information

Article

Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks

Noor Suhani Sulaiman [1,*], Muhammad Ashraf Fauzi [1,*], Suhaidah Hussain [1] and Walton Wider [2]

[1] Faculty of Industrial Management, University Malaysia of Pahang (UMP), Gambang 26300, Malaysia
[2] Faculty of Business and Communications, INTI International University, Nilai 71800, Malaysia
* Correspondence: suhani.sulaiman@gmail.com (N.S.S.); ashrafauzi@ump.edu.my (M.A.F.)

Abstract: This study examines the factors influencing government employees' cybersecurity behavior in Malaysia. The country is considered the most vulnerable in Southeast Asia. Applying the protection motivation theory, this study addresses the gap by investigating how government employees behave toward corresponding cyberrisks and threats. Using partial least-squares structural equation modeling (PLS-SEM), 446 respondents participated and were analyzed. The findings suggest that highly motivated employees with high severity, vulnerability, response efficacy, and self-efficacy exercise cybersecurity. Incorporating the users' perceptions of vulnerability and severity facilitates behavioral change and increases the understanding of cybersecurity behavior's role in addressing cybersecurity threats—particularly the impact of the threat response in predicting the cybersecurity behavior of government employees. The implications include providing robust information security protection to the government information systems.

Keywords: cybersecurity behavior; protective motivation theory; government employee; threat awareness; protection habit

check for updates

Citation: Sulaiman, N.S.; Fauzi, M.A.; Hussain, S.; Wider, W. Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information* **2022**, *13*, 413. https://doi.org/10.3390/info13090413

Academic Editor: Jiguo Li

Received: 6 August 2022
Accepted: 24 August 2022
Published: 31 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The growth of technology has increased the number of internet users. Businesses rely entirely on the infrastructure of computer networks and underlying information systems. Organizations' reliance on information technology and the widespread use of the internet and computers necessitate the ongoing access to vital data. Such data are exposed to external cybercrime threats and the risk of information leakage [1]. The perpetrators of this cybercrime can use personal and organizational expertise, such as intellectual property and consumer data, to participate in illicit operations, such as data manipulation, for financial gain [2]. An organization must establish stringent, proactive cybersecurity procedures to safeguard their data and limit the possibilities of any data breaches [3].

Cybersecurity is a broad field that encompasses both technological and human elements. Most security breaches occur due to poor judgment, user mistakes, or a combination of the two [4]. However, poorly behaved computer users can jeopardize organizations. Numerous privacy breaches have affected millions of individuals worldwide [2]. Network intrusions include the user's lack of awareness, ignorance, negligence, resistance, apathy, and mischievousness [5]. Such reported data breaches emphasize the importance of adequate security awareness training to increase computer users' comprehension and drive positive behavioral changes.

Malaysia's internet users accounted for 87.4% of the population, ranking second in the region, and were identified as the most vulnerable to cyberattacks [6]. Malaysians have become an easy target for cybercrime, fraud, and phishing due to a lack of understanding, an inability to curb, and a failure to recognize an actual threat. Computer users' actions in defending and securing resources create vulnerabilities in the network's infrastructure.

Inadequate and inconsistent user behavior can be costly for businesses. Additionally, research reveals that businesses experience at least one data breach [7–9]. The increasing number of data breaches caused by human mistakes has altered the industry's perspective on information security [10].

To understand the determinants of an employee's cybersecurity behavior, this study examines the protection motivation theory (PMT) domains: threat appraisal and coping appraisal. This study aims to establish a link between user awareness and threat appraisal when a cyberattack is detected and the impact of habit in influencing user coping evaluation.

2. Literature Review

In recent years, the science of cyberbehavior has advanced tremendously [11]. Numerous studies have been conducted on cybersecurity behavior, most notably on human behavior, cognition, and emotion [12]. No matter how sophisticated an organization is and how much money they spend on security systems, the human element will always be the weakest link, prone to failure and error [13]. Although previous research has established a link between human characteristics and ineffective security practices, a thorough grasp of the subject remains uncommon and limited [14]. Individuals who are more likely to fall victim to cybercrime can be recognized, which benefits researchers, network security employees, organizations, and the nation.

Cybercriminals have few predetermined aims when they conduct cyberattacks. Unauthorized banking activities and credit card usage are at the top of the list [15]. Other offences include the installation of ransomware, theft of medical records, and intellectual property infringement [16]. As consumers, governments, and business owners rely extensively on the internet and cyberinfrastructure, there are growing concerns about harmful cyberactivity [17]. While user awareness has increased and expanded in lockstep with emerging technology via media and press coverage on cyberthreats, most users are exposed to unknown threats and risks [18]. These threats result from criminals constantly evolving their ideas and tactics for duping potentially vulnerable consumers.

While developing countries fundamentally lag behind their industrialized counterparts in terms of acceptance and internet use, they account for roughly two point five billion mass users compared to the latter's one billion [19]. As a developing country transitioning to developed status, Malaysia has one of the highest internet penetration rates in the region, with the Malaysian population increasing from 76.9% in 2016 to 87.4% [20]. Having a strong security system in place and an advanced understanding among the population on how to deal with cyberattacks is critical for society and the country's economic progress. Thus, understanding cybersecurity is deemed critical in recognizing threats (threat appraisal) and removing threats (coping appraisal). These domains fall under the umbrella of the PMT, which serves as the underpinning theory in this study.

2.1. Protection Motivation Theory (PMT)

The theory refers an individual's cognitive capability and processes for mediating a specific behavior in the face of danger [21]. When individuals perceive a threat, they focus on two assessment processes: the threat and their ability to overcome it. This is referred to as threat and coping evaluation.

Threat appraisal is made up of two components, which are perceived severity and perceived vulnerability. In the context of this study, perceived severity is a judgment that one makes when confronted with a threat that could result in severe damage at work or anywhere else with an internet connection [22]. If an employee perceives the seriousness of a potential attack, they may engage and take preventative action by attending training or adapting their security knowledge and practices. Individuals' perceptions of vulnerability reflect their fear of a cyberattack and their knowledge that they lack preventative procedures to thwart such attacks [1]. On the other hand, individuals with prior experience dealing with cyberattacks are less likely to be vulnerable.

A coping appraisal consists of three domains. Perceived barriers vary according to an individual's experience in dealing with cyberattacks and having prior experience would motivate them to take cybersecurity protective and preventative measures. Response efficacy is the degree to which an individual believes that a recommended response will effectively mitigate their threat [23]. They will know who can counter cyberthreats based on their experience. On the other hand, self-efficacy refers to an individual's impression of their ability to withstand a cyberattack by taking adequate precautions and coping with the threat [1].

Previous studies using PMT have shown its potential in predicting people's computer-safe behavior at home and in organizational contexts [24–26]. As a result, PMT has been used in various cybersecurity studies. There have been studies on internet users' awareness [27], undergraduate college students' desktop security behavior [28], college students' protective behavior via personal responsibility [29], online security behavior [30], and employee protection on organization information assets [31].

On the whole, based on the scant available literature on user cybersecurity behavior among government employees, this study presents a framework model comprising two significant areas that directly impact user cybersecurity behavior among Malaysian government employees by incorporating user habits and threat awareness as the antecedents of threat and coping appraisal.

2.2. Hypothesis Development and Research Model

2.2.1. Threat Awareness and Perceived Severity

Awareness of information security or comprehension of the threat to information security may result in one or more information security responses [32]. Hughes [33] found that raising employee understanding and enforcing information security regulations can help enhance organizational security attitudes. Additionally, organizations must thoroughly understand information security, including monitoring and evaluating the information security program [34]. Thus, research on information security awareness and communication has demonstrated that consistent communication about information security can benefit the organization [35]. Additionally, organizational insiders with a high level of organizational identification may feel more concerned by the repercussions of cyberattacks on the organization than those with a low level of organizational identification, even if their perceived severity is the same. An individual is aware of feasible countermeasures to such risks and should assess their feasibility in practice [28]. Thus, it is proposed that threat awareness has a positive effect on the user's perception of severity:

H1. *Threat awareness has a positive influence on the user's perceived severity.*

2.2.2. Threat Awareness and Perceived Vulnerability

Individual cybersecurity awareness, which may be usefully classified as low, medium, or high, is critical in determining information security risk. Awareness-raising entails familiarity with cyberdangers and the ability to prevent them [36]. Shaw et al. [37] described that users recognize the value of information security and its associated obligations and employ suitable information security management mechanisms to safeguard organizational data and network behavior. Meanwhile, an employee more exposed to his organization's information systems will be more prepared to take preventative measures specified as perceived vulnerability. Numerous analyses have revealed that workers' perceived vulnerability to cyberattacks pushes them to embrace cybersecurity practices [3,38]. Thus, it is proposed that threat awareness will positively influence a user's perceived vulnerability.

H2. *Threat awareness has a positive influence on the user's perceived vulnerability.*

2.2.3. Protection Habits and Perceived Barrier

Habit is a significant antecedent of individual cybersecurity behavior [1]. Habit refers to a pattern of conduct measured using previous behavior or behavioral frequency. Integrating habits within the coping appraisal domain has been shown to predict individual cybersecurity behavior [39]. Perceived barriers are utilized to determine the inconvenience associated with cybersecurity issues. It is inextricably linked to preventive protection behavior. The perceived barriers to behavior change are critical when analyzing behavioral change [40]. In addition, perceived impediments add to the perceived cost and the complexity of conducting cybersecurity operations individually [25]. Individuals' perceptions of data protection challenges in cybersecurity are based on their prior experiences. As cybersecurity prevention methods were implemented, it was observed that the perceived low barriers were influenced by their prior experience. Thus, the following hypothesis is presented:

H3. *Protection habits have a negative influence on the user's perceived barrier.*

2.2.4. Protection Habits and Response Self-Efficacy

Within the PMT framework, a deeper understanding of the behaviors and routine of those behaviors, which is protection habits, could assist in delivering new insights and increasing the model's predictive potential [41]. Prior research has examined habit from three viewpoints in light of these arguments: the moderating influence of habit on the relationship between intention and information technology usage, the direct effect of habit on information technology use, and the direct effect of habit on intentions to use information technology [42]. Vance et al. [1] stated that many acts occur automatically and are completed because individuals are accustomed to completing them; frequently repeated behavior is more influenced by situational signals than conscious decision-making. In the context of cybersecurity awareness, the response efficacy refers to the amount workers believe that the proposed remedies will significantly reduce their level of risk [43] and the effectiveness of the recommended behavior in eradicating or averting possible harm [44]. Additionally, the same study discovered a substantial correlation between employee response efficacy and their plans to adopt cybersecurity measures. Hence, the following hypothesis is drawn:

H4. *Protection habits have a positive influence on the user's response self-efficacy.*

2.2.5. Protection Habits and Security Response Efficacy

Security response efficacy relates to an individual's belief in the effectiveness of protective action in repelling a threat. Individuals skeptical about the efficacy of protective action as a security reaction are less likely to utilize it [41]. An argument in a fear appeal will drive an individual to create efficacy cognitions [45]. The former is referred to as security response efficacy, which relates to how effectively a person believes the reaction is addressing a cyberthreat [46]. Meso et al. [44] stated that it is the belief that the proposed conduct can be successfully implemented. It is an individual's assessment of their capacity to withstand a cybersecurity attack by implementing proper safeguards and coping with the threat [1]. A positive cybersecurity behavioral habit can help prevent and protect individuals from cyber-related incidents.

Meanwhile, harmful cybersecurity behavioral habits can expose individuals to additional cybersecurity threats. However, some studies in information security behavior have recognized the importance of habits [30,47]. Findings suggest habits have been found to predict intentions to follow information system security policies. A person with a high level of reaction efficacy regarding cybersecurity behaviors will strongly believe in his or her ability to avert cyberattacks successfully. This will increase the likelihood of previously practiced cybersecurity activities being repeated with a goal in mind [48]. As a result, we proposed the following hypothesis:

H5. *Protection habits have a positive influence on the user's security response efficacy.*

2.2.6. Perceived Severity and Cybersecurity Behavior

Perceived severity can be defined as the individual perception of an event's consequence [44]. It is related to trust in the magnitude of the consequences of the circumstances [49]. Previous research indicates that the perceived severity of the penalty has a detrimental effect on one's willingness to abuse information systems [50]. The perceived severity is determined in response to a dangerous security event [30]. The higher one's perceived threat, the more probable it is that online users will be protected [29]. Employee's perceptions of the severity of cyberrisks significantly impact their safety concerns [51]. Subsequently, perceived severity effectively reduces information infrastructure misuse [52]. Furthermore, individual behavior depends on the perceived severity of the impact, which increases a consumer's desire to take action to mitigate the threat, thus reducing the likelihood of threats [53,54]. Hence, we propose the following hypothesis:

H6. *Perceived severity has a positive influence on the user's cybersecurity behavior*.

2.2.7. Perceived Vulnerability and Cybersecurity Behavior

Employee vulnerability is another dimension of cybersecurity threat assessment. Employees who believe their company's information system is at risk are more likely to take preventive steps. According to certain studies, employees' perceived vulnerability to cyberattacks motivates them to adhere to cybersecurity regulations [38]. Perceived vulnerability is a person's assessment of the possibility of being confronted with threatening situations, such as becoming a victim of cybercrime [3]. For example, in e-mail security, perceived vulnerability to malicious attachments has been connected to computer security behavior [55]. As a result, De Kimpe et al. [56] hypothesized that perceived cybercrime vulnerability would be linked to a protective motive in the same way.

H7. *Perceived vulnerability has a positive influence on the user's cybersecurity behavior*.

2.2.8. Perceived Barrier and Cybersecurity Behavior

Perceived barriers refer to an employee's perceived annoyance and cost associated with cybersecurity protection activities [22]. It was found that perceived barriers have a detrimental effect on users' behavior in computer security [57]. Perceived barriers can be depicted in terms of aggravation, time constraints and addiction that influence user behavior. Employees consider perceived hurdles a challenge they must overcome, lowering their commitment to comply with cybersecurity regulations and take preventative action [22]. Therefore, the following hypothesis is developed:

H8. *Perceived barrier has a negative influence on the user's cybersecurity behavior*.

2.2.9. Response Self-Efficacy and Cybersecurity Behavior

Situational supports such as interpersonal assistance, supervisor or colleague support, and appropriate time for practice behaviors would be conducive to individual self-efficacy in information security behaviors [58]. Self-efficacy benefits from using protective information technologies [59]. Individuals' decisions to engage in cybersecurity behavior are influenced by their perception of the probability of good consequences [60]. Surroundings and the environment provide individuals adequate situational support to increase self-efficacy, influencing information security practices [48]. Thus, the following hypothesis is proposed:

H9. *Response self-efficacy has a positive influence on the user's cybersecurity behavior*.

2.2.10. Security Response Efficacy and Cybersecurity Behavior

Users who benefit from better privacy due to a personalization platform will have fewer privacy concerns specific to the system and will be more receptive to using it as a tool

for privacy [61]. Self-efficacy and response efficacy are critical components of frameworks that attempt to explain the process by which cybersecurity activities become habits. They are frequently used to explain the establishment of information security behaviors [62]. Individuals with high self-efficacy to engage in cybersecurity behaviors will be strongly correlated. Consequently, individuals demonstrating a high level of reaction efficacy will firmly believe in their ability to prevent cyberattacks. This will increase the likelihood of previously practiced cybersecurity activities with a predetermined goal [48]. Based on this, the following hypothesis is developed:

H10. *Security response efficacy has a positive influence on the user's cybersecurity behavior.*

The following Figure 1 illustrates the study research model.

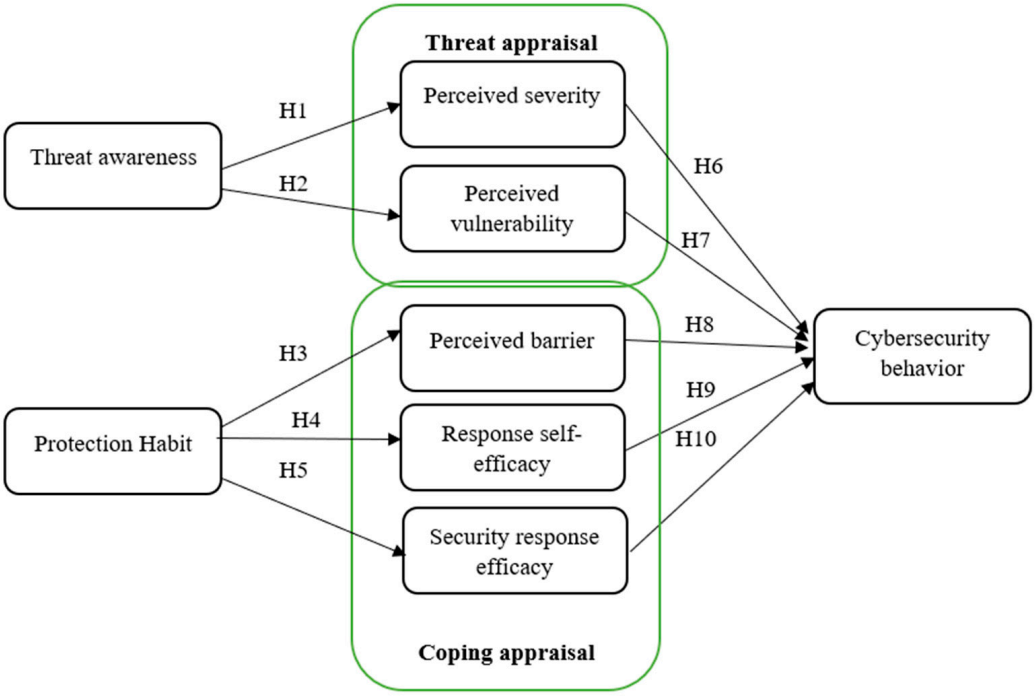

Figure 1. Research model.

3. Methodology

3.1. Data Collection

This study used a quantitative research design through a self-administered questionnaire. The study used an online poll to collect data from a representative sample of government employees in Malaysia who were also internet users. A quota sampling of 20:30:50 was used to collect 446 respondents from government employees of Malaysia. A total of 78 respondents were gathered from top management, 229 respondents were collected from middle management, and 325 were obtained from supporting staff.

GPower 3.1.9.7 software [63] was used in this study to determine the population impact measurement based on the model to be tested. This software can calculate the minimum number of respondents needed for the survey. This study required a minimum sample size of 153 samples. Figure 2 depicts the analysis performed with GPower software to determine the sample size for testing the model. Thus, based on the sample size calculation (Krecjie & Morgan, 1970), 384 samples will be obtained out of the 446 samples to be collected.

$$s = X^2\ N\ P\ (1 - P)/d^2\ (N - 1) + X^2\ P\ (1 - P)$$

where,

s—Required sample size.

X^2—The table value of chi-square for 1 degree of freedom at the desired confidence level (0.05 = 3.841).

N—The population size.

P—The population proportion (assumed to be 0.50 since this would provide the maximum sample size.

D—The degree of accuracy expressed as proportion (0.05).

$$s = \frac{3.841^2(1,600,000 \times 0.5)(1–1,600,000)}{0.05^2(1,600,000-1) + 3.841^2 \times 1,600,000(1–1,600,000)}$$

s = 384 samples

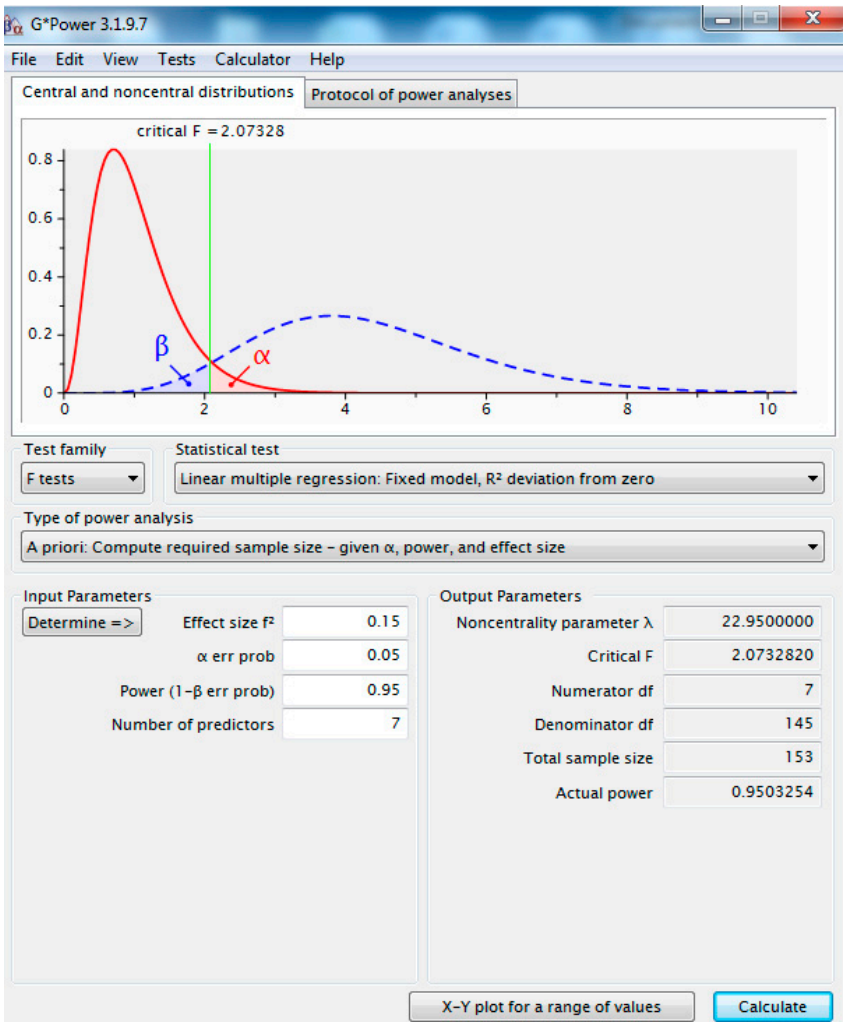

Figure 2. Sample size calculation using G Power 3.1.9.7.

3.2. Measure

The study used a quantitative design in which data were acquired from primary sources of information. A closed-ended survey questionnaire based on the 7-point Likert scale was used as the instrument. The instrument contains eight variables quantified using a seven-point Likert scale, ranging from 1—strongly disagree to 7—strongly agree. The scale for perceived severity and perceived vulnerability were adapted from Burns et al. [11]. Safa et al. [5] adapted the scale for cybersecurity awareness. Next, perceived barrier items were adapted from Li et al. [22]. Both response self-efficacy and security response efficiency were adapted from Hina et al. [64]. Meanwhile, protection habit items were adapted

from Dutton et al. [65]. Lastly, the cybersecurity protection behaviors were adapted from Anwar et al. [66].

4. Result and Analysis

The partial least-squares structural equation modeling (PLS-SEM) was performed using SmartPLS version 3.2.8 [67] to examine the relationship between the variables. PLS-SEM is preferable to covariance-based SEM (CB-SEM) for measurement estimation models and multigroup analysis [68]. The primary reason we employed PLS-SEM was due to the study's exploratory nature. The PLS-SEM approach was also employed in light of the current study's complex model [69], employing a predictive study [70] and data abnormalities [71]. Hence, PLS-SEMm better fit the study's aims than CB-SEM.

4.1. Demographic Information

The demographic data are presented in Table 1. According to the quota sampling, the majority of the respondents were middle management staff (49%), supporting staff (34%), and top management (17%). This final sampling occurred by the ratio sampling strategy.

Table 1. Demographic Information.

Categories	Type	Frequency (n)	Percentage (%)
Gender	Male	276	59
	Female	191	41
Age	21–25	10	2
	26–30	31	7
	31–35	64	14
	36–40	123	26
	41–45	122	26
	46–50	63	13
	51–55	38	8
	More than 56	16	3
Ethnicity	Malay	416	89
	Chinese	8	2
	Indian	8	2
	Sabah native	18	4
	Sarawak native	14	3
	Others	3	1
Position	Top Management	78	17
	Middle Management	229	49
	Support Staff	160	34
Type of computer protection that use at work	Antivirus	415	89
	Antimalware	219	47
	Firewall	320	69
	Virtual Private Network (VPN)	220	47
	Pop-up blockers	229	49
	Others	43	9
	I'm not using any computer protection at work	7	1

In terms of gender, an equal distribution of males (59%) and females (41%) was achieved. Furthermore, the majority of respondents were Malay (89%), with the remainder comprising Sabah natives (4%), Sarawak natives (3%), Chinese and Indian (2% each), and others (1%). Based on the type of computer protection at work, antivirus was the most used (89%), followed by firewalls (69%), pop-up blockers (49%), antimalware and VPNs, (each obtaining 47%), and others (9%).

4.2. Common Method Bias

This study used a statistical technique to address a prevalent method bias that frequently occurs in behavioral research [72]. According to Kock [73], a comprehensive collinearity test can be performed to analyze common method bias in PLS-SEM. A variance inflation factor (VIF) of less than 3.3 does not exhibit common method bias. This model has no serious issues, as all latent constructs have VIF values of less than 3.3, as determined by the full collinearity test shown in Table 2.

Table 2. Full Collinearity.

Construct	CSB	PB	PS	PV	PH	RSE	SRE	TA
VIF	2.564	1.263	1.532	1.661	3.304	2.094	1.326	1.665

CSB = cybersecurity behavior; PB = protection barrier; PS = perceived severity; PV = perceived vulnerability; PH = protection habit; RSE = response self-efficacy; SRE = security response efficacy; TA = threat awareness.

4.3. Measurement Model

We tested the model built using a 2-step approach according to Anderson and Gerbing's [74] recommendations. We tested the measurement model first to ensure the validity and reliability of the instruments employed [75,76].

We evaluated the measurement model's loadings, average variance extracted (AVE), and composite reliability (CR). The loadings values should be $\geq$0.5, the CR should be $\geq$0.7, and the AVE should be $\geq$0.5 [75]. According to Urbach and Ahlemann [69], an indicator is dependable if it accurately measures what it is designed to measure. The dependability of indicators is determined by determining the extent to which they are consistent with the metric they are intended to measure. Typically, convergent validity can be assessed by examining the average variance extracted (AVE). Convergent validity establishes a relationship between two measures measuring the same construct. Henseler et al. [77] emphasized the importance of a construct's AVE being at least 0.5 to achieve convergent validity. Based on Table 3, four loadings on cybersecurity behavior items were less than 0.708, which was likewise acceptable [75]. The AVEs were all greater than 0.5, indicating convergent validity. The CR were all greater than 0.7, indicating acceptable internal consistency reliability.

Table 3. Reliability and validity analysis.

Construct	Items	Loadings	Composite Reliability	Average Variance Extracted (AVE)
Threat Awareness	ACS1	0.843	0.879	0.644
	ACS2	0.744		
	ACS3	0.803		
	ACS4	0.819		
Cybersecurity behaviors	CSPB1	0.662	0.891	0.507
	CSPB2	0.719		
	CSPB3	0.785		
	CSPB4	0.697		
	CSPB5	0.645		
	CSPB6	0.689		
	CSPB7	0.768		
	CSPB8	0.719		
Perceived Barriers	PB1	0.798	0.904	0.703
	PB2	0.901		
	PB3	0.873		
	PB4	0.774		

Table 3. *Cont.*

Construct	Items	Loadings	Composite Reliability	Average Variance Extracted (AVE)
Protection habit	PH1	0.889	0.922	0.575
	PH2	0.888		
	PH3	0.861		
	PH4	0.683		
	PH5	0.865		
	PH6	0.6		
	PH7	0.737		
	PH8	0.717		
	PH9	0.471		
Perceived Severity	PS1	0.907	0.923	0.749
	PS2	0.906		
	PS3	0.802		
	PS4	0.842		
Perceived Vulnerability	PV1	0.864	0.95	0.827
	PV2	0.917		
	PV3	0.92		
	PV4	0.936		
Response Self-Efficiency	RSE1	0.851	0.892	0.675
	RSE2	0.859		
	RSE3	0.746		
	RSE4	0.825		
Security Response Efficiency	SRE1	0.942	0.966	0.876
	SRE2	0.954		
	SRE3	0.949		
	SRE4	0.897		

The discriminant validity was then examined in step two using the HTMT criterion [77]. The HTMT values should be $\leq$0.85 for the stricter criterion, and the more lenient criterion should be $\leq$0.90 [76]. As this study is an exploratory study, all the values must be less than the HTMT0.90 threshold value, indicating good discriminant validity. Table 4 indicated that the HTMT values were lower than the stricter criterion of $\leq$0.85, implying that the respondents recognized the eight constructs as being separate constructs, thus indicating substantial discriminant validity.

Table 4. Heterotrait-Monotrait Ratio of Correlations (HTMT).

Construct	CSB	PB	PS	PV	PH	RSE	SRE	TA
CSB								
PB	0.297							
PS	0.155	0.282						
PV	0.076	0.405	0.624					
PH	0.888	0.261	0.141	0.046				
RSE	0.666	0.171	0.105	0.08	0.779			
SRE	0.398	0.132	0.077	0.171	0.416	0.478		
TA	0.601	0.122	0.204	0.117	0.667	0.615	0.399	

4.4. Structural Model Assessment

After establishing the measurement model, we proceeded with evaluating the structural model as shown in Figure 3. Bootstrapping was utilized to create results for each path relationship in the model by reinstating the initial sample to generate a bootstrap sample and provide standard errors for each hypothesis tested [70]. Chin [78] recommended performing bootstrapping with 1000 resamples concerning the number of resamples.

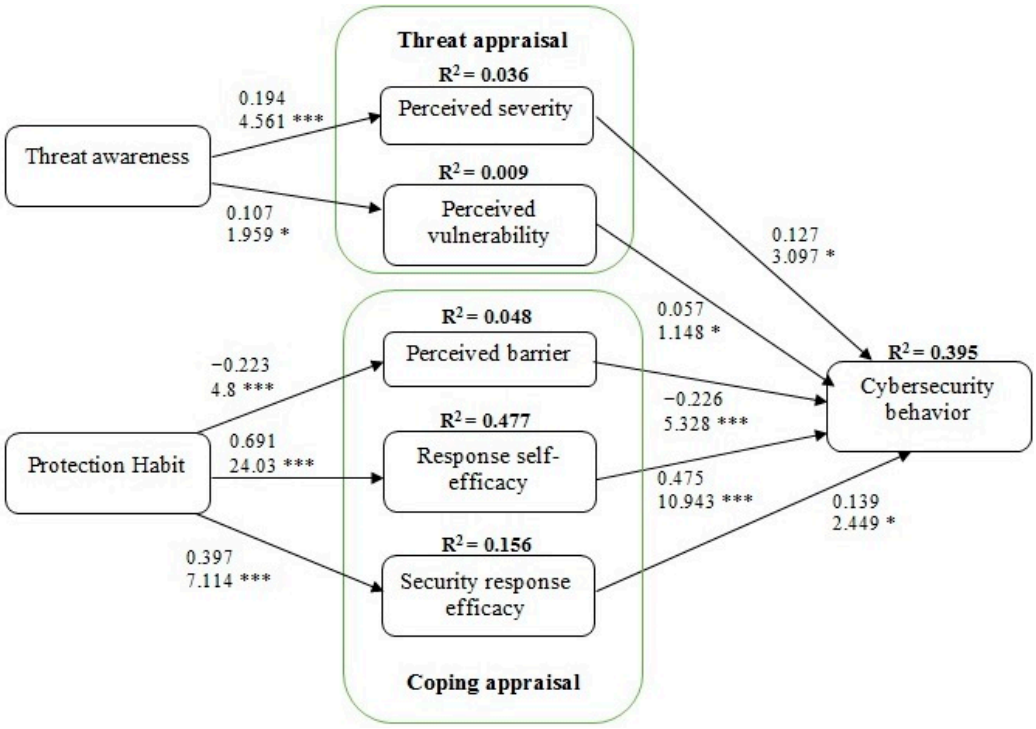

Figure 3. Results of the structural model. Note: * $p < 0.05$; *** $p < 0.001$.

To validate the model against the hypotheses, the path coefficient between exogenous and endogenous variables (β-value), t-values, and squared multiple correlations (R2) were analyzed to determine the explained variation on the endogenous variable. First, we tested the effects of TA on PS and PV. The R2 was 0.036 and 0.009, which showed 36% and 9% of the explained variance in CSB. PS (β = 0.194, $p < 0.01$) and PV (β = 0.107, $p < 0.01$), were positively related to CSB; thus, H1 was supported while H2 was not. Next, we tested the effects of PH on PB, RSE, and SRE. The R2 values were 0.048, 0.477, and 0.156, which showed that the explained variances of PH were 48%, 47.7%, and 15.6%, respectively. PB (β = −0.223, $p < 0.01$), RSE (β = 0.691, $p < 0.01$), and SRE (β = 0.397, $p < 0.01$), were all positively significant, hence supporting H3, H4, and H5. Lastly, the R2 for the effect of the five predictors on CSB was 0.398, indicating that the five predictors explained 39.8% of the variance in CSB. PS (β = 0.127, $p < 0.01$), PV (β = 0.057, $p < 0.01$), PB (β = −0.226, $p < 0.01$), RSE (β = 0.475, $p < 0.01$), and SRE (β = 0.139, $p < 0.01$), were all positively related to CSB, except for PV. Thus, H6, H8, H9, and H10 were supported, except for H7. Table 5 summarizes the result of hypothesis testing.

Table 5. Summary of the structural model.

Hypothesis	Relationship	Path Coefficient, β	T Value	*p* Value	BCI LL	BCI UL	Effect Size, f2	Decision
H1	TA → PS	0.194	4.561	0	0.128	0.285	0.039	Supported
H2	TA → PV	0.107	1.959	0.05	−0.007	0.214	0.012	Not Supported
H3	PH → PB	−0.223	4.8	0	−0.318	−0.137	0.052	Supported
H4	PH → RSE	0.691	24.03	0	0.636	0.747	0.915	Supported
H5	PH → SRE	0.397	7.114	0	0.294	0.507	0.187	Supported
H6	PS → CSB	0.127	3.097	0.002	0.05	0.206	0.018	Supported
H7	PV → CSB	0.057	1.148	0.251	−0.049	0.15	0.003	Not Supported
H8	PB → CSB	−0.226	5.328	0	−0.309	−0.145	0.073	Supported
H9	RSE → CSB	0.475	10.943	0	0.386	0.557	0.3	Supported
H10	SRE → CSB	0.139	2.449	0.015	0.034	0.25	0.026	Supported

BCI LL = Bias confidence interval lower limit; BCI UL = Bias confidence interval upper limit.

5. Discussion

The PMT model incorporates two domains of coping and threat appraisals. The findings depicted that all PMT variables significantly impacted cybersecurity behavior except for perceived vulnerability. However, PMT was highlighted as one of the most convincing justifications for a person's decision to take precautions [26]. Furthermore, this study found that coping and threat appraisal positively affects the cybersecurity behavior of government employees in Malaysia. According to PMT, this is consistent with previous research indicating that individual variables can induce protective behaviors [79]. In light of this, a person's perceived vulnerability is an assessment of whether they believe they could be at risk for dangers [32]. Moreover, Ifinedo [3] discovered that perceived severity is utilized to gauge how well users comprehend the severe repercussions of potentially harmful cybersecurity acts. Meanwhile, consumer confidence in the danger of cyberthreats is gauged using perceived vulnerabilities. Employees' perceptions of the severity and vulnerability of cybersecurity incidents are also positively impacted [22].

Regardless of technological advancements, the human aspect is considered the security system's weakest link due to people's ignorance and lack of security concerns [80]. This study discovered that threat awareness positively influences users' perceived severity. Similar to the recent study by Li et al. [22], perceived severity is a judgment made when confronted with a threat on cyber-related activities. In order to mitigate security risks, security awareness courses and training are required. Meanwhile, this study discovered that threat awareness does not influence a user's perceived vulnerability. According to Aldossary and Zeki [81], internet users with moderate security awareness use weak passwords, open email attachments from unfamiliar senders, and other unprotective behavior. Even though they were aware of the risks, they undervalued them.

The most significant factors to consider when analyzing behavioral change are the perceived barriers [40]. They contribute to individuals' perceptions of the cost and difficulty of conducting cybersecurity activities [25]. Individuals' perceptions of cybersecurity data protection barriers are based on their prior experiences, and it was observed that the low barriers they perceived were influenced by their previous experiences. Ye and Potter [82] proved that personal habits could mitigate the impact of other beliefs on certain services. Meanwhile, Barnes and Boheinger [83] discovered that habit is a significant predictor of continuing use intention for internet users. Thus, this study discovered that protection habits negatively influence users' perceived barriers.

A habit may be seen as an automatic behavioral response generated by a situational stimulus that does not require cognitive processing due to the learned relationship between one behavior and pleasing outcomes [84]. As a result, habit formation necessitates an inevitable repetition or practice level [85]. Once a habit is established, behavior becomes automatic [86]. However, the extent to which habits are utilized in study models differs. While some researchers argue that habits act as moderators in the link between intention and its determinants [87,88], others assert that habits have a direct effect on the intention to use the internet [83,89].

Additionally, Vance et al. [1] demonstrate that reaction efficacy is the belief in the perceived benefits of the coping behavior due to the danger being removed. Meanwhile, self-efficacy refers to an individual's belief in his or her ability to carry out protective behaviors. As a result, this study discovered that regular compliance with cybersecurity policies benefits self-efficacy and response efficacy.

This study finds that perceived barriers have a negative influence on online security behaviors as expected. The construct reflects an individual's fear of the challenges of adopting a new behavior, and it is directly related to proactive security behaviors [90]. It was also posited that if habits could be deactivated as quickly as they are developed, they would not provide a barrier to changing behavior [91]. Once developed, a habit affects how we look for and process information. Finally, user resistance results from perceived barriers such as inconvenience, time commitment, and habit change.

6. Implications

6.1. Theoretical Implications

This study emphasizes the protective coping appraisal of employees' cybersecurity behavior. The study reported similar findings on the reliability of PMT in understanding and predicting employee security behavior as reported in the literature [1,3,21,27,28,30,44]. Meanwhile, Burns et al. [11] claimed that cybersecurity behavior has largely overlooked positive coping mechanisms, such as self-efficacy, and has framed security motivation exclusively in terms of fear appeals. We discovered that the coping features of PMT were more significant on an employee's cybersecurity behavior than threat appeals. Hanus and Wu [28] observed that three coping appraisal variables (perceived barrier, self-efficacy, and response-efficacy) were significant predictors of reported security behavior.

In contrast, the threat elements (perceived severity and perceived vulnerability) did not. As a result, government employees in Malaysia can engage in specific behaviors and assess their capacity to implement the cybersecurity behaviors outlined. However, they are ignorant of the threat to user perceptions since they do not consider themselves vulnerable to cyberthreats.

A habit is a significant predictor of human behavior and conduct. Cybersecurity behavior research can help provide new viewpoints to render more comprehensive explanations of the mechanisms behind establishing cybersecurity habits [48]. Furthermore, situational conditions play a significant role in habit formation, and the frequency with which a behavior is displayed cannot entirely explain the self-consciousness that habits imply [39]. Thus, in this study, we attempted to define habit formation in terms of the influence of significant situational factors, which refer to the range of relevant situations that an individual has previously faced.

This study contributes significantly to the body of knowledge by presenting the theory of cybersecurity behavior as a strong predictor of coping and threat evaluation processes. This demonstrates that it is not sufficient to establish a "fear appeal" [45] in the hope of inspiring people to act when undertaking threat awareness. Users are more likely to be motivated if they are aware of and confident in using precautionary measures. While technology has increased both locally and globally in recent years, effective cybercrime awareness must be considered [92]. This study concludes that Malaysian government employees are accountable for increasing cybersecurity awareness among their constituents. As a result, governments must contribute to the fight against cybercrime through their different authorities and organizations.

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation, as well as the experimental conclusions that can be drawn.

6.2. Practical Implications

The outcome of this study would provide empirical insights into reducing the unfavorable consequences of cyberthreats on the user in Malaysia. Policymakers and government bodies such as the Malaysian Communications and Multimedia Commission can create effective regulations on human behavior relating to direct connection with cyberconnected practices. On the ground, individuals within organizations who interact closely with end users (network engineers, programmers, and others) would determine the most critical antecedents with high risk or associated aspects that can withstand cyberattacks.

This study's findings may help protect society from cyberattacks such as phishing, fraud, and other cyberrisks. As the region's most susceptible country, Malaysia needs a comprehensive solution to this issue to prevent being readily targeted by criminals and fraudsters. Aside from technological and physical safeguards, governments and industry partners should intervene and establish methods to increase people's cybersecurity protection. Furthermore, investors want to invest in countries that are perceived to be safe and stable. The country's goal of being recognized as a haven for cyberusers may be accomplished by increasing cybersecurity via user behavior.

7. Recommendation for Future Works

Even though the level of technology has gone up in the last few years worldwide, the awareness of cybercrime needs to be effectively taken into account. This study examines the factors influencing Malaysia's employees' cybersecurity behavior using PMT. It is used to elucidate the individual beliefs that contribute to the adoption of security behavior and how instruction influences them. The proposed model is a good predictor of security behavior. In this sense, our research lays the groundwork for fostering acceptable long-term individual behavior in system security.

Besides that, future work should dig deeper into the knowledge gap regarding cybersecurity behaviors to adopt and evaluate the efficiency of various coping messages for individuals with varying levels of cybersecurity literacy. This would necessitate a more nuanced application of PMT to comprehend how interventions might target self- and response-efficacy knowledge and beliefs. This study also provides insight into how small behavioral encouragement can result in more significant security effects.

8. Conclusions

From the perspectives of PMT, threat awareness, and habit, this study shed insight into how government personnel behave in the face of cyberattacks. The rising usage of tablets and smartphones for personal and financial information underscores the need for more information security research focusing on cybersecurity behavior. The study adequately predicts Malaysian government employee cybersecurity behavior. Factors ranging from threat knowledge to perceived severity and vulnerability, protection habits to the perceived barrier, self-efficacy, and response efficacy contribute to a government employee of Malaysia's cybersecurity behavior. Furthermore, cybersecurity is a crucial issue in today's organizations, especially in a government department where in certain departments there are sensitive and highly confidential data related to national security. Cybersecurity measures, particularly human behavior, must be further reinforced to ensure the Malaysian government is regarded as a cybercrime-protected government agency.

Author Contributions: Conceptualization, N.S.S. and M.A.F.; methodology, N.S.S. and M.A.F.; software, N.S.S. and M.A.F.; validation, N.S.S. and M.A.F.; formal analysis, N.S.S. and M.A.F.; investigation, N.S.S. and M.A.F.; resources, N.S.S. and M.A.F.; data curation, N.S.S.; writing—original draft preparation, N.S.S.; writing—review and editing, M.A.F., W.W. and S.H.; visualization, N.S.S. and M.A.F.; supervision, M.A.F.; project administration, N.S.S.; funding acquisition, M.A.F. All authors have read and agreed to the published version of the manuscript.

Funding: Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme FRGS RACER/1/2019/SS03/UMP//1 (University Grant no. RDU192619).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Vance, A.; Siponen, M.; Pahnila, S. Motivating IS security compliance: Insights from habit and protection motivation theory. *Inf. Manag.* **2012**, *49*, 190–198. [CrossRef]
2. Hammond, S.T. Threat and Coping Appraisals on Information Security Awareness Training Effectiveness: A Quasi-Experimental Study. Ph.D. Thesis, Capella University, Minneapolis, MN, USA, 2019.
3. Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Comput. Secur.* **2012**, *31*, 83–95. [CrossRef]
4. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining cybersecurity. *Technol. Innov. Manag. Rev.* **2014**, *4*, 13–21. [CrossRef]
5. Safa, N.S.; Sookhak, M.; Von Solms, R.; Furnell, S.; Ghani, N.A.; Herawan, T. Information security conscious care behaviour formation in organizations. *Comput. Secur.* **2015**, *53*, 65–78. [CrossRef]

6. MCMC. Internet Users Survey 2020: Malaysian Communications And Multimedia Commission: 2020; Cyberjaya, Selangor, Malaysia. pp. 25–39. Available online: https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/IUS-2020-Report.pdf (accessed on 5 August 2022).
7. Arlitsch, K.; Edelman, A. Staying safe: Cyber security for people and organizations. *J. Libr. Adm.* **2014**, *54*, 46–56. [CrossRef]
8. Montesdioca, G.P.Z.; Maçada, A.C.G. Measuring user satisfaction with information security practices. *Comput. Secur.* **2015**, *48*, 267–280. [CrossRef]
9. Willison, R.; Warkentin, M. Beyond deterrence: An expanded view of employee computer abuse. *MIS Q.* **2013**, *37*, 1–20. [CrossRef]
10. Shahraki, A.S.; Nikmaram, M. Human errors in computer related abuses. *J. Theor. Appl. Inf. Technol.* **2013**, *47*, 93–97.
11. Burns, A.J.; Posey, C.; Roberts, T.L.; Lowry, P.B. Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Comput. Hum. Behav.* **2017**, *68*, 190–209. [CrossRef]
12. Yan, Z.; Robertson, T.; Yan, R.; Park, S.Y.; Bordoff, S.; Chen, Q.; Sprissler, E. Finding the weakest links in the weakest link: How well do undergraduate students make cyber security judgment? *Comput. Hum. Behav.* **2018**, *84*, 375–382. [CrossRef]
13. Gratian, M.; Bandi, S.; Cukier, M.; Dykstra, J.; Ginther, A. Correlating human traits and cyber security behaviour intentions. *Comput. Secur.* **2018**, *73*, 345–358. [CrossRef]
14. Egelman, S.; Harbach, M.; Peer, E. Behaviour ever follows intention? A validation of the Security Behaviour Intentions Scale (SeBIS). In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 7–12 May 2016; pp. 5257–5261.
15. Lee, S.K.; Kang, T.I. Adaptive multi-layer security approach for cyber defense. *J. Internet Comput. Serv.* **2015**, *16*, 1–9.
16. Torten, R.; Reaiche, C.; Boyle, S. The impact of security awarness on information technology professionals' behaviour. *Comput. Secur.* **2018**, *79*, 68–79. [CrossRef]
17. Ravindran, S.K. *Impact of Probable and Guaranteed Monetary Value on Cyber Security Behaviour of Users*; Missouri University of Science and Technology: Rolla, MO, USA, 2018.
18. Furnell, S.; Clarke, N. Power to the people? The evolving recognition of human aspects of security. *Comput. Secur.* **2012**, *31*, 983–988. [CrossRef]
19. Kabanda, S.; Tanner, M.; Kent, C. Exploring SME cyber security practices in developing countries. *J. Organ. Comput. Electron. Commer.* **2018**, *28*, 269–282. [CrossRef]
20. MCMC. Internet Users Survey 2018: Statistical Brief Number Twenty-Three. Internet Users Surv. 2018; pp. 1–39. Available online: https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018.pdf (accessed on 1 February 2020).
21. van Bavel, R.; Rodríguez-Priego, N.; Vila, J.; Briggs, P. Using protection motivation theory in the design of nudges to improve online security behaviour. *Int. J. Hum.-Comput. Stud.* **2019**, *123*, 29–39. [CrossRef]
22. Li, L.; He, W.; Xu, L.; Ash, I.; Anwar, M.; Yuan, X. Investigating the impact of cyber security policy awareness on employees' cyber security behaviour. *Int. J. Inf. Manag.* **2019**, *45*, 13–24. [CrossRef]
23. Boss, S.R.; Galletta, D.F.; Lowry, P.B.; Moody, G.D.; Polak, P. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviours. *MIS Q.* **2015**, *39*, 837–864. [CrossRef]
24. Lee, Y.; Larsen, K.R. Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *Eur. J. Inf. Syst.* **2009**, *18*, 177–187. [CrossRef]
25. Ng, B.Y.; Xu, Y. Studying users' computer security behavior using the Health Belief Model. In Proceedings of the PACIS 2007—11th Pacific Asia Conference on Information Systems: Managing Diversity in Digital Enterprises, Auckland, New Zealand, 4–6 June 2007.
26. Anderson, C.L.; Agarwal, R. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Q.* **2010**, *34*, 613–643. [CrossRef]
27. Shillair, R.; Cotten, S.R.; Tsai, H.Y.S.; Alhabash, S.; LaRose, R.; Rifon, N.J. Online safety begins with you and me: Convincing Internet users to protect themselves. *Comput. Hum.* **2015**, *48*, 199–207. [CrossRef]
28. Hanus, B.; Wu, Y.A. Impact of users' security awareness on desktop security behaviour: A protection motivation theory perspective. *Inf. Syst. Manag.* **2016**, *33*, 2–16. [CrossRef]
29. Boehmer, J.; LaRose, R.; Rifon, N.; Alhabash, S.; Cotten, S. Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behav. Inf. Technol.* **2015**, *34*, 1022–1035. [CrossRef]
30. Tsai, H.Y.S.; Jiang, M.; Alhabash, S.; LaRose, R.; Rifon, N.J.; Cotten, S.R. Understanding online safety behaviours: A protection motivation theory perspective. *Comput. Secur.* **2016**, *59*, 138–150. [CrossRef]
31. Posey, C.; Roberts, T.L.; Lowry, P.B. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *J. Manag. Inf. Syst.* **2015**, *32*, 179–214. [CrossRef]
32. Yoon, C.; Hwang, J.W.; Kim, R. Exploring Factors That Influence Students' Behaviors in Information Security. *J. Inf. Syst. Educ.* **2012**, *23*, 407–416.
33. Hughes, A. Student Information Security Behaviours and Attitudes at a Private Liberal Arts University in the Southeastern United States. Ph.D. Thesis, Northcentral University, San Diego, CA, USA, 2016.
34. Siau, K.; Hall, R. *Impact of Framing and Base Size of Computer Security Risk Information on User Behavior*; Faculty of the Graduate School of the Missouri University of Science and Technology: Rolla, MO, USA, 2019.
35. Mishra, A.; Awal, A.; Elijah, J.; Rabiu, I. An Assessment of the Level of Information Security Awareness among Online Banking Users in Nigeria. *Int. J. Comput. Sci. Mob. Comput.* **2017**, *6*, 373–387.

36. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behaviour: A comparative study. *J. Comput. Inf. Syst.* **2022**, *62*, 82–97.
37. Shaw, R.S.; Chen, C.C.; Harris, A.L.; Huang, H.J. The impact of information richness on information security awareness training effectiveness. *Comput. Educ.* **2009**, *52*, 92–100. [CrossRef]
38. Siponen, M.; Adam Mahmood, M.; Pahnila, S. Employees' adherence to information security policies: An exploratory field study. *Inf. Manag.* **2014**, *51*, 217–224. [CrossRef]
39. Verplanken, B.; Orbell, S. Reflections on past behaviour: A self-report index of habit strength 1. *J. Appl. Soc. Psychol.* **2003**, *33*, 1313–1330. [CrossRef]
40. Djatsa, F. How Perceived Benefits and Barriers Affect Millennial Professionals' Online Security Behaviours. *J. Inf. Secur.* **2019**, *10*, 278–301.
41. Shillair, R.J. Mind the Gap: Perceived Self-Efficacy, Domain Knowledge and Their Effects on Responses to a Cyber Security Compliance Message. Ph.D. Thesis, Michigan State University, East Lansing, MI, USA, 2018.
42. Venkatesh, V.; Thong, J.Y.; Xu, X. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Q.* **2012**, *36*, 157–178. [CrossRef]
43. Alghamdi, M.I. Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. Mater. *Today Proc.* **2021**. [CrossRef]
44. Meso, P.; Ding, Y.; Xu, S. Applying protection motivation theory to information security training for college students. *J. Inf. Priv. Secur.* **2013**, *9*, 47–67. [CrossRef]
45. Johnston, A.C.; Warkentin, M. Fear appeals and information security behaviours: An empirical study. *MIS Q.* **2010**, *34*, 549–566. [CrossRef]
46. Warkentin, M.; Johnston, A.C.; Shropshire, J. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *Eur. J. Inf. Syst.* **2011**, *20*, 267–284.
47. Pahnila, S.; Siponen, M.; Mahmood, A. Employees' behaviour towards IS security policy compliance. In Proceedings of the 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Waikoloa, HI, USA, 3–6 January 2007; p. 156b, IEEE.
48. Hong, Y.; Furnell, S. Understanding cyber security behavioural habits: Insights from situational support. *J. Inf. Secur. Appl.* **2021**, *57*, 102710.
49. Jones, C.L.; Jensen, J.D.; Scherr, C.L.; Brown, N.R.; Christy, K.; Weaver, J. The health belief model as an explanatory framework in communication research: Exploring parallel, serial, and moderated mediation. *Health Commun.* **2015**, *30*, 566–576. [CrossRef]
50. Cheng, L.; Pei, J.; Danesi, M. A sociosemiotic interpretation of cyber security in US legislative discourse. *Soc. Semiot.* **2019**, *29*, 286–302.
51. Herath, T.; Rao, H.R. Protection motivation and deterrence: A framework for security policy compliance in organisations. *Eur. J. Inf. Syst.* **2009**, *18*, 106–125. [CrossRef]
52. D'Arcy, J.; Hovav, A.; Galletta, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Inf. Syst. Res.* **2009**, *20*, 79–98. [CrossRef]
53. Palladino, B.E.; Menesini, E.; Nocentini, A.; Luik, P.; Naruskov, K.; Ucanok, Z.; Dogan, A.; Schultze-Krumbholz, A.; Hess, M.; Scheithauer, H. Perceived severity of cyberbullying: Differences and similarities across four countries. *Front. Psychol.* **2017**, *8*, 1524. [CrossRef] [PubMed]
54. Adhikari, K.; Panda, R.K. Users' information privacy concerns and privacy protection behaviours in social networks. *J. Glob. Mark.* **2018**, *31*, 96–110. [CrossRef]
55. Ng, B.Y.; Kankanhalli, A.; Xu, Y.C. Studying users' computer security behaviour: A health belief perspective. *Decis. Support Syst.* **2009**, *46*, 815–825. [CrossRef]
56. De Kimpe, L.; Ponnet, K.; Walrave, M.; Snaphaan, T.; Pauwels, L.; Hardyns, W. Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Comput. Hum. Behav.* **2020**, *108*, 106310. [CrossRef]
57. Lian, J.W. Understanding cloud-based BYOD information security protection behaviour in smart business: In perspective of perceived value. *Enterp. Inf. Syst.* **2021**, *15*, 1216–1237. [CrossRef]
58. Menard, P.; Warkentin, M.; Lowry, P.B. The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Comput. Secur.* **2018**, *75*, 147–166. [CrossRef]
59. Rhee, H.S.; Kim, C.; Ryu, Y.U. Self-efficacy in information security: Its influence on end users' information security practice behaviour. *Comput. Secur.* **2009**, *28*, 816–826. [CrossRef]
60. Van Eerde, W.; Thierry, H. Vroom's expectancy models and work-related criteria: A meta-analysis. *J. Appl. Psychol.* **1996**, *81*, 575. [CrossRef]
61. Fida, R.; Tramontano, C.; Paciello, M.; Ghezzi, V.; Barbaranelli, C. Understanding the interplay among regulatory self-efficacy, moral disengagement, and academic cheating behaviour during vocational education: A three-wave study. *J. Bus. Ethics* **2018**, *153*, 725–740. [CrossRef]
62. Wall, J.D.; Palvia, P.; Lowry, P.B. Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *J. Inf. Priv. Secur.* **2013**, *9*, 52–79. [CrossRef]
63. Faul, F.; Erdfelder, E.; Buchner, A.; Lang, A.G. Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behav. Res. Methods* **2009**, *41*, 1149–1160. [CrossRef]

64. Hina, S.; Selvam, D.D.D.P.; Lowry, P.B. Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behaviour in higher education institutions in the developing world. *Comput. Secur.* **2019**, *87*, 101594. [CrossRef]
65. Dutton, W.H.; Creese, S.; Shillair, R.; Bada, M. Cyber security Capacity: Does It Matter? *J. Inf. Policy* **2019**, *9*, 280–306. [CrossRef]
66. Anwar, M.; He, W.; Ash, I.; Yuan, X.; Li, L.; Xu, L. Gender difference and employees' cyber security behaviours. *Comput. Hum. Behav.* **2017**, *69*, 437–443. [CrossRef]
67. Hair, J., Jr.; Hult, G.T.; Ringle, C.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2nd ed.; SAGE Publications, Inc.: Los Angeles, CA, USA, 2017.
68. Hair, J.F., Jr.; Matthews, L.M.; Matthews, R.L.; Sarstedt, M. PLS-SEM or CB-SEM: Updated guidelines on which method to use. *Int. J. Multivar. Data Anal.* **2017**, *1*, 107. [CrossRef]
69. Urbach, N.; Ahlemann, F. Structural equation modeling in information systems research using partial least squares. *J. Inf. Technol. Theory Appl.* **2010**, *11*, 5–40.
70. Hair, J.F.; Ringle, C.M.; Sarstedt, M. PLS-SEM: Indeed a silver bullet. *J. Mark. Theory Pract.* **2011**, *19*, 139–152. [CrossRef]
71. Hair, J.F., Jr.; Sarstedt, M.; Hopkins, L.; Kuppelwieser, V.G. Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *Eur. Bus. Rev.* **2014**, *26*, 106–121. [CrossRef]
72. Podsakoff, P.M.; MacKenzie, S.B.; Podsakoff, N.P. Sources of method bias in social science research and recommendations on how to control it. *Annu. Rev. Psychol.* **2012**, *63*, 539–569. [CrossRef] [PubMed]
73. Kock, N. Common method bias in PLS-SEM: A full collinearity assessment approach. *Int. J. E-Collab.* **2015**, *11*, 1–10. [CrossRef]
74. Anderson, J.C.; Gerbing, D.W. Structural equation modeling in practice: A review and recommended two-step approach. *Psychol. Bull.* **1988**, *103*, 411. [CrossRef]
75. Hair, J.F.; Risher, J.J.; Sarstedt, M.; Ringle, C.M. When to use and how to report the results of PLS-SEM. *Eur. Bus. Rev.* **2019**, *31*, 2–24. [CrossRef]
76. Ramayah, T.J.F.H.; Cheah, J.; Chuah, F.; Ting, H.; Memon, M.A. Partial least squares structural equation modeling (PLS-SEM) using smartPLS 3.0. In *An Updated Guide and Practical Guide to Statistical Analysis*; Pearson Malaysia Sdn Bhd: Kuala Lumpur, Malaysia, 2018.
77. Henseler, J.; Ringle, C.M.; Sarstedt, M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. Acad. Mark. Sci.* **2015**, *43*, 115–135. [CrossRef]
78. Chin, W.W. How to write up and report PLS analyses. In *Handbook of Partial Least Squares*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 655–690.
79. Clubb, A.C.; Hinkle, J.C. Protection motivation theory as a theoretical framework for understanding the use of protective measures. *Crim. Justice Stud.* **2015**, *28*, 336–355. [CrossRef]
80. Smith, M. *The Importance of Employee Awareness to Information Security*; The Security Company Ltd.: London, UK, 2006; pp. 115–128.
81. Aldossary, A.A.; Zeki, A.M. Web user'knowledge and their behaviour towards security threats and vulnerabilities. In Proceedings of the 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Kuala Lumpur, Malaysia, 8–10 December 2015; pp. 256–260.
82. Ye, C.; Potter, R. The role of habit in post-adoption switching of personal information technologies: An empirical investigation. *Commun. Assoc. Inf. Syst.* **2011**, *28*, 35. [CrossRef]
83. Barnes, S.J.; Böhringer, M. Modeling use continuance behaviour in microblogging services: The case of Twitter. *J. Comput. Inf. Syst.* **2011**, *51*, 1–10.
84. Yen, Y.S.; Wu, F.S. Predicting the adoption of mobile financial services: The impacts of perceived mobility and personal habit. *Comput. Hum. Behav.* **2016**, *65*, 31–42. [CrossRef]
85. Aarts, H.; Verplanken, B.; Van Knippenberg, A. Predicting behaviour from actions in the past: Repeated decision making or a matter of habit? *J. Appl. Soc. Psychol.* **1998**, *28*, 1355–1374. [CrossRef]
86. Orbell, S.; Blair, C.; Sherlock, K.; Conner, M. The theory of planned behaviour and ecstasy use: Roles for habit and perceived control over taking versus obtaining substances. *J. Appl. Soc. Psychol.* **2001**, *31*, 31–47. [CrossRef]
87. Agag, G.; El-Masry, A.A. Understanding the determinants of hotel booking intentions and moderating role of habit. *Int. J. Hosp. Manag.* **2016**, *54*, 52–67. [CrossRef]
88. Chiu, C.M.; Hsu, M.H.; Lai, H.; Chang, C.M. Re-examining the influence of trust on online repeat purchase intention: The moderating role of habit and its antecedents. *Decis. Support Syst.* **2012**, *53*, 835–845. [CrossRef]
89. Lankton, N.K.; Wilson, E.V.; Mao, E. Antecedents and determinants of information technology habit. *Inf. Manag.* **2010**, *47*, 300–307. [CrossRef]
90. Lee, D.; Larose, R.; Rifon, N. Keeping our network safe: A model of online protection behaviour. *Behav. Inf. Technol.* **2008**, *27*, 445–454. [CrossRef]
91. Klöckner, C.A.; Prugsamatz, S. Habits as barriers to changing behaviour. *Psykol. Tidsskr.* **2012**, *16*, 26–30.
92. Alzubaidi, A. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon* **2021**, *7*, e06016. [CrossRef]