Journal of
Cybersecurity and Privacy

MDPI

Article

Work Experience as a Factor in Cyber-Security Risk Awareness: A Survey Study with University Students

Tibor Pósa * and Jens Grossklags

Department of Informatics, Technical University of Munich, 85748 Garching, Germany; jens.grossklags@in.tum.de
* Correspondence: tibor.posa@tum.de

Abstract: The emergence of the COVID-19 pandemic in early 2020 has transformed how individuals work and learn and how they can apply cyber-security requirements in their, mostly remote, environments. This transformation also affected the university student population; some needed to adjust to new remote work settings, and all needed to adjust to the new remote study environment. In this online research study, we surveyed a large number of university students (n = 798) to understand their expectations in terms of support and help for this new remote work and study environment. We also asked students to report on their practices regarding remote location and Wi-Fi security settings, smart home device usage, BYOD (bring your own device) and personal device usage and social engineering threats, which can all lead to compromised security. A key aspect of our work is a comparison between the practices of students having work experience with the practices of students having no such additional experience. We identified that both the expectations and the level of cyber-security awareness differ significantly between the two student populations and that cyber-security awareness is increased by work experience. Work experience students are more aware of the cyber-security risks associated with a remote environment, and a higher portion of them know the dedicated employee whom they can contact in the event of incidents. We present the organizational security practices through the lens of employees with initial work experience, contributing to a topic that has so far received only limited attention from researchers. We provide recommendations for remote study settings and also for remote work environments, especially where the existing research literature survey results differ from the findings of our survey.

Keywords: cyber-security risks; remote work and Wi-Fi risks; cyber-security awareness; smart home device risks; social engineering in cyber-security; shadow IT security; cyber-security risk measurement

check for updates

Citation: Pósa, T.; Grossklags, J. Work Experience as a Factor in Cyber-Security Risk Awareness: A Survey Study with University Students. *J. Cybersecur. Priv.* **2022**, *2*, 490–515. https://doi.org/10.3390/jcp2030025

Academic Editor: Steven Furnell

Received: 24 February 2022
Accepted: 16 June 2022
Published: 28 June 2022

1. Introduction

The sudden arrival of COVID-19 and the later geographic spread of the pandemic has transformed the everyday life of 7.8 billion people globally. Similarly, a large proportion of the world's population underwent radical changes in many work-related activities, which also influenced cyber-security and privacy concerns due to the nature of work-from-home or remote location settings.

Historically, remote work or distance work started to gain momentum in the early 1980s and 1990s [1], when telecommunications technology began to make it a viable option for a number of professions. The spread of Wi-Fi and virtual private network (VPN) [2] technologies in the early 2000s extended this option to a wider circle of employees and industries. Consequently, remote work and other remote activities are not new phenomena. What is new, however, is the acceleration of the change from the old norm of office-based work and other on-site activities to the new norm of remote and home-based activities, or at very least a significant increase in a hybrid approach.

Looking forward, there is also a debate about how many of these changes will last and which entities, such as employers and other institutions, will settle into this new reality. Some employers and educational institutions have opted to make a permanent change in their mode of operation. Large global consultancy companies and technology giants have already stated that employees need no longer go into the office [3], with the exception of one or two days a month. Some education institutions, such as colleges and universities, have decided to move graduate programs online, with just a few exemptions for irregular campus visits, or have permanently changed their online strategy to ensure that the programs remain relevant [4]. It is important to note that these decisions are not independent of the declared priorities and preferences of employees and students [5]. For example, several technology and other companies surveyed their employees in early 2021, prior to the anticipated migration back to regular office settings during the subsequent months. They concluded that, in spite of potential incentives and previously held employer beliefs, employees do not necessarily want to return to the office environment (see, for example, [6]). In the online surveys, employees listed numerous advantages of remote working.

However, the increasingly important work-from-home setting poses a number of challenges for both individuals and organizations. Companies and other organizations need to ensure that adequate protection is available at each endpoint [7]. As initial studies have shown, depending on the time and energy invested prior to the pandemic, there is a wide spread in the readiness and actual resilience of individuals and organizations [8]. Moreover, cyber-security attack surfaces are continuously developing and expanding. For example, prior to the pandemic, the smart home domain did not affect organizational cyber-security preparation as much as it does now since the shift to a remote or home environment [9]. Further, while transitioning to the remote environment at an increased rate, the necessary increase in security-related education and awareness did not always take place in parallel [10]. For example, while VPN usage is a proactive security measure in many organizations, users may still face security threats and attacks due to the use of unsecured Wi-Fi networks or other unsecured devices in the home environment [11]. In addition, higher education campuses have also been transformed [12], and e-learning platforms have become the norm, enabling a hybrid learning strategy. Finally, while the existing literature is detailed enough to describe the technical aspects and the importance of education or cyber-security awareness training in general when transitioning to the remote environment, other factors are less frequently analyzed.

To contribute to this research area, we surveyed two lecture groups of bachelors and masters students (n = 798) from the Technical University of Munich (TUM), both registered for comparable information technology lecture courses. Through the analysis of the data from the detailed questionnaire, we attempt to assess the cyber-security-related awareness and perception differences between students with and without work experience. In particular, we aim to explore whether work-related experience is associated with significantly increased cyber-security and privacy awareness amongst university students. More specifically, we raise and attempt to answer the following research questions:

- What is the role of initial work experience at student age in improving cyber-security risk awareness?
- What are the specific security topics where increased awareness is associated with work experience, and what are the topics that are unrelated?

Our guiding expectation is that various measures in the work environment, that normally include IT and security policy frameworks, regular and focused tutorials, corporate IT devices or applications with physical, logical and functional access restrictions, all contribute to higher cyber-security awareness. We also assume that these characteristics of the work environment have such a significant effect that even a comparatively short period of work experience will serve to differentiate between students with and without work experience and that this difference can be measured. Using the online survey results, together with the existing literature, our aim is to formulate recommendations and improvement points for organizations.

The paper is organized as follows. In Section 2, we discuss related work and introduce the four topic categories that form the basis of our survey. In Section 3, we introduce our survey study approach and summarize demographic details of the survey participants. We present our analysis of the survey data in Section 4. We discuss our findings in Section 5, before we offer concluding remarks in Section 6. Supplementary materials are included in Appendixes A–C.

2. Related Work

2.1. Cyber-Security Risk Landscape and Information Security Awareness

Information security awareness (ISA) and cyber-security awareness and the associated risks are interrelated in any given institution, both in educational and corporate settings. There are a number of theories describing employee behavior relating to ISA, but prior work has shown that four theories, in particular, have been researched and tested in individual studies [13]: the Theory of Planned Behavior, General Deterrence Theory, Protection Motivation Theory, and the Technology Acceptance Model.

Employee behavior, driven by IS knowledge and other factors such as culture and personality, is such a crucial factor in adapting to and enhancing ISA that systematic research has attempted to identify the key drivers for ISA enhancement in private and public entities [14]. Among other approaches, regular training (including gamification models) and regular employee awareness campaigns were highlighted as highly effective and common in both private and public organizations, including universities. The actual ISA behavior of university students and the individual drivers behind that behavior were analyzed in a survey study [15]. The overall assessment indicated that certain individual factors, including higher age, area of study (e.g., IT studies), contribute to increased ISA, whereas there was no statistically significant correlation identified between work experience and ISA. The one factor also highlighted in the same survey study as a statistically significant contribution to both calculated and perceived ISA was the availability of training and awareness programs.

Some universities already offer comprehensive ISA training programs, but they lack a strategy for persuading students to participate in these programs [16]. ISA training is such an important factor that even public institutions have to plan by job category in order to determine existing awareness gaps and risk levels in each job category [17]. In each institution, whether private or public, the success of the ISA-related training framework will depend on how much the actual program is tailored to the individual employee's or user's needs and perceptions. One research article [18] clearly highlights that the success of security education, training, and awareness (SETA) programs depends on numerous factors that directly (30 factors) or indirectly (19 factors) influence individual behavior. Typical examples of directly influencing factors include culture, security policies or perceived social norms, while typical examples of indirectly influencing factors include control and sanctions, general attitude to social norms and law or self-control. These individual factors can differ significantly, and any given institution must tailor the design, implementation and follow-up of their own SETA programs accordingly.

There are also a number of cyber-security risk factors affecting employees in organizational settings such as spam emails, malware, ransomware, fake social accounts, mobile device threats and many more. Prior work has attempted to list and analyze the most important factors [11,19] and partially also focused on sorting or clustering them in broad categories to support mitigation strategies in the constantly evolving risk landscape. However, we could not identify a cyber-risk categorization methodology in the literature that would be universally accepted for *remote and work-from-home* environments. For example, there is an incident information clustering methodology proposal at a national level [20], but the focus is on incidents and not risk, while corporate specifics are not evaluated. Other approaches define cyber-risk with operational risk categories relating to IT assets and IT systems [21] while not emphasizing electronic communication networks.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework was first introduced in the United States in 2014 and has quickly become the de facto standard of IT executives and has been globally adopted [22]. Despite its popularity, gaps have also been identified, including the underrepresentation of organizational climate (organizational culture) and social aspects. Indeed, achieving compliance is significantly influenced by organizational culture and social aspects, which was established by previous work [23]. For example, cyber-incident reporting and processing can often suffer from underreporting or incorrect reporting in practice [24].

A discussion of the cyber-security risk landscape would not be complete without mentioning cyber-risk insurance. The existing research literature [25] illustrates that cyber-risk insurance started to gain momentum in the early 2010s, but the calculation of policy premiums is often decided primarily based on metrics related to revenue or the number of employees. Another key factor that should affect cyber-insurance take-up at a detailed level is organizational behavior such as the actual preparedness with backup management and other organizational factors. Ransomware attacks are a good example of a threat scenario [26], where the actual willingness of insurance companies to underwrite policies should be closely related to organizational preparedness. Recently, when cyber-security attacks grew due to the pandemic, other challenges affecting the cyber-risk insurance industry were also highlighted [27].

The various existing methodologies all have merit in terms of attempting to list and report relevant individual cyber-security risk factors. Our aim is not to offer a new methodology for identifying or categorizing cyber-security risk factors but rather to discuss different existing and evolving cyber-security risk items that are of relevance to the work-from-home context. This categorization approach will then be used for the online survey and the discussion of the survey results in later sections.

The proposed approach will place important known cyber-security risk factors associated with remote work into four categories. The four proposed categories are: (1) remote work and Wi-Fi settings, (2) smart home devices, (3) personal devices, BYOD or BYOS (bring your own service), and (4) social engineering threats. We discuss these categories in the following subsections. In particular, we briefly discuss the various technologies and practices that are then addressed in the survey.

2.2. Remote Work (Study) Security and Wi-Fi Settings

An important security challenge that any user faces when transitioning to a remote (home) location is the method of electronic communication. Within a company or other organization, the offered methods of electronic communication may include wired or wireless options. These organizational settings can define a general security framework supported by applications, network and hardware security features as well as a wide range of policies that users are required to comply with. Governance of IT security is also typically in place, and third parties, such as consultants, can review the IT security preparedness either on request or based on regulatory and other legal requirements.

The remote location, typically the home environment, mostly has one device that channels all electronic communications. This device, the Wi-Fi router, is also a central hub for all other smart devices present in the same environment. The security of this device is essential for establishing a secure line of communication [28]. As such, it needs to be continuously maintained to keep up with the growing use of this wireless technology.

The term Wi-Fi broadly refers to a family of wireless network protocols based on the standard family of IEEE 802.11 a/b/g/n. Wi-Fi is pervasively used for access in private homes, within offices, at publicly available places, etc. [28]. The typical security and encryption protocols (WEP, WPA, WPA2, WPA3) are used by all remote users, while Wi-Fi router devices allow the selection of the required level of security for individual cases. There is a wide range of security issues relating to Wi-Fi communication technology [29]. The WEP protocol is renowned for its security weaknesses relating to the encryption mechanism, capture of wireless signals and eavesdropping attempts. The WPA security protocol was introduced to tackle these shortcomings, but surprisingly WEP is still offered by Wi-Fi device manufacturers as an available option when users are setting up these devices. The WPA protocol also has vulnerabilities [30], such as susceptibility to FMS attacks aimed at recovering secret keys, but subsequent versions have been developed to mitigate these risks. WPA2/WPA3 are considered to be the current protocol of choice for remote users, with WPA3 addressing most but not all of the attack vectors applicable to WPA2 [31].

VPNs are another technology tool used by both organizations and individuals to increase the security of electronic communication through encryption. Among the many technology solutions present in the market today for organizations working in a remote setting, VPN is the solution of choice for creating a secure connection through the public Internet by extending the private network. It provides the convenience of a public network combined with the security of a private network by establishing a tunnel between sender and receiver. VPN technology has evolved over time, and considerable energy and effort have been invested in designing a secure networking model [32]. A number of vulnerabilities have been exposed and listed in the context of VPN hardware, software, configuration and actual implementation [33], thus organizations must assess their own VPN configuration on a regular basis to mitigate the risks.

Remote employees are also often instructed to work with smartphones together with traditional computers and laptops. The typical employee smartphone will provide access to the same electronic mail system and other applications as are available on computers and laptops. A mobile device VPN can help to address security and data privacy issues when these devices and the installed apps have access to organizational or customer data. Research has shown [34] that the conceptual model and design methodology of mobile VPN can use the experience accumulated through the use of VPN technology with non-mobile devices, but it also needs to provide convenience for the mobile users. The mobile VPN has several security benefits [35], including easy access to organizational data, and the same level of security that is already present in the remote (home) environment.

We analyze the topics of Wi-Fi settings, VPN usage and other details later in our survey results, with a focus on comparing the actual practices of students with and without work experience (see Section 4.1).

2.3. Smart Home Devices

Smart home systems represent the most dominant and exponentially growing segment of IoT (Internet of Things) devices penetrating home environments. Smart TVs, smart household devices, sensors and other devices provide convenience for the user but also introduce security and privacy concerns that are complex to manage [36]. In the United States, 69% of households have at least one smart device at home, and 12% have more than one device, meaning that there will only be a small number of remote workers where the remote (home) location does not include any of these smart devices.

The available technology for smart home settings and home automation [37] includes a number of solutions for user interfaces (central point to control the system) and options for transmission (wired or wireless). Almost all of them use the same communication interface, with a Wi-Fi router present in most homes, and only a few of them use other options, such as direct access to telecommunication networks.

Although the smart home is a very different environment, the overall nature of security threats is related to threats in other domains. Confidentiality, authentication and integrity threats are also present in the home environment [38]. Most smart devices are designed to be low cost in order to achieve high market penetration, and, therefore, security or privacy concerns do not necessarily have a high priority in the device manufacturing process. The average home user has a widely varying degree of technical knowledge and also a varying degree of security awareness of potential risks. As such, the installation and configuration of these smart devices are often in the hands of mostly untrained users.

A number of smart home device manufacturers assume that they can delegate security to the smart home's underlying architecture, such as the Wi-Fi router firewall [39]. This approach can result in exploitation by malicious third parties, which can include eavesdropping, impersonation, software exploitation and other attack vectors. One recommendation of manufacturers is proper and tailored installation and configuration. The other recommendation for the whole lifecycle of devices is regular updating of the device software.

Voice activation is an additional feature recently added to some smart home devices. The benefit is the convenience of control and comfort of usage the risks are new attack vectors and access to sensitive user data [40]. The mitigation of these newly emerged risks is ongoing, but one minor step is changing the initial voice activation code or phrase immediately after installation.

We investigate the topics of smart home device security settings, smartphone usage and other details for both student groups in our survey results section (see Section 4.2).

2.4. Personal Devices and Shadow IT, BYOD

Utilizing personal IT devices, software applications or other IT services for remote work is not a new phenomenon. However, the sudden transition to the remote (home) environment in early 2020 accelerated the adoption of this practice by users and organizations. Users suddenly had to rely on what they already privately owned to complement the IT support they received from their organization.

There are a number of definitions for shadow IT, and we use the terminology described in [41]: "...shadow IT which is hardware, software, or services built, introduced, and/or used for the job without explicit approval or even knowledge of the organization". The category of shadow IT is related to the categories of BYOD (bring your own device) or BYOS (bring your own service), where users are encouraged to use their own devices according to preset rules and conditions. The key challenge for any organization is the IT governance and control over the use of private devices and services [41].

Existing literature [42] indicates that governing shadow IT or, more generally, the usage of personal IT space is unlikely to be beneficial for both organizations and users without some sort of dialogue. One survey [43] of three private and two public companies has also identified how hard it is to come to an agreement between an organization and its employees when users are very selective in what policy and regulation details they are willing to accept. Another factor described is user alignment and user acceptance when faced with technology upgrades relating to BYOD devices and technology [44]. This study demonstrates that even a technology solution that has enhanced security can result in user resentment or opposition without the required alignment. The requirements are defined by the organization through informal and formal channels, where policies and guidelines cover only the formal part. There are two different aspects for users to think about when considering shadow IT [45]. The first relates to application development when the current application functionalities do not match user expectations. The second relates to the benefit of potential innovation. This can be the case if application development meets the rigorous functionality, regulatory and other requirements.

Shadow IT could also become a governance issue from a different perspective. In a decentralized unit of an organization, without the consent and knowledge of the central IT function, users could even develop an application that did not go through the regular security, functionality and other tests.

Within the shadow IT space, the governance of personal devices can be partially implemented and controlled. Deactivating USB connections on company devices or restricting access to core applications via VPN tokens on company laptops are two good examples of this. Governance of shadow IT applications is more complicated, and there are parts of the shadow IT space that might require even more attention, such as the use of personal cloud services. Recent research [46] has shown that many open questions still exist about what action to take in organizations where the use of personal cloud services intersects with the use of organizational data.

There are also a number of open research directions [42] that can be identified for future shadow IT research, e.g., exploring generation Z's attitudes and behaviors towards shadow IT.

We address the topics of personal device usage, cloud services usage and other details through targeted survey questions (see Section 4.3).

2.5. Social Engineering Threats

Social engineering can occur in many different—simple and complex—ways and has emerged as one of the most challenging cyber-security threats [47]. Hadnagy [48] defines social engineering as "any act that influences a person to take an action that may or may not be in their best interest". It is important to note that the nature of the threat is not primarily technical because the exploitation of vulnerabilities focuses on the human element to achieve the attacker's objectives.

Since many users transitioned to a remote environment in early 2020, the security threats through social engineering techniques have multiplied [49]. When faced with potential threats, the same user who had access to peer communication or feedback in an office or campus environment is much less able to rely on this method in the absence of physical proximity to other users. Phishing emails or impersonation via phone calls are good examples of security-related social engineering threats, but there are a number of others, such as identity theft, targeted attacks (CEO fraud) or something as simple as dumpster diving.

Social engineering attacks are often blended with other methods of attack. The Twitter attack of 15 July 2020 [50] is a good example of this approach. The perpetrators offered small incentives and used other technical skills to obtain employee credentials and, ultimately, earnings denominated in Bitcoin. All these steps were supported by social engineering skills, including impersonation and pretending to be a company employee.

The complexity of these types of cyber-security attacks using the arsenal of tools available to a skilled social engineering adversary means that mitigation efforts frequently lag behind the knowledge and experience of the perpetrators. Furthermore, the countermeasures need to take into account that these attacks focus on all types of users and employees, not just IT or IT security employees. Many organizations have realized that there is little chance of addressing these threats and improve employee behavior without heightening awareness through training.

A number of research studies highlight that all users or employees need to be aware of important social engineering attack vectors because technical measures (such as email filtering) are not sufficient for managing these events. User knowledge and attitudes towards organizational policies and guidelines are both important [51] when fighting attacks. In addition, prior work [52] highlights the importance of introducing a training and awareness framework in a sophisticated manner. Information Security Awareness (ISA), Information Security Education (ISE) and Information Security Training (IST) can differ in the method of delivery or the purpose and focus, but they are all needed in the organizational journey to a better mitigation program.

A literature review [47] concluded that there is no better option than regularly investing in users and employees by providing them with education and frequent training. In a number of cases, perpetrators seem to have a lead due to the nature of the quickly evolving attacker skill set. This makes it even more important to understand actual user behavior and the practice of user self-reporting, relating to social engineering attacks and attempted attacks.

We analyze the topics of phishing emails, as well as regular training options and other social engineering threat mitigation options in Section 4.4.

3. Materials and Methods

Our study focused on university bachelor and masters students (Technical University of Munich, TUM) during their study programs, where all survey participants were registered for comparable interdisciplinary information systems lecture courses.

The online survey was conducted in July 2021, during which time students had been assigned practical tasks as part of the courses, which included a limited number of research-related activities. The SoSci survey platform (https://www.soscisurvey.de/en/ (first accessed for this project on 20 June 2021)) was selected for the survey based on the data protection arrangements of this survey site. Each survey participant could select between two options, completing the survey as a work experience student or as a student without work experience. Students were asked to classify themselves as those with remote work experience if they had any remote work experience since March 2020 (start of the pandemic), including their current work experience (see Appendix B). Remote work was defined as an arrangement in which employees do not commute or travel to a central place of work, such as an office building or other facility. Work experience could include part-time or full-time work, internship or any other work-related activity. Students were asked to self-categorize as those without remote work experience if, since March 2020 (start of the pandemic), they had no remote work experience at all.

The online survey was structured into five distinct sections; four related to cyber-security risks, and the fifth related to demographics. Demographic questions covered age, work or study location, work-related role and the length of experience plus other details.

Each of the four cyber-security-related topics, i.e., (1) covering remote work and study with Wi-Fi settings, (2) smart home device usage, (3) BYOD and personal device usage, and (4) cyber-security-related social engineering threats, had ten to fifteen questions. We approached each of the four broad topics with a distinct block of questions; however, with a consistent structure. First, we inquired about formal organizational policy expectations, including policies or guidelines. Organizational policy was defined as company or corporate policy for those who completed the survey as a work experience student and university policy for those who completed the survey as a student without work experience. Second, we asked for the expected level of support needed in the given topic space in order to understand if the level of current support was sufficient or additional support was needed. Third, we asked participants to describe the possible technology guidance that they would need or information about technologies they would potentially try themselves. This would include targeted training courses or case studies and utilization of organizational technology solutions for personal use. Fourth, we assessed the actual security practices through detailed technology questions. Depending on the topic block, we asked for details such as password management, reporting of unusual emails and phone calls, practices for managing application and smartphone apps, or the management of smart home devices.

All survey participants were informed about the survey procedure and data privacy details and explicitly asked to give consent of their agreement to those details (see Appendix A). Those participants who did not agree with the consent form or did not fully complete the survey were removed from the dataset, and their data were not part of any further analysis. Completion of the survey was voluntary but incentivized as part of a series of tasks awarding a grade bonus for the final exam.

Threats to validity were evaluated for a number of topics to avoid potential bias in the collection, processing and evaluation of data. Firstly, the full set of survey questions was evaluated by volunteer participants on the survey platform prior to the launch of the survey to avoid ambiguous question wording and to provide general feedback. Secondly, the surveyed student population was selected to be large enough to create a diverse sample regarding experiences but also demographic and non-demographic factors. Thirdly, participants were recruited from two interdisciplinary information systems lecture courses from two different study programs, which increases the diversity of the surveyed population; however, all participants had some connection to IT-related study subjects. Fourthly, our survey data collection is affected by the inherent limitations of self-reporting. Lastly, participating students completed the survey online. Paper-based survey completion was not a viable option during the pandemic, and the online survey ensured the anonymity of all participants. Survey completion was incentivized by being part of a number of voluntary tasks to become eligible for a grade bonus on the final exam. The survey did not stand out in terms of time commitment or complexity of the task.

Most of the participants (85.8%) were students within the 18–25 age range, while 10.9% were in the 26–29 age category, with only the remaining 3.3% either below the age of 18 or above the age of 29 (see Table 1).

There was a higher proportion of male students (n = 464, 58.0%), a smaller proportion of female students (n = 323, 40.5%), and the remaining students (n = 11, 1.5%) chose not to disclose their gender details.

Survey participants were classified as either work experience students (n = 448) or students without any work experience (n = 350). Table 2 summarizes the self-reported duration of work experience.

Table 1. Age distribution of participants.

Age Category	Number	Percentage
under 18	3	0.4%
18–21	374	46.9%
22–25	311	38.9%
26–29	87	10.9%
30–33	11	1.4%
34–37	2	0.2%
Over 37	4	0.5%
Not disclosed	6	0.8%
Total	798	100.0%

Most of the students (n = 594) were residents in Germany, while the remainder (n = 204) self-reported to normally reside outside Germany or outside Europe. The regular place of remote work and remote study was the home location or the student dormitory location, and only a small number of students selected other alternative locations.

Table 2. Work experience distribution of participants.

Work Experience Category	Number	Percentage
0–6 months	181	40.4%
6–12 months	106	23.7%
1–2 years	87	19.4%
2 years or more	74	16.5%
Total	448	100.0%

We used statistical analysis to substantiate cyber-security awareness differences between the two subgroups of students (students with and without work experience). Primarily, we conducted Pearson's chi-square tests to assess whether the frequency distributions of the comparable survey questions (students with and without work experience) are independent of each other. When any other statistical method or analysis was used, the details are highlighted in the results part of this paper.

We defined survey questions to be as comparable as possible for the two subgroups of students (students with and without work experience); the only difference was typically in the survey question wording itself (question either included "remote work" or "remote study"). We carefully pretested the survey with various colleagues and integrated any feedback received. Sample questions for the different topic categories and for the two subgroups of students are available in Appendix C.

4. Results

In this section, we provide a detailed account of the results for the four cyber-security related topics in the respective subsections. We also offer a summary of key findings for each topic in tabular form.

4.1. Remote Work (Study) Security and Wi-Fi Settings

Formal cyber-security requirements for remote work and remote study provide users or employees working away from the office or campus environment with crucial information. These requirements can guide the regular work or study behavior and, in the case of questions or doubt, can help to identify the policy details that each user should comply with or raise questions referenced to the policy details. These policy details are usually covered in various guidelines, including the IT security policy, cyber-security policy, remote work or study policy, or other comparable policies. Our first question covered the organizational policy expectations of the participants.

Survey results (Table 3) indicate that students with work experience (W) are already aware of these policies, and more than half of them (W: 51%) can name one that includes guidance on remote work. Students without work experience (NW) rarely mention any source of guidance (NW: 10%) for compliant behavior. The policy awareness difference compared to the work student population is significant ($p < 0.001$). Likely reasons for this finding are that either non-working students do not familiarize themselves with relevant university policies, or these policies do not specifically address remote study.

Table 3. Summary of key findings: Remote work (study) security and Wi-Fi settings.

Question Category	Key Findings
Informal and formal policy expectations	Work experience students are more likely to be aware of remote work policies. **($p < 0.001$)**
User expectations	Work experience does not translate into a significantly increased support need. ($p = 0.68$)
Technology guidance	Work experience is more likely associated with facing a mandatory requirement to use 2FA for VPN access from the remote environment. **($p < 0.001$)** Work experience students are more likely to have received cyber-security training in the past 12 months. **($p < 0.001$)**
Assessment of actual technology and practices	Work experience students are less likely to forward emails to private email accounts. **($p < 0.001$)** Work experience does not translate into a significantly increased level of security for Wi-Fi protocol settings. ($p = 0.74$) Work experience does not translate into a significantly increased awareness in relation to updating the initial Wi-Fi password. ($p = 0.59$) Work experience does not translate into a significantly increased security awareness regarding devices with legacy operating systems (Windows 7 or XP) being connected to the home Wi-Fi network. ($p = 0.54$) Work experience does not translate into a significantly more likely usage of more complex Wi-Fi passwords. ($p = 0.69$) Work experience students are more likely required to use a VPN when connecting to the organizational network from the home Wi-Fi network. **($p < 0.001$)**

These differences do not translate into different levels of cyber-security support need. When testing the independence of the answer frequencies ($p = 0.68$), both groups of students are almost equally satisfied with the currently offered support and rarely mention the need for any potential additional support, such as advice on the type of Wi-Fi router or enhanced VPN security. However, there is a significant ($p < 0.001$) difference in the variation of answers on cyber-security training details. Students with remote-work experience often confirmed that they received cyber-security-related training during the past 12 months (W: 35%), whereas for the group without work experience, this figure was much lower (NW: 1%).

Forwarding of university or company emails to private email accounts is a practice found in both surveyed student groups, but there are major differences ($p < 0.001$). While 81% of students without work experience regularly do this, less than 5% of the work experience students do. This is one policy detail that many companies emphasize even during onboarding training and through discussions with fellow employees, but there are also employers who are lenient about this security practice [53].

One area where work experience does not appear to enhance security awareness ($p = 0.69$) is Wi-Fi password usage. Both working and non-working students confirmed (W: 74% and NW: 75%) that they use complex passwords, defined by a number of characteristics, including 8–10 characters, a variety of symbols, special characters and lowercase and uppercase letters. In previous research, student employees with onboarding experience [53] described that even limited training covered password usage and regular password update. Acceptance of the creation and maintenance of complex passwords for the whole password cycle is also related to the overall awareness of IT system security and cyber-security policies [54]. One possible driver for this high password security awareness is probably linked to age. Generation Z (born between 1997–2012) is the age group of most survey students. The available research [55] confirms that even at the elementary school age, the population of Generation Z already had the appropriate mental models and understood the reasons for password protection, while they already managed 5–6 passwords both in school and at home.

Survey results also confirm that usage of secure Wi-Fi security protocols ($p = 0.74$) and following the practice of changing the factory-provided Wi-Fi password ($p = 0.59$) are independent of work experience. Further, we did not observe that usage of devices with legacy operating systems (that are no longer supported by the manufacturer) connected to the Wi-Fi network differed across the two groups ($p = 0.54$).

Most of the students (W: 72% and NW: 77%), who reported using Wi-Fi security protocols, have a WPA2 setup. However, in each survey group, almost half of the participants could not identify or recall the actual Wi-Fi security setting. This result might indicate that at least some of these Wi-Fi devices are not protected at all. Existing literature has estimated the unprotected portion of home Wi-Fi devices to be 35% [56], which is comparable with our results, if we assume that at least half of the unidentified cases are actually unprotected. An initial Wi-Fi password update was not performed by an almost identical portion of each survey group (W: 37%, and NW: 36%). We could not identify a research paper specifically measuring Wi-Fi password updates, but one recent general password usage survey of 2500 consumers [57] reported that 35% never updated their passwords. Our results are in line with those survey findings and further highlight to any corporate IT security manager that a perhaps surprisingly weak link is present in many remote work environments.

Another actual practice that increases risks is the presence of devices with operating systems (Windows 7 or Windows XP) that are no longer supported by the manufacturers. Both student groups confirmed the presence of these devices (W: 11% and NW: 15%). These figures are also confirmed by recent research papers, including [58], citing statistics that 20% of all computers with a Windows operating system are still using Windows 7. However, the number of computers with Windows XP is much smaller, only in the single digit percent range and in continuous decline [59].

As one additional technology solution, a VPN connection is considered to be standard for many companies and also becoming a useful tool in many university environments. While VPN usage in company environments is required for remote access in general, in our surveyed university environment, it is only necessary to connect to specific services (e.g., to access library resources). Only 30% of non-working students stated that they were unable to connect to (a part of) the university network without VPN. In contrast, the same figure was 60% for work experience students when referring to their organization's network ($p < 0.001$).

A 2FA (two-factor authentication) can further strengthen the access security of the VPN connection. In total, 25% of students with work experience confirmed that this is already mandatory, while only 1% of the non-working students faced such a mandatory requirement ($p < 0.001$).

We attempted to identify an additional layer of factors within the work experience student population that could have an increased positive effect on cyber-security awareness. We did not include the study-only students in this additional analysis because they had not received formal training from the university in most cases. We analyzed the potential correlation between work-provided security training and general remote work behavior. We used ordered logistic regression to identify a relationship between formal remote work training (independent variable) and key areas such as "email forwarding to private email accounts" and "family members sharing work devices" as dependent variables. Our results show that work experience students who received formal remote work training are less likely to share their work devices with family members ($p < 0.05$), but such training did not result in less forwarding of work emails to private accounts ($p = 0.31$).

As a first takeaway, we argue that the survey results in the topic block of remote work and Wi-Fi security support the view that there is a relationship between work experience and increased security awareness. However, this does not apply to all technologies and security practices, such as password security.

4.2. Smart Home Devices

Smart home devices are present in almost all private homes. This makes it even more important to understand the corresponding security implications. We know that most students with or without work experience both confirmed the home as the regular work or study location, at least since the start of the pandemic. The following tables show the distributions for the regular work (Table 4) or study location (Table 5) of the participants. Table 6 summarizes the key results from this section.

Table 4. Regular location of students with work experience.

Location	Number	Percentage
Home	381	85.0%
Student dormitory	45	10.0%
Work office	12	2.7%
Other location	7	1.6%
Do not want to disclose	3	0.7%
Total	448	100.0%

Table 5. Regular location of students without work experience.

Location	Number	Percentage
Home	270	77.1%
Student dormitory	66	18.9%
Other location	12	3.4%
Do not want to disclose	2	0.6%
Total	350	100.0%

The majority of work experience students (87%), as well as students without work experience (97%), are unaware of formal cyber-security requirements regarding smart home devices, but a statistical difference between the groups is nonetheless apparent ($p < 0.001$). To put it differently, at least some working students (13%) can name an actual policy or regulation in this topic domain, such as a cyber-security policy, IT security policy or some other relevant policy documents. The corresponding proportion for students without work experience was only 3%.

The required cyber-security support relating to smart home devices is not different for the two student groups. When testing the independence of the answer frequencies ($p = 0.087$), both groups of students are almost equally satisfied with the currently received support. However, a minority (24% and 29%) mention the need for potential additional support, such as recommended lists of smart devices or standard security packages for different smart devices. These results are in line with research paper conclusions relating to requested user support. One recent interview study of smart home device users [60] highlighted that users understand risks associated with smart home devices, but they are willing to accept these in exchange for perceived benefits.

Table 6. Summary of key findings: Smart home devices.

Question Category	Key Findings
Informal and formal policy expectations	Work experience students are more likely to be aware of smart device policies. **(p < 0.001)**
User expectations	Work experience does not translate into a significantly increased support need. (p = 0.087)
Technology guidance	-
Assessment of actual technology and practices	Work experience is more likely associated with careful usage of smartphones when accessing smart devices through public Wi-Fi connections. **(p < 0.001)** Work experience does not translate into a significantly increased likelihood of conducting smartphone security updates. (p = 0.097) Work experience does not translate into a significantly increased likelihood of changing the initial voice-activated password on smart home devices. (p = 0.0634)

Smartphone usage and specifically managing smart home devices with these phones through public Wi-Fi connections differs significantly. Company devices, including company smartphones, are able to access even core applications and are in many cases subject to the same security governance standards as company computers. For this reason, it is no surprise that work experience students manage these devices more carefully and rarely (11%) use public Wi-Fi connections to manage their home smart devices. Contrary to this practice (p < 0.001), students without work experience use public Wi-Fi with their own smartphone for the same purpose much more frequently (37%).

An actual practice that does not differ at an aggregate level is the security management of these smart home devices. More specifically, we asked how regularly students update the security settings of their smart home devices. The frequency of answers (measured by Likert scale) was not independent (p = 0.097). We found that 27.6% of work experience students and 21.4% of students without work experience never perform these steps.

An interesting actual practice relates to the voice activation services of smart devices. These are used by both student groups to a limited degree, 127 (W: 28%) of work experience students and 126 (NW: 36%) of students without work experience confirmed usage of these services. Only 26 (W: 6%) and 23 (NW: 7%) students in the same groups highlighted that they have changed the initial passcode or passphrase. As such, work experience does not translate into a significant positive effect on cyber-security awareness (p = 0.0634) relating to voice activation services. Current research [40] is just beginning to explore what mitigation strategies would be feasible. Outside a work environment, it appears even more difficult to learn about mitigation tactics for voice-activated services, given the rapidly evolving nature of this particular risk landscape.

Taken together, we observe that the overall survey results on the smart home security topic partly support our expectation that there is a relationship between work experience and increased security awareness of smart home devices. However, we also point out that the responses of the two student populations do not differ for some more technical factors, such as updating smart device security settings.

4.3. Personal Device Usage and BYOD

Shadow IT, including personal devices as well as unsanctioned software applications and services and their use for work-related activities, requires clearly defined policies to govern this part of the IT space. Formal cyber-security requirements regarding Shadow IT are rarely (5%) mentioned by study-only stream students or work experience students (19%), while work experience is still a factor in increased policy awareness (p < 0.001). In both student groups, the rate of survey participants who cannot identify any relevant IT policy in this area is over 80%, the highest of all the four broad surveyed categories. Table 7 shows a summary of the key survey results in this section.

Table 7. Summary of key findings: Personal device usage and BYOD.

Question Category	Key Findings
Informal and formal policy expectations	Work experience students are more likely to be aware of Shadow IT policies. **(p < 0.001)**
User expectations	Work experience does not translate into a significantly increased support need. **(p < 0.05)**
Technology guidance	Work experience is more likely associated with using only approved apps on organizational *mobile* devices (phone, tablet). **(p < 0.001)** Work experience is more likely associated with using only approved applications on organizational devices (desktop, tablet). **(p < 0.001)**
Assessment of actual technology and practices	Work experience students are less likely to store work or study-related data using personal cloud-based services. **(p < 0.001)** Work experience students are more likely to have endpoint security software installed on their (company) smartphones. **(p < 0.001)**

Regarding shadow IT support expectations, work experience students confirmed that they do not need further support (28%), while study-only stream students confirmed this choice with only 19%. The distribution of students who stated an additional support need was almost identical, 29% and 30%. The frequency of support need is statistically independent (p < 0.05; Bonferroni correction applied). This contrasts with the statistical findings from the other three topic categories analyzed in Sections 4.1, 4.2 and 4.4, where there was no statistically significant difference regarding support needs.

We observe that 90 (26%) of the students without work experience self-reported having access to a university-owned mobile device such as a tablet (presumably because they volunteer in teaching, research, or extracurricular activities). In contrast, 183 (41%) of the working students receive such a device from their employer. The actual practice of using only organizationally approved apps on mobile devices was confirmed by only 7% (i.e., 29% of those with access to such a device) of the study-only stream students, while 25% (i.e., 62% of those with access to such a device) of work experience students comply with this practice (p < 0.001).

Since the mental models of our participants regarding apps and more elaborate software applications may differ, we asked about both terms separately. We observed a similar difference for software application installations for mobile IT devices and desktops (p < 0.001). Only 7% of study-only students confirmed that they only used software applications based on university-provided information, while 35% of work experience students confirmed that they used software based on company requirements and that a company-approved list of software applications existed.

Another actual practice relates to the use of a cloud service during work or study. The corresponding governance framework is a typical topic that still has many open questions [46]. One clear difference we observed is in the rate of security awareness, while 79% of study-only students use this option for study-related data, the work experience students are much more cautious, and only 34% use the same options for work-related data (p < 0.001).

Finally, we analyzed the actual security practices relating to smartphone security. Smartphones, whether personal or organizational property, require enhanced security to avoid data privacy/confidentiality issues in case the device is lost or stolen. Endpoint security (advanced antivirus protection or application isolation and other capabilities) can make a difference when there is an attempt to access smartphone data without authorization. Study-only students confirmed that 40% of their personal devices are equipped with such a technology option, and for those work experience students who received such a device, the figure is even higher (55%), resulting in statistical differences (p < 0.001). An endpoint security framework, when used in a preemptive way [61], can also enhance the security of the smartphone; in particular, if it is equipped with other security features such as mandatory passcodes, standard virus protection or encryption tools. Encryption tools on smartphone devices can also trigger functionality and performance considerations, including energy consumption monitoring [62]. For example, when encrypting partial or full datasets on these devices, appropriate algorithm selection is crucial in managing the related energy consumption.

Taken together, the overall survey results of the Shadow IT topic support our expectation that there is a relationship between work experience and increased security awareness in respect of Shadow IT. Interestingly, the "support need" for personal devices and BYOD scenarios differs for the two student groups. This relationship was not detected in the other three topic categories.

4.4. Social Engineering Threats

Social engineering is probably one of the most challenging cyber-security threats that any student, employee or organization can face [47].

Offering trainings and regular updating of the acquired knowledge are paramount in mitigating the risks of cyber-threats through social engineering tactics. We have explored the existence of training options and other dedicated support in our survey and compared the differences across the two student groups; see Table 8 for a summary of key results.

Awareness of formal cyber-security requirements relating to social engineering differs significantly between the two student groups. Work experience students confirmed with a much higher rate (42%) that they are aware of policies relating to social engineering attacks, while students without work experience only confirmed the same with a very low rate (5%). The difference in these figures is highly significant ($p < 0.001$).

Only 25–30% of both student groups would require additional support when facing this threat ($p = 0.35$). The majority of respondents in both student groups confirmed that they do not need support or that the current level of support is sufficient. However, students without work experience might be less likely to be targets because such attacks more often aim for corporate credentials, assets or other valuables, such as data.

The actual details of practical training differ significantly. Work experience survey participants have confirmed that they are much more likely (4 or 5 times more likely) to receive simulated emails or social engineering attack case studies in comparison to the study-only participants; the difference is statistically significant ($p < 0.001$). The level of self-reported participation of the work experience students in simulated email training (23%) and case study training (30%) is modest, while the same values for study-only students are even lower (5% and 8%). None of these figures appear sufficient to sustain the required awareness [63]. A better scenario would be regular training for all users every 4–6 months.

Higher training participation might strongly influence the reported number of attempted phishing email attacks, as phishing is the most commonly identified social engineering attack vector. Only 1% of the study-only participants reported phishing attacks, while 22% reported the same in the work experience student stream ($p < 0.001$). Phishing email reporting is also correlated with the ability to timely report an actual suspicious email when the given institution is running a simulation campaign [64]. The time elapsed since the arrival of the phishing email in the mailbox is crucial; once more than 24 h have elapsed, the probability that the user has become a victim is much higher.

The practice of fraud awareness or compliance training is another tool for addressing social engineering attack vectors. While only 5% of the study-only stream confirmed such training, the work experience stream reported a much higher figure (38%), resulting in significant differences ($p < 0.001$). Risks related to insider attack emails, as well as other security risks related to spam emails, are two additional factors that are covered by such trainings. In both cases, the increased awareness effect of work-related training could be confirmed, with ($p < 0.05$) for insider attack emails and ($p < 0.01$) for spam emails. Phishing emails are a similar story; while only 8 study-only stream students identified actual phishing emails in their correspondence, 127 work experience students confirmed receiving such emails ($p < 0.001$). Organizations typically describe more than one variation of phishing emails in training materials and regularly probe users with simulated phishing email attacks; thus, the success rate of user identification is higher.

Table 8. Summary of key findings: social engineering threats.

Question Category	Key Findings
Informal and formal policy expectations	Work experience students are more likely to be aware of social engineering threat policies. **($p < 0.001$)**
User expectations	Work experience does not translate into a significantly increased support need. ($p = 0.35$)
Technology guidance	Work experience students are more likely to receive social engineering attack case studies and actual emails simulating those attacks. **($p < 0.001$)** Work experience students are more likely to receive fraud awareness and compliance training, focusing on phishing emails and other compromise attempts. **($p < 0.001$)**
Assessment of actual technology and practices	Work experience students are more likely to report phishing email attacks if they received any of those attack emails. **($p < 0.001$)** Work experience students are more likely to identify phishing emails in their email correspondence. **($p < 0.001$)** Work experience students are more likely to identify the dedicated person in the organization who they can contact in case of phishing or other attack attempts. **($p < 0.001$)** Work experience students are more likely to recognize insider attack emails originating from organizational partners. **($p < 0.05$)** Work experience students are more likely to recognize spam emails that were not initially identified by the organizational spam filter. **($p < 0.01$)**

Another key practice, which is important to any user in case of questions or doubts is to have a dedicated person or group of people who they can contact. Only 12% of study-only stream students could identify such a person or group, while 55% did in the work experience stream ($p < 0.001$). While it is obvious what advantages it brings to have such a dedicated person or group of persons in a traditional office environment, the importance is much higher when the actual user is in a remote environment and no immediate peer help or support is available.

We attempted to identify additional layers of factors within the general work experience student population that could have an increased positive effect on cyber-security awareness. We did not include the study-only students in this additional analysis as they did not receive any formal training from the university. We analyzed the potential correlation between work training and social engineering threat behavior. We used ordered logistic regression to identify a relationship between formal phishing email work training (independent variable) and the key topic of "reporting of phishing emails" as a dependent variable. Our results show that students who received formal phishing email work training are much more likely to report phishing email incidents ($p < 0.001$).

Overall, the survey results for the topic of social engineering threats support our expectation that there is a relationship between work experience and increased security awareness. All but one of our individual survey questions were associated with significant differences between the two groups. Only the question about the need for increased support had a comparable result.

5. Discussion

In this section, we discuss the implications of our results and recommendations for the future development of a cyber-security risk management framework in the four topic areas: (1) remote work and Wi-Fi settings, (2) smart home devices, (3) social engineering threats, and (4) personal devices, BYOD.

5.1. Remote Work (Study) Security and Wi-Fi Settings

We have observed that work experience is a key factor in work from home or work from remote location settings. More specifically, our expectations for the positive effects of work experience were confirmed in respect of the measurements of awareness and knowledge of the existence of relevant IT policies.

In contrast, the level of support expected from the organization (university or workplace) did not differ in most cases; except for the shadow IT and BYOD topic. We suggested that the higher rate of IT policy awareness of work experience students does not necessarily translate into an increased support need as the relevant students might not have processed and read all the policy details. For example, Hudock et al. [53] report that the couple-of-dozen-pages-long IT policies are often only flipped through and signed or electronically approved (during onboarding) without understanding the actual content or contacting a designated person for further clarification. Lack of accessibility, corporate culture and other factors [65] also contribute to a limited understanding when policy compliance is requested.

Each organization must ensure and regularly check that the actual policy details are understood by users and that compliance can be maintained. Video material and electronic training documents can increase the awareness for part of the user population but might not be sufficient for all age groups. Gamification can also potentially benefit that organizational purpose [65,66], in particular, because Generation Z may require a different approach. Gamification can potentially overcome the gap between just knowing that a particular policy exists or that users understand and can apply those policy details.

Our survey results suggest that certain remote work policy details are well-known to work experience users. Our expectations relating to the positive effects of work experience were, for example, confirmed for email forwarding to personal email accounts, or VPN usage with or without 2FA. Routine email forwarding to personal email accounts is a characteristic of the study-only student group, while more than half of the work experience group confirmed that they do not engage in such a practice. We argue that the reason for this is the knowledge acquired through additional corporate communications channels, such as direct communication with workplace colleagues.

Our argument for VPN access with or without 2FA is more nuanced. It is true that a company can enforce the usage of these technologies, and the increased usage is not related to work experience, which is demonstrated by the confirmed company mandates for both VPN and 2FA. On the other hand, we have observed that work experience students are much more likely to request optional 2FA, even if it is not required by their company. This suggests that they see the benefit of 2FA, even if this comes with a more complex verification process.

Work experience is not a key factor in Wi-Fi password settings and the used Wi-Fi security framework. It appears that any prior awareness and knowledge in this topic space for both student groups are not shaped by work experience, perhaps because the security of Wi-Fi equipment is not a typical part of corporate security training for traditional workplace settings. The general notion that 35% of users never update passwords [57] was confirmed in this context. This observation also has implications for other Wi-Fi-related security settings, such as Wi-Fi security protocols, connected devices with unsupported operating systems and other details. We recommend that in the new normal of post-pandemic remote work, each IT and cyber-security manager should evaluate the risks associated with home Wi-Fi settings and create an action and training plan to mitigate those.

5.2. Smart Home Devices

Smart home devices are present in many home environments and mostly use the same electronic communication infrastructure (e.g., Wi-Fi router). The security compromise of any of these smart devices may ultimately result in the potential compromise of other work or study-related devices, which are connected to the same Wi-Fi network.

Work experience students confirmed that they are much more likely to identify smart-device-related IT policies, but this does not translate into additional requested support. In fact, only a relatively small number of students (in both groups) would request any additional support relating to smart device security. We suspect that the novelty of these devices and potentially the lack of content related to smart devices in IT policies could contribute to this result.

Our results suggest that work experience contributes to an increased security awareness regarding the risks of public Wi-Fi access. Public Wi-Fi may be used when remote management of smart devices is necessary. Work experience students are much less likely to use the company smartphones with public Wi-Fi to access smart devices. We argue that additional research is needed to understand the use of personal smartphones in the work context. We also argue that personal smartphones require more attention from IT or cyber-security managers, especially if organizational data are managed with or through them. This security topic space is further elaborated in the discussion part of the Shadow IT section.

For voice-activated services and the regular security updating of smart devices in a home environment, we have not observed a significant relationship with work experience. For voice-activated services, the work environment is probably still lagging behind in terms of security-related advice because it is only recently that the first research [40] has been carried out in an attempt to understand the various security implications. Likewise, for smart home device security updates, we suspect that these devices are unlikely to be mentioned in many IT policies and, as such, work experience is not a likely source of security awareness improvements.

We recommend that responsible IT and cyber-security managers should learn about the risks associated with home smart devices, as mitigation is a benefit for both organizations and users. These devices are connected to the same home Wi-Fi network, which is the electronic communication channel of organizational VPN networks. Research has indicated [67] that home users are aware of the risks, but they might underestimate the implications. The list of perceived risks might include privacy risks, but users tend to ignore security risks [68]. Research findings [69] also indicate that the security and privacy risks of smart home devices have implications in a broader context, including in respect of industry standards, manufacturers or even employers. Organizations also need to play their part in supporting the user to better match their security or privacy expectations, especially within the new norm of extended remote work.

5.3. Personal Device Usage and BYOD

Prior work [42] has identified several directions for future shadow IT research, including user attitudes to shadow IT strengths and weaknesses or Generation Z's specific attitudes and behaviors. The governing of shadow IT or, more generally, the use of personal IT space is unlikely to be optimal for both organizations and users without some sort of dialogue.

In our survey, we illustrate that work experience students have an increased awareness of related IT policies ($p < 0.001$). Nonetheless, there are other fundamental difficulties. None of the other three topic areas of our survey have as large a share of participants that cannot identify any relevant IT policy to comply with (82% of work experience and 95% of study only students). A better dialogue would require the transparent introduction of expected guidelines by the organization for all users.

Downloading apps to mobile devices issued by organizations or downloading software applications to desktops or other computing devices issued by the university or company is handled differently by work experience students. The existence of a pre-approved list is associated with work experience students being more aware of security risks.

We also asked questions about smartphone usage (both personal and organization-owned) and the associated security measures, as these devices are frequently used for organizational purposes. Endpoint security was confirmed to be installed on a higher portion of company-issued devices.

We also studied those students who either have personal smartphones or work-related smartphones. We identified that a higher proportion of students with work experience (55%) confirmed using endpoint security compared to the lower portion (41%) of study-only students.

The use of personal cloud services and the associated cyber-security and privacy risks should be a concern for both corporate entities and teaching institutions. Although the use of unsanctioned cloud services is less prevalent in the group of work experience students, we found that 34% of them are still using personal clouds for company files, but the actual nature and volume of the uploaded company data are unknown and were not part of our survey.

We recommend that responsible IT-security and cyber-security managers should take steps to analyze, at least by exploratory means, the nature of the uploaded company data and update the requirements in a shadow IT or BYOD/BYOS policy. More importantly, we suggest that organizations should take the first step with the formulation and communication of their general expectations in relation to shadow IT. Without this introduction, the much-needed dialogue with users is unlikely to start.

5.4. Social Engineering Threats

Social engineering is probably one of the most challenging cyber-security threats that any student, employee or organization can face [47]. Training and regular updating of the acquired knowledge is paramount in mitigating the risks of cyber-threats resulting from social engineering tactics. Our survey results have confirmed that work experience is positively associated with recognizing social engineering-related IT policies, but this increased awareness does not translate into additional support needs.

Prior work [53] has also substantiated that some newly hired employees tend to receive training for hypothetical social engineering threats ("corporate espionage") but are less likely to receive training on actual cases with the possibility of Q and A (question and answer) sessions afterward.

Our survey provides evidence that work experience is associated with improved awareness of specific social engineering threats. Work experience students reported that they are much more likely to receive regular (every 6 months) emails to simulate attacks and case studies to describe actual cases. They are also more likely to report phishing email attacks.

This difference only applies to those who receive training. However, the problem is that the majority of the work experience students still do not receive (or do not remember) any of these training courses. This applies to regular emails, which 77% of them did not receive, and case study emails, which 70% of them did not receive. We argue that it is not a surprise that, with such a low level of training, only 21% of work experience students report phishing email attacks.

Somewhat unsurprisingly, compliance or fraud awareness training is another area where we have survey confirmation that work experience students report completion with much higher rates, but again, 62% of them did not receive or did not remember this kind of training. The positive effect of work experience could also be confirmed for both insider email attacks and increased spam email activity.

We also inquired about the willingness of students to report phishing email attacks. Within the work experience stream, 97 out of the 127 students, who confirmed receiving at least one such email, have made at least one report. Surprisingly, only eight participants (of 350) in the study-only group mentioned receiving phishing emails, and only four students confirmed the reporting of such emails. We suspect that recalling such attacks is related to general awareness and concern regarding this security threat, which may explain the low numbers of the non-working students. Further, while there is a reporting gap, the observation that 97 of 127 working students at least reported one phishing attempt is encouraging. However, reporting could be further improved if support personnel were available for questions and queries relating to phishing and other attack attempts. While a modest 55% of work experience students could identify a dedicated person, only 11% of the student-only stream could do so.

We recommend that responsible IT-security and cyber-security managers should initiate comprehensive training options for all users, for example, according to the basic principles outlined in [51,52]. Our results also suggest that key insights from related literature [47] are confirmed in our survey, meaning that continuously raising awareness about social engineering threats is critical. Acknowledging that actual training might not cover all newly emerging risks is also important in raising general scrutiny because the skills of perpetrators might, in certain cases, be ahead of countermeasures. In the context of social engineering prevention, gamification also appears particularly suitable for addressing problems such as habituation and boredom during repeated training exercises [65,66]. The design of such training courses can also specifically address the remote work context and can be tailored to actual social engineering threats.

5.5. Limitations

The survey study was conducted with university students who have participated in interdisciplinary IT-related lecture courses. Previous work has shown that IT-related studies positively influence cyber-security awareness [15] as measured by calculated and perceived ISA when compared to other study fields. However, this also means that our results cannot be generalized to other university study fields. In addition, most of the students with work experience confirmed that they only participated in an internship or part-time work and had primarily up to 12 months of work experience. Interns or student employees do often receive onboarding security training [53], but such courses might not be as comprehensive as an onboarding training course for a full-time young professional after graduation. In addition to comprehensiveness, tailoring to the actual training program can also make a substantial difference [18] when considering the different individual behavioral factors of users or employees. Our survey results can be used when assessing the security practices of employees with initial work experience, while bearing in mind that some of the base assumptions are different for work experience students than for junior full-time employees.

6. Conclusions

In this work, we surveyed 798 university students online and asked them to complete a survey relating to cyber-security risks either as a work experience student or as a student without work experience. We queried the survey population regarding cyber-security risk awareness across four topic categories: (1) remote work and Wi-Fi settings, (2) smart home devices, (3) personal devices, BYOD or BYOS, and (4) social engineering threats.

The analysis of the survey data illustrates that general cyber-security risk awareness is significantly associated with the work experience of university students across a broad range of topics and specific issues. As such, our results demonstrate a further benefit of being able to gain work experience during the study programs. At the same time, our research contributes to the sparse literature aimed at exploring the security awareness and practices of employees with limited work experience (see, for example, [53]).

However, we also encountered cyber-security risk awareness topics that appear less related to the initial work experience of university students. We proposed explanations for the underlying reasons and also propose to broaden future research to analyze other factors for cyber-security risk awareness. This could include security experience gained during early formal education, building on early childhood practices or experience from longer periods of full-time employment. For example, our participants, who mostly stemmed from Generation Z and Generation Alpha, demonstrated good security practices in some areas (irrespective of work experience). Cyber-security education can reinforce these practices, and organizations, as well as society, can benefit from these early experiences. This was not the case for earlier generations, where quite simply, the technologies and platforms either did not exist or were not easily available during the formative years of education.

We also propose one additional topic for future research, i.e., the use of survey research in conjunction with the measurement of existing organizational cyber-security risks (see, for example, [70–72]) for the work-from-home context. While measurement of security risk is already taking place inside and at the boundary of organizations, it is important to understand the actual security practices, at least for a representative subset of employees and to contrast these results with self-reported measures.

Author Contributions: Conceptualization, T.P. and J.G.; methodology, T.P. and J.G.; survey development, data collection, T.P.; analysis, T.P.; writing—original draft preparation, T.P.; writing—review and editing, T.P. and J.G. All authors have read and agreed to the submitted version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Our institution does not require a formal ethics review for basic survey studies. We solicited informed consent and avoided any questions that could be used to re-identify any survey participant.

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

Data Availability Statement: Data are available from the authors upon request.

Acknowledgments: We are thankful for the support and contribution of Emmanuel Syrmoudis for the review of this paper and the highlighting of details that could be further developed.

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

Appendix A. Online Survey Introduction (Consent Form)

Hereby, I acknowledge that I voluntarily participate in this study. I was informed about the following:

Procedure:

In this survey, you will be asked questions mainly addressing your remote work (or study) activities. It consists of five parts. This includes the remote work (or study) environment, smart devices, social engineering attempts, shadow IT and demographics. In total, the time needed to fill out the survey is around 30 minutes.

Anonymity:

Collected data is anonymously stored and analyzed. No personal information (e.g., e-mail) is captured.

Reward:

Participation is rewarded with a bonus code which is part of your course grade bonus tasks. You will receive a bonus code at the end of the survey. This code is not stored with your answers.

Data Usage:

Due to academic transparency, anonymized data is available to third parties for re-use after completion of the study. The anonymized, personal code is removed beforehand. Purpose, type, and extent of this re-use cannot be foreseen.

Consent Form:

By checking the box below, I acknowledge that I was informed about the procedure of the study and that I agree to the text above.

- Yes, I agree
- No, I do not agree (I do not want to participate in the survey)

Appendix B. Survey Participation Options

There are two options, when you are completing this survey:

1. Student with remote work experience
2. Student without remote work experience

Please select the option of "Student with remote work experience" if you had any remote work experience since March 2020 (start of the pandemic), including your current work experience. Remote work is an arrangement in which employees do not commute or travel to a central place of work, such as an office building or other facility. Work experience can include part- or full-time work, internship or any other work-related activity.

Please only choose the "Student without remote work experience" option if you had no remote work experience at all, since March 2020 (start of the pandemic).

Please select your survey participation options below:

- Student with remote work experience
- Student without remote work experience

Appendix C. Survey Questions (Sample)

Survey participants were presented with questions about demographics and from four topics based on their survey participation selection. The categories and a sample of questions are listed below.

Path 1—Students with remote work experience completed the following question categories:

1. DE—Demographics
   - DE01—What is (or was) your regular remote work location?
   - DE06—How long have you been working as an intern/employee?
2. SD—Smart devices
   - SD02—Are you aware of any formal cyber security company requirements relating to smart home devices?
   - SD03—What is the level of cyber security support, relating to smart home devices, that you would expect from your company?
3. RW—Remote work
   - RW04—Did you get any cyber security company training in the past 12 months to cover remote work requirements?
   - RW08—Was the initial password for your home Wi-Fi network at least once updated? (Initial password is provided by the Wi-Fi router manufacturer.)
4. SE—Social engineering attacks
   - SE03—What is the level of cyber security support, relating to phishing and other social engineering attacks that you would expect from your company?
   - SE07—Did you report the phishing email attacks to your company, if you received any in the past 12 months?
5. SI—Shadow IT
   - SI03—What is the level of cyber security support, relating to shadow IT/BYOD that you would expect from your company?
   - SI09—Are you using personal cloud based services (i.e., Google Drive, Amazon Cloud, Microsoft Cloud, . . .) to store work related data?

Path 2—Students without remote work experience completed the following question categories:

1. DE—Demographics
    - DE11—What is your regular study location?
    - DE03—What is your age?
2. ST—Smart devices, TUM
    - ST01—Are you aware of any formal cyber security TUM requirements relating to smart home devices?
    - ST02—What is the level of cyber security support, relating to smart home devices, that you would expect from TUM?
3. RS—Remote study, TUM
    - RS04—Did you get any cyber security training at TUM in the past 12 months to cover remote study requirements?
    - RS05—Did you have the possibility to contact IT Support/IT Helpdesk in every case when you had a remote study related security question?
4. SA—Social engineering attacks, TUM
    - SA02—What is the level of cyber security support, relating to phishing and other social engineering attacks that you would expect from TUM?
    - SA03—Do you get regular (at least every 6 months) emails from TUM simulating actual social engineering attacks?
5. BY—Shadow IT, TUM
    - BY02—What is the level of cyber security support, relating shadow IT/BYOD that you would expect from TUM?
    - BY08—Are you using personal cloud based services (i.e., Google Drive, Amazon Cloud, Microsoft Cloud, . . .) to store study related data?

References

1. Olson, M.H. Remote office work: Changing work patterns in space and time. *Commun. ACM* **1983**, *26*, 182–187. [CrossRef]
2. Zhang, Z.; Zhang, Y.Q.; Chu, X.; Li, B. An overview of virtual private network (VPN): IP VPN and optical VPN. *Photonic Netw. Commun.* **2004**, *7*, 213–225. [CrossRef]
3. Wyld, D.C. The black swan of the coronavirus and how American organizations have adapted to the new world of remote work. *Eur. J. Bus. Manag. Res.* **2022**, *7*, 9–19. [CrossRef]
4. Child, F.; Frank, M.; Lef, M.; Sarakatsannis, J. *Setting a New Bar for Online Higher Education*; McKinsey and Company: New York, NY, USA, 2021. Available online: https://www.mckinsey.com/industries/education/our-insights/setting-a-new-bar-for-online-higher-education (accessed on 21 January 2022).
5. Barrero, J.M.; Bloom, N.; Davis, S.J. *Let Me Work from Home, or I Will Find Another Job*; Working Paper 2021-87; Becker Friedman Institute for Economics, University of Chicago: Chicago, IL, USA, 2021. Available online: https://dx.doi.org/10.2139/ssrn.3890988 (accessed on 27 June 2022).
6. Schiffer, Z. The Verge Technology News Website: Apple Employees Push Back against Returning to the Office in Internal Letter. Available online: https://www.theverge.com/2021/6/4/22491629/apple-employees-push-back-return-office-internal-letter-tim-cook (accessed on 31 May 2022).
7. Ahmad, T. *Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity*. SSRN Working Paper SSRN 3568830. 2020. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3568830 (accessed on 31 May 2022).
8. Georgiadou, A.; Mouzakitis, S.; Askounis, D. Working from home during COVID-19 crisis: A cyber security culture assessment survey. *Secur. J.* **2021**, *35*, 1–20. [CrossRef]
9. Andrade, R.O.; Garcés, I.O.; Cazares, M. Cybersecurity attacks on Smart Home during Covid-19 pandemic. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 398–404.
10. Venkatesha, S.; Reddy, K.R.; Chandavarkar, B.R. Social engineering attacks during the COVID-19 pandemic. *SN Comput. Sci.* **2021**, *2*, 1–9. [CrossRef]
11. Chigada, J.; Rujeko, M. Cyberattacks and threats during COVID-19: A systematic literature review. *S. Afr. J. Inf. Manag.* **2021**, *23*, 1–11. [CrossRef]

12. Skulmowski, A.; Günter, D.R. COVID-19 as an accelerator for digitalization at a German university: Establishing hybrid campuses in times of crisis. *Hum. Behav. Emerg. Technol.* **2020**, *2*, 212–216. [CrossRef]
13. Lebek, B.; Uffen, J.; Neumann, M.; Hohler, B.; Breitner, M.H. Information security awareness and behavior: A theory-based literature review. *Manag. Res. Rev.* **2014**, *37*, 1049–1092. [CrossRef]
14. Khando, K.; Gao, S.; Islam, S.M.; Salman, A. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Comput. Secur.* **2021**, *106*, 102267. [CrossRef]
15. Farooq, A.; Isoaho, J.; Virtanen, S.; Isoaho, J. Information security awareness in educational institution: An analysis of students' individual factors. In Proceedings of the 2015 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Helsinki, Finland, 20–22 August 2015; pp. 352–359.
16. Kim, E.B. Recommendations for information security awareness training for college students. *Inf. Manag. Comput. Secur.* **2014**, *22*, 115–126. [CrossRef]
17. Alhuwail, D.; Al-Jafar, E.; Abdulsalam, Y.; AlDuaij, S. Information security awareness and behaviors of health care professionals at public health care facilities. *Appl. Clin. Inform.* **2021**, *12*, 924–932. [CrossRef] [PubMed]
18. Kirova, D.; Baumöl, U. Factors that affect the success of security education, training, and awareness programs: A literature review. *J. Inf. Technol. Theory Appl.* **2018**, *19*, 56–82.
19. Rea-Guaman, A.M.; Mejia, J.; San Feliu, T.; Calvo-Manzano, J.A. AVARCIBER: A framework for assessing cybersecurity risks. *Clust. Comput.* **2020**, *23*, 1827–1843. [CrossRef]
20. Skopik, F.; Wurzenberger, M.; Settanni, G.; Fiedler, R. Establishing national cyber situational awareness through incident information clustering. In Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), London, UK, 8–9 June 2015; pp. 1–8.
21. Cebula, J.L.; Young, L.R. *A Taxonomy of Operational Cyber Security Risks*; Technical Note CMU/SEI-2010-TN-028; Carnegie-Mellon Univ, Software Engineering Institute: Pittsburgh, PA, USA, 2010. Available online: https://apps.dtic.mil/sti/citations/ADA537111 (accessed on 27 June 2022).
22. Krumay, B.; Bernroider, E.; Walser, R. Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST Cybersecurity Framework. In *Nordic Conference on Secure IT Systems*; Springer: Cham, Switzerland, 2018; pp. 369–384.
23. Bauer, S.; Bernroider, E. From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: Database Adv. Inf. Syst.* **2017**, *48*, 44–68. [CrossRef]
24. Bidgoli, M.; Grossklags, J. End user cybercrime reporting: What we know and what we can do to improve it. In Proceedings of the 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, BC, Canada, 12–14 June 2016; pp. 1–6.
25. Eling, M.; Werner, S. What do we know about cyber risk and cyber risk insurance? *J. Risk Financ.* **2016**, *17*, 474–491. [CrossRef]
26. Laszka, A.; Farhang, S.; Grossklags, J. On the economics of ransomware. In *International Conference on Decision and Game Theory for Security*; Springer: Cham, Switzerland, 2017; pp. 397–417.
27. United States Government Accountability Office. *Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market*; GAO-21-477; Government Accountability Office: Washington, DC, USA, 2021. Available online: https://www.gao.gov/assets/gao-21-477.pdf (accessed on 27 June 2022).
28. Kumar, U.; Gambhir, S. A literature review of security threats to wireless networks. *Int. J. Future Gener. Commun. Netw.* **2014**, *7*, 25–34. [CrossRef]
29. Peng, H. WIFI network information security analysis research. In Proceedings of the 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, China, 21–23 April 2012; pp. 2243–2245.
30. Mekhaznia, T.; Zidani, A. Wi-Fi security analysis. *Procedia Comput. Sci.* **2015**, *73*, 172–178. [CrossRef]
31. Kohlios, C.P.; Hayajneh, T. A comprehensive attack flow model and security analysis for Wi-Fi and WPA3. *Electronics* **2018** *7*, 284. [CrossRef]
32. Luo, Z.; Yu, G.; Qi, H.; Liu, Y. Research of a VPN secure networking model. In Proceedings of the 2nd International Conference on Measurement, Information and Control, Harbin, China, 16–18 August 2013; pp. 567–569.
33. Bansode, R.; Girdhar, A. Common vulnerabilities exposed in VPN – A survey. *J. Phys. Conf. Ser.* **2021**, *1714*, 1–8. [CrossRef]
34. Uskov, A.V. Information security of mobile VPN: Conceptual models and design methodology. In Proceedings of the IEEE International Conference on Electro/Information Technology, Indianapolis, IN, USA, 6–8 May 2012; pp. 1–6.
35. Hong, Y.R.; Kim, D. Security enhancement of smart phones for enterprises by applying mobile VPN technologies. In *International Conference on Computational Science and Its Applications*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 506–517
36. Amraoui, N.; Zouari, B. Securing the operation of Smart Home Systems: A literature review. *J. Reliab. Intell. Environ.* **2021**, *8*, 67–74. [CrossRef]
37. Gunge, V.S.; Yalagi, P.S. Smart home automation: A literature review. *Int. J. Comput. Appl.* **2016**, *2016*, 6–10.
38. Lin, H.; Bergmann, N.W. IoT privacy and security challenges for smart home environments. *Information* **2016**, *7*, 44. [CrossRef]
39. Geneiatakis, D.; Kounelis, I.; Neisse, R.; Nai-Fovino, I.; Steri, G.; Baldini, G. Security and privacy issues for an IoT based smart home. In Proceedings of the 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017; pp. 1292–1297.

40. Zhang, N.; Mi, X.; Feng, X.; Wang, X.; Tian, Y.; Qian, F. Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), San Francisco, CA, USA, 19–23 May 2019; pp. 1381–1396.
41. Haag, S.; Eckhardt, A. Shadow IT. *Bus. Inf. Syst. Eng.* **2017**, *59*, 469–473. [CrossRef]
42. Raković, L.; Sakal, M.; Matković, P.; Marić, M. Shadow IT—Systematic literature review. *Inf. Technol. Control.* **2020**, *49*, 144–160. [CrossRef]
43. Silic, M. *Emerging from the Shadows: Survey Evidence of Shadow IT Use from Blissfully Ignorant Employees*. SSRN 2633000. 2015. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2633000 (accessed on 31 May 2022).
44. Weidman, J.; Grossklags, J. I like it, but I hate it: Employee perceptions towards an institutional transition to BYOD second-factor authentication. In Proceedings of the 33rd Annual Computer Security Applications Conference, Orlando, FL, USA, 4–8 December 2017; pp. 212–224.
45. Tambo, T.; Olsen, M.; Bækgaard, L. Motives for feral systems in Denmark. In *Web Design and Development: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2016; pp. 193–222.
46. Walterbusch, M.; Fietz, A.; Teuteberg, F. Missing cloud security awareness: investigating risk exposure in shadow IT. *J. Enterp. Inf. Manag.* **2017**, *30*, 644–665. [CrossRef]
47. Aldawood, H.; Skinner, G. Educating and raising awareness on cyber security social engineering: A literature review. In Proceedings of the IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, Australia, 4–7 December 2018; pp. 62–68.
48. Hadnagy, C. *Social Engineering: The Science of Human Hacking*; John Wiley & Sons: Hoboken, NJ, USA, 2018.
49. Hijji, M.; Alam, G. A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats during the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access* **2021**, *9*, 7152–7169. [CrossRef]
50. Department of Justice, USA. Three Individuals Charged for Alleged Roles in Twitter Hack. 2020. Available online: https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack (accessed on 13 January 2022).
51. Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M.; Jerram, C. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Comput. Secur.* **2014**, *42*, 165–176. [CrossRef]
52. Amankwa, E.; Loock, M.; Kritzinger, E. Enhancing information security education and awareness: Proposed characteristics for a model. In Proceedings of the Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, South Africa, 15–17 November 2015; pp. 72–77.
53. Hudock, A.; Weidman, J.; Grossklags, J. Security onboarding: An interview study on security training for temporary employees. In Proceedings of the Conference on Mensch und Computer, Magdeburg, Germany, 6–9 September 2020; pp. 183–194.
54. Choong, Y.Y.; Theofanos, M. What 4,500+ people can tell you—Employees' attitudes toward organizational password policy do matter. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*; Springer: Cham, Switzerland, 2015; pp. 293–310.
55. Choong, Y.Y.; Theofanos, M.F.; Renaud, K.; Prior, S. "Passwords protect my stuff"—A study of children's password practices. *J. Cybersecur.* **2019**, *5*, tyz015. [CrossRef]
56. Said, H.; Guimaraes, M.; Al Mutawa, N.; Al Awadhi, I. Forensics and war-driving on unsecured wireless network. In Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates, 11–14 December 2011; pp. 19–24.
57. Moscaritolo, A. 35 Percent of People Never Change Their Passwords, PC Magazine (UK). 2018. Available online: https://uk.pcmag.com/password-managers/116459/35-percent-of-people-never-change-their-passwords (accessed on 13 January 2022).
58. Quilantang, K.A.G.; Rivera, J.A.C.; Pinili, M.V.M.; Magpantay, A.J.N.R.; Busia Blancaflor, E.; Pastrana, J.R.A.M. Exploiting Windows 7 vulnerabilities using penetration testing tools: A case study about Windows 7 vulnerabilities. In Proceedings of the 9th International Conference on Computer and Communications Management, Singapore, 16–18 July 2021; pp. 124–129.
59. Kotzias, P.; Bilge, L.; Vervier, P.A.; Caballero, J. Mind Your Own Business: A Longitudinal Study of Threats and Vulnerabilities in Enterprises. In Proceedings of the Network and Distributed Systems Security (NDSS), San Diego, CA, USA, 24–27 February 2019; pp. 1–15.
60. Haney, J.M.; Furman, S.M.; Acar, Y. Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In *International Conference on Human-Computer Interaction*; Springer: Cham, Switzerland, 2020; pp. 393–411.
61. Yoo, S.J. Study on Improving Endpoint Security Technology. *Converg. Secur. J.* **2018**, *18*, 19–25.
62. Mujtaba, G.; Tahir, M.; Soomro, M.H. Energy efficient data encryption techniques in smartphones. *Wirel. Pers. Commun.* **2019**, *106*, 2023–2035. [CrossRef]
63. Reinheimer, B.; Aldag, L.; Mayer, P.; Mossano, M.; Duezguen, R.; Lofthouse, B.;Volkamer, M. An investigation of phishing awareness and education over time: When and how to best remind users. In Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS), Online Conference, 7–11 August 2020; pp. 259–284.
64. Jampen, D.; Gür, G.; Sutter, T.; Tellenbach, B. Don't click: Towards an effective anti-phishing training. A comparative literature review. *Hum.-Centric Comput. Inf. Sci.* **2020**, *10*, 1–41. [CrossRef]
65. Scholefield, S.; Shepherd, L.A. Gamification techniques for raising cyber security awareness. In *International Conference on Human-Computer Interaction*; Springer: Cham, Switzerland, 2019.

66. Rieff, I. Systematically Applying Gamification to Cyber Security Awareness Trainings: A Framework and Case Study Approach. Master's Thesis, Faculty of TPM, Delft University of Technology, Delft, The Netherlands, 2018.
67. Tabassum, M.; Kosinski, T.; Lipford, H.R. "I don't own the data": End user perceptions of smart home device data practices and risks. In Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS), Santa Clara, CA, USA, 11–13 August 2019; pp. 435–450.
68. Wang, X.; McGill, T.J.; Klobas, J.E. I want it anyway: Consumer perceptions of smart home devices. *J. Comput. Inf. Syst.* **2018**, *60*, 437–447. [CrossRef]
69. Shouran, Z.; Ashari, A.; Priyambodo, T. Internet of things (IoT) of smart home: Privacy and security. *Int. J. Comput. Appl.* **2019**, *182*, 3–8. [CrossRef]
70. Hubbard, D.W.; Seiersen, R. *How to Measure Anything in Cybersecurity Risk*; John Wiley & Sons: Hoboken, NJ, USA, 2016.
71. Kerkdijk, R.; Tesink, S.; Fransen, F.; Falconieri, F. Evidence-Based Prioritization of Cybersecurity Threats. ISACA. 2021. Available online: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/evidence-based-prioritization-of-cybersecurity-threats (accessed on 13 January 2022).
72. Le, A.; Chen, Y.; Chai, K.K.; Vasenev, A.; Montoya, L. Incorporating FAIR into Bayesian network for numerical assessment of loss event frequencies of smart grid cyber threats. *Mob. Netw. Appl.* **2019**, *24*, 1713–1721. [CrossRef]