Falling and failing (to learn): Evidence from a Nation-Wide Cybersecurity Field Experiment with SMEs*

David Gonzalez-Jimenez[a], Francesco Capozza[b], Thomas Dirkmaat[c], Amber van Druten[c], Evelien van de Veer[c], and Aurélien Baillon[d]

[a]Erasmus University Rotterdam
[b]WZB and Berlin School of Economics
[d]Emlyon business school
[c]Ministry of Economic Affairs of the Netherlands

September 25, 2024

Abstract

Prior experiences are crucial in shaping risk prevention behavior. Previous studies have shown that experiencing a simulated phishing attack (a "phishing drill") reduces the likelihood of clicking on unsafe links and disclosing one's password. In a large field experiment involving 670 small and medium-sized enterprises (SMEs) and their 33,000 employees, we examined the impact of experience on individuals' ability to detect cyber-security threats, and whether this effect persisted over several months. We collected data at both the company and individual levels, including risk preference, time preference, and trust. Our findings indicate only a non-systematic, short-term effect of previous phishing emails on clicking behavior. A cluster of individuals with greater patience, trust, and risk seeking was the most likely to benefit from phishing drills.

keywords: Field experiment; replication; phishing drill; prevention; patience; risk attitude.
JEL codes: C93, D83.

*The authors report no conflict of interest.

1 Introduction

Due to the dramatic shift in the economic activities performed online in the last 20 years (Goldfarb and Que, 2023), privacy concerns have been rising (Acquisti et al., 2016). In particular, the uncertainty of the consequences of privacy-related behavior and the malleability of privacy concerns make it extremely difficult for individuals to adopt strategies to minimize privacy risks (Acquisti et al., 2015, 2020). This trend has marked a growing concern about the risks associated with online crime (Moore et al., 2009). For example, the rise of remote and hybrid work has resulted in a significant increase in the number of phishing attacks and their financial impact. According to the 2021 Ponemon Cost of Phishing Study, large organizations now incur an average annual cost of over $1,500 per employee, due to these attacks (Ponemon, 2021). Malware and credential attacks, business email compromise (BEC), and ransomware are the main contributors to this growing threat.

Phishing drills, also known as phishing simulations, are a popular cybersecurity tool used by companies to test their employees' vulnerability to deceptive emails that mimic the characteristics of real phishing attacks. In these drills, employees who click on links or download web content are alerted that they fell for a phishing simulation and receive training on how to identify and avoid real phishing attacks. Phishing drills offer two main advantages: first, they allow companies to track employees' clicking behavior to identify and address vulnerabilities. Second, they provide training as no technical solution can accurately detect every malicious email an individual receives. For instance, Baillon et al. (2019) found in a large field experiment that a phishing drill was at least as effective as an information campaign. Phishing drills seemed to provide a promising approach to increase cybersecurity.

The purpose of the paper is two-fold. First, we attempt to replicate the effect that phishing drills reduce employees' propensity to fall into a phishing attack. We do so in a large field experiment, involving 33,016 employees from 667 small and medium enterprises (SMEs) across different sectors in the Netherlands. Our conceptual replication further studies whether the effect of phishing drills exists after a longer period. This first purpose contributes to the growing debate on the necessity to fight the file-drawer problem biasing scientific publishing (Brodeur et al., 2020) and on the sometimes disappointing results of systematic replication studies (Benjamin et al., 2018). Fortunately, replication studies are becoming popular (e.g. Ankel-Peters et al., 2023). They are even more crucial for studies whose results are used daily by companies, such as studies claiming the effectiveness of phishing drills.

Second, in an exploratory approach,[1] we study whether company and employee characteristics are associated with the effectiveness of phishing drills. In our experiment, we collected company information and also ran surveys among employees. The surveys included behavioral questions that are popular in economic experiments and measure risk preferences, patience, and general trust (Dohmen et al., 2011; Falk et al., 2018). These additional data allow us to explore possible determinants of the effectiveness of phishing drills (or the lack thereof).

The experimental setup is as follows. Every employee of the 667 SMEs received two phishing emails, but not all at the same time. We could thus compare whether having received a first phishing email (say, email A) decreased the propensity to click on the second (say, email B) compared to those for whom email B was the first email they received. We found that sending a first phishing email (the phishing drill) reduced the propensity to click on the link provided in the second phishing email, but not systematically and only in the short term, which was around one month. Such reduction in propensity was not associated with SME characteristics, such as sector or owning their IT processes by having an in-house IT department, which did relate to the propensity to click on the link in the first email. Instead, we found evidence that the reduction was related to the preferences measured, in particular risk and patience. Overall, the results nuance the promise of phishing drills as an effective method cybersecurity. The effect may neither be systematic nor

[1] We call this part exploratory because the experiment was not pre-registered and, unlike, the main treatments, this part of the research is based on surveys that do not limit much researcher degrees of freedom.

long-lasting.

1.1 Related literature

Security is not just a technical issue solvable by engineering solutions; it also encompasses significant behavioral aspects that must be considered and addressed (Asghari et al., 2016). A widespread literature has developed on the behavioral aspects of cyber-security, and of phishing susceptibility especially.

Many studies have focused on factors that drive victimization, such as demographic or personality variables (e.g. Curtis et al., 2018; Halevi et al., 2015; Hong et al., 2013; Lawson et al., 2020). In a meta-study of 45 papers, Sommestad and Karlzén, 2019 found that personality traits have no, or at best weak, correlation with susceptibility to phishing. For example, it remains uncertain whether individuals who are generally trusting are more prone to falling for phishing emails.

The meta-study of Sommestad and Karlzén, 2019 does find that training and technical system warnings tend to be effective prevention methods. However, they did not review the impact of phishing drills. A reason is that phishing drill research has been mostly used to study contextual factors such as email complexity or persuasiveness on susceptibility to phishing (Burda et al., 2020; Goel et al., 2017; Harrison et al., 2016; Jalali et al., 2020; Wright et al., 2014). These studies do not provide insights into behavior changes following experience with a phishing drill or their persistence over time.

More recent literature has begun to explore the potential training benefits of phishing drills in the field and on a large scale. In a convenience sample of six healthcare institutions, Gordon et al. (2019) found a positive correlation between exposure to multiple phishing drills and a decrease in clicking rates on phishing emails. In a field experiment conducted on a single governmental institution, Baillon et al. (2019) administered different email training schemes in phishing detection and found that those schemes that included a previous phishing drill were more effective in reducing clicking rates on subsequent phishing emails than those that only provided information. However, as the sample in these studies was either limited in size or homogeneous among economic sectors, questions remain about the effectiveness of phishing drills across different economic sectors and enterprises with fewer IT resources, which are primary targets for cyber-attacks (Ministerie van Justitie en Veiligheid, 2022).

One may worry whether phishing drills, even if effective in the short term, are also effective in a longer term. For instance, Epperson and Gerster, 2021 show that exposing individuals to information about living conditions of animals in intensive farming impacted their consumption behavior, but only temporarily. This may be explained by positive false memory, which may enhance confidence in one's future self but prevent full learning from experience (Chew et al., 2020). Unlike previous studies of phishing drills, we vary the duration between a phishing drill and the email used to measure its effectiveness.

Clicking or not on an email can also be seen as a decision under risk involving one's privacy. Hence, we complement the evidence that studies how people evaluate their privacy (Acquisti et al., 2013; Winegar and Sunstein, 2019), make information-sharing decisions (Schudy and Utikal, 2017), and insure their personal information (Biener et al., 2020). Assessing the rationality of privacy preferences has provided mixed evidence (Lee and Weber, 2019; Tomaino et al., 2023).

Finally, by documenting the relatively short-lived effect of feedback about cyber-secure behavior, we contribute to the more general literature studying feedback on different economic behaviors such as fuel management among bus drivers (Romensen and Soetevent, 2021), exam performances (Tran and Zeckhauser, 2012), disaster experience on willingness to get insured (Cai and Song, 2017), traumas on the willingness to purchase health insurance (Shai, 2022), savings (Avdeenko et al., 2019), and feedback on the usage of blood on blood donation (Goette and Tripodi, 2020).

The paper is structured as follows. Section 2 describes the experimental design. Section 2.5 illustrates the identification strategy. Section 3 describes the results of the phishing drills. Finally, Section 4 concludes.

2 Methods

2.1 Participants

We performed a field experiment to identify the effect of being exposed to a phishing e-mail on subsequent cyber-secure behaviors. The research was organized by the Dutch Ministry of Economic Affairs and Climate Policy, where three authors of this paper work. Companies were recruited by campaigns and letters with an invitation to join the study. A partner organization (Regionaal Platform Criminaliteitsbeheersing Noord-Holland, RPC NH) was in charge of the recruitment and a private cyber-security company was in charge of the technical aspects, i.e. sending phishing emails, tracking participant clicking behavior, and collecting survey data. They provided us with the anonymized data. An internal ethical assessment was conducted by the Ministry.[2]

Dutch SMEs were first informed about the phishing test through newsletters from various industry organization and business associations, and the phishing test was promoted at events organized by RPC NH. Because the response to this was insufficient, 14.000 invitation letters were sent to the companies with information about the phishing test. Companies could register their interest to join the test on the RPC NH website. A total of 1.200 companies did so in 2020 and early 2021. They were asked to finalize their participation in the project, giving consent by signing a service and data processing agreement and providing company characteristics (described below). Companies with a minimum of 8 and a maximum of 250 employees with a business email address could participate. Companies with fewer than 8 employees

[2] The research was under the responsibility of the Dutch Ministry for Economic Affairs and Climate Policy and we followed the applicable procedure there, which differs from the procedure in academia because of the absence of an ethical committee. The three authors of this paper in charge of the study at the Ministry filled out a form, covering the purpose of the research, (public) interests, the positive and negative effects of the research on the different stakeholders, and the trade-off between the ethical dilemmas. The form was then discussed with an ethics expert within the Ministry and it was concluded that there was no ethical concerns preventing the research from being conducted. The three authors from academia consulted with the data privacy officer of their institution at the time (Erasmus University Rotterdam) to ensure that the data treatment was in line with the applicable European regulation.

could not participate because the privacy of employees could not be guaranteed. Ultimately, 667 companies participated in the experiment, for a total of 33,016 employees. The distribution of the economic sectors represented in the experiment is shown in Figure 1.

Each enterprise had an internal contact person who gave a list of employees' email addresses who would participate in the phishing drills as well as provided information about the firms' characteristics. The list of the questions asked to each firm's contact person is available in Appendix A.1.[3]

We created a set of variables from the survey and the firms' characteristics. *Num email* is a proxy for the SME size as it gives the number of Email addresses participating in the experiment divided by 10.[4] Sector dummy variables indicate whether the enterprise is from ICT, Industry, Services, Trade, and retail, or another sector. As the study was conducted in 2021, the dummy variable *Covid pressure* refers to the contact person saying they are very busy or busy due to pandemic pressure and *Post covid – office rate* describes the proportion of people working in the office. *Internet dependency* indicates the company reported they were "very dependent" or "dependent" on the Internet; *Full (partial) cloud* means full (partial) dependency on the cloud to store their data. We also coded whether they had any policy regulating Internet access (*Has internet policy*), whether they have an internal IT department that develops and implements most of IT policies (*Internal IT*) or partly outsource some functions (*Partially outsourced IT*), and whether they do daily backups of their data (*Daily backup*). Out of the 667 companies, 626 had complete data. Appendix D describes the proportion of missing values per variable per group.

In total 33,016 employees participated in the two phishing drills across all the companies. The employees were neither warned in advance about the phishing drills nor did they know about their participation in the phishing

[3] A second company-level survey was sent after the experiment to collect feedback about the experiment. For completeness, questions asked in this survey can be found in Appendix A.2. We do not use the second survey in this paper as it is unrelated to our research questions but it was used by the Ministry for its report on the study.

[4] The division by 10 makes coefficients better readable in the regressions analysis below.

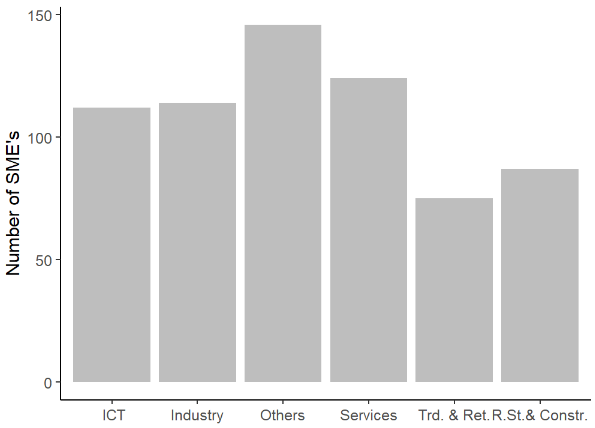


Figure 1: Sectorial composition of the Sample of SMEs

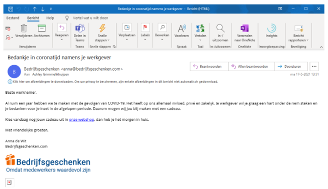
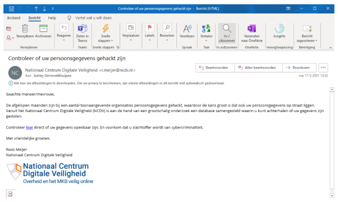
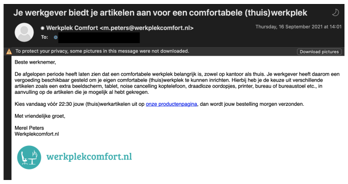
drills. To preserve the participants' personal information, the cyber-security company performed the data collection.

2.2 Experimental treatments

Each firm was randomly assigned to one of four treatment groups, where we varied the time frame between the two phishing drills and the content of the email sent to the employees of that specific SME. Three types of phishing emails were used in the experiment. We identify them as Phishing email *A*, *B*, and *C*. The screenshots of the emails are available in Table 1. The messages invited employees to click on a link to receive some benefit such as choosing a gift from a webshop (Email A)[5], checking whether their data were not leaked (Email B), or getting free home-office supplies to work from home from the employer (Email C). The experimental design had legal and logistical constraints. For example, we were not allowed to use logos or names of real companies in the phishing emails (unlike what cyber-criminals do), and every treatment group had to receive two emails. Another practical constraint was to design emails that were general enough and believable for the employees across the SMEs.

[5] It is a common practice of Dutch employers, especially after the Covid pandemic to thank the employees.

Table 1: Emails with Translations

Name	Screenshot	Translation
Email A	 Bedankje in coronatijd namens je werkgever - Bericht (HTML) Bestand Bericht Help Vertel wat u wilt doen Verwijderen Archiveren Reageren Delen in Teams Snelle stappen Verplaatsen Labels Bewerken Voorlezen Vertalen In-/uitzoomen Verzenden naar OneNote Insights Bericht rapporteren Beantwoorden Allen beantwoorden DoorsturenBedankje in coronatijd namens je werkgever Bedrijfsgeschenken <anna@bedrijfsgeschenken.com> Aan Ashley Grimmelikhuijsen ma 17-5-2021 13:51 Klik hier om afbeeldingen te downloaden. Om uw privacy te beschermen, zijn enkele afbeeldingen in dit bericht niet automatisch gedownload. Beste werknemer, Al ruim een jaar hebben we te maken met de gevolgen van COVID-19. Het heeft op ons allemaal invloed, privé en zakelijk. Je werkgever wil je graag een hart onder de riem steken en je bedanken voor je inzet in de afgelopen periode. Daarom mogen wij jou blij maken met een cadeau. Kies vandaag nog jouw cadeau uit in onze webshop, dan heb je het morgen in huis. Met vriendelijke groeten, Anna de Wit Bedrijfsgeschenken.com Bedrijfsgeschenken Omdat medewerkers waardevol zijn	Dear employee, We have been dealing with the consequences of COVID-19 for more than a year. It affects all of us, privately and professionally. Your employer would like to encourage you and thank you for your efforts in the past period. That is why we can make you happy with a gift. Choose your gift today in our webshop, and you will receive it tomorrow. Best regards, Anna de Witt Bedrijfsgeschenken.com
Email B	 Controleer of uw persoonsgegevens gehackt zijn - Bericht (HTML) Bestand Bericht Help Vertel wat u wilt doen Verwijderen Archiveren Reageren Delen in Teams Snelle stappen Verplaatsen Labels Bewerken Voorlezen Vertalen In-/uitzoomen Verzenden naar OneNote Insights Bericht rapporteren Beantwoorden Allen beantwoorden DoorsturenControleer of uw persoonsgegevens gehackt zijn Nationaal Centrum Digitale Veiligheid <r.meijer@ncdv.nl> Aan Ashley Grimmelikhuijsen ma 17-5-2021 13:52 Klik hier om afbeeldingen te downloaden. Om uw privacy te beschermen, zijn enkele afbeeldingen in dit bericht niet automatisch gedownload. Geachte meneer/mevrouw, De afgelopen maanden zijn bij een aantal toonaangevende organisaties persoonsgegevens gehackt, waardoor de kans groot is dat ook uw persoonsgegevens op straat liggen. Vanuit het Nationaal Centrum Digitale Veiligheid (NCDV) is aan de hand van een grootschalig onderzoek een database samengesteld waarin u kunt achterhalen of uw gegevens zijn gestolen. Controleer hier direct of uw gegevens openbaar zijn. En voorkom dat u slachtoffer wordt van cybercriminaliteit. Met vriendelijke groeten, Roos Meijer Nationaal Centrum Digitale Veiligheid Nationaal Centrum Digitale Veiligheid Overheid en het MKB veilig online	Dear Sir/Madam, In recent months, personal data has been hacked at a number of leading organizations, so there is a good chance that your personal data is also on the street. Based on a large-scale investigation, the National Centre for Digital Security (NCDV) has compiled a database in which you can find out whether your data has been stolen. Check here directly whether your data is public. And avoid becoming a victim of cybercrime. Best regards, Rose Meijer National Center for Digital Security
Email C	 Je werkgever biedt je artikelen aan voor een comfortabele (thuis)werkplek Werkplek Comfort <m.peters@werkplekcomfort.nl> Thursday, 16 September 2021 at 14:01 To: [redacted] To protect your privacy, some pictures in this message were not downloaded. Beste werknemer, De afgelopen periode heeft laten zien dat een comfortabele werkplek belangrijk is, zowel op kantoor als thuis. Je werkgever heeft daarom een vergoeding beschikbaar gesteld om je eigen comfortabele (thuis)werkplek te kunnen inrichten. Hierbij heb je de keuze uit verschillende artikelen zoals een extra beeldscherm, tablet, noise cancelling koptelefoon, draadloze oordopjes, printer, bureau of bureaustoel etc., in aanvulling op de artikelen die je mogelijk al hebt gekregen. Kies vandaag vóór 22:30 jouw (thuis)werkartikelen uit op onze productenpagina, dan wordt jouw bestelling morgen verzonden. Met vriendelijke groet, Merel Peters Werkplekcomfort.nl werkplekcomfort.nl	Dear employee, The past period has shown that a comfortable workplace is important, both at the office and at home. Therefore, your employer has made an allowance available to help you set up your own comfortable (home) office. You can choose from various items such as an extra monitor, tablet, noise canceling headphones, wireless earbuds, printer, desk or office chair, etc., in addition to the items you may have already received. Choose your (home) office items on our products page before 10:30 PM today, and your order will be shipped tomorrow. Yours sincerely, Merel Peters Werkplekcomfort.nl

We implemented four treatments consisting of different combinations of pairs of emails sent, time-lapse between emails, and order of emails. There were four dates in which emails were sent t_i, $i \in \{1,2,3,4\}$, the time lapse between t_1 to t_2, t_2 to t_3, and t_3 to t_4 were 35, 77 and 28 days respectively.[6] Firms were divided into four groups that were named according to the order of the emails sent *A-B*, *B-C*, *C-B*, and *long A-B*. Once the employee clicked on the link of the email, they would be redirected to a page with information

[6] Mails in t_1 where sent on the 27th of May, t_2 was the 1st of July, t_3 the 16th of September and t_4 the 14th of October

about the telltale signs of a phishing email, and their clicking behavior was recorded by the cyber-security firm. The screenshots of the feedback pages can be found in Appendix B.

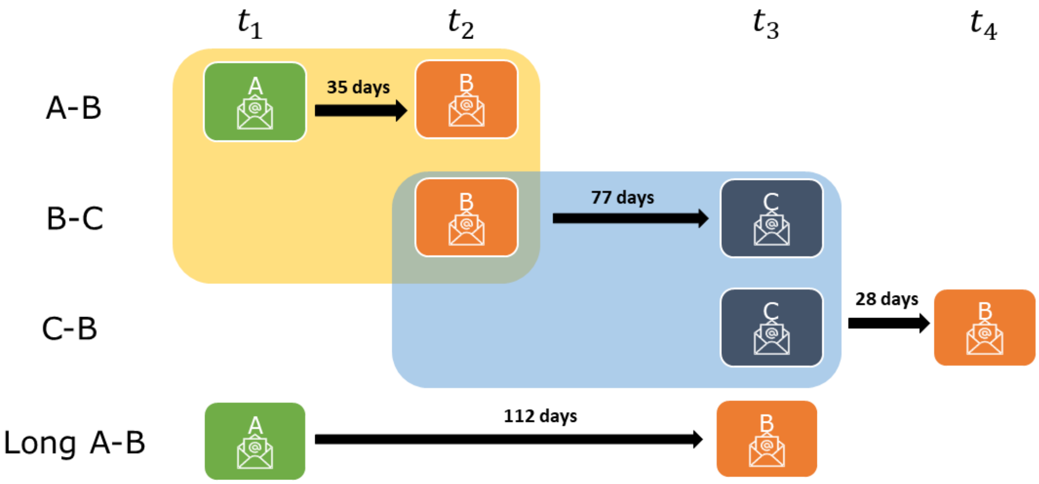


Figure 2: Scheme of dispatch of Phishing E-mails by group and type of E-mail

The dispatch of emails was staggered, meaning that not all treatment groups received their first phishing email at the same time as shown in Figure 2. A phishing email nature and timing can influence people's propensity to fall for it. Hence, to isolate the effect of experience, we should compare individuals who received an email as their second one with those who received the same email on the same date but as their first. We are able to isolate the effect of experience for two groups: for group *A-B* first, we can compare the clicking rate on the second email with that of group *B-C* because they both received *email B* at t_2; second, we can compare group *B-C* and group *C-B* as they both received *email C* at t_3.

Two other groups, *long A-B* and *C-B* do not have a clear control to compare their second email clicking rate with, because no group received email B as the first email at t_3 or t_4. Ideally, *long A-B* should have received email C as their second email at time t_3, such that it could be compared with email C of the group *C-B*. However, a technical difficulty prevented us from doing so. To ensure phishing emails would go through firewalls, a technical contact person of each participating firm was notified of the domain from which emails would be sent, to whitelist this domain. The technical contact people of group *long A-B* received details referring to Email B instead of C. It could not be changed without risking confusion and annoyance. In the analysis, we will still compare the clicking rate of *long A-B* and *C-B* with the typical clicking rate on Email B. However, the result is only a proxy, in that it does not isolate the effect of experience from a possible timing effect.

2.3 Randomization

Every SME was assigned to one treatment group using block randomization by sector of the economic activity, size, and whether or not they (partially) outsourced their IT security. Table 2 shows the number of firms and employees in each treatment group. [7]

	A-B	B-C	C-B	Long A-B
Number of companies	168.00	166.00	167.00	166.00
Num. Email by company				
Mean	49.05	49.23	48.28	51.44
SD	52.46	50.15	52.42	58.94
Sector				
ICT	29.00	26.00	29.00	28.00
Industry	27.00	30.00	28.00	29.00
Services	31.00	29.00	33.00	31.00
Trade and retail	18.00	18.00	19.00	20.00
Constr. and Real Estate	24.00	21.00	22.00	20.00
Other	37.00	38.00	36.00	35.00
Number of employees	8241.00	8173.00	8063.00	8539.00

Table 2: Distribution of companies and employees

[7] A fifth group, including companies interested in the study but with more than 300 employees or less than 3 and therefore excluded from the study, was used for technical tests.

Table 2 shows that the number of companies and the overall number of employees are balanced across the four experimental conditions. Table 3 summarizes the characteristics of the firms across experimental conditions in terms of dummy variables and tests for differences. Table 13 in Appendix E reports tests for differences in terms of *Post covid – office rate* and *Num email.* The randomization of the firms across the different experimental conditions seems successful.

Table 3: Fisher's test on SME survey variables

Name	Value	Freq.A-B	Freq.B-C	Freq.C-B	Freq.Long A-B	p-value
Internal IT	No	122	126	126	124	0.94
	Yes	42	37	39	40	
Partially outsorced IT	No	112	107	112	110	0.96
	Yes	52	56	53	54	
Internet Dependency	No	14	14	13	15	0.98
	Yes	150	146	153	148	
Full Cloud	No	95	84	95	81	0.37
	Yes	70	79	70	81	
Partial Cloud	No	95	84	95	81	0.08
	Yes	70	79	70	81	
Internet Policy	No	65	59	67	63	0.85
	Yes	100	104	97	100	
Daily data backup	No	15	17	21	16	0.73
	Yes	153	149	146	150	
Covid rel. Pressure	No	104	98	109	97	0.61
	Yes	56	56	54	65	

2.4 Individual-level preference data

One week after receiving each phishing email, an email was sent to all employees participating in the phishing drill. This email was sent by the cybersecurity company to inform them that a phishing drill had taken place, to explain its objective, and to invite them to answer the survey. The survey elicited the employees' personal demographic data, as well as perceived digital knowledge, past experiences with phishing emails, and the number of phishing emails they had received in the previous 12 months. Finally, we elicited individual employees' risk preferences, patience, and trust. These variables are *Risk seeking*, *Patience*, and *Trust*, coded from 0 to 1, with 0 indicating low risk-seeking, patience, and trust respectively. In this paper, we focus on the risk preference, time preference, and trust measures (Falk et al., 2018; Falk et al., 2016). There is evidence of a negative relationship between risk-seeking (Chen et al., 2017), trust (Arduin, 2023), and the ability to detect internet scams. Patience is measured because the literature focusing on personality characteristics has found an effect of lack of self-control in phishing detection activities (Vishwanath et al., 2018). To measure these preferences we used the survey-based components of risk preferences, patience, and trust from the preference survey module from Falk et al. (2016). The complete set of questions asked to the employees is available in Appendix A.3.[8]

The surveys administered to the employees were answered by a total of 8978 employees after the first phishing email, while 7659 employees answered the survey after the second phishing email. Combining the two statistics, 4728 answered the survey on both occasions. Table 4 provides a more detailed breakdown of survey completion by group.

Table 4: Survey Answers by Group

A-B	First	1870
A-B	Second	1847
B-C	First	2641
B-C	Second	2317
C-B	First	2330
C-B	Second	1611
Long A-B	First	2137
Long A-B	Second	1884

Filling in the end-line survey was completely voluntary. This potentially introduces self-selection in the completion of the survey. To maximize the completion rate of the survey, we collected two measurements of the preferences as we sent the same survey after each phishing email. Given that both surveys

[8] The preference module is the only part of the survey added by the academic part of the team. To limit researcher degree of freedom, we do not include the rest of the survey in the main analysis. An analysis concerning age and gender is provided in Appendix G at a reviewer's request.

were post-treatment measurements, either one of the measurements should be equally useful for our purposes. Hence, the choice of variables was guided by reducing the possible self-selection bias introduced to the analysis.

We considered the following four options: the first option was to use the survey measurement corresponding to the email studied (*Corresp*), another was to create a measure using the average for those who answered both surveys and any answer available for those who did not (*Average*). The remaining option was to use exclusively one of the survey measurements either of the first or the second survey measurement for both groups, irrespective of the email we studied. For each option, we tested if the mean was equal for groups that received the same phishing email on the same day. The results of t-tests (clustered at the SME level) are displayed in Tables 5 and 6 with *Corresp, First, Second*, or *Average* indicating the four options under consideration.

Table 5: Comparison of means for preference measures of groups *A*-*B* and *B*-*C*

Measure	Mean A-B	Mean B-C	t-test	p-value
Patience - Corresp	0.55	0.54	-0.67	0.50
Patience - First	0.55	0.54	-1.49	0.14
Patience - Second	0.55	0.54	-0.46	0.65
Patience - Average	0.55	0.54	-1.23	0.22
Risk taking - Corresp	0.45	0.42	-2.22	0.03
Risk taking - First	0.46	0.42	-3.83	0.00
Risk taking - Second	0.45	0.45	0.06	0.95
Risk taking - Average	0.45	0.43	-2.08	0.04
Trust - Corresp	0.44	0.43	-0.57	0.57
Trust - First	0.44	0.43	-1.06	0.29
Trust - Second	0.44	0.45	1.37	0.17
Trust - Average	0.44	0.44	0.12	0.91

Second is the only measurement such that all the differences between the three preference constructs are not significant. We use it in the remainder of the paper. It also has the advantage of keeping the intensity of the intervention constant (everyone has received two phishing email at that stage) when preferences are measured.

Table 6: Comparison of means for preference measures of groups *B-C* and *C-B*

Measure	Mean B-C	Mean C-B	t-test	p-value
Patience - Corresp	0.54	0.54	-0.33	0.74
Patience - First	0.54	0.54	-0.10	0.92
Patience - Second	0.54	0.54	-0.50	0.62
Patience - Average	0.54	0.53	-0.62	0.54
Risk taking - Corresp	0.45	0.44	-0.42	0.67
Risk taking - First	0.42	0.44	1.82	0.07
Risk taking - Second	0.45	0.45	-0.16	0.87
Risk taking - Average	0.43	0.44	0.82	0.41
Trust - Corresp	0.45	0.45	-0.51	0.61
Trust - First	0.43	0.45	1.64	0.10
Trust - Second	0.45	0.45	0.03	0.98
Trust - Average	0.44	0.45	0.87	0.39

As a quality check, we can compare the trust measure to that obtained by Falk et al. (2018) in a representative sample of the Dutch population.[9] In 2012, they obtained a mean trust score[10] of 0.621 with a standard deviation of 0.22. Individuals in our sample have lower trust scores than in the 2012 representative sample, with an average of 0.45, although all our measurements still fall between one standard deviation from the mean.

2.5 Analysis

We will first focus on the effect of a phishing-drill experience on employees' clicking behavior. Hence, we need to estimate the propensity to click on each email that was sent and the effect that having received a previous phishing email has on said propensity.

We estimate the propensity to click with a linear probability model, with standard errors clustered at the SME level, i.e. at the randomization level. The dependent variable is the binary variable $Click_j \in \{0, 1\}$, with 1 meaning

[9] It is only possible to compare trust because the raw risk and patience of Falk et al. (2018) are not available.

[10] when recoded between 0 and 1, as we did for our variables.

the employee clicked on the link. The main explanatory variables describe which email the potential click refers to (dummy variables *EmailA*, *EmailB*, and *EmailC*) and which email (if any) they have experienced before. Variable *Experience_A* is a dummy variable that takes value 1 if the click concerns the second email of group *A*-*B*, hence indicating that the employee had experienced Email A. Similarly, variable *Experience_B* takes value 1 for the second email of group *B*-*C*, *Proxy_LT_Exp_A* for that of group *long A*-*B*, and *Proxy_Exp_C* for that of group *C*-*B*. If it is a participant's first email, all four experience variables are 0.

$$\begin{aligned} Click_j = \beta_1 Experience\_A_j + \beta_2 Experience\_B_j + \\ \beta_3 Proxy\_LT\_Exp\_A_j + \beta_4 Proxy\_Exp\_C_j + \\ \beta_5 Email\_A_j + \beta_6 Email\_B_j + \beta_7 Email\_C_j + \epsilon_j \end{aligned} \quad (1)$$

In this regression, β_6 captures the clicking rate of group *B*-*C* for the first email. For group *A*-*B*, the propensity to click will be β_5 for the link in the first email (main effect of Email A) and the sum of β_1 and β_6 for the link in the second email (sum of the effect of Email B and having experienced Email A). Hence β_1 isolate the effect of having experienced Email A. It is equivalent to directly comparing the clicking rate on Email B in t_2 between group *A*-*B* and *B*-*C*. Our approach, however, allows us to implement all the comparisons at once, and to then add firm and individual characteristics. Equation 1 is the basic regression we use. In all other specifications, we add company-level or individual-level variables, and in some cases, their interactions.

3 Results

3.1 Descriptives

The clicking rate, without discriminating by the different groups, is 23.5% for all first emails, while 17.8% for all second emails. This suggests that the second

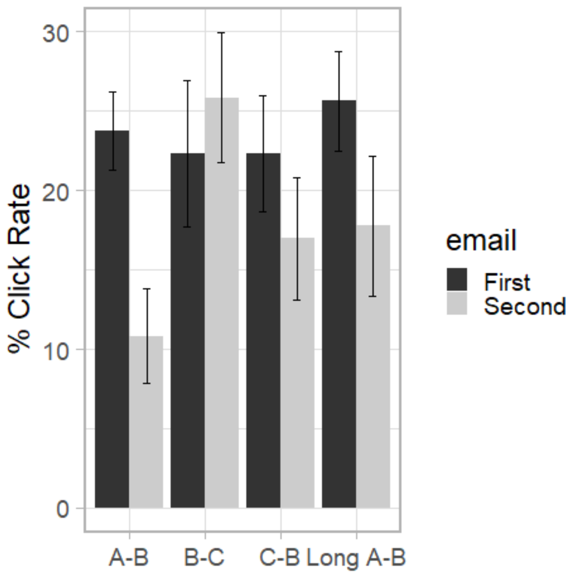


Figure 3: Click rate in percentage discriminated by group

emails were less clicked than the first emails. Zooming into the clicking rates by the different groups as seen in Figure 3 reveals large heterogeneity. The group *A*-*B* had the largest decrease from 23.7% to 10.8%, while the clicking rate of the group *B*-*C* increased from 22.3% to 25.3%.

3.2 Company-level analysis

We now turn to the regression analysis to assess the effect of the different treatments on clicking behavior. Table 7 shows the estimation of two linear probability models with clustered standard errors at the SME level. Column 1 shows the effects of different emails and experience treatments on the overall propensity to click, while the second column provides estimates after controlling for SME variables. From the two identifiable effects in the study (*Exp A* and *Exp B*), only the former has evidence of affecting the propensity to click. Having received an email A decreased the probability of clicking on a subsequent phishing email by 11 percentage points, which had a short time gap between the two phishing drills (35 days).

Table 7: Linear Probability Analysis of the propensity to click

	Click	
	(1)	(2)
Experience A	−0.11 (0.06)*	−0.11 (0.06)*
Experience B	0.03 (0.05)	0.02 (0.05)
Proxy LT Exp. A	−0.05 (0.06)	−0.05 (0.06)
Proxy. Exp. C	−0.05 (0.06)	−0.05 (0.06)
Email A	0.25 (0.02)***	0.14 (0.11)
Email B	0.22 (0.05)***	0.11 (0.11)
Email C	0.22 (0.04)***	0.12 (0.11)
SME Num email adrss.		0.01 (0.00)*
S. ICT		0.00 (0.08)
S. Industry		−0.05 (0.07)
S. Other		−0.13 (0.07)*
S. Services		−0.01 (0.08)
S. Trade and retail		−0.16 (0.07)*
Covid rel. pressure		0.01 (0.03)
post-Cov office occ		−0.00 (0.00)
Internet dependecy		0.07 (0.05)
Full cloud		0.09 (0.03)**
Partial cloud		0.07 (0.03)*
Has Internet policy		0.03 (0.04)
Internal IT		−0.02 (0.05)
Part. outsorced IT		−0.00 (0.04)
Daily backup		−0.04 (0.08)
R^2	0.22	0.26
Adj. R^2	0.22	0.26
Num. obs.	66032	60814

Note: OLS regressions with standard errors clustered at company level. Column (1) measures at the effect of being exposed to email A or email B on subsequent clicking behavior. Column (2) repeats the analysis including company-level characteristics. Significance code: $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$.

Column 2 allows us to compare how correlated the different characteristics of the SMEs are to the clicking behavior. Characteristics such as economic sectors or having some type of cloud service are strongly correlated with clicking behavior. The SME size, as proxied by the number of emails sent to the company (*Num email*), influenced clicking behavior. Being part of a company with 10 more employees increased the probability of clicking by 0.01 percentage point. Variables such as declared internet dependency, if the company managed its IT process or outsourced it, were included but appear not to correlate with clicking behavior. In addition, the analysis included some variables related to the Covid-19 pandemic given the time frame of the experiment. Neither the occupancy rate in the office nor the SME noticing more pressure on its business compared to before COVID-19 was significant. This result underlines the heterogeneity of our sample and how different characteristics of the different SMEs relate to the clicking behavior of the employees.

It is worth noting that in the second column, the effect of *Exp A* does not change in this estimation, while the propensities to click change when introducing company characteristics. This suggests that the change in clicking behavior is not associated with the type of company individuals are in, unlike the initial propensities to click. The variables *Email A*, *Email B*, and *Email C* indeed lose significance when SME characteristics are included.

3.3 Individual-level analysis

Table 8: Central values of each preference measurement of classification done by K-means

	Risk Seeking	Trust	Patience
Cluster 1	0.21	0.30	0.34
Cluster 2	0.58	0.54	0.66

Risk and patience are often correlated (Dean and Ortoleva, 2019), which is also the case in our data ($r = 0.49, p < 0.05$). There is also a positive correlation for *Trust* and *Patience*, albeit a lower one ($r = 0.33, p < 0.05$). Such levels of correlation might create a problem of multicollinearity when the variables are included together in a regression. To avoid this, we classified the whole sample into groups using a k-means algorithm using the answers on the preference measurements as attributes. The resulting grouping enables us to estimate if there is an effect of the preferences on clicking behavior without a multicollinearity bias as both groups are mutually exclusive.

The application of the K-means algorithm suggests that the optimal number of groups is two (see Appendix F), with roughly 38.07% and 61.92% of the sample for cluster 1 and cluster 2 accordingly. The central value for each of the three measurements is reported in Table 8, individuals in cluster 1 have a lower value in all measures while those in cluster 2 seem to have a higher value of risk-seeking, patience, and trust. In the regression analysis below, *Cluster 2* captures the effect of having high values in the three preference measures.

Table 9 shows the results of the link between individual preferences and learning from phishing experience. The results show that risk preferences, patience, and trust affect the initial propensity to click, but the association is less strong for trust. Considering interaction terms, only patience and risk seeking seem to affect the effect of having experienced email A (see the coefficients of $Exp.A \times Risk$ and $Exp.A \times Patience$). Column 4 shows that the coefficient for *Cluster 2* is positive indicating that individuals with high values in all three attributes have a higher propensity to click. This is in line with the results in the rest of the table. However, the effect is lower than in those in models 1,2 and 3, as expected, because we collapsed three measures into one binary classification. The coefficient for the interaction with *Experience A* suggests that individuals in the second group, with higher trust, risk-seeking, and patience, are affected the most by having previously been sent Email A. Again the coefficient is lower than in models 1,2 and 3.

Table 17 in Appendix G shows that adding SME-level control variables does not affect the results. We also replicate the analysis by adding age and gender, and their interaction with experience. Table 18 shows that older employees seemed to learn less from having experienced Email A.

Table 9: Linear probability model of the propensity to click with preference variables

	Click			
	(1)	(2)	(3)	(4)
Experience A	-0.04 (0.07)	-0.02 (0.07)	-0.05 (0.07)	-0.06 (0.07)
Experience B	0.02 (0.08)	0.05 (0.08)	0.05 (0.07)	0.03 (0.07)
Proxy LT Exp. A	0.01 (0.08)	-0.02 (0.08)	-0.00 (0.08)	0.00 (0.07)
Proxy. Exp. C	-0.01 (0.07)	-0.00 (0.07)	-0.02 (0.07)	0.00 (0.08)
email A	0.22 (0.03)***	0.21 (0.03)***	0.24 (0.03)***	0.23 (0.03)***
email B	0.18 (0.05)***	0.17 (0.05)**	0.20 (0.05)***	0.19 (0.05)***
email C	0.24 (0.06)***	0.24 (0.06)***	0.27 (0.06)***	0.26 (0.06)***
Risk seeking	0.10 (0.03)***			
Patience		0.09 (0.03)***		
Trust			0.05 (0.03)	
Cluster 2				0.04 (0.01)***
Exp. A x Risk	-0.10 (0.04)*			
Exp. B x Risk	-0.01 (0.05)			
Proxy L.T. A. x Risk	-0.04 (0.04)			
Proxy Exp. C x Risk	0.04 (0.05)			
Exp. A x Patience		-0.13 (0.04)**		
Exp. B x Patience		-0.06 (0.05)		
Proxy L.T. A. x Patience		0.01 (0.06)		
Proxy Exp. C x Patience		0.02 (0.05)		
Exp. A x Trust			-0.08 (0.05)	
Exp. B x Trust			-0.09 (0.05)	
Proxy L.T. A x Trust			-0.03 (0.07)	
Proxy Exp. C x Trust			0.06 (0.06)	
Exp. A x Cluster 2				-0.05 (0.03)*
Exp. B x Cluster 2				-0.02 (0.02)
Proxy Exp. C x Cluster 2				0.01 (0.02)
Proxy L.T. A x Cluster 2				-0.03 (0.02)
R^2	0.25	0.25	0.25	0.25
Adj. R^2	0.25	0.25	0.25	0.25
Num. obs.	15318	15318	15318	15318

Note: OLS regressions with standard errors clustered at company level. Significance code: $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$.

4 Discussion and conclusion

We assessed the impact of phishing drills on the probability of falling for another phishing attack. We varied both the time between the emails and the type of the emails sent. We found that a substantial proportion of the sample clicked on the first phishing email, while the proportion was lower for the second phishing email. The usable evidence allowed us to conclude that individuals changed their clicking behavior only when the time gap between phishing drill emails was short. On average, individuals decreased their propensity to click by 11 percentage points in the group *A*-*B* which had a short time gap between the two phishing drills (35 days). Taking into account that the initial probability to click in *Email B* is 22%, this means that the probability to click almost halved when they had experience with *Email A*. None of the other experience variables were significant.

From a replication perspective, the only significant result—the reduction of 11 percentage points—is comparable to what was found by Baillon et al., 2019, in a field experiment conducted in the same country. Their field experiment involved employees of the Dutch Ministry of Economic Affairs. Conducted in November and December 2015, and with a delay 40 days between the first and the second email, the experiment showed an 8 to 12 points reduction of the propensity to click (depending on the specification). The effect was deemed large and therefore promising enough to replicate it with SMEs by conducting the field experiment reported in the present paper.

The results of this second experiment, conducted a bit more than 5 years later, nuances the promise of the first one. Only one of the phishing drills led to a significant reduction of the propensity to click on the link in the second phishing email. Several reasons may be proposed. First, it may be that Email A was more effective as a learning experience than Email B or C. The similar clicking rates on Emails A, B, and C when received first (between 22 and 25%, see Table 7) do not seem do support this explanation. As a side note, this propensity is comparable to the average propensity found by Sommestad and Karlzén, 2019 in their meta-study, 24%. Second, it could be that the experience effect does not last long. This is a plausible explanation but the proxy effect estimated for group *C-B*, after only 4 weeks, is quite low and not significant. Third, employees in 2020 were more aware about phishing and more had experienced it than in 2015. Hence, it may be that phishing drills do not bring as much awareness than they use to. What was once a salient experience to learn from has become more banal.

Such a large field experiment involving many companies cannot be perfectly controlled. Two aspects could bias the results. Some companies had a surprisingly high clicking rate (100%), which could be caused by companies' URL scanners, and in others, many employees reported having heard of the phishing drills. We assessed the robustness of our findings by conducting the main analysis with a restricted sample of SMEs. In particular, we excluded from the analysis companies where all the employees had clicked within 10 minutes from the dispatch of the emails, and the companies where at least half the employees reported to have been informed about the phishing drill. Table 15 in Appendix G confirms that the results are not qualitatively different from the main results documented in the paper.

We found that the initial propensity to click on each email was correlated with company characteristics. This could be because characteristics such as sector or cloud use might proxy other variables such as the education of the employees, whether companies have an intensive of cloud services, or their experience with proper data handling. For example, companies that have more intensive use of the cloud, and do not have their own data centers would have less experience with data safeguards such as phishing protection. It could also be the case that some sectors might be more prone to being targeted by phishing emails, thus their employees are more experienced and click less than others. However, we also found that the effect of experience with phishing emails was not associated with company characteristics.

Our evidence suggests that preferences are not only associated with the initial propensity to click but also with the change in clicking behavior due to experience. In particular, we found that both more patient individuals and risk-seeking individuals were more likely to click. The literature had already provided evidence of a negative relationship between risk-seeking and the ability to detect internet scams (Chen et al., 2017). However, lack of self-control rather than patience has been found to decrease phishing detection abilities (Vishwanath et al., 2018). Hence, the correlation of patience with clicking propensity is surprising. It could be an artefact of the type of email that was sent. Individuals had to click on a link to claim their gift and were probably expecting to have to perform another time-consuming task such as giving personal data. Meanwhile, risk seekers could have clicked more as they were more willing to take the risk of malicious emails to obtain the promised reward.

That both preferences affect clicking behavior may come from the fact that they are correlated. A positive correlation between being more patient and being more risk-seeking, although counterintuitive, has also been found by Falk et al. (2018) with the same preference measurements we use and by Dean and Ortoleva (2019) using incentivized measurements. The relation between patience and changes in clicking behavior could be explained by a higher disposition of these individuals to read the information given to them once they clicked on the first phishing email and more attention in scrutinizing the emails they have received.

Our results demonstrate the added value of replication studies. They partially support the effectiveness of phishing drills established in previous studies but also highlight limitations, as phishing drills seemed to have neither a systematic nor a long-lasting impact. A specific cluster of employees, risk-seeking and patient, were simultaneously more likely to fall for a phishing attack and more likely to learn from it. These exploratory results illustrate the potential of simple behavioral elicitation questions in field studies, where more complex preference measurements may not be feasible.

A Surveys

A.1 Company Survey before the experiment

Which sector does your company belong to?

- Construction and Real Estate
- Communication and Media
- Consultancy
- energy companies
- Facility management
- fast Moving Consumer Goods
- Financial services
- Healthcare and welfare
- Trade and retail
- Hospitality, Recreation, Tourism and Culture
- Industry
- Information and Communication Technology (ICT)
- Intermediaries
- Legal services
- Agriculture and horticulture
- Teaching and research
- Government and semi-government
- Technical services

- Telecommunications
- Transport and logistics
- Retail
- Other

How many employees does your company consist of?

- Less than 10
- 10 to 50
- 50 to 250
- 250 or more

To what extent do you experience change in your business activities as a result of COVID-19?

- Much less busy
- Less busy
- No change
- Busier
- Much busier
- I do not know

What percentage of your employees worked in the office before COVID-19? Enter a number between 0 and 100.

What percentage of your employees currently work in the office? Enter a number between 0 and 100.

To what extent do you agree with the following statement? “The business processes within my company are completely dependent on the internet and computers.”

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree
- I don't know/no opinion

Is IT security outsourced within your company?

- Yes, fully outsourced
- Yes, partly outsourced
- No, completely in-house

Does your company use a Cloud service?

- Yes
- Partially
- No

How regularly are backups made?

- Daily
- Weekly
- Monthly
- Annually
- No backups are made

Have policy agreements been made within your company for the use of the internet (for example with a login procedure)?

- Yes
- No

A.2 Company Survey after the experiment

How did you experience the SME Phishing Test?

- Very useful
- Useful
- Neutral
- Useless
- Very useless
- I don't know / no opinion

Are you planning to take measures in the coming period to increase your resilience against phishing? [Displayed only if the respondents said 'Yes' in the previous question]

- Yes
- No

What measures do you plan to take to increase your resilience to phishing?

- Provide training to employees on cybersecurity
- (More often) perform a phishing test
- Technical measures

Did your company take additional measures to prevent phishing between [date test 1] and [date test 2]? If yes, which ones.

- Yes
- No

A.3 Employee Survey Instructions

Did you receive an email from [domain]?

- Yes
- No

Were you informed in advance by your employer about this phishing test?

- Yes
- No

Were you warned by a colleague who had already seen the phishing email before opening the phishing email?

- Yes
- No

Where were you working when you received the phishing email?

- At the office
- From home
- Public place
- On the go
- I don't know

Have you ever been the victim of a phishing email in the past?

- Yes
- No
- I do not know

How many phishing emails do you think you have received on your work email in the past month?

- None
- 1-3 phishing emails
- 3-5 phishing emails
- More than 5 phishing emails

My knowledge about digital and online security is...

- Very limited
- Limited
- Reasonable
- Good
- Very good
- Do not know

What is your gender?

- Male
- Female
- Non binary

What is your age?

- under the age of 18
- 18-24 years
- 25-29 years

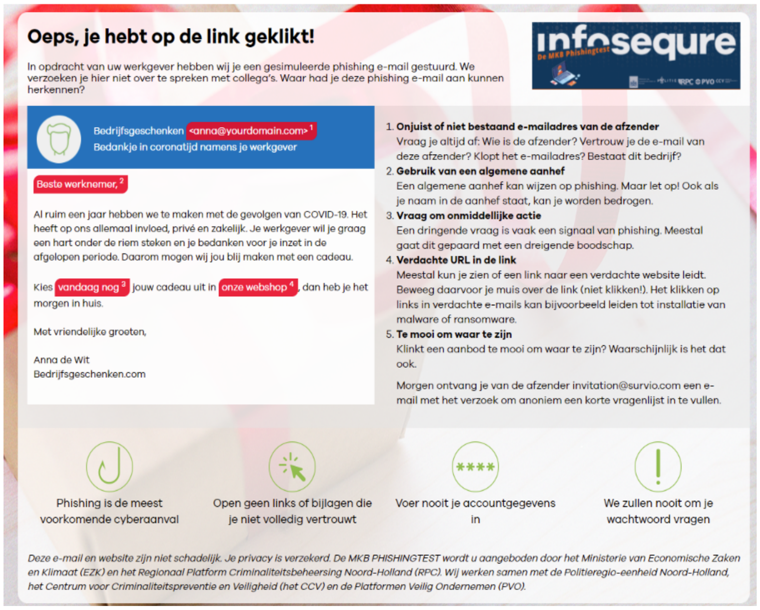
- 30-34 years
- 35-39 years
- 40-44 years
- 45-49 years
- 50-54 years
- 55-59 years
- 60-64 years
- 65 years or older

In general, to what extent are you willing or unwilling to take risks? Please use a scale of 0-10, where 0 means “not at all willing to take risks” and a 10 means you are “very willing to take risks”.

To what extent are you willing to give up something that benefits you today in order to benefit more in the future? Please use a scale of 0 to 10, where 0 means “completely unwilling to give up something today in order to benefit more in the future” and a 10 means that you are “very willing to give up something today in order to take advantage of it more in the future.”

To what extent do you assume that people only have the best intentions? Please use a scale of 0 to 10, where 0 means “I never assume people have only the best intentions” and 10 means “I always assume people only have the best intentions”. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

B Screenshot of the Feedback



Oeps, je hebt op de link geklikt!

In opdracht van uw werkgever hebben wij je een gesimuleerde phishing e-mail gestuurd. We verzoeken je hier niet over te spreken met collega's. Waar had je deze phishing e-mail aan kunnen herkennen?

Bedrijfsgeschenken <anna@yourdomain.com>[1]
Bedankje in coronatijd namens je werkgever

Beste werknemer,[2]

Al ruim een jaar hebben we te maken met de gevolgen van COVID-19. Het heeft op ons allemaal invloed, privé en zakelijk. Je werkgever wil je graag een hart onder de riem steken en je bedanken voor je inzet in de afgelopen periode. Daarom mogen wij jou blij maken met een cadeau.

Kies vandaag nog[3] jouw cadeau uit in onze webshop[4], dan heb je het morgen in huis.

Met vriendelijke groeten,

Anna de Wit
Bedrijfsgeschenken.com

1. **Onjuist of niet bestaand e-mailadres van de afzender**
   Vraag je altijd af: Wie is de afzender? Vertrouw je de e-mail van deze afzender? Klopt het e-mailadres? Bestaat dit bedrijf?
2. **Gebruik van een algemene aanhef**
   Een algemene aanhef kan wijzen op phishing. Maar let op! Ook als je naam in de aanhef staat, kan je worden bedrogen.
3. **Vraag om onmiddellijke actie**
   Een dringende vraag is vaak een signaal van phishing. Meestal gaat dit gepaard met een dreigende boodschap.
4. **Verdachte URL in de link**
   Meestal kun je zien of een link naar een verdachte website leidt. Beweeg daarvoor je muis over de link (niet klikken!). Het klikken op links in verdachte e-mails kan bijvoorbeeld leiden tot installatie van malware of ransomware.
5. **Te mooi om waar te zijn**
   Klinkt een aanbod te mooi om waar te zijn? Waarschijnlijk is het dat ook.

Morgen ontvang je van de afzender invitation@survio.com een e-mail met het verzoek om anoniem een korte vragenlijst in te vullen.

Phishing is de meest voorkomende cyberaanval

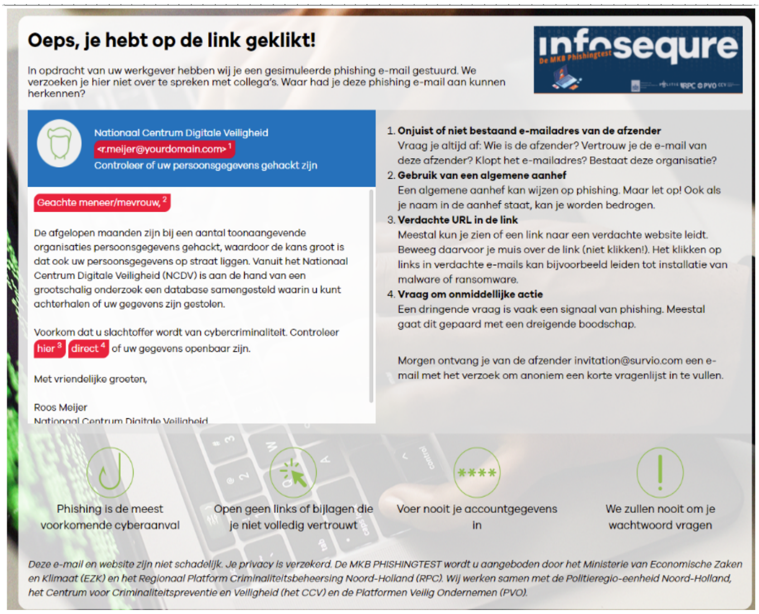
Open geen links of bijlagen die je niet volledig vertrouwt

Voer nooit je accountgegevens in

We zullen nooit om je wachtwoord vragen

Deze e-mail en website zijn niet schadelijk. Je privacy is verzekerd. De MKB PHISHINGTEST wordt u aangeboden door het Ministerie van Economische Zaken en Klimaat (EZK) en het Regionaal Platform Criminaliteitsbeheersing Noord-Holland (RPC). Wij werken samen met de Politieregio-eenheid Noord-Holland, het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV) en de Platformen Veilig Ondernemen (PVO).

Figure 4: Feedback A



Oeps, je hebt op de link geklikt!

In opdracht van uw werkgever hebben wij je een gesimuleerde phishing e-mail gestuurd. We verzoeken je hier niet over te spreken met collega's. Waar had je deze phishing e-mail aan kunnen herkennen?

Nationaal Centrum Digitale Veiligheid
<r.meijer@yourdomain.com>[1]
Controleer of uw persoonsgegevens gehackt zijn

Geachte meneer/mevrouw,[2]

De afgelopen maanden zijn bij een aantal toonaangevende organisaties persoonsgegevens gehackt, waardoor de kans groot is dat ook uw persoonsgegevens op straat liggen. Vanuit het Nationaal Centrum Digitale Veiligheid (NCDV) is aan de hand van een grootschalig onderzoek een database samengesteld waarin u kunt achterhalen of uw gegevens zijn gestolen.

Voorkom dat u slachtoffer wordt van cybercriminaliteit. Controleer hier[3] direct[4] of uw gegevens openbaar zijn.

Met vriendelijke groeten,

Roos Meijer
Nationaal Centrum Digitale Veiligheid

1. **Onjuist of niet bestaand e-mailadres van de afzender**
   Vraag je altijd af: Wie is de afzender? Vertrouw je de e-mail van deze afzender? Klopt het e-mailadres? Bestaat deze organisatie?
2. **Gebruik van een algemene aanhef**
   Een algemene aanhef kan wijzen op phishing. Maar let op! Ook als je naam in de aanhef staat, kan je worden bedrogen.
3. **Verdachte URL in de link**
   Meestal kun je zien of een link naar een verdachte website leidt. Beweeg daarvoor je muis over de link (niet klikken!). Het klikken op links in verdachte e-mails kan bijvoorbeeld leiden tot installatie van malware of ransomware.
4. **Vraag om onmiddellijke actie**
   Een dringende vraag is vaak een signaal van phishing. Meestal gaat dit gepaard met een dreigende boodschap.

Morgen ontvang je van de afzender invitation@survio.com een e-mail met het verzoek om anoniem een korte vragenlijst in te vullen.

Phishing is de meest voorkomende cyberaanval

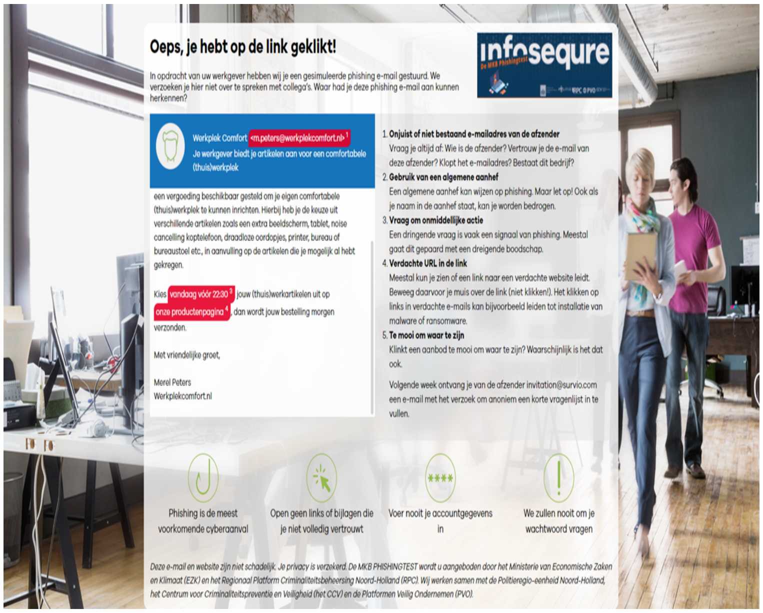
Open geen links of bijlagen die je niet volledig vertrouwt

Voer nooit je accountgegevens in

We zullen nooit om je wachtwoord vragen

Deze e-mail en website zijn niet schadelijk. Je privacy is verzekerd. De MKB PHISHINGTEST wordt u aangeboden door het Ministerie van Economische Zaken en Klimaat (EZK) en het Regionaal Platform Criminaliteitsbeheersing Noord-Holland (RPC). Wij werken samen met de Politieregio-eenheid Noord-Holland, het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV) en de Platformen Veilig Ondernemen (PVO).

Figure 5: Feedback B



Oeps, je hebt op de link geklikt!

In opdracht van uw werkgever hebben wij je een gesimuleerde phishing e-mail gestuurd. We verzoeken je hier niet over te spreken met collega's. Waar had je deze phishing e-mail aan kunnen herkennen?

Werkplek Comfort <m.peters@werkplekcomfort.nl> [1]
Je werkgever biedt je artikelen aan voor een comfortabele (thuis)werkplek

een vergoeding beschikbaar gesteld om je eigen comfortabele (thuis)werkplek te kunnen inrichten. Hierbij heb je de keuze uit verschillende artikelen zoals een extra beeldscherm, tablet, noise cancelling koptelefoon, draadloze oordopjes, printer, bureau of bureaustoel etc., in aanvulling op de artikelen die je mogelijk al hebt gekregen.

Kies vandaag vóór 22:30 [3] jouw (thuis)werkartikelen uit op onze productenpagina [4], dan wordt jouw bestelling morgen verzonden.

Met vriendelijke groet,

Merel Peters
Werkplekcomfort.nl

1. **Onjuist of niet bestaand e-mailadres van de afzender**
   Vraag je altijd af: Wie is de afzender? Vertrouw je de e-mail van deze afzender? Klopt het e-mailadres? Bestaat dit bedrijf?
2. **Gebruik van een algemene aanhef**
   Een algemene aanhef kan wijzen op phishing. Maar let op! Ook als je naam in de aanhef staat, kan je worden bedrogen.
3. **Vraag om onmiddellijke actie**
   Een dringende vraag is vaak een signaal van phishing. Meestal gaat dit gepaard met een dreigende boodschap.
4. **Verdachte URL in de link**
   Meestal kun je zien of een link naar een verdachte website leidt. Beweeg daarvoor je muis over de link (niet klikken!). Het klikken op links in verdachte e-mails kan bijvoorbeeld leiden tot installatie van malware of ransomware.
5. **Te mooi om waar te zijn**
   Klinkt een aanbod te mooi om waar te zijn? Waarschijnlijk is het dat ook.

Volgende week ontvang je van de afzender invitation@survio.com een e-mail met het verzoek om anoniem een korte vragenlijst in te vullen.

Phishing is de meest voorkomende cyberaanval

Open geen links of bijlagen die je niet volledig vertrouwt

Voer nooit je accountgegevens in

We zullen nooit om je wachtwoord vragen

Deze e-mail en website zijn niet schadelijk. Je privacy is verzekerd. De MKB PHISHINGTEST wordt u aangeboden door het Ministerie van Economische Zaken en Klimaat (EZK) en het Regionaal Platform Criminaliteitsbeheersing Noord-Holland (RPC). Wij werken samen met de Politieregio-eenheid Noord-Holland, het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV) en de Platformen Veilig Ondernemen (PVO).

Figure 6: Feedback C

English translation Feedback pages

Oops, you clicked the link!
On behalf of your employer, we have sent you a simulated phishing email. We request you to not discuss this with colleagues. How could you have recognized this phishing email?

1. **Incorrect or non-existent sender's email address**
   Always ask yourself: Who is the sender? Do you trust the email address from this sender? Is the email address correct? Does this company exist?

2. **Use of a general salutation**
   A general salutation may indicate phishing. But pay attention! Even if your name is in the salutation, you can be deceived.

3. **Demand for immediate action**
   An urgent question is often a signal of phishing. It is usually accompanied by a threatening message.

4. **Suspicious URL in the link**
   You can usually tell if a link leads to a suspicious website. To do this, move your mouse over the link (don't click!). Clicking on links in suspicious emails can for example lead to installation of malware or ransomware.

5. **Too good to be true**
   Does an offer sound too good to be true? It probably is.

Next week you will receive an email from the advertisement sender invitation@survio.com with the request to anonymously complete a short questionnaire.

translation of the items below the circles

- Phishing is the most common cyber attack
- Do not open links or attachments that you do not fully trust
- Never enter your account details
- We will never ask for your password

This email and website are not harmful. Your privacy is assured. The MKB PHISHING TEST is offered to you by the Ministry of Economic Affairs and Climate and the North Holland Regional Crime Control Platform (RPC). We work together with the North Holland police regional unit, the Center for Crime Prevention and Safety (CCV) and the Safe Business Platforms (PVO).

C Descriptives of main individual variables by group

Table 10: Answers by email and gender

	First Email				Second Email			
Group	Respondents	Males	Females	Prop. Fem	Respondents	Males	Females	Prop. Fem
Overall	8978	5455	3422	0.38	7659	4652	2905	0.38
A-B	1870	1228	617	0.33	1847	1180	637	0.34
B-C	2641	1578	1036	0.39	2317	1377	911	0.39
C-B	2330	1490	812	0.35	1611	1009	583	0.37
Long A-B	2137	1159	957	0.45	1884	1086	774	0.41

Table 11: Mean and Standard deviation for main variables and Age

	Overal		A-B		B-C		C-B		Long A-B	
Variable	Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD
First Email										
Age	42.19	11.88	41.91	11.95	41.95	11.98	42.89	11.78	41.97	11.78
Risk Seeking	0.44	0.25	0.46	0.24	0.42	0.25	0.44	0.25	0.44	0.25
Patience	0.54	0.24	0.55	0.23	0.54	0.24	0.54	0.24	0.54	0.24
Trust	0.44	0.23	0.44	0.23	0.43	0.23	0.45	0.23	0.45	0.23
Second Email										
Age	43.63	11.84	43.59	11.91	42.71	11.89	44.23	11.81	44.27	11.65
Risk Seeking	0.44	0.25	0.45	0.25	0.45	0.24	0.45	0.25	0.42	0.25
Patience	0.54	0.24	0.55	0.24	0.54	0.23	0.54	0.24	0.54	0.24
Trust	0.45	0.23	0.44	0.23	0.45	0.23	0.45	0.23	0.44	0.23

D Proportion of missing values in SME variables by treatment group

Table 12

variable	A-B	B-C	C-B	Long A-B
No. of SME's	168	166	167	166
More Covid relative pressure	0.05	0.07	0.02	0.02
Internet dependency	0.02	0.04	0.01	0.02
Full Cloud	0.02	0.02	0.01	0.02
Partial Cloud	0.02	0.02	0.01	0.02
Internet Policy	0.02	0.02	0.02	0.02
Internal IT	0.02	0.02	0.01	0.01
Partially Outsorced	0.02	0.02	0.01	0.01
Daily Backup	0.00	0.00	0.00	0.00

E Balance tests

Table 13: Test of between groups differences in *Post covid – office rate* and *Num email*

	(1)	(2)
Constant	39.83^{***}	4.91^{***}
	(2.46)	(0.41)
Group B-C	-1.25	0.02
	(3.49)	(0.59)
Group C-B	3.40	-0.08
	(3.49)	(0.59)
Group Long A-B	0.36	0.24
	(3.48)	(0.59)
R^2	0.00	0.00
Adj. R^2	-0.00	-0.00
Num. obs.	654	667

Note: in column (1), the dependent variable is *Post covid – office rate* and in column to it is *Num email*. Significance code: $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$.

F Cluster analysis of preferences

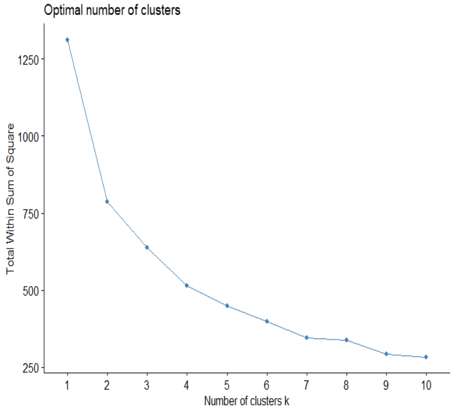


Figure 7: Elbow plot classification by preferences

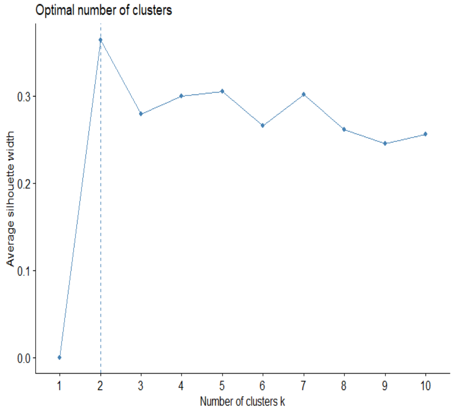


Figure 8: Silhouette showing the optimal number of clusters

G Robustness checks

Table 14: Replication Table 7 taking out speeders and more than 50% of informed respondents

	Click	
	(1)	(2)
Experience A	−0.10 (0.06)$^{\cdot}$	−0.09 (0.05)$^{\cdot}$
Experience B	0.03 (0.06)	0.02 (0.05)
Proxy LT Exp. A	−0.05 (0.06)	−0.04 (0.06)
Proxy. Exp. C	−0.04 (0.06)	−0.04 (0.06)
email A	0.23 (0.02)***	0.09 (0.10)
email B	0.20 (0.05)***	0.04 (0.10)
email C	0.21 (0.04)***	0.07 (0.10)
SME Num email adrss.		0.01 (0.00)**
S. ICT		0.00 (0.08)
S. Industry		−0.07 (0.07)
S. Other		−0.14 (0.07)*
S. Services		−0.03 (0.08)
S. Trade and retail		−0.16 (0.06)*
Covid rel. pressure		0.02 (0.03)
post-Cov office occ		−0.00 (0.00)
Internet dependecy		0.10 (0.05)*
Full cloud		0.09 (0.03)**
Partial cloud		0.05 (0.03)$^{\cdot}$
Has Internet policy		0.02 (0.03)
Internal IT		0.00 (0.05)
Part. outsorced IT		0.01 (0.04)
Daily backup		−0.02 (0.08)
R^2	0.20	0.25
Adj. R^2	0.20	0.25
Num. obs.	62430	57338

Note: OLS regressions with standard errors clustered at company level. Column (1) measures the effect of being exposed to email A or email B. Column (2) repeats the analysis including company-level characteristics. Significance code: $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$; $^{\cdot}p < 0.1$.

Table 15: Replication Table 9 taking out speeders and more than 50% of informed respondents

	Click			
	(1)	(2)	(3)	(4)
Experience A	−0.03 (0.07)	−0.02 (0.07)	−0.05 (0.07)	−0.05 (0.07)
Experience B	0.02 (0.08)	0.05 (0.08)	0.04 (0.08)	0.02 (0.08)
Proxy LT Exp. A	−0.02 (0.07)	−0.05 (0.07)	−0.03 (0.07)	−0.02 (0.07)
Proxy. Exp. C	−0.01 (0.08)	0.00 (0.08)	−0.01 (0.08)	0.00 (0.08)
email A	0.20 (0.02)***	0.19 (0.02)***	0.22 (0.02)***	0.21 (0.02)***
email B	0.16 (0.05)**	0.15 (0.05)**	0.18 (0.05)***	0.18 (0.05)***
email C	0.23 (0.06)***	0.23 (0.06)***	0.26 (0.06)***	0.25 (0.06)***
Risk seeking	0.11 (0.02)***			
Patience		0.10 (0.02)***		
Trust			0.06 (0.03)*	
Cluster 1				0.05 (0.01)***
Exp. A x Risk	−0.13 (0.04)**			
Exp. B x Risk	−0.04 (0.05)			
Proxy L.T. A. x Risk	−0.02 (0.04)			
Proxy Exp. C x Risk	0.04 (0.06)			
Exp. A x Patience		−0.13 (0.04)**		
Exp. B x Patience		−0.09 (0.05)$^{\cdot}$		
Proxy L.T. A. x Patience		0.04 (0.05)		
Proxy Exp. C x Patience		0.02 (0.05)		
Exp. A x Trust			−0.08 (0.05)$^{\cdot}$	
Exp. B x Trust			−0.09 (0.05)$^{\cdot}$	
Proxy L.T. A x Trust			−0.00 (0.07)	
Proxy Exp. C x Trust			0.05 (0.06)	
Exp. A x Cluster 1				−0.06 (0.03)*
Exp. B x Cluster 1				−0.03 (0.02)
Proxy Exp. C x Cluster 1				0.02 (0.03)
Proxy L.T. A x Cluster 1				−0.02 (0.02)
R^2	0.24	0.24	0.23	0.24
Adj. R^2	0.24	0.23	0.23	0.23
Num. obs.	14640	14640	14640	14640

Note: OLS regressions with standard errors clustered at company level. Significance code: $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$.

Table 16: Propensity to click to second phishing by group

	Click Email B		Click Email C
	AB-BC	AB-CB-long AB	BC-CB
Constant	0.22 (0.05)***	0.22 (0.05)***	0.22 (0.04)***
Group AB	-0.11 (0.06)*	-0.11 (0.06)*	
Group long AB		-0.05 (0.06)	
Group BC			0.03 (0.05)
R^2	0.02	0.02	0.00
Adj. R^2	0.02	0.02	0.00
Num. obs.	32828	49906	32472

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$.Clustered standard errors at the SME level. Group AB is a binary variable indicating if subject belongs to group AB

Table 17: Linear probability model of the propensity to click with preference variables with company characteristic controls

	Click			
	(1)	(2)	(3)	(4)
Experience A	−0.04 (0.07)	−0.02 (0.07)	−0.06 (0.07)	−0.05 (0.06)
Experience B	0.02 (0.06)	0.05 (0.06)	0.03 (0.06)	0.02 (0.06)
Proxy LT Exp. A	−0.00 (0.07)	−0.02 (0.07)	−0.01 (0.07)	−0.01 (0.07)
Proxy. Exp. C	−0.01 (0.07)	0.00 (0.07)	−0.01 (0.07)	0.00 (0.07)
email A	0.02 (0.12)	0.01 (0.12)	0.03 (0.12)	0.03 (0.12)
email B	−0.03 (0.12)	−0.03 (0.12)	−0.01 (0.12)	−0.02 (0.12)
email C	0.04 (0.12)	0.04 (0.12)	0.06 (0.12)	0.05 (0.12)
Risk seeking	0.06 (0.02)**			
Patience		0.06 (0.02)*		
Trust			0.03 (0.02)	
Cluster 2				0.03 (0.01)*
Exp. A x Risk	−0.11 (0.05)*			
Exp. B x Risk	−0.03 (0.04)			
Proxy L.T. A. x Risk	−0.03 (0.04)			
Proxy Exp. C x Risk	0.04 (0.05)			
Exp. A x Patience		−0.12 (0.04)**		
Exp. B x Patience		−0.08 (0.04)		
Proxy L.T. A. x Patience		0.00 (0.05)		
Proxy Exp. C x Patience		0.01 (0.05)		
Exp. A x Trust			−0.07 (0.05)	
Exp. B x Trust			−0.06 (0.04)	
Proxy L.T. A x Trust			−0.03 (0.06)	
Proxy Exp. C x Trust			0.05 (0.06)	
Exp. A x Cluster 2				−0.06 (0.03)*
Exp. B x Cluster 2				−0.03 (0.02)
Proxy Exp. C x Cluster 2				0.01 (0.02)
Proxy L.T. A x Cluster 2				−0.02 (0.02)
Company Controls	YES	YES	YES	YES
R^2	0.32	0.32	0.32	0.32
Adj. R^2	0.32	0.32	0.32	0.32
Num. obs.	14118	14118	14118	14118

Note: OLS regressions with standard errors clustered at company level. Significance code: $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$.

Table 18: Linear Probability model of Propensity to click with demographic variables

	Click			
	(1)	(2)	(3)	(4)
Experience A	−0.05 (0.07)	−0.01 (0.07)	−0.05 (0.07)	−0.05 (0.07)
Experience B	0.03 (0.08)	0.06 (0.08)	0.06 (0.08)	0.04 (0.08)
Proxy LT Exp. A	−0.02 (0.07)	−0.05 (0.07)	−0.02 (0.08)	−0.02 (0.07)
Proxy. Exp. C	−0.04 (0.08)	−0.03 (0.09)	−0.04 (0.08)	−0.02 (0.08)
email A	0.24 (0.03)***	0.23 (0.03)***	0.25 (0.03)***	0.25 (0.03)***
email B	0.20 (0.05)***	0.19 (0.05)***	0.21 (0.05)***	0.21 (0.05)***
email C	0.26 (0.06)***	0.26 (0.06)***	0.28 (0.06)***	0.28 (0.06)***
Risk seeking	0.08 (0.03)**			
Patience		0.08 (0.03)**		
Trust			0.05 (0.02)*	
Cluster 2				0.04 (0.01)**
Exp. A x Risk	−0.08 (0.04)*			
Exp. B x Risk	−0.02 (0.05)			
Proxy Exp. C x Risk	0.07 (0.06)			
Proxy L.T. A x Risk	−0.02 (0.04)			
Exp. A x Patience		−0.12 (0.04)**		
Exp. B x Patience		−0.07 (0.05)		
Proxy L.T. A x Patience		0.03 (0.05)		
Proxy Exp. C x Patience		0.04 (0.05)		
Exp. A x Trust			−0.07 (0.05)	
Exp. B x Trust			−0.09 (0.05)*	
Proxy L.T. A x Trust			−0.03 (0.06)	
Proxy Exp. C x Trust			0.06 (0.06)	
Exp. A x Cluster 2				−0.04 (0.02)*
Exp. B x Cluster 2				−0.02 (0.02)
Proxy Exp. C x Cluster 2				0.02 (0.03)
Proxy Exp. C x Cluster 2				0.02 (0.03)
Age in decades	−0.01 (0.01)	−0.01 (0.01)	−0.01 (0.01)	−0.01 (0.01)
Female	−0.03 (0.02)	−0.03 (0.02)	−0.04 (0.02)	−0.03 (0.02)
Exp. A x Age	0.03 (0.02)*	0.03 (0.02)*	0.04 (0.02)*	0.03 (0.02)*
Exp. B x Age	−0.00 (0.02)	−0.00 (0.02)	−0.00 (0.02)	−0.00 (0.02)
Proxy Exp. C x Age	0.00 (0.02)	0.00 (0.02)	0.00 (0.01)	0.00 (0.02)
Proxy L.T. A x Age	0.01 (0.02)	0.02 (0.02)	0.01 (0.01)	0.01 (0.02)
Exp. A x Female	−0.04 (0.03)	−0.05 (0.03)	−0.04 (0.03)	−0.04 (0.03)
Exp. B x Female	−0.01 (0.03)	−0.02 (0.03)	−0.01 (0.03)	−0.02 (0.03)
Proxy Exp. C x Female	0.03 (0.06)	0.03 (0.06)	0.03 (0.06)	0.03 (0.06)
Proxy L.T. A x Female	0.03 (0.05)	0.04 (0.05)	0.04 (0.05)	0.03 (0.05)
R^2	0.25	0.25	0.25	0.25
Adj. R^2	0.25	0.25	0.25	0.25
Num. obs.	14956	14956	14956	14956

Note: OLS regressions with standard errors clustered at company level. Age in decades is the Age transformed by substracting the mean and dividing by 10. Significance code: $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, *30*(4), 736–758.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, *42*(2), 249–274.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of economic Literature*, *54*(2), 442–492.

Ankel-Peters, J., Fiala, N., & Neubauer, F. (2023). Do economists replicate? *Journal of Economic Behavior & Organization*, *212*, 219–232.

Arduin, P.-E. (2023). A cognitive approach to the decision to trust or distrust phishing emails. *International Transactions in Operational Research*, *30*(3), 1263–1298.

Asghari, H., van Eeten, M., & Bauer, J. M. (2016). Chapter 13: Economics of cybersecurity. *Handbook on the Economics of the Internet*, 262–287.

Avdeenko, A., Bohne, A., & Frölich, M. (2019). Linking savings behavior, confidence and individual feedback: A field experiment in ethiopia. *Journal of Economic Behavior & Organization*, *167*, 122–151.

Baillon, A., de Bruin, J., Emirmahmutoglu, A., van de Veer, E., & van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks (T. Ren, Ed.). *PLOS ONE*, *14*(12), e0224216. https://doi.org/10.1371/journal.pone.0224216

Benjamin, D. J., Berger, J. O., Johannesson, M., Nosek, B. A., Wagenmakers, E.-J., Berk, R., Bollen, K. A., Brembs, B., Brown, L., Camerer, C., et al. (2018). Redefine statistical significance. *Nature human behaviour*, *2*(1), 6–10.

Biener, C., Eling, M., & Lehmann, M. (2020). Balancing the desire for privacy against the desire to hedge risk. *Journal of Economic Behavior & Organization*, *180*, 608–620.

Brodeur, A., Cook, N., & Heyes, A. (2020). Methods matter: P-hacking and publication bias in causal analysis in economics. *American Economic Review*, *110*(11), 3634–3660.

Burda, P., Chotza, T., Allodi, L., & Zannone, N. (2020). Testing the effectiveness of tailored phishing techniques in industry and academia: A field experiment. *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 1–10. https://doi.org/10.1145/3407023.3409178

Cai, J., & Song, C. (2017). Do disaster experience and knowledge affect insurance take-up decisions? *Journal of Development Economics*, *124*, 83–94.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in human behavior*, *70*, 291–302.

Chew, S. H., Huang, W., & Zhao, X. (2020). Motivated false memory. *Journal of Political Economy*, *128*(10), 3913–3939.

Curtis, S. R., Rajivan, P., Jones, D. N., & Gonzalez, C. (2018). Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Computers in Human Behavior*, *87*, 174–182. https://doi.org/10.1016/j.chb.2018.05.037

Dean, M., & Ortoleva, P. (2019). The empirical relationship between nonstandard economic behaviors. *Proceedings of the National Academy of Sciences*, *116*(33), 16262–16267.

Dohmen, T., Falk, A., Huffman, D., Sunde, U., Schupp, J., & Wagner, G. G. (2011). Individual risk attitudes: Measurement, determinants, and behavioral consequences. *Journal of the European Economic Association*, *9*(3), 522–550.

Epperson, R., & Gerster, A. (2021). Information avoidance and moral behavior: Experimental evidence from food choices. *Available at SSRN 3938994*.

Falk, A., Becker, A., Dohmen, T., Enke, B., Huffman, D., & Sunde, U. (2018). Global evidence on economic preferences. *The Quarterly Journal of Economics*, *133*(4), 1645–1692.

Falk, A., Becker, A., Dohmen, T., Huffman, D., & Sunde, U. (2016). The Preference Survey Module: A Validated Instrument for Measuring Risk, Time, and Social Preferences, 69.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1), 2.

Goette, L., & Tripodi, E. (2020). Does positive feedback of social impact motivate prosocial behavior? a field experiment with blood donors. *Journal of Economic Behavior & Organization*, *175*, 1–8.

Goldfarb, A., & Que, V. F. (2023). The economics of digital privacy. *Annual Review of Economics*, *15*.

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open*, *2*(3), e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015)*.

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*, *40*(2), 265–281. https://doi.org/10.1108/OIR-04-2015-0106

Hong, K. W., Kelley, C. M., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2013). Keeping Up With The Joneses: Assessing Phishing Susceptibility in an Email Task. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1), 1012–1016. https://doi.org/10.1177/1541931213571226

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. *Journal of Medical Internet Research*, *22*(1), e16775. https://doi.org/10.2196/16775

Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied ergonomics*, *86*, 103084.

Lee, Y., & Weber, R. (2019). *Revealed privacy preferences: Are privacy choices rational?* (Tech. rep.). Working paper.

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *Journal of Economic Perspectives*, *23*(3), 3–20.

Ponemon, I. (2021). 2021 cost of phishing study.

Romensen, G.-J., & Soetevent, A. R. (2021). *Improving worker productivity through tailored performance feedback: Field experimental evidence from bus drivers* (tech. rep.). Kiel, Hamburg, ZBW - Leibniz Information Centre for Economics. http://hdl.handle.net/10419/246811

Schudy, S., & Utikal, V. (2017). 'you must not know about me'—on the willingness to share personal data. *Journal of Economic Behavior & Organization*, *141*, 1–13.

Shai, O. (2022). Out of time? the effect of an infrequent traumatic event on individuals' time and risk preferences, beliefs, and insurance purchasing. *Journal of Health Economics*, *86*, 102678.

Sommestad, T., & Karlzén, H. (2019). A meta-analysis of field experiments on phishing susceptibility. *2019 APWG symposium on electronic crime research (eCrime)*, 1–14.

Tomaino, G., Wertenbroch, K., & Walters, D. J. (2023). Intransitivity of consumer preferences for privacy. *Journal of Marketing Research*, *60*(3), 489–507.

Tran, A., & Zeckhauser, R. (2012). Rank as an inherent incentive: Evidence from a field experiment. *Journal of Public Economics*, *96*(9-10), 645–650.

van Justitie en Veiligheid, M. (2022). *Cyber Security Assessment Netherlands 2021 - Publication - National Coordinator for Security and Counterterrorism* (tech. rep.). https://english.nctv.nl/documents/publications/2021/08/05/cyber-security-assessment-netherlands-2021

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, *45*(8), 1146–1166.

Winegar, A. G., & Sunstein, C. R. (2019). How much is data privacy worth? a preliminary investigation. *Journal of Consumer Policy*, *42*, 425–440.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research Note: Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information Systems Research*, *25*(2), 385–400. Retrieved August 3, 2022, from https://www.jstor.org/stable/24700179