Research Paper

Who will take the bait? Using an embedded, experimental study to chart organization-specific phishing risk profiles and the effect of a voluntary microlearning among employees of a Dutch municipality

Remco Spithoven and Anthonie Drent

1Head of Research Group of Public Security at School of Governance, Law & Urban Development, Saxion University of Applied Sciences, Wapenrustlaan 11, 7321 DL Apeldoorn, the Netherlands
2Cyber Security Advisor at the National Cyber Security Centre (NCSC), Ministry of Justice and Security, Turfmarkt 147, 2511 DP The Hague, the Netherlands

∗Corresponding author. Head of Research Group of Public Security, School of Governance, Law & Urban Development, Saxion University of Applied Sciences. Postal adress: Wapenrustlaan 11, 7321 DL Apeldoorn, The Netherlands. E-mail: r.spithoven@saxion.nl

Received 9 December 2023; revised 22 March 2024; accepted 21 May 2024

Abstract

Phishing can lead to data leaks or infiltration of computer networks. Protection against the risks of phishing is particularly important for public organizations such as municipalities, that process a large amount of sensitive personal information and whose operational processes can have major societal impact. This makes phishing a direct threat to operational continuity and the reputation of the organization and raises the question of how public organizations can combat this effectively and which resources they can deploy to mitigate the risks of phishing. In this experiment, two test phishing emails were sent to the total population of one of the 15 largest Dutch municipalities. We performed an embedded experiment, with employees experiencing the risks of phishing first hand with extensive attention for the ethics of this approach. Senior and middle-aged employees clearly run the biggest risk of becoming victims of phishing at this specific organization, but they are not automatically prepared to do an online, educational microlearning on phishing. This is also the case for young staff. Less voluntary education should be aimed at these groups of employees in this organization to make them and the organization, more resilient to the risks of phishing. Also, the microlearning did not have an effect on the results of our participants. We advocate a tailor-made approach of offline training to raise awareness and resilience against phishing among employees of public organizations, municipalities, and organizations in general. Our experimental design can be reused in this direction. We conclude to also look at how never-clickers think and act, with further theoretical substantiation and research into the application of the human-as-solution approach.

Keywords: phishing; cybercrime; public organizations; cyber resilience; awareness; human-as-solution

Introduction

For many years phishing has been top of the list as the most frequently occurring digital crime in organizations [1, 2]. This comes as no real surprise. Cybercriminals often use phishing as a springboard (initial access) to other forms of digital crime, such as hacking, ID fraud, and ransomware [3]. After all, it is easier to infiltrate computer systems by deceiving people than exploiting technical vulnerabilities in the same systems [4–9]. This has made phishing a major problem
worldwide [3]. The Netherlands is no exception with victimization through phishing a frequent occurrence according to recent research by the Central Bureau of Statistics Netherlands [10]: ‘In 2021, more than two out of three (68%) Dutch people aged 15 years or older say they have received at least one phone call, email or other message in the past 12 months that was most likely from a scammer. Two percent said they fell for it. Almost half of these (0.8%, more than 100 thousand people) ended up losing money because of it.’

Phishing is not only a problem for private citizens, but also for organizations [11]. As a result of phishing, companies risk reputational damage, interruption of business continuity, and bankruptcy [12]. Phishing attacks, including clicking on malicious URLs or opening infected attachments, remain a prominent way to access organizations. For example, it is estimated by the cyber security sector that around 40% of the cyber incidents at organizations are preceded by phishing attacks (IBM Security, 2024). Protection against the risks of phishing is particularly important for public organizations that process a large amount of sensitive personal information and whose operational processes can have major societal impact [9, 13]. Phishing can lead to data leaks or infiltration of computer networks. This makes phishing a direct threat to operational continuity in the public sector [9, 14–16], such as municipalities [17].

This raises the question of how public organizations and municipalities can combat this effectively and which resources they can deploy to mitigate the risks of phishing. The main question of our experimental study into organization-specific phishing risk profiles for an anonymous municipality organization in the Netherlands is: ‘Which groups of employees at Municipality X run a high risk of falling victim to phishing based on an embedded experimental design and what is the learning effect of a voluntary e-learning?’. In an attempt to answer this question, we sent two test phishing emails to all employees based on an ethically sound experimental design. Between these two test-attacks, a random group of employees were offered a voluntary, online microlearning on phishing to find out whether staff with a high risk of clicking on fraudulent links and filling in their credentials, would do such a training out of their own initiative.

In this paper, we contribute to the existing literature on strategies to mitigate the risk of phishing in organizations [16, 18, 19] and in municipalities more specifically [17] by providing insight into context factors that may affect phishing vulnerability of employees. We also add to the literature on the effectiveness of trainings on the risk of phishing [20, 21] and the ethics of applying test phishing mails [22]. Last but not least, we contribute to the literature of so called embedded awareness trainings [20, 23, 24] and offer an—ethically substantiated—experimental method, which can be reused to subtract organization-specific phishing risk profiles that may function as a foundation for tailor-made trainings to raise awareness and resilience among employees against phishing attacks [8, 25].

Before discussing the research results, we will first explore what is already known in scientific literature and previous empirical research into phishing. Subsequently, we will look at the research design, outline the research limitations and after examining the results, we will draw conclusions, and give our recommendations for practice and further research.

Theory and previous research on resilience to phishing

We will now first explore what is already known from scientific theory and previous empirical research into resilience to phishing attacks.

What is phishing and how does it work?

Phishing can roughly be defined as: ‘a scalable form of deception using the impersonation of an actor to obtain information from a target’ [5, pp. 25, 3]. Such an attack is usually carried out by email but may be done through offline postal correspondence or for example through text messages. In this paper, we focus on phishing by email. This includes a distinction between a general phishing attack and a spear phishing attack. In a general attack, a message is sent to a large group of receivers in an attempt to get as many people as possible to fall for the message. In a spear phishing attack, a specific message is sent to a specific target or specific target group [26]. According to Steinmetz et al. (2020) [58], a phishing attack tries to engender trust, uses as much inside and publicly available knowledge as possible. Phishing emails are also professionally formatted and spell-checked, deploy well-known brands with almost identical details and exploit recipients’ emotions, perceptions, and flaws. Cybercriminals have an arsenal of psychological tricks available to them from offline experiences with fraud and from the world of marketing. Phishing is a type of crime that does not target technology, but rather the person behind the screen [5, 6, 27].

Human factors in phishing victimization

With limited technological opportunities to detect phishing e-mails [9, 16], one of the key focal points in the research into phishing is to ascertain, which human factors contribute to making one person more susceptible and another not or less susceptible for phishing [28]. We will consecutively discuss what is known about the influence of demography, context factors, personality traits, and digital literacy on susceptibility to phishing and risk profiles.

Demography. Some studies see older people become victims of phishing [10, 17] while others see young people [4, 23, 29, 30] and there are authors who see either slight or no influence of age [6, 8]. The same goes for gender [4, 6, 8, 31, 32]. And this is also the case with educational level [6, 23, 33, 34].

Context factors. In sum, susceptibility to phishing cannot be directly explained in terms of a fixed set of demographic factors, but needs to be primarily examined within specific contexts [35–37]. However, this research is scarce [24, 38]. According to Viswanath et al. [39] and Luo et al. [40], workload also has influence, as those having to process larger numbers of emails appear more susceptible to phishing than those with a lower number of received daily emails [17]. Also, staff who spend a lot of time online [23, 34] run a greater risk of becoming victims of phishing attacks. It appears that people ‘take the bait’ more readily when emails have been sent by a recognizable authority and we are more inclined to act quickly when we experience time constraints [5, 41]. Also, the more experience someone has with particular software or a platform, the more likely they are to spot any abnormalities [35, 42–44].

Personality traits. In addition to demographic and context factors, academics focus on the relationship between victimization and personality traits [45]. It seems that decreased emotional stability, extraversion, and agreeableness increase susceptibility to phishing [7, 29–31, 37, 45–49]. Furthermore, these personality traits are closely linked to levels of self-control, and therefore a greater chance of becoming victims of crimes like phishing [45, 46]. Conversely, conscientious, emotionally stable, and introvert types are better at recognizing phishing [4, 29, 50, 51].

Digital literacy. People who are more familiar with digital devices and internet are more capable of recognizing phishing [52, 53]. How-
ever, it is worth noting that those who spend more time online are also more likely to become phishing victims [25, 34].

Risk profiles. There is a noticeable lack of attention for repeat victimization and the context in which this victimization occurs [38]. Caputo et al. [24] distinguish between ‘never clickers,’ ‘occasional clickers,’ and ‘repeat clickers.’ Canham et al. [38] took this a step further by also including the desired behaviour (stewardship) of reporting phishing in their experiments. Classifying staff in such risk profiles provides an organization with tools for tailor made educational, organizational, or technical measures to fit the vulnerabilities and needs of staff.

Measures against phishing
Technical measures can provide support in organizational resilience against phishing attacks [19]. But it is unrealistic to expect that phishing can be successfully combated solely through education and organizational norms [54]. In any event, it is accepted that a multilayered approach is most promising—this combines technical and organizational measures as well as the training of individual employees [16, 18, 19]. It is generally considered to be worthwhile training individual employees to recognize phishing attacks [2, 8, 20, 21, 55]. Such an awareness training is held to be most effective when employees experience the risks of phishing first-hand—embedded [20, 23–25]. This can be done by testing employees with test phishing emails and subsequently offering them tailored training [8]. Stockhardt et al. [56] found in their study that training given by instructors is most successful in staff recognizing phishing emails. Instructors are better at focusing on the actual situation and work context and this makes the training more interactive [8]. Another condition for effective education is repetition. The positive effects of the training decrease with time, sometimes already after only two weeks [8, 19, 21, 57]. As a result, Jampen et al. [20] propose that phishing education should ideally be repeated four times per year to maintain phishing resilience levels among employees.

Research set-up
Despite the earlier findings that computer-based training courses to raise employee awareness of phishing have repeatedly proven to be rather ineffective [20, 23, 56], we aimed to verify this by making steps towards more complex and expensive, tailor-made training programs [8]. After all, computer-based trainings have the benefit of being flexible in time and are relatively cheap [23]. Additionally, this experiment took place during the Covid-pandemic with almost every employee working from home, making any other types of training rather impossible. In this section, we will deal with the selection of the organization, research questions, methods, ethical considerations, and describe the participants and limitations of our research.

Selection of organization and generalizability
Like Hanus et al. [17] have done in the USA, we have conducted the fieldwork of this study at a municipal organization. We performed our study at one of the 15 largest Dutch municipalities: ‘Municipality X.’ Before our experiment, only a very small part of the employee received prior training on phishing as a part of their onboarding process. Therefore, we hold Municipality X to be representative for Dutch, lager municipalities, public organizations as well as organizations in general with a high risk and high impact of phishing attacks. Especially for these organizations where employees have received little to none training on phishing. But, like these authors outlined before, the results of a study at a single organization should be approached with caution [17].

Research questions
The central question of this research is: ‘Which groups of employees at Municipality X run a high risk of falling victim to phishing based on an embedded experimental design and what is the learning effect of a voluntary e-learning?’ The subquestions are respectively:

1. What are the shared characteristics of Municipality X employees who clicked on the link or entered their credentials in the baseline measurement ( \( T = 1 \) )?
2. What are the shared characteristics of Municipality X employees who clicked on the link or entered their credentials in the second measurement ( \( T = 2 \) )?
3. Which employees at Municipality X appear to belong to the high-risk group of potential phishing victims?
4. What are the shared characteristics of employees at Municipality X have who did a voluntary microlearning on phishing?
5. What is the learning effect of the microlearning on phishing on employees at Municipality X?

Research design
In this research, we have used the design of an experiment [9, 17, 36]: two test phishing emails were sent to the total population of Municipality X. The test phishing emails were based on principles of social engineering described by various authors on phishing [58–60]:

- The baseline measurement email ( \( T = 1 \), Fig. 1) capitalized on the then current theme of working from home during the covid pandemic. The story was that the MS Teams program (probability) needed an update to rid it of a delay (credible story) and that this had to be carried out before the end of the week, otherwise MS Teams would no longer function (urgency). As this mail was sent on a Tuesday afternoon, this baseline measurement included mild time pressure. Furthermore, the account from which the email was sent was from another domain for those who cared to look (typo squatting). The referred link was extremely long and appeared to be an internal link at first glance (name of municipality with some extra characters (e.g. mun[n]icipalityX.com). When the recipients clicked on the link, they arrived in an environment showing an imitation of a Microsoft 365 login screen and they were requested to log in by entering their credentials;
- The second email ( \( T = 2 \), Fig. 2) capitalized on the topical New Year (credible story) and on the incentive that there was still credit available for an end-of-year gift (greed) but this would only be available for a limited period (urgency). The referred link was again extremely long and was external to the organization (offence.com). After clicking on the link—one again a very long link, outside the organization’s own domain—the respondent had to log in using their credentials.

During our experiment, the organization’s email system did not allow people to report these messages as suspicious by simply clicking a button. The procedure was to report suspicious e-mails at the IT Service Desk, which was logged and later pseudonymized for analyses. Unfortunately, this was not done accurately for the second measurement ( \( T = 2 \)) due to communication problems with the IT Service Desk. For both test phishing mails ( \( T = 1 \) and \( T = 2 \)) the variables and potentials scores were:
 Beste medewerker,

Sinds de coronacrisis werken we steeds meer thuis met behulp van MS Teams. Omdat de belasting op onze servers steeds groter wordt, werken we met man en macht eraan om een stabiele omgeving te kunnen garanderen. Het is daarom van belang dat we regelmatig updates uitvoeren zodat we optimaal van Teams gebruik kunnen blijven maken.

Misschien heb je het ook wel gemerkt dat Teams wat minder snel was. Gelukkig hebben de meeste medewerkers de update al uitgevoerd maar uit onze administratie blijkt dat jij de noodzakelijke updates nog niet hebt uitgevoerd. Onze vraag aan jou is of je dat nog voor het einde van deze week wil doen. Doe je dit niet voor het einde voor de week, dan werkt Teams mogelijk niet meer.

Je kunt updates door op onderstaande link in te loggen en dan wordt de update automatisch via Microsoft Teams uitgevoerd:

https://www.xxx.nl/teams-update

Alvast hartelijk dank!

Met vriendelijke groet,

Servicedesk

LET OP: antwoord op deze e-mail zal niet worden verwerkt.

---

**Figure 1.** Test phishing email used at baseline measurement \((T = 1)\).

- **Result:** ‘email not delivered’ (0); ‘successfully delivered’ (1); ‘email link clicked’ (2); and ‘credentials supplied’ (3).
- **Click, time of day:** ‘early in the morning 06–09 h’ (1); ‘late in the morning 09–12 h’ (2); ‘early in the afternoon 12–15 h’ (3); ‘late in the afternoon 15–18 h’ (4); ‘in the evening 18–24 h’ (5); and in ‘the night 00–06 h’ (6).
- **Click, time of day office hours:** ‘during office hours 09–18 h’ (0) and ‘outside office hours 18–09 h’ (1).

For the baseline measurement \((T = 1)\) we have also measured:

- **Report \(T = 1\):** ‘employee did not report e-mail as suspicious’ (0) and ‘employee reported e-mail as suspicious’ (1).

Additionally we have gathered the following data on the employees:

- **Gender:** ‘unknown’ (0); ‘male’ (1); and ‘female’ (2).
- **Age group:** ‘unknown’ (0) and in groups of 10 years starting at ‘10–20 years’ (1) up to ‘70–80 years’ (7).
- **Type of employment contract:** ‘unknown’ (0); ‘parttime’ (1); ‘fulltime’ (2); and ‘otherwise’ (3).
- **Number of years of service:** ‘0–1 year’ (0); ‘2–5 years’ (1); ‘6–10 years’ (2); ‘11–15 years’ (3); and ‘15 + years’ (4).
- **Microlearning:** ‘not invited’ (0); ‘invited’ (1); and ‘completed’ (2).

In the data-sets of both measurements, each participant could be uniquely identified by one’s email address. After combining the participant’s scores on both measurements \((T = 1\) and \(T = 2\)), the background data of participants and the data provided by the IT service desk on reporting the baseline measurement \((T = 1)\) in one file, the data was pseudonymized [17]. The participants’ email addresses were replaced by a respondent number. The combination of this number and the initial email address was not kept due to ethical considerations (see Ethical considerations).

Since all employees of Municipality X received these test phishing mails, there was no control group for the overall design. This is called a one-group–premeasurement–postmeasurement-design [61]. This part of the research design answers the first three subquestions of the research. Part of our design was another experiment. Between the two test phishing emails \((T = 1\) and \(T = 2\)), a random sample of personnel received an invitation to take a voluntary online microlearning. In this instance there is a control group. The group that accepted the invitation and took part in the online microlearning is the experimental group and the group that received the invitation but decided not to take the online microlearning is the control group. We call this a premeasurement–postmeasurement–control-group-design [61]. This part of the research design answers subquestions four and five.

To exclude historical influence, the other employees who were not invited to take part in an online microlearning, were not included in the analysis of this second experiment (ibidem). The effect of the voluntary microlearning was assessed by comparing scores on the baseline \((T = 1)\) and second measurement \((T = 2)\). The latter took place a month after the online microlearning closed, due to earlier insights of the effects of education on phishing decreasing with time [8, 21, 57].

**Ethical considerations**

As Resnik and Finn [22] pointed out, phishing experiments raise significant ethical concerns, because (i) participants will be part of our
experiment without their consent and (ii) the experiment itself will contain deception. Using deception in experiments is highly controversial in academic research, because it (i) violates the good standard of informed consent, (ii) might damage trust in research, and (iii) it can cause temporary minimal harm in the form of anger and frustration to a small percentage of our participants. Resnik and Finn [22] explained that realistic phishing experiments cannot be done with the consent of participants, because asking for their consent would compromise the very validity of the experiment: it would raise their awareness to the risk of phishing and thereby lead to unrealistic results.

The authors therefore concluded that researchers must make an effort to limit the negative impact of the experiment with effective debriefing [9]. Effective debriefings explain to participants how deception was used, why this was necessary, and what can be learned from this experience. Such debriefing hold the potential to turn the experience of deception into a long-term, positive effect by the personal experience of susceptibility. Crucial for the reception of this debriefing is that it must not come out of the blue to its participants. So, the debriefing on the phishing experiment must always be preceded by a general message that cybersecurity research will be done at the organization, in order to prevent the debriefing to arrive unexpected. Also, potential participants must have the opportunity to opt out.

We have applied Resnik and Finn’s ethical guidelines [22] in our phishing experiment in the following ways. First of all, we have proactively evaluated the potential impact of our experiment on the participants and discussed them in depth with the board, works council and ethical advisor of Municipality X and our strategy to counter negative effects and they approved our strategy, as did the Ethical Research Committee of the University of Applied Sciences involved. Second, we have announced that test phishing emails would be send to all employees two weeks in advance on the general intranet environment of the organization. Employees were informed by this message and were given the opportunity to contact the research team by two e-mail addresses: one of the general IT department and one of a specific e-mail address. In both waves of the test phishing emails, no employee has contacted the IT-department or the research team to opt out.

We have also made sure that effective debriefing was given to all participants by a general e-mail to all employees of the organization after every test phishing wave in our experiment. This message contained how deception was used on our participants, how they can notice these realistic tactics in the future, and the meta data of the experiments were shared. We again added both email addressed to contact the researchers to this e-mail, which was used by one respondent who expressed some frustration. The research team contacted this respondent by telephone. This person’s frustration actually had more to do with not getting the New Years present \( (T = 2) \), than it had to do with our use of deception in general. The person understood our approach after our explanation.

In addition to this digital and quantitative debriefing, we have also included a qualitative debriefing after the first wave of test phishing emails by both an offline and online meeting for employees who were interested in the results. All four debriefing meetings had \(~30\) visitors. The research team had visited two teams after the second
wave of test phishing emails: the team that performed best and the team that performed worst on the tests. The first team was given a cake, a trophy, and public praise on the general intranet environment of the organization. The second team was given a positively framed training on how they can recognize phishing emails in the future and what to do when in doubt or after finding out that you have fallen victim of phishing. Of course the identity of the second team is kept confident to date. Also, we have only used aggregated data in all our debriefings. Our research design including our ethical considerations are reflected in Fig. 3.

Participants
Our measurements led to a total of 1660 employees who participated in the study. Unfortunately, we had to delete some cases, as 133 respondent who received the second measurement \((T = 2)\) on 17 March 2022 were not employed by Municipality X at the time of the baseline measurement \((T = 1)\). For another 90 cases, it was unclear why the baseline measurement test phishing mail \((T = 1)\) was not delivered on 26 October 2021. We had to perform listwise deletion to these cases, because our research questions mainly compare the scores for the baseline \((T = 1)\) and second measurement \((T = 2)\). This makes a total population of 1437 participants to our experiment. The characteristics of the total group of participants are outlined in the first column of Table 1.

In total, a random sample of 332 employees of Municipality X (20% of the total population) received an invitation to take part in an online microlearning on phishing. Of these, 92 employees (27.7%) took part in the microlearning (experimental group) and 240 employees (72.3%) ignored the microlearning invitation (control group). The characteristics of these two groups are outlined in the second and third columns in Table 1. The other 1105 employees who did not receive the invitation for the microlearning were not included in the analysis for subquestions 4 and 5, as previously indicated.

Limitations
Just like all research, this study is also subject to limitations. First, for subquestions 1–3, the effect of the experimental treatment (repeated measurement) cannot be fully explained. A possible difference may occur between the baseline \((T = 1)\) and second measurement \((T = 2)\) as a result of the maturing of participants (i.e. they have become better at recognizing phishing attacks) or history (they have heard about large-scale phishing attacks in the news or an acquaintance has recently become a victim of phishing) [61]. Also, the difference between the experimental and control group in subquestions 4 and 5 could be explained by the Hawthorne effect (the experimental group got more attention), the appeal of the microlearning and the guiding influence of the baseline measurement \((T = 1)\), which in any case made participants more aware of phishing (ibidem).

Due to the intake of a relatively large number of new personnel between measurements as well as unknown causes, it is impossible to record the risk profile for a portion of employees \((n = 113)\) as they only participated in one measurement. In addition, due to regard for privacy, only a limited number of background characteristics were included, namely gender, age group, years of service at the organization, and contract type. As a result we can only make more general statements regarding risk profiles relating to potential victimization by phishing. Last but not least, the experimental group was very limited, containing only 5.5% of employees \((n = 92)\), as a result of self-selection through the offer of an online microlearning on phishing, and also had a rather skewed demographic distribution as described earlier. It would have been better to invite the total population or subpopulation that clicked on the link or filled in credentials at the baseline measurement \((T = 1)\) to take part in the microlearning.

Unfortunately, we only have accurate measurements on the reporting behaviour of our participants to the baseline measurement \((T = 1)\) and had to drop results to the second measurement \((T = 2)\), so we could not analyse the effect of the experiment or treatment to reporting behaviour of the employees. Additionally, we have not discussed with the participants to inquire whether and why they did or did not click on the links in the e-mails as we only analysed pseudonymized data for ethical concerns. Also, we did not log whether or not e-mails were opened by the receivers due to both ethical and technical concerns, although 108 employees who received the baseline measurement email did report the email to the IT Service Desk. For these participants we are sure that they have opened and read the email, but unfortunately were not sure for all our participants. Last but not least, we emphasize that this study at a single organization should be complemented with data from similar and other organizations [17].

Results
Between 26 October 2021 \((T = 1)\) and 17 March 2022 \((T = 2)\), two test phishing mails were send to all employees of Municipality X. Between these dates, a randomly selected group of employees received an offer to do an online microlearning about phishing. We will initially explore the results of the baseline \((T = 1)\) and second measurements \((T = 2)\) and subsequently look at which groups are most at risk of becoming phishing victims. Afterwards
we will weigh up the risks of offering voluntary education about phishing to staff and explore the learning effects of the microlearning. We will start with the results of the baseline measurement ($T = 1$).

**Results of the baseline measurement ($T = 1$)**

The baseline measurement e-mail (Fig. 1) was received by 1437 accounts in the organization on 26 October 2021. A total of 64.4% ($n = 926$) of the recipients did not click on the link. A total of 7.4% ($n = 105$) solely clicked on the link and 28.3% ($n = 406$) also entered their credentials. Clicking on the link as well as entering credentials mainly occurred early in the morning between 06:00 and 09:00 (44%, $n = 225$), followed by early afternoon between 12:00 and 15:00 (29.2%, $n = 149$) and late morning between 09:00 and 12:00 (14.1%, $n = 72$). Numbers were negligible at other times of the day. In slightly more than half of cases (50.1%, $n = 245$) this occurred during office hours (between 09:00 and 18:00) with the remainder (49.9%, $n = 244$) outside office hours.

When we look at the characteristics of recipients in the baseline measurement who clicked on the link in the message and/or filled in credentials, the following picture emerges:

- No significant differences were found in the reaction to the baseline measurement regarding gender ($X^2 = 5.073$, d.f. = $4 < X^2_{critical} = 9.488$).
- The differences found were significant among age groups ($X^2 = 49.056$, d.f. = $14 > X^2_{critical} = 23.685$) and it was clear that particularly in the age groups 40–50, 50–60, and 60–70 more than average had clicked on the link and filled in their credentials.
- There were also significant differences found relating to the number of years of service ($X^2 = 30.775$, d.f. = $8 > X^2_{critical} = 15.507$) and it was noticeable that recipients employed at the organization for 2–5 years clicked on the link more than average; recipients who worked at the organization for 11–15 years and recipients who had worked at the organization for more than 15 years clicked on the link more than average and in addition filled in their credentials more than average.
- The different types of employment contract also turned out to be significant ($X^2 = 18.639$, d.f. = $6 > X^2_{critical} = 12.592$), it was mainly full-timers who clicked on the link more than average, whereas part-timers filled in their credentials more than average.

The baseline test-phishing e-mail was reported as suspicious at the IT Service Desk by 11.8% of the employees ($n = 169$), while 88.2% of the employees ($n = 1268$) did not. Analysis shows mainly employees who had clicked on the link and got a message that they clicked on a test-phishing link (27.6%, $n = 29$) reported the baseline measurement e-mail as suspicious to the IT Service Desk. A relatively smaller proportion of the employees who reported the e-mail (11.7%, $n = 108$) simply recognized it as phishing after successful delivery of the email (Table 2):

| Table 2. Combination of results from the baseline ($T = 1$) and reporting behaviour. |
|----------------------------------------|-----------------|-----------------|
| Did not report baseline e-mail to IT service desk | Did report baseline e-mail to IT service desk |
| Successfully delivered                | 88.3% ($n = 818$) | 11.7% ($n = 108$) |
| E-mail link clicked                    | 72.4% ($n = 76$)   | 27.6% ($n = 29$)  |
| Credentials supplied                  | 92.1% ($n = 374$)  | 7.9% ($n = 32$)   |
Table 3. Combination of results from the baseline (T = 1) and second measurements (T = 2).

<table>
<thead>
<tr>
<th>Category</th>
<th>N</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never clickers—low risk: did not click and did not enter any credentials in T1 or T2</td>
<td>815</td>
<td>56.7</td>
</tr>
<tr>
<td>Occasional clickers—average risk: clicked once or filled in credentials in T1 or T2</td>
<td>435</td>
<td>30.3</td>
</tr>
<tr>
<td>Repeat clickers—high risk: clicked twice or filled in credentials in both T1 and T2</td>
<td>187</td>
<td>13</td>
</tr>
</tbody>
</table>

$d.f. = 3 < X^2_{critical} = 7.815$, or types of employments contract $(X^2 = 6.317, d.f. = 4 < X^2_{critical} = 9.488)$.

Results of the second measurement (T = 2)

On 17 March 2022 (T = 2), a second test phishing email (Fig. 2) was send to all employees. This measurement was received by 1437 accounts in the organization. Of these, 63.8% ($n = 917$) of recipients did not click on the link nor fill in credentials. A total of 15.5% ($n = 223$) solely clicked on the link and 20.7% ($n = 297$) also entered their credentials. Once again clicking on the link and entering credentials again primarily occurred early in the morning between 06:00 and 09:00 (59.2%, $n = 308$), followed by later in the morning between 09:00 and 12:00 (26.3%, $n = 137$) followed by in the early afternoon between 12:00 and 15:00 (9.2%, $n = 48$). Nearly two out of five cases (39.2%, $n = 204$) where the link was clicked or credentials were filled in occurred during office hours (between 09:00 and 18:00); in three out of five cases (60.8%, $n = 316$) this happened outside office hours (between 18:00 and 9:00).

When we look at the characteristics of recipients who clicked on the link in the message and/or filled in credentials, then the following picture emerges:

- No significant differences were found in the reaction to the second measurement regarding gender ($X^2 = 1.484, d.f. = 4 < X^2_{critical} = 9.488$).
- There were also no significant differences found regarding age group in the second measurement ($X^2 = 20.568, d.f. = 14 < X^2_{critical} = 23.685$).
- There were no significant differences found in the number of service years ($X^2 = 14.516, d.f. = 8 < X^2_{critical} = 15.507$).
- The difference in contract type proved significant in the second measurement ($X^2 = 21.946, d.f. = 6 > X^2_{critical} = 12.592$) and in particular full-timers had clicked on the link and filled in their credentials more than average.
- No significant differences were found in the reaction to the second measurement regarding reporting behaviour to the baseline measurement (T = 1) ($X^2 = 4.037, d.f. = 2 < X^2_{critical} = 5.991$).

Risk profiles: potential repeat phishing victims

When we combine the results of the baseline (T = 1) and second measurements (T = 2), then the following picture emerges (Table 3).

It is clear that more than half of staff (56.7%, $n = 815$) who received both test messages run a low risk of becoming phishing victims. It can be said that for nearly a third (30.3%, $n = 435$) there is an average risk and for more than 1 in 10 (13%, $n = 187$) there is a high risk, as they, in both cases clicked on the link or filled in credentials. When we look at the characteristics of recipients running a high risk of victimization, then the following picture emerges:

- No significant differences were found regarding gender ($X^2 = 8.613, d.f. = 4 < X^2_{critical} = 9.488$).
- The found differences in age groups are significant ($X^2 = 23.826, d.f. = 14 > X^2_{critical} = 23.685$) and in particular the age groups 40–50, 50–60, and 70–80 run a high risk of becoming victims of phishing.
- Also the differences in contract type are significant ($X^2 = 29.165, d.f. = 6 > X^2_{critical} = 12.592$) with in particular full-time employees running a high risk of becoming victims of phishing.
- The differences in the number service years are not significant ($X^2 = 7.739, d.f. = 8 < X^2_{critical} = 15.507$).
- No significant differences were found regarding reporting behaviour to the baseline measurement (T = 1) ($X^2 = 3.427, d.f. = 2 < X^2_{critical} = 5.991$).

Self-selection through the interim offer of an online microlearning on phishing

Between the two measurements a randomly selected portion of employees, namely 332 staff members (20%) received an invitation for a microlearning on phishing. Ultimately only 94 of the 332 employees (28.3%) who received an invitation for the microlearning actually completed it. Therefore, 240 selected employees (72.3%) chose not to do the 4-min online microlearning. This is an interesting finding in its own right, as apparently such an invitation to do an online microlearning on phishing can only count on a very low level of willingness among staff.

When we look at the characteristics of staff who completed this microlearning, the following picture emerges:

- There are no significant differences found regarding gender ($X^2 = 5.697, d.f. = 4 < X^2_{critical} = 9.488$).
- Differences relating to age groups were found to be significant ($X^2 = 37.314, d.f. = 14 > X^2_{critical} = 23.685$). It was notably employees in age categories 50–60 and 60–70 who in particular and above average did the microlearning.
- Differences relating to the number of service years were also found to be significant ($X^2 = 74.914, d.f. = 8 > X^2_{critical} = 15.507$) and most noticeable was that it was particularly longer-serving staff (11–15 years and over 15 years) who above average, did the microlearning, whereas it was short-term staff (up to 5 years in service) who were above average in ignoring the microlearning invitation;
- Differences relating to contract type were not found to be significant ($X^2 = 12.272, d.f. = 6 < X^2_{critical} = 12.592$).
- There are no significant differences found regarding reporting behaviour to the baseline measurement (T = 1) ($X^2 = 2.731, d.f. = 2 < X^2_{critical} = 5.991$).

If we subsequently look at whether self-selection has taken place within the previously found risk profiles, then the following picture emerges (Table 4).

The differences found are significant ($X^2 = 9.855, d.f. = 4 > X^2_{critical} = 9.488$). The microlearning was mainly taken by employees with an average or high risk of becoming phishing victims. Despite this, staff with a high risk of becoming phishing victims were more often less likely (13.4%) than likely (8%) to do the online microlearning they were offered. So it seems that—in any case for this organization—it is wise to provide such online training courses solely on a voluntary basis.
Learning effect of online microlearning
Table 5 contrasts the results of these groups in the second measurement with their results in the baseline measurement in order to gauge the learning effect of the microlearning. The differences between the baseline and second measurement proved not to be significant ($X^2 = 3.980$, d.f. = 4 < $X^2_{critical} = 9.488$) for the experimental group. This was also the case for the control group ($X^2 = 5.122$, d.f. = 4 < $X^2_{critical} = 9.488$). This means no significant differences were found in the response to the test phishing emails in both the baseline and second measurements between the experimental and control groups, regarding the extent to which links were clicked and credentials filled in. Unfortunately, this means that there is no significant visible learning effect of the online microlearning done by the experimental group.

Conclusions, discussion, recommendations, and suggestions for further research
In this section, we evaluate our findings and by answering our subquestions we will be able to answer our main question. Subsequently, we will look at our results in a broader theoretical and empirical context. After that we will make several recommendations for strengthening employee resilience to phishing and suggestions for further research.

Conclusions
The first subquestion was: ‘What are the shared characteristics of employees at Municipality X who clicked on the link or entered their credentials in the baseline measurement ($T = 1$)?’ This was mainly done by full-time staff aged 40 and older. This occurred most early in the morning between 06:00 and 09:00 but overall predominantly in office hours. Full-timers with 2–5 years of service and 11–15 years of service or more were most likely to click on the link and part-timers who had been at the organization for more than 15 years, were most likely to fill in their credentials. Slightly more than 1 out of 10 employees reported the baseline phishing e-mail to the IT Service desk but these were mainly employees who had clicked on the link and got a message that they clicked on a test-phishing link. This picture largely corresponds with that of the employees who clicked on the link and filled in their credentials in the second measurement. The answer to the second subquestion: ‘What are the shared characteristics of Municipality X employees who clicked on the link or entered their credentials in the second measurement ($T = 2$)?’ is that it was again mainly full-timers, only this time mainly outside office hours, early in the morning before 09:00.

The third subquestion: ‘Which employees at organization X run a high risk of becoming a victim of phishing?’ helps us zoom in on the high-risk category, or rather the repeat clickers. These are employees who divulged their credentials in both measurements. These were primarily full-time staff aged between 40 and 50, 50 and 60, and 70 and 80 of age. The fourth subquestion: ‘What are the shared characteristics of employees who volunteered to do a microlearning on phishing?’ looks at whether self-selection took place regarding being offered a microlearning on phishing. This was definitely the case, as the microlearning was mainly taken by employees with an average or high risk of becoming a victim of phishing. However, more of the high-risk category of the previous subquestion chose not to do the microlearning than to do it. Younger employees and those only employed at the organization for a short time more frequently ignored the microlearning invitation.

For the fifth and final subquestion—‘What is the learning effect of the microlearning on phishing on employees at Municipality X?’—the results of the second measurement compared the group of employees who did the microlearning (experimental group) with the group of employees who ignored the invitation (control group). There was unfortunately no significant learning effect visible as a result of the online microlearning done by the experimental group. This brings us to the central question of this research: ‘Which groups of employees at Municipality X run a high risk of falling victim to phishing and are they prepared to do a voluntary online phishing awareness microlearning when offered and what is the learning effect of this education?’ It is clear that senior and middle-aged employees run the biggest risk of becoming victims of phishing in this Dutch municipality, but they are not automatically prepared to do an educational microlearning on phishing. This is also the case for young staff who have only been employed for a short time. Less voluntary education should be aimed at these specific groups to make them and therefore the organization, more resilient to the risks of phishing. Also, the online microlearning proved to have no significant learning effect.

Discussion and suggestions for further research
Contrary to for instance Sheng et al. [56], we did not encounter any effect of gender on phishing susceptibility. Most participants who either clicked on the links or provided their credentials were aged 40 and older. This aligns with the findings of Hanus et al. [17] as well as the Central Bureau of Statistics Netherlands [10], but might well be a function of lesser amounts of computer self-efficacy, web experience and security knowledge [23] and digital literacy [32, 33] among these employees. We also found that younger participants with 2–5 years of service were more at risk of phishing victimization. This aligns with earlier findings of other authors [4, 29, 30, 55] but contradicts the findings of Hanus et al. [17] at an American municipal organization. For both the baseline and second measurement, most clicks and filled in credentials happened early in the morning between 06:00 and 09:00. This might be an indication of a relation that other authors [7, 18] found between e-mailing habits and phishing susceptibility as well as an indication of a high e-mail load [39].

It is highly questionable whether a voluntarily, computer-based training of employees can be expected to have an optimum effect [20].

Table 4. Analysis of self-selection and risk profiles.

<table>
<thead>
<tr>
<th></th>
<th>Invitation microlearning received</th>
<th>Invitation microlearning received, but ignored</th>
<th>Invitation microlearning received and followed up</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Never clickers</strong>—low risk: did not click and did not enter any credentials in T1 or T2</td>
<td>78.8% ($n = 642$)</td>
<td>16.2% ($n = 132$)</td>
<td>5% ($n = 41$)</td>
</tr>
<tr>
<td><strong>Occasional clickers</strong>—average risk: clicked once or filled in credentials in T1 or T2</td>
<td>72.6% ($n = 316$)</td>
<td>19.1% ($n = 83$)</td>
<td>8.3% ($n = 36$)</td>
</tr>
<tr>
<td><strong>Repeat clickers</strong>—high risk: clicked twice or filled in credentials in both T1 and T2</td>
<td>78.6% ($n = 147$)</td>
<td>13.4% ($n = 25$)</td>
<td>8% ($n = 15$)</td>
</tr>
</tbody>
</table>
Table 5. Analysis of the learning effect of the microlearning.

<table>
<thead>
<tr>
<th>Results baseline measurement (T = 1)</th>
<th>Results second measurement (T = 2)</th>
<th>Results second measurement (T = 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email ignored</td>
<td>Clicked on link</td>
<td>Filled in credentials</td>
</tr>
<tr>
<td>Email ignored</td>
<td>Clicked on link</td>
<td>Filled in credentials</td>
</tr>
<tr>
<td>Email ignored</td>
<td>Clicked on link</td>
<td>Filled in credentials</td>
</tr>
<tr>
<td>Email ignored</td>
<td>Clicked on link</td>
<td>Filled in credentials</td>
</tr>
</tbody>
</table>

We see possibilities for future research to not only incorporate test-phishing e-mails into an experiment to reveal organization specific risk profiles as we have done in this study, but make this design part of a holistic research approach combining the methods of experiments, questionnaires, and embedded training [18, 35, 62, 63]. In this approach, personal, organizational, and personality factors can be studied in cohesion with a focus on e.g. personality factors [63] and formal and collectively shared injunctive norms [62]. We also see good possibilities for incorporating games [23] as means to teach employees how to safeguard themselves and their organization against phishing, but stress the importance of (at least initial) instructor based training [56].

Nearly 80% of the never clickers in Municipality X had in no way whatsoever taken head of the online microlearning on phishing. Therefore, we conclude that a significant part is going well in the workplace of this organization. When we research the risk of phishing in specific contexts and this is more common, this needs to be given the acknowledgement it deserves in both a practical and scientific sense. An alternative can be found in the ‘human-as-solution’ approach of Zimmermann and Renaud [64]. Here, the problem is not sought in human behaviour but rather more in the complexity and opacity of the socio-technical environment where people work. We align ourselves with this approach—as a consequence of insights gained—where testing employees by deploying test phishing emails is just one part of a broader, more positive treatment of personnel as part of the solution [12]. We also think that the ethics of phishing experiments [22] might further benefit from such a positive treatment of personnel in the future. Clearly, this positive approach needs more attention in future research into the resilience of organizations and employees to the risk of phishing.

Practical recommendations

Computer-based training courses to raise employee awareness of phishing have repeatedly proven to be rather ineffective [56]. Live in-person instructors are better at focusing on the actual situation and the work context [35] and that makes the training more interactive [8]. A multilayered approach—combining the training of individual employees with technical and organizational measures—seems to be most promising [18, 19]. We advocate to use test phishing emails in this context to compile organization-specific risk profiles, which can then subsequently be used to develop tailored awareness-training courses. We advise to only use test phishing emails as part of a broader, positive approach of employees, where the test phishing mails are primarily used for learning purposes and their potential contribution to protect the organization against phishing attacks [12, 64]. But repeating education on phishing is still crucial for all staff as knowledge and experience gained doesn’t stick easily [8, 19–21, 57].

Our advice to other municipalities, public organizations, and fellow researchers is to repeat our experimental set up at multiple organizations and do more research into repeat clickers and the context factors that play a role in their potential repeated victimization by phishing [24, 35, 36, 38]. Given results of an earlier empirical studies and indications in our own results we recommend to pay special attention to staff who experience a high work load, a higher number of emails that need to be processed, and time pressure causing people to deal more quickly with reacting to emails [5, 17, 39–41]. We emphasize that more data from similar and other organizations would strengthen the approach for embedded, experimental studies to chart organization-specific phishing risk profiles [17]. However, we advise not to only to research how personnel in organizations are vulnerable to phishing emails but rather also look at how never clickers think and act by observing behaviour in realistic scenarios (e.g. in a lab-setting). In addition, it is certainly worthwhile recommending further theoretical substantiation and research into the application of the human-as-solution [64] approach to cyber resilience in organizations.

Author contributions

Remco Spithoven (Conceptualization [equal], Formal analysis [equal], Investigation [equal], Methodology [equal], Resources [equal], Supervision [equal], Visualization [equal], Writing – original draft [equal], Writing – review & editing [equal], and Anthonic Drenth (Conceptualization [equal], Data curation [equal], Formal analysis [equal], Investigation [equal], Methodology [equal], Project administration [equal], Resources [equal], Visualization [equal], Writing – original draft [equal], Writing – review & editing [equal])

Conflict of interest: None declared.

Funding

None declared.

References


