sustainability

MDPI

Article

Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia

Saqib Saeed

Saudi Aramco Cybersecurity Chair, Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; sbsaed@iau.edu.sa

Abstract: In the post pandemic era, the telecommuting of business employees has widely become acceptable in organizations, which demands extensive dependence on digital technologies. In addition, this poses additional security threats for business employees as well as organizations. In order to better respond to security threats, business employees must have a higher level of awareness of the potential threats that are relevant to digital infrastructure used within the workplace. In this paper, we present a quantitative study conducted in line with the theory of planned behavior to gain insight into employee behavior toward information security within different business sectors in Saudi Arabia. The key factors chosen for our model were password management, infrastructure security management, email management, organizational security policy, organizational support and training, and the perception of the level of security. We have applied structured equation modelling to identify most of the relevant factors based on the respondents' feedback. The results based on the business employee behavior showed that they respondents did not perceive all of the constructs of our model as relevant security factors, which can potentially result in security lapses. This indicates that more security-related measures should be put in place and that business employees should be updated periodically about potential security threats. To this effect, we divided the studied security measures into those which should be implemented at organizational and individual levels. The results will potentially help business managers to design appropriate security trainings, guidelines, and policies for their employees to ensure more information security awareness and protect their technological infrastructure, especially within home office environments.

Keywords: human security; cybersecurity; privacy; user education; cybersecurity policies; personal security; organizational security; digital citizenship

Citation: Saeed, S. Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. *Sustainability* **2023**, *15*, 6019. https://doi.org/10.3390/su15076019

Academic Editors: Juan Sebastián Fernández-Prados, Cristina Cuenca-Piqueras and Antonia Lozano-Díaz

Received: 9 March 2023
Revised: 26 March 2023
Accepted: 29 March 2023
Published: 30 March 2023

1. Introduction

Due to the increased diffusion of digital technologies in everyday activities, cybersecurity has become a critical challenge. Cybersecurity is a complex multi-faceted phenomenon; the association of computing machinery (ACM) has categorized eight knowledge areas for cybersecurity: data security, software security, component security, connection security, system security, human security, organizational security, and societal security [1]. Data security refers to protecting digital data from unauthorized access, while software security focuses on protecting software systems from vulnerabilities. The component security knowledge area focuses on securing individual components which are integrated into larger systems, whereas connection security is concerned with the security issues that could arise while components are connected together physically and logically. System security focuses on security issues within systems as a whole, which could consist of different components. The human security knowledge area deals with securing individual data within personal and organizational contexts. Organizational security is aimed at protecting organizational infrastructures from internal and external threats, while societal security mainly focuses on cybercrime, ethics, law, and privacy related issues concerning the society. Due to these

multi-dimensional challenges, software systems are often left open to cyberattacks, and users must be more proactive to keep themselves and their work protected.

As with every other sector, digital transformation within business organizations has provided organizations with a vast number of opportunities to optimize the services that they offer to their customers [2,3]. However, this has resulted in more challenges for businesses to protect their technological infrastructure from unauthorized access. The majority of businesses have invested heavily to protect their technological infrastructure by establishing dedicated departments or outsourcing their security operations. Cyber-attacks, however, have increased dramatically, and cyber criminals are finding new ways to attack organizations and steal sensitive information. Recent studies have highlighted humans as the weakest link, and there is a need to ensure their awareness of cybersecurity risks to improve the lines of defense against attacks.

Furthermore, COVID-19-related lockdowns pushed businesses to adopt digital technologies at a rapid speed to keep their operations running [4]. This resulted in many of these businesses' employees needing to work remotely and use personal computers which were likely less protected than office computing infrastructure in dealing with cybersecurity threats. Therefore, it is interesting to gain an insight into the information security behavior of business employees while conducting their work.

In this paper, we have focused on exploring the information security behavior exhibited by employees working in different business organizations across Saudi Arabia. To sustain secure technological usage among employees, there is a need to adopt secure practices at work. When employees are aware of potential security breaches, they act more cautiously while using computing devices and vice versa, which will potentially lead them to a more sustainable use of technologies in the workplace. Therefore, our work mainly overlaps with human security and organizational security knowledge areas. We have used the theory of planned behavior as a reference model, which highlights the favorable integration of behavioral attributes, subjective norms, and perceived behavioral control, which leads to a stronger intention and which result in increased chances of fostering desired behavior [5]. Our focus is to understand the information security practices of business employees in Saudi Arabia, relate them with our model, and identify the gaps in information security practices. We have outlined password management, infrastructural security management, email management, organizational security policies, and security perception as key constructs for our model. The core focus of our work is to obtain answers for the following questions:

1. What are the information security practices employed by the business employees in Saudi Arabia?
2. Which security factors are considered relevant/irrelevant by employees working in different business domains in Saudi Arabia?
3. How can the security behavior of business employees in Saudi Arabia be improved by adopting more secure practices?

To answer these questions, we conducted a quantitative study using an online questionnaire with more than 500 respondents. Our findings will potentially help security managers and business managers to develop training programs to improve the security awareness of their employees, to better equip them to deal with cybersecurity challenges, and to protect organizational resources.

The rest of the paper is structured as follows: Section 2 discusses the theoretical basis of our work and hypotheses of study, followed by our research methodology in Section 3. Section 4 presents a discussion on the results, followed by a discussion and a conclusion in Sections 5 and 6, respectively.

2. Theoretical Basis and Hypothesis

Digital transformation has gained enormous attention from researchers over the years, and more so now due to COVID-19 pandemic-related lockdowns [5]. As a result, cybersecu-

rity has become a critical topic for researchers and practitioners. In the following sections, we describe the relevant existing work in detail.

2.1. Digital Transformation and Cybersecurity

Artamonov and Artamonova have documented potential cybersecurity threats for organizations in their pursuit of digital transformation; such a listing can help organizations to proactively guard against threats [6]. Medoh and Telukdarie have highlighted that strategic planning can help businesses in combatting cybersecurity threats and to progress towards industry 4.0 [7]. Their findings showed that a proactive strategic and tactical decision-making approach positively helps in responding to security threats. Mishra et al. argued that cybersecurity requirements vary among organizations based on their area of business; therefore, organizational cybersecurity policies should be based on the nature of the information in question as well as the security requirements of each individual organization [8]. Thus, a standardized security policy may not suffice for all business domains collectively. Diaz et al. discussed how the digital transformation of business processes generates huge amounts of digital data which poses risks to businesses as well as consumers; therefore, security and privacy aspects must be addressed [9]. Lee and Hwang concluded that voice behavior by employees has a positive impact on fostering information security practices within organizations [10]. Nemec Zlatolas et al. [11] carried out an empirical study to establish an understanding of the security perception of IoT devices and found that users' awareness of security breaches has an impact on the relative importance of IoT security, and that users often do not review or ignore security settings and feel safe while using IoT devices. The adoption of advanced technologies can help in improving and optimizing security levels within an organization. Mehrnezhad and Toreini [12] investigated users' risk awareness while working with sensor enabled apps and found that users lacked security risks awareness; however, they found that user training significantly enhanced the security behavior of mobile users. Goh and Teoh analyzed the bring your own device (BYOD) security policy compliance among Malaysian tele workers based on protection motivation theory [13]. They highlighted that BYOD initiatives were a quick fix for organizations to avoid disruptions in their operations; however, compliance to security policy by employees is still a major challenge in itself.

Jarlhem and Stigsson have highlighted that remote work due to pandemic lockdowns has resulted in a surge in security attacks. The results of their study showed that employees who were more technically competent were more aware of cyber threats. Furthermore, the results confirmed that education and training of employees alone is not a strong enough measure against cybercrimes, and that the willingness of employees to understand security threats is also vital [14]. Dangheralou and Jahankhani analyzed the impact of general data protection regulation (GDPR) guidelines while working from the home during the pandemic lockdowns. They concluded that consumer protections and transparency are important tools for organizations to establish trust with their consumers and that businesses must invest more in the management of security risks [15]. Arogbodo studied the cybersecurity situation in academic institutions as they switched to online learning during the pandemic. He discussed how cybersecurity measures within educational institutions have improved; however, improving cybersecurity is a continuous process that is essential to combating security threats [16]. Yang and Linkeschová highlighted that there was an increase in cyber-attacks to take advantage of employees teleworking during COVID-19 pandemic, which requires increased employee cyber protection [17]. Carlsten et al. investigated the readiness of organizations to document best practices for working from home scenarios during COVID-19 and found that most organizations were prepared to handle a work from home scenario as they already had well-developed technological infrastructure [18]. Borkovich and Skovira [19] discussed the direct correlation between the number of cyber-attacks and employees working from home due to COVID-19 lockdowns, and highlighted the human element as the weakest link. Furthermore, Powell [20] argued

that organizations must train and provide software resources to their employees to secure their network while working remotely.

2.2. Password Management

Effective password management is a critical activity to foster secure usage behavior. Tam et al. presented their findings on how users are aware of setting good and poor passwords; however, they still violate common password management practices such as storing it on their computer, as the negative consequences of these are not immediate [21]. Tarwireyi et al. [22] discussed how security awareness programs could help users in fostering a preventive information security culture. They set up a security awareness study on password management and found that, even though students are aware of security issues, they still refused to implement proper password management. For instance, even though students knew password sharing is risky, almost half of them shared their passwords. They also found that, as students' progress through the education levels, they tend to use stronger passwords. Zezschwitz et al. [23] looked into how organizations enforcing password change policies has negatively affected the employees' behavior toward information security, as they engage in setting weak passwords which may originate from older passwords and may also be reused across accounts. On the other hand, Habib et al. [24] argued that there is neither a positive nor negative impact of forced password change policies within organizations. These studies highlight that a single strategy may not work; therefore, there is a need for a combination of measures to foster effective password management strategies.

2.3. Infrastructure Security

A secure infrastructure reduces the probability of vulnerabilities within a system. Sanok Jr. [25] reiterated that antivirus software is an effective tool to provide basic security measures against computer viruses and attacks. Al-Saleh et al. [26] argued that, although antivirus software provides basic security to users, due to the inherently intrusive behavior of antivirus software, it negatively affects the performance of computers. Tiwari and Karlapalem [27] highlighted how avoiding updating the definition of the term virus for antivirus software is a major security risk. Hayajneh et al. [28] investigated how firewalls are essentially the first line of defense for a network; therefore, a rigorous performance assessment of firewalls must be carried out periodically. Lee and Kozar [29] set up an empirical study to identify the factors motivating users to adopt anti-spyware applications and found that user's intentions, subjective norms, perceived behavioral controls, and denial of responsibility positively affect the adoption of anti-spyware. Gurung et al. [30] highlighted that anti-spyware tools can help in protecting consumers against cyber-attacks. Albrechtsen and Hovden [31] highlighted that the participation and engagement of users in establishing information security culture can help in improving behaviors such as locking the computers when stepping away from their desks. Almeida [32] highlighted that usage of social media carries additional security challenges; therefore, many organizations block the usage of such applications within their office space. Koushik et al. [33] proposed that users ought to adopt the practice of locking their machines when stepping away or going out of the office, even if it is just with a locked screensaver. Rao and Prasad [34] highlighted weaknesses of web browsers and applications which could result in cross-site scripting attacks, and detailed how blocking such scripting could keep the network secure. Therefore, it is important that technological infrastructure is well protected by adopting and implementing different security mechanisms across the board.

2.4. Email Security Management

Email is one of the most widely used communication medias, and Kruger et al. [35] discussed how email communication is more prone to identity theft and virus attacks, and that most users would open emails with vulnerable content without any consideration of the risks. Such handling of email messages can result in several security breaches. Rudd

et al. [36] used machine learning to identify potentially harmful attachments in emails. Such an automated approach can intelligently sniff email messages to differentiate between safe and potentially risky emails. In addition, email communication can be secured from intruders by using encryption algorithms [37,38]. Roth et al. [39] highlighted diversity of user agents, network access methods, and language settings as providing a uniform security policy, and that inconsistencies in these areas can result in serious security breaches. In another study, Villamarín-Salomón et al. [40] highlighted that email clients should understand context and that it should guide users to proceed or refrain from opening email attachments that could be potentially harmful. Certain context-aware applications employ artificial intelligence algorithms to make informed judgement regarding the security level of email communications. User support is another important measure in user training. Bilal et al. [41] studied how establishing helpdesks to support employees with their information security queries helps in different organizational security contexts. Stafford et al. [42] found that user training needs based on a careful internal audit can possibly improve compliance with the security policies of businesses. Internal audits reveal security shortcomings of an organization which can then be addressed by designing appropriate training programs.

2.5. Security Education and Training

Alongside training, fostering a knowledge sharing culture among employees can improve organizational resilience against security vulnerabilities. Safa et al. [43] presented a discussion on knowledge sharing regarding information security, experience, and collaboration among employees and its positive contribution to compliance with organizational security policy. Similarly, Herath and Rao [44] studied how the certainty of violation detection is critical, whereas the punishment severity is negatively related with security behavior; therefore, organizations must establish violation detection mechanisms as well as roles, responsibilities, and implications of employee behavior that puts the entire organization at risk. Furthermore, Knapp et al. [45] highlighted that establishing information security policy has become vital for organizations; therefore, they have proposed a generic information security policy process model to help organizations establish security policies. Such generic frameworks are more helpful for small-and medium-scale enterprises to enable them to have basic information security protocols in place with their limited resources. In a similar study, Hagen et al. [46] investigated critical implementation issues to make an organizational information security policy more effective in practice. Since end users are key stakeholders in implementing an information security policy, Huang et al. [47] carried out a study to identify the factors which influence the information security perception of users. They identified hackers, worms, viruses, Trojan horses, and backdoor programs as five major threats and highlighted how the users perceive the danger of these threats.

2.6. Security in Social Networks

Social network platforms are in high demand, with millions of users worldwide, and security on these platforms is also a very critical issue. Al-Molhem et al. [48] employed social network analysis on the telecom data such as customers call details to model the social networks of users to understand the social connections among different telecom users. Similarly, Li et al. [49] categorized information disclosure on social network platforms in voluntary and mandatory disclosure, and they argued that the results of studies focusing on voluntary information sharing may not be extended to mandatory information disclosure behavior, as there is a fundamental difference in both approaches. In another work, Cerruto et al. [50] investigated user profiles on different social network platforms to highlight the vulnerability of user data present in social network applications to provide more awareness to social networking users regarding security threats.

2.7. Theory of Planned Behavior in Security Research

To understand the security behavior of users, recently, the theory of planned behavior has been used by information security researchers as a theoretical lens. As shown in

Figure 1, the theory of planned behavior states that, if an individual perceives an activity to be enjoyable and beneficial, receives support from his social group, and feels that they have the abilities and the skills to meet the demand of the required behavior, this will result in stronger intention, and there is a higher probability that the individual will engage in the desired behavior. In the context of our topic, we explore how different factors, such as knowledge of password management, email and infrastructure security combined with organizational support, and the perceptions of employees, can result in strong intention towards secure behavior and, in turn, cause the adoption of secure behavior while interacting with digital infrastructure. Kim and Mou [51] employed the structural equation modeling approach and highlighted the three factors of the theory of planned behavior that have a significant impact on user intention. However, Sommestad et al. [52] argued that additional constructs from protection motivation theory along with constructs of the theory of planned behavior result in better predication of the information security compliance behavior of users. Protection motivation theory reflects that fear of potential harm encourages individuals to adopt higher protective behavior. In another work, Grassegger and Nedbal [53] carried out an empirical study to understand the information security awareness of employees and their resilience against social engineering attacks. The findings highlighted that the theory of planned behavior is also relevant in order to understand employees' responses to social engineering attacks.

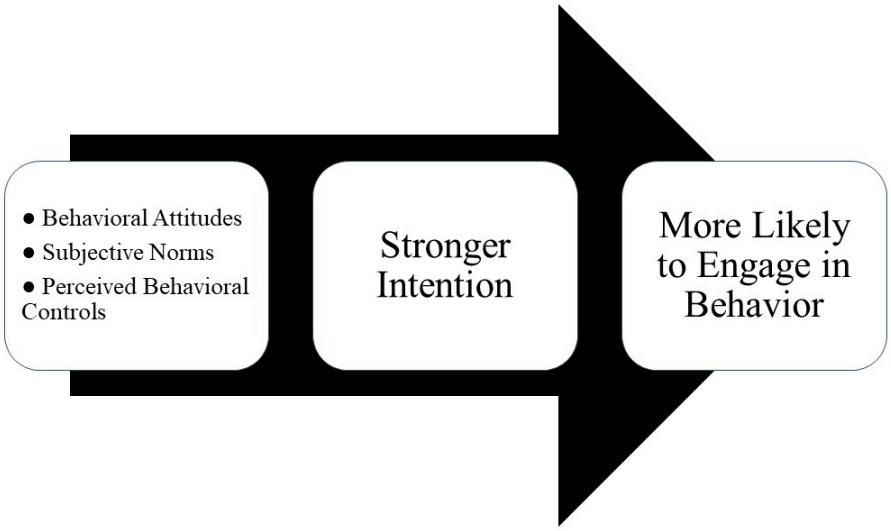

Figure 1. Theory of planned behavior.

2.8. Information Security Research in Saudi Arabia

There have also been some studies carried out in the context of information security research in Saudi Arabia. AlMindeel and Martins [54] carried out an empirical study in the government sector of Saudi Arabia and highlighted that user behavior and different environment variables play significant roles in shaping users' information security awareness. In another study, Almutairi et al. [55] provided the current state of information security management practices employed in Saudi Arabia and highlighted important areas in which to improve information security in the country, which provides a framework for improved security management at the national level. Securing organizational infrastructure is of key importance for business continuity, and Alharbi [56] highlighted that many academic institutions lack appropriate cybersecurity measures to protect their technological infrastructure. Alsulami [57] carried out a study to investigate the social media security awareness among users in Saudi Arabia and found that awareness level plays a key role in users' attitudes towards information security. In another study, Gull et al. [58] investigated the ecommerce security perception of buyers in Saudi Arabia based on consumer ratings, the trustworthiness of e-commerce portals, and credit card security, and found variations

among users' security perceptions of different e-commerce sites. Alzubaidi [59] highlighted that there is an innate need to increase users' awareness regarding cybercrimes in Saudi Arabia. Aljohni et al. [60] have found university students studying computing related courses in Saudi Arabia are more aware of information security concerns than students from other disciplines.

2.9. Hypotheses Formulation for Our Study

The protection of information infrastructure is still a critical challenge for researchers and practitioners; therefore, there is a need to enrich the current body of knowledge to improve compliance [61–64]. While there have been previous research initiatives, as discussed in the preceding sections, there is no study that has explored business employees' information security behavior in the context of Saudi Arabia. Rapid digital transformation by the business sector requires that employees exhibit secure behavior to protect organizational technological infrastructure. Therefore, in this study, we adopted the theory of planned behavior as a theoretical lens to understand the information security behavior of business employees in Saudi Arabia. We have designed the six following hypotheses for our research.

Hypothesis 1: *Effective password management leads to positive information security behavior*.

Hypothesis 2: *Effective management of infrastructural security resources leads to positive information security behavior*.

Hypothesis 3: *Appropriate email management activities lead to positive information security behavior*.

Hypothesis 4: *Organizational security policy leads to positive information security behavior*.

Hypothesis 5: *Organizational support and training leads to positive information security behavior*.

Hypothesis 6: *Security perception has an impact on positive information security behavior*.

Table 1 highlights how the constructs of our study and associated subfactors are aligned with theory of planned behavior constructs. Furthermore, the relevant literature sources for each subfactor are also listed, along with abbreviation.

Table 1. Study constructs and relevant literature source.

Theory of Planned Behavior Constructs	Construct of Study		Subfactors of Constructs	Relevant Literature Source
Perceived Behavioral Controls	Password Management	PM1	Single password reuse	[23,24]
		PM2	Password change only when mandatory due to organizational policy	[23,24]
		PM3	New password resembling old password	[23,24]
		PM4	Password storage on a paper or electronic file	[21]
		PM5	Password storage in a software	[21]
		PM6	Password sharing with colleagues	[22]
Perceived Behavioral Controls	Infrastructure Security Management	ISM1	Antivirus presence	[25]
		ISM2	Antivirus update	[27]
		ISM3	Firewall usage	[28]
		ISM4	Anti-spyware usage	[29,30]
		ISM5	Allowing scripting	[34]
		ISM6	Locking computer while away	[31,33]
		ISM7	Password protected screensaver	[33]
		ISM8	Usage of social applications	[32]

Table 1. *Cont.*

Theory of Planned Behavior Constructs	Construct of Study		Subfactors of Constructs	Relevant Literature Source
Perceived Behavioral Controls	Email Management	EM1	Opening unknown emails	[35]
		EM2	Opening attachments from unknown emails	[36]
		EM3	Usage of encryption in emails	[37,38]
		EM4	Analyzing security settings of web-based email clients	[40]
Subjective Norms	Organizational Security Policy	OSP1	Attention to computer security	[47]
		OSP2	Presence of organizational security policy	[45]
		OSP3	Understandability of organizational security policy	[46]
		OSP4	Deviation from organizational security policy	[43]
		OSP5	Perception of coworkers' deviation of organizational security policy	[43]
		OSP 6	Repercussions of security policy violations	[44]
Subjective Norms	Organizational Support and Training	OST1	Availability of helpdesk	[41]
		OST2	Provision of training	[42]
		OST3	Enhanced understanding of security policy due to training	[42]
Behavioral Attitudes	Perception of Security	POS1	Personal computer is safe	[47]
		POS2	I can protect my computer	[47]
		POS3	Computer security is worrying	[47]
		POS4	Special attention to security makes difference	[47]
		POS5	My information is not interesting for hackers	[47]
		POS6	Hacking is unavoidable	[47]

3. Materials and Methods

This is a cross sectional study where we have collected quantitative data using an online questionnaire, shown in Appendix A. To develop the questionnaire, initially, we analyzed existing available questionnaires [65–68] to identify important aspects that were analyzed within those studies. After the initial analysis, we reused some of the questions from these existing questionnaires and added some of our own additional questions which are relevant to our research constructs, shown in Table 1. Once the questionnaire was prepared, we had it reviewed by two colleagues for the content validity of the questions in line with our research problem. After the review, the questionnaire was updated and uploaded to Google forms for data collection. To collect data, we employed the snowball sampling technique [69,70], where we requested the students enrolled on our business courses to have the survey filled by their contacts who work in any organizational setting. Once early respondents were engaged, we asked for recommendations for respondents from their peers. The eligibility criteria to fill out the questionnaire was that a respondent is employed in an organization in Saudi Arabia and that their work requires the usage of computing devices. To reach a confidence level of 95%, we intended to collect at least 385 responses. At the end of the survey period, there were a total of 566 responses received, out of which four responses were discarded due to not meeting our qualification criteria of completeness. Out of our respondents, 212 were in the age group of 19–25 years, 198 respondents were in the age group of 26–35 years, 124 respondents were in 36–50 years age group, and 28 respondents were above 50 years old. Out of these, 346 were male respondents and 216 were female respondents. Further, 70 respondents belonged to manufacturing sectors, 137 belonged to the service industry, 157 belonged to government organizations, 39 belonged to nonprofit organizations, and 159 respondents were from various other sectors. To process the data in Smart PLS 4, we transformed the data into numeric values and applied the bootstrapping method with 5000 iterations using two-tailed tests. Once the model was formulated, we identified the p values to approve or reject our hypotheses.

4. Results

To explore the relationship among the constructs and subconstructs, we carried out factor analysis, as shown in Figure 2. For a construct to be relevant, a factor loading of 0.7 is recommended; however, it can be lowered to 0.2 [71,72]. In our work, we kept the factor loading to a value of 0.6 and, after removing the irrelevant factor, we redrew the model in Figure 3.

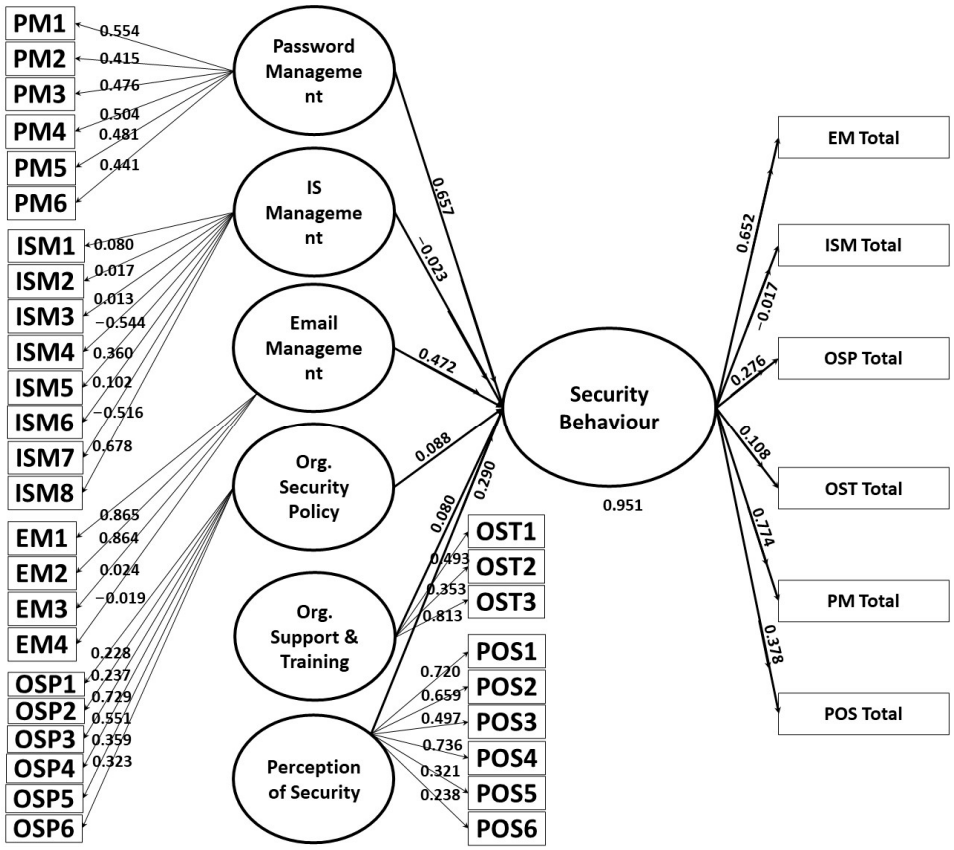

Figure 2. Factor analysis using structured equation modelling.

Figure 3 highlights that employees in Saudi Arabian businesses adopt some of the listed information security practices. In the case of password management, employees perceive reusing a single password and the storage of password in a software or in another format as a security concern. In the case of email management, employees think that opening unknown emails and attachments is a security concern; however, IT infrastructure management was not considered to be a relevant factor in employees' security perception. In the case of organizational security policy, employees believe that the understandability of organizational policy and clear deviation from organizational security policy are relevant factors. In the case of organizational support and training, the availability of a helpdesk and training are key resources in improving the security perception among business employees.

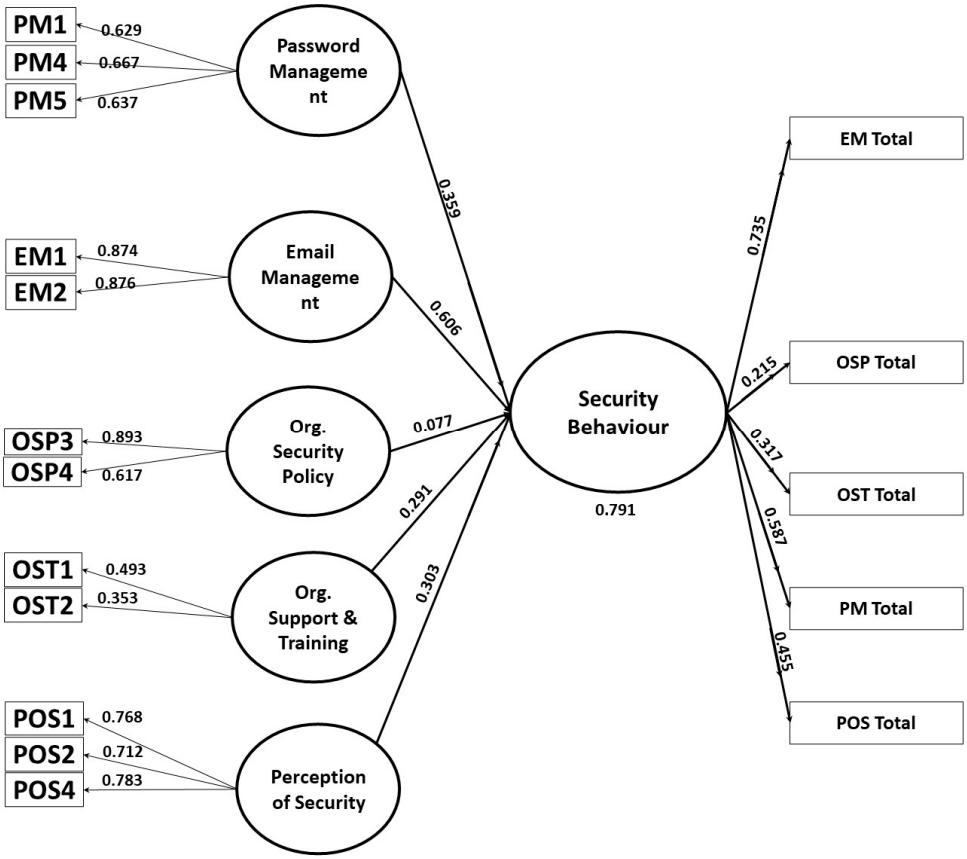

Figure 3. Refined factor analysis model using structured equation modelling.

Consumer ratings of different perceived security threats affect the security and privacy perceptions of employees. In the context of security perception, business employees believe that their personal computers are safe, that they have the technical capabilities to protect their computer, and that a special emphasis on security makes a difference in the security behavior. To prove a hypothesis, the *p*-value must be less than 0.05 [72], and, as shown in Table 2, Hypotheses 1, 3, and 4 are approved, whereas hypotheses 2, 5, and 6 are rejected. The sample mean, standard deviation, and T-statistics are also listed in Table 2.

Table 2. Hypotheses results.

Hypothesis	Sample Mean	Standard Deviation	T Statistics	*p* Values	Result
Hypothesis 1	0.594	0.129	5.086	0.000	Approved
Hypothesis 2	0.027	0.096	0.237	0.812	Rejected
Hypothesis 3	0.434	0.096	4.910	0.000	Approved
Hypothesis 4	0.075	0.041	2.149	0.032	Approved
Hypothesis 5	0.150	0.162	0.493	0.622	Rejected
Hypothesis 6	0.268	0.162	1.790	0.074	Rejected

Discriminant Validity

To measure the discriminant validity, we used the Fornell-Lacker criterion, which highlights that the average variance of a construct must be greater than the correlation of the same construct with all other constructs [73]. As shown in Table 3, email management's AVE value 0.612 is higher than all other values of other constructs in the same column; similarly, the infrastructure management value (0.382), organizational security policy value (0.443), organizational support and training value (0.586), and password mange value (0.480) are higher than the relevant construct values; therefore, discriminant validity is established.

Table 3. Discriminant validity using Fornell-Larcker criterion.

Fornell-Larcker Criterion	Email Management	Infrastructure Management	Organizational Security Policy	Organizational Support & Training	Password Management	Perception of Security
Email Management	0.612					
Infrastructure Management	0.150	0.382				
Organizational Security Policy	0.095	0.104	0.443			
Organizational Support & Training	−0.015	0.020	0.002	0.586		
Password Management	0.196	0.144	0.132	0.041	0.480	
Perception of Security	0.138	0.170	0.033	0.066	0.044	0.563

5. Discussion

Factor analysis of our empirical data highlighted that infrastructure security is not a relevant factor in the security behavior of our respondents. Some earlier studies, however, have highlighted updating antivirus software [25,27], and the adoption of a firewall [28] and antispyware tools [29,30] provide a significant shield against cybersecurity attacks. Furthermore, blocking scripts execution [34], and practices such as password protected screensavers [30], locking computer screen when stepping away from the work desk [31,33], and refraining from social media usage at workplace [32] decreases cybersecurity attacks; however, again, this was not a significant factor based on our empirical data. Therefore, there is a need to train end users to make them aware of the implications of vulnerabilities in technological infrastructure, so that this can become an important factor in their security behavior.

Furthermore, the empirical data highlighted that password management was considered an important factor in the security behavior and, specifically, reuse of the same password, storage of the password on paper or electronic file, and storage of the password in software were considered important factors, which falls in line with the earlier findings within the existing literature [21,23,24]; however, other factors which were found to be important in the earlier literature, such as sharing the password with colleagues [22], resemblance of a new password with an old password [23,24], and changing the password only when enforced by organization policy [22,24] were found to be not significant in our study.

In the case of email management, our study highlighted that our subjects considered opening unknown emails, or attachments from unknown sources, a significant factor, which is aligned with findings of previous studies [35,38]. However, the encryption of emails and security settings of web-based email clients were insignificant, which is not consistent with the findings of earlier studies [37,38,40]. In the context of organizational security policy, our findings highlighted that, in line with the previous literature [43,46], respondents think that the understandability of organizational security policy and clear examples of deviation from policy positively correlate with security behavior. Furthermore, the establishment of helpdesks and training help in improving security behavior among respondents, which supports earlier findings [41,42].

5.1. Theoretical Implications

The theory of planned behavior focuses on establishing the intended behavior of individuals based on perceived behavioral controls, perceived norms, and behavioral attitudes of respondents. In this study, the password management practices, technology infrastructure security management practices, and email management practices of users were taken as perceived behavioral controls. Information security policy, as well as organizational support and training, were modelled as subjective norms and security perception was categorized as behavioral attitudes. The theory of planned behavior helped to better understand the factors which affect the security behavior of respondents. The results will help to develop guidelines to improve the security behavior of end users.

5.2. Managerial Implications

To sustain the security behavior of business employees, a two-pronged strategy is presented in Figure 4, where both employees and businesses are required to work on improving employee security behavior. At the individual level, business employees must follow more strict password security management procedures, as our findings highlighted that, out of six subfactors of the password management construct, only three had a factor rating that was more than 0.6.

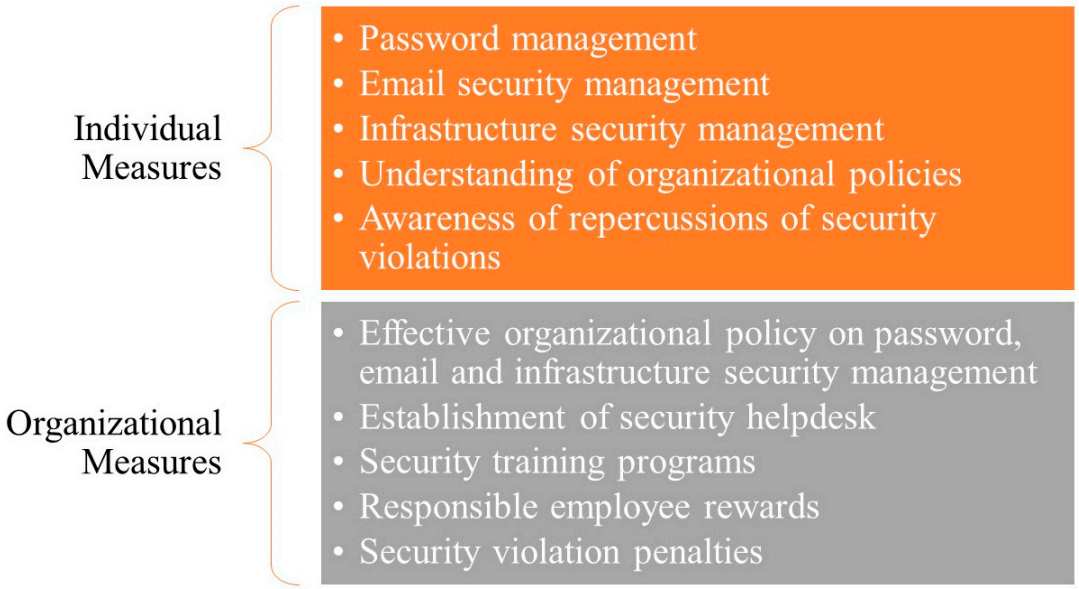

Figure 4. Strategy to improve security behavior among business employees.

In the case of email security management, only two out of four subfactors were significant, which also highlights that employees of business organizations require more awareness to understand the security threat of other factors. In the case of infrastructure security management, our findings highlighted that employees of business organizations did not consider these factors to be relevant; however, such factors can have a negative impact on user security. Therefore, individuals must acquire a better understanding of security issues related to information technology infrastructure. Business employees must acquire a better understanding of organizational security policies, as our model highlighted that some factors were not considered important based on the empirical data. Furthermore, an increased understanding of the impact of security violations at the individual and organizational levels can help to positively improve the security behavior of business employees in Saudi Arabia.

At the organizational level, there is a need to establish and implement security policies on effective password, email, and infrastructure security. The increased home-office culture also requires that business employees are more careful in using technological equipment. The establishment of helpdesks and training programs can help employees to keep themselves abreast with leading-edge security challenges. The establishment of reward and penalty mechanisms for employees can also be helpful in promoting a security culture within business organizations.

5.3. Limitations and Future Directions

Our study was conducted with a limited set of respondents; therefore, the findings may not be reflective of the information security practices of all employees working in the business sector across different domains in Saudi Arabia. Our analysis did not include the geographical location of respondents in Saudi Arabia or the business domain of business organizations where respondents were working. Furthermore, the sampling was based on

snowball sampling, which may also be affected by representation bias. In future studies, each type of organization might be explored to have a comparison of security practices adopted across users belonging to different domains. Additionally, responses from different regions across Saudi Arabia must be investigated to understand whether all regions in Saudi Arabia have the same level of security awareness.

6. Conclusions

Cybersecurity is a critical issue and an increased telecommuting culture in organizations makes business employees more vulnerable to security threats. Cultural and social implications affect users' perceptions and motivations in adopting secure behavior while working with digital systems. Therefore, it is scientifically very interesting to document case studies in diverse geographical and professional contexts to gain a better insight into user behavior. Such a set of empirical studies will potentially help to formulate the best practices for end users to adopt more secure behavior in dealing with technological artifacts. In this paper, we have explored the security behavior of employees in Saudi Arabian business organizations and found that many critical factors documented in the literature are not considered relevant by employees, showing a lack of awareness. Therefore, we have established a set of actions to be followed at the individual as well as at the organizational level to sustain the digital citizenship behavior of business employees. These findings will help relevant practitioners to improve information security compliance in their organizational settings.

Funding: The author would like to thank SAUDI ARAMCO Cybersecurity Chair, Imam Abdulrahman Bin Faisal University, for funding this project.

Institutional Review Board Statement: The request was approved in department of computer information systems 24th board meeting held on 13 June 2022. Institutional review board approval was granted on 12 February 2023. (IRB-2023-09-67).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The authors would like to thank respondents for spending their time in filling the questionnaires and Tooba Nasir for language review of the manuscript.

Conflicts of Interest: The author declares no conflict of interest.

Appendix A

Dear Respondents, Due to COVID-19, the digital transformation has increased in business organizations. With this exponentially increased dependence on information technology, cybersecurity has become a more critical concern for businesses. In this study we are collect data related to human aspects of cybersecurity to understand how the users in business organizations adhere to and deviate from policies and guidelines. The deviation from policies makes the organizations more vulnerable and prone to internal as well as external threats. We are asking you to fill out this questionnaire which should take about 10 min of your time. Your responses are anonymous and strictly confidential and will be only used for scientific reports/publications without revealing your identity. If you are willing to help the research team by participating in the study, then proceed to record your responses for the questions.

Q1: Your Gender
Female
Male
Q2: Age?
Less than 18 Years
19–25 Years
26–35 Years

36–50 Years
Above 50 Years
Q3: What is the business domain of your organization?
Manufacturing
Service Industry
Government Organization
Nonprofit Organization
Other
Q4: I use same password to access multiple systems.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q5: I primarily change my password; it is because of the company's policy.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q6: When I change my password, I use my old password as a basis.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q7: I keep my username/passwords in an electronic file or write them down.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q8: I use a software to keep track of my passwords.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q9: I share my password with other colleagues.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q10: My personal computer has an anti-virus program installed.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q11: The antivirus program is regularly updated.
Strongly Agreed
Agreed
Neutral

Disagreed
Strongly Disagreed
Q12: I have a firewall installed on my computer.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q13: I use an anti-spyware tool on my computer.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q14: I allow "scripting" on my computer.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q15: I always log off or lock the computer when I step away from it.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q16: I use a password protected screensaver.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q17: I use social/ professional networking sites on my work computer.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q18: I open emails even if I do not know who the sender is
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q19: I open even attachments from the emails where I do not know the sender is.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q20: I use encryption when sending emails.
Strongly Agreed
Agreed
Neutral

Disagreed
Strongly Disagreed
Q21: While using web-based email or calendar software, I pay attention to the security settings of the web-based software.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q22: My organization has a computer and information security policy.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q23: I understand the computer security and information policy of my organization.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q24: I deviate or work around the computer security policy of my organization.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q25: I think my co-workers deviate/work around the computer security policy.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q26: If you or your co-workers deviate or work around the computer security policy, and someone finds out about it, are there any repercussions?
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q27: If I have problems with a computer application, it is easy for me to contact my network or system administrator or the help desk.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q28: I received training on computer and information security.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed

Q29: The training on information security helped me to better understand organization's security policy?
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q30: I think I can protect my computer from hackers/phishers, if I take good care of computer security.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q31: I think it is important to pay attention to computer security.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q32: Computer security worries me.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q33: I think it makes a difference, if I pay special attention to computer security, such as installing a browser that is less vulnerable.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q34: I think the information that I keep on my computer is not interesting enough for people to try and hack into my computer.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
Q35: I think it does not matter what I do, if people have bad intentions, they will be able to hack into my computer and our network.
Strongly Agreed
Agreed
Neutral
Disagreed
Strongly Disagreed
You have reached to the end of questionnaire. We are very thankful to you for spending time in filling out responses. You can reach us by email to receive findings once we finish the research.

References

1. ACM Cybersecurity Curricula 2017. Available online: https://dl.acm.org/doi/book/10.1145/3184594 (accessed on 10 November 2022).
2. Gull, H.; Alabbad, D.A.; Saqib, M.; Iqbal, S.Z.; Nasir, T.; Saeed, S.; Almuhaideb, A.M. E-Commerce and Cybersecurity Challenges: Recent Advances and Future Trends. In *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*; IGI Global: Hershey, PA, USA, 2023; pp. 91–111.
3. Saeed, S. A Customer-Centric View of E-Commerce Security and Privacy. *Appl. Sci.* **2023**, *13*, 1020. [CrossRef]
4. Saeed, S.; Bolívar MP, R.; Thurasamy, R. *Pandemic, Lockdown, and Digital Transformation*; Springer: Berlin/Heidelberg, Germany, 2021.
5. Ajzen, I. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.* **1991**, *50*, 179–211. [CrossRef]
6. Artamonov, V.A.; Artamonova, E.V. The Cybersecurity in Conditions of the Digital Transformation. *Digit. Transform.* **2022**. Available online: https://ideas.repec.org/a/abx/journl/y2022id642.html (accessed on 10 November 2022).
7. Medoh, C.; Telukdarie, A. The Future of Cybersecurity: A System Dynamics Approach. *Procedia Comput. Sci.* **2022**, *200*, 318–326. [CrossRef]
8. Mishra, A.; Alzoubi, Y.I.; Gill, A.Q.; Anwar, M.J. Cybersecurity Enterprises Policies: A Comparative Study. *Sensors* **2022**, *22*, 538. [CrossRef]
9. Díaz, A.; Guerra, L.; Díaz, E. Digital Transformation Impact in Security and Privacy. In *Developments and Advances in Defense and Security*; Springer: Singapore, 2022; pp. 61–70.
10. Lee, W.J.; Hwang, I. Sustainable Information Security Behavior Management: An Empirical Approach for the Causes of Employees' Voice Behavior. *Sustainability* **2021**, *13*, 6077. [CrossRef]
11. Nemec Zlatolas, L.; Feher, N.; Hölbl, M. Security perception of IoT devices in smart homes. *J. Cybersecur. Priv.* **2022**, *2*, 65–73. [CrossRef]
12. Mehrnezhad, M.; Toreini, E. What is this sensor and does this app need access to it? *Informatics* **2019**, *6*, 7. [CrossRef]
13. Goh, C.H.; Teoh, A.P. Determining Bring Your Own Device (Byod) Security Policy Compliance among Malaysian Teleworkers: Perceived Cybersecurity Governance as Moderator. In *Proceedings of the 2021 IEEE 5th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Purwokerto, Indonesia, 24–25 November 2021*; IEEE: Piscataway, NJ, USA, 2021; pp. 305–310.
14. Jarlhem, J.; Stigsson, J. Digital Vulnerability Awareness: In a "Working from Home" Environment during COVID-19. Bachelor Thesis. Available online: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1576133&dswid=3885 (accessed on 10 November 2022).
15. Dangheralou, A.; Jahankhani, H. The Impact of GDPR Regulations on Cyber Security Effectiveness Whilst Working Remotely. In *Artificial Intelligence in Cyber Security: Impact and Implications*; Springer: Cham, Switzerland, 2021; pp. 253–279.
16. Arogbodo, M. Impacts of the COVID-19 Pandemic on Online Security Behavior within the UK Educational Industry. Available online: https://doi.org/10.31234/osf.io/h5qgk (accessed on 10 November 2022).
17. Yang, J.; Linkeschová, L. Remote Working and Cybersecurity in the Pandemic: Research on the Employee Perceptions of Remote Work and Cybersecurity in an International Organisation during COVID-19. Ph.D. Thesis, University of Geneva, Geneva, Switzerland, 2021.
18. Carlsten, F.; Hultman, E.; Nilsson, D.E. Work from Home-Information Security Threats and Best Practices. Master's Thesis, Lund University, Lund, Sweden, 2021.
19. Borkovich, D.J.; Skovira, R.J. Working from home: Cybersecurity in the age of COVID-19. *Issues Inf. Syst.* **2020**, *21*, 234–246.
20. Powell, C.R. The Impact of Telework on Organizational Cybersecurity during the COVID-19 Pandemic. Ph.D. Thesis, Utica College, Utica, NY, USA, 2021.
21. Tam, L.; Glassman, M.; Vandenwauver, M. The psychology of password management: A tradeoff between security and convenience. *Behav. Inf. Technol.* **2010**, *29*, 233–244. [CrossRef]
22. Tarwireyi, P.; Flowerday, S.; Bayaga, A. Information security competence test with regards to password management. In *Proceedings of the 2011 Information Security for South Africa, Johannesburg, South Africa, 15–17 August 2011*; IEEE: Piscataway, NJ, USA, 2011; pp. 1–7.
23. Zezschwitz, E.V.; Luca, A.D.; Hussmann, H. Survival of the shortest: A retrospective analysis of influencing factors on password composition. In *IFIP Conference on Human-Computer Interaction, Cape Town, South Africa, 2–6 September 2013*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 460–467.
24. Habib, H.; Naeini, P.E.; Devlin, S.; Oates, M.; Swoopes, C.; Bauer, L.; Christin, N.; Cranor, L.F. User behaviors and attitudes under password expiration policies. In Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), Baltimore, MD, USA, 12–14 August 2018; pp. 13–30.
25. Sanok, D.J., Jr. An analysis of how antivirus methodologies are utilized in protecting computers from malicious code. In Proceedings of the 2nd Annual Conference on Information Security Curriculum Development, Kennesaw, GA, USA, 23–24 September 2005; pp. 142–144.
26. Al-Saleh, M.I.; Espinoza, A.M.; Crandall, J.R. Antivirus performance characterisation: System-wide view. *IET Inf. Secur.* **2013**, *7*, 126–133. [CrossRef]
27. Tiwari, R.K.; Karlapalem, K. Cost Tradeoffs for Information Security Assurance. In Proceedings of the Workshop on the Economics of Information Security, Cambridge, MA, USA, 1–3 June 2005.

28. Hayajneh, T.; Mohd, B.J.; Itradat, A.; Quttoum, A.N. Performance and information security evaluation with firewalls. *Int. J. Secur. Its Appl.* **2013**, *7*, 355–372. [CrossRef]
29. Lee, Y.; Kozar, K.A. An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Inf. Manag.* **2008**, *45*, 109–119. [CrossRef]
30. Gurung, A.; Luo, X.; Liao, Q. Consumer motivations in taking action against spyware: An empirical investigation. *Inf. Manag. Comput. Secur.* **2009**, *17*, 276–289. [CrossRef]
31. Albrechtsen, E.; Hovden, J. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Comput. Secur.* **2010**, *29*, 432–445. [CrossRef]
32. Almeida, F. Web 2.0 technologies and social networking security fears in enterprises. *arXiv* **2012**, arXiv:1204.1824. [CrossRef]
33. Koushik, P.; Chandrashekhar, A.M.; Takkalakaki, J. Information security threats, awareness and cognizance. *Int. J. Tech. Res. Eng.* **2015**, *2*, 19–28.
34. Rao, G.R.K.; Prasad, D.R.S. Combating Cross-Site Scripting Assaults without Proprietary Software. *Int. J. Appl. Eng.* **2017**, *12*, 6788–6796.
35. Kruger, H.; Drevin, L.; Steyn, T. Email security awareness—A practical assessment of employee behaviour. In *Proceedings of the Fifth World Conference on Information Security Education, West Point, NY, USA, 19–21 June 2007*; Springer: New York, NY, USA, 2007; pp. 33–40.
36. Rudd, E.M.; Harang, R.; Saxe, J. Meade: Towards a malicious email attachment detection engine. In *Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 23–24 October 2018*; IEEE: Piscataway, NJ, USA, 2018; pp. 1–7.
37. Wei, W.; Ding, X.; Chen, K. Multiplex encryption: A practical approach to encrypting multi-recipient emails. In *Proceedings of the International Conference on Information and Communications Security, Beijing, China, 10–13 December 2005*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 269–279.
38. Wei, J.; Chen, X.; Wang, J.; Hu, X.; Ma, J. Forward-secure puncturable identity-based encryption for securing cloud emails. In *Proceedings of the European Symposium on Research in Computer Security, Luxembourg, 23–27 September 2019*; Springer: Cham, Switzerland, 2019; pp. 134–150.
39. Roth, S.; Calzavara, S.; Wilhelm, M.; Rabitti, A.; Stock, B. The Security Lottery: Measuring Client-Side Web Security Inconsistencies. In Proceedings of the 31st USENIX Security Symposium, Boston, MA, USA, 10–12 August 2022.
40. Villamarín-Salomón, R.; Brustoloni, J.; DeSantis, M.; Brooks, A. Improving User Decisions About Opening Potentially Dangerous Attachments in E-Mail Clients. In Proceedings of the Poster, Symposium on Usable Privacy and Security, CMU, Pittsburgh, PA, USA, 12–14 July 2006.
41. Bilal, K.; Khaled, S.A.; Syed, I.N.; Muhammad, K.K. Effectiveness of information security awareness methods based on psychological theories. *Afr. J. Bus. Manag.* **2011**, *5*, 10862–10868. [CrossRef]
42. Stafford, T.; Deitz, G.; Li, Y. The role of internal audit and user training in information security policy compliance. *Manag. Audit. J.* **2018**, *33*, 410–424. [CrossRef]
43. Safa, N.S.; Von Solms, R.; Furnell, S. Information security policy compliance model in organizations. *Comput. Secur.* **2016**, *56*, 70–82. [CrossRef]
44. Herath, T.; Rao, H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decis. Support Syst.* **2009**, *47*, 154–165. [CrossRef]
45. Knapp, K.J.; Morris Jr, R.F.; Marshall, T.E.; Byrd, T.A. Information security policy: An organizational-level process model. *Comput. Secur.* **2009**, *28*, 493–508. [CrossRef]
46. Hagen, J.M.; Albrechtsen, E.; Hovden, J. Implementation and effectiveness of organizational information security measures. *Inf. Manag. Comput. Secur.* **2008**, *16*, 377–397. [CrossRef]
47. Huang, D.L.; Rau PL, P.; Salvendy, G. Perception of information security. *Behav. Inf. Technol.* **2010**, *29*, 221–232. [CrossRef]
48. Al-Molhem, N.R.; Rahal, Y.; Dakkak, M. Social network analysis in Telecom data. *J. Big Data* **2019**, *6*, 99. [CrossRef]
49. Li, K.; Cheng, L.; Teng, C.I. Voluntary sharing and mandatory provision: Private information disclosure on social networking sites. *Inf. Process. Manag.* **2020**, *57*, 102128. [CrossRef]
50. Cerruto, F.; Cirillo, S.; Desiato, D.; Gambardella, S.M.; Polese, G. Social network data analysis to highlight privacy threats in sharing data. *J. Big Data* **2022**, *9*, 19. [CrossRef]
51. Kim, J.; Mou, J. Meta-analysis of Information Security Policy Compliance Based on Theory of Planned Behavior. *J. Digit. Converg.* **2020**, *18*, 169–176.
52. Sommestad, T.; Karlzén, H.; Hallberg, J. The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Inf. Comput. Secur.* **2015**, *23*, 200–217. [CrossRef]
53. Grassegger, T.; Nedbal, D. The role of employees' information security awareness on the intention to resist social engineering. *Procedia Comput. Sci.* **2021**, *181*, 59–66. [CrossRef]
54. AlMindeel, R.; Martins, J.T. Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia. *Inf. Technol. People* **2020**, *34*, 770–788. [CrossRef]
55. Almutairi, M.M.; Halikias, G.; Yamin, M. An overview of security management in Saudi Arabia. In *Proceedings of the 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 12–14 March 2020*; IEEE: Piscataway, NJ, USA, 2020; pp. 261–265.

56. Alharbi, T. Developing Cost-effective Cybersecurity Management System for Academic Institutions in Saudi Arabia. *J. Eng. Appl. Sci.* **2022**, *9*, 57. [CrossRef]
57. Alsulami, M. Social Media Security Awareness in Saudi Arabia. *Tehnički Glasnik* **2022**, *16*, 213–218. [CrossRef]
58. Gull, H.; Saeed, S.; Iqbal, S.Z.; Bamarouf, Y.A.; Alqahtani, M.A.; Alabbad, D.A.; Saqib, M.; Al Qahtani, S.H.; Alamer, A. An empirical study of mobile commerce and customers security perception in Saudi Arabia. *Electronics* **2022**, *11*, 293. [CrossRef]
59. Alzubaidi, A. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon* **2021**, *7*, e06016. [CrossRef] [PubMed]
60. Aljohni, W.; Elfadil, N.; Jarajreh, M.; Gasmelsied, M. Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 276–281. [CrossRef]
61. Shahid, J.; Ahmad, R.; Kiani, A.K.; Ahmad, T.; Saeed, S.; Almuhaideb, A.M. Data protection and privacy of the internet of healthcare things (IoHTs). *Appl. Sci.* **2022**, *12*, 1927. [CrossRef]
62. Iqbal, Y.; Tahir, S.; Tahir, H.; Khan, F.; Saeed, S.; Almuhaideb, A.M.; Syed, A.M. A Novel Homomorphic Approach for Preserving Privacy of Patient Data in Telemedicine. *Sensors* **2022**, *22*, 4432. [CrossRef]
63. Zulkifl, Z.; Khan, F.; Tahir, S.; Afzal, M.; Iqbal, W.; Rehman, A.; Saeed, S.; Almuhaideb, A.M. FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs. *IEEE Access* **2022**, *10*, 15644–15656. [CrossRef]
64. Faklaris, C.; Dabbish, L.A.; Hong, J.I. A {Self-Report} Measure of {End-User} Security Attitudes. In Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), Santa Clara, CA, USA, 11–13 August 2019; pp. 61–77.
65. Security Awareness Survey. Available online: https://www.securitymentor.com/resources/surveys/security-awareness-survey (accessed on 17 October 2022).
66. Hammarstrand, J.; Fu, T. Information security awareness and behaviour: Of trained and untrained home users in Sweden. Bachelor's Thesis, University of Borås, Borås, Sweden, 2015.
67. Computer and Information Security End User Questionnaire. Available online: https://cqpi.wisc.edu/wp-content/uploads/sites/599/2016/07/Pilot_Study_Questionnaire.pdf (accessed on 17 October 2022).
68. SANS Security Awareness, Human Risk Assessments and Surveys, SANS Institute. Available online: https://www.sans.org/blog/getting-support-for-your-human-risk-assessments-and-surveys/ (accessed on 17 October 2022).
69. Parker, C.; Scott, S.; Geddes, A. *Snowball Sampling*; SAGE: New York, NY, USA, 2019.
70. Zickar, M.J.; Keith, M.G. Innovations in Sampling: Improving the Appropriateness and Quality of Samples in Organizational Research. *Annu. Rev. Organ. Psychol. Organ. Behav.* **2023**, *10*, 315–337. [CrossRef]
71. Vinzi, V.E.; Chin, W.W.; Henseler, J.; Wang, H. *Handbook of Partial Least Squares: Concepts, Methods and Applications*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2010.
72. Hair, J.F.; 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]
73. Discriminant Validity. Available online: https://www.analysisinn.com/post/discriminant-validity-through-fronell-larcker-criterion/#:~:text=The%20Fronell%2DLarcker%20criterion%20is,construct%20and%20any%20other%20construct (accessed on 17 October 2022).