Employees’ Attitudes towards Phishing Simulations: “It’s like when a child reaches onto the hot hob”

Katharina Schiller
katharina.schiller@hof-university.de
Hof University of Applied Sciences
Hof, Bavaria, Germany

Florian Adamsky
florian.adamsky@hof-university.de
Hof University of Applied Sciences
Hof, Bavaria, Germany

Christian Eichenmüller
christian.eichenmueller@fau.de
Friedrich-Alexander-Universität
Erlangen-Nürnberg (FAU)
Erlangen, Bavaria, Germany

Matthias Reimert
matthias.reimert@gmail.com
Independent Researcher
Munich, Bavaria, Germany

Zinaida Benenson
zinaida.benenson@fau.de
Friedrich-Alexander-Universität
Erlangen-Nürnberg (FAU)
Erlangen, Bavaria, Germany

ABSTRACT

E-mail phishing attacks remain one of the most significant challenges in IT security and are often used for initial access. Many organizations rely on phishing simulations to educate their staff to recognize suspicious e-mails. Previous studies have analyzed the effectiveness of these phishing simulations with mixed findings. However, the perception of and attitudes towards phishing simulations among staff have received little to no attention. This paper presents findings from a study that we carried out in cooperation with a multinational company that conducted phishing simulations over more than 12 months. We first conducted a quantitative survey involving 757 employees and then qualitative interviews with 22 participants to gain deeper insights into the perception of phishing simulations and the corresponding e-learning. We could not find evidence that employees feel attacked by their organization, as previous studies suspected. On the contrary, we found that a majority (86.9 %) have a positive or very positive attitude towards phishing simulations. The interviews revealed that some employees developed new routines for e-mail processing, but most describe themselves as having become more vigilant without concrete changes. Furthermore, we found evidence that phishing simulations create a false sense of security, as the employees feel protected by them. Additionally, a lack of communication and feedback can negatively impact employees’ attitudes and lead to adverse consequences. Finally, we show that only a small portion of the employees who clicked on the phishing website interacted with the interactive e-learning elements, which raises questions about its objective usefulness, although they are perceived as useful.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**.

CCS ’24, October 14–18, 2024, Salt Lake City, UT, USA
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0636-3/24/10.
https://doi.org/10.1145/3658644.3690212

KEYWORDS

phishing simulations, embedded training, security awareness

ACM Reference Format:
Katharina Schiller, Florian Adamsky, Christian Eichenmüller, Matthias Reimert, and Zinaida Benenson. 2024. Employees’ Attitudes towards Phishing Simulations: “It’s like when a child reaches onto the hot hob”. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS ’24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3658644.3690212

1 INTRODUCTION

“*Phishing is once again the most common vector for initial access*”—is one of the key messages of a report published by the European Union Agency for Cybersecurity in 2023 [11]. The Anti-Phishing Working Group (APWG) [1] monitored nearly 5 million phishing attacks in 2023 and calls it the worst year for phishing so far. Consequently, phishing remains one of the biggest cyber security threats.

Many companies extended their security portfolio to add phishing awareness training for their employees. One method that is commonly deployed in the industry is called *phishing simulations*, usually accompanied by *embedded training*. In this method, the employees get simulated phishing e-mails, and when they click on the link or try to enter their credentials, they get forwarded to a special learning website. Phishing simulations are now a common business model of companies specializing in awareness training programs [19, 27, 32, 35]. Phishing simulations are quite controversial in the scientific literature. In particular, various studies [5, 6, 18, 20, 22, 24] analyzed the efficacy of phishing simulations and either concluded that there is only a short-term reduction in the click-through rate, which disappears after a while or even found no effect at all. Lain et al. [24] say that “*such training method may cause unexpected and negative side effects, such as increased susceptibility to phishing*”. Apart from doubts about efficacy, there are also multiple assumptions in the literature that phishing simulations are perceived negatively by employees. Volkamer et al. [39] stated that “*the perception that they are being attacked by their own organisation while working to deliver its productivity goals can have a negative impact on staff trust in the organisation*”. Additionally, there is negative media coverage, e. g., in 2020, a phishing simulation in a US company went wrong and caused outrage and anger among employees [26]. One of the fake phishing e-mails promised a bonus to the employees, but this, in fact, did not exist. To the best of our knowledge, there is no study yet that systematically investigates the employees' attitudes towards phishing simulations conducted by their organization.

We accompanied a multinational manufacturing company in conducting a phishing simulation and introducing an interactive security awareness e-learning program with gamification elements. Four to five months after the phishing simulation began, we conducted an anonymous survey of employees and invited them to participate in personal interviews. While other studies focused on the efficacy of phishing simulations in the detection rate of simulated phishing attacks, we focused on users' perceptions and attitudes. We conducted our study with the following Research Questions (RQs) in mind:

RQ1 What is the employees' perception of, and attitude to, phishing simulations conducted by the company?
RQ2 Which behavioural changes do employees report?
RQ3 What is the employees' perception of, and attitude to, a parallel security awareness e-learning program?

To address these RQs, we first conducted a quantitative survey with 757 staff members. Out of these, we later chose 22 voluntary participants for qualitative interviews to get deeper insights into the perception of phishing simulations and e-learning. Our work makes the following contributions:

- Employees feel more confident in detecting phishing and feel protected by their company through the phishing simulation. This may result in a false sense of security, as phishing simulations are not a protection measure per se.
- Employees have a positive attitude towards the phishing simulation and do not feel attacked by their organization, as assumed by Volkamer et al. [39].
- A reporting button, in combination with a clear communication path, as Volkamer et al. [39] suggest, helps people to have a clear and straightforward path to report incidents, and feedback on these reports is positively received.
- Labelling e-mails from senders outside the organization with `[EXTERNAL]` helps people classify e-mails as phishing.
- Employees appreciate the combination of phishing simulation and parallel e-learning programs because they feel prepared, skilled and continuously trained.

2 PHISHING SIMULATION MECHANICS

In a phishing simulation, an organization intentionally sends phishing e-mails to its employees to train them (see Figure 1). The following explanation refers mainly to how the simulation is organized in the company we worked with. Other simulations may differ in detail, e. g., in whether there is a reporting button and feedback.

In Step (1), the simulated phishing e-mails are sent to the employees. These are sent randomly and at various times to ensure that not all employees receive the same e-mail simultaneously. Employees who do not click on the link or attachment[1] in the e-mail (2a) and ignore or delete the e-mail (3b) receive no further notification (4b). This may occur because the employee has not seen the e-mail or classified it as suspicious. If they report the e-mail using a reporting function in the e-mail client (3a), they receive immediate feedback (4a). If an employee clicks on a link or attachment, there can be two outcomes. In Step (5), the employee opens a fake phishing website with their click. They can either be immediately forwarded to a learning website, or the simulation can wait for their next steps. If the employee can recognize the fake website or the simulated phishing e-mail as suspicious, they leave the website (5a). Otherwise, if the employee starts interacting with the website (5b) by typing in their credentials, they are forwarded to a learning website, where their interactions with it are measured (7).

Due to anonymization, it is not possible to measure whether someone is intentionally entering falsified credentials. Simultaneously, the organization measures the views of the e-mail, clicks on links or attachments and the views or interactions with the faked phishing website (click-through rate) (6). The objective is to reduce the click-through rate over time. The company commissioned an external provider to conduct the simulation and purchased various training modules tailored to its requirements, as we describe in more detail in Section 4. Collaboration with the organization's IT department is required to ensure that the simulated phishing e-mails reach the users, e. g., adjustment of allowed listing. Ideally, responsible employees in the IT department must be briefed to be able to react correctly to reports of simulated phishing e-mails.

3 RELATED WORK

Technical measures alone are not sufficient to prevent employees from falling for phishing. Besides, organizations do not always implement and apply technical measures correctly, as Hu et al. [16] show in their study about the adoption of technical measures. Thus, suspicious e-mails still end up in users' inboxes.

Companies rely on user education and awareness training to make employees aware of the dangers and support them in recognizing threats. Many studies analyze the effectiveness [6, 21, 23, 29, 33, 37, 41, 42], repetition rates [28], or user preferences [38] of various training measures. A special training method brought into focus by Kumaraguru et al. [21] is *embedded training* that is shown immediately after the misconduct of clicking on a phishing link. This training is supposed to be effective because users see it without delay; it is integrated into their working routine and not limited to a one-time training. Moreover, it only concerns the people who make mistakes in recognizing phishing. Some studies [6, 12, 15, 18, 21–23, 34, 44] show the advantages of embedded training over other methods, such as pure text-based or in-class training. Other studies [7, 10, 25, 40] use simulated phishing e-mails to measure the effectiveness of different training measures. Greene et al. [13] say that a phishing simulation can be helpful for regularly raising users' awareness of current threats. Yet, it makes even more sense to develop an early warning system by encouraging users to report suspicious e-mails and provide a reporting channel.

However, some researchers show that phishing simulations can have adverse effects. Volkamer et al. [39] critically analyzed phishing simulations. They state that the validity of the results is controversial and depends on many factors. They also criticize organizations for changing existing security measures to carry out phishing simulations, such as adjusting e-mail filters to allow simulated

[1] Attachments in this case are fake links in the e-mail body that are placed above the text and imitate a file.

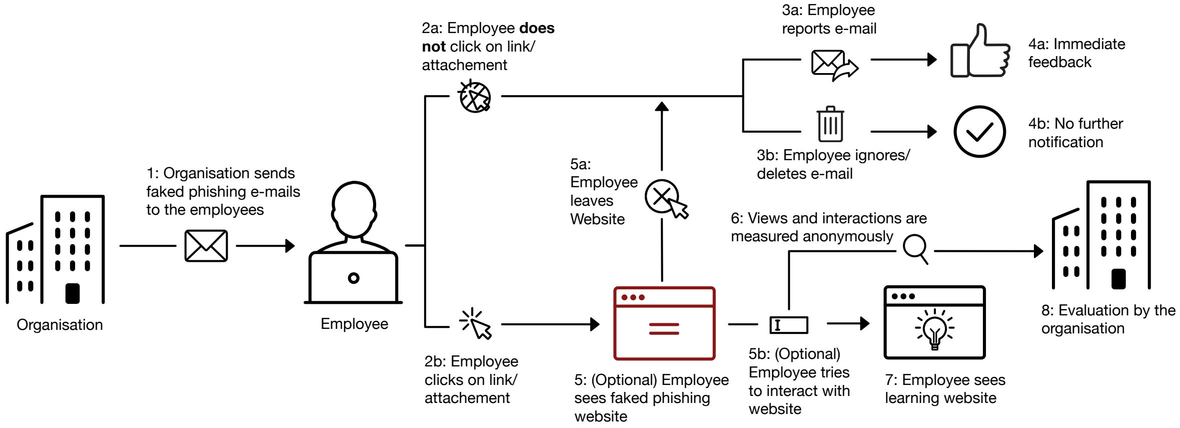

1: Organisation sends faked phishing e-mails to the employees
Organisation
Employee
2a: Employee **does not** click on link/ attachement
2b: Employee clicks on link/ attachement
3a: Employee reports e-mail
3b: Employee ignores/ deletes e-mail
4a: Immediate feedback
4b: No further notification
5a: Employee leaves Website
5: (Optional) Employee sees faked phishing website
5b: (Optional) Employee tries to interact with website
6: Views and interactions are measured anonymously
7: Employee sees learning website
8: Evaluation by the organisation

Figure 1: Procedure model of an organization that runs a phishing simulation with embedded training.

phishing e-mails to pass through. Notably, they assume adverse effects on the relationship of trust between employees and management. As the phishing simulation requires much preparation in terms of communication and work assignments, they recommend investing this effort and money in technical measures and other awareness training methods. A study by Brunken et al. [3] actually found hidden costs and a large time investment involving more employees than expected. They conducted interviews with the company's key actors during the preparation of a phishing simulation. Ultimately, the company chose an offer that only fulfilled some of their requirements. Schwab et al. [31] investigate which factors lead to employee acceptance of phishing simulations. For example, they show that consent is essential, but monetary incentives in the simulated phishing e-mails are seen as negative.

Lain et al. [24] conducted a large-scale phishing study over 15 months. They show that phishing simulations are ineffective and may lead to "*unexpected side effects*". In their study, the click-through rate for employees who saw a learning website was higher than for those who did not receive such training. As the learning website was voluntary, it is unclear whether the participants read it. However, they suspect a false sense of security, as the participants feel protected by the company through the learning website. Caputo et al. [5] also could not find a significant difference in the decrease in click rates. In interviews, they found that the learning materials are not read and are, therefore, similar to no training. Greitzer et al. [14] found that participants who clicked in the first few weeks were more likely to click in the last few weeks. Canham [4] investigated the reasons for repeated clickers and non-clickers.

Furthermore, a number of studies [5, 8, 13, 24, 43] found that employees might develop a false sense of security and overestimate the companies' security measures. In Williams et al. [43], the focus groups mentioned doubts about reporting suspicious e-mails as they did not know what would happen afterwards. Distler [9] mentions a fear of getting others in trouble for reporting suspicious e-mails. Huaman et al. [17] found employees did not foresee a high risk of cyber attacks for their companies. There is also a multitude of studies investigating the reasons behind employees' susceptibility to phishing. A suitable context is mentioned as the reason why someone falls for phishing [2, 13–15, 44]. Other reasons are curiosity [2, 15] or fear of negative consequences [13]. Zhuo et al. [45] specifically analyzed the effects of workload and found that a higher workload does not lead to a higher susceptibility.

Although the scientific community has thoroughly studied phishing simulations' click-through rates and reasons for clicking and not clicking, we have not yet found a study that systematically addresses the perceptions of simulated phishing e-mails.

4 METHODOLOGY

4.1 Timeline of the Study

The company planned the original phishing simulation over a period of one year. Figure 2 shows the timeline of that period. In advance, they created an information article on their intranet and sent a newsletter e-mail to brief all employees about the phishing simulation (1). Thereupon, the initial phase of the phishing simulation started (2). In this phase, all employees received the same three simulated phishing e-mails in a random order and on a random date within one month. After the initial phase, the company reported the results again via intranet and e-mailed newsletter and introduced the collaboration with our university (3). After a pause of approximately 2.5 months, the subsequent phase started. Every employee received one simulated phishing e-mail every five to six weeks in random order. One exception was a special simulated phishing e-mail (see Listing 1) that served as a basis for our survey (5). Every employee received the special e-mail at a random time and in a random order within approximately four weeks before the survey to ensure everyone had the chance to see and remember it.

4.2 Phishing Simulation and E-Learning

When we first contacted the company, they had already commissioned a phishing awareness program consisting of phishing simulations and e-learning courses via an external service provider. The program initially ran for one year and three months. The design of the phishing simulation or e-learning is not part of our

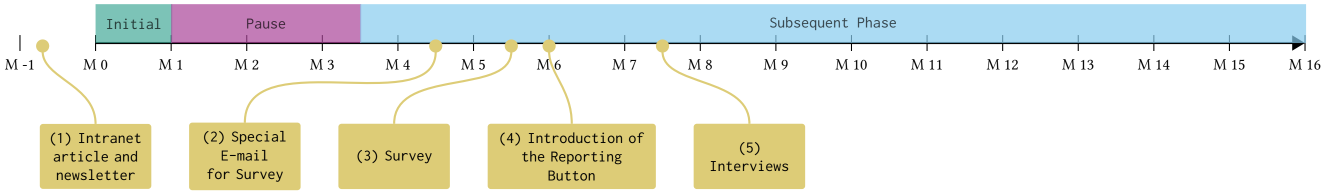


Figure 2: The timeline shows the different events in months (M) from the phishing simulation, starting in June 2022 and ending in November 2023. The first month was the initial phase, followed by a pause of 2.5 months and the subsequent phase. In the light brown boxes, we show the starting points of the other events (special e-mail for survey, survey, introduction of the reporting button and interviews).

Listing 1: The special simulated phishing e-mail for our survey was sent to all employees during the same period. It seems to be from the HR department and refers to migrating to a new HR system. The company and recipient names are blacked out.

```
From: "[EXTERNAL] [redacted] Update" <update@[redacted].com>
To: [redacted]
Subject: New HR system "easyHR"

Dear colleagues,

We are pleased to inform you that starting in November,
our current HR system will shift to the new HR system, "
easyHR." The new HR tool will significantly simplify and
digitalize many time-consuming processes such as leave
requests, absences and approval processes.

Please activate your access by October 24, 2022 at https
://easyhr.[redacted].com/activate to ensure that no data is
lost.

Until the actual launch, the new system is in a test
stage. Please note that changes will be made until the
actual launch. Errors and suggestions for changes can be
forwarded to easyHR until the launch.

All information about easyHR and the protection of your
personal data can be found here.

Kind regards,

Your Update Team
```

study design. We accompanied the company and observed the program provided by the external provider. The design of the phishing e-mails or the schedule in which the e-mails were sent was suggested upon by the external provider and agreed by the company. Based on previous experience with other companies, the external provider offers a portfolio of e-mails of varying complexity. The company selected various customized simulated phishing e-mails from the external service provider's portfolio. This means, for example, that colors, logos, and sender addresses were adapted to match the corporate design and internal workflows. The language of the simulated phishing e-mails was also customized to match the recipient, which means that the e-mails are available in a total of 19 languages. The simulated phishing e-mails contained links and/or attachments that either led directly to a learning website or after an interaction with a simulated phishing website. Likewise, the learning website also fit the company's corporate design (see the Extended Version [30]). It showed the simulated phishing e-mail that the recipient had just clicked on and presented step by step how it could be identified as phishing. Furthermore, the learning website contained general information and explained the potential consequences of phishing. It also stated that no personal data is stored, i. e., who clicked is not traceable. The company solely coordinated the details and the design of the special simulated phishing e-mail with us.

The second part of the awareness program is e-learning. The e-learnings are small interactive learning units divided into different chapters and learning modules. The company has created a learning path with five phases, dividing the modules into introduction and deep-dive modules. For example, an introduction module covers phishing in general, while a deep-dive module scheduled in a later phase focuses on spear phishing. The e-learning modules cover information security in general and go beyond pure e-mail phishing. Usually, an e-learning module takes a few minutes. They are assigned to employees via an internal training pool and must be completed within a certain period. Employees can repeat e-learning at any time. The e-learnings are independent of the phishing simulation but started simultaneously with the phishing simulation and continued throughout it.

The company had already carried out compulsory awareness training beforehand. Yet, this was the first phishing simulation. It can be assumed that employees who have been with the company for several years have already taken part in one or more awareness training courses. Since phishing e-mails were also part of these courses, most employees already had a basic understanding of phishing.

4.3 Selection of the Phishing E-Mails

The phishing e-mails offered by the external provider differed in difficulty, psychological tactics, technological vector, and context and were customized afterwards. The external provider uses its own methodology to classify the level of difficulty, which is strongly based on the *Phish Scale* by Steves et al. [36]. We could not influence the selection of the phishing e-mails except for the special phishing e-mail that served as a basis for our survey. We chose the e-mail in Listing 1 because it seemed plausible and had the [EXTERNAL] marker. According to the provider, the selected e-mail is a medium difficult e-mail. The [EXTERNAL] marker needed to be present, as we wanted to investigate its effect on the employees' phishing susceptibility.

4.4 Further Anti-Phishing-Measures

The company has been using external marking for all e-mails from senders outside the company for some years. This means that the label [EXTERNAL] is displayed in front of the sender's name (see, e. g., Listing 1). The company did not switch off this label for the simulated phishing e-mails. In addition, the company migrated to Microsoft 365 during the phishing simulation. As part of this, they introduced a reporting button for phishing e-mails. If employees report a phishing e-mail from the simulation, they receive direct feedback that they have correctly recognized phishing and that it was part of the simulation. If it is not a simulated phishing e-mail, the employee receives a query as to why they consider the e-mail suspicious, and it is forwarded to a support employee. As this function was used frequently by employees, the workload for the support employees increased. For this reason, the company later added another query to the report button, asking whether the employee needed feedback or not.

4.5 Ethics

The Chief Information Security Officer (CISO) and the company's management agreed to collaborate and allowed us to conduct the survey and the interviews. The external service provider who conducted the phishing simulation is located in Germany. All data is stored on German or European servers, ensuring compliance with stringent data protection regulations. To send the simulated phishing e-mails, the provider stores some information about the employees, including e-mail addresses or department affiliations. An evaluation by individual departments or locations is possible if the number of employees is large enough. We were given access to these aggregated evaluations, as was the company. The company announced the awareness program and the phishing simulation in an intranet article, which was also sent via a newsletter e-mail. Prior notification is usually necessary in order to obtain the approval of the work council. The external provider also recommends this process. After all employees received the special simulated phishing e-mail, the company announced its cooperation with us and invited employees to our survey.

4.5.1 Survey Ethics. We used the German website SoSci survey[2], which stores the collected data on German servers. The survey started with a consent form. Participation in the survey was anonymous. However, the participants who agreed to participate in the interview had to provide their e-mail addresses, which were then stored together with their answers, which were later used to select the interviewees. This was emphasized at the beginning and again in the specific survey question. We only used these e-mail addresses to contact the employees later for the interview invitations and a raffle of four Amazon vouchers worth € 25 each, in which all participants who chose this option took part. The collected data was shared with the company only in aggregated and anonymized form. The company is, therefore, unable to establish any correlations with the answers of individual employees. Furthermore, the company does not know which employees participated in the survey.

4.5.2 Interview Ethics. Participation in the interviews was voluntary and counted as working time. It should not be an additional burden for the participants to take part in the interviews in their free time. This was arranged with the company in order to show the participants that the topic and the employees' opinions are relevant to the company. Even if an employee had provided their e-mail address, they could withdraw their participation anytime. Together with an invitation for the interviews, we sent out a consent form for the interviews. The employee also received a link to an appointment selection. By confirming an appointment, the employee also agreed to the consent form. We conducted the interviews via Zoom. Participants were informed in advance that we would record the audio of the interview locally on the device and transcribe it later. We recommended scheduling an interview either in the home office or using a separate meeting room if offices are shared, such that the participants could speak freely and were not influenced by colleagues in the same room. Most of the participants were working from home or alone in the office. In two cases, we recognized other employees in the office. However, these participants did not feel bothered by their colleagues. At the beginning of the interview, the participants were again asked if they agreed to the consent form and the recording. Recordings and transcripts were saved with a unique identifier and without the employee's name. The collected data was shared with the company only in aggregated and anonymized form. The names and e-mail addresses of the participants were only used to contact them and were not further evaluated or disclosed to the company. Therefore, the company does not know who took part in the interviews. To transcribe the interviews, we used OpenAI Whisper on our local devices and later corrected the transcripts manually so that no data was disclosed to third parties.

4.6 Survey Methodology

The company shared the link to the survey via an intranet article and an e-mailed newsletter with a description of the study. In the company, it is the norm to put a German version of the content at the beginning and then an English version. Thus, the English text contained the link to the English version of the survey. Participants could later switch the language on the survey website between those two languages. Three researchers independently translated the German survey into English and then scheduled a meeting in which the three researchers created a joint version. The Extended Version [30] provides an overview of the survey. We designed the survey based on our research questions but also integrated questions relevant to the company. Initially, we asked whether the participant was familiar with the phishing simulation and whether they could remember the special simulated phishing e-mail which is shown in Listing 1. We asked about their reason for clicking or not clicking on the link in that e-mail and used selection options based on Benenson et al. [2]. This was followed by questions about the learning website, i. e., how they felt when they saw it and how helpful it was. Then, a block of questions followed, based on the participants' general attitude towards the phishing simulation and whether they could imagine it being continued in the future. The

[2] https://www.soscisurvey.de/

last block was related to e-learning. Finally, we asked demographic questions. Completing the survey took around 5 min to 6 min on average.

4.7 Interview Methodology

In the survey, 186 participants said they were willing to participate in the interviews. We tried to recruit interview participants from all continents to consider cultural differences and provided interview slots during typical core working hours. However, only 21 participants from outside Europe indicated that they would like to participate in the interview. We asked the company whether another invitation could be sent to recruit more international participants. However, the distribution of employees is not globally balanced. For example, according to the company, there are only a handful of employees in Australia and Oceania. Similarly, in Bulgaria, there are only three employees participating in the phishing simulation. For that reason, the company rejected another invitation to the interviews, as in their opinion, getting any more international participants would have been unlikely. In addition, other factors were more relevant for us, such as the general attitude or interesting answers to open-ended questions.

To reflect as many different opinions as possible, we coded the free-text responses in the survey on the general attitude towards the phishing simulation. We created nine codes for all free text answers. Examples are the codes "helps privately" for statements that indicate that the phishing simulation helps participants in their private lives or "not enough time/takes time away" for statements that are critical towards the time factor. In particular, we also tried to recruit participants with a negative attitude toward the phishing simulation. We selected 36 participants based on their general attitude (free text response and rating), demographics, whether or not they clicked on the special simulated phishing e-mail, and interesting statements in other free text fields. Only three participants with a negative attitude provided an e-mail address. We invited two of them because the third participant's answers were inconclusive. In the end, we were able to arrange 22 interviews. Unfortunately, none of these 22 participants had a negative general attitude or were located outside Europe.

We designed the interview guide based on our research questions and survey findings, which allowed us to examine some statements thoroughly. Since we planned semi-structured interviews, there is no fixed order. Nevertheless, we created a basic outline with the four sections:

- *Everyday work/Dealing with e-mails:* as an introduction;
- *Phishing campaign:* everything related to phishing simulation, but especially focused on the personal perception, the perception of colleagues and behavioral changes;
- *E-Learnings/Reporting button:* perception of the e-learnings and comparison with the phishing simulation;
- *Demographics* if it was not included in the survey.

An overview of the interview guide can be found in the Extended Version [30]. An interview took an average of 32 min. Since not all of the participants were familiar with Zoom, we recommended that everyone should plan a short amount of extra time. In order to keep to the time limit for the interviews, we color-coded the questions in the interview guide and structured them according to their relevance to our research. We also included alternative formulations.

Table 1: Demographics of the 757 survey participants.

	Demographics	Number	Percentage
Sex	male	500	66.1 %
	female	245	32.4 %
	diverse	3	0.4 %
	no answer	9	1.2 %
Age	younger than 20 years	3	0.4 %
	20–29 years	93	12.3 %
	30–39 years	186	24.6 %
	40–49 years	213	28.1 %
	50–59 years	204	27.0 %
	60–69 years	48	6.3 %
	70 years or older	1	0.1 %
	no answer	9	1.2 %
Area	Europe	699	92.3 %
	North America	26	3.4 %
	South America	10	1.3 %
	Asia	8	1.0 %
	Africa	6	0.8 %
	Australia/Oceania	2	0.3 %
	no answer	6	0.8 %
Employment	less than 1 year	57	7.5 %
	1 to 3 years	76	10.0 %
	4 to 6 years	99	13.1 %
	7 to 9 years	45	5.9 %
	more than 9 years	470	62.1 %
	no answer	10	1.3 %
Screen time/day	less than 2 h	10	1.3 %
	2–4 h	46	6.1 %
	5–6 h	105	13.9 %
	6–8 h	297	39.2 %
	more than 8 h	293	38.7 %
	no answer	6	0.8 %

4.8 Demographics of Participants

The survey was completed by 757 participants (see Table 1). Most of them are male (66.1 %), between 30 and 59 years old and work in Europe (92.3 %). The majority (62.1 %) has been employed by the company for over 9 years. Most participants spend 6 hours or more of their working day in front of a screen. Table 2 shows an overview of the 22 interview participants' demographics. Most came from Germany (18), two from Switzerland, and one each from Latvia and Spain. The participants' employment levels range from trainees to project and division managers.

4.9 Data Analysis

The quantitative data from the survey was analyzed descriptively using customized scripts. To code the free text responses to the survey, one researcher used an inductive method and created a small codebook for each free text field. The resulting codes were then discussed with a second researcher, and every statement was assigned

Table 2: Demographics of the interview participants, how often they clicked on simulated phishing e-mails, their confidence in using the Internet (self-assessment) on a scale from 1 (very unconfident) to 5 (very confident), and their general attitude stated in the survey from very negative to very positive.

ID	Sex	Age (in years)	Location	Area	Management responsibility	Screen time per day	Clicked	Self-assessment	Attitude
P01	f	50–59	Spain	Internal Office	no	6 h to 8 h	1	3	neutral
P02	m	20–29	Germany	Startup	yes	more than 8 h	0	4	very positive
P03	f	30–39	Germany	Predevelopment	no	more than 8 h	0	5	very positive
P04	f	20–29	Switzerland	Purchasing	no	more than 8 h	0	4.5	very positive
P05	m	20–29	Germany	Engineer	no	6 h to 8 h	0	4	very positive
P06	m	20–29	Germany	SAP	no	6 h to 8 h	1	5	very positive
P07	f	40–49	Germany	Project Management	no	6 h to 8 h	0	4	positive
P08	m	30–39	Germany	Software Development	no	more than 8 h	0	5	neutral
P09	m	30–39	Germany	Project Management	no	5 h to 6 h	0	4.5	positive
P10	m	50–59	Germany	Sales Force	no	6 h to 8 h	2–3	3	very positive
P11	m	40–49	Germany	Sales	no	2 h to 4 h	1	3	very positive
P12	m	50–59	Germany	IT	yes	more than 8 h	0	4	positive
P13	f	40–49	Germany	Product Development	no	more than 8 h	2	3	very positive
P14	m	50–59	Germany	Product Development	no	6 h to 8 h	2	3	very positive
P15	m	< 20	Germany	Trainee	no	less than 2 h	0	4.5	positive
P16	m	60–69	Germany	Product Development	no	6 h to 8 h	0	4	very positive
P17	m	30–39	Germany	Product Development	no	6 h to 8 h	0	4	positive
P18	m	50–59	Germany	Prototyping	yes	6 h to 8 h	1–3	5	very positive
P19	m	60–69	Latvia	Area Management	yes	2 h to 4 h	0	3.5	neutral
P20	f	30–39	Germany	Corporate Communications	no	6 h to 8 h	1	4.5	very positive
P21	m	40–49	Germany	Development	no	6 h to 8 h	1	4	very positive
P22	m	> 70	Switzerland	Finances	yes	2 h to 4 h	0	n.a.	positive

to a code. For example, for the "other" field for the feeling when someone saw the learning website, we created ten codes, such as "Embarrassed/caught" for statements that express embarrassment or "Clicked on purpose" for statements that show someone knew what would happen. If there were several statements in one comment, we assigned several codes.

To transcribe the interviews, we used OpenAI Whisper on local devices (without a cloud connection) and corrected the transcripts manually. First, one researcher coded the interviews using an inductive method and created a codebook. In addition, another researcher conducted an inductive coding of three interviews and created a codebook. The three interviews were selected in such a way that they reflect different demographics and clicking behavior. Afterward, the codebooks were discussed in groups of three, and all 116 codes were consolidated. We then structured the codes to fit the main parts of the interview guide and be thematically relevant. This resulted in the following structure:

Demographics and Everyday Work: General descriptions of everyday work unrelated to phishing or IT security.

General IT Security: Experience and knowledge that does not originate from the program.

Communication and Information Exchange: Descriptions of communication within the company. Especially e-mail use in everyday working life. Feedback from colleagues based on exchanges with them.

General Phishing: General statements on phishing, handling, reporting processes, recognizing and the threat of phishing.

Phishing Simulation: Concrete statements on the phishing simulation, its evaluation, degree of difficulty, and differentiation. Also, how the person felt when they clicked on a simulated phishing e-mail.

E-Learnings: Concrete statements on the e-learnings, their evaluation, degree of difficulty and structure.

Changes and Impact: Has the participant's behavior changed and how? What are the effects on everyday working or private life, and what lessons has the person learned?

Summary of the Program: Summarizing rating, usually based on the interview's final question about preference for phishing simulation or e-learning.

We coded judgemental statements as positive, negative, or neutral if present. Similarly, the difficulty levels of phishing simulation and e-learning were divided into easy, medium, and difficult. Moreover, we assigned the feeling when the person has clicked to different emotions.

To categorize unclear statements, we conducted an interpretation workshop, where excerpts from six interviews were discussed. Both researchers who created the codebooks and six other researchers from our lab took part. The discussion concentrated especially on when something is a new behavior and which statements are positive, negative, or neutral. Subsequently, one researcher conducted a second coding round based on the final codebook.

5 RESULTS

This section shows the changes in the click-through rate, findings from the survey and the interviews. We refer to the participants

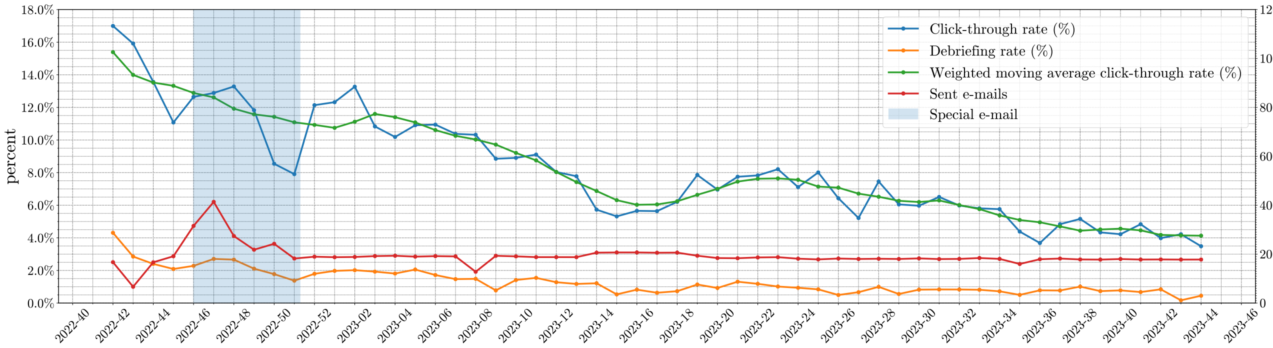


Figure 3: The blue line shows the click-through rate in percent over the subsequent phase in calendar weeks, including the special simulated phishing e-mail (highlighted blue). The red line shows the e-mail count of all simulated phishing e-mails over the same time range. The debriefing rate is shown with the orange line relative to the click-through rate.

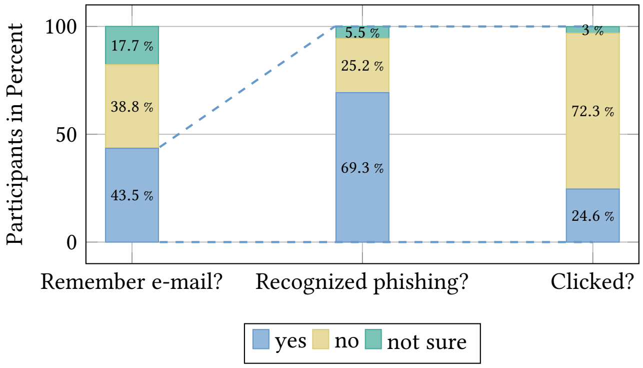


Figure 4: The first bar shows how many participants could remember the special simulated phishing e-mail ($n = 757$). The second bar shows how many of the participants recognized it as phishing ($n = 329$). The last bar shows the number of reported clickers ($n = 329$).

with a unique identifier consisting of *S* for survey participant or *P* for interview participant and a sequential number.

5.1 Phishing Simulation Results

The external provider that was commissioned to conduct the phishing simulation reported the data they measured to us. Figure 3 shows an overview of the click-through and debriefing rates and the number of sent simulated phishing e-mails. With the debriefing rates, the company measured how many people interacted with the learning website. The click-through rate in the first week was 17 %. After a year, the rate decreased to 3.5 % in the last week. The debriefing rates remained relatively constant. On average, 16.2 % of employees who saw the learning website interacted with it. The number of simulated phishing e-mails sent remains constant (on average, 1920 per week). An exception is the blue area, where our special simulated phishing e-mail was sent in parallel.

5.2 Survey Results

Of all participants, 72.8 % (551) were aware of the phishing simulation. The special simulated phishing e-mail was remembered by 329 participants, and of these, 228 recognized it as phishing, see Figure 4. Furthermore, 81 participants (that is 10.7 % of all 757 who completed the survey) indicated that they clicked. According to the actual measured click rate, 14.6 % clicked (see the blue highlighted area in Figure 3). The discrepancy may be explained by the fact that this is self-reported data and not all employees took part in the survey. More than half of the participants stated that they could not remember the special simulated phishing e-mail or were unsure.

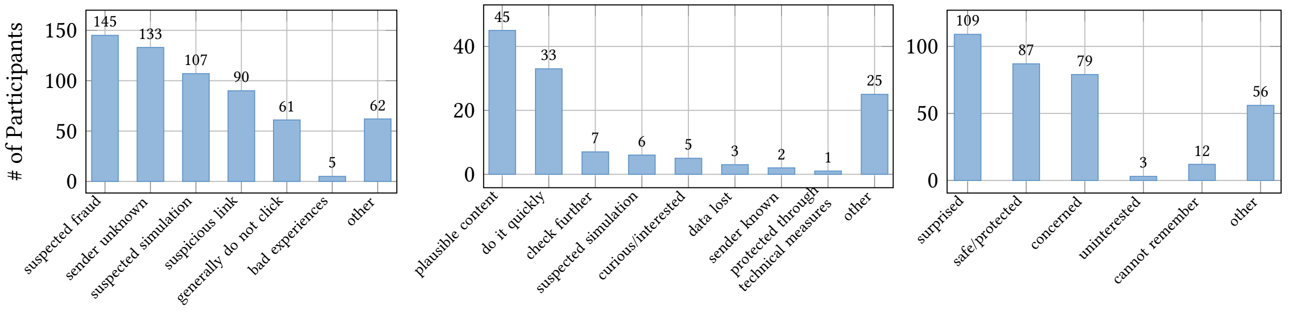
5.2.1 Reasons for clicking or not clicking. In Figure 5, we show the reasons participants stated for clicking or not clicking on the links in the special simulated phishing e-mail. The majority who clicked said that the content seemed plausible or they wanted to handle it quickly. Most participants who entered a free text answer stated that they were stressed, under time pressure, or unconcentrated (13). For eight participants, the context fit included, for example, the current migration processes. Thus, S491 stated:

> "*[...] In the prior days we got e-mails from HR about the changes in the employee evaluation process and [...] currently we are in process of switching to M365, all that together rushed me into just clicking without reading.*"

Two participants stated they clicked out of curiosity to see the underlying learning website.

> **Key Insight 1**: Most participants clicked because the content seemed plausible, or they had a lot to do and wanted to get it done quickly (time scarcity). Thus, plausibility and stress were the prime drivers for clicking on phishing e-mails.

The majority of participants who did not click stated they suspected fraud or the sender was unknown to them. For the "other" option, 46 participants mentioned the [EXTERNAL] marker in connection with a supposedly internal sender as a hint for a suspicious e-mail. We intentionally did not offer the [EXTERNAL] marker as a pre-selected answer to avoid making an answer too easy. Another participant mentioned that the actual HR department sent



(a) The chart shows the reasons why participants did NOT click on the links in the special simulated phishing e-mail (*n* = 238).

(b) The chart shows the reasons why participants clicked on the links in the special simulated phishing e-mail (*n* = 81).

(c) The chart shows how participants felt when they saw a learning website. (*n* = 258).

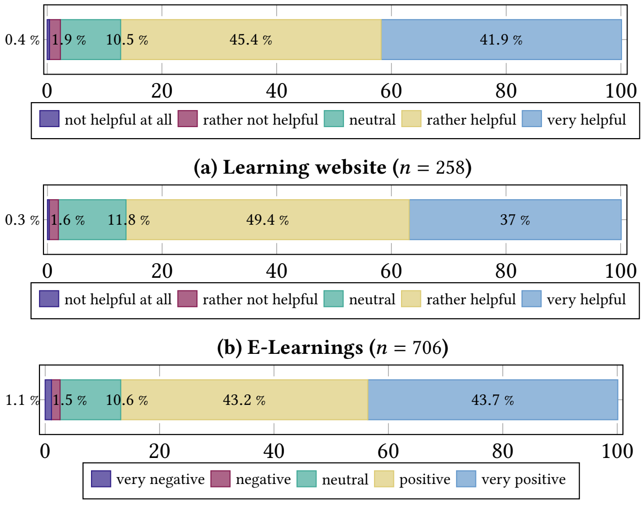
Figure 5: The distribution of reasons for clicking or not clicking and the feeling than someone has fallen for a simulated phishing e-mail. All answers were multiple choice.

a warning that the special simulated phishing e-mail was not real. However, this was only reported by one participant in the survey, and we did not find any further comments on this.

5.2.2 Learning Website. In total, 258 participants (34.1 %) remembered seeing a "learning website" at least once. Figure 5c shows how these participants felt when they saw it. Mostly, the participants chose the pre-selections as *surprised*, *safe/protected*, and *concerned.* For the "Other" field, nine participants entered that they had clicked on purpose or as confirmation. Ten participants felt embarrassed or caught out by the company. On the other hand, eighteen participants stated they were annoyed by themselves or disappointed in themselves for not recognizing a simulated phishing e-mail.

Key Insight 2: The majority of participants felt surprised when they saw the learning website. Others felt safe/protected or concerned.

In Figure 6a, we show how helpul/not helpful the participants rated the learning website. In total, 87.3 % found it rather helpful or very helpful. As a reason, 70 participants said it raised their awareness, refreshed their knowledge, and reminded them to remain vigilant. For example, S357 stated: "*A reminder that I made a mistake which I will not do again.*" Ten participants criticized the learning website because they already knew the content or it did not fit the simulated phishing e-mail. Further, five participants rated it as a confirmation, because they already assumed the phishing e-mail was part of the simulation or clicked out of curiosity.



(a) Learning website (*n* = 258)

(b) E-Learnings (*n* = 706)

(c) General Attitude (*n* = 757)

Figure 6: The charts show the rating of how helpful/not helpful the participant found the learning website and the e-learnings. The last chart shows the general attitude of the participants on a scale from very negative to very positive.

5.2.3 General Rating of the Phishing Simulation. The rating regarding the general attitude can be seen in Figure 6c. The reasons given are divided into 630 positive, 76 negative, and 18 other statements. Most positive statements (335) referred to the fact that the participant's awareness increased or they were reminded of the dangers. For example, S380 said:"*This makes you aware of the issue and you get used to checking e-mails for phishing and reacting accordingly.*" This is followed by 111 statements indicating that participants understand the importance and relevance of the simulation or are aware of the consequences. In 85 statements, participants said that they prefer the phishing simulation over a training course, as it is integrated into their working day and allows them to learn by doing. Furthermore, participants stated that they learned something new or were trained (59), the simulation helped them privately (16), they felt protected (15) and they liked the structure (9).

Key Insight 3: Nearly 87 % of the participants indicated a positive or very positive attitude to the phishing simulation.

Most negative comments were related to the time factor (18), since these participants receive too many simulated phishing e-mails and already feel time pressure in their daily work. S99: "*Sometimes it's a bit too much in daily doing that you also have to deal* *with whether this is another simulated phishing e-mail. Less is sometimes more.*" Ten participants fear negative consequences from the phishing simulation, like general distrust or that employees could intentionally click on phishing e-mails. S444 described the problem as follows: "*At some point, too much simulation is no longer taken seriously. Do you know the story of the shepherd boy and the wolf (false alarm)?*" Eight participants criticized the difficulty level of the phishing simulation. While one participant said that some simulated phishing e-mails were difficult to detect, the others thought the simulated e-mails were too easy and "*obviously fake*" (S42). Another point of criticism is the communication regarding the simulation. Here, participants mentioned that they were inadequately informed about the simulation or felt confused on about how to handle a supposed phishing e-mail. This problem is further described in the interview results in Section 5.3.3. Three participants mentioned that the simulated phishing e-mails increase effort for certain employees or departments, like the IT service or the intentionally incorrectly used sender department. Thirteen participants felt annoyed by the simulated phishing e-mails in their everyday work. Eight participants mentioned feeling confused or tricked through the phishing simulation. However, these comments are not purely negative. For example, it is also mentioned that this was only the first thought, and after reflecting on what happened, the simulation is considered positive.

Key Insight 4: The minority that feel negative towards the phishing simulation, name the already high time pressure as an issue. The negative comments also suggest that participants are not necessarily against or negative about phishing simulation but disfavor confusing, too frequent, or difficult simulations. Some participants who found it negative at first reflected on it later and changed their minds.

5.2.4 E-Learning Rating. In Figure 6b we display the rating of the parallel e-learning program. The majority (86.4 %) found it to be rather helpful or very helpful. Similar to the general attitude, the majority said that awareness increased or they were reminded of the dangers (187 statements). Likewise, 137 statements indicated that e-learning is helpful in gaining new knowledge, and 125 statements compliment the design and structure. Most negative statements say that e-learning covers already familiar knowledge (25) or increases time pressure and stress (20).

5.3 Interview Results

5.3.1 E-Mails and Phishing. Out of 22 participants, 21 described e-mails as their primary communication medium, especially for communication with external contacts. Internally, e-mail is increasingly being replaced by chat, but that depends on the department. When it comes to arrangements that are documented in writing, e-mail is still relevant. P09 explained: "*That's the entire written communication, both internally and externally, to document or describe facts, to agree on procedures, it's simply not possible without e-mail every day.*" Six participants appreciated the asynchronous communication in e-mails, which makes it possible to answer later, does not interrupt the workflow, and makes it easier to communicate with colleagues on other continents.

5.3.2 Significance of the [EXTERNAL] tag. The `[EXTERNAL]` marker is the most frequently mentioned reason for recognizing phishing. Fifteen named it on their own, while six participants were asked about it and then said that they were using it. Employees with few external contacts found the `[EXTERNAL]` marker especially helpful. Due to her position in the company, P20 receives many e-mails from external senders, which makes the `[EXTERNAL]` marker less helpful for her. P20: "*Unfortunately, it is relatively ineffective for me, as I also have a lot to do with external people. [...] no alarm goes off for me that something potentially doesn't affect me.*"

Further, 18 participants named the content or context as a reason. A similar number of participants (17) said they checked the sender. P07 describes this as follows: "*The e-mail address was strange. I was supposed to check some accounts. But I knew I didn't have an account there.*" These statements match the ones from the survey. It seems these "*basic things*" (P20) were already known before the program started. Things that are covered later in the e-learning and are less basic are mentioned by fewer participants, e. g., link checking (8). Participants considered these aspects more interesting and valuable, as we show in Section 5.3.8.

Key Insight 5: The `[EXTERNAL]` marker is perceived as very helpful and is the first clue to recognize phishing.

5.3.3 General Attitude. The interviews revealed a positive general attitude. The main reasons given by the participants were that their awareness increased, that they were continuously trained during their working day, and that they were better able to consolidate what they had learned in the e-learning. The key point of criticism was the level of difficulty, on which the participants had widely varying opinions. The majority (11) stated that they found the e-mail difficulty mainly appropriate, whereas nine participants found the e-mails rather easy. The reason for the low difficulty level was that they were mostly internal concerns sent from external senders.

No one mentioned that the simulation caused insecurity in daily work. P04 and P10 felt tested by the company, but in a positive context, as they were on guard. As P04 explained:

> "*Because if it's done regularly and people are aware of it, then they might be a bit more attentive, because they feel like they're being checked or tested, and they have a little bit in the back of their mind: "Yes, that's definitely one of those test e-mails now." Even though it might not be one, it doesn't matter, they deleted it anyway, which helps.*"

5.3.4 Handling Phishing. Some participants felt uncertain handling (simulated) phishing e-mails. Although the survey and the interviews showed that employees were aware of the phishing simulation and that they should not click on links in phishing e-mails or respond to them, they were unsure what to do if they identified a supposedly malicious e-mail. P08 said:

> "*So you got the e-mail and then yes, what do you do now? Do you go to the hotline, do you report it to your supervisor or even higher, do you have to escalate it to IT security, because this is still something critical? You don't really know if it's a test or if it's a real attack on the company [...]*"

P03 did not want to burden the IT service and was therefore also unsure how to handle the e-mail: "*[...] and then there was the question, what do you do with the phishing e-mail? Send it to [the IT service number], that's our IT hotline. Or is that a burden on them?*" The issue was partially resolved through an e-learning course and a reporting button for suspicious e-mails introduced during the migration to Microsoft 365.

Key Insight 6: Participants did not feel tricked by their company or IT department, but missing information about a reporting channel made them feel uncertain.

5.3.5 Reporting button. Participants who were already familiar with the button rated it positively. Those who were not yet familiar with it also expressed a positive attitude towards this idea. The simplification of the reporting process was especially appreciated, so P20: "*I think anything that makes handling easier, especially if you work with a lot of e-mails a day, every click less counts, [...]. So anything that makes the journey shorter is a good thing.*" Furthermore, P20 liked the direct feedback when reporting simulated phishing. The button takes the burden off the employees and "*[they] still have the feeling that 'Yes, I have reported it.'* " (P04). For P08, the introduction of a reporting button changed the overall perception and evaluation of the phishing simulation from *neutral* in the survey to *positive* in the interview, as it provided them with an official communication channel for suspicious e-mails:

> "*Now it doesn't bother me anymore that I get [simulated phishing] e-mails. So before it was always in the unpleasant situation, yes, and now? [Now you] give it to the phishing department or to the robot and then it will be checked more closely.*"

Only P10 feared causing more damage by forwarding the e-mail using the reporting button to the IT Service: "*For me, it's like this again: when I forward such a phishing e-mail, am I possibly making a mistake and causing damage again?*"

Key Insight 7: The reporting button makes it quick and easy for employees to handle suspicious e-mails. They like the immediate feedback for simulated phishing e-mails.

5.3.6 Risk awareness. The participants are aware of the danger associated with phishing and IT attacks in general. However, this is not exclusively a consequence of the training program. Six participants reported that they had already been directly or indirectly affected by cyber attacks or scam attempts. The associated circumstances led to an increased awareness of the dangers. P10 reports:

> "*Customers of mine, craftsmen, who said: Don't order from the wholesaler at the moment, nothing works there [because of the attack]. You can possibly call, and the colleague in the warehouse can go to the storage compartment with the phone and see: Okay, it's there, we'll write a hand delivery note [...] But it's all very time-consuming and complicated.*"

P13 describes a similar incident: "*Because we've also noticed that our competitors [...] have had a few problems with phishing. That probably shut down the company for three or four months.*"

Besides, participants mentioned the media and current world events as a reason for their awareness, so P16:

> "*[...] because there are more reports in the media about what is happening, with encryption and so on and blackmail attempts. And that's why people are becoming more cautious, but not because of this campaign.*"

We found different perceptions of individual risk. On the one hand, some participants understand the impact an individual employee's behaviour can have on the entire company. P04 said:

> "*I think it's good when I know that everyone else has been made once again aware of it. A bit like road traffic. And I know they all have a [driver's license] test too. [...] Because at the end of the day, it doesn't matter who clicked on the links. If we all get hacked, then we'll have the same problem.*"

In contrast, other participants seemed not to understand the connection between the individual risk and the risk for the company. P10 said: "*And personally, I think I'm too uninteresting for anyone as a small sales employee to get involved with me. For a company [...] it's obviously a huge risk.*" P06 answered the question of whether they feel threatened through phishing as follows: "*I don't have that feeling. Perhaps because people now know about it to a certain degree, I don't feel directly threatened by it.*"

This statement already reveals a false sense of security, as we also found among other participants. The company's measures made them feel protected against actual phishing attacks. P14 explained: "*Well, it just happened on my smartphone while I was on vacation. But I didn't think anything more of it. I said: Hey, we have a good IT department, nothing can happen.*" P16 said: "*I don't feel threatened right now, simply because things are relatively well protected.*"

Key Insight 8: Participants are aware of the dangers of cyber attacks but do not feel personally threatened. At the same time, they experience a false sense of security because they feel protected by the company due to training.

5.3.7 Clicking on Simulated Phishing. Nine participants stated that they remembered clicking on at least one simulated phishing e-mail. The main reasons for clicking were plausible or fitting content or not reading the e-mail and its information (e. g., sender) in detail. For example, it was difficult to identify on a smartphone screen that provided not all information (P14), or they were distracted by other tasks, such as a phone call (P13). Some participants felt pressured by the e-mail content. They already had many other (similar) e-mails in their inbox and wanted to process them quickly.

Similar to Caputo et al. [5], we found that participants who clicked were disappointed in themselves, as in hindsight, it was possible to recognize the e-mails as phishing. The participants emphasized that their anger was not directed against the company. Instead, they felt well prepared due to the company's e-learning and information, which led to even more disappointment in themselves. P11 described:

> "*Yes, because I mean, firstly, the training courses we were given, they were not bad. Secondly, you often could have noticed it. So, yes, I don't know. It's like telling someone an April Fool's joke and then falling for the same one the next year.*"

Participants felt dismayed, especially before they realized that the learning website was part of the company's program. They assumed that their behavior was safe and were frightened to learn otherwise, so P21:

> "*To be honest, I was actually shocked because I've always been very self-critical. Whether it's ordering something on the Internet or something like that, where you first have to check a dozen times whether it's really serious. And that I then simply fell for such an easy e-mail.*"

Although they felt caught at the first moment, it was later seen humorously, as P14 says: "*Okay, then I'll be included in the statistics next time. [laughs].*" Participants also felt relief after they realized that it was not a real phishing e-mail. For example, P01 said that it was a "*load off my mind*".

Key Insight 9: The main reasons for clicking on a link are a plausible or fitting content of the e-mail or inattention, i. e., due to multitasking. Participants felt disappointed in themselves after they fell for the e-mail.

5.3.8 E-Learnings. Generally, the e-learning received positive feedback, which mainly relates to the structure and gamification elements. The short modules allow the employees to finish them, if they have a short gap in their everyday working routine. Therefore, interruptions, such as ringing telephones (P03), are not so bad and do not lead to larger sections needing to be repeated. This also includes the general scope of the e-learning, which 13 participants considered appropriate. P02 said: "*I think it's okay [...] one hour of IT security work per year isn't actually that much. People drink ten times more coffee than that.*"

Two participants said that the audio output from the text on the slides is too long compared to the time one would need to read. P11 said: "*[...] by the time the guy has read down what's written on the slide, you're already done three times.*" The style of the e-learning and the associated interactive gamification elements were rated particularly positively. Compared to other online training courses, the participants described the e-learning as "*less dry*" (P13) and "*diversified*" (P04). P20 explained:"*So just really funny didactic tools that go beyond 'read five pages of PDF and then answer three multiple choice questions'.*"

On the other hand, P21 mentioned that they perceive the e-learnings as too kitschy. Appreciated was content that goes beyond the basics of cyber security or phishing. While participants considered several basics (e. g., lock the screen) as repetitions, they found more advanced content more engaging and gained the most new insights from it. For instance, P03, P13, P17, and P19 stated that they learned to read URLs and identify fraudulent links.

Key Insight 10: The majority of participants like an interactive gamification approach for the e-learning. Topics that go beyond the basics are especially interesting.

5.3.9 Changes in Behavior and Negative Consequences. All but one (P16) said that they either felt more aware (17 participants) and/or that they had adopted new behaviors (12 participants) due to the company's program. P16 mentioned that they "*become more cautious*" not because of the program, but because of the focus on cyber attacks in the media. Some participants seem to have developed new routines for reading an e-mail. This means they also pay attention to aspects besides the content of the e-mail, i. e., tap the sender on their smartphone to see the complete e-mail address. Others say that they are more conscious, or take more time processing e-mails and no longer handle them alongside other tasks.

Half of the participants could remember e-mails they accidentally classified as phishing (false positives) in a work-related or private context. No one experienced any serious negative consequences as a result. Usually, the participants noticed their mistake after they reported the e-mail to the IT department or because the sender or other colleagues involved asked about it. Only P20 suspected the number of false positives had increased due to the company's program. Of the interviewees, 18 participants stated that the program also helped them in their private lives, because they can transfer the new knowledge. P16 said: "*Because privately we don't have such good protection. Nothing is labeled 'External'.*"

Key Insight 11: The behavior of the participants seems to change to a limited extent. Most describe themselves as more vigilant. However, most do not report actual or concrete changes in e-mail processing routines. The negative consequences of false positives are usually contained by the IT department or colleagues.

5.3.10 Learning by Doing. At the end of each interview, we asked the participants to decide between phishing simulation and e-learning. Despite the question, 15 said they liked the mixture and would not want to do without either. P17 explained:

> "*Both actually, because both have their justification. So if I had to choose, well, the phishing simulation is usually useless without prior knowledge, because then it's like being thrown in at the deep end and seeing how you get through. And the other way round, I don't think e-learning is as good in terms of learning content without the subsequent simulations. Therefore, I would say that the two actually work quite well together. To be honest, I wouldn't want to choose one over the other.*"

Eventually, there was a preference for the phishing simulation. Participants mentioned that the phishing simulation is more practical, realistic, and integrated into their workday. While working through the e-learning, participants mentioned that they were already in a state of expectation, but the simulated phishing e-mails still arrived unexpectedly in their inboxes. For these reasons, some participants saw the simulation as more long-lasting. P03 mentioned that "*It's like when a child reaches onto the hot hob*", and P14 says that "*the bang is bigger*" when you have experienced it yourself. P12 (who is an IT manager) states the simulated phishing e-mails are a verification of the knowledge learned from the e-learnings, "*because there is the proof, did I succeed or not. [...] In terms of efficiency, this is the most clever way to build up understanding.*" We note, however, that P12 voiced this generalizing opinion without having deeper insight into what actually happens in the company. Participants P04, P09, P15, and P18 stated that the advantage of e-learning was that more topics were covered than in the phishing simulation.

Key Insight 12: Most participants prefer a mixture of e-learning and phishing simulation. Due to its integration into the workday and continuous nature, the latter is perceived by some participants as a more enduring and effective method.

6 DISCUSSION

6.1 Positive Attitude

Regarding RQ1, our findings show that most employees have a positive attitude toward the phishing simulation conducted by their organization. The main reasons for this are that the participants' awareness has increased and that they are aware of the relevance of the training. They also liked that the training was continuous and integrated into their working day. A clear communication path for reporting of suspicious e-mails is essential for a positive attitude, supporting the assumption by Volkamer et al. [39]. A reporting button for phishing, which also provides immediate feedback on the phishing simulation, is, therefore, especially helpful. However, a lack of clarity about handling (simulated) phishing e-mails can lead to discomfort with the whole phishing simulation.

Negative attitudes stem from a lack of information and time pressure worsened by extra e-mails. In contrast, we could not find evidence that employees felt attacked by their organization as Volkamer et al. [39] indicate. On the contrary, employees support the organization's initiative and activities to protect the entire unit from attacks. Employees have been affected by attacks or have heard about them from colleagues or the media, so they appreciate the measures taken by the organization. Even participants who fell for a simulated phishing e-mail stated they were disappointed with themselves, not with the company.

6.2 False Sense of Security

Concerning RQ2, we found that employees feel more confident in detecting phishing e-mails and feel protected by the organization, as they experience its security measures. Although the participants know the risk, they feel more secure because of the phishing simulation, which can cause a false sense of security. For example, most employees who clicked on a phishing e-mail did not interact with the learning website, as already noticed by Caputo et al. [5]. A false sense of security requires a discrepancy between perceived and objective security. In our case, we observed a consistent decrease in the click-through rate, as seen in Figure 3. However, we cannot say if this was caused by the phishing simulation solely, because the company introduced the reporting button, and the employees had mandatory e-learning courses. When we combine perceived security (feel more secure), present among our respondents, with the objective security from other studies [5, 24] (click-through rate remains the same), we come to the conclusion that it is most likely a false sense of security against phishing.

Additionally, we found, similar to Conway et al. [8], Greene et al. [13], or Williams et al. [43], a false sense of confidence in the company's security measures, as phishing simulation per se does not protect against phishing. Due to the anonymization of the data, we cannot make any statements about all-clickers, as Caputo et al. [5], or repeated clickers, as Canham [4]. However, we can support the claims of other studies [2, 13–15, 44] that the main reason for clicking is suitable content and context. At the same time, the content and context of the e-mail is also the main reason for classifying it as suspicious, depending on the particular circumstances.

6.3 Mix of Phishing Simulation and E-Learnings

What also contributes to the positive attitude regarding the phishing simulation is the combination with the interactive e-learning courses. The e-learning enabled equal start conditions for every employee regardless of their previous knowledge. Only a few participants wanted to choose between the phishing simulation and the e-learning. Instead, the majority preferred the mixture of both. In our case, the fact that the employees felt prepared and were not thrown in at the deep end contributed to the positive attitude. Therefore, regarding RQ3, the participants have a positive attitude toward a parallel security awareness program. Another reason is the e-learning structure, which differs from other courses through interactive gamification and is described as "*less dry*". At the same time, it is positive when training content avoids repetition and offers new insights to experienced participants.

6.4 Marking of External E-Mails

We found that the `[EXTERNAL]` marking is essential for recognizing suspicious e-mails. However, participants who clicked on a simulated phishing e-mail came back later to check if the e-mail was marked as `[EXTERNAL]` and were annoyed with themselves for not noticing it, which means that its helpfulness depends on the state of mind of the recipient. The marking is particularly helpful for employees with limited external contacts.

6.5 Recommendations

Upon reflection of our findings, we have derived the following recommendations for companies that want to conduct phishing simulations and for employees who work in such companies:

For companies:

- Employees like the combination of e-learning and simulation, meaning that it is advisable to run both in parallel.
- Employees want to learn enough in advance to be able to recognize the simulations.
- Communication on how employees should deal with the (simulated) phishing e-mails is important so that they do not feel overburdened.
- A reporting button simplifies the process of handling phishing for employees. However, it leads to increased effort in the IT department; it is unclear whether new staff may be required. The possibility for employees to indicate that they do not need assistance but only report the e-mail, might reduce this effort.
- Phishing simulations might cause a false sense of security or a false sense of confidence, which is why one should not rely exclusively on this method.

- Easy-to-implement security measures, such as the [EXTERNAL] marking, could assist employees in spotting and avoiding phishing e-mails, though they might experience a habituation effect for the [EXTERNAL] tag too.

For employees:

- Employees should not be afraid to use the security measures, such as the reporting button, that the company makes accessible to them.
- The knowledge obtained from simulation and e-learning can also be transferred to private life.
- Employees should be aware that phishing simulations do not imply that the company is more secure.

6.6 Study Limitations

6.6.1 E-Learnings. We accompanied the company in an awareness program, which an external provider provided. The design of the program was not part of our study design. Therefore, we did not influence the design of the e-mail templates or the scheduling of the various elements of the awareness program, such as the sequence of e-learnings.

6.6.2 Selection of E-Mails. The phishing e-mail templates cover a wide range of different phishing techniques, based on the past history of phishing e-mails that the phishing company has witnessed in professional settings similar to ours. Their methodology is also based on *A Phish Scale* by Steves et al. [36]. The selection of those e-mails, which we did not influence, may have yielded different perceptions according to their difficulty and the domain they covered. However, the external company chose a well-balanced mix of different difficulties (according to their experience with other campaigns) over the period of our study. By being passive observers, we provide insights into this common industry practice of fighting against phishing.

6.6.3 Participant and Scope. Concerning the survey, we had low answer rates for employees outside Europe and for those with negative attitudes to phishing simulations. The study's main limitation is the absence of interview participants with a negative attitude. Although a small minority revealed negative attitudes in the survey, we could not explore their reasons further because they either did not leave their e-mail addresses to be interviewed or did not react to an interview invitation. Furthermore, we could only focus on European employees, mainly Germans, and therefore cannot make any statement about cultural differences. Additionally, we conducted our study in just one company. Most of the participants are office workers and spend much of their workday at the computer. It is not clear whether the findings apply to other business sectors.

7 CONCLUSION AND FUTURE WORK

We conducted a survey and interviews to investigate the employees' perception of a phishing simulation. Most participants had a positive attitude regarding it. Furthermore, participants feel more confident in detecting phishing e-mails. We could not find that the phishing simulation leads to distrust or creates a division between employees and management/IT service, who are responsible for the security measures. Yet, a false sense of confidence in the company's security seems to be created. Clear communication about the planned phishing simulation is essential. Otherwise, uncertainty might arise among the employees because they do not know how to handle the simulated phishing e-mails. We found that a reporting button is helpful because it provides a clear communication path for employees. For future work, it would be interesting to see the changes in attitude over a longer time and to connect security feelings with security behavior and the actual security of the company.

ACKNOWLEDGMENTS

This work was partly funded by the European Union under grant number ROF-SG20-3066-3-2-2. We would like to thank Sebastian Pahl for reading the early drafts and helping us analyse the data. Also, we would like to thank Martin Heckel for helping us with the translations.

REFERENCES

[1] Anti-Phishing Working Group (APWG). 2023. *Phishing Activity Trends Report.* Technical Report. Anti Phishing Working Group (APWG). https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf

[2] Zinaida Benenson, Freya Gassmann, and Robert Landwirth. 2017. Unpacking Spear Phishing Susceptibility. In *Financial Cryptography and Data Security.* Springer International Publishing, 610–627. https://doi.org/10.1007/978-3-319-70278-0_39

[3] Lina Brunken, Annalina Buckmann, Jonas Hielscher, and M. Angela Sasse. 2023. ”To Do This Properly, You Need More Resources”: The Hidden Costs of Introducing Simulated Phishing Campaigns. In *32nd USENIX Security Symposium.* Anaheim, CA, 4105–4122.

[4] Matthew Canham. 2023. Repeat Clicking: A Lack of Awareness Is Not the Problem. In *HCI International 2023 – Late Breaking Papers. HCII 2023.* https://doi.org/10.1007/978-3-031-48057-7_20

[5] D. Caputo, S. Pfleeger, J. Freeman, and M. Johnson. 2013-08-23. Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security & Privacy* 12 (2013-08-23), 28–38. https://doi.org/10.1109/MSP.2013.106

[6] A. Carella, Murat Kotsoev, and T. Truta. 2017. Impact of Security Awareness Training on Phishing Click-Through Rates. In *IEEE International Conference on Big Data (Big Data).* IEEE, 4458–4466. https://doi.org/10.1109/BigData.2017.8258485

[7] Xiaowei Chen, Margault Sacré, Gabriele Lenzini, Samuel Greiff, Verena Distler, and Anastasia Sergeeva. 2024. The Effects of Group Discussion and Role-playing Training on Self-efficacy, Support-seeking, and Reporting Phishing Emails: Evidence from a Mixed-design Experiment. (Feb. 2024). https://doi.org/10.1145/3613904.3641943 arXiv:2402.11862 [cs].

[8] Dan Conway, Ronnie Taib, Mitch Harris, Kun Yu, Shlomo Berkovsky, and Fang Chen. 2017. A Qualitative Investigation of Bank Employee Experiences of Information Security and Phishing. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017).* USENIX Association, Santa Clara, CA, 115–129. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/conway

[9] Verena Distler. 2023. The Influence of Context on Response to Spear-Phishing Attacks: an In-Situ Deception Study. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems.* ACM, Hamburg Germany, 1–18. https://doi.org/10.1145/3544548.3581170

[10] Ronald C. Dodge, Curtis Carver, and Aaron J. Ferguson. 2007. Phishing for user security awareness. *Computers & Security* 26, 1 (Feb. 2007), 73–80. https://doi.org/10.1016/j.cose.2006.10.009

[11] European Union Agency for Cybersecurity. 2023. *ENISA Threat Landscape 2023: July 2022 to June 2023.* Technical Report. Publications Office. https://data.europa.eu/doi/10.2824/782573

[12] William J. Gordon, Adam Wright, Ranjit Aiyagari, Leslie Corbo, Robert J. Glynn, Jigar Kadakia, Jack Kufahl, Christina Mazzone, James Noga, Mark Parkulo, Brad Sanford, Paul Scheib, and Adam B. Landman. 2019. Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open* 2, 3 (2019), e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

[13] Kristen Greene, Michelle Steves, Mary Theofanos, and Jennifer Kostick. 2018. User Context: An Explanatory Variable in Phishing Susceptibility. In *Proceedings 2018 Workshop on Usable Security.* Internet Society, San Diego, CA. https://doi.org/10.14722/usec.2018.23016

[14] Frank L. Greitzer, Wanru Li, Kathryn B. Laskey, James Lee, and Justin Purl. 2021. Experimental Investigation of Technical and Human Factors Related to Phishing

Susceptibility. *ACM Transactions on Social Computing* 4, 2 (June 2021), 1–48. https://doi.org/10.1145/3461672

[15] Doron Hillman, Yaniv Harel, and Eran Toch. 2023. Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security* 132 (Sept. 2023), 103364. https://doi.org/10.1016/j.cose.2023.103364

[16] Hang Hu, Peng Peng, and Gang Wang. 2018. Towards Understanding the Adoption of Anti-Spoofing Protocols in Email Systems. In *2018 IEEE Cybersecurity Development (SecDev)* (Cambridge, MA). IEEE, 94–101. https://doi.org/10.1109/SecDev.2018.00020

[17] Nicolas Huaman, Bennet von Skarczinski, Christian Stransky, Dominik Wermke, Yasemin Acar, Arne Dreißigacker, and Sascha Fahl. 2021. A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 1235–1252. https://www.usenix.org/conference/usenixsecurity21/presentation/huaman

[18] K. Jansson and R. V. Solms. 2013. Phishing for Phishing Awareness. *Behaviour & Information Technology* 32, 6 (2013), 584–593. https://doi.org/10.1080/0144929X.2011.632650

[19] knowbe4. [n. d.]. *Security Awareness Training | KnowBe4*. https://www.knowbe4.com/

[20] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. 2009. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 3, 12 pages. https://doi.org/10.1145/1572532.1572536

[21] Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*. Association for Computing Machinery, New York, NY, USA, 905–914. https://doi.org/10.1145/1240624.1240760

[22] P. Kumaraguru, Y. Rhee, Steve Sheng, S. Hasan, A. Acquisti, L. Cranor, and J. Hong. 2007. Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit (eCrime '07)*. https://doi.org/10.1145/1299015.1299022

[23] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason I. Hong. 2010-05. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology* 10 (2010-05), 1–31.

[24] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. 2022. Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. 842–859. https://doi.org/10.1109/SP46214.2022.9833766

[25] Steven McElwee, George Murphy, and Paul Shelton. 2018. Influencing Outcomes and Behaviors in Simulated Phishing Exercises. In *SoutheastCon 2018*. IEEE, St. Petersburg, FL, 1–6. https://doi.org/10.1109/SECON.2018.8479109

[26] Aimee Picchi. 2020. *Tribune workers got an email dangling a bonus — but it was a hoax from their employer - CBS News*. https://www.cbsnews.com/news/tribune-bonus-email-hoax-cybersecurity-test/

[27] Proofpoint. 2020. *Assess - Phishing Simulations, Tests & Training | Proofpoint US*. https://www.proofpoint.com/us/products/security-awareness-training/phishing-simulations

[28] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana von Landesberger, and Melanie Volkamer. 2020. An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, 259–284. https://www.usenix.org/conference/soups2020/presentation/reinheimer

[29] Stefan A. Robila and James W. Ragucci. 2006. Don't be a phish: steps in user education. In *Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education*. ACM, Bologna Italy, 237–241. https://doi.org/10.1145/1140124.1140187

[30] Katharina Schiller, Florian Adamsky, Christian Eichenmüller, Matthias Reimert, and Zinaida Benenson. 2024. Extended Version: Employees' Attitudes towards Phishing Simulations: "It's like when a child reaches onto the hot hob". In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24)*. ACM. https://florian.adamsky.it/research/publications/2024/phishing-simulation-ext.pdf

[31] Jasmin Schwab, Alexander Nußbaum, Anastasia Sergeeva, Florian Alt, and Verena Distler. 2024. What Makes Phishing Simulation Campaigns (Un)Acceptable? A Vignette Experiment on the Acceptance and Manipulation Intention Related to Phishing Simulation Campaigns. 4737715 (Feb. 2024). https://doi.org/10.2139/ssrn.4737715

[32] Terranova Security. 2024. *Phishing Simulation*. https://terranovasecurity.com/phishing-simulation/

[33] Steve Sheng, Bryant Magnien, P. Kumaraguru, A. Acquisti, L. Cranor, J. Hong, and Elizabeth Ferrall-Nunge. 2007. Anti-Phishing Phil: The Design and Evaluation of a Game that Teaches People not to Fall for Phish. In *Proceedings of the 3rd Symposium On Usable Privacy and Security (SOUPS)*. https://doi.org/10.1145/1280680.1280692

[34] Hossein Siadati, Sean Palka, Avi Siegel, and Damon McCoy. 2017. Measuring the Effectiveness of Embedded Phishing Exercises. In *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*. USENIX Association, Vancouver, BC. https://www.usenix.org/conference/cset17/workshop-program/presentation/siadatii

[35] SoSafe. 2022. *Drive secure behavior at scale*. https://sosafe-awareness.com/

[36] Michelle Steves, Kristen Greene, and Mary Theofanos. 2020. Categorizing human phishing difficulty: a Phish Scale. *Journal of Cybersecurity* 6, 1 (09 2020), tyaa009. https://doi.org/10.1093/cybsec/tyaa009

[37] Simon Stockhardt, Benjamin Reinheimer, M. Volkamer, P. Mayer, Alexandra Kunz, P. Rack, and D. Lehmann. 2016. Teaching Phishing-Security: Which Way is Best?. In *Proceedings of the 31st International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2016)*.

[38] Kai Florian Tschakert and Sudsanguan Ngamsuriyaroj. 2019. Effectiveness of and user preferences for security awareness training methodologies. *Heliyon* 5, 6 (June 2019), e02010. https://doi.org/10.1016/j.heliyon.2019.e02010

[39] Melanie Volkamer, Martina Angela Sasse, and Franziska Boehm. 2020. Analysing Simulated Phishing Campaigns for Staff. 312–328. https://doi.org/10.1007/978-3-030-66504-3_19

[40] Rick Wash and Molly M. Cooper. 2018. Who Provides Phishing Training?: Facts, Stories, and People Like Me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal QC Canada, 1–12. https://doi.org/10.1145/3173574.3174066

[41] Patrickson Weanquoi, J. Johnson, and Jinghua Zhang. 2018-12. Using a Game to Improve Phishing Awareness. *Journal of Cybersecurity Education, Research and Practice* 2018, 2 (2018-12). https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss2/2

[42] Zikai Alex Wen, Z. Lin, Rowena Chen, and E. Andersen. 2019-05. What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12. https://doi.org/10.1145/3290605.3300338

[43] Emma J. Williams, Joanne Hinds, and Adam N. Joinson. 2018. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies* 120 (2018), 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

[44] William Yeoh, He Huang, Wang-Sheng Lee, Fadi Al Jafari, and Rachel Mansson. 2022. Simulated Phishing Attack and Embedded Training Campaign. *Journal of Computer Information Systems* 62, 4 (July 2022), 802–821. https://doi.org/10.1080/08874417.2021.1919941

[45] Sijie Zhuo, Robert Biddle, Lucas Betts, Nalin Asanka Gamagedara Arachchilage, Yun Sing Koh, Giovanni Russello, and Danielle Lottridge. 2024. The Impact of Workload on Phishing Susceptibility: An Experiment. In *Symposium on Usable Security and Privacy (USEC)*. https://doi.org/10.14722/usec.2024.23024