Journal of Universal Computer Science, vol. 25, no. 11 (2019), 1458-1477
submitted: 15/2/19, accepted: 26/7/19, appeared: 28/11/19

Testing the Human Backdoor: Organizational Response to a Phishing Campaign

Anže Mihelič
(University of Maribor, Faculty of criminal justice and security, Ljubljana, Slovenia
anze.mihelic@um.si)

Matej Jevšček
(Faculty of organization studies in Novo mesto, Novo mesto, Slovenia
matej.jevscek@t-2.net)

Simon Vrhovec
(University of Maribor, Faculty of criminal justice and security, Ljubljana, Slovenia
simon.vrhovec@um.si)

Igor Bernik
(University of Maribor, Faculty of criminal justice and security, Ljubljana, Slovenia
igor.bernik@fvv.uni-mb.si)

Abstract: To exploit the human as the “back door” to compromising well-protected information systems of organizations, phishing-type attacks are becoming increasingly sophisticated. There is however a significant lack of real-world studies of phishing campaigns in industrial settings even though it is a wide-spread way to hack information systems of organizations and many notorious cyberattacks started with some sort of a human exploitation. To fill this void, we conducted a case study in a large Central European manufacturing company Manco (fake company name) and observed the targeted employees’ and IT department staff’s response to a phishing campaign. Even though the IT department staff reacted very fast (their procedures started fifteen minutes after the first phishing e-mail was sent), results suggest significant data leakage and a high potential for successful malware installation. The observed click rate was 69.4 percent and real personal data submission rate was at least 49.0 percent. The average response time of targets (i.e., time between sending the phishing e-mail and visiting the phishing website) was 20 minutes, from 25 seconds to 203 minutes. The results suggest that a phishing campaign can be successful even if the targeted organization’s response time is very short. Also, the phishing campaign may not be effective only due to the susceptibility of targets but also due to the investigative techniques of the first responders.

Keywords: cyber-attack, social engineering, spear phishing, detection, response, case study
Categories: K.6.1, K.6.5, L.4.0, L.5

1 Introduction

Phishing-type attacks seem to be a very popular component of cyberattacks. According to [Symantec 2018], spear-phishing is by far the most used attack vector employed by 71 percent of cyberattacks. Every year we see an increase in compromises of business e-mails, by even more than 1,000 percent [Steer 2017]. A huge share of successful data breaches up to 90 percent or more has its roots in phishing-type attacks [Caldwell 2013, Steer 2017]. Since technical means of mitigating cyberattacks are becoming increasingly sophisticated, the human factor remains a "lever" which helps attackers compromise the security of organizations' information systems and various forms of phishing attacks are among the most popular social engineering techniques capable of leading to fruitful results. Despite the omnipresence of phishing-type attacks, research on detection and especially response to spear phishing campaigns by employees and IT departments seems to be particularly scarce. Most phishing studies focus on the susceptibility of individuals leaving the organizational aspect of phishing campaigns almost unresearched, especially in industrial settings. In this paper, we focus on detection and response to a phishing campaign in real-world settings.

The aim of this paper is to study the detection and organizational response to a simulated phishing campaign by a third party. A context-aware targeted phishing e-mail template and phishing website for submitting sensitive data have been set up. Afterwards, the targeted company has been attacked with all employees except for two being unaware of it. Data on phishing attack susceptibility (e.g., click rates, submitted sensitive data), detection (e.g., reports to the IT department) and response (e.g., IT department actions, contacts inside and outside of the targeted organization) have been collected during and after the phishing campaign.

In next section, we conceptualize phishing-type attacks. In Section 3, related literature is presented through a structured literature review. In Section 4, we present the methodology used in this case study. Results are presented in Section 5 and discussion with theoretical and practical implications is provided in Section 6. We conclude the paper with some final remarks in Section 7.

2 Phishing conceptualization

The concept of phishing was first described in 1987 as a technique in which a third party imitates a legitimate source in order to perform a malicious act [Felix and Hauck 1987]. However, there seems to be no definitive conceptualization of phishing-type techniques. Several terms related to phishing are frequently used in the literature, such as phishing, spear phishing, targeted phishing, context-aware phishing and whaling.

Definitions of *phishing*, sometimes also referred to as *mass*, *spam* and *blanket phishing*, are mostly uniform about their key elements, such as a large volume of sent messages, deception of targeted individuals, sender impersonation, information gathering via social engineering, and an opportunistic approach [Heartfield and Loukas 2015, Hong 2012, Lastdrager 2014, Nguyen 2013, Parmar 2012]. Definitions of *spear phishing* which is sometimes also referred to as *targeted phishing* [e.g. Neupane, Satvat, Saxena, Stavrinos and Johnson Bishop 2018, Wang, Herath, Chen, Vishwanath and Rao 2012, Williams, Hinds and Joinson 2018] and *context-aware phishing* [Jakobsson and Myers 2007] however seem to be quite far from uniform. In a broader sense, spear phishing is characterized by personalized messages (e.g., translated into the native language of the recipients) or messages sent to a targeted group (e.g., an organization) [Downs, Holbrook and Cranor 2006, Heartfield and Loukas 2015, Parmar 2012]. In a narrower sense, spear phishing (also known as *spear phishing-APT*) is a highly sophisticated and personalized attack with customized messages based on gathered personal data and accurate contextual information, and with relevant timing [FireEye 2016, Heartfield and Loukas 2015, Nguyen 2013]. For example, such attacks may involve monitoring targets' e-mails and hopping in when an opportunity for sending an e-mail with an attachment arises [Heartfield and Loukas 2015]. *Whaling* is commonly discussed as a separate social engineering technique [Olifer, Goranin, Kaceniauskas and Cenys 2017] however it does not seem to differ significantly from spear phishing. It is essentially spear phishing targeting the a specific type of targets, namely, the top and higher management of organizations [Krombholz, Hobel, Huber and Weippl 2015, Nguyen 2013].

In this paper, we propose to distinguish three types of phishing similarly to [Heartfield and Loukas 2015] based on the degree of personalization, context awareness and timing of an attack: blanket phishing, targeted phishing and spear phishing. *Blanket phishing* is a scalable, opportunistic and untargeted social engineering attack via messages where impersonation and deception are used to achieve a malicious aim without any context awareness. *Targeted phishing* also uses impersonation and deception elements however the attack is aimed at a specific group (e.g., an organization or a department). Messages are personalized and timed in a limited way based on some contextual awareness (e.g., sending e-mails relevant for a targeted department). The number of targets is significantly smaller than in blanket phishing however it may still be relatively high as the e-mails are sent indiscriminately to the members of a target group. *Spear phishing* is also aimed at a specific group however the potential victims are carefully selected typically after extensive collection of publicly available information (e.g., search engines, social networks, out of office automatic replies) and intelligence (e.g., insiders, previous contacts) on the target group. Contextual awareness is high, and messages may be highly personalized and well-timed. The success rate of phishing attacks usually increases with the degree of contextual awareness, personalization and proper timing.

3 Related literature

To provide an overview of existing studies reporting on e-mail spear phishing research in real organizational settings or realistic experiments, we conducted a structured literature review of research on spear phishing. We searched on Web of Science, Scopus, ACM DL and IEEE Xplore databases with the query *(spear OR targeted OR blanket OR campaign) AND phishing*. The searches yielded 825 hits which resulted in 448 unique results after excluding duplicates. Two authors independently screened the papers for inclusion in further examination according to the inclusion and exclusion criteria presented in Table 1. Discrepancies were solved through discussion.

Inclusion criteria	**Exclusion criteria**
Published in 2008 or later	Published in 2007 or earlier
Spear phishing campaigns	Theoretical paper
Email-based spear phishing	Not email-based phishing
Real organizational settings or realistic experiments	Poorly described research method or results
Focused on human factors	Abstract or presentation only
Journal article or conference paper	Poster
Published in English	Published in languages other than English
	Full text not accessible to researchers

Table 1: Paper inclusion and exclusion criteria

The details of papers included in the literature review are presented in Table 2.

Paper and topic	Methodology and sample	Key results
[Burns, Johnson and Caputo 2019] Using spear phishing campaigns as a training method.	Experiment *Round 1:* *260 organizational members* *Round 2:* *400 organizational members*	Click rate dropped from 70 percent to 54 percent (including the control group with 140 organizational members in round 2). Click rate of the control group in round 2 was 58 percent.
[Gordon et al. 2019] Employee susceptibility to phishing attacks at health care institutions.	Retrospective *6 health care institutions, 95 simulated phishing campaigns*	Click rate 14.2 percent ranging from 7.4 to 16.7 percent. Increasing campaigns were associated with decreased click rates suggesting a potential benefit of phishing simulation and awareness.
[Musuva, Getao and Chepken 2019] Phishing campaign copying recent real phishing attacks at a university.	Case study (experiment and survey) *Phishing campaign:* *4,483 insiders (students, staff, adjunct faculty, full-time faculty, management, interns, mailing list users, unknown)* *Survey:* *241 insiders*	Click rate was 1.7 percent. 88 percent of subjects that clicked on the link, also entered data (i.e., their credentials). Threat detection ability is the key determinant of phishing victimization.
[De Kimpe, Walrave, Hardyns, Pauwels and Ponnet 2018] Using an integrative lifestyle exposure model to study the effects of risky online routine activities that make a target more likely to come across a motivated offender.	Survey *723 internet users*	Support for a relationship between both online purchasing behavior and digital copying behavior, and phishing targeting. Online shoppers and users who often share and use copied files online should be trained to deal with phishing attacks.
[Martin, Dubé and Coovert 2018] Measuring phishing and spear-phishing susceptibility with signal detection theory framework.	Survey *344 Amazon Mechanical Turk users*	Participants were significantly less likely to identify spear-phishing e-mails as threatening than phishing e-mails; however, conscientiousness failed to predict performance.
[McElwee, Murphy and Shelton 2018] Exploring different approaches to reducing susceptibility to phishing using the primary mechanisms of agency theory. Training by simulating phishing attacks.	Case study *1,000 employees of a single organization*	Behavior-based controls were more successful in reducing susceptibility to phishing, primarily when implemented as targeted training that was repeated multiple times.

[Neupane et al. 2018] Understanding the performance of users with autism in identifying real and fake (phishing) websites.	Experiment and survey *15 individuals with autism and 15 individuals without autism*	Gullibility of users with autism may not make them more susceptible to phishing attacks, and, in fact, their detail-oriented nature may make them better equipped to combat phishing attacks, when contrasted with the individuals without autism.
[Williams et al. 2018] Study is exploring the factors that influence susceptibility to spear phishing e-mails within the workplace.	Case study and focus groups *Study 1: 62,000 employees* *Study 2: 32 employees*	Work based norms and routines likely represent a primary factor impacting response behavior to phishing-type e-mail messages influencing the development of context- specific habits, expectations and perceptions of risk.
[Bakar, Mohd and Sulaiman 2017] Phishing campaign simulation at a university.	Case study *553 employees of five faculties of a university in Malaysia*	209 (38%) subjects entered official IDs and passwords.
[Bakhshi 2017] Exploring end-user vulnerabilities to spear-phishing attacks and vulnerability in recognizing a prominent method for intrusion and compromise of information systems.	Experiments *Experiment 1: 49 employees* *Experiment 2: 15 USB sticks*	High proportion (46-60 percent) of the users failed to identify the phishing attacks. Lack of user awareness was the primary cause of the success of the attacks.
[Benenson, Gassmann and Landwirth 2017] Exploring Facebook and e-mail users' susceptibility to phishing attacks.	Experiment and survey *280 Facebook users and 975 e-mail users*	Results showed significant difference in clicking rates: 20 percent of e-mail messages versus 42.5 percent of Facebook recipients. Factors affecting click rates seem to be curiosity, fit of the message to recipient's expectations, assuming to know the sender.
[Bullee, Montoya, Junger and Hartel 2017] Authors investigated the susceptibility to phishing and spear-phishing attacks and the personal characteristics that influence the probability of compliance.	Experiment *593 employees*	Compliance to a general phishing e-mail was 19.3 percent, and 28.9 percent for a spear phishing e-mail. No main effects of gender or age on compliance were found however employees who worked longer in the organization were found to be less vulnerable to phishing e-mails.
[Carella, Kotsoev and Truta 2017] Exploring the impact of security awareness training on click rates.	Experiment and survey *150 participants*	In-class training is the most effective in the short term. Document based training has the greatest impact of click rates and is persisting in the long term. There is a visible impact of both training approaches over no training.
[Goel, Williams and Dincelli 2017] Susceptibility of users to phishing and spear phishing attacks.	Experiment and survey *7,250 undergraduate students*	Results show an opened e-mail rate of 27.3 percent, and a click rate of 13.3 percent. Females, students from business and social majors were more likely to open an e-mail message than males and students from humanities majors.

[Oliveira et al. 2017] Authors investigated factors of spear phishing susceptibility (age, weapon of influence, life domain).	Experiment and survey *158 internet users*	Results suggest that older women were the most susceptible group to spear phishing e-mail attacks. While younger users were most susceptible to scarcity, older users were most susceptible to reciprocation. Authority was highly effective in both age groups and both age groups.
[Sokol, Glova and Mezešova 2017] Susceptibility of users to phishing and spear phishing attacks.	Experiment *First phase:* *10,154 employees* *Second phase:* *10,119 employees* *Third phase:* *9,655 employees*	First phase: Click rate 2.82 percent, click and filling rate 0.23 percent. Second phase: Click rate 4.47 percent, click and filling rate 1.13 percent. Third phase: Click rate 2.92 percent, click and filling rate 3.54 percent.
[Canfield, Fischhoff and Davis 2016] Using signal detection theory (SDT) methods to assess phishing vulnerability by treating phishing detection as a vigilance task (detection and response of individuals).	Experiment *Experiment 1:* *152 participants* *Experiment 2:* *100 participants*	Participants know what to do about phishing e-mails but not when to do it. The tasks deciding whether a message is legitimate and what to do about it are naturally intertwined. Participants use different decision strategies for the two tasks. Individual performance varies widely.
[Harrison, Svetieva and Vishwanath 2016] Exploring user susceptibility by unpacking the mechanisms that may influence individual victimization.	Experiment *194 students*	47 percent divulged their private information to a bogus form page. Phishing susceptibility was predicted by a combination of both low attention to the e-mail elements and high elaboration of the phishing message. The presence of a threat or reward-based phishing message did not affect phishing susceptibility. Individual factors such as knowledge and experience with e-mail increased resilience to the phishing attack.
[Heartfield, Loukas and Gan 2016] Social network users' susceptibility to semantic social engineering attacks.	Experiments *Study 1:* *4,333 internet users* *Study 2:* *315 internet users*	Security training makes a noticeable difference in a user's ability to detect deception attempts. Important predictors were computer literacy, familiarity and frequency of access to a specific platform.
[Chuchuen and Chanvarasuth 2015] Exploring user personality types and their relation to several phishing techniques.	Survey *400 internet users in Bangkok*	Each personality type is susceptible to techniques at a different level. User personality types seem to influence vulnerability to different phishing techniques.

[Rocha Flores, Holm, Nohlberg and Ekstedt 2015] Investigating the correlation between a sample of personal psychological and demographic factors and resistance to phishing, and if national culture moderates the strength of these correlations.	Survey and experiment *2,099 employees of nine organizations in Sweden, USA and India (431 completed the survey)*	Significant even though not strong correlations between determinants of phishing and phishing. Differences based on cultures might exist based on firm characteristics within a country.
[Caputo, Pfleeger, Freeman and Johnson 2014] Exploring the effectiveness of embedded training against phishing and spear phishing.	Experiment and survey *1,359 employees*	The results from three trials showed that training had no significant effect on the likelihood that a participant would click a subsequent spear phishing e-mail and that many participants either clicked all links or none regardless of whether they received training. The study was unable to determine whether the embedded training materials affected the susceptibility to spear phishing attacks.
[Holm, Rocha Flores, Nohlberg and Ekstedt 2014] Difference between phishing attacks including target-related information and not. Additional data on employee reactions (including employees reporting about the phishing attack, when the attack was reported, and how it was reported) was collected.	Experiments *5 organizations, 158 employees*	Significant difference between targeted and non-targeted phishing attacks for click rates (27.2 and 5.1 percent) and binary execution (8.9 and 3.2 percent). The IT managers were aware of the phishing campaigns and issued warnings about the phishing campaigns after 10-30 minutes. Employees were however still trying to access the malicious website after the official warning (latest attempt 64 hours after non-targeted and 3 hours after targeted attacks).
[Wright, Jensen, Thatcher, Dinger and Marett 2014] Phishing campaign at a university. IT staff was aware of the phishing campaign.	Experiment *2,624 students*	6.8 percent of subjects provided their credentials. Participants were less vulnerable to phishing influence techniques that relied on fictitious prior shared experience and were more vulnerable to techniques offering a high level of self-determination.
[Clark 2012] Investigating the degree to which privacy preserving technologies can protect an organization against attacks, including phishing.	Case study (survey and experiment) *160 participants*	92 participants (58 percent) fell victim to the phishing campaign.
[Dodge, Coronges and Rovira 2012] Impact of information security training to phishing susceptibility.	Experiment *892 employees*	The results indicate that over very short periods of time (10 days), there is no significant difference in susceptibility based on training. However, over longer periods (63 days) of time, training does contribute significantly to the reduction in susceptibility.

[Mohebzada, Zarka, Bhojani and Darwish 2012] Phishing campaigns in university community.	Experiments *10,917 academics (faculty, students, alumni)*	First experiment: 8.74 percent of subjects provided their credentials. 18 hours after experiment the subjects were sent warnings by the IT department. 114 subjects still provided their credentials afterwards. Second experiment: 2 percent of subject failed to detect the phishing campaign. IT department sent a warning 2 hours after the phishing attack. 90 subjects fell for the phishing attack afterwards.
[Wang et al. 2012] Study examines how users' attention to visual triggers and phishing deception indicators influence their decision-making processes.	Survey *321 members of a public university community*	Results of the study suggest that an individual's response to a phishing e-mail is most influenced by visceral triggers and deception indicators.
[Egelman, Cranor and Hong 2008] Impact of web browser phishing warnings to phishing susceptibility.	Experiment *60 employees*	Study found that 97 percent of participants fell for at least one of the phishing e-mail messages, 79 percent of participants heeded active warnings.
[Kumaraguru, Sheng, Acquisti, Cranor and Hong 2008] Impact of different training approaches to phishing susceptibility in real-world conditions.	Case study *311 employees*	A large percentage of individuals who clicked on links in simulated e-mail messages proceeded to give some form of personal information to fake phishing websites. Individuals trained with spear phishing training material did not make better decisions in identifying spear phishing e-mail messages. Employees in technical jobs were not different from employees with non-technical jobs.
[Workman 2008] Simulation of a phishing campaign at a government-regulated services organization involved in the insurance and financial industries. Pretexts were made with telephone calls to subjects where student actors pretended to be various officials, internal employees, employees of trading partners, customers, utility companies, and financial institutions, and solicited confidential information using the study range of persuasive techniques.	Case study (survey and observation) *588 employees*	People who are high in normative commitment feel obligated to reciprocate social engineering gestures and favors by giving up information. People who are high in continuance commitment tend to provide information to escalating requests. High affective commitment individuals tend to provide information because they want to be part of a socially desirable group or to be accepted. People who are trusting were more likely to fall victim to social engineering more than those who are distrusting. Higher degrees of obedience to authority were an important factor in whether people responded to social engineering attacks incorporating authoritative commands and fear tactics.

Table 2: Summary of papers included in the literature review

Most research on spear phishing focuses on how individuals react to spear phishing messages rather than how organizations react (i.e., detect and respond) to spear phishing campaigns. Studies frequently focus on the effectiveness of spear phishing in terms of click rates (i.e., the number of clicks on URLs in fraudulent messages in relation to the total number of sent phishing messages) and meaningful interaction (e.g., relevant user input, install of fraudulent software) [Bakar et al. 2017, Benenson et al. 2017, Bullee et al. 2017, Burns et al. 2019, Clark 2012, Goel et al. 2017, Gordon et al. 2019, Halevi, Memon and Nov 2015, Harrison et al. 2016, Holm et al. 2014, Mohebzada et al. 2012, Musuva et al. 2019, Sokol et al. 2017, Williams et al. 2018]. Additionally, only a limited number of real-world spear phishing studies in industrial settings can be found in the literature [Bakhshi 2017, Bullee et al. 2017, Burns et al. 2019, Caputo et al. 2014, Dodge et al. 2012, Egelman et al. 2008, Gordon et al. 2019, Holm et al. 2014, Kumaraguru et al. 2008, McElwee et al. 2018, Rocha Flores et al. 2015, Sokol et al. 2017, Williams et al. 2018, Workman 2008].

Analysis beyond click rates is further hindered by research methods issues, such as poorly designed quasi-experiments [Benenson et al. 2017, Bossetta 2018]. Our analysis of the literature shows that click rates vary quite substantially, i.e., from 1.7 percent [Musuva et al. 2019] to 97 percent [Egelman et al. 2008]. In industrial settings, click rates vary slightly less, i.e., from 3.4 percent [Sokol et al. 2017] to 62.5 percent [Halevi et al. 2015]. The causes for such extreme variations in click rates may be sought in the message content, research methods, demographics of the targeted population, message content, timing and frequency of messages (e.g., number of e-mails sent to an individual) etc. Click rates are most affected by persuasiveness combined with reputation mechanisms and other cues that cause the recipient to recognize a fraudulent message as legitimate (e.g., plausibility of the message content, recognizability of the message design, recognizability of the sender) [Yates and Harris 2015]. Since social engineering attacks are becoming increasingly sophisticated [Krombholz et al. 2015], poor message quality is a serious flaw calling for studies that focus more on accurate replications of the advanced phishing attacks frequently witnessed recently.

There seems to be a significant lack of a systematic analysis beyond the click rates. Some quasi-experiment studies researched factors affecting the vulnerability of individuals to spear phishing attacks [Benenson et al. 2017, Canfield et al. 2016, Caputo et al. 2014, Chuchuen and Chanvarasuth 2015, De Kimpe et al. 2018, Goel et al. 2017, Harrison et al. 2016, Heartfield et al. 2016, Martin et al. 2018, Musuva et al. 2019, Neupane et al. 2018, Oliveira et al. 2017, Wang et al. 2012, Williams et al. 2018, Workman 2008, Wright et al. 2014]. Most surveys focused primarily on demographic factors, and results are not uniform. While some results suggest that females are more susceptible to phishing-type attacks than males [Goel et al. 2017, Oliveira et al. 2017], others found no statistical difference between genders [Benenson et al. 2017, Martin et al. 2018], even though some older studies show that demographic factor significantly influence the susceptibility to phishing-type attacks [Sheng, Holbrook, Kumaraguru, Cranor and Downs 2010, Wang et al. 2012]. The inconsistency of the results can be further seen in the susceptibility of individuals coming from different professional or academic backgrounds. Researchers found significant differences between students of business and social sciences, and humanities (the latter were less susceptible for phishing-type attacks) [Goel et al. 2017] while no significant differences have been observed between technical and non-technical jobs [Kumaraguru et al. 2008]. Studies focusing on factors other than demographics, include testing training frameworks [Caputo et al. 2014, Carella et al. 2017, Dodge et al. 2012, Gordon et al. 2019, Heartfield et al. 2016, Kumaraguru et al. 2008, McElwee et al. 2018], autism [Neupane et al. 2018], work related norms and routines [Williams et al. 2018], political orientation [Bossetta 2018], and decisional heuristics [Benenson et al. 2017].

Some studies provide some insights on how employees responded to fraudulent e-mail messages by reporting them to the IT department [Bakhshi 2017, Holm et al. 2014]. From 49 targeted individuals (click rate was 46 percent), only two reported the phishing attack to the IT department. Generally, research shows a high share of employees failing to recognize phishing attacks and very few of them reporting a detected phishing attack. Research suggests that company-wide warnings about phishing campaigns may not be effective as users still get phished after their issue (e.g., warnings issued after 10-30 minutes and attempts to access a phishing website continued until 64 hours after non-targeted and 3 hours after targeted attacks [Holm et al. 2014], warnings issued 18 hours and 2 hours after the experiments, 114 (12 percent) and 90 (41 percent) subjects, respectively, provided fell for the phishing attack afterwards [Mohebzada et al. 2012]). No studies have been found however studying how IT departments react to employees' reports of phishing attacks.

4 Methodology

In this section, we first present the ethical considerations of the presented research. Next, we present the case study and its context, the phishing website and e-mail setup, and the phishing campaign.

4.1 Ethical considerations

Phishing-type attacks include multiple discrete steps [Goel et al. 2017] and are by their definition based on impersonation and deception. Jakobsson et al. [Jakobsson, Johnson and Johnson 2008, Jakobsson and Ratkiewicz 2006] discussed the ethics of such studies in detail and come to conclusion that real-world testing without the respondents consent and without debriefing can be permissible. However, this statement in its narrowest sense could be controversial [Benenson et al. 2017]. In order to perform a case study simulating real-world conditions in industrial settings, the research was conducted in confidence with an ethical and legal approval obtained from the Chief executive officer (CEO) and the Project manager responsible for implementation of security standards (hereafter Project manager) in the form of written non-disclosure agreement (NDA). The CEO and Project manager were the only Manco employees that had any knowledge about the case study and the planned phishing campaign. The NDA also included details about the research methodology, invasion level of the attacks, number of e-mails that could be sent, handling data during the research and after the research was finished.

4.2 Case study

A case study was used as research approach due to several reasons. First, it is appropriate for investigating contemporary events with no control over the environment. Next, it is suitable for studying events in natural organizational settings. The unit of analysis was a targeted phishing attack on a large Central European manufacturing company Manco (a fake company name due to the NDA). Manco has approximately 1,200 employees out of which 407 employees (e.g., accounting, human resources, IT department etc.) use their e-mail daily as most employees are working in manufacturing and only rarely use their work e-mails if at all. The list of employees that use e-mail regularly was provided to the researchers by Manco. Employees who used e-mail regularly had general information security training during a project aiming at the implementation of security standards in December 2018. News on online threats were regularly published on the internal company portal and in the company's internal newsletter monthly to raise the awareness of Manco's employees. Manco however did not conduct regular awareness trainings before the security standards project or afterwards.

The researchers learned about a recent update of the job classification system at Manco and prepared a phishing backstory about some issues during the update. First, the targeted phishing attack included the registration of a domain name mimicking the Manco's original domain name. The fake domain name had a duplicated first letter (e.g., *mmanco.eu* instead of *manco.eu*). On the fake domain, a phishing website with an input form supporting the phishing backstory was set up. The phishing website contained center-aligned company logo at the top of the page. In the middle of the page was an input form with three fields (i.e., first name, last name, department), accompanying consent text (i.e., "I agree to the processing of my data collected with this form") and a submit button. The phishing website was prepared in the native language of employees however it was not designed to resemble any of the existing pages that employees use daily. A redirect to the real Manco's website was additionally set up from any URL other than the phishing website on the fake domain name including any errors (e.g., HTTP 404 Not Found).

Next, a phishing e-mail has been prepared (see Table 3). The phishing e-mail was based on the phishing backstory and included the key elements of an effective phishing e-mail, namely an issue, a solution, a sense of urgency and an authoritative sender. It appeared to come from the CEO asking the employees to follow the provided link and fill in the form with their personal data. The e-mail design (font style and size, signature text and image) followed very closely the design of authentic e-mail. It contained only elements that could be obtained from any e-mail from the company (e.g., a customer support service reply, automated out-of-office reply). The phishing e-mail and website did not contain any attachments or malware.

Hello, Some information about your employment got mixed during the last update of the job classification system. Please enter your actual data as soon as possible using the form available <u>here</u>. Kind regards, [full CEO e-mail signature] [Manco company logo]

Table 3: Phishing e-mail

From the list of 407 e-mails of employees that use their e-mail daily, e-mails of the IT and HR departments staff, CEO and Project manager were removed. We removed IT department's e-mails to ensure ecological validity of studying their response to others' reports of phishing e-mails. HR department's e-mails were removed because of their insight into the phishing backstory which would compromise their susceptibility. CEO's and Project manager's e-mails were removed as they knew about the phishing campaign. To achieve an adequate degree of randomization, a unique random number was generated for each of the remaining 391 e-mails. The list of e-mails was then sorted by the random number.

A fake e-mail address *f.lastname@mmanco.eu* (*f* – first name initial) was created for the CEO at the fake domain following the pattern used by Manco. The phishing campaign was launched on one of the Tuesdays in January 2019. Phishing e-mails were sent one-by-one following the sorted list of e-mails. A total of 49 phishing e-mails were sent from 8:35 AM to 9:35 AM (CET). One e-mail was sent every 73.5 seconds on average to avoid any automated network alarms.

Data were collected through server logs, a database collecting submitted data, written reports by IT staff, project documentation (e.g., security training materials) and the follow-up meeting between the IT department, the project manager and the researchers. Data from different sources was triangulated and any discrepancies were discussed at the follow-up meeting.

5 Results

Results are presented in two parts. In the first subsection, we present the susceptibility of targeted employees to phishing e-mails in terms of the click rate and personal data input rate. Additionally, we provide insights into the average response time and the amount of different IP addresses exposed during the campaign. In the second subsection, we present the detection and response to the phishing campaign by Manco employees.

5.1 Phishing susceptibility

The first visit of the phishing website by a target was recorded 5 minutes after the first phishing e-mail was sent. The last visit of the phishing website was 248 minutes later. During this period, 34 unique targets clicked the URL in the phishing e-mail providing for a click rate of 69.4 percent. From the targets that clicked the URL, 27 unique targets submitted data through the form (55.1 percent of all targets) and at least 24 unique targets submitted their real personal data (49.0 percent of all targets). In two cases the submission form failed to record the submitted data and in one case the target submitted irrelevant data. At least 24 unique targets out of 34 that clicked the URL (70.6 percent) therefore submitted their real data.

The average response time of targets (i.e., time between sending the phishing e-mail and visiting the phishing website) was 20 minutes. The shortest response time was 25 seconds and the longest 203 minutes. The response times of only 3 targets were above 60 minutes. When excluding them from the calculation, the average response time was 10 minutes.

Manco uses a single public IP address. All except two targeted employees accessed the phishing website from Manco's public IP address. One of them accessed the phishing website from 5 different IP addresses and devices in addition to the first access from Manco's public IP address. He also submitted fake data and is the only confirmed case of fake data submission in the phishing campaign. A total of 7 different IP addresses from which the phishing website was accessed were recorded.

5.2 Phishing campaign detection and response

The IT department had the primary responsibility for responding to cyberattacks on Manco, including phishing campaigns. The e-mail server administrator from the IT department received the first report of a suspicious e-mail 15 minutes after the start of the phishing campaign. The report was filed by a target after examining the phishing e-mail and website for approximately 11 minutes. The e-mail server administrator started investigating right away the e-mail header, the fake domain name (e.g., registration details, owner, IP address) etc. and found out that the domain was registered to one of the authors of this paper through his research institution. As the author is a cybersecurity expert, the e-mail server administrator considered two key scenarios. Either Manco was being tested with a cyberattack (either independently or by being hired) or it was a part of an indirect cyberattack via a hacked cybersecurity researcher. The e-mail server administrator established that the attack should be taken as seriously as possible in any of his scenarios. He started preparing an urgent newsletter regarding the phishing e-mails to be forwarded to the Department of corporate communications which handled all company-wide communication.

In the meantime, the Chief information officer (CIO) got the first report of a suspicious e-mail during a meeting 33 minutes after the start of the phishing campaign. After being contacted also by the e-mail server administrator, a short briefing of the IT department staff is held 4 minutes later. At the briefing, the IT department staff determined that there have been four reports of suspicious e-mails and agree on the course of action to be taken. Other employees reported the phishing e-mails later however the IT department staff did not pay any special attention to them anymore as they assumed that they were all related to the on-going phishing attack. The IT department staff then double-checked for any information on the registered domain in-house (i.e., for testing or running projects) and at a third-party Manco website provider.

Incoming e-mails from the fake domain or IP address were blocked on the mail relay 85 minutes after the start of the phishing campaign which is 25 minutes after the last phishing e-mail was sent. Approximately at the same time, the firewall administrator contacted the national CERT by phone. They were notified about the phishing campaign however no specific action has been made on their part. The national CERT informed the IT staff that the incident needs to be reported separately to the Police if they wished to as they are not authorized to forward their report to them. The e-mail server administrator then contacted the CEO and reported to him about the incident and their response. The CEO did not remember that he approved the phishing campaign a couple of months earlier which enabled the case to continue uninterrupted. The firewall and e-mail server administrators contacted the Police who asked them to report the incident at the Police station in person. Reporting of the phishing campaign to the Police was first delayed and finally never done due to on-going activities and a lack of authorization of both administrators to submit it.

The Department of corporate communications issued an alert for all employees 100 minutes after the start of the phishing campaign. 5 minutes later the firewall and e-mail server administrators called one of the authors of this paper. A few minutes later the situation has been cleared up when the Project manager calls both the CEO and the CIO.

Even though the employees have been alerted and the e-mail domain has been blocked, 4 targeted employees submitted data through the phishing website afterwards. Out of them, 3 real personal data submissions have been recorded with the latest real data being submitted 253 minutes after the start of the phishing campaign which is 153 minutes after the company-wide alert regarding the phishing campaign.

6 Discussion

6.1 Theoretical implications

This study has several theoretical contributions. To the best of our knowledge, this is the first paper that studies a company's response (e.g., response time, protocols followed, actual behavior) to a real-world phishing campaign in industrial settings. The results revealed a very fast detection of the spear phishing campaign (first report was 15 minutes after the start of the spear phishing campaign) and a relatively short response time (all key countermeasures were taken within 100 minutes) of the IT department whose staff strictly followed the emergency protocol. Nevertheless, the consequences of the phishing campaign would be devastating if the attack would involve a specially prepared phishing website that could potentially infect up to 39 devices with malware by sending 49 phishing e-mails.

First, the case study showed that a phishing campaign can be successful even if the targeted organization's response time is very short. High click rates characteristic for targeted and spear phishing e-mails coupled with short response times of targets are a lethal combination that outweigh the ability to respond in a timely manner. 17 respondents (34.7 percent) clicked on the URL less than 2 minutes after receiving the e-mail and 4 respondents (8.2 percent) did so before a single minute has passed. Such short response times make it impossible to mitigate the cyberattack in real time by the IT department and call for automated solutions for first response.

Second, the phishing campaign may not be effective only due to the susceptibility of targets but also due to the investigative techniques of the first responders. The targeted employee that first reported his phishing e-mail to the IT department later joined the IT department staff in inspecting the phishing e-mails and website. They together accessed the phishing website from different devices from the Manco network and from outside. In addition to exposing 5 additional IP addresses related to Manco's employees they also accessed the phishing website without the necessary precautions (e.g., using a sandbox) potentially infecting 5 additional devices.

Third, we established the need for better classification of phishing-type attacks due to varying definitions that can be found in the literature, especially for phishing-type attacks that involve personalization of messages. We propose to distinguish three key types of phishing in ascending degree of personalization and context-awareness: blanket phishing, targeted phishing and spear phishing. The removal of ambiguity contributes to better understanding of phishing-type attacks and poses a basis for future research on phishing.

6.2 Practical implications

The results of this study have several practical implications for different stakeholders in phishing campaign resilience. First, employee training on phishing-type attacks is essential to lower click rates. Even though it would be utopian to expect employees to detect all phishing e-mails, lowering the click rates would improve most the resilience to phishing campaigns as even the best technical measures and response procedures may not be effective at the cyberattack front-line.

Second, adequate protocols and tools (e.g., virtual machines, sandboxes, anonymous network connections) need to be readily available to first responders for investigating phishing e-mails and websites. The results showed that an inadequate investigation led to an unnecessary data leak and potential exposure of additional devices to the attackers.

Third, the IT department staff stopped paying attention to reports on phishing e-mails after the first few ones. This could expose the organization to a second (or more), parallel, phishing campaign(s) that may be carefully coordinated with the first one. Terrorists frequently use a similar concept in double bombings. The purpose of setting off the first bomb is to gather people interested to check out the situation around the scene of the bombing. After a crowd has gathered, the second bomb is set off usually causing significantly more damage and victims. Similarly, the phishing campaign may be just a diversion for the IT department to focus on while a second cyberattack (e.g., another phishing campaign impersonating the IT department staff) may take place. Therefore, the IT department staff should pay attention to all reported incidents and not assume that all reports that come in a certain time period is related to the same cyberattack.

Fourth, a technical solution may help targeted employees to consider e-mails seemingly coming from organizational insiders more thoroughly. For example, an e-mail could be marked if the e-mail address of the sender matches or closely resembles an existing organizational e-mail address. Such a note may draw enough attention from the targeted employee that he would consider for longer if an e-mail is legitimate or not.

Fifth, the case study showed that testing response protocols in practice may contribute to their improvements. Even though Manco had robust cyberattack response protocols that were consistently followed, the phishing campaign exposed some weaknesses of the response protocol that could be improved. Conducting the phishing campaign also helped to raise awareness of employees regarding phishing-type attacks and could be considered as a form of cyberattack response training.

6.3 Limitations and future work

There are some limitations of this case study that the reader should note. First, the case study was conducted in industrial settings in Central Europe. A similar study in other settings and cultural background may produce different results. Conducting an experiment in industrial settings would help shed more light on the factors affecting the susceptibility of company employees. It would be also beneficial to conduct a sequence of different phishing campaigns (e.g., different phishing sites, timings, degrees of personalization of messages) to determine how organizations react to them. This would help improve phishing training for employees.

7 Conclusion

We conducted a case study in a large Central European manufacturing company to test its resilience and response to phishing campaigns. The results of our study contribute to the knowledge on how organizations detect and respond to spear phishing campaigns. Phishing campaign may be successful even if the response time of the organization is short calling for automated solutions for phishing response, possibly including some degree of human interaction, e.g., as one of the best detectors of new (zero-day) spear phishing e-mails. Employee detection seems to be a key issue as not all employees are able to detect phishing e-mails. Therefore, training on phishing-type attacks would be beneficial although training is not always effective. The success of a phishing campaign may also depend on the response from the IT department (e.g., investigative techniques, paying attention to all reports of phishing e-mails). The IT department needs to be adequately trained to investigate and respond to phishing campaigns, possibly with training by conducting phishing campaigns by third parties. These insights may help organizations better prepare for phishing attacks and especially their responses to them.

References

[Bakar, Mohd and Sulaiman 2017] Bakar, N. A., Mohd, M., Sulaiman, R.: 'Information leakage preventive training'; In 2017 6th International Conference on Electrical Engineering and Informatics (ICEEI). IEEE (2017), pp. 1–6. https://doi.org/10.1109/ICEEI.2017.8312403

[Bakhshi 2017] Bakhshi, T.: 'Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors'; In 2017 13th International Conference on Emerging Technologies (ICET). IEEE (2017), pp. 1–6. https://doi.org/10.1109/ICET.2017.8281653

[Benenson, Gassmann and Landwirth 2017] Benenson, Z., Gassmann, F., Landwirth, R.: 'Unpacking Spear Phishing Susceptibility'; In International Conference on Financial Cryptography and Data Security (FC 2017) (2017), pp. 610–627. https://doi.org/10.1007/978-3-319-70278-0_39

[Bossetta 2018] Bossetta, M.: 'A simulated cyberattack on Twitter: Assessing partisan vulnerability to spear phishing and disinformation ahead of the 2018 U.S. midterm elections'; First Monday, Vol. 23, No. 12 (2018), pp. 1–23. https://doi.org/10.5210/fm.v23i12.9540

[Bullee, Montoya, Junger and Hartel 2017] Bullee, J.-W., Montoya, L., Junger, M., Hartel, P.: 'Spear phishing in organisations explained'; Information and Computer Security, Vol. 25, No. 5 (2017), pp. 593–613. https://doi.org/10.1108/ICS-03-2017-0009

[Burns, Johnson and Caputo 2019] Burns, A. J., Johnson, M. E., Caputo, D. D.: 'Spear phishing in a barrel: Insights from a targeted phishing campaign'; Journal of Organizational Computing and Electronic Commerce, Vol. 29, No. 1 (2019), pp. 24–39. https://doi.org/10.1080/10919392.2019.1552745

[Caldwell 2013] Caldwell, T.: ‘Spear-phishing: how to spot and mitigate the menace’; Computer Fraud & Security, Vol. 2013, No. 1 (2013), pp. 11–16. https://doi.org/10.1016/S1361-3723(13)70007-1

[Canfield, Fischhoff and Davis 2016] Canfield, C. I., Fischhoff, B., Davis, A.: ‘Quantifying Phishing Susceptibility for Detection and Behavior Decisions’; Human Factors: The Journal of the Human Factors and Ergonomics Society, Vol. 58, No. 8 (2016), pp. 1158–1172. https://doi.org/10.1177/0018720816665025

[Caputo, Pfleeger, Freeman and Johnson 2014] Caputo, D. D., Pfleeger, S. L., Freeman, J. D., Johnson, M. E.: ‘Going Spear Phishing: Exploring Embedded Training and Awareness’; IEEE Security & Privacy, Vol. 12, No. 1 (2014), pp. 28–38. https://doi.org/10.1109/MSP.2013.106

[Carella, Kotsoev and Truta 2017] Carella, A., Kotsoev, M., Truta, T. M.: ‘Impact of security awareness training on phishing click-through rates’; In 2017 IEEE International Conference on Big Data (Big Data). IEEE (2017), pp. 4458–4466. https://doi.org/10.1109/BigData.2017.8258485

[Chuchuen and Chanvarasuth 2015] Chuchuen, C., Chanvarasuth, P.: ‘Relationship between phishing techniques and user personality model of Bangkok internet users’; Kasetsart Journal - Social Sciences, Vol. 36, No. 2 (2015), pp. 322–334.

[Clark 2012] Clark, J. W.: ‘Everything But the Kitchen Sink: Determining the Effect of Multiple Attacks on Privacy Preserving Technology Users’; In Nordic Conference on Secure IT Systems (NordSec 2012) (2012), pp. 199–214. https://doi.org/10.1007/978-3-642-34210-3_14

[De Kimpe, Walrave, Hardyns, Pauwels and Ponnet 2018] De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., Ponnet, K.: ‘You’ve got mail! Explaining individual differences in becoming a phishing target’; Telematics and Informatics, Vol. 35, No. 5 (2018), pp. 1277–1287. https://doi.org/10.1016/j.tele.2018.02.009

[Dodge, Coronges and Rovira 2012] Dodge, R., Coronges, K., Rovira, E.: ‘Empirical Benefits of Training to Phishing Susceptibility’; In IFIP International Information Security Conference (SEC 2012) (2012), pp. 457–464. https://doi.org/10.1007/978-3-642-30436-1_37

[Downs, Holbrook and Cranor 2006] Downs, J. S., Holbrook, M. B., Cranor, L. F.: ‘Decision Strategies and Susceptibility to Phishing’; In Symposium on usable privacy and security. Pittsburgh, PA (2006), pp. 1–12.

[Egelman, Cranor and Hong 2008] Egelman, S., Cranor, L. F., Hong, J.: ‘You’ve been warned: An empirical study of the effectiveness of web browser phishing warnings’; In Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems - CHI ’08. ACM Press (2008), p. 1065. https://doi.org/10.1145/1357054.1357219

[Felix and Hauck 1987] Felix, J., Hauck, C.: ‘System Security: A Hacker’s Perspective’; In Proceedings of the 1987 North American conference of Hewlett-Packard business computer users (1987).

[FireEye 2016] FireEye: ‘Spear-phishing attacks: why they are successful and how to stop them’; (2016).

[Goel, Williams and Dincelli 2017] Goel, S., Williams, K., Dincelli, E.: ‘Got Phished? Internet Security and Human Vulnerability’; Journal of the Association for Information Systems, Vol. 18, No. 1 (2017), pp. 22–44.

[Gordon, Wright, Aiyagari, Corbo, Glynn, Kadakia, et al. 2019] Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., et al.: 'Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions'; JAMA Network Open, Vol. 2, No. 3 (2019), p. e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

[Halevi, Memon and Nov 2015] Halevi, T., Memon, N., Nov, O.: 'Spear-Phishing in the Wild : A Real-World Study of Personality , Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks'; (2015).

[Harrison, Svetieva and Vishwanath 2016] Harrison, B., Svetieva, E., Vishwanath, A.: 'Individual processing of phishing emails'; Online Information Review, Vol. 40, No. 2 (2016), pp. 265–281. https://doi.org/10.1108/OIR-04-2015-0106

[Heartfield and Loukas 2015] Heartfield, R., Loukas, G.: 'A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks'; ACM Computing Surveys, Vol. 48, No. 3 (2015), pp. 1–39. https://doi.org/10.1145/2835375

[Heartfield, Loukas and Gan 2016] Heartfield, R., Loukas, G., Gan, D.: 'You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks'; IEEE Access, Vol. 4 (2016), pp. 6910–6928. https://doi.org/10.1109/ACCESS.2016.2616285

[Holm, Rocha Flores, Nohlberg and Ekstedt 2014] Holm, H., Rocha Flores, W., Nohlberg, M., Ekstedt, M.: 'An Empirical Investigation of the Effect of Target-Related Information in Phishing Attacks'; In 2014 IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations. IEEE (2014), pp. 357–363. https://doi.org/10.1109/EDOCW.2014.59

[Hong 2012] Hong, J.: 'The state of phishing attacks'; Communications of the ACM, Vol. 55, No. 1 (2012), p. 74. https://doi.org/10.1145/2063176.2063197

[Jakobsson, Johnson and Johnson 2008] Jakobsson, M., Johnson, P. F., Johnson, N.: 'Why and How to Perform Fraud Experiments'; IEEE Security & Privacy, , No. 2 (2008), pp. 66–68. https://doi.org/10.1109/MSP.2008.52

[Jakobsson and Myers 2007] Jakobsson, M., Myers, S.: 'Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft'; New Jersey: John Wiley & Sons, Inc. (2007).

[Jakobsson and Ratkiewicz 2006] Jakobsson, M., Ratkiewicz, J.: 'Designing Ethical Phishing Experiments : A study of (ROT13) rOnl query features'; In WWW. ACM Press (2006), pp. 1–10.

[Krombholz, Hobel, Huber and Weippl 2015] Krombholz, K., Hobel, H., Huber, M., Weippl, E.: 'Advanced social engineering attacks'; Journal of Information Security and Applications, Vol. 22 (2015), pp. 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

[Kumaraguru, Sheng, Acquisti, Cranor and Hong 2008] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., Hong, J.: 'Lessons from a real world evaluation of anti-phishing training'; In 2008 eCrime Researchers Summit. IEEE (2008), pp. 1–12. https://doi.org/10.1109/ECRIME.2008.4696970

[Lastdrager 2014] Lastdrager, E.: 'Achieving a consensual definition of phishing based on a systematic review of the literature'; Crime Science, Vol. 9, No. 3 (2014), pp. 1–10. https://doi.org/10.1186/s40163-014-0009-y

[Martin, Dubé and Coovert 2018] Martin, J., Dubé, C., Coovert, M. D.: 'Signal Detection Theory (SDT) Is Effective for Modeling User Behavior Toward Phishing and Spear-Phishing Attacks'; Human Factors: The Journal of the Human Factors and Ergonomics Society, Vol. 60, No. 8 (2018), pp. 1179–1191. https://doi.org/10.1177/0018720818789818

[McElwee, Murphy and Shelton 2018] McElwee, S., Murphy, G., Shelton, P.: 'Influencing Outcomes and Behaviors in Simulated Phishing Exercises'; In SoutheastCon 2018. IEEE (2018), pp. 1–6. https://doi.org/10.1109/SECON.2018.8479109

[Mohebzada, Zarka, Bhojani and Darwish 2012] Mohebzada, J. G., Zarka, A. El, Bhojani, A. H., Darwish, A.: 'Phishing in a university community: Two large scale phishing experiments'; In 2012 International Conference on Innovations in Information Technology (IIT). IEEE (2012), pp. 249–254. https://doi.org/10.1109/INNOVATIONS.2012.6207742

[Musuva, Getao and Chepken 2019] Musuva, P. M. W., Getao, K. W., Chepken, C. K.: 'A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility'; Computers in Human Behavior, Vol. 94 (2019), pp. 154–175. https://doi.org/10.1016/j.chb.2018.12.036

[Neupane, Satvat, Saxena, Stavrinos and Johnson Bishop 2018] Neupane, A., Satvat, K., Saxena, N., Stavrinos, D., Johnson Bishop, H.: 'Do Social Disorders Facilitate Social Engineering? A Case Study of Autism and Phishing Attacks A Case Study of Autism and Phishing Attacks'; In COMPUTER SECURITY APPLICATIONS CONFERENCE (2018), pp. 467–477. https://doi.org/10.1145/3274694.3274730

[Nguyen 2013] Nguyen, V.: 'Attribution of Spear Phishing Attacks : A Literature Survey'; Edinburgh (2013).

[Olifer, Goranin, Kaceniauskas and Cenys 2017] Olifer, D., Goranin, N., Kaceniauskas, A., Cenys, A.: 'Controls-based approach for evaluation of information security standards implementation costs'; Technologial and Economic Development of Economy, Vol. 23, No. 1 (2017), pp. 196–219. https://doi.org/10.3846/20294913.2017.1280558

[Oliveira, Ebner, Rocha, Yang, Ellis, Dommaraju, et al. 2017] Oliveira, D., Ebner, N., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., et al.: 'Dissecting Spear Phishing Emails for Older vs Young Adults'; In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17 (2017), pp. 6412–6424. https://doi.org/10.1145/3025453.3025831

[Parmar 2012] Parmar, B.: 'Protecting against spear-phishing'; Computer Fraud & Security, Vol. 2012, No. 1 (2012), pp. 8–11. https://doi.org/10.1016/S1361-3723(12)70007-6

[Rocha Flores, Holm, Nohlberg and Ekstedt 2015] Rocha Flores, W., Holm, H., Nohlberg, M., Ekstedt, M.: 'Investigating personal determinants of phishing and the effect of national culture'; Information and Computer Security, Vol. 23, No. 2 (2015), pp. 178–199. https://doi.org/10.1108/ICS-05-2014-0029

[Sheng, Holbrook, Kumaraguru, Cranor and Downs 2010] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., Downs, J.: 'Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions'; In Conference on Human Factors in Computing Systems. Atlanta, Georgia: ACM Press (2010), pp. 1–10.

[Sokol, Glova and Mezešova 2017] Sokol, P., Glova, M., Mezešova, T.: 'Lessons Learned from Phishing Test'; In P. Doucek, G. Chroust & V. Oškrdal (Eds.), Digitalization in Management, Society and Economy (2017), pp. 297–304.

[Steer 2017] Steer, J.: 'Defending against spear-phishing'; Computer Fraud & Security Bulletin, Vol. 2017, No. 8 (2017), pp. 18–20. https://doi.org/10.1016/S1361-3723(17)30074-X

[Symantec 2018] Symantec: 'Internet Security Threat Report'; (2018).

[Wang, Herath, Chen, Vishwanath and Rao 2012] Wang, J., Herath, T., Chen, R., Vishwanath, A., Rao, H. R.: 'Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email'; IEEE Transactions on Professional Communication, Vol. 55, No. 4 (2012), pp. 345–362. https://doi.org/10.1109/TPC.2012.2208392

[Williams, Hinds and Joinson 2018] Williams, E. J., Hinds, J., Joinson, A. N.: 'Exploring susceptibility to phishing in the workplace'; International Journal of Human Computer Studies, Vol. 120, No. June 2017 (2018), pp. 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

[Workman 2008] Workman, M.: 'Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security'; Journal of the American Society for Information Science and Technology, Vol. 59, No. 4 (2008), pp. 662–674. https://doi.org/10.1002/asi.20779

[Wright, Jensen, Thatcher, Dinger and Marett 2014] Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., Marett, K.: 'Research Note —Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance'; Information Systems Research, Vol. 25, No. 2 (2014), pp. 385–400. https://doi.org/10.1287/isre.2014.0522

[Yates and Harris 2015] Yates, D., Harris, A. L.: 'Phishing Attacks Over Time : A Longitudinal Study'; In Twenty-first Americas Conference on Information Systems. Puerto Rico (2015), pp. 1–6.