# Understanding Cybersecurity Behavioral Habits：

# Insights from Situational Support

**Abstract** While the Internet has become an indispensable aspect of personal and professional lives, it has also served to render many individuals vulnerable to cybersecurity threats. Thus, the promotion of cybersecurity behaviors can effectively protect individuals from these threats. However, cybersecurity behaviors do not necessarily come naturally, and people need support and encouragement to develop and adopt them. A habit is an important factor that may motivate cybersecurity behaviors, but it has often been overlooked in past studies. To address this limitation, this study examined the formation of cybersecurity behavioral habits. Hierarchical regression analysis was used to analyze cybersecurity behavior survey data obtained from 393 college student participants. The results revealed the following: (1) efficacy and behavioral comprehensiveness predict cybersecurity behavioral habits; (2) efficacy has a positively impact on behavioral comprehensiveness; (3) situational support has a positive influence on efficacy. These findings suggest that cybersecurity behavioral habits can be formed by promoting the diversity of cybersecurity measures practiced (behavioral comprehensiveness) and efficacy.

*Keywords*: cybersecurity; behavioral habit; situational support; behavioral comprehensiveness; self-efficacy; response efficacy

# 1 Introduction

Cybersecurity incidents are often caused by human errors or a lack of knowledge. The International Business Machines Corporation (IBM) X-Force Threat Intelligence Index 2020 indicated that insiders' mistakes were largely to blame for over 8.5 billion records be compromised in 2019 which was more than 200 percent of the number lost in 2018 (International Business Machines Corporation, 2020). The Ernst & Young Global Information Security Survey 2018-19 reported that 34% of organizations saw carelss/unaware employees as the biggest vulnerability of cybersecurity, and phishing (22%) was considered as the biggest threat to organizations (Ernst & Young, 2018). The National Cyber Security Centre (NCSC) in the United Kingdom found that 23.2 million victim accounts worldwide used "123456" as their passwords (NCSC, 2019). According to the Annual Cybersecurity Report that was published by Cisco (2018), phishing and spear phishing emails were at the root of some of the biggest cybersecurity breaches in recent years. Therefore, the promotion of cybersecurity behaviors is an important means by which home and organizational users can be protected from threats. Indeed, the human and technological aspects of information security must be simultaneously addressed to guarantee a secure cyber environment. Motivated behaviors emerge from the interactions between intentions and habits (Wood & Quinn, 2005). Intentions are controlled by consciousness, whereas habits

lead to unconscious automated behaviors (Ouellette & Wood, 1998). Many studies have tried to explain the formation of information security behaviors from the perspective of intentions. By contrast, although some studies have examined information security behavioral habits as predictors of intention (Vance, Siponen, & Pahnila, 2012; Tsai et al., 2016; Pahnila, Siponen, & Mahmood, 2007), only a few of them have delineated the mechanism by which information security behavioral habits are formed.

Cybersecurity behaviors emerge from the interaction between an environment and the individuals within it (Warkentin, Johnston, & Shropshire, 2011). Several factors such as culture (Chang & Lin, 2007), policies, participation in the Security Education, Training, and Awareness program (Han, Kim, & Kim, 2017), organizational structure (Hong & Furnell, 2019), managerial participation, and leadership (Hu et al., 2012; Guhr, Lebek, & Breitner, 2019) have been examined as environmental influences. Moreover, the support from the organization be also considered as an important environmental factor that can promote positive performance of employee (Eisenberger, et al., 1986). According to situational constraint theory that has been proposed by Peters & O 'Connor (1980), situational constraints are important factors that will hinder individuals' utilization of their abilities and reduce their performances. Many studies use the concept of situational support which is the opposite of a situational constraint to positively predict the individuals' organizational behaviors and performances. Such as in the area of information security, Warkentin et al. (2011) believe that individuals who are provided with situational supports (e.g. interpersonal helping, support from supervisor or colleagues, supply adequate time for practice behaviors) sufficiently will be conductive to their self-efficacy, and thereby leading to the formation of information security behaviors.

In this study, we examined the formation of cybersecurity behavioral habits from the perspective of situational support. The remainder of this paper is organized as follows: in Section 2, the conceptual background and the hypotheses that were formulated for this study are presented; in Section 3, an in-depth description of the methodology of this study, including details about the participants, measures, and data analytic strategies are articulated; in Section 4, the results of the analyses are presented; and in Section 5, the conclusions and implications of the study are delineated.

# 2 Conceptual background and hypothesis development

In this section, based on the analysis of the formation of habits, we developed a series of hypotheses and proposed the research conceptual framework by integrating the variables of self-efficacy, response efficacy, behavioral comprehensiveness, from the perspective of situational support.

## 2.1 Cybersecurity behaviors and habits

The formation of cybersecurity behaviors can be predominantly explained in existing literature by deterrence theory, the theory of planned behavior (TPB), and protection motivation theory (PMT). Deterrence theory suggests that the cybersecurity behaviors can be controlled by the certainty and severity of punishment (Ameen,

Tarhini, Shah, Madichie, Paul, & Choudrie, 2021). TPB considers individuals' attitude, subjective norms, perceived behavioral control determine the behavioral decision-making (Ajzen, 1991), and many scholars verified the feasibility of using TPB to explain the formation mechanism of cybersecurity behaviors (Lee & Kozar, 2005; Dinev & Qing, 2007). Meanwhile, PMT is also widely used in the area of cybersecurity behavior (Chen & Zahedi, 2016; Tsai, Jiang, Alhabash, LaRose, Rifon, & Cotton, 2016) that considers that the protecting motivation is generated from threat appraisal and coping appraisal. Threat appraisal describes the individual's perception of the risk level of the threat, including perceived vulnerability and perceived severity; coping appraisal refers to an individual's assessment of his/her ability responding to and avoiding potential damage from threats, including self-efficacy, response efficacy, and response costs (Rogers, 1983). Furthermore, neutralization theory, health belief model, theory of reasoned action, theory of interpersonal behavior, extended parallel processing model etc. has also been used to explain the formation of security behaviors (Moody et al., 2018).

A review of these existing literature reveals that many studies have tried to explain the formation of security behaviors from the perspective of intentions, such as

- the intention to comply with security policies (Herath & Rao, 2009; Hu, Dinev T, Hart P, & Cooke, 2012; Safa, Von Solms, & Furnell, 2016; Hwang & Cha, 2018; Yoo, Sanders, & Cerveny, 2018);
- the intention to take security actions (Johnston & Warkentin, 2010; Anderson & Agarwal, 2010; Menard, Bott, & Crossler, 2017);
- the intention to use protective technologies (Dinev & Qing, 2007);
- online security intentions (Tsai et al., 2016).

However, except the intentions that under the assumption of rationality in decision-making (D'Arcy & Lowry, 2019), the generation of habits is another important formation mechnsim of behavior (Wood & Quinn, 2005). A good cybersecurity behavioral habit (e.g. backup files, scan for viruses when plugging in a USB) could prevent and protect individuals from cyber-related incidents, while a bad cybersecurity behavioral habit (e.g. neglecting to install a security update, using one password for everything, install apps without verifying) could expose individuals to more cybersecurity threatens. Although some studies in the area of information security behavior have realized the importance of habits, such as Pahnila, Siponen, & Mahmood (2007) and Vance, Siponen, & Pahnila (2012) used habits to predict the intentions to comply with information system security policy, Tsai et al. (2016) found habits can positively impact on online safety behavioral intentions. Unfortunately, only a few of them have delineated the mechanism by which information security behavioral habits are formed.

A habit is a type of daily behavior that is automatically initiated under certain circumstances (Ouellette & Wood, 1998). It had typically been measured in terms of the extent to which past behaviors are repeated. However, Verplanken & Orbell (2003) corrected this view by underscoring the important role of self-consciousness in habit formation. Moreover, many behaviors may be exhibited unconsciously if they are already a part of an individual's behavioral repertoire. If people have developed habits,

their behaviors will be more automatic, require fewer cognitive resources (Aarts & Dijksterhuis, 2000; Khare & Inman, 2006). Guiding individuals to form good cybersecurity habits thus can reduce their cybersecurity vulnerability both effortless and efficient (Lindbladh & Lyttkens, 2002). To find actionable variables for fostering cybersecurity behaviors from a self-conscious perspective, in this study, we tried to explore the formation mechanism of cybersecurity behavioral habits, especially considering the influences of organizational factor (i.e. situational support), cognitive factor (efficacy), and behavioral factor (behavioral comprehensiveness). The variables and their relationships are further described in the remainder of this section.

### 2.2 Generation of habits

Habit formation was initially stimulated by an environmental cue that pertained to a specific task (Neal, Wood, & Quinn, 2006). The more confident a person is about his or her ability to complete a task, the more likely he or she is to complete the task without expending substantial amounts of cognitive effort (e.g. weigh the pros and cons before decision-making) (Wang, Harris, & Patterson, 2013). To form a habit, a behavior must be practiced in the presence of cues that are strong enough to elicit previously learned responses to stimuli (Hull, 1943, 1950; Lally, van Jaarsveld, Potts, & Wardle, 2010; Lally & Gardner, 2013) , in other words, the individual needs to have a high level of belief in successfully practicing responses. In addition, a habit is an "outcome-directed" type of automaticity, and it develops based on the fundamental principle that rewarded responses will be repeated (Verplanken & Aarts, 1999; Neal et al., 2006; Wood & Rünger, 2016), in other words, to form a habit, the individual needs to have a high level of belief in successfully reaching the outcome. The habit formation process is depicted in Figure 1.

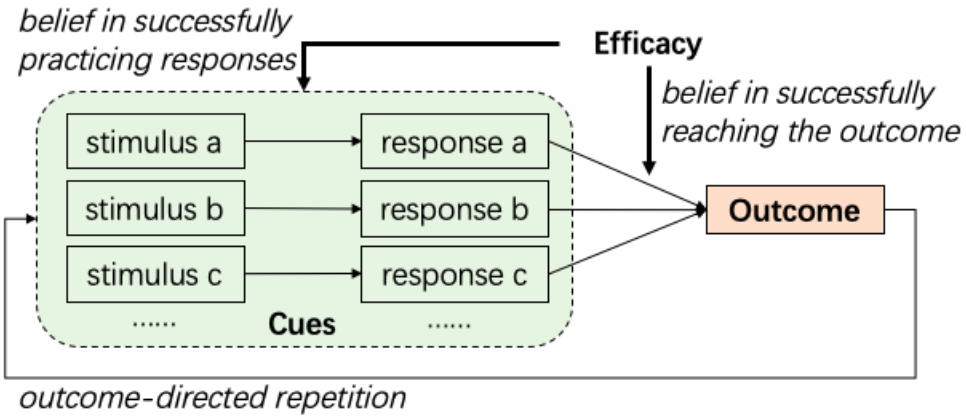


**Figure 1: The formation of habits**

### 2.3 Behavioral comprehensiveness and habits

Behavioral comprehensiveness is a term that was originally used in the area of information system (IS) usage. It is a dimension of actual behavior that refers to the extent to which an individual makes use of the various applications or functions that are offered under a single IS (Limayem, Hirt, & Cheung, 2007). Limayem, Hirt, & Cheung (2007) have contended that individuals who use ISs in different ways and across different situations tend to form stronger behavioral habits than those who use ISs in limited ways and across a fewer set of situations. They took an example of web

usage, considering that individuals that use the web extensively in a range of different ways, such as searching for information, e-mail, online chat, downloading materials, online shoping, managing finances, will tend to develop a stronger WWW use habit than the individual uses the WWW in more restricted ways.

To describe the cues that elicit responses to stimuli in the context of cybersecurity, we used the concept of cybersecurity measures can be conceptualized as a cue that activates the stimulus-response association and in turn triggers automatic cybersecurity behaviors (Vance et al., 2012; Wood & Neal, 2009). Cybersecurity behavioral comprehensiveness refers to the extent to which an individual practices several types of cybersecurity measures to avoid or attenuate the types of cyber threats that they are vulnerable to (e.g., utilization of protection software, limited browsing of unsafe websites, carefulness, data backup). Cybersecurity behavioral comprehensiveness increase the cues that strengthen the link between stimulus and response and consequently help users develop strong information security behavioral habits. Therefore, we speculated that an individual who adopts many types of information security measures will tend to develop stronger cybersecurity behavioral habits than one who practices a limited range of cybersecurity measures (Lally & Gardner, 2013). The positive effect of behavioral comprehensiveness on habits had been previously established in the area of information technology (Limayem et al., 2007; Barnes & Böhringer, 2011; Han & Farn, 2013). Therefore, an initial hypothesis was proposed as follows:

*H1: Behavioral comprehensiveness will have a positive impact on habits.*

**2.4 Efficacy, behavioral comprehensiveness, and habits**

In this study, efficacy was defined in terms of two dimensions: self-efficacy and response efficacy. Self-efficacy stems from social cognitive theory (Bandura 1986), it refers to the degree to which an individual believed that he or she can successfully perform a particular behavior (Bulgurcu, Cavusoglu, & Benbasat, 2010; Bandura, 1991; Ajzen 2002; Ng, Kankanhalli, & Xu, 2009). Response efficacy is derived from protection motivation theory (Rogers 1975), it refers to the degree to which an individual believed that he or she can perform the behaviors that are necessary to successfully reach a goal (Johnston & Warkentin, 2010; Rogers, 1975; Witte, 1992). Self-efficacy and response efficacy are indispensable to frameworks that seek to explain the habit formation process of cybersecurity behaviors, they are often used together to explain the formation of information security behaviors (Johnston & Warkentin, 2010; Wall et al., 2013). Individuals with high levels of self-efficacy to practice cybersecurity behaviors will be characterized by a strong association between a stimulus and its response. Further, an individual with high levels of response efficacy to practice cybersecurity behaviors will strongly believe that he or she can successfully avert cyber threats. This in turn will enhance the outcome-directed repetition of previously practiced cybersecurity behaviors. Therefore, we proposed the following additional hypotheses*:*

*H2: Self-efficacy will have a positive impact on habits.*
*H3: Response efficacy will have a positive impact on habits.*

Moreover, the individuals with more comprehensiveness cybersecurity protection behaviors may have higher degree of beliefs that they can successfully perform the various behaviors (self-efficacy) as well as that they can reach their targets successfully by perform the behaviors (response efficacy). These relatinships are supported by protection motivation theory (PMT) indicating that protection motivation is driven by threat and coping appraisals. Coping appraisal is an individual's assessment of his/her ability responding to and avoiding potential damage from threats, including self-efficacy, response efficacy, and response costs (Rogers, 1983). PMT has been widely used to explain the formation of information security behaviors (Lee & Larsen, 2009; Johnston & Warkentin, 2010; Liang & Xue, 2010; Vance, Siponen, & Pahnila, 2012; Tsai et al. 2016; Warkentin et al. 2016; Thompson, et al. 2017). In this regard, self-efficacy and response efficacy are two important dimensions of coping appraisal that can positively impact security behaviors (Rogers, 1983). Workman, Bommer, & Straub (2008) found that both self-efficacy and response efficacy have a significant impact on objective measures of information security behaviors. Rhee, Kim, & Ryu (2009) found that self-efficacy has a positive effect on the usage of protective information technologies. Ng et al. (2009) found that self-efficacy has a positive influence on computer security behaviors. Besides, individuals' decisions about whether they must engage in a specific behavior are influenced by the perceived likelihood of positive outcomes (Van Eerde & Thierry, 1996). Behavioral comprehensiveness entails not only actual cybersecurity behaviors but also systematic patterns and diversity that underlie behaviors. Only individuals with adequate knowledge and skills and high levels of belief in their ability to succeed will learn how they must respond to cyber threats by practicing various types of security measures.

Therefore, we proposed the following further hypotheses*:*

*H4: Self-efficacy will have a positive impact on behavioral comprehensiveness.*
*H5: Response efficacy will have a positive impact on behavioral comprehensiveness.*

**2.5 Situational support and efficacy**

Maurer, Weiss, & Barbeite (2003) conceptualized situational support as a construct that consists of two variables: work and nonwork support. They proposed that situations with adequate support and resources enhance one's judgment that he or she will be able to succeed. Specifically, when an organization provides adequate institutional guarantee to take information security measures, it will raise individuals' awareness, and promote them tend to learn the knowledge and skills. Besides, the structural mechanism for communication will also increase the diffusion of knowledges among individuals (Adler & Borys,1996; Cordón-Pozo, García-Morales, Aragón-Correa, 2006; De Clercq, Dimov, & Thongpapanl,2013). Their self-efficacy thus can be increased. Moreover, well-established rules, procedures, and policies

include the best practices that learned from experience, thus can help individuals dealing with contingencies more effectively, so that can increase their response efficacy (Adler & Borys,1996; Pertusa-Ortega, Zaragoza-Sara, & Claver-Cortél, 2010). When an organization provides training to take information security measures as well as arrange special persons for solve the problems of individuals related to taking information security meansure, the individuals' knowledge, skills, and confidence will also be promoted. Warkentin et al. (2011) contended that environments that provide an individual with sufficient situational support will have a positive impact on self-efficacy, and this in turn may influence information security behaviors. Herath & Rao (2009) found that resource availability has a positive impact on self-efficacy. According to PMT, sources of information influence cognitive factors such as response efficacy (Floy, Prentice-Dunn, & Rogers, 2000). Sources of information, especially environmental sources such as verbal persuasion and observational learning, are influenced by situational support such as security training and information consultation. Therefore, we proposed the following final hypotheses*:*

*H6: Situational support will have a positive impact on self-efficacy.*
*H7: Situational support will have a positive impact on response efficacy.*

The conceptual framework of the present research, incorporating the seven hypotheses, is presented in Figure 2.

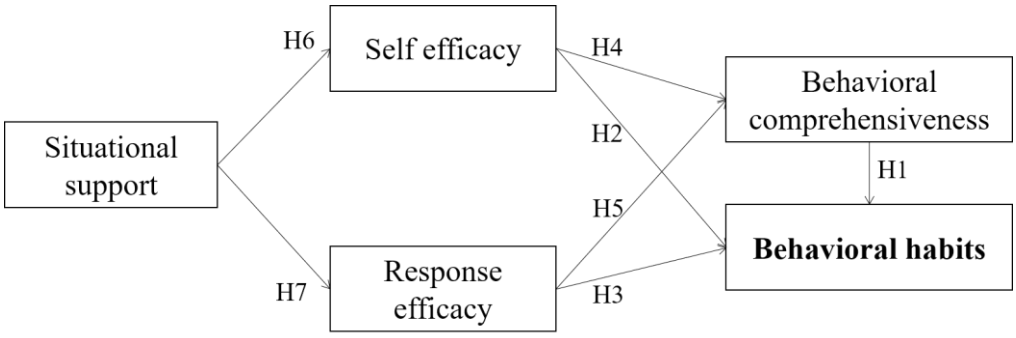


**Figure 2: The Research Conceptual Framework**

# 3 Methods

We used a cross-sectional survey to test the research model. A hypothetical scenario method was also used to provide the invitees with a detailed vignette describing a cybersecurity-related behavioral decision-making, and the invitees were required to read one scenario before they answered the questions. We developed vignettes not only because these are reliable and valid measurement strategies but also because they were expected to be more appealing to the respondents and in turn increase their likelihood of participating in the study (Wason, Polonsky, & Hyman, 2002). Currently, this method has been used in some information security behavioral literature (Guo, et al., 2011; D 'arcy et al., 2009; Vance et al., 2012). Based on the method that has been proposed by Wason et al. (2002), an open-ended question was

used to investigate the cybersecurity experiences of 100 college students. Then, content analysis was used to classify and rank the answers. Following discussions with experts in the field, five vignettes that described different cybersecurity scenarios were developed: fake ecommerce refunds, fake bank links, fake gifts, online bargains, and fake links from friends (Table 1). These were considered to representative of the type of situations and scams that the previously surveyed users had genuinely encountered in practice. The sociodemographic details of the participants, the measure scales, and the data analytic strategy were also presented in the remainder of this section.

**Table 1. Information Security Behavior Scenarios**

| No. | Scenarios |
|---|---|
| 1 | Li was presented with a webpage that informed her that she was eligible to avail a refund on her recent online purchases. She was required to provide her personal and bank information on this webpage. After Li provided the required information, a representative from her bank had called to inform her that they had noticed unusual activities on her bank account, namely, four cash withdrawals. |
| 2 | Chen received a text message on his mobile phone. He recognized that the number was that of a customer service center of his bank. The text message contained the following text: "click www. * * * *.com to immediately win a cash gift of 898 yuan." Since the number was that of his bank customer service center, Chen accessed the link that was included in the text message. On the page to which he was redirected, he provided his name, identification number, phone number, and the password for his bank card. Consequently, money had been stolen from his bank account. |
| 3 | Zhang received an email that carried the following subject: "A company and B company jointly gives you QQ coins." The following link was also provided: "http://www.1enovo.com." Zhang felt that this link is reliable because it is A company's website. Therefore, he provided his QQ account number and password as required. Consequently, his QQ account had been stolen. Later, it had been found that the scammers had used the number "1" in the place of the lower case letter "l" in "lenovo." Since the digit and lowercase letter look similar, Zhang had been misled. |
| 4 | Lu received a text message, which contained the following information: "iPhone 6s: panic buying price: only 1390 yuan." Lu immediately opened the website. The webpage was one of the ecommerce websites that he regularly accessed. Lu quickly bought a mobile phone on the webpage. Later, he found out that the phone was nothing more than a cheap replica of the shell of an iPhone. |
| 5 | Lin received a request from his classmate Wang regarding a vote. The voting website reminded him to log into his QQ account. Lin entered the account password but could not login to his account. Lin asked Wang why he could not log in. Wang said that he did not know the reason and that his QQ account had been stolen in the recent past. Lin realized he had been cheated. When he logged into his QQ account again, he found out that all his friends had been deleted from his account. |

*Note: QQ is an instant messaging app developed by the company of Tencent. QQ coin is a virtual currency launched by the Tencent that can be used to pay for online services.*

### *3.1 Study Participants*

The 41st Statistical Report on Internet Development in China revealed that there were 772 million Internet users in China in 2017, and students constituted the highest proportion of this user population (25.4%) (China Internet Network Information Center, 2018). College students regularly use the Internet for activities like sending emails, participating in online courses, accessing social networking sites, and online shopping; thus, they are potentially exposed to many cybersecurity threats (Yoon, Jae-Won, & Kim, 2012; Kim, 2013, 2014). According to a survey by Olmstead &

Smith (2017), 55% of 18–29-year-old Americans had experienced at least one type of data theft. Since college students constitute one of the largest demographic groups of Internet users and are highly exposed to cybersecurity threats, we chose to use them as the participants of the present study. Also, as a generation that will have grown up with this technology around them, they arguably stand the best chance of being IT and cybersecurity literate (i.e. when comparted to the wider population). In this sense, any results observed from this group is likely to represent a 'best case' amongs the population at large. The data are collected by using web-based surveys. According to the sample sizes of previous studies (Warkentin et al.,2016; Parsons et al.,2017; Moody et al., 2018), a total of five hundred web-based questionnaires accompanied by an invitation letter that describes the purpose of the survey were distributed to the universities students in Hangzhou. Twenty student volunteers were hired to lease the online questionnaires to their circle of friends who are study in the universities in Hangzhou. Each scenario was arranged with four volunteers, who were required to consider the balance of participants' gender, grade, and major when sending the questionnaires. A total of 432 questionnaires were collected, and data contained in 393 of them were included for analysis. The resulting questionnaires were completed by 200 males (51%) and 193 female respondents (49%). Further, 39 (10%), 108 (27%), 169 (43%), and 77 (20%) respondents were freshmen (first-year students), sophomores (second-year students), juniors (third-year students), and seniors (fourth- and final-year students), respectively. Moreover, 223 (57%), 141 (36%), and 29 (7%) respondents were majoring in economics and management, science and engineering, and other disciplines, respectively. The sociodemographic details of the participants are summarized in Table 2.

**Table 2 Results of Mean, SD and ANOVA (n=393)**

| | SS | SE | RE | BC | HA |
|---|---|---|---|---|---|
| **All** | 3.14(1.02) | 3.49(0.99) | 4.04(0.83) | 3.32(1.83) | 3.31(1.02) |
| **Gender** | | | | | |
| Male (50.9%, n=200) | 3.31(1.06) | 3.66(1.03) | 4.09(0.82) | 3.30(1.97) | 3.50(1.06) |
| Female (49.1%, n=193) | 2.97(0.95) | 3.32(0.92) | 4.01(0.84) | 3.34(1.68) | 3.11(0.94) |
| *F* | 11.533[b] | 11.997[a] | 0.941[a] | 0.040[b] | 14.752[b] |
| *P* | 0.001 | 0.001 | 0.333 | 0.842 | <0.001 |
| **Grade** | | | | | |
| Freshmen (9.9%, n=39) | 3.55(1.09) | 3.50(1.02) | 3.91(0.84) | 2.97(1.94) | 3.36(1.10) |
| Sophomores (27.5%, n=108) | 3.14(1.00) | 3.42(0.94) | 4.01(0.85) | 3.44(1.81) | 3.28(0.93) |
| Juniors (43.0%, n=169) | 3.03(0.95) | 3.43(0.96) | 4.05(0.80) | 3.18(1.76) | 3.24(1.00) |
| Seniors (19.6%, n=77) | 3.19(1.12) | 3.73(1.10) | 4.18(0.88) | 3.61(1.91) | 3.47(1.12) |
| *F* | 2.794[a] | 1.921[a] | 1.123[a] | 1.602[a] | 0.974[a] |
| *p* | 0.040 | 0.126 | 0.340 | 0.188 | 0.405 |
| **Major** | | | | | |
| Science & Engineering (35.9%, n=141) | 3.30(1.01) | 3.69(1.00) | 4.12(0.79) | 3.44(1.84) | 3.40(1.01) |
| Economic & Management (56.7%, n=223) | 3.05(0.97) | 3.39(0.96) | 4.02(0.82) | 3.24(1.76) | 3.25(1.00) |
| others (7.4%, n=29) | 3.06(1.34) | 3.36(1.08) | 3.92(1.07) | 3.28(2.27) | 3.26(1.17) |
| *F* | 2.688[b] | 4.298[a] | 1.036[a] | 0.549[a] | 0.974[a] |
| *p* | 0.075 | 0.014 | 0.356 | 0.578 | 0.379 |

| | | | | | |
|---|---|---|---|---|---|
| **Scenario** | | | | | |
| fake e-commerce refundS (22.1%, n=87) | 3.03(1.12) | 3.45(1.08) | 4.11(0.88) | 3.83(2.05) | 3.41(1.08) |
| fake bank link (18.6%, n=73) | 3.21(1.04) | 3.82(0.98) | 4.27(0.77) | 3.47(1.68) | 3.42(1.13) |
| fake gifts (19.8%, n=78) | 3.16(0.95) | 3.28(0.94) | 3.93(0.83) | 3.14(1.73) | 3.25(0.95) |
| online bargain (19.8%, n=78) | 3.14(0.94) | 3.45(0.87) | 3.91(0.79) | 2.96(1.79) | 3.16(0.87) |
| fake links from friend (19.6%, n=77) | 3.19(1.06) | 3.50(1.02) | 4.02(0.84) | 3.14(1.75) | 3.29(1.02) |
| *F* | 0.373[a] | 2.971[a] | 2.428[a] | 2.970[a] | 0.971[b] |
| *p* | 0.828 | 0.019 | 0.047 | 0.019 | 0.424 |

*Note: Standard deviations are in parentheses. [a]Statistical analysis was performed using One-way ANOVA, [b]Statistical analysis was performed using Welch test. SS=situational support, SE=self-efficacy, RE= response efficacy, BC= behavioral comprehensiveness, HA= behavioral habits.*

### *3.2 Measures*

The measurement tools that were used in this study are conventionally used standardized assessments. However, since these assessments were designed to be used in a context and with a sample that differs from those that the present study entailed, we modified these assessments. Firstly, we translated the original scales into Chinese. Then, we asked professionals who were fluent in English to translate the Chinese text into English and compare the original and back-translated English versions to determine the consistency between the Chinese and English versions of the scales. Then, we revised a part of the items into scenario-specific items by adding certain factors to the scenarios. After repeated verification and discussion with experts in language and information security, the initial scales were modified in such a manner that they are grammatically correct (i.e., in Chinese) and can match the features of different scenarios while simultaneously retaining the intended meaning of the text. Finally, some items were combined or deleted through pretests; this yielded the final Chinese version of the scale. The final versions of scales that were translated into Chinese are described in the paragraphs that follow.

**Situational support (SS).** We measured SS using three items that were adapted from Warkentin et al.'s (2011) questionnaire: (i) "I find that my university provides adequate institutional guarantee to take information security measures," (ii) "I find that my university provides adequate training to take information security measures," and (iii) "I find that there is someone in my university that I can approach if I have questions about how to take information security measures." Responses to all the items were recorded on a 5-point Likert scale that ranged from 1 (do not agree at all) to 5 (strongly agree). The Cronbach's alpha of this scale was 0.906.

**Self-efficacy (SE).** We measured SE using three items that were adapted from Bulgurcu et al. (2010) and Hu et al.'s (2012) questionnaires: (i) "I have enough knowledge to take information security measures," (ii) "I have enough skills to take information security measures," and (iii) "I have enough resources to take information security measures." Responses to all the items were recorded on a 5-point Likert scale that ranged from 1 (do not agree at all) to 5 (strongly agree). The Cronbach's alpha of this scale was 0.928.

**Response efficacy (RE).** RE was measured using three items that were adapted from Johnston & Warkentin (2010) and Ifinedo's (2012) questionnaires: (i) "Taking

information security measures is an effective protective strategy," (ii) "Taking information security measures can protect me from being cheated," and (iii) "Taking information security measures can help me avoid potential losses in such kinds of incidents." Responses to all the items were recorded on a 5-point Likert scale that ranged from 1 (do not agree at all) to 5 (strongly agree). The Cronbach's alpha of the scale was 0.915.

**Habit (HA).** HAs were assessed using three items that were adapted from Tsai et al.'s (2016) questionnaire: (i) "Taking information security measures has become a habit for me," (ii) "Taking information security measures is something that I automatically do," and (iii) "Taking information security measures is a part of my regular routine." Responses to all the items were recorded on a 5-point Likert scale that ranged from 1 (do not agree at all) to 5 (strongly agree). The Cronbach's alpha of this scale was 0.925.

**Behavioral comprehensiveness (BC)**. We measured BC using the method that had been used in Limayem et al.'s (2007) study. Specifically, we asked the respondents to check all the measures that they had taken to prevent cybersecurity incident: (1) install safety protection software; (2) upgrade and patch operating systems in a timely manner; (3) limit browsing of unfamiliar websites, refrain from downloading unknown files, and exercise caution when opening emails from strangers; (4) scan email attachments using antivirus software before opening, and scan mobile hard disks and other devices using an antivirus software before using them; (5) check whether the website that one is logged into or the program that is being used is closed in public place; (6) perform system and data backups on a regular basis; (7) periodically change usernames and passwords; and (8) encrypt important information that is stored on a device. The composite score for information security BC was computed by counting the number of checked items. The total scores could range from 0 (taken none of these measures) to 8 (taken all of these measures).

**Control variables.** Socio-demographic characteristics can influence cybersecurity behaviors. For example, Hearth & Rao (2009) found that gender plays a significant role in security policy compliance intention. Vance et al. (2012) also found that different scenarios have a significant influence on IS security compliance intention. Therefore, gender, grade, college major, and scenarios were used as control variables in this study.

### *3.3 Data analysis*

In this study, we examined the validity of measurements using confirmatory factor analysis (CFA). One-way analyses of variance (ANOVAs) were used to determine the statistical significance of group differences (i.e., by gender, grade, major, and scenario; greater than or equal to two groups) on SS, SE, RE, BC, and HA (all of them are continuous variables). To find the cause-effect relationships among the variables, hierarchical regression analysis was used to test the hypotheses. Statistical Product and Service Solutions (SPSS) 19.0 was used to analyze the data.

# 4 Results

### *4.1 Measurement Validity*

Prior to the data analysis, this study conducted an internal consistency reliability analysis and confirmatory factor analysis (CFA) to examine the qualities of given scales and acquired samples. Cronbach's α coefficient was used to test internal consistency, as it is the most common measure of reliability. The Cronbach's α coefficient of the overall questionnaire was 0.927, which suggests that the questionnaire had good internal consistency. The results showed that the Kaiser-Meyer-Olkin value was 0.881 (which is above the accepted threshold of 0.8), and the results of Bartlett's test of sphericity was significant. These results suggested that the data could be subjected to factor analysis. As shown in Table 3, the loadings of all the items were greater than 0.50, all the composite reliability (CR) values were greater than 0.7, and all the average variance extracted (AVE) values were greater than 0.5. Therefore, the assessment was considered to have good convergent validity. As shown in Table 4, the square root of the AVE value for each construct was higher than the correlations that emerged between it and all other constructs. Therefore, the assessment was considered to have good discriminant validity (Fomell & Larker, 1981). The correlations that emerged between the study variables provided preliminary support for the study hypotheses.

Moreover, one-way Analysis of Variance (ANOVA) was used to examine group differences in SS, SE, RE, BC, and HA. The Welch test was also used for variable with data distributions that did not fulfill the assumption of homogeneity of variance. Means, SDs, and the results of ANOVA are shown in Table 2. According to the results of ANOVA, we found a statistically significant difference between those groups who were male and female. The perceived situational support ($p=0.001$), self-efficacy ($p=0.001$), and habits ($p<0.001$) were higher in men comparing to women. Regarding grade, first year students had significantly higher perceived situational support ($p=0.040$) than other students. Regarding major, the students majored in Science & Engineering had significantly higer self-efficacy ($p=0.014$) than other students.

**Table 3 Factor Loading of Items**

| Construct | Item | Loading | CR | AVE |
|---|---|---|---|---|
| SS | SS1 | 0.836 | 0.895 | 0.739 |
| | SS2 | 0.875 | | |
| | SS3 | 0.868 | | |
| SE | SE1 | 0.809 | 0.868 | 0.687 |
| | SE2 | 0.857 | | |
| | SE3 | 0.821 | | |
| RE | RE1 | 0.831 | 0.903 | 0.756 |
| | RE2 | 0.885 | | |
| | RE3 | 0.891 | | |
| HA | HA1 | 0.799 | 0.861 | 0.673 |
| | HA2 | 0.857 | | |
| | HA3 | 0.804 | | |

*Note. Behavioral Comprehensiveness is a single-item construct.*

**Table 4 Correlations Between Constructs**

| Construct | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1. SS | 0.860 | | | | |
| 2. BC | 0.126* | - | | | |
| 3. SE | 0.466** | 0.227** | 0.829 | | |
| 4. RE | 0.366** | 0.233** | 0.587** | 0.869 | |
| 5. HA | 0.612** | 0.288** | 0.651** | 0.466** | 0.820 |

*Note. Diagonal elements are squared roots of AVE, * p <0.05, ** p < 0.01*

### *4.2 Hypotheses testing*

Regression analysis was used to test the study hypotheses after controlling for gender, grade, major, and scenario. As shown in Table 5, regression model 1 was constructed with habits as the dependent variable, the results showed that behavioral comprehensiveness (Model 1, $\beta = 0.077$, $p < 0.001$), self-efficacy (Model 1, $\beta = 0.556$, $p < 0.001$), and response efficacy (Model 1, $\beta = 0.138$, $p < 0.05$) had positive impacts on habits, H1, H2, H3 were thus supported. Then, regression model 2 was constructed with behavioral comprehensiveness as the dependent variable, the results showed that self-efficacy (Model 2, $\beta = 0.274$, $p < 0.05$) and response efficacy (Model 2, $\beta = 0.297$, $p < 0.05$) had positive impacts on behavioral comprehensivenss, H4 and H5 were thus supported. Futhure, regression model 3 and model 4 were constructed with self-efficacy and response efficacy as the depedent variables respectively, the results showed that situational supports had positive effcts on self-efficacy (Model 3, $\beta = 0.443$, $p < 0.001$) and response efficacy (Model 4, $\beta = 0.306$, $p < 0.001$) . Therefore, H6 and H7 were supported.

**Table 5 Results of Regression**

| Variables | Model 1 (HA) | | Model 2 (BC) | | Model 3 (SE) | | Model 4 (RE) | |
|---|---|---|---|---|---|---|---|---|
| | *β* | *p* | *β* | *p* | *β* | *p* | *β* | *p* |
| GE | -0.249** | 0.003 | 0.160 | 0.412 | -0.152 | 0.114 | 0.037 | 0.661 |
| GR | -0.041 | 0.369 | -0.033 | 0.759 | 0.111* | 0.037 | 0.086 | 0.068 |
| MJ | 0.124 | 0.075 | -0.077 | 0.639 | -0.086 | 0.288 | -0.044 | 0.541 |
| SC | -0.032 | 0.262 | -0.171* | 0.011 | -0.011 | 0.748 | -0.040 | 0.173 |
| BC | 0.077** | <0.001 | | | | | | |
| SE | 0.556** | <0.001 | 0.274* | 0.015 | | | | |
| RE | 0.138* | 0.015 | 0.297* | 0.026 | | | | |
| SS | | | | | 0.443** | <0.001 | 0.306** | <0.001 |
| $R^2$ | 0.467 | | 0.086 | | 0.24 | | 0.153 | |

*Note. GE=gender, 1=men, 2=women; GR=grade: 1=freshman, 2=sophomore, 3=junior, 4=senior; MJ=major: 1=Economic & Management, 2=Science & Engineering, and 3= Humanities & Social Sciences; SC= scenario: 1= fake e-commerce refunds, 2= fake bank link, 3= fake gifts, 4= online bargain, 5= fake links from friend.*

### *4.3 Additional findings*

Although not hypothesized, according to the regression results, we suspected that there might exist a serial multiple mediating mechanism by which situational support impacts cybersecurity behavioral habits through enhanced efficacy and behavioral comprehensivness. In order to test this idea, we constructed the following two serial multiple mediator models ($M_1$, $M_2$) because efficacy has two dimensions:

$M_1$ had three indirect effects: SS→SE→HA, SS→BC→HA, SS→SE→BC→HA

$M_2$ had three indirect effects: SS→RE→HA, SS→BC→HA, SS→RE→BC→HA

We used Model 6 of the PROCESS macro (Hayes, 2013) to test the mediating effects of both $M_1$ and $M_2$. To test the mediating effects of $M_1$, we generated 5,000 bootstrap samples. The independent variable was situational support, the mediators were self-efficacy and behavioral comprehensiveness, and the dependent variable was habits. We also included gender, grade (year), major, and scenario as covariates in the model. The results (Table 6) indicated that self-efficacy and behavioral comprehensiveness partly mediated the relationship between situational support and habits (total indirect effects = 0.2135, 95% confidence interval (CI) = 0.1502, 0.2887; direct effect = 0.3869, 95% CI = 0.3121, 0.4618). Specifically, self-efficacy mediated the relationship between situational support and habits (indirect effect = 0.1952, 95% CI = 0.1346, 0.2645), and self-efficacy and habits mediated the relationship between situational support and habits in a serial fashion (indirect effect = 0.0131, 95% CI = 0.0050, 0.0267). The mediating effect of behavioral comprehensiveness on the relationship between situational support and habits was not significant (indirect effect = 0.0052, 95% CI = -0.0115, 0.0257).

**Table 6 Bootstrap Analysis of Significance Test on Serial Multiple Mediation Effects of Self-efficacy and Behavioral Comprehensiveness**

| Path | Effect | Boot SE | CI=95% | | Significance |
|---|---|---|---|---|---|
| | | | LLCI | ULCI | |
| Direct effect | 0.3869 | 0.0381 | 0.3121 | 0.4618 | significant |
| Total indirect effect | 0.2135 | 0.0357 | 0.1502 | 0.2887 | significant |
| SS→SE→HA | 0.1952 | 0.0337 | 0.1346 | 0.2645 | significant |
| SS→BC→HA | 0.0052 | 0.0092 | -0.0115 | 0.0257 | not significant |
| SS→SE→BC→HA | 0.0131 | 0.0054 | 0.0050 | 0.0267 | significant |

*Note. Boot SE= Bootstrap standard error; LLCI = lower limit confidence interval; ULCI = upper limit confidence interval.*

We tested the mediating effects of $M_2$ in the same manner in which the mediating effects of $M_1$ were tested. The results (Table 7) indicated that response efficacy and behavioral comprehensiveness partly mediated the relationship between situational support and habits (total indirect effect = 0.1116, 95% CI = 0.0726, 0.1594; direct effect = 0.4888, 95% CI = 0.4099, 0.5677). Specifically, response efficacy mediated the relationship between situational support and habits (indirect effect = 0.0893, 95% CI = 0.0555, 0.1332), and response efficacy and habits mediated the relationship between situational support and habits in a serial fashion (indirect effect = 0.0123, 95% CI = 0.0048, 0.0249). The mediating effect of behavioral comprehensiveness on the relationship between situational support and habits was also not significant in $M_2$ (indirect effect = 0.0100, 95% CI = -0.0079, 0.0335).

**Table 7 Bootstrap Analysis of Significance Test on Serial Multiple Mediation Effects of Response Efficacy and Behavioral Comprehensiveness**

| Path | Effect | Boot SE | CI=95% | | Significance |
|---|---|---|---|---|---|
| | | | LLCI | ULCI | |
| Direct effect | 0.4888 | 0.0401 | 0.4099 | 0.5677 | significant |

| | | | | | |
|---|---|---|---|---|---|
| Total indirect effect | 0.1116 | 0.0217 | 0.0726 | 0.1594 | significant |
| SS→RE→HA | 0.0893 | 0.0197 | 0.0555 | 0.1332 | significant |
| SS→BC→HA | 0.0100 | 0.0103 | -0.0079 | 0.0335 | not significant |
| SS→RE→BC→HA | 0.0123 | 0.0051 | 0.0048 | 0.0249 | significant |

# 5 Discussion and conclusion

In this study, the mechanism by which cybersecurity behavioral habits are formed was examined from the perspective of situational support. Analysis of data from 393 participants revealed the following: (1) self-efficacy, response efficacy, and behavioral comprehensiveness have a positive impact on cybersecurity behavioral habits; (2) both self-efficacy and response efficacy have a positive impact on behavioral comprehensiveness; (3) Situational support has a positive influence on both self-efficacy and response efficacy; and (4) Situational support can promote cybersecurity behavioral habits through the serial multiple mediating effects of self-efficacy and behavioral comprehensiveness as well as response efficacy and behavioral comprehensiveness. Thus, all the hypotheses that were formulated for this study were supported.

## *5.1 Implications for Research*

Previous studies have delineated the formation mechanism of objective behaviors from the perspective of consciousness (e.g., behavioral intentions). However, the aspects of habits that do not result from consciousness have largely been neglected. A habit is an important factor that motivates human behaviors. Studies on the formation mechanism of cybersecurity behavioral habits can expand the boundaries of research on information security behavior and can provide new perspectives from which more comprehensive descriptions of formation mechanisms of information security behaviors can be rendered. Additionally, a habit is largely controlled by the situational factors, and the frequency with which a behavior is exhibited cannot fully explain the self-consciousness that habits entail (Verplanken & Orbell, 2003). Therefore, in this study, we tried to describe habit formation with regard to the influence of important situational factors such as behavioral comprehensiveness, which refers to the range of pertinent situations that an individual has previously experienced, and efficacy, which refers to an individual's belief in his or her ability to exhibit the responses to a stimulus that are required to yield desired outcomes (Wood & Quinn, 2005). Our empirical finding that efficacy and behavioral comprehensiveness predict the formation of cybersecurity behavioral habits is consistent with existing theories on habit formation (Wood & Quinn, 2005; Ouellette & Wood, 1998).

## *5.2 Practical Implications*

This research suggests that situational support can increase individuals' cybersecurity habits by the improvement of self-efficacy, response efficacy, and behavioral comprehensiveness. However, the situational support for cybersecurity in practice is often still limited. For example, the Ernst & Young Global Information Security Survey 2018-19 reported that 87% of the organizations do not have a enough budget to improve cybersecurity (Ernst & Young, 2018). Meanwhile, the UK Cyber Security Breaches Survey 2019 reported that only 33% of businesses have formal

policies covering cybersecurity, only 16% have formal cybersecurity incident management processes, and only 27% have staff that have attended training on cybersecurity in the last 12 months (Department for Digital, Culture, Media and Sport, 2019). Due to the important role of situational support in shaping human cybersecurity habits, in order to help people develop cybersecurity behavioral habits, organizations and communities must enhance their situational support such as by improving effective policies, providing tailored education and training programs that address one's needs (Furnell & Vasileiou, 2017), and by employing more cybersecurity experts who can answer questions and help individuals take information security measures. Moreover, given the mediating effects of efficacy and behavioral comprehensiveness on the relationship between situational support and the formation of individuals' cybersecurity habits, situational support could be more geared toward training individuals to use a more diversified range of security measures and encouraging them about their knowledge, skills, and ability to provide responses to stimuli that yield successful outcomes.

### *5.3 Limitations and Suggestions for Future Research*

This study has its limitations. Although situational support influences the formation of cybersecurity behavioral habits through efficacy and behavioral comprehensiveness, this process takes time. Furthermore, it is necessary to explore the causal relationships between these variables using a longitudinal research design. Such efforts are required because the cross-sectional design of the present study does not allow us to draw inferences about the causality of the emergent relationships. The organizations or communities could provide diversified situational support for shaping individuals' cybersecurity behavioral habits, such as expert supports, instituaional guarantees, and training opportunities. In this study we integrated these supports as a unified dimension. However, in practice, we need a more actionable support strategy in the resource-limited scenarios. Future research could examine the different combinations of various types of situational supports, and discover the best combination to help shaping the cybersecurity behavioral habits more effectively and efficiently. The cybersecurity behaviors in realistic are formed under the combination of rational and habitual mechanisms. However, whether it is in this study or most of the previous studies, these two mechanisms are often separated into independent studies. Future studies thus need construct a more comprehensive model that includes intentions, habits, and objectively measured behaviors.

## References


Adler, P.S., Borys, B. (1996). Two types of bureaucracy: enabling and coercive. *Administrative Science Quarterly, 41*(1):61-89.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2):179-211.

Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior. *Journal of Applied Social Psychology,32*(4),665-683.

Ameen, N., Tarhini, A., Shah. M.H., Madichie. N., Paul. J., & Choudrie. J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior, 114*.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes,50*(2),248-287.

Barnes, S.J., Böhringer, M. (2011). Modeling Use Continuance Behavior in Microblogging Services: The Case of Twitter. *Journal of Computer Information Systems,51*(4),1-10.

Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,34*(3),523-548.

Chang, S.E., & Lin, C.S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107*, 438-458

Chen, Y., & Zahedi, FM. (2016). Individuals' Internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly, 40*(1): 205-222.

China Internet Network Information Center. (2018) *The 41st China Statistical Report on Internet Development*. [Available from: https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf]

Cisco. (2018) *Annual cybersecurity report*. [Available from: https://www.cisco.com/c/dam/m/hu_hu/campaigns/ security-hub/pdf/acr-2018.pdf]

Cordón-Pozo E, García-Morales VJ, Aragón-Correa JA. (2006). Interdepartmental collaboration and new product development success: a study on the collaboration between marketing and R&D in Spanish high-technology firms. *International Journal of Technology Management, 35*(1/2/3/4):52-79.

D'Arcy, J., & Lowry, P.B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1):43-69.

De Clercq D, Dimov D, Thongpapanl N. (2013). Organizational social capital, formalization, and Internal knowledge sharing in entrepreneurial orientation formation. *Entrepreneurship Theory and Practice, 37*(3):505-537.

Dinev, T., Qing, H. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems,8*(7):386-408.

Department for Digital, Culture, Media and Sport. (2019) Cyber Security Breaches Survey 2019.[Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf]

Eisenberger, R., Huntington, R., Hutchison, S., & Sowa, D (1986). Perceived organizational support. Journal of Applied Psychology, *71* (3).

Ernst & Young. (2018). *EY Global Information Security Survey 2018-19*. New York.

Fomell, C., & Larker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1): 39-50.

Furnell, S., Vasileiou, I. (2017). Security education and awareness: just let them burn? *Network Security*, (12),5-9.

Guhr, N., Lebek, B., & Breitner, M.H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal, 29*(2), 340-362.

Han, Y.M., Farn, C.K. (2013). A Study on the Effects of Empowerment and Habit on Continuance Usage of Pervasive Business Intelligence Systems. *46th Hawaii International Conference on System Sciences*, 3768-3777.

Han, J., Kim, Y.J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security, 66*, 52-65.

Hayes, A.F. (2013) *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. New York, NY, US Guilford Press.

Herath, T., Rao, H.R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems,18*(2),106-125.

Hong, Y., & Furnell, S. (2019). Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization, *Journal of Computer Information Systems*.

Hu, Q., Dinev, T., Hart, P., Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences,43*(4),615-660.

Hull, C.L. (1943) *Principles of behavior: an introduction to behavior theory*. Oxford, England Appleton-Century.

Hull, C.L. (1950). Behavior postulates and corollaries—1949. *Psychological Review,57*(3), 173-180.

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior, 81*, 282-293.

International Business Machines Corporation. (2020). IBM X-force threat intelligence index 2020. New York.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security,31*(1):83-95.

Johnston, A.C., Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly,34*(3),549-566.

Khare, A., Inman, J.J. (2006). Habitual Behavior in American Eating Patterns: The Role of Meal Occasions. *Journal of Consumer Research,32*(4):567-575.

Kim, E.B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security,22*(1),115-126.

Kim, E.B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. *Information Security Journal: A Global Perspective,22*(4),171-179.

Lally, P., van Jaarsveld, C.H.M., Potts, H.W.W., & Wardle, J. (2010). How are habits formed: Modelling habit formation in the real world. *European Journal of Social Psychology,40*, 998-1009.

Lally, P., Gardner, B. (2013). Promoting habit formation. *Health Psychology Review,7*, S137-S158.

Lee, Y., & Kozar, K. A. (2005). Investigating Factors Affecting the Adoption of Anti-Spyware Systems. *Communications of the ACM, 48*(8): 72-77.

Lindbladh, E., & Lyttkens, C.H. (2002). Habit Versus Choice: The Process of Decision-Making in Health-Related Behaviour. *Social Science & Medicine, 55*(3),451-465.

Limayem, M., Hirt, S.G., Cheung, C.M.K. (2007). How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance. *MIS Quarterly,31*(4),705-737.

Maurer, T.J., Weiss, E.M., & Barbeite, F.G. (2003). A model of involvement in work-related learning and development activity: The effects of individual, situational, motivational, and age variables. *Journal of Applied Psychology,88*, 707-724.

Menard, P., Bott, G.J., & Crossler, R.E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems, 3*4(4), 1203-1230,

National Cyber Security Centre of UK. *Most hacked passwords revealed as UK cyber survey exposes gaps in online security*, 2019-4-21. [Available from: https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security]

Neal, T., Wood, W., Quinn, J.M. (2006). Habits – A Repeat Performance. *Current Directions in Psychological Science,15* (4), 198-202.

Ng, B.Y., Kankanhalli, A., Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems,46*(4),815-825.

Ouellette, J.A., Wood, W. (1998). Habit and intention in everyday life: The multiple processes by which past behavior predicts future behavior. *Psychological Bulletin,124*(1), 54-74.

Olmstead, K., Smith, A. *Americans and cybersecurity 2017* [Available from: http://www.pewinternet.org/2017/01/26/ americans-and-cybersecurity.]

Pahnila, S., Siponen, M., Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *40th Annual Hawaii International Conference on System Sciences,*156-166.

Pertusa-Ortega E, Zaragoza-Sara P, Claver-Cortél E. (2010). Can formalization, complexity, and centralization influence knowledge performance? *Journal of Business Researc*h, 63(3): 310-320.

Peters, L.H., O'Connor, E.J. (1980). Situational Constraints and Work Outcomes: The Influences of a Frequently Overlooked Construct. *The Academy of Management Review,5*(3),391-397.

Rhee, H.S., Kim, C., Ryu, Y.U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security,28*(8),816-826.

Rogers, R.W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology,91*(1),93-114.

Rogers, R.W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation//Cacioppo, B.L., & Petty, L.L. (eds.), *Social Psychology: A Source Book*, London: Guildford Press, pp.153-176.Safa, N.S., Von Solms, R., Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security,56,*70-82.

Symantec. *Internet security threat report 2016* [Available from: http://www.symantec.com/content/dam/symantec/ docs/ reports/istr-21-2016-en.pdf.]

Tsai, H.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., Cotton, S.R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59,*138-150.

Van Eerde, W., Thierry, H. (1996). Vroom's expectancy models and work-related criteria: A meta-analysis. *Journal of Applied Psychology,81*(5),575-586.

Vance, A., Siponen, M., Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management,49*(3),190-198.

Verplanken, B., Aarts, H. (1999). Habit, Attitude, and Planned Behaviour: Is Habit an Empty Construct or an Interesting Case of Goal-directed Automaticity? *European Review of Social Psychology,10*(1), 101-134.

Verplanken, B., & Orbell, S. (2003). Reflections on past behavior: a self-report index of habit strength. *Journal of Applied Social Psychology, 33* (6),1313-1330.

Wall, J.D., Palvia, P., & Lowry, P.B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy and Security, 9*(4), 52-79.

Wang, C., Harris, J., Patterson, P. (2013). The Roles of Habit, Self-Efficacy, and Satisfaction in Driving Continued Use of Self-Service Technologies: A Longitudinal Study. *Journal of Service Research,16*(3):400-414.

Wason, K.D., Polonsky, M.J., Hyman, M.R. (2002). Designing Vignette Studies in Marketing. *Australasian Marketing Journal,10*(3),41-58.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs,59*(4),329-349.

Wood, W., Neal, D.T. (2009). The habitual consumer. *Journal of Consumer Psychology,19*(4), 579-592.

Wood, W., Quinn, J.M. (2005) Habits and the structure of motivation in everyday life. In: Forgas, J.P., Williams, K.D., & Laham, S.M., eds. *Social motivation: Conscious and unconscious processes* (pp. 55-70). New York, NY, US: Cambridge University Press.

Wood, W., & Rünger, D. (2016). Psychology of habit. *Annual Review of Psychology, 67*,289-314.

Warkentin, M., Johnston, A.C., Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems,20*(3),267-284.

Williams, G., McGregor, H., King, D., Nelson, C., & Glasgow, R. (2005). Variation in perceived competence, glycemic control, and patient satisfaction: Relationship to autonomy support from physicians. *Patient Education and Counseling, 57*(1), 39-45.

Workman, M., Bommer, W.H., Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior,24*(6), 2799-2816.

Yoo, C.W., Sanders, G.L., & Cerveny, R.P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems, 108*, 107-118.

Yoon, C., Jae-Won, H., Kim, R. (2012). Exploring Factors That Influence Students' Behaviors in Information Security. *Journal of Information Systems Education,23*(4),407-415.