How to Successfully Implement Phishing Awareness Training in Organizations: A Technology Adoption Perspective

Tim Geppert
ZHAW, Switzerland
Tim.Geppert@zhaw.ch

Tibor Dudas
ZHAW, Switzerland
Tibor.Dudas@zhaw.ch

Severin Zimmermann
ZHAW, Switzerland
s.zimmermann18@gmail.com

Thomas Sutter
ZHAW, Switzerland
Thomas.Sutter@zhaw.ch

Nico Ebert
ZHAW, Switzerland
Nico.Ebert@zhaw.ch

Abstract

Phishing awareness training (PAT) is crucial for protecting organizations against such attacks. While most debate focuses on innovative approaches or the effectiveness of training, organizational aspects of PAT adoption are often overlooked. Success in implementing new technology depends greatly on organizational factors, making understanding their influence on PAT adoption essential. This paper examines PAT adoption using the technology organization environment (TOE) framework, a standard model in technology adoption studies. Key organizational factors in Switzerland were identified through a literature review and expert interviews, including staff traits, behavior, reporting procedures, norms, policies, and ethics. Technological factors such as integration, personalization, and training content are also critical, while legal regulations and external support are essential from an environmental perspective. These factors are mapped to adoption phases to guide practitioners and researchers regarding the risks and opportunities at each stage of PAT adoption.

Keywords: phishing awareness, phishing training, TOE, adoption

1. Introduction

Phishing is a growing problem that threatens the online security of businesses and consumers (Desolda et al., 2022). Attackers use fake emails, websites, and other methods to steal confidential information such as passwords, bank details, or other private data (Jampen et al., 2020). According to a Federal Bureau of Investigation's public service announcement (2020), the cost to U.S. businesses from compromised emails was estimated to be $2.1 billion between 2014 and 2019. Many companies have employed a two-tier defense strategy to protect themselves from such attacks. This two-tier defense strategy includes technical protection, where systems are configured to detect and block phishing automatically, and human protection, where employees exercise caution (Wash & Nthala, 2021). However, PAT remains one of the most popular methods to reduce this risk and strengthen the second layer of defense against cyber threats (Kävrestad et al., 2022). For PAT to be effective, every organization must consider its adoption (Lain et al., 2022). Alwanain (2019) goes further still and recommends making PAT mandatory for employees.

The issue of phishing and phishing awareness has been discussed extensively in the literature, with researchers mainly focusing on the effectiveness of specific solutions. However, organizational aspects of PAT design, implementation, and long-term anchoring in organizations have been insufficiently considered in current studies (e.g., Lain et al., 2022), and adoption factors are not the focus of most studies. For example, Butavicius et al. (2020) addressed the issue of employees no longer clicking on legitimate links following PAT, and noted the problem of overconfidence in operator abilities. These organizational issues are mentioned in the literature but seldom considered in greater detail (Volkamer et al., 2020).

This paper contributes to existing research by compiling organizational factors that influence the adoption of PAT using a systematic literature review and expert interviews to answer the following research question:

What environmental, organizational, and technological factors influence the successful adoption of PAT?

Adoption factors will be structured according to the technology organization environment (TOE) framework (Tornatzky et al., 1990; Baker, 2012), as this has already been used to analyze the adoption of a variety of technological innovations in organizations (Geppert et al., 2022). The paper is structured as follows: In the first section, we described phishing and PAT. Next, the

URI: https://hdl.handle.net/10125/109585
978-0-9981331-8-8

current literature is examined for factors that may arise during the adoption of PAT and enriched with insights from interviews with experts who have extensive experience in introducing PAT into organizations. The interviews aim to identify relevant factors when adopting PAT from a practitioner's viewpoint. The following discussion synthesizes the findings from all individual results and highlights common factors for adopting PAT in organizations. A final outlook will provide insights for follow-up research.

2. Background

Adopting new technologies like PAT in organizations is a complex process that can be effectively understood and managed through the TOE framework (Tornatzky et al., 1990) since it gives a useful analytical framework for studying the assimilation of diverse sorts of innovation at the organizational level (Oliveira & Martins 2011, Geppert et al. 2022). This framework helps delineate the impact of new technologies across three domains – the technology itself, the organizational context, and the external environment. The TOE framework was for example used to determine the security readiness of organizations (Hasan et al., 2021). In summary, the TOE framework is appropriate for analyzing information technology adoption and may be utilized to research cybersecurity technology adoption across various industries (Hasani et al., 2023). Phishing attacks typically involve misleading emails, websites, phone calls, and text messages, where criminals impersonate legitimate individuals or companies to steal sensitive information from users (Chetioui et al., 2022). From the perspective of the CIA triad, phishing directly effects confidentially but also integrity and availability (Gut & Kammermann, 2021). PAT involves security programs designed to mitigate phishing attacks by promoting behavioral change and increased employee awareness (Gut & Kammermann, 2021). As technical measures alone are insufficient to counteract phishing attacks fully, employee awareness is crucial (Darem, 2021). This paper will mainly focus on embedded PAT, which involves sending simulated phishing emails to users without prior notice to test their detection skills. Individuals who fall for these simulated attacks are immediately directed to training modules, which help reinforce learning points and improve phishing detection capabilities. This method also includes follow-up emails to assess progress and the retention of training content (Jampen et al., 2020).

Adopting new technologies involves navigating three crucial phases – design, implementation, and usage (Esteves & Pastor, 1999). During the design phase, it is essential to outline the system's specifications tailored to organizational needs. Effective PAT design includes developing content that targets specific organizational vulnerabilities and user behavior, requiring a solid understanding of user requirements and organizational objectives (Rogers et al., 2008). The implementation phase focuses on deploying the technology. This involves setting up the training infrastructure, integrating training modules with existing IT systems, and conducting initial sessions. Successful implementation relies on effective change management strategies and leadership support to ensure a smooth transition and high adoption rates (Kotter, 2012). The usage phase centers on maintaining engagement with the technology over time. For PAT, this means regularly updating training materials to address new threats, continuously assessing the effectiveness of training, and integrating feedback iteratively. The objective is to keep awareness relevant and effective, fostering a culture of continuous improvement and adaptation (Delone & McLean, 2003).

By employing the TOE framework, this analysis not only examines the technical specifications and implementations of PAT but also considers the broader organizational and environmental contexts that influence its adoption – something current studies often overlook or insufficiently consider, as the literature review highlights. The framework guides the structuring of factors related to PAT adoption, supporting the literature review and organizing expert interviews to ensure a comprehensive understanding of all influences and their interconnections.

3. Methodology

The following section presents the research methods used in this work and includes details of the literature review and interview partners.

Literature Review: A systematic literature search, based on Webster and Watson (2002), was conducted to identify relevant literature. Search terms related to phishing, awareness, and organizational aspects (chances, risks, behavior, factors, users, campaign, education, training) were combined into queries and executed in ProQuest (308), Web of Science (807), and the ACM Digital Library (528). Restricted to titles and abstracts, the search yielded 1,643 results, with 1,288 being unique. The results were first filtered by title to exclude obvious mismatches. Next, the abstract was read, and irrelevant literature was removed. This process reduced the dataset to 49 references. Snowballing expanded this to the 73 relevant references used for analysis (Supplement Table 1).

Expert Interviews: These interviews aimed to identify adoption factors relevant to the implementation of PAT based on practical experience. Swiss experts from different organizations were chosen as interviewees owing to their prior experience implementing such training within organizations. We shorthand each individual expert with E followed by a number 1-8. E1 (scientific staff), E3 (security engineer), E4 (CISO), E5 (SOC team), and E6 (SOC team) all work in the same further education organization. E2 works for a phishing training provider, and E7 and E8 are IT consultants for phishing awareness in two different companies. A semi-structured interview guide was utilized for the expert interviews, comprising general context questions, central questions, and detailed inquiries. The main questions focused on the organizational adoption factors of PAT from the three TOE perspectives. Detailed follow-up questions were derived from relevant aspects identified in the literature review. Interviews were primarily conducted individually, except for E5 and E6, who requested a paired interview. All the interviews were conducted online (45 minutes each) in April 2023 and recorded. Full transcription was completed following transcription guidelines outlined by Dresing and Pehl (2020). The transcripts were deductively coded by a single coder using the TOE domains and in a second step inductively based on the factors from the literature review, also allowing for new emerging codes.

4. Results

Based on the literature review, we identified nine factors that influence the adoption of PAT. These factors spanned all three TOE perspectives (Figure 1, Supplement Table 2) and were further discussed with eight PAT experts.

The different adoption factors will be presented in more detail below. Corresponding literature from the literature review and interview information is also provided.

4.1. Organizational Context

Within their organizational context, employees play a significant role in the adoption of PAT. Here, personal traits and behavior can be differentiated. Additional factors related to the company could be identified, primarily focusing on culture, norms, and ethics. As a last factor, the reporting possibilities are discussed.

Personal Traits: The literature discusses several demographic factors that influence susceptibility to phishing, which must be addressed when adopting PAT. Bardsley-Marcial (2022) identified differences in age, gender, and IT literacy as influencing factors. The general technical affinity of employees also seems to affect the success of PAT (Jampen et al., 2020).

Unexpectedly, however, the technical affinity of IT staff does not reduce their susceptibility to phishing attacks. IT or technically skilled employees are just as vulnerable to phishing attacks as less technically skilled employees (Alwanain, 2019; Anawar et al., 2019; Ebner, 2018; Jampen et al., 2020). In a survey by Wilkinson (2022), as many as 47 percent of IT employees stated they had been caught by a phishing attack at some point, highlighting that PAT needs to be implemented for all personnel.

Additional general human factors such as stress resistance and awareness (Desolda et al., 2022), as well as risk-taking and decision-making styles (Abroshan et al., 2021b), were also identified as influential in the context of PAT. These factors can significantly impact how individuals perceive and respond to phishing threats, affecting their susceptibility to falling victim to such attacks. Furthermore, as highlighted by Abroshan

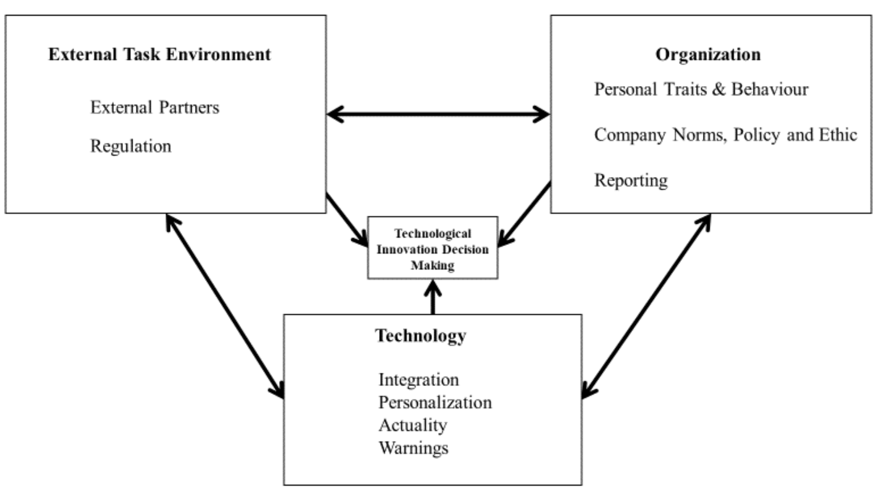

Figure 1: Factors influencing the adoption of PAT grouped by the different TOE domains. Adapted from (Baker, 2012).

(Abroshan et al., 2021a) and Merz et al. (2019), emotional factors such as tiredness play a role in shaping an individual's cognitive and behavioral response to phishing attempts. Therefore, considering these human factors alongside organizational and technological aspects is essential for designing effective and comprehensive PAT programs. The experts also mentioned that employees may be curious about what would happen if they clicked on a phishing link (E4): "*At home, I would not click on this, but here at work, I was interested in what would happen*." Such comments demonstrate how personal traits can influence the company-specific adoption of PAT.

Personal Behavior: Abroshan et al. (2021b), for example, found in their study that risk-taking employees are also more susceptible to phishing attacks. At the same time, Alwanain (2019) suggested that security-conscious employees may fail to trust a legitimate link. A similar effect to that of an employee's willingness to take risks can occur if simulated phishing messages are too easily recognizable, which should be addressed during the introduction of PAT. In such cases, training may lead to phishing desensitization and cause an overestimation of phishing detection skills, which corresponds to the "knowing-doing gap" (Chen et al., 2020; Kearney & Kruger, 2016).

Working under pressure or at high speed also favors a phishing attack (Frank et al., 2022; Wilkinson, 2022). The same effect can also be seen when looking at the influencing factor "fatigue, which, among other things, affects concentration and, thus, attitude toward a potential phishing email (Merz et al., 2019). One of the most significant human behavioral challenges is that most employees view online security as a secondary priority (Roepke et al., 2020). Such attitudes can lead to employees refusing to invest sufficient time in safety training (Hurt, 2018). This problem is particularly pronounced among senior-level employees who may feel their time is too valuable to undergo formal PAT (Hurt, 2018). When adopting PAT, any company-specific hierarchies must be addressed.

In practice, several technical security measures can protect against phishing attacks. However, technological measures can also lead to a false sense of security among employees (Butavicius et al., 2020; Jampen et al., 2020). This is mainly the result of a lack of understanding of the limitations of technology (Butavicius et al., 2020), leading employees to become complacent and take risks (Butavicius et al., 2020). All the experts interviewed were convinced that PAT can demonstrate the limitations of IT system security, and this must be kept in mind when adopting PAT. Another problem with PAT is that employees disregard the training material and do not complete the training session (De Bona & Paci, 2020). To counteract this problem, regulations such as compulsory completion or penalties for defaulters could also be introduced (Alwanain, 2019; Bora et al., 2020).

Company Norms, Policies, and Ethics: Another way to prevent phishing attacks is to create and implement norms and policies and promote an effective cybersecurity culture (Alshaikh, 2020). In their work, Corradini and Nardelli (2019) described building norms as an effective way to influence employee behavior toward cyber threats. The same opinion is shared by Petrič and Roer (2022), who found that norms can influence employee behavior without obliging employees to comply with elaborate procedures. One argument against implementing cybersecurity guidelines and corresponding standards is in a study by Shahbaznezhad et al. (2021), who found that protection against phishing attacks based on norms performed significantly worse than technical and training-based measures. In addition, the difficulty and length of time required to establish norms in a company and embed them in the culture also renders this solution less effective in the short term (Leidner & Kayworth, 2006).

The experts also reported that adopting PAT can help establish a security culture, as it can effectively communicate the company's norms and policies during training sessions (E2). E8 stressed that this helps to show that everyone within an organization is responsible for online security, indicating the importance of a cybersecurity culture for PAT adoption. Experts also recommended considering the existing culture while implementing PAT (E4). Conducting PAT, especially around phishing simulations, is regarded as an ethical grey area due to misleading emails (Sutter et al., 2022). For this reason, PAT should be reviewed and approved by an ethical committee before implementation. However, when reviewing ethical guidelines and approvals by ethics committees, it should be noted that these can delay the start of PAT (Nijland, 2022). For example, E7 mentioned that care must be taken to ensure that individuals are not blamed for poor results. The experts also stated that PAT content should not enter ethically questionable areas, although genuine phishing would exercise no such restraint.

Another common error is implementing a training campaign too quickly (Alshaikh et al., 2018), perhaps owing to pressure to achieve security standards (Alshaikh et al., 2018). According to Volkamer et al. (2020), whether employees should be informed about a planned phishing simulation and its impact on effectiveness should be weighed for all employees. Here, the long-term adoption strategy should be considered. According to Miranda (2018), the problem is that affected entities (including IT staff) need to be informed in advance. However, informing IT staff about an upcoming phishing simulation limits the campaign's effectiveness since they will already be on their guard. The experts added that it would also be possible for employees to warn each other in advance (E3&E4). In any case, employees should be informed about the campaign after a phishing simulation, indicating that such an approach will be adopted in the future (Volkamer et al., 2020).

Regardless of the effectiveness of advance notice, all employees, including IT staff, need to receive training (William et al., 2022). E2 mentioned that it was unlikely that the information helped detect a phishing attack, but it did increase awareness of the phase of the planned attack. Several experts recommended informing relevant personnel as unplanned escalation could occur otherwise, rendering the whole exercise meaningless, by blacklisting the phishing attack. "*I took the phone and asked the CISO if he was attacking us because we were in the process of blocking the phishing sources and deleting all emails received*" (E6). Miranda (2018) also recommended informing the affected entities, thereby preventing the non-recognition of actual phishing attacks or an adverse reaction by IT staff.

It goes without saying that regular repetition of PAT is crucial for reinforcing knowledge and skills over an extended period. By revisiting the training material regularly, employees can consolidate their understanding of critical concepts and practices, reducing the risk of forgetting important information over time. This approach not only helps to maintain awareness of phishing threats but also encourages the application of learned strategies in real-world scenarios. Additionally, frequent PAT can serve as timely reminders of evolving threats and best practices, ensuring that employees remain vigilant and updated in their security practices. Overall, the repetition of training at regular intervals is essential for sustaining long-term effectiveness in combating phishing attacks (Volkamer et al., 2020), which must be considered when a decision to adopt PAT is made. However, when determining the time interval, it should be noted that phishing awareness training is time-intensive and increases the employee workload (Desolda et al., 2022; Rizzoni et al., 2022). Recipients of training said they would find up to five mailings per year acceptable (results unpublished). Therefore, the frequency of sessions should be decided carefully so as not to overburden employees or demotivate them because of excessive repetition (Jampen et al., 2020). All experts agreed that this was highly relevant in practice. The implementation of PAT, especially in the area of phishing simulations, is considered an ethical gray area due to misleading emails (Sutter et al., 2022). It is therefore advisable to have PAT reviewed and approved by an ethics committee before it is carried out. The PAT should also be reviewed and coordinated on the basis of ethical guidelines (Sutter et al., 2022). However, when reviewing ethical guidelines and approvals by ethical committees, it should be noted that these can take a long time and thus cause a delay in adopting PAT (Nijland, 2022).

Reporting: Establishing a reporting platform through which employees can report suspicious mails or receive information is significant for an organization's cyber security (Alshaikh et al., 2018). The relevance of a reporting platform arises, among other things, because most phishing attacks affect several employees within the same organization (Protasova & Mazko, 2021). With the help of a reporting platform, the department responsible for security can be directly informed, and appropriate countermeasures can be taken; this would be significantly faster than other options, as experts 1, 6 and 7 explained. Such an approach is an integral part of cybersecurity and influences the phishing awareness of the entire organization (Bayl-Smith et al., 2022).

However, according to a study by Jaeger and Eckhard, reporting suspicious emails is still rare (Jaeger & Eckhardt, 2021). Therefore, it is essential to teach employees how to deal with suspicious emails and report them to the appropriate office (Jaeger & Eckhardt, 2021; Protasova & Mazko, 2021; Zainab et al., 2021). In practice, however, transparent reporting and feedback processes rarely exist, or it is unclear what form they should take (Jampen et al., 2020; Volkamer et al., 2020). PAT can help implement and embed this process knowledge, as E2 mentioned, "*for example, report buttons within email programs could help to report emails correctly*."

An added effect of such buttons would be increasing awareness through constant visibility in the email platform. However, without clear reporting procedures in place, PAT risks the department concerned being inundated with tickets during a phishing simulation (Althobaiti et al., 2021). This risk leads to a further risk of genuine phishing attacks being overlooked owing to the large number of messages generated by a phishing simulation (Mihelic et al., 2019). The experts agreed that PAT could lead to increased workloads as spam would also be reported, but stressed that giving feedback was still very important, as otherwise, the motivation to report would be lower (E4&E5). Safeguards must also ensure employees are not afraid to report wrongly (E5&E7). Reported click-through rates following PAT can be used to justify continuing or abandoning the sessions (Steves et al., 2020).

Justifications based on click-through rates are particularly challenging for chief information security officers (CISOs) (Steves et al., 2020). As a result of different levels of difficulty, click-through rates can vary and should be assessed according to their level of difficulty (Steves et al., 2020). The experts noted the consistent perception and added that consideration must be given to whether all clicks are legitimate and to assess the severity of the risk (credential loss vs. link clicking; E1,E3&E5).

4.2. Technological Context

Integration: In principle, there are two types of training – direct and embedded (Alabdan, 2020, Alhashmi et al. 2021). Direct training can be sent as an email or delivered as a group lesson, workshop, or story-based session (Alhashmi et al., 2021;; Reinheimer et al., 2020). In contrast, embedded training uses simulated phishing emails containing links or attachments. If the recipients react incorrectly to these emails, access the link, or open the attachment, they are directed to undergo training (Alabdan, 2020).

The technological defense measures against phishing used in practice start with straightforward spam filters that classify emails based on the words in the content and flag or block them as spam (Alhashmi et al., 2021). At the same time, these measures can also block the delivery of simulated phishing emails and thus counteract the benefits of PAT (Volkamer et al., 2020). The undesired blocking of simulated phishing emails can be circumvented through safelisting, i.e., the general unblocking of specific senders (Volkamer et al., 2020). However, establishing such safelisting measures leads to the risk of exploitation by real phishing emails through email spoofing, in which a false sender is impersonated (Volkamer et al., 2020). This notion is supported by experts who recommend that during the adoption of PAT, only expert users should carry out such measures, or it might be beneficial to involve external experts in these tasks (E1,E2,E3, &E7).

Training materials generally teach users how to handle phishing emails on the most used platform – the desktop computer. As a result, people may correctly apply their knowledge to phishing attacks on desktop computers but be unable to adapt it for mobile platforms (Dixon et al., 2022). The problem is that link checking on mobile phones does not work in the same way as on desktop computers (Rizzoni et al., 2022). For example, mobile phones have no way to hover over a link to see the URL, as is possible on a desktop computer (Rizzoni et al., 2022). In response to the increasing use of mobile platforms and the associated risks, training measures should also be adapted accordingly. E2 and E7 reported that mobile platforms can be helpful in training measures and should be considered.

Personalization of PAT offers a way to maintain employee attention and motivation (Alshaikh et al., 2021; Rizzoni et al., 2022; Röpke et al., 2020). Since attackers also use confidential information and personalize their phishing attacks, personalizing training material can increase the effect (Alshaikh et al., 2021; Rizzoni et al., 2022; Röpke et al., 2020). Personalization in simulated phishing emails should include the content, tools, and tasks relevant to the user (William et al., 2022). Content adaptation like this can effectively challenge users, enhancing the learning experience and boosting effectiveness. These considerations must be addressed during the adoption of PATs. (Jaeger & Eckhardt, 2021).

Varying the difficulty level in both the training content and simulated phishing attacks is also significant (Jampen et al., 2020; Steves et al., 2020). One way to implement different difficulty levels is to send initial simulated phishing emails and then subdivide them based on the click behavior of the recipient (Younis & Musbah, 2020). Another option would be to include employee behavior (Alshaikh et al., 2019), but this would require a prior behavioral analysis to classify individuals into suitable categories (Alshaikh et al., 2019).

The experts agreed that individualization would support training sessions, but as this information is currently unavailable, only function-based personalization could be applied: "*Demographics are not in any digital system,*" and using such data would be very complex (E4). System solutions or providers offering up-to-date material and additional customization options come with a high price tag (Burita et al., 2022).

Actuality: Cybercriminals constantly adapt their strategies to circumvent technical security measures or exploit new employee vulnerabilities (Zainab et al., 2021). This creates a burden for companies, as they find it expensive to adjust their technical security measures and update training materials continually. (Zainab et al., 2021). Nevertheless, it is essential to keep training materials current to ensure adequate protection (Rosser et al., 2022) even after PAT – a finding confirmed by the experts. During the evaluation and selection of a training program, care should be taken to ensure it is completely up to date (Rosser et al., 2022). Many system solution providers offer a wide range of possible tools that can help implement phishing awareness training quickly and efficiently. However, these must be evaluated in detail. To ensure their effectiveness, providers must keep their products updated and adapt to the changing methods of actual phishing attacks (Higashino et al., 2019).

The experts recommend that a company's ethical standards be reflected in the content but that some content should not be used in a PAT context as it could trigger negative emotions.

Warnings: Warnings for end users are frequently displayed in external emails or when loading a web page. However, Kävrestad et al. (2022) and Yang et al. (2017) found that awareness training alone does not provide sufficient protection against phishing attacks. Instead, warnings should be used alongside training as a supplementary awareness-raising measure (Kävrestad et al., 2022; Yang et al., 2017). The implementation of warnings offers an extra supplementary security measure and, thus, additional protection against phishing attacks. At the same time, however, warnings can also make PAT too straightforward and negatively affect the outcome. The experts also recommended that these warnings mirror the real warnings used in an organization's emails.

The literature also confirms that many warnings are ignored owing to flooding effects (Desolda et al., 2019; Jampen et al., 2020), but this problem can be minimized through the structure and design of the warnings (Desolda et al., 2019). The experts also added that PAT can help test whether users understand the warnings (E1). If this is not the case, these should be modified or removed completely.

4.3. Environmental Context

This section describes the adoption factors that can arise in relation to the environment surrounding PAT.

External Partners can offer the opportunity to adopt PAT even more efficiently and effectively thanks to their specialization in this area (Kweon et al., 2021) – an insight that all the experts confirmed. They added that partners can help with support, creating material and shaping it to look realistic (E2,E5,&E8). External support also reduces the internal workload during adoption and can help test the internal IT department (E4&E6). Working with external providers can also present risks, however. Burita et al. (2022) noted that giving external partners sufficient information about the internal processes and procedures is essential.

E2 also mentioned a lack of information as a reason for suboptimal results. Furthermore, working with external partners can lead to additional security problems. For example, if a data leak occurs within the provider organization, sensitive data such as names, email addresses, and information used to conduct phishing simulations could fall into the hands of cybercriminals, further compromising an organization's security (Higashino et al., 2019). Using external system solutions also entails the risk that attackers might obtain information about the timing or content of phishing simulations via the provider. An additional security issue cited by the experts was access to the active directory, which should be kept to a minimum (E2). This risk can be exacerbated if the external partner operates from a location with different security or legal regulations. Burita et al. (2022) and Innab (2018) pointed to this issue and stressed that foreign partner companies should be chosen cautiously or may even be legally prohibited due to country regulations. One solution would be to hire external services only from countries with the same level of legal protection (E1, E2, &E7).

Regulation: Phishing simulations for PAT are one of the most employed methods in practice. Mostly, well-known brand logos such as Google, Microsoft, etc. are used to design realistic-looking emails for phishing simulations (Sutter et al., 2022). However, owing to trademark protection, the use of trademarks can have legal consequences (Sutter et al., 2022; Volkamer et al., 2020). These legal bases can vary from country to country and should always be assessed in relation to the country where the PAT is conducted (Sutter et al., 2022). This was supported by E1 and E5, who mentioned trademark protection, copyright, and data protection legislation as areas for consideration.

Labor law regulations must also be factored in (Volkamer et al., 2020). Depending on the organization and its labor law provisions, it may be necessary for data related to PAT to be anonymized or pseudonymized before any analysis takes place (Volkamer et al., 2020). The experts emphasized the importance of large organizations informing relevant security departments about external regulators before implementing PAT, as these entities could potentially interfere with the process. These external organizations could include the domain registrar or even the state security department.

5. Discussion

In the following discussion, we summarize the critical factors that must be considered to implement PAT successfully. As such, it offers guidance for organizations at each phase of PAT adoption.

From an organizational perspective, addressing personal traits, behavior, reporting procedures, norms, policies, and ethics is crucial for PAT adoption. Early consideration of employee traits during the project design phase can mitigate risks and ensure real-world behavior during implementation. This confirms that the human factor should be prioritized as early as possible during PAT adoption. Experts and the literature agree that increased awareness during the implementation phase can also reveal IT system limitations. Special attention must be given to the difficulty and context of PAT, as the risk of overconfidence and desensitization of users must be avoided.

Establishing companywide norms and policies may prolong the design phase, but it is worthwhile for long-term adoption and mitigating risks during implementation. phase. During this phase it is important to inform employees about security actions and the security team to encourage a cybersecurity culture within the organization. Reporting processes should be implemented at the beginning of the design phase to allow employees to test the reporting processes and internalize them. From the outset, it is crucial to account for the additional time and cost required for implementation through realistic capacity planning. Technologically, PAT implementation involves personalization, timely content updates, and effective warning messages.

The extensive literature on PAT adoption and expert input emphasizes opportunities such as using different platforms (mobile/desktop) and determining training frequency. Striking a balance in training frequency is essential to maintain employee motivation without overburdening them during implementation and longtime usage of PAT. Changing training methods can also help focus attention. Personalizing PAT to the company, department, role, or individual behavioral aspects can increase complexity and enhance efficiency. During the usage phase of PAT, it is essential to ensure training materials are up to date, and additional funding must be ringfenced for this. Another consideration is the warnings provided by the existing email system. Testing these during the implementation phase can determine their effectiveness for users, potentially leading to future adjustments or removal of ineffective warnings.

From the environmental perspective, two broad areas were identified: First, all aspects related to external partners that can help during the design and implementation of PAT. The experts were confident that organizations could profit from external partners by reducing the workload and offering specialist expertise. However, external partners could also pose a risk as they could be an access point for malicious third parties during implementation or the usage phase.

Second, it must be remembered that different legal situations apply in other countries and that external agencies must be informed during the design phase to prevent any conflict.

This paper has some limitations: In the literature search, an attempt was made to cover as broad a spectrum as possible using a systematic literature search. Nevertheless, there may be gaps in the relevant literature due to the selection of queries and restrictions. Eight Swiss experts were selected for the interviews, which provides depth in the Swiss context but could also reduce the representativeness of the practitioner insights.

6. Outlook

Phishing attacks have become increasingly prevalent, with the current trend showing no signs of diminishing. At the same time, most cybersecurity incidents still stem from an incorrect response to a phishing attack. Accordingly, continuous PAT is essential to maintain lasting protection. While the adoption of PAT to an organization presents various opportunities, it also carries risks, and it is advisable to consider the opportunities and risks listed in Section 5 of this paper. It is also advisable to assess them individually, as they may vary depending on the industry or country.

For research purposes, further investigation of these unilateral findings would be valuable. Additional studies should substantiate insights exclusively derived from expert interviews.

Lastly, it should be noted that the legal status of PAT appears unclear in both literature and practice. A detailed examination of the legal landscape would contribute significantly to academia and practical application.

7. Acknowledgments

We thank all our experts for providing insights into working practices related to PAT. Financial support was provided by Swiss National Science Foundation (207550) and Digitalization Initiative of the Zurich Higher Education Institutions (DIZH).

8. References

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021a). COVID-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. IEEE access: practical innovations, open solutions, 9, 121916–121929.

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021b). Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. IEEE Access, 9, 44928–44949.

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future Internet, 12(10), 168.

Alhashmi, A. A., Darem, A., & Abawajy, J. (2021). Taxonomy of cybersecurity awareness delivery methods: A countermeasure for phishing threats.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003.

Alshaikh, M., Maynard, S., & Ahmad, A. (2019). Toward sustainable behaviour change: An approach for cyber security education training and awareness.

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. Computers & Security, 100, 102090.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations.

Althobaiti, K., Jenkins, A. D. G., & Vaniea, K. (2021). A Case Study of Phishing Incident Response in an Educational Organization. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2), 338:1-338:32.

Alwanain, M. I. (2019). An evaluation of user awareness for the detection of phishing emails. International Journal of Advanced Computer Science and Applications, 10(10).

Anawar, S., Kunasegaran, D. L., Mas'ud, M. Z., & Zakaria, N. A. (2019). Analysis of phishing susceptibility in a workplace: A big-five personality perspectives. J Eng Sci Technol, 14(5), 2865–2882.

Baker, J. (2012). The Technology–Organization–Environment Framework. In Y. K. Dwivedi, M. R. Wade, & S. L. Schneberger (Hrsg.), Information Systems Theory (Bd. 28, S. 231–245). Springer New York.

Bardsley-Marcial, B. (2022). Common factors in susceptibility to phishing. International Journal of Information, Business and Management, 14(4), 97–104.

Bayl-Smith, P., Taib, R., Yu, K., & Wiggins, M. (2022). Response to a phishing attack: Persuasion and protection motivation in an organizational context. Information & Computer Security, 30(1), 63–78.

Bora, K., Do-Yeon, L., & Beomsoo, K. (2020). Deterrent effects of punishment and training on insider security threats: A field experiment on phishing attacks. Behaviour & Information Technology, 39(11), 1156.

Burita, L., Klaban, I., & Racil, T. (2022). Education and training against the threat of phishing emails. International Conference on Cyber Warfare and Security, 17(1), 7–18.

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., & Calic, D. (2020). When believing in technology leads to poor cyber security: Development of a trust in technical controls scale. Computers & Security, 98, 102020.

Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. Decision Support Systems, 133, 113287.

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. Procedia Computer Science, 198, 656–661.

Corradini, I., & Nardelli, E. (2019). Building organizational risk culture in cyber security: The role of human factors. In T. Z. Ahram & D. Nicholson (Hrsg.), Advances in human factors in cybersecurity (S. 193–202). Springer International Publishing.

Darem, A. (2021). Anti-phishing awareness delivery methods. Engineering, Technology & Applied Science Research, 11(6), 7944–7949.

De Bona, M., & Paci, F. (2020). A real world study on employees' susceptibility to phishing attacks. Proceedings of the 15th International Conference on Availability, Reliability and Security, 1–10.

Delone, W. H., & McLean, E. R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. Journal of Management Information Systems, 19(4), 9–30.

Desolda, G., Di Nocera, F., Ferro, L., Lanzilotti, R., Maggi, P., & Marrella, A. (2019). Alerting users about phishing attacks. In A. Moallem (Hrsg.), HCI for cybersecurity, privacy and trust (S. 134–148). Springer

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human factors in phishing attacks: A systematic literature review. ACM Computing Surveys, 54(8), 1–35. https://doi.org/10.1145/3469886

Dixon, M., Nicholson, J., Branley-Bell, D., Briggs, P., & Coventry, L. (2022). Holding your hand on the danger button: Observing user phish detection strategies across mobile and desktop. Proc. ACM Hum.-Comput. Interact.

Dresing, T., & Pehl, T. (2020). Transkription. In G. Mey & K. Mruck (Hrsg.), Handbuch qualitative forschung in der psychologie (S. 835–854). Springer.

Ebner, T. (2018). 3 steps to better cybersecurity. Associations Now, 14(3), 44–47.

Esteves, J. M., & Pastor, J. A. (1999). An ERP Life-cycle-based Research Agenda (Druck, Link). 13.

Frank, M., Jaeger, L., & Ranft, L. M. (2022). Contextual drivers of employees' phishing susceptibility: Insights from a field study. Decision Support Systems, 160.

Geppert, T., Anderegg, J., Frei, L., Moeller, S., Deml, S., Sturzenegger, D., & Ebert, N. (2022). Overcoming Cloud Concerns with Trusted Execution Environments? Exploring the Organizational Perception of a Novel Security Technology in Regulated Swiss Companies. Proceedings of the 55th Hawaii International Conference on System Sciences, 6822–6829.

Gut, M., & Kammermann, M. (2021). CompTIA Security+: IT-Sicherheit verständlich erklärt; die umfassende Prüfungsvorbereitung zur CompTIA-Prüfung SYO-601

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications, 58, 102726.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. SN Business & Economics, 3(5), 97.

Higashino, M., Kawato, T., Ohmori, M., & Kawamura, T. (2019). An anti-phishing training system for security awareness and education considering prevention of information leakage. 2019 5th international conference on information management (ICIM), 82–86.

Hurt, J. (2018). 5 strategies to avoid phishing attacks in today's medical practices. Ophthalmology Times, 43(8).

Innab, N., Al-Rashoud, H., Al-Mahawes, R., & Al-Shehri, W. (2018). Evaluation of the effective anti-phishing awareness and training in governmental and private organizations in riyadh. 2018 21st saudi computer society national computer conference (NCC), 1–5.

Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security–related behaviour. Information Systems Journal, 31(3), 429–472.

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. Human-centric Computing and Information Sciences, 10(1), 33.

Kävrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., Roos, R., & Furnell, S. (2022). Evaluation of contextual and game-based training for phishing detection. Future Internet, 14(4), 104. https://doi.org/10.3390/fi14040104

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? Computers & Security, 61.

Kotter, J. P. (2012). Leading Change. Harvard Business press.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. Proceedings of the SIGCHI conference on human factors in computing systems, 905–914.

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: An empirical evidence. Information Systems Frontiers, 23(2), 361–373.

Lain, D., Kostiainen, K., Capkun, S., (2022). Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. 2022 IEEE Symposium on Security and Privacy (SP)

Leidner, D. E., & Kayworth, T. (2006). Review: A review of culture in information systems research: Toward a theory of information technology culture conflict. MIS Quarterly, 30(2), 357.

Merz, T. R., Fallon, C., & Scalco, A. (2019). A context-centred research approach to phishing and operational technology in industrial control systems. Journal of Information Warfare, 18(4), 24–36.

Mihelic, A., Jevscek, M., Vrhovec, S., & Bernik, I. (2019). Testing the human backdoor: Organizational response to a phishing campaign. JOURNAL OF UNIVERSAL COMPUTER SCIENCE, 25(11), 1458–1477.

Miranda, M. J. A. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. International Management Review, 14(2), 5-10,56.

Nijland, J. G. W. (2022). Gamification of cyber security awareness for phishing against university students.

Oliveira, T., Martins M.F. (2011) Literature review of information technology adoption models at firm
level. Electron J Inf Syst Eval 14(1):110–121

Petrič, G., & Roer, K. (2022). The impact of formal and informal organizational norms on susceptibility to phishing: Combining survey and field experiment data. Telematics and Informatics, 67, 101766.

Protasova, D., & Mazko, E. (2021). How to protect your organization against phishing attacks?

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., von Landesberger, T., & Volkamer, M. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. Sixteenth symposium on usable privacy and security (SOUPS 2020), 259–284.

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. DIGITAL HEALTH, 8.

Roepke, R., Koehler, K., Drury, V., Schroeder, U., Wolf, M. R., & Meyer, U. (2020). A pond full of phishing games—Analysis of learning games for anti-phishing education. In G. Hatzivasilis & S. Ioannidis (Hrsg.), Model-driven simulation and training environments for cybersecurity (S. 41–60). Springer International Publishing.

Rogers, E. M., Singhal, A., & Quinlan, M. M. (2008). Diffusion of Innovations. In An Integrated Approach to Communication Theory and Research (2.) Routledge.

Röpke, R., Schroeder, U., Drury, V., & Meyer, U. (2020). Towards personalized game-based learning in anti-phishing education. IEEE 20th international conference on advanced learning technologies (ICALT), 65–66.

Rosser, H., Mayor, M., Stemmler, A., Ahuja, V., Grover, A., & Hale, M. (2022). Phish Finders: Crowd-powered RE for anti-phishing training tools. 2022 IEEE 30th international requirements engineering conference workshops (REW), 130–135.

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? Journal of Computer Information Systems, 61(6).

Steves, M., Greene, K., & Theofanos, M. (2020). Categorizing human phishing difficulty: A phish scale. Journal of Cybersecurity, 6(1).

Sutter, T., Bozkir, A. S., Gehring, B., & Berlich, P. (2022). Avoiding the hook: Influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception. IEEE access: practical innovations, open solutions, 10.

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). The processes of technological innovation. Lexington.

Volkamer, M., Sasse, M. A., & Boehm, F. (2020). Analysing Simulated Phishing Campaigns for Staff. In I. Boureanu, C. C. et al., Computer Security (S. 312–328). Springer.

Wash, R., & Nthala, N. (Hrsg.). (2021). Knowledge and capabilities that non-expert users bring to phishing detection.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS quarterly, xiii–xxiii.

Wilkinson, L. (2022). 4 tips to protect IT employees from phishing attacks. Construction Dive.

William, Y., He, H., Wang-Sheng, L., Fadi, A. J., & Rachel, M. (2022). Simulated phishing attack and embedded training campaign. Journal of Computer Information Systems, 62(4), 802–821.

Yang, W., Xiong, A., Chen, J., Proctor, R. W., & Li, N. (2017). Use of phishing training to improve security warning compliance: Evidence from a field experiment. Proceedings of the hot topics in science of security: Symposium and bootcamp, 52–61.

Younis, Y. A., & Musbah, M. (2020). A framework to protect against phishing attacks. Proceedings of the 6th international conference on engineering & MIS 2020.

Zainab, A., Chaminda, H., Liqaa, N., & Imtiaz, K. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.