.

### 3.9. Perceived avoidability to wishful thinking

When an individual's ability to avoid malware is high, one is less concerned about the chance of being a malware victim. In such a circumstance, wishful thinking is more likely to prevail (Chen & Liang, 2019). Individuals who believe an IT threat is preventable, in contrast, are driven to take precautions and are more likely to engage in wishful thinking (Liang & Xue, 2009). Consequently, people were more inclined to participate in wishful thinking if they had more trust in avoidability. As a consequence, we can suggest the following hypothesis.

**H10**. Perceived avoidability has a positive impact on wishful thinking

The suggested research model for this study is shown in Fig. 2. It is designed based on past research with the goal of filling the research gaps. It affirms that avoidance motivation (AM) and wishful thinking (WT) are determined by the perceived threat (PT) and perceived avoidability (PA). Besides, the perceived threat is predicted by perceived susceptibility (PSU) and perceived severity (PS). On the other hand, perceived effectiveness (PEF), perceived cost (PC), self-efficacy (SE), and perceived threat perform as the determinants of perceived avoidability. In addition, perceived avoidability performs as a mediator between perceived threat and coping modes (avoidance motivation and wishful thinking). The results of the two evaluation processes, perceived threat and perceived avoidability, have often been viewed as static and independent, which is a weakness of the previous TTAT-supported studies (Liang & Xue, 2010). Moreover, Chen and Liang (2019) contend that human coping and assessment are context-dependent and dynamic. So, it is still unclear how these two variables are related. Therefore, the mediation effect of perceived avoidability can better explain the dynamic relationship between these variables and the outcome variables (Avoidance motivation and wishful thinking) as well.

This study has followed Chen and Liang (2019) from the naming of variables perspective where Chen and Liang (2019) used the terms perceived effectiveness and safeguard effectiveness along with perceived cost and safeguard cost as synonymous and interchangeably.

## 4. Methodology

The proposed TTAT model's instruments were adapted from previous research. Minor adjustments were made to the components to ensure that they fit inside the structure. Perceived susceptibility (4 items), perceived effectiveness (4 items), perceived cost (4 items), self-efficacy (3 items), and avoidance motivation (3 items) were adapted from Chen and Liang (2019). In addition, Liang et al. (2019) were followed to determine perceived avoidability (3 items), perceived threat (3 items), wishful thinking (4 items), and Bax et al. (2021) for perceived severity (6 items). Furthermore, we employed a 7-point Likert scale (from strongly agree to strongly disagree) in self-administered, quantitative, and cross-sectional surveys. We also conducted a pre-test (7 people) and a pilot survey (32 people) on the selected respondents to ensure that the modified instruments were valid and trustworthy. The participants double-checked the items' wording and length during the pre-test. Following that, the modified questionnaire was delivered to participants during the pilot survey. However, two items from perceived severity were removed during the pilot survey because of a low factor loading score. The remaining 32 items achieved a satisfactory level of internal consistency, indicator validity, indicator reliability, convergent validity, and discriminant reliability. The following were the 32 items that were utilized in the final survey (see Table 3).

Non-probabilistic sampling does not rely on a sample frame and depends on the researchers' opinions (Sharma, 2017). So, this method was chosen for this research over probabilistic sampling Purposive sampling, which does not need theories or a set number of participants, was used in this study as an example of non-probabilistic sampling. Additionally, this strategy involves only competent and knowledgeable individuals (Etikan, 2016). Data were collected from those who fulfilled the following criteria.

1. Women
2. 15–24 years old
3. Resident of Dhaka city
4. Online social media user
5. Aware of the digital security act 2018

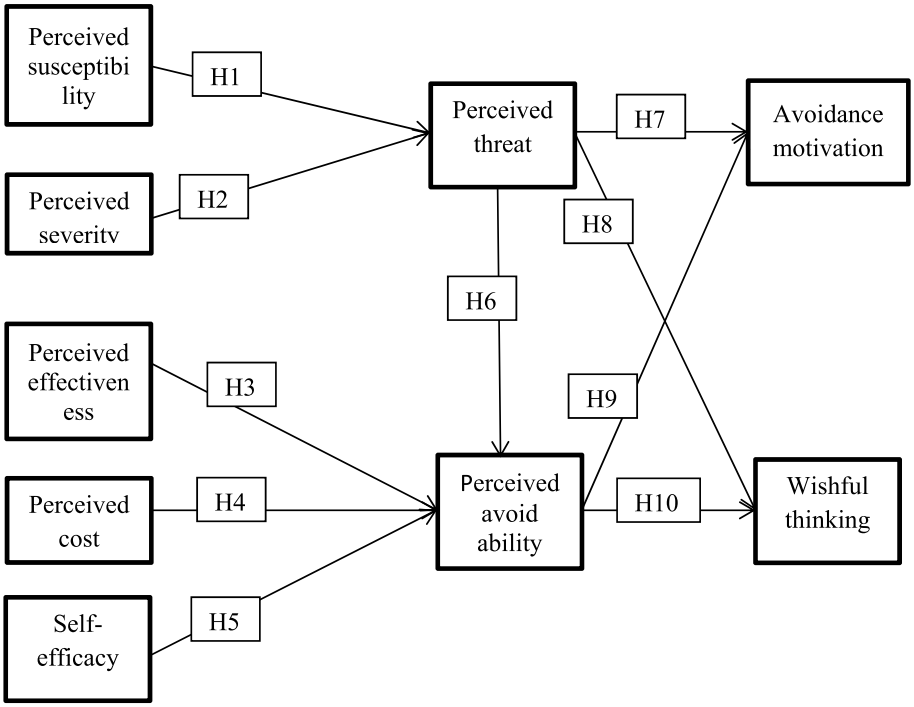


**Fig. 2.** Proposed conceptual model.

**Table 3**
Adapted items.

| Variables | Code | Items | Source |
|---|---|---|---|
| Perceived severity | PS1 | Becoming a victim of cyberbullying on online social media is a serious problem for me | Bax et al. (2021) |
| | PS2 | Becoming a victim of cyberbullying on online social media would have serious consequences for me | |
| | PS3 | Becoming a victim of cyberbullying on online social media can cause my whole life to change | |
| | PS4 | If I were to become a victim of cyberbullying on online social media, I would suffer a lot of mental anguish | |
| Perceived susceptibility | PSU1 | It is very likely that cyberbullying will happen to me on online social media. | Chen and Liang (2019) |
| | PSU2 | I will be affected by cyberbullying on online social media in the near future. | |
| | PSU3 | Cyberbullying on online social media will attack me in the near future. | |
| | PSU4 | Cyberbullying on online social media will cause negative consequences to me in the near future. | |
| Perceived effectiveness | PEF1 | The digital security act 2018 available to me can prevent major problems caused by cyberbullying on online social media. | |
| | PEF2 | The digital security act 2018 available to me is effective in reducing the negative consequences of cyberbullying on online social media. | |
| | PEF3 | The digital security act 2018 available to me is helpful with detecting possible cyberbullying on online social media. | |
| | PEF4 | The digital security act 2018 available to me can reduce the harm caused by cyberbullying on online social media. | |
| Perceived cost | PC1 | There are too many overheads associated with the digital security act 2018 for cyberbullying on online social media. | |
| | PC2 | It requires considerable efforts to counteract cyberbullying on online social media using the digital security act 2018 | |
| | PC3 | It is time-consuming to implement the digital security act 2018 to cope with cyberbullying on online social media. | |
| | PC4 | Trying to avoid cyberbullying on online social media using the digital security act 2018 is too much troublesome | |
| Self-efficacy | SE1 | I am confident that I can implement the digital security act 2018 as a countermeasure for cyberbullying on online social media. | |
| | SE2 | I believe I am able to use the digital security act 2018 as a countermeasure for cyberbullying on online social media. | |
| | SE3 | I have confidence in my ability to apply the digital security act 2018 as countermeasures for cyberbullying on online social media. | |
| Avoidance motivation | AM1 | I can avoid cyberbullying on online social media by using the digital security act 2018. | |
| | AM2 | I can protect myself from cyberbullying on online social media by using the digital security act 2018. | |
| | AM3 | I am motivated to counteract cyberbullying on online social media by taking effective means, i.e., the digital security act 2018. | |
| Perceived avoidability | PA1 | Taking digital security act 2018 into consideration, cyberbullying on online social media can be prevented | Liang et al. (2019) |
| | PA2 | Taking the digital security act 2018 into consideration, I can protect myself from cyberbullying on online social media | |
| | PA3 | Taking digital security act 2018 into consideration, cyberbullying on online social media is avoidable | |
| Perceived threat | PT1 | The hateful nature of the cyberbullying on online social media threatens me | |
| | PT2 | The threat of cyberbullying on online social media is fearful | |
| | PT3 | The threat of cyberbullying on online social media makes me anxious | |
| Wishful thinking | WT1 | I fantasize that cyberbullying on online social media will go away or somehow be over with. | |
| | WT2 | I fantasize that I will somehow come across a magical solution for cyberbullying on online social media. | |
| | WT3 | I fantasize that all of a sudden cyberbullying on online social media disappears by itself. | |
| | WT4 | I fantasize that cyberbullying on online social media turns out just fine as if nothing happened. | |

Due to the epidemic in Dhaka, data was collected using an online survey (Google Form) from August 20 to November 15, 2021. Questionnaires were sent by e-mail, Messenger, and WhatsApp, among other online ways. On the flip side, reliability, effect size, and indicator number must all be taken into account when choosing the sample size, according to Henseler et al. (2009). In addition, the power level supplied in the a priori data analysis may be used to estimate the sample size (Cohen, 1988). Therefore, the sample size was determined using the G*power 3.1 tool which provides an efficient way to analyze predictive power before the study is actually conducted. Additionally, it is advised to incorporate G*power into structural equation modeling's partial least square approach (Ringle et al., 2014). Notably, even with extremely complicated models, PLS-SEM may be applied with substantially smaller sample sets. Therefore, the minimum number of samples was calculated as 129. In any case, 271 persons attempted to complete the survey, but only 252 copies were finished successfully, resulting in a 92.98% response rate. They were mostly between the ages of 21 and 22 (56.74%). In addition, virtually all of the participants were students with a bachelor's degree or a comparable academic level. Furthermore, the ratio of unmarried to married people was roughly 9:1. Finally, the majority of respondents had 2–5 years of online social media experience; with the majority of them being heavy users (see Table 4).

## 5. Results

The demographic data and preliminary findings were analyzed using SPSS v26. Besides, the common method variance (CMV) was also calculated using Harman single factor, yielding a result of about 35.9%. So, there was no evidence of a CMV problem. It is worth noting that CMV occurs when a single item accounts for more than half of the item covariance (50%) (Podsakoff & Organ, 1986). Nonetheless, in the online survey, all questions had to be answered. As a consequence, missing values were not an issue in this study. Our suggested TTAT was further put to the test using partial least squares of structural equation modeling. Additionally, the data from our model was evaluated using the SmartPLS 3.3.3 program, which is widely used by researchers (Wong, 2013). This evaluation technique was broken down into three parts: verification of the measurement model, structural model, and mediation analysis.

Table 5 shows the outcomes of four measurement model parts. First and foremost, factor loading is a metric that assesses the strength of a link between two or more components (Yong & Pearce, 2013). Second,

**Table 4**
Demographic characteristics.

| Area | Grouping | Occurrence | Percentage |
|---|---|---|---|
| Age | 15 years | 3 | 1.19 |
| | 16 years | 4 | 1.59 |
| | 17 years | 3 | 1.19 |
| | 18 years | 9 | 3.57 |
| | 19 years | 22 | 8.73 |
| | 20 years | 28 | 11.11 |
| | 21 years | 75 | 29.76 |
| | 22 years | 68 | 26.98 |
| | 23 years | 17 | 6.75 |
| | 24 years | 23 | 9.13 |
| Highest academic qualification | No recognized academic degree | 1 | 0.40 |
| | SSC or equivalent | 10 | 3.97 |
| | HSC or equivalent | 49 | 19.44 |
| | Diploma or equivalent | 3 | 1.19 |
| | Bachelor or equivalent | 175 | 69.44 |
| | Masters or equivalent | 9 | 3.57 |
| | PhD or equivalent | 0 | 0.00 |
| | Post Doctorate or equivalent | 0 | 0.00 |
| | Others | 5 | 1.98 |
| Marital status | Single | 227 | 90.08 |
| | Married | 25 | 9.92 |
| Occupation | Don't work | 17 | 6.75 |
| | Public sector | 1 | 0.40 |
| | Private sector | 6 | 2.38 |
| | Student | 220 | 87.30 |
| | Business | 2 | 0.79 |
| | Freelancing | 2 | 0.79 |
| | Others | 4 | 1.59 |
| Online social media usage Experience | Less than 1 year | 6 | 2.38 |
| | 1–2 years | 38 | 15.08 |
| | 2–5 years | 132 | 52.38 |
| | 5–10 years | 68 | 26.98 |
| | More than 10 years | 8 | 3.17 |
| Online social media usage per day | Less than 30 min | 5 | 1.98 |
| | 30 minutes-1 hour | 28 | 11.11 |
| | 1–2 h | 71 | 28.17 |
| | 2–6 h | 101 | 40.08 |
| | More than 6 h | 47 | 18.65 |

multicollinearity affects dependability, as assessed by the variance inflation factor (VIF) (Daoud, 2018). Third, internal consistency is a phenomenon in which the indicator varies in response to the hidden variable and may be assessed using composite reliability. Finally, convergent validity assesses the degree to which various items converge in their correlations which can be evaluated with average variance extracted (AVE) (Hair et al., 2014; Urbach & Ahlemann, 2010). To be allowed, all components must have factor loading, CR, and AVE values more than or equal to 0.5, 0.7, and 0.5, respectively (Hair et al., 2014). Additionally, VIF values, those larger than 5, are not permitted (Daoud, 2018). As per Table 5, all of the conditions were satisfied.

To determine discriminant validity in this study, the Fornell-Larker criteria were used. The diagonal values must be higher than the corresponding row and column values, according to these criteria. The measures passed the discriminant validity test, as shown in Table 6.

Table 7 displays the results of the coefficient of determination ($R^2$) and cross validated redundancy ($Q^2$). Here, the $R^2$ is a metric for assessing the explanatory power of a structural model (Chin, 2010) and $Q^2$ confirms the predictive relevance (Hair et al., 2014). In this study, the $R^2$ values for AM, PA, PT, and WT were 73.2%, 63.6%, 31.7%, and 9.8%, respectively. Moreover, the $Q^2$ values of AM, PA, PT, and WT were 60.9%, 50.5%, 22.1%, and 5.3% respectively which was greater than 0 and confirmed that the model was sufficiently predictive (Hair et al., 2014).

With values more than or equal to 0.02, 0.15, and 0.35, the effect size may be divided into three categories: minor, moderate, and substantial (Hair et al., 2014). As per Table 8, there was a major effect, two moderate effects, and four minor effects.

Table 9 revealed that 7 out of 10 hypotheses were significant. Among them, six hypotheses were highly supported ($P < 0.001$) and one was weakly supported ($P < 0.05$). Moreover, the perceived threat was found to be influenced by perceived susceptibility, perceived severity, and perceived avoidability by perceived effectiveness, self-efficacy, and perceived threat. However, the perceived cost could not influence perceived avoidability. Besides, perceived avoidability was the predictor of both avoidance motivation and wishful thinking. Just the opposite, none of the avoidance motivation and wishful thinking was influenced by the perceived threat. As such, H1-H3, H5-H6, and H9-H10 were supported but H4 and H7-H8 were not.

Finally, we used perceived avoidability as a mediator between perceived threat and two outcomes (avoidance motivation and wishful thinking). We did not find any direct impact of perceived threat on wishful thinking and avoidance motivation. For this reason, it became important to find its indirect effect. The result of the indirect effect is shown in Table 10.

As reported by our result, the indirect effect of perceived threat was significant. Therefore, it can be claimed that perceived avoidability performed as an effective mediator between perceived threat and outcome variables.

## 6. Discussion

Online safety has become a significant worry in Bangladesh as the number of social media users grows. Cyberbullying, a type of online crime, on the other hand, has primarily targeted women of Gen-Z. Fortunately; Bangladesh's government has enacted the digital security act 2018, which allows victims of cyberbullying to receive legal assistance. Because the regulation is new, it is critical to assess how this law affects these young women's motivation to prevent cyberbullying. In consequence, we adopted the TTAT model to assess these young women's adaptive (avoidance motivation) and maladaptive (wishful thinking) approaches to cyberbullying. A set of hypotheses was offered following the model to study the relationships between the model's variables.

The performances of the TTAT variables in this suggested model were evaluated against some of the current literature (see Table 11). Since they fall within the purview of our investigation, these studies were chosen. Specifically, these works have used TTAT in the area of information security. The factors have also served as a predictor of wishful thinking and avoidance motivation, which is congruent with the results of this study. Liang and Xue (2010) made an effort to comprehend the procedures by which users of personal computers prevent IT threats. The technology threat avoidance theory, on the other hand, was used by Chen and Liang (2019) to assess how volitional computer users handle IT threats.

In line with Hypothesis H1, a greater PSU level equals a higher PT level. The findings strongly support H1, with the PSU having a positive influence on PT ($\beta = 0.29$, $p < 0.001$). The data also reveal that PSU has a minor effect on PT ($f^2 = 0.096$). Furthermore, this discovery is supported by previous studies (Chen & Liang, 2019; Liang & Xue, 2010). Hypothesis H1's findings have led Gen-Z women to believe that they are vulnerable to cyberbullying which is a major threat. Furthermore, if no precautionary measures are taken, the risk of this disastrous incident will grow.

As per Hypothesis H2, a higher PS value will lead to a higher PT value. According to the data, the PS ($\beta = 0.369$, $p < 0.001$) has a significant positive influence on PT. Both Liang and Xue (2010) and Chen and Liang (2019) found similar results in the setting of threat avoidance. Corresponding to the findings, the PS has a moderate impact ($f^2 = 0.154$) on PT. As a consequence, it is plausible to conclude that cyberbullying poses an extraordinary risk or threat. They also feel that if they do nothing to combat the danger, significant problems will occur.

Based on hypothesis H3, the PEF and PA have a positive relationship. Chen and Liang (2019), who came to the same result, back up this claim.

**Table 5**
Factor loadings, VIF, CR, and AVE.

| Variable | Items | Factor loadings | VIF | Composite Reliability | Average Variance Extracted (AVE) |
|---|---|---|---|---|---|
| Avoidance motivation | AM1 | 0.925 | 3.230 | 0.940 | 0.840 |
| | AM2 | 0.930 | 3.502 | | |
| | AM3 | 0.894 | 2.465 | | |
| Perceived avoidability | PA1 | 0.896 | 2.334 | 0.925 | 0.805 |
| | PA2 | 0.908 | 2.641 | | |
| | PA3 | 0.887 | 2.338 | | |
| Perceived cost | PC1 | 0.849 | 1.713 | 0.865 | 0.619 |
| | PC2 | 0.856 | 1.810 | | |
| | PC3 | 0.776 | 1.788 | | |
| | PC4 | 0.649 | 1.521 | | |
| Perceived effectiveness | PEF1 | 0.903 | 3.304 | 0.945 | 0.812 |
| | PEF2 | 0.919 | 3.712 | | |
| | PEF3 | 0.872 | 2.594 | | |
| | PEF4 | 0.911 | 3.239 | | |
| Perceived severity | PS1 | 0.869 | 2.942 | 0.928 | 0.764 |
| | PS2 | 0.894 | 3.338 | | |
| | PS3 | 0.850 | 2.396 | | |
| | PS4 | 0.884 | 2.736 | | |
| Perceived susceptibility | PSU1 | 0.770 | 1.828 | 0.901 | 0.696 |
| | PSU2 | 0.843 | 2.205 | | |
| | PSU3 | 0.887 | 2.616 | | |
| | PSU4 | 0.833 | 1.750 | | |
| Perceived threat | PT1 | 0.834 | 1.663 | 0.887 | 0.724 |
| | PT2 | 0.847 | 1.801 | | |
| | PT3 | 0.871 | 1.860 | | |
| Self-efficacy | SE1 | 0.890 | 2.293 | 0.927 | 0.809 |
| | SE2 | 0.899 | 2.507 | | |
| | SE3 | 0.910 | 2.693 | | |
| Wishful thinking | WT1 | 0.836 | 1.945 | 0.874 | 0.638 |
| | WT2 | 0.888 | 2.212 | | |
| | WT3 | 0.815 | 1.979 | | |
| | WT4 | 0.635 | 1.509 | | |

**Table 6**
Discriminant validity.

| Variable | AM | PA | PC | PEF | PS | PSU | PT | SE | WT |
|---|---|---|---|---|---|---|---|---|---|
| AM | 0.916 | | | | | | | | |
| PA | 0.856 | 0.897 | | | | | | | |
| PC | 0.526 | 0.589 | 0.787 | | | | | | |
| PEF | 0.730 | 0.696 | 0.583 | 0.901 | | | | | |
| PS | 0.295 | 0.357 | 0.565 | 0.404 | 0.874 | | | | |
| PSU | 0.181 | 0.247 | 0.440 | 0.257 | 0.480 | 0.834 | | | |
| PT | 0.305 | 0.390 | 0.504 | 0.226 | 0.508 | 0.467 | 0.851 | | |
| SE | 0.784 | 0.747 | 0.605 | 0.694 | 0.348 | 0.264 | 0.353 | 0.900 | |
| WT | 0.262 | 0.323 | 0.343 | 0.367 | 0.147 | 0.162 | 0.150 | 0.343 | 0.799 |

**Table 7**
$R^2$ and $Q^2$ values.

| Dependent variable | $R^2$ | $R^2$ Adjusted | $Q^2$ |
|---|---|---|---|
| AM | 0.734 | 0.732 | 0.609 |
| PA | 0.642 | 0.636 | 0.505 |
| PT | 0.323 | 0.317 | 0.221 |
| WT | 0.105 | 0.098 | 0.053 |

**Table 8**
Effect size.

| Relationships | $f^2$ value | Remarks |
|---|---|---|
| PSU → PT | 0.096 | Weak effect |
| PS → PT | 0.154 | Moderate effect |
| PEF → PA | 0.136 | Weak effect |
| PC→ PA | 0.007 | No effect |
| SE → PA | 0.235 | Moderate effect |
| PT → PA | 0.032 | Weak effect |
| PT → AM | 0.004 | No effect |
| PT → WT | 0.001 | No effect |
| PA→ AM | 2.414 | Substantial effect |
| PA → WT | 0.092 | Weak effect |

The path coefficient and effect size are also calculated to be $\beta = 0.323$, $p < 0.001$, and $f^2 = 0.136$, showing that PEF has a weak effect and beneficial influence on PA. Hence, participants are found to have great trust in the digital security act 2018 which can be used effectively to combat cyberbullying. Furthermore, increasing individuals' awareness of this security law leads them to assume that cyberbullying can be avoided or controlled.

PC and PA, as specified by Chen and Liang (2019), are unrelated. The findings of the present investigation, similarly, are identical to those of the prior study. The path coefficient and effect size are calculated to be $\beta = 0.074$, $p > 0.05$, and $f^2 = 0.007$, respectively, implying that PC has no effect on PA and therefore rejects H4. Because of this, surveyees do not consider the cost of enacting such a regulation in the country to be a deterrent. Furthermore, they consider the discomfort, overhead, difficulty, and complexity that come with it to be trivial problems.

Hypothesis H5 demonstrates that SE has a positive impact on PA. In line with the data, the SE ($\beta = 0.433$, $p < 0.001$) has a significant influence on PA. As a consequence, Hypothesis H5 is determined to be valid. Furthermore, the results reveal that SE has a moderate influence

**Table 9**
Results of hypotheses.

| Hypotheses no | Relationships | Original Sample (O) | Sample Mean (M) | Standard Deviation (STDEV) | T Statistics (\|O/STDEV\|) | P Values | Remarks |
|---|---|---|---|---|---|---|---|
| H1 | PSU → PT | 0.290 | 0.293 | 0.074 | 3.929 | 0.000 | Supported |
| H2 | PS → PT | 0.369 | 0.371 | 0.081 | 4.541 | 0.000 | Supported |
| H3 | PEF → PA | 0.323 | 0.328 | 0.069 | 4.684 | 0.000 | Supported |
| H4 | PC → PA | 0.074 | 0.080 | 0.065 | 1.145 | 0.253 | Not supported |
| H5 | SE → PA | 0.433 | 0.423 | 0.086 | 5.061 | 0.000 | Supported |
| H6 | PT → PA | 0.127 | 0.127 | 0.054 | 2.345 | 0.019 | Supported |
| H7 | PT → AM | −0.034 | −0.033 | 0.041 | 0.829 | 0.408 | Not supported |
| H8 | PT → WT | 0.028 | 0.031 | 0.075 | 0.376 | 0.707 | Not supported |
| H9 | PA → AM | 0.870 | 0.867 | 0.026 | 32.968 | 0.000 | Supported |
| H10 | PA → WT | 0.312 | 0.316 | 0.078 | 3.989 | 0.000 | Supported |

**Table 10**
Mediation effect of perceived avoidability.

| Relationships | Original Sample (O) | Sample Mean (M) | Standard Deviation (STDEV) | T Statistics (\|O/STDEV\|) | P Values | Remarks |
|---|---|---|---|---|---|---|
| PT → PA → WT | 0.039 | 0.040 | 0.020 | 1.987 | 0.047 | Supported |
| PT → PA → AM | 0.110 | 0.110 | 0.047 | 2.341 | 0.020 | Supported |

**Table 11**
Comparison with previous studies.

| Hypotheses no | Liang and Xue (2010) | Chen and Liang (2019) | Outcome of this research |
|---|---|---|---|
| H1 | $\beta = 0.41$, $p < 0.01$, significant | $\beta = 0.52$, $p < 0.01$, significant | $\beta = 0.29$, $p < 0.001$, significant |
| H2 | $\beta = 0.27$, $p < 0.01$, significant | $\beta = 0.23$, $p < 0.01$, significant | $\beta = 0.369$, $p < 0.001$, significant |
| H3 | Not evaluated | $\beta = 0.56$, $p < 0.01$, significant | $\beta = 0.323$, $p < 0.001$, significant |
| H4 | Not evaluated | $\beta = -0.05$, $p > 0.05$, non-significant | $\beta = 0.074$, $p > 0.05$, non-significant |
| H5 | Not evaluated | $\beta = 0.25$, $p < 0.01$, significant | $\beta = 0.433$, $p < 0.001$, significant |
| H6 | Not evaluated | Not evaluated | $\beta = 0.127$, $p < 0.05$, significant |
| H7 | $\beta = 0.26$, $p < 0.01$, significant | $\beta = 0.21$, $p < 0.05$, significant | $\beta = -0.034$, $p > 0.05$, non-significant |
| H8 | Not evaluated | $\beta = 0.34$, $p < 0.01$, significant | $\beta = 0.028$, $p > 0.05$, non-significant |
| H9 | Not evaluated | $\beta = 0.16$, $p < 0.05$, significant | $\beta = 0.870$, $p < 0.001$, significant |
| H10 | Not evaluated | $\beta = -0.08$, $p > 0.05$, non-significant | $\beta = 0.312$, $p < 0.001$, significant |

on PA ($f^2 = 0.235$). The findings are consistent with previous research (Chen & Liang, 2019). As per the findings, Gen-Z women have the necessary knowledge and skills to use the digital security act 2018 to combat cyberbullying. Furthermore, the legislation is seen to be competent and straightforward to apply.

Hypothesis H6 has similar results to Hypothesis H5 and is supported as well. In accordance with the H6 hypothesis, PT has a positive impact on PA. The results of this study also suggest that the PT ($\beta = 0.127$, $p < 0.05$) has a significant influence on PA. Furthermore, the effect size, $f^2 = 0.032$ indicates that the PT has a minor impact on PA. This newly created association has been empirically evaluated, and they have established a substantial relationship. Furthermore, respondents think that the legislation is far stronger than the threat. Besides, cyberbullying can be effectively addressed by the digital security act 2018.

A greater PT level leads to a higher AM level, as per Hypothesis H7. The findings do not support H7, with AM ($\beta = -0.034$, $p > 0.05$) not being influenced by the PT. The results also suggest that PT has no effect on AM ($f^2 = 0.004$). Furthermore, this discovery appears to be at odds with previous studies (Chen & Liang, 2019; Liang & Xue, 2010). On account of this, participants are unable to discover any link between perceived threat and avoidance motivation. Furthermore, they argue that the threat of cyberbullying cannot immediately lead to the acceptance of an avoidance strategy.

In line with Hypothesis H8, a greater PT value equals a higher WT value. As reported by the data, PT ($\beta = 0.028$, $p > 0.05$) has no influence on WT. Chen and Liang (2019) found similar results in the setting of threat avoidance. The results also suggest that the PT has no effect on WT ($f^2 = 0.001$). Due to the fear of cyberbullying, Gen-Z women are not encouraged to use emotional coping strategies, similar to H7. They also feel that they don't need an excuse to overlook the threat of cyberbullying.

As per hypothesis H9, the PA and AM have a positive relationship. Chen and Liang (2019), who came to the same result, back up this claim. Furthermore, the path coefficient and effect size are calculated to be $\beta = 0.870$, $p < 0.001$, and $f^2 = 2.414$, showing that PA has a substantial effect and positive influence on AM. Therefore, as perceived avoidability rises, participants are more encouraged to use the avoidance method via the digital security act 2018. They are extremely encouraged to take a constructive attitude since the cyberbullying problem may be avoided by utilizing such a law.

PA has a positive influence on WT, based on hypothesis H10. Likewise, according to the data, the PA ($\beta = 0.312$, $p < 0.001$) has a significant influence on WT. As a consequence, hypothesis H10 is deemed to be supported. Furthermore, the results reveal that the PA has little influence on WT ($f^2 = 0.092$). The gained results do not correspond to previous studies (Chen & Liang, 2019). On this account, similar to H9, it may be claimed that a high reliance on the digital security act 2018 leads to respondents adopting emotion-based coping.

We have addressed the 4 research objectives of this study through the support of these 10 hypotheses and mediation analysis. As for illustration, hypotheses, H7-H10 comprise the 1st research objective. As reported by our findings, both the coping approaches (avoidance motivation and wishful thinking) are directly influenced by perceived avoidability but not by the perceived threat. Afterward, 2nd research objective is addressed by hypotheses H1-H2. As per the results, the perceived threat is efficiently predicted by both perceived severity and perceived susceptibility. Subsequently, hypotheses H3-H6 have established the 3rd research objective. In accordance with our results, perceived effectiveness, self-efficacy, and perceived threat is the determinant of perceived avoidability whereas perceived cost is not. Finally, perceived avoidability has a mediation effect on the relationships between the perceived threat and coping approaches which ensures the 4th research objective. Due to this, it can be stated that coping approaches are indirectly influenced by perceived threat only in the presence of perceived avoidability.

## 7. Conclusion

Cyberbullying is common in Bangladesh, with Gen-Z women accounting for 80% of victims. Therefore, the Bangladesh government has just legislated the digital security act 2018 to address this issue. After all, this commandment is new; it is questionable whether the law will be accepted by Gen-Z women. Due to this, the TTAT has been used to assess two coping strategies: avoidance motivation and wishful thinking. Where perceived threat has no direct impact on coping techniques, 7 out of 10 hypotheses are significant, as reported by our findings. Rather, it has an indirect impact due to the support of the perceived avoidability mediation effect. Aside from the 73.4% and 10.5% variances obtained from avoidance motivation and wishful thinking, we may draw three key findings. To begin with, the data nearly entirely supports the proposed conceptual model. Second, both coping mechanisms may coexist and complement one another rather than be mutually incompatible. Finally, because of their fear of cyberbullying, Gen-Z women favor adaptive (use of the digital security act 2018) over maladaptive (wishful thinking) measures. In addition, we have matched our findings to those of other research. Some of our findings are comparable to earlier research, while others are not. Importantly, the findings of wishful thinking, associated correlations, and mediation effect were pretty much unknown in this context before this study, and they have opened up a new line of research.

## 8. Theoretical and practical implications

From a theoretical standpoint, this study has tackled various previously unknown subjects. To begin with, this is one of the first studies to investigate the factors that impact the motivations of Gen-Z women to use digital security legislation to combat cyberbullying. Because the digital security act 2018 is a new law, its acceptability has not yet been thoroughly investigated. TTAT is also one of the newest models, and as far as we know, it has never been used to solve cyberbullying concerns. Second, wishful thinking has been introduced as an emotional coping mechanism along with the current avoidance motivation. The existing theory has been expanded to include such coping mechanisms. Prior empirical research considered problem-focused coping as the only coping outcome coming from cognitive appraisals; however, this study backs up TTAT by showing that one can use a variety of approaches to avoid cyberbullying issues, including wishful thinking. We also show that the two types of cognitive assessments play different roles in explaining coping decisions. These two sorts of qualities, we argue, do not have to be mutually exclusive; instead, they may coexist and complement one another. Finally, avoidability, on the flip side, acts as a mediator between threat and coping techniques. It assures that the remedy is far more powerful than the issues and the legislation is capable of reducing the threat of cyberbullying.

From a practical standpoint, this research incorporates Gen-Z woman's motivation to get protected from cyberbullying, allowing for the adoption of the digital security act 2018. As a result, the study's findings can give the Bangladesh government the information it needs to make the right decisions and lessen controversy around the digital security act 2018. In addition, the findings might help the government to educate these young women about the hazards of cyberbullying and the way to defend them. For avoidance motivation, we have got 73.4% variance and 10.5% for wishful thinking. It assures that young women rely on the digital security act 2018 to deal with cyberbullying concerns. In our research, problem-based coping was proven to be far more effective than emotional coping. These women are expected to address cyberbullying by enforcing existing laws rather than just denying or ignoring them. Anyhow, this variation is substantially higher than in earlier investigations. As such, it is possible to assert that the acquired data closely matches the model. Moreover, as specified by the conclusions of this study, it is vital to involve female students in cyberbullying awareness programs at schools, colleges, and universities. Through these students, institutions can start a variety of community-based programs that can increase people's understanding of the digital security act 2018 and incentives to act. Furthermore, public media and communication initiatives should be well-designed to appeal to a bigger audience and improve people's willingness to participate. The outcomes of this study might be utilized to pique people's interest in using the digital security act 2018 to mitigate the detrimental effects of cyberbullying, particularly in underdeveloped countries.

## 9. Limitations and future study

Our research has certain flaws that will be addressed in future research. To begin, this study model was specifically designed to assess the factors that impact Gen-Z women's willingness to use the digital security act 2018 to combat cyberbullying. It is unclear, though, if the conclusions may be extended and used for a larger variety of other security laws. The demographics of users in various nations might not be the same as those of the research participants. As a result, similar factors might not be as important in other nations, especially in industrialized nations. However, we need further investigations to claim the proposed model as the generalized one. Second, we only looked at women between the ages of 15 and 24. Notably, males and adult women can also be victims of cyberbullying. As a result, males and females of various ages might be considered. Third, we presumed only wishful thinking as a type of emotional coping mechanism. Denial, acceptance, distance, self-blame, self-isolation, and turning to religion are some more instances of emotional coping that might be examined (Chen & Liang, 2019). Finally, certain essential cyberbullying characteristics like trust, privacy, fear, and incentives were overlooked in this study.

## Declaration of competing interest

We have no conflicts of interest to disclose.

## Data availability

The data that has been used is confidential.

## Appendix

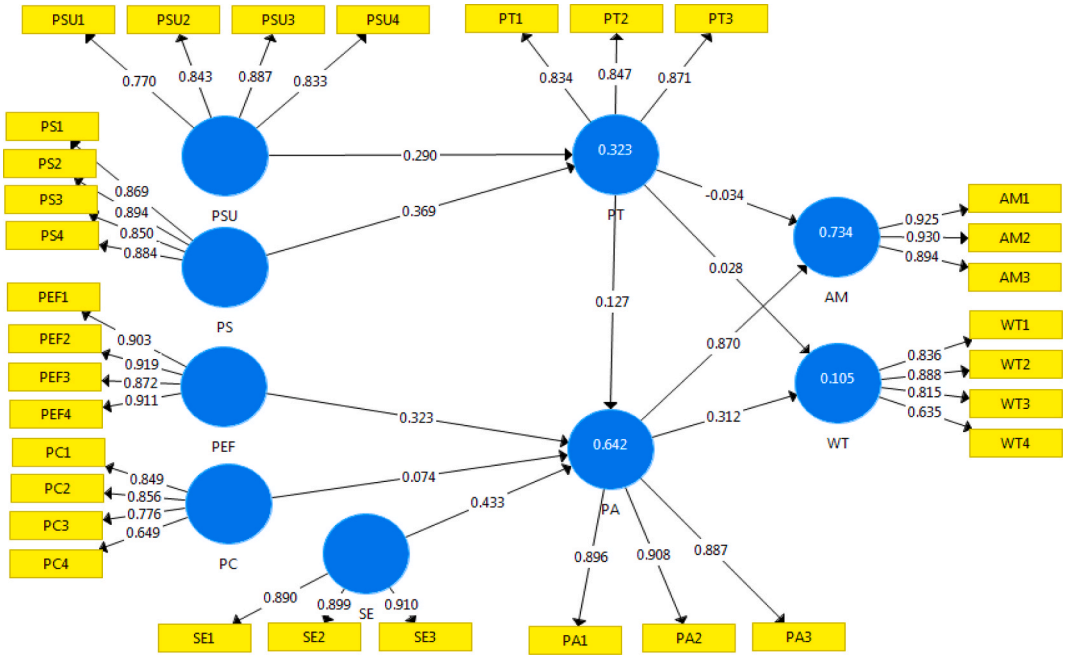


**Fig. ure.** Measurement model results from SmartPLS

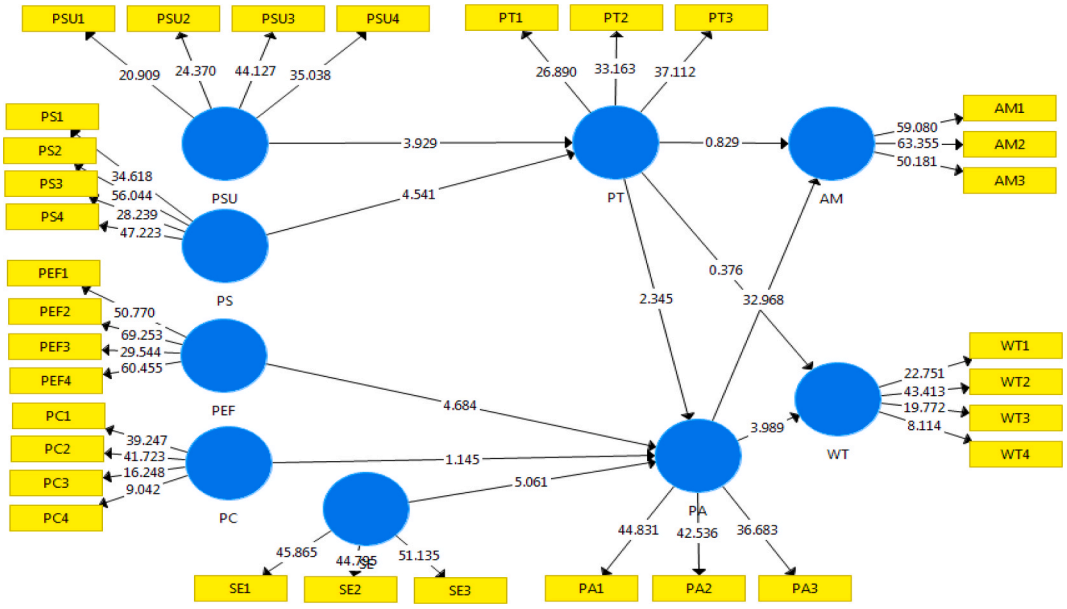


**Fig. ure.** Structural model results from SmartPLS
ns = non-significant, *p < 0.05, **p < 0.01, ***p < 0.001

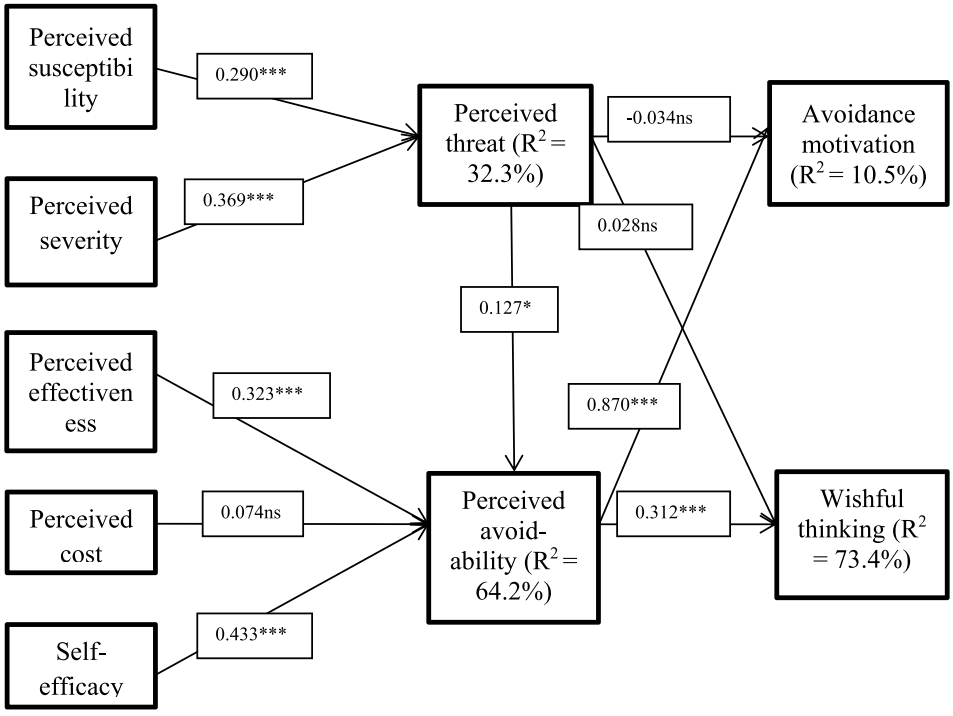


**Fig. ure.** Hypotheses testing results

## References


Alomar, N., Alsaleh, M., & Alarifi, A. (2019). Uncovering the predictors of unsafe computing behaviors in online crowdsourcing contexts. *Computers & Security, 85*(5), 300–312. https://doi.org/10.1016/j.cose.2019.05.001

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304–312.

Arachchilage, N. A., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior, 60*, 185–197.

Aribake, F. O., & Aji, Z. M. (2020). Modelling the phishing avoidance behaviour among internet banking users in Nigeria: The initial investigation. *Journal of Computer Engineering and Technology, 4*(1), 1–17.

Babu, K. E. K., & Ullah, M. A. (2021). Cyber legislation and cyber-related legal issues in Bangladesh: Inadequacies and challenges. *International Journal of Electronic Security and Digital Forensics, 13*(2), 180–196. https://doi.org/10.1504/ijesdf.2021.113379

Bangladesh Computer Council. (2019). *BGD e-GOV CIRT | Bangladesh e-government computer incident response team*. Bangladesh Computer Council. https://www.cirt.gov.bd/.

Bari, M. E., & Dey, P. (2019). The enactment of digital security laws in Bangladesh: No place for dissent. *George Washington International Law Review, 51*(4), 595–631.

Bax, S., McGill, T., & Hobbs, V. (2021). Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. *Computers & Security, 106*, 1–14.

Beaudry, A., & Pinsonneault, A. (2005). Understanding user responses to information technology: A coping model of user adaption. *MIS Quarterly, 29*(3), 493–524.

Betts, L. R., Spenser, K. A., & Gardner, S. E. (2017). Adolescents' involvement in cyber bullying and perceptions of school: The importance of perceived peer acceptance for female adolescents. *Sex Roles, 77*, 471–481. https://doi.org/10.1007/s11199-017-0742-2

Boysen, S., Hewitt, B., Gibbs, D., & McLeod, A. J. (2019). Refining the threat calculus of technology threat avoidance theory. *Communications of the Association for Information Systems, 45*(5), 95–115.

Butler, M., & Butler, R. (2021). The influence of mobile operating systems on user security behavior. In *2021 IEEE 5th international conference on cryptography, security and privacy* (pp. 134–138). https://doi.org/10.1109/CSP51677.2021.9357568, 8-10 Jan. 2021, Zhuhai, China.

Cao, G., Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2021). Understanding managers' attitudes and behavioral intentions towards using artificial intelligence for organizational decision-making. *Technovation, 106*, 1–15.

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems, 44*(1), 380–407. https://doi.org/10.17705/1CAIS.04422

Carver, C. S., Scheier, M. F., & Weintraub, J. K. (1989). Assessing coping strategies: A theoretically based approach. *Journal of personality and social psychology, 56*(2), 267–283.

Cénat, J. M., Hébert, M., Blais, M., Lavoie, F., Guerrier, M., & Derivois, D. (2014). Cyberbullying, psychological distress and self-esteem among youth in Quebec schools. *Journal of Affective Disorders, 169*, 1–7.

Chen, D., & Liang, H. (2019). Wishful thinking and IT threat avoidance: An extension to the technology threat avoidance theory. *IEEE Transactions on Engineering Management, 66*, 552–567.

Chin, W. W. (2010). How to write up and report PLS analyses. In *Handbook of partial least squares* (pp. 655–690). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-32827-8_29.

Choi, H. S., Carpenter, D., & Ko, M. S. (2022). Risk taking behaviors using public wi-fi. *Information Systems Frontiers, 24*(3), 965–982.

Cho, V., & Ip, A. W. (2018). A Study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems, 12*, 659–673.

Chowdhury, F. (2020). Bullying of students in academic institutions: A qualitative study. *Educational Process: International Journal, 9*(2), 122–132.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Erlbaum.

Daoud, J. I. (2018). Multicollinearity and regression analysis. *Journal of Physics: Conference Series, 949*, 1–6. https://doi.org/10.1088/1742-6596/949/1/012009

Defenders, F. (2020). Two years since coming into force, Bangladesh's Digital Security Act continues to target human rights defenders and suppress free speech. *Front Line Defenders*. https://www.frontlinedefenders.org/en/statement-report/two-years-coming-force-bangladeshs-digital-security-act-continues-target-human.

Dhiraj, A. B. (2018). *Countries where cyber-bullying was reported the most in 2018. CEOWORLD magazine*. Available in https://ceoworld.biz/2018/10/29/countries-where-cyber-bullying-was-reported-the-most-in-2018/.

Dodel, M., & Mesch, G. S. (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers & Security, 86*(3), 75–91.

Etikan, I. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

Fakir, M. K. J. (2023). Cyberbullying among university students: A study on Bangladeshi universities. *Journal of Social, Humanity, and Education, 3*(2), 119–132.

Folkman, S., & Lazarus, R. S. (1985). If it changes it must be a process: Study of emotion and coping during three stages of a college examination. *Journal of personality and social psychology, 48*(1), 150–170.

Folkman, S., Lazarus, R. S., Dunkel-schetter, C., DeLongis, A., & Gruen, R. J. (1986). Dynamics of a stressful encounter: Cognitive appraisal, coping, and encounter outcomes. *Journal of personality and social psychology, 50*(5), 992–1003.

Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior, 108*(4), 1–12.

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review, 26*(2), 106–121. https://doi.org/10.1108/EBR-10-2013-0128

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing, 20*, 277–320.

Hewitt, B., Dolezel, D., & McLeod, A. (2017). Mobile device security: Perspectives of future healthcare workers. *Perspectives in Health Information Management, 14*, 1–4.

Hossain, A., Abdul Wahab, J., Islam, M. R., Khan, M. S. R., & Mahmud, A. (2022). *Cyberbullying perception and experience among the university students in Bangladesh*. IGI Global. https://doi.org/10.4018/978-1-7998-9187-1.ch012, 248–269 https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-9187-1.ch012.

Hossen, S. (2021). Nature and aftermath of cyberbullying with female university students in Bangladesh. *IOSR Journal of Humanities and Social Science, 26*(10), 45–53.

Hunter, S. C., Boyle, J. M. E., & Warden, D. (2007). Perceptions and correlates of peer-victimization and bullying. *British Journal of Educational Psychology, 77*(4), 797–810. https://doi.org/10.1348/000709906X171046

Internet Subscribers. (2021). *Btrc* [Accessed on 26th January, 2022] Available from: World Wide Web: http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-november-2021.

Jain, S., & Agrawal, S. (2020). Perceived vulnerability of cyberbullying on social networking sites: Effects of security measures, addiction and self-disclosure. *Indian Growth and Development Review, 14*(2), 149–171.

Kim, D. J., Phillps, B., B, & Ryu, Y. U. (2018). Impact of perceived risk, perceived controllability, and security self-efficacy on secure intention from social comparison theory perspective. In *Proceedings of theNational cyber summit* (pp. 58–63). https://doi.org/10.1109/NCS.2018.00014, 5-7 June 2018, Huntsville, AL, USA.

Križan, Z., & Windschitl, P. D. (2007). The influence of outcome desirability on optimism. *Psychological Bulletin, 133*(1), 95–121.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71–90.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Liang, H., Xue, Y., Pinsonneault, A., & Yu. (2019). What users do besides problem-focused coping when facing IT security threats: An emotion-focused coping perspective. *MIS Quarterly, 43*(2), 1–18.

Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management, 54*(1), Article 102152.

Mallik, C. I. (2020). Adolescent victims of cyberbullying in Bangladesh- prevalence and relationship with psychiatric disorders. *Asian Journal of Psychiatry, 48*, Article 101893. https://doi.org/10.1016/j.ajp.2019.101893

Mansbach-Kleinfeld, I., Ifrah, A., Apter, A., & Farbstein, I. (2015). Child sexual abuse as reported by Israeli adolescents: Social and health related correlates. *Child Abuse & Neglect, 40*, 68–80. https://doi.org/10.1016/j.chiabu.2014.11.014

Manzano, D. L. (2012). *The cybercitizen dimension: A quantitative study using a threat avoidance perspective (doctoral thesis)*. Capella University.

Marett, K., Vedadi, A., & Durcikova, A. (2019). A quantitative textual analysis of three types of threat communication and subsequent maladaptive responses. *Computers & Security, 80*, 25–35. https://doi.org/10.1016/j.cose.2018.09.004

Mogaji, E. (2022). Wishful thinking? Addressing the long-term implications of COVID-19 for transport in Nigeria. *Transportation Research Part D: Transport and Environment, 105*(2), Article 103206. https://doi.org/10.1016/j.trd.2022.103206

Mogumder, A. (2022). *Infringing upon our basic freedoms | Dhaka tribune. Dhaka tribune*. https://www.dhakatribune.com/op-ed/2022/04/25/infringing-upon-our-basic-freedoms.

Monni, S. S., & Sultana, A. (2016). Investigating cyber bullying: Pervasiveness, causes and socio-psychological impact on adolescent girls. *Journal of Public Administration and Governance, 6*(4), 12. https://doi.org/10.5296/jpag.v6i4.10132

Mwagwabi, F., McGill, T., & Dixon, M. (2014). *. Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. In *Proceedings of the 47th Hawaii international conference on system Sciences* (pp. 3188–3197). https://doi.org/10.1109/HICSS.2014.396, 6-9 January 2014, Waikoloa, HI, USA.

Nabi, R. L., Wolfers, L. N., Walter, N., & Qi, L. (2022). Coping with COVID-19 stress: The role of media consumption in emotion- and problem-focused coping. *Psychology of Popular Media, 11*(3), 292–298. https://doi.org/10.1037/ppm0000374

Riaz, A., & Zaman, F. (2022). Working under the "sword of damocles": Experiences of journalists in a hybrid regime. In A. E. Ruud, & M. Hasan (Eds.), *Masks of authoritarianism*. Singapore: Palgrave Macmillan. https://doi.org/10.1007/978-981-16-4314-9_3.

Ringle, C. M., Da Silva, D., & Bido, D. D. S. (2014). Modelagem de Equações estruturais com utilização do smartpls. *Revista Brasileira de Marketing, 13*(2), 56–73. https://doi.org/10.5585/remark.v13i2.2717

Sabera, T. (2021). All that is wrong with the world. https://www.thedailystar.net/law-our-rights/news/all-wrong-the-digital-security-act-2057321. The Daily Star.

Samhan, B. (2017). Security behaviors of healthcare providers using hit outside of work: A technology threat avoidance perspective. In *Proceedings of the 8th international conference on information and communication systems* (pp. 342–347), 4-6 April 2017, Irbid, Jordan.

Sarker, S., & Shahid, A. R. (2018). *Cyberbullying of high school students in Bangladesh: An exploratory study* (Vols. 1–5). http://arxiv.org/abs/1901.00755.

Sharma, G. (2017). Pros and cons of different sampling techniques. *International journal of applied research, 3*(7), 749–752.

Smriti, A. A., & Nahar, N. (2019). Cyberbullying and preventive measures: Bangladesh in context. *BiLD Law Journal, 4*(1), 123–135.

Sohel, M. (2018). *How section 57 morphed into digital security act provisions | Dhaka tribune. Dhaka tribune*. https://www.dhakatribune.com/bangladesh/law-rights/2018/08/10/how-section-57-morphed-into-digital-security-act-provisions.

The Business Standard. (2022). *Most DSA cases filed by ruling party people: Study*. The Business Standard. https://www.tbsnews.net/bangladesh/most-dsa-cases-filed-ruling-party-people-study-408398.

Uddin, R., Burton, N. W., Maple, M., Khan, S. R., & Khan, A. (2019). Suicidal ideation, suicide planning, and suicide attempts among adolescents in 59 low-income and middle-income countries: A population-based study. *The Lancet Child and Adolescent Health, 3*(4), 223–233. https://doi.org/10.1016/S2352-4642(18)30403-6

Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. *Journal of Information Technology Theory and Application, 11*(2), 5–40.

Wachs, S., Jiskrova, G. K., Vazsonyi, A. T., Wolf, K. D., & Junger, M. (2016). A cross-national study of direct and indirect effects of cyberbullying on cybergrooming victimization via self-esteem. *Psicologia Educativa, 22*, 61–70.

Wynn, D., Williams, C. K., Karahanna, E., & Madupalli, R. (2013). Preventive adoption of information security behaviors. In *Thirty third international conference on information systems* (pp. 1–18) (Milan).

Yong, A. G., & Pearce, S. (2013). A beginner's guide to factor analysis: Focusing on exploratory factor analysis. *Tutorials in Quantitative Methods for Psychology, 9*(2), 79–94. https://doi.org/10.20982/tqmp.09.2.p079

Young, D. K., Carpenter, D., & McLeod, A. J. (2016). Malware avoidance motivations and behaviors: A technology threat avoidance replication. *AIS Transactions on Replication research, 2*(8), 1–17.

Youth and the 2030 agenda. (2018). *World youth report*. United Nations Publication. Retrieved from https://www.un.org/development/desa/youth/wpcontent/uploads/sites/21/2018/12/WorldYouthReport-2030Agenda.pdf.

Zheng, D., Luo, Q., & Ritchie, B. W. (2022). The role of trust in mitigating perceived threat, fear, and travel avoidance after a pandemic outbreak: A multigroup analysis. *Journal of Travel Research, 61*(3), 581–596. https://doi.org/10.1177/0047287521995562

***Arif Mahmud*** is currently a PhD student in the School of Computer Sciences at the Universiti Sains Malaysia in Pulau Pinang, Malaysia. Besides, he is employed as Assistant Professor at the department of Computer Science and Engineering in Daffodil International University, Bangladesh. He has received the Degree of Master of Science with Major in Computer Engineering from Mid Sweden University, Sweden. He worked as teaching assistant and project assistant in Mid Sweden University and Stockholm University respectively. His current research interest comprises Management Information Systems, IT Operations & Management, Software engineering, and Social Networking with Communication systems.

***Jannatul Bakia Sweety*** has successfully completed her Masters in Science in Sustainable Cities and Communities from Universiti Sains Malaysia. She has achieved 'Gold Medal' for her research works as a post graduate student. Besides, she is working as a Research Officer in Sustainable Development area. Her research area includes but not limited to; sustainable cities and urban planning, youth, women and behavioral patterns, social exclusion and smart transportation system.

***Aftab Hossain*** is currently a Ph.D. student at the School of Communication, University of Science Malaysia. He is also working as a Senior Lecturer of the Department of Journalism and Mass Communication, Daffodil International University from, Bangladesh from 2016. His core research areas are Communication, Social Media, and Journalism

***Mohd Heikal Husin*** is an Information System lecturer in the School of Computer Sciences at the Universiti Sains Malaysia in Pulau Pinang, Malaysia. He has published in both local and international conferences as well as international journals on the topic of social media usage policy development within organizations as well as effective technology adoption approaches. He holds a Bachelor of Multimedia Computing from INTI International University (formerly known as INTI College Malaysia), a Master in e-Commerce and a PhD in IT from the School of Computer and Information Science at the University of South Australia. His current research interests include Government 2.0, Enterprise 2.0, Social Networking, and Software Testing