ROLE OF AWARENESS TO PREVENT PERSONAL DISASTERS: REDUCING THE RISKS OF FALLING FOR PHISHING BY STRENGTHENING USER AWARENESS

BETTINA ISER & ROMAN BRANDTWEINER
Vienna University of Economics and Business, Austria

ABSTRACT

Phishing still represents a main security threat in the digital world. Attackers primarily by means of email try to gain access to user's sensitive personal credentials. By using these credentials, attackers cause disasters on the individual level by inflicting, for example, severe economic losses or reputational damage due to identity theft. Awareness is one important factor to increase resilience. This paper based on recent literature first gives a general overview on social engineering as mean for phishing and then evaluates how awareness as preventive measure is considered effective in the selected literature. Information on phishing is one measure to raise awareness, others are trainings and phishing test campaigns to evaluate risk exposure and increase awareness. With regards on information sharing a case study, focusing on portals and homepages of selected Austrian financial institutions was conducted. In this case, study we emphasis on content and eventual differences in the presentation of information concerning prevention and mitigation.

Keywords: disaster prevention and mitigation, social engineering, phishing, risk awareness, security management.

1 INTRODUCTION

Phishing is a social engineering attack used by malicious threat agents in order to gain confidential logon information from users [1] either in companies as administrators or end users as bank users to commit identity theft and misuse the data for further attacks on company data or to commit fraud. Awareness of users is considered one measure to reduce the risk from disclosing sensible data to attackers [2]. In today's private and business life email is an important mean of digital communication and therefore an interesting attack vector for phishers directly targeting the end users.

Phishing mails are regularly sent to random target populations and leverage on victims being found within. The classic approach how phishers try to lure their victims to click on a malicious link is raising concerns/fear on user-side preventing them from being cautious, e.g. the text of the message refers to their account being blocked [3].

Starting from a general introduction on social engineering and phishing in general the paper will address awareness information on selected Austrian banking websites, search for available information regarding a trend about the phishing threat and based on literature evaluate the contribution of awareness to phishing prevention.

As visible on the phishing alerts on the selected internet portals and by Austrian cyber security organizations like Cert.at (Cyber Emergency Response Team Austria) phishing is a persistent threat to users in their digital communication.

2 RESEARCH QUESTION AND METHODOLOGY

Phishing represents a threat to users and companies concerning financial and reputational losses. Customers that in the course of a successful phishing campaign lost money not only consider the financial loss but may also loose the trust in their (financial) service providers [4].

WIT Transactions on The Built Environment, Vol 207, © 2021 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/DMAN210061

2.1 Research question

Following the persistent threat of experiencing personal disasters triggered by phishing this paper will address the following research question: How can user awareness as effective measure of risk mitigation lead to avoidance or at least to the reduction of losses from phishing hazards?

2.2 Methodology

The research was executed as desk research, therefore as methodology a systematic literature review [5] has been applied accompanied by statistics and information shared by law enforcement authorities with a focus on the Austrian market. Main literature sources will be scientific articles published not before 2010 and accessible via Web of Science and Google Scholar. Additionally, information from cases especially the awareness information available on the homepages of selected banks and other financial institutions in Austria will be evaluated and compared.

3 PHISHING AS A FORM OF SOCIAL ENGINEERING

Hong [1] states that the best security concepts applied on technical level are limited if "the person behind the keyboard falls for a phish". Phishing is considered the most widely spread of social engineering and addresses emails that either are sent in the forms of spam to a large group of recipients or could also be sent to target recipient groups [6].

Social engineering following Hadnagy [6] is defined as action that motivates somebody to perform an action that is to be considered as resulting in a disadvantage. The social engineers try to create an atmosphere of trust and relationship that motivates the victim to click, e.g. on a malicious link. Alternatively the social engineer is using curiosity, threat or authority to get the victim follow the intended link and to insert personal credential in, for example, the faked website [6].

The attacker usually claims to be someone else; such mails could claim to come from a bank, social media platforms or various other platforms requiring user credentials to logon. Sending those mails can be done at very low cost from the attackers [7]. Clicking on the phishing link directs the victim to a manipulated website where usually sensitive credentials as password and user-id are to be inserted. Having those collected, the attacker – often without being recognized by the victim – has access to the different services and can continue the fraudulent activities.

Sometimes the attackers create fear with the victim claiming to have recognized malicious activity on one of the payment accounts and asking for a logon in order to proceed with clean-up of the comprised accounts [3].

As Fig. 1 shows apart from fear there are other motivators that can attract users to follow malicious links in phishing mails [3]. Once having clicked on a link the victim either is asked to insert personal credentials or (unconsciously) downloads malware that then is used to gain access to user credentials and further misuse them. These motivators can repeatedly be found in research literature [8].

Hong [1] describes the anatomy of a phishing attack following a three phases approach. The first phase is sending out phishing mails to the targeted users. Here motivation factors as described in Fig. 1 are used to get the victims fall into it. Those phishing mails in many cases direct the users to phishing sites, faked websites, claiming to be another target website users there are requested to insert their credentials assuming they are on their target websites (e.g.

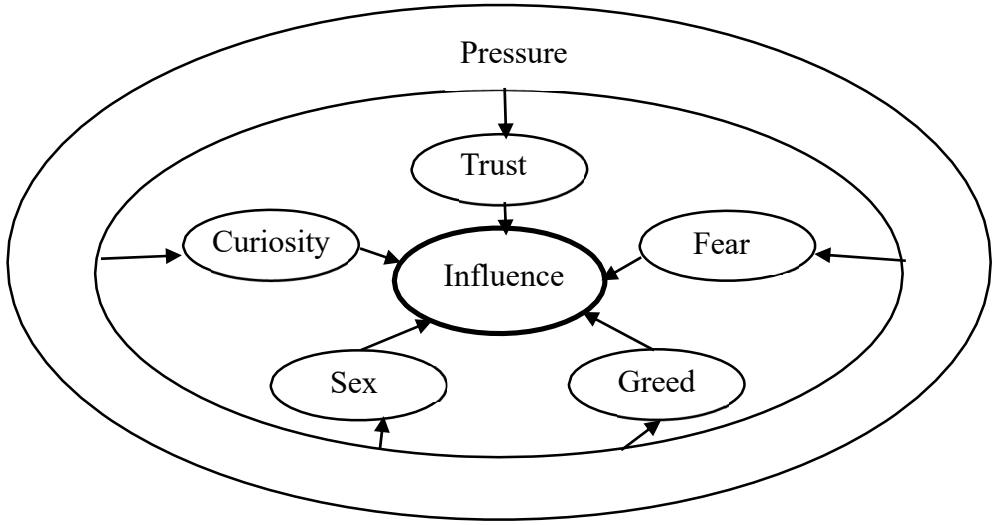

Figure 1: Motivators in social engineering [3].

their banking webpage) while instead are on a phishing site [4]. Meanwhile there exist services offered to institutions monitoring faked sites and supporting takedowns to mitigate the risk, what leads to attackers also leveraging on more enhanced and sophisticated technology. Last step of the attack is following this definition the monetarization of the stolen information, either by the attackers themselves or by the information being sold on illegal marketplaces to other criminals [1].

4 CURRENT SITUATION IN AUSTRIA

The Austrian CERT (Cyber Emergency Response Team) in its yearly report 2019 [9] identifies in the statistics of malicious web trends phishing and phishing sites as continuous threat.

Online services like Watchlist Internet [10] are additionally monitoring the phishing situation in Austria and providing updated information on their website.

In Austria, the Cyber Security Center of the Austrian Ministry of the Interior is permanently monitoring the situation of overall cybersecurity in Austria. In the respective monthly reports, the so-called *OpKoord (Operative Koordinierungsstruktur) Lagebericht* [11], a continuous trend of phishing is visible.

Throughout October, a series of phishing/SPAM waves is reported with faked postal or package deliveries – via mail as via messenger services like WhatsApp. Aim of those campaigns is to get logon credentials like payment information, e.g. credit or other payment data.

In the report of November a constant trend of phishing mails, e.g. on bank institutions or post are reported. In particular, as of end of October also a phishing campaign against users of *Finanz Online* was launched. *Finanz Online* is the official portal of the Austrian Ministry of Finance where Austrian citizens can submit their tax declarations. This phishing campaign was remarking a tax reimbursement of 1.850 Euro and linking to a phishing site where *Finanz Online* credentials were collected.

In December, the reports state an increasing number of phishing shops and phishing mails being sent around which following the report is regularly seen around Christmas time.

International research shows the continuous worldwide trend of phishing targeting end users and customers equally as employees in companies [12]. In addition, other research indicates that phishing will remain an important threat vector [13].

The global consortium "Anti Phishing Workgroup" (APWG) in a joint cooperation with users and companies providing security solutions or being in scope of phishing attacks monitor the global evolution of phishing. In its report on the third quarter of 2020, it considers a continuously high number of phishing sites. Additionally, it states that phishing sites increasingly (up to 2/3) are using SSL (secure socket layer) encryption (visible as "https://" at the beginning of URLs) to gain trust of the users [14].

5 RISK MITIGATION

Beißel [3] defines the focus of awareness to apply a set of tools and methods in order to increase the consciousness of users about malicious activities and to facilitate a desired behaviour in case of, for example a phishing attack. He defines three aspects on security-relevant behaviour that could be the desired or the not desired one: behaviour in line with the policies/rules, risk behaviour and behaviour in problematic situations.

Awareness measures could be distributed on various levels – could be print media, electronic media or also audio/video measures.

5.1 Approaches and measures to create awareness among users

Arachchilage and Love [13] in their study evaluated the self-efficacy of users to thwart from falling into phishing and see conceptual knowledge (know why) and procedural knowledge (know how) as positively influencing the threat avoidance and threat behaviour of users. Their study was considering younger users aged between 18 und 25. An age group that is often reported to be at higher risk to fall into phishing, eventually also due to minor experience [1].

With regards to awareness trainings, targeting training to users not yet sufficiently aware of the threat and avoiding "overtraining" is another aspect to be considered. The latter could result in non-fraudulent mails being misinterpreted as fraudulent [15].

Arachchilage and Love [13] identify a lack of user knowledge as a main reason for a successful attack. They propose a mix of information including even games to improve users' ability to thwart phishing attacks.

Research demonstrates that awareness among users is positively affecting the resilience and on detection capabilities of users. With increasing connectivity and use of smartphones there is identified a strong need to train people especially about phishing [16].

Ebot [8] introduces an additional aspect concerning phishing by identifying different stages that users might be in when clicking on phishing mails. This could be a potential explanation why, for example, in some evaluated literature awareness leads to less clicks and in others the perceived awareness leads users to be less cautious and click on malicious mails. Understanding the different stages and their characteristics would lead to a fine-tuned training and awareness approach allowing designing awareness based on the users current risk profile. In the study by Ebot [8], users are classified in three different stages when clicking on an email. Stage 1 refers to the naïve users, not experienced with IT and little knowledge. At this stage, the priority in trainings should be given to raising understanding of phishing and all and providing a solid background. Stage 2 includes users with already basic understanding on phishing that went through some training already. They would click on mails that do not

fall into standard phishing mails and have indicators that are not familiar to the users or are more complex to identify. For those users, simulated phishing mails and more detailed training on typical phishing indicators should be the priority. The last stage then covers users with a deep understanding that went through several programs and test phishing campaigns. In addition, such users still tap into phishing mails. For those users information should be kept reminded, also avoiding creating overconfidence leading to less awareness [8].

5.2 Raising user awareness: The case of Austrian financial services providers

Awareness can be considered as the first step towards a sustainable protection from phishing fraud since it helps to make the users aware of the risk and realize exposure to this threat [17]. Financial institutions and their customers are regular targets of phishing campaigns as the information shared on the homepages of selected Austrian financial institutions demonstrate.

Having a deeper look at the homepages of selected Austrian financial institutions: Erste Bank, BAWAG as established financial institutions and N26 as fintech gets visible that phishing is an important threat to banking users. All institutions provide information on phishing, most recent samples and tips how to prevent from falling into phishing [18], [19]. The review of the warnings shared on the different webpages shows that phishing campaigns are repeatedly started targeting customers of various institutions. The phishing campaigns are regularly adopted to actual topics as the case of COVID-19 or the implementation of the *Payment Services Directive 2* (PSD2) shows.

Butler and Butler [17] underline the importance of websites as a source of security awareness effort for financial institutions. The quality of phishing related information plays therefore an important role and can significantly contribute to help users identify phishing attacks and avoid from falling into them. However, there is also reference to online users not knowing where to find the related information or users actively seeking for such information. There is also reference to users not reading related information even when receiving clear recommendation on respective information sections [17].

Erste Bank und Sparkasse on their internet representation has a dedicated portal "*Sicherheits-Center*" to provide security information to the end users. The portal provides most recent warnings of ongoing phishing campaigns, tricks to increase security and contact information to get support in case of an incident or to report an attempted fraud.

The important security tips include an overview on the 10 most important rules for digital security. The three top rules are [20]:

- to open the internet banking only via verified webpages (visible in the URL);
- to protect logon information against access by third parties;
- to use dedicated special authorization method for login and signing.

The portal further includes details on phishing and how to recognize phishing mails. An example given are the checks of the sender mail-address as also checking the destination address. The information is supported by samples to increase recognition. The information is then followed also by guidelines how to behave in case fraudulent mails received and the request to share phishing mails with the fraud-service center.

In addition, BAWAG PSK has on its website not only a collection of most recent phishing campaigns but also recommendations how to keep online and mobile banking safe. Apart from warning of fraudulent mails there are also warnings on phishing SMS.

The portal warns on 16 September [21] from phishing mails in the context of PSD2, the updated payment directive introducing various additional Security features as one-time

password in addition to logon credentials. Fraudsters adopted their campaigns to be considered more trustworthy when claiming to be the respective institution and to provide information or requests for an update of logon data to its users. In addition, BAWAG asks its customers to report phishing mails to a dedicated mailbox.

N26, a Fintech offering its services in Austria, provides on its internet representation an overview on its security implementations as well as short information on phishing. The information displayed is kept shorter than on the homepages of the other institutions. It offers a security guide to be downloaded with a variety of information concerning security. The 10 important rules to safely use digital services are not focused on banking but include more general rules too, e.g. trusted sellers or careful use of unprotected Wi-Fi networks. In addition, the Fintech is asking its customers to report phishing mails or phishing sites to them [22].

Ebot [8] summarizes that in general the simple providing of information has limits with regard to user awareness. Users receive such information via books, emails or other types of instructions. Due to missing reciprocity and missing feedback, there is a lack of transforming such information into awareness. Therefore, recommendations go towards involving learning by doing and anti-phishing games.

5.3 Raising user awareness through regular test campaigns

Apart from information being provided there are different other possibilities to increase the awareness of users.

A few years ago Google has released an online test on phishing recognition accessible for any user [23]. It provides some samples of mails with embedded links or documents where the user needs to decide whether it is a legitimate mail or a phishing mail. For any answer there is then a walkthrough explaining the information embedded allowing to properly distinguishing valid from fake. This is accessible for anybody.

Within companies, simulated phishing attacks can be considered as an additional method to raise the awareness of users towards phishing attacks. As a second channel to raise awareness more related likely to a company perimeter are regular test phishing campaigns to detect weaknesses in employee awareness and provide targeted mitigation training.

Some authors, for example Jampen et al. [12], underline the importance of user awareness additional to countermeasures implemented on technical layers (e.g. spam filters). Key elements of institutional anti-phishing trainings are ranging from information material provided to the users, dedicated trainings or phishing simulations. In case of a phishing simulation, there are different steps feasible after a user fell into it. There could be immediately an information shown on phishing, and how to prevent it or the clicks could be monitored and users provided with dedicated trainings, which are then tracked. Which setting a company decides to apply depends also on risk–benefit evaluations.

Even more benefit could be gained if phishing awareness is embedded in a game format. Students are learning better from game based learning formats [16]. In case of phishing, it could be an option not to have the game purely online but in a combination of non-online and online. Non-online part could be used to identify potentially suspicious URLs what in the study revealed that certain combinations like URLs containing numbers, IP addresses or containing abbreviations are likely to be erroneously considered trustworthy by users [16], after a game walkthrough the recognition rate was more significantly higher. Additionally, crucial considered make users aware about how their data is being disclosed publicly. In this approach study participants not only had to respond to phishing but also to design by themselves phishing mails based on social information provided to them.

Purkait et al. [4] evaluated what kind of factors lead to users clicking on phishing mails and found that "the Internet user's level of phishing awareness, safe Internet habits, past experiences of being phished, years of performing financial activity over the Internet, short-term memory and attention vigilance are all positively related to his/her ability of identifying phishing sites. On the other hand, his/her age and frequency of online transactions had an inverse relationship with the same" [4, p. 22] Other evaluated criteria as technical experience, gender or family size in their study didn't have a significant impact on user's capability to identify a phishing website [4].

5.4 User awareness alone is not the solution

While various literature refers to user awareness being an important pillar of successful prevention against phishing [1], [16] there are remarks also on limitations with regards to awareness. Technical measures are equally important to reduce the risk from phishing. Such measures are transparent to the users and applied on infrastructure level [7] as with antispam solutions, web content filtering solutions or scanning solutions capable to identify malicious content in mail and quarantining the malicious content. Additionally, cooperation with security providers offering services to take down identified phishing sites [1], [12].

Ebot remarks that training might also create overconfidence with the users, feeling familiar with phishing threat and being too sure on recognizing phishing mails though overseeing less familiar indications in phishing mails [8].

The human element will remain in digital communication and there will remain a residual small percentage of users that despite technical measures and awareness programs will click on phishing mails and provide their credentials to fraudsters. Measurable, consistent and continuous awareness programs will contribute to minimizing this percentage [12].

6 LIMITATIONS

Within this paper, the whole industry of phishing and spamming, that from the literature chosen, can be considered as a significant malicious business domain [17] couldn't be further investigated in.

About the awareness measures taken by selected Austrian banks, we could consider only the information presented and shared on their homepages. It would be worth a further investigation on additional measures being imposed by the institutions such as ad hoc messages integrated with the mobile/online banking, eventual training possibilities for customers or active acknowledgement of customers about phishing updates being shared. Such measures would strongly increase the value and contribution to user awareness and represent a difference [17].

Even though law enforcement was not evaluated, it could represent an interesting additional aspect to understand possibilities and limitations of current law enforcement agencies to fight against the phishing industry considering national competences versus globally acting fraudsters and phishing sites distributed over the world.

Focus of this paper was on awareness of users as the parts of the protection chain and therefore excluded measures applied on technical level to prevent from phishing frauds. Such solutions – which were not discusses in thus paper – could be anti-spam filters or evolutions on browser side [1].

7 CONCLUSIONS

Considering the literature review and the data available from current phishing campaigns it can be summarized that phishing is a tremendous hazard, and will remain one. Even though

technical solutions are increasingly available to mitigate the risk of phishing, also fraudsters are adopting their approaches to become more efficient. Focusing purely on technology and not consider the user awareness will not be sufficient [13], [17].

Phishing allows attackers to target the user as the potentially weakest link in the chain [3] and by gaining legitimate access; credentials bypass various technical protection measures. In other scenarios, users are lured to access websites where they download malicious software putting at risk personal and company data. Further Security education and awareness measures allow reaching out to the end users, and motivating them to process emails more systematically and review certain criteria to determine potential phishing mails. Organizations nevertheless should not fully rely on the user awareness since there is indication on partially ineffectiveness of trainings provided [8].

Awareness has been generally discussed as an important contribution to reduce the exposure but also referring to risks as overconfidence in case of users feeling well aware about phishing and therefore being less cautious when receiving malicious mail that are set-up well [8]. In this context, the approach of different levels of awareness trainings being provided to users with different levels of expertise was introduced [8]. Such distinction would allow taking more into consideration the underlying reasons why users may click on a phishing mail and allow to have targeted training. Such approach could also be helpful to avoid users being bored from too general trainings not reflecting their level of knowledge on the threat.

As the evaluation on selected webpages of Austrian financial institutions has shown, there are continuous campaigns ongoing that are also visible from statistical data available with Austrian organizations aiming to increase the level of Cybersecurity (e.g. Cert.at). Reporting to such structures the information on phishing sites allows them to share the information on their portals and also support to take down phishing sites reducing the risk from falling into the same phishing mail for other customers.

In the literature, examples of commercial platforms are described allowing a broad customer base to leverage on the "crowd" as source of phishing campaigns [16]. "PhishMe" as company is cited where users can report on experienced phishing attempts, experts analyse the reports and add them to their database available again to all users.

All literature indicates that it is unlikely that phishing as threat will vanish within the upcoming years especially since attackers are also leveraging on newly upcoming technologies and therefore remain in a race with those protecting user data [1], [7].

This implies jointly with the proposed stage-approach on user-awareness [8] that awareness measures cannot be considered one-time activities but need to be done repeatedly including updates with most recent information. In this regard, when it comes to users within an organization the awareness needs to be assured on all hierarchy levels since trainings and test campaigns need to be financially covered [2].

Providing and sharing information is one measure to increase the recognition of phishing mails and raise awareness among users. Information sharing can be done in different ways to address the various target groups [13].

While pure information sharing is considered as the weakest measure in raising phishing awareness, resulting from the need for users that are willing to read the information, reflect and apply the read information in their daily life. Other measures as regular training including active feedback, phishing test campaigns with dedicated particular training/information shared to users that clicked on malicious mails or phishing training in form of games are reflected as being more efficient with regards to the contribution on awareness [7], [12].

Trainings and awareness measures therefore are subject to continuous evolution. These activities need to cover either contextual knowledge with general understanding of phishing

and related threats as procedural aspects including proper reaction and reporting of malicious sites as remarked on the security websites of Austrian financial institutions. These measures are also an important contribution in reducing the risk for other users.

Even though it has been reflected that there will remain a residual subset of users clicking on phishing mails awareness measures are considered to contribute positively to increase the knowledge of users on the threat and their ability to identify phishing mails. By increasing the awareness of the users, the success rates for the attackers can be reduced [7].

Our research shows that a bundle of measures reaching from technical arrangements to awareness measures is most promising to fight against phishing threats successfully. As shown in the paper attackers use social engineering techniques and stimuli known from psychological analysis to target the users and gain access to their confidential data [3]. Despite several years of anti-phishing solutions in place and awareness trainings being done, there is still a continuous threat resulting from it visible [12] that requires ongoing initiatives to reduce the risk.

REFERENCES

[1] Hong, J., The state of phishing attacks. *Communications of the ACM*, **55**(1), pp. 74–81, 2012.

[2] Miranda, M.J.A., Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, **14**(2), pp. 5–10, 2018.

[3] Beißel, S., *Security Awareness: Grundlagen, Maßnahmen und Programme für die Informationssicherheit*, Walter de Gruyter GmbH: Berlin and Boston, 2019.

[4] Purkait, S., Kumar De, S. & Suar, D., An empirical investigation of the factors that influence internet user's ability to correctly identify a phishing website. *Information Management and Computer Security*, **22**(3), pp. 194–234, 2014.

[5] Tranfield, D., Denyer, D. & Smart, P., Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, **14**(3), pp. 207–222, 2003.

[6] Hadnagy, C., *Social Engineering Enttarnt: Sicherheitsrisiko Mensch*, mitp-Verlag: Heidelberg, 2014.

[7] Purkait, S., Phishing counter measures and their effectiveness: Literature review. *Information Management and Computer Security*, **20**(5), pp. 382–420, 2012.

[8] Ebot, A.T., Using stage theorizing to make anti-phishing recommendations more effective. *Information and Computer Security*, **26**(4), pp. 401–419, 2018.

[9] Cert.at, Bericht Internet Sicherheit Österreich 2019. https://cert.at/de/berichte/. Accessed on: 21 Dec. 2020.

[10] Watchlist Internet, Internet-betrug, fallen und fakes im blick. https://www.watchlist-internet.at/news/jahresrueckblick-2020-diese-themen-beschaeftigten-uns-heuer/. Accessed on: 21 Dec. 2020.

[11] OpKoord (Operative Koordinierungsstruktur) Lagebericht, Report cyber security, 2019. https://www.bundeskanzleramt.gv.at/dam/jcr:0a5d5734-a53f-4a60-9e64-70092b554c09/EN-Cybersicherheit_Bericht_2019.pdf. Accessed on: 30 Dec. 2020.

[12] Jampen, D., Gur, G., Sutter, T. & Teilenbach, B., Don't click: Towards an effect anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, **10**(1), pp. 1–41, 2020.

[13] Arachchilage, N.A.G. & Love, S., Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behaviour*, **38**, pp. 304–312, 2014.

[14] Anti Phishing Workgroup (APWG). https://apwg.org/trendsreports/. Accessed on: 2 Jan. 2021.

[15] Jansson, K. & von Solms, R., Phishing for phishing awareness. *Behaviour and Information Technology*, **32**(6), 2013.
[16] Rubia, F., Affan, Y., Liu, L. & Wang, J., How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Science*, **27**(6), pp. 581–612, 2019.
[17] Butler, R. & Butler, M., Assessing the information quality of phishing-related content on financial institutions' websites. *Information and Computer Security*. **26**(5), pp. 514–532, 2018.
[18] Bawag. https://www.bawagpsk.com/BAWAGPSK/Sicherheit. Accessed on: 27 Oct. 2020.
[19] Erste Bank. https://www.sparkasse.at/sicherheitscenter-en/current-warning. Accessed on: 27 Oct. 2020.
[20] Sparkasse. https://www.sparkasse.at/sicherheitscenter-en/important-security-tips. Accessed on: 27 Oct. 2020.
[21] BAWAG. https://www.bawagpsk.com/BAWAGPSK/Sicherheit/475006/20190916.html. Accessed on: 27 Oct. 2020.
[22] N26. https://n26.com/en-at/security. Accessed on: 27 Oct. 2020.
[23] Google. https://phishingquiz.withgoogle.com. Accessed on: 30 Dec. 2020.