Field Studies on the Impact of Cryptographic Signatures and Encryption on Phishing Emails

Stefanie Pham[1], Matthias Schopp[2], Lars Stiemert[2], Sebastian Seeber[2], Daniela Pöhn[2] and Wolfgang Hommel[2]

[1]*Ludwig-Maximilians-Universität München, Munich, Germany*

[2]*Research Institute CODE, Universität der Bundeswehr München, Munich, Germany*

Keywords: Phishing, Social Engineering, Security, Email, Signatures.

Abstract: Phishing is a type of scam designed to steal users' personal information, e.g. passwords, credit card information, or other account details. Phishing websites look similar to legitimate ones, making it difficult for users to differentiate between them. Phishing attacks are constantly being improved and the range of techniques used are continuously expanded. Signatures and encryption in emails are security mechanisms that phishers could attempt to misuse. This paper analyses the potential of these methods. Two comparative studies on the effect of Pretty Good Privacy (PGP) signatures and encryption in phishing mails were conducted. The effect was analysed in social and security-related contexts and with computer-savvy as well as regular recipients. We examined the factors computer experience, signature, encryption, signature and encryption, as well as interaction between computer experience and signatures. The results indicate a potential for misuse. Observations made during this study are stated along with future work.

1 INTRODUCTION

Phishing is one of the leading causes of data breaches and a method for identity theft, financial fraud, and skimming trade secrets or military information (PhishLabs, 2019). Thereby, phishing is a significant threat to the security of individual internet users and companies up to states. Attackers attempt to obtain confidential data, such as passwords or bank details, through digital communication using deception. Traditionally, phishing messages are sent by email and, under a trustworthy pretext, prompt you to visit a website that requests personal information. The collected data is then used for further attacks. Phishing attacks typically adapt to seasonal events; for example, phishing emails are currently tailored for COVID-19, where, e. g. the World Health Organization (WHO) (World Health Organization, 2020) and the US Center of Disease Control (Centers of Disease Control and Prevention, 2020) were imitated as senders.

For successful attacks, emails must appear trustworthy and authentic. Phishers use a repertoire of techniques and tools, which is constantly being improved and expanded. This makes it increasingly difficult for users and detection systems, like spam filters, to identify these attempts of fraud. The techniques include professional design, clever fake sender addresses, and inconspicuous links (Chaudhry et al., 2016). Persuasion strategies are used to manipulate recipients (Ferreira et al., 2015) and publicly available or otherwise acquired data enable the personalisation of messages (Benenson et al., 2017). Furthermore, phishers attempt to make their attacks appear secure, in order to gain their victims' trust. They increasingly incorporate security mechanisms such as HTTPS to feign security on their websites (PhishLabs, 2019); It can be expected that further security mechanisms will be exploited in the same way. Other security mechanisms that have the potential to be misused and are yet under-investigated in research are end-to-end encrypted and cryptographically signed emails. OpenPGP and Secure / Multipurpose Internet Mail Exchange (S/MIME) are standards that provide these security services. OpenPGP creates confidentiality and authenticity in emails with the underlying web of trust. Similarly to HTTPS, OpenPGP encryption does not guarantee authenticity, signatures however are a means to authenticate senders. If used and understood correctly, they are in fact an instrument to prevent phishing. In addition, encryption can be seen as a form of personalisation, as the recipient's public

Pham, S., Schopp, M., Stiemert, L., Seeber, S., Pöhn, D. and Hommel, W.
Field Studies on the Impact of Cryptographic Signatures and Encryption on Phishing Emails.
DOI: 10.5220/0010206003840390
In *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021)*, pages 384-390
ISBN: 978-989-758-491-6

key is used. Detection systems running on the mail servers of individual organizations or cloud service providers cannot analyse encrypted mails, increasing the probability of successful attacks. To examine whether signatures and encryption can be misused for phishing, we conducted two field studies investigating the mechanisms' influence on the effectiveness of phishing attacks.

The rest of the paper is organized as follows: Related approaches are described in Section 2, which build the basis for our studies in Section 3. The outcomes of our two field studies are described in Section 4 and discussed in Section 5. Section 6 concludes the paper and gives future directions.

2 RELATED WORK

Several researchers have published work on phishing. We want to highlight phishing mediums and how different factors impact the success of phishing attempts. Phishing research has so far mainly focused on webpages and was mostly conducted via user studies (Ferreira and Vieira-Marques, 2018). This may be the case because websites are the most common phishing medium, followed by email. Other means of communication used for phishing are text messages or phone calls (Yeboah-Boateng and Amanor, 2014), social media like Facebook (Jagatic et al., 2007; Benenson et al., 2017) and Twitter (Seymour and Tully, 2016), or recently QR codes (Vidas et al., 2013). Signed emails can be embedded into anti-phishing approaches (Ren et al., 2007; Crain et al., 2010), but to our knowledge no study targets signatures and encryption as a means for phishers.

Recent related work researched the impact of various factors on the effectiveness of phishing attacks. The factors can be categorised into user-based factors and the overall phishing setup. The following related work describes the correlation between demographic characteristics and phishing vulnerability: (Sheng et al., 2010) and (Kumaraguru et al., 2009) show that individuals between 18 and 25 years are more vulnerable than older people. This result is confirmed by (Diaz et al., 2020), including only young and mid-aged people. Another study extends the scope of this research by including older people (Lin et al., 2019). They observed a maximum vulnerability to phishing in women over the age of 60 years. Further studies (Sheng et al., 2010; Jagatic et al., 2007; Halevi et al., 2015) confirm that women are overall more vulnerable to phishing than men. Recent work supports the thesis that computer-savvy people are less vulnerable to phishing and that web skills correlate to lower phishing susceptibility (Downs et al., 2007). In a study at a university, researchers analysed how publicly available information in social networks can be misused for phishing attacks (Jagatic et al., 2007). They observed that students from technology majors were the least vulnerable group. The success rate for phishing attempts from an unknown sender was as low as 0%, whereas it was up to 50% for students from other departments. A comparable result was found in (Diaz et al., 2020) during simulated phishing attacks. Information technology and engineering students had the lowest click rates in this study. Low susceptibility was also related to frequent interaction with computers and participation in computer training. In contrast, (Alsharnouby et al., 2015) found no correlation between technical competences and the ability to identify phishing correctly. Unlike computer experience, IT security experience is often described as a factor that distorts the results of a study. To eliminate this factor, knowledge in IT security was an exclusion criterion in a set of phishing studies, e.g. (Jakobsson et al., 2007) excluded students who attended an IT security lecture and (Downs et al., 2006) excluded subjects if their answers in a survey indicated increased security awareness. The setup of the phishing attack itself is pivotal for its effectiveness. Targeted content raises the success rate of phishing messages, but the effectiveness depends on the recipient. A widespread spear-phishing experiment was performed by (Williams et al., 2018). They observed that people are more vulnerable at their workplace if phishing messages use persuasion techniques such as authority and urgency. The impact of different persuasion techniques in relation to the recipients' demography was explored by (Lin et al., 2019). They determined that young adults are most responsive to scarcity and older adults to reciprocation.

These observations support our assumption that the effect of signatures and encryption depends on the recipients and the email context. Therefore, computer experience and security-related email content are factors considered in our studies.

3 STUDIES

This paper presents the results of studies on whether signatures and encryption can be misused to increase the effectiveness of phishing attacks. The relationship is examined both in a security-related and in a social context. Additionally, it is determined whether the recipient being computer-savvy has an impact on the effectiveness of encryption and signatures in phishing emails. Two field studies with realistic OpenPGP

signed emails were designed and carried out. Publicly available email addresses were collected and emails were sent with links to websites that asked for sensitive data in some manner.

The emails were sent in four different variants: plain, plain with signature, encrypted, and encrypted with signature. In order to examine the effects in different contexts, two studies were conducted. In the first study, the message was non-security-related (social) and in the second one it was security-related. The number of subjects clicking the link was collected as well as the number that entered data on the websites. Those two values were used to measure the effectiveness of the phishing approach.

The studies were designed in such a way that no login data for existing online services were requested. No sensitive data was transmitted to the servers. The email accounts used to send the mails were locked when the study was concluded and the subjects' email addresses were deleted. Before conducting these studies, we conferred with the chairman of the ethics committee of the Universität der Bundeswehr München. We concluded that we would perform our research as a pilot study with a small sample size. For future large-scale studies, approval will be requested from an ethics board.

The following two sections describe the implementation of the studies. The first section describes the setup and implementation of study 1 and the acquisition of the subjects as well as the data collection and the final steps. This is followed by the setup and implementation of study 2. The results of both studies are outlined afterwards.

3.1 Study 1: PhotoBay

In the first study, the influence of the following factors on the effectiveness of the phishing attempt was analysed:

1. Computer experience of the subject receiving an unsigned email.
2. Computer experience of the subject receiving a signed email.
3. Signing an email with an OpenPGP signature sent to a non-computer-savvy subject.
4. Signing an email with an OpenPGP signature sent to a computer-savvy subject.
5. Encrypting an email with the subject's public key.
6. Signing an email with an OpenPGP signature and encrypting it with the subject's public key.
7. Interaction between the effects of computer experience and signatures.

The email sent in this study allegedly contained a link to party pictures. The link led to a fake cloud-service website. In order to see the pictures, the website requested registration as shown in Figure 1. The email was an adapted version of the one used by (Benenson et al., 2017):

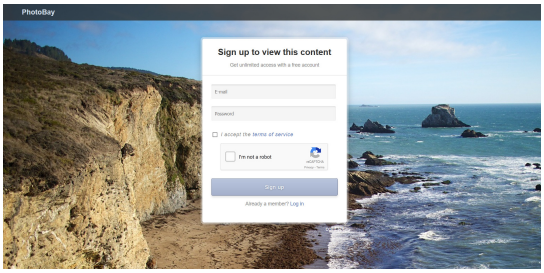

Figure 1: Website Study 1 PhotoBay.

Subject: Pictures from party last week

Hi!
The party was awesome! Here are the pictures:
`https://www.photobay.net?a=<ID>`
But please don't share them with people who haven't been there!
See you next time,
Tony

The alleged sender was a fictitious person with a common gender-neutral English name. The link included in the email used an anonymised ID to track the subject in order to identify duplicates, i. e. the same recipient following the link multiple times. The subjects were acquired by using a script that collects publicly available email addresses on search engines. This decision was made to simulate a realistic phishing attack by using publicly available and easy-to-use tools and data sources. The collected subjects were divided into six groups:

- Not computer-savvy, receive a plain email (N = 110).
- Computer-savvy, receive a plain email (N = 110).
- Not computer-savvy, receive a signed email (N = 110).
- Computer-savvy, receive a signed email (N = 110).
- Computer-savvy, receive an encrypted email (N = 99).
- Computer-savvy, receive a signed and encrypted email (N = 99).

For this study, *computer-savvy* refers to a person who is presumed to use computers more frequently or to have better comprehension of comput-

ers than average. In order to find computer-savvy subjects, email addresses were collected from websites with computer- and programming-related topics, such as linux and coding forums. Respectively, *non-computer-savvy* refers to a person who is presumed to have average computer knowledge. These email addresses were extracted from social networks, where published personal information can be expected, such as (LinkedIn, 2020) and (Instagram, 2020). OpenPGP certificates were created for the sender addresses and published on the Synchronizing Key Server (SKS) network. These were used for the signatures that were attached to the emails. To send an encrypted email, the recipient needs an OpenPGP key pair. The required public keys were retrieved from a key server. Consequently, only subjects with a published public key were in the groups receiving encrypted emails. It can be assumed a person with keys is computer-savvy (Braun and Oostveen, 2019) and, therefore, there was no group of non-computer-savvy subjects receiving encrypted emails.

The efficiency of the phishing attack was then measured based on the access requests of the website and the input of data by the subjects. To determine the number of subjects that followed the link in the email, the ID included in the link was saved on the server side for every access request. The IDs were then compared to a list of valid IDs for this study to filter out access requests that were not the result of a subject following the link in the email. The IDs were 16-character strings containing the group and study affiliation and the hashed email address of the subject. Thus, a conclusion to the group, but not to the individual subjects was possible. To track the number of subjects that entered data, a subject's ID was logged when they attempted to register. The stored IDs for access requests and data input allowed us to detect duplicates, so it was possible to determine if the same subject had visited the website multiple time or if the same subject had attempted to register multiple times. In order to filter bots, a captcha had to be solved in order to register. In addition, a `robots.txt` file was used for the website.

The website was available for two weeks. Afterwards, the OpenPGP keys that had been published for the signed emails were revoked and the collected IDs were deleted after evaluation. The phishing website was replaced by one informing about the study, which included contact details for questions and further information.

3.2 Study 2: EvilGnome

In the second study, the influence of the following factors was analysed:

1. Signing an email with an OpenPGP signature.
2. Encrypting an email with the subject's public key.
3. Signing an email with an OpenPGP signature and encrypting it with the subject's public key.

The subject acquisition, data collection, and final steps were similar to study 1. The study aimed to analyse the effect of signatures and encryption of phishing mails in a security-related context. The subjects were warned of a malicious software by a fake security magazine. The link led to a maintenance website for this magazine with the option to register for a newsletter as shown in Figure 2. The email content was as follows:

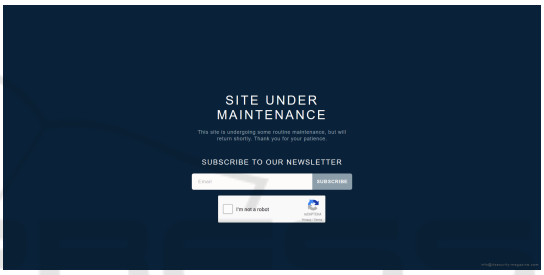

Figure 2: Website Study 2 EvilGnome.

> *Subject:* New wave of EvilGnome – A backdoor implant spies on Linux users
>
> A premature test version of the EvilGnome spyware was first discovered by security researchers in July. Several devices have now been infected by a newer version which includes several added malicious modules.
> Security and antivirus products are currently failing to detect the malware.
> Read more: `https://www.itsecurity-magazine.com?a=<ID>`

The email was only sent to subjects with imputed IT security experience to ensure a basic interest. To collect suitable email addresses, IT security websites such as forums and news websites were searched. The subjects were divided into four groups:

- Receive a plain email (N = 110).
- Receive a signed email (N = 110).
- Receive an encrypted email (N = 92).
- Receive a signed and encrypted email (N = 92).

4 RESULTS

In the first study, 3.5% of the subjects followed the link in the phishing mail and more than 50% of these requested the website multiple times. Only three subjects tried to register on the page from study 1. Therefore, no significant information about the registration attempts was observable, but all attempts resulted from signed emails. To evaluate the influence of the analysed factors, the click rates were tested for statistical significance. Factors one to six were analysed by exact Fisher-tests ($\alpha = 0.05$). The only significant factor was the signature for non-computer-savvy subjects. Table 1 shows the results for study 1.

Factor seven, i.e. the interaction between the computer experience of the subject and signing the email, was analysed with a Breslow-Day test. For this, the click rate was used as the dependent variable and the computer experience and signature as independent variables. The result shows that the interaction between the variables computer experience and signatures is significant ($p < 0.05$). This means the effect of either independent variable on the click rate depends on the other independent variable. So, the factor computer experience lessens the positive effect of signatures on the click rates. The test might be insufficient due to small input values resulting from the study's small sample size. The results are listed in Table 2.

In study 2, the small sample size combined with low click rates led to no significant differences being observable.

5 DISCUSSION

The results show that the success rate among non-computer-savvy subjects was higher when the link was sent in a signed email than in an unsigned email. This effect could not be observed with computer-savvy subjects. A possible explanation is that the signed emails were regarded as unusual and therefore drew attention. According to (Benenson et al., 2017), curiosity is the most common reason for following the link in a phishing email. An alternative explanation for this behaviour is that the signatures were correctly identified as a method of authentication, but falsely interpreted by the non-computer-savvy group. Other security indicators are often misinterpreted as (Downs et al., 2006) explain. Most participants perceived, e.g., the padlock symbol, which indicates encrypted transmissions in browsers, as a sign that it was safe to enter their personal data. Similarly, a signed email may appear to be more secure even from an unknown sender due to a lack of understanding. This interpretation is consistent with the interaction effect observed between signatures and computer experience. Computer-savvy subjects will be more likely to understand the proper usage of signatures. If knowledge on the topic is the reason for computer experience to weaken the positive effect of signatures on the click rate, then education and awareness training may be effective countermeasures.

Although study 2 did not yield significant information in regard to the research questions, the low click rate itself is notable. Since the subjects were specifically chosen to have an interest in IT security, it is likely they correctly identified the email as phishing and therefore did not follow the link.

The primary limitation to these studies were the sample sizes. The small study setup was caused by legal restrictions, which can be addressed in future work. Furthermore, the method used to acquire subjects did not guarantee to return actively used email addresses. In (Benenson et al., 2017), where an email similar to the one used in study 1 was sent, a click rate of 20% was recorded, compared to 3.5% in this study. The main difference between the two studies was that the other study was conducted at a university and, therefore, the email addresses were known to be actively used. Due to the acquisition method, there was further information that could not be established on the subjects. The subjects' presumed computer experience and security interest or lack thereof could not be verified and the reasoning behind their behaviour could not be determined. Collecting the email addresses at an institution or recruiting subjects for a cover-up study can address these issues in future studies. However, the method used in this study portrays a more realistic common phishing attempt. In future work, the issue of small values in the data can be mitigated by larger test groups.

6 CONCLUSION AND OUTLOOK

Phishing attacks are constantly being improved. Various techniques are used to increase the success of phishing attempts, including security mechanisms. Using digital signatures and encryption for phishing emails are strategies that attackers could take advantage of. In this paper, we conducted two field studies to assess the effectiveness of these strategies. The studies additionally take the recipients' computer experience into consideration as well as the context of the phishing email. The results offer first insights on the misuse potential of signatures, suggesting they can be exploited by attackers. These and future stud-

Table 1: Exact Fisher-tests results.

Factor	Followed link	p-value
Computer experience (unsigned)	Non-computer-savvy: 1/110 (0.91%) Computer-savvy: 7/110 (6.36%)	0.0654
Computer experience (signed)	Non-computer-savvy: 8/110 (7.27%) Computer-savvy: 2/110 (1.82%)	0.1014
Signed (non-computer-savvy)	Unsigned: 1/110 (0.91%) Signed: 8/110 (7.27%)	**0.0353**
Signed (computer-savvy)	Unsigned: 7/110 (6.36%) Signed: 2/110 (1.82%)	0.1706
Encrypted	Unencrypted: 7/110 (6.36%) Encrypted: 1/99 (1.01%)	0.0681
Signed & encrypted	Neither: 7/110 (6.36%) Both: 3/99 (3.03%)	0.3388

Table 2: Breslow-Day test result.

Followed link	p-value
Non-computer-savvy / Unsigned: 1/110 (0.91%) Non-computer-savvy / Signed: 8/110 (7.27%) Computer-savvy / Unsigned: 7/110 (6.36%) Computer-savvy / Signed: 2/110 (1.82%)	**0.0037**

ies are critical because only if research stays ahead of attackers in phishing strategies, preventive measures can be developed to protect users from phishing attacks.

For future work, we plan to extend our field studies to confirm our results and to gather more conclusive data on the effects of encryption and security-related context, and to examine further aspects. These include authority figures, different persuasion techniques, and using S/MIME as opposed to OpenPGP. Additionally, we plan to consider legal aspects and a more comprehensive mail selection in terms of confidentiality. Finally, we intend to investigate the reasons for people's behaviour in response to phishing and the effect of awareness training.

REFERENCES

Alsharnouby, M., Alaca, F., and Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82:69–82.

Benenson, Z., Gassmann, F., and Landwirth, R. (2017). Unpacking Spear Phishing Susceptibility. In Brenner, M., Rohloff, K., Bonneau, J., Miller, A., Ryan, P. Y., Teague, V., Bracciali, A., Sala, M., Pintore, F., and Jakobsson, M., editors, *Financial Cryptography and Data Security*, pages 610–627. Springer International Publishing.

Braun, S. and Oostveen, A.-M. (2019). Encryption for the masses? An analysis of PGP key usage. *Mediatization Studies*, 2:69.

Centers of Disease Control and Prevention (2020). COVID-19-Related Phone Scams and Phishing Attacks. https://www.cdc.gov/media/phishing.html. [Online, December 19, 2020].

Chaudhry, J., Chaudhry, S., and Rittenhouse, R. (2016). Phishing attacks and defenses. 10:247–256.

Crain, J., Opyrchal, L., and Prakash, A. (2010). Fighting Phishing with Trusted Email. In *2010 International Conference on Availability, Reliability and Security*, pages 462–467.

Diaz, A., Sherman, A. T., and Joshi, A. (2020). Phishing in an Academic Community: A Study of User Susceptibility and Behavior. *Cryptologia*, 44(1):53–67.

Downs, J. S., Holbrook, M., and Cranor, L. F. (2007). Behavioral Response to Phishing Risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, eCrime '07, pages 37–44, New York, NY, USA. Association for Computing Machinery.

Downs, J. S., Holbrook, M. B., and Cranor, L. F. (2006). Decision Strategies and Susceptibility to Phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS 06, pages 79–90. Association for Computing Machinery.

Ferreira, A., Coventry, L., and Lenzini, G. (2015). Principles of Persuasion in Social Engineering and Their Use in Phishing. In Tryfonas, T. and Askoxylakis, I., editors, *Human Aspects of Information Security, Privacy, and Trust*, pages 36–47. Springer International Publishing.

Ferreira, A. and Vieira-Marques, P. (2018). Phishing Through Time: A Ten Year Story based on Abstracts. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP*, pages 225–232. INSTICC, SciTePress.

Halevi, T., Memon, N., and Nov, O. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015)*.

Instagram (2020). Instagram. https://www.instagram.com. [Online, December 19, 2020].

Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. (2007). Social Phishing. *Communications of the ACM*, 50(10):94–100.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., and Lim, Y.-K. (2007). What Instills Trust? A Qualitative Study of Phishing. In *International Conference on Financial Cryptography and Data Security*, pages 356–361, Berlin, Heidelberg. Springer.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., and Pham, T. (2009). School of Phish: A Real-World Evaluation of Anti-Phishing Training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS 09. Association for Computing Machinery.

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., and Ebner, N. C. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 26(5):1–28.

LinkedIn (2020). LinkedIn. https://www.linkedin.com. [Online, December 19, 2020].

PhishLabs (2019). Phishing Trends and Intelligence Report - The Growing Social Engineering Threat. Technical report.

Ren, Q., Mu, Y., and Susilo, W. (2007). SEFAP: An Email System for Anti-Phishing. In *6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007)*, pages 782–787.

Seymour, J. and Tully, P. (2016). Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter. *Black Hat USA*, 37:1–39.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI 10, pages 373–382. Association for Computing Machinery.

Vidas, T., Owusu, E., Wang, S., Zeng, C., Cranor, L. F., and Christin, N. (2013). QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. In *International Conference on Financial Cryptography and Data Security*, pages 52–69. Springer.

Williams, E. J., Hinds, J., and Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120:1–13.

World Health Organization (2020). Beware of criminals pretending to be WHO. https://www.who.int/about/communications/cyber-security. [Online, December 19, 2020].

Yeboah-Boateng, E. O. and Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, 5(4):297–307.