CMP417 Engineering Resilient Systems: Human-Centred Security

Mairi MacLeod
School of Design and Informatics
Abertay University
DUNDEE, DD1 1HG, UK

ABSTRACT

This paper was written to provide recommendations for preventing successful phishing campaigns by the hacktvist organisation targeting the company. Phishing and the different types are defined along with; the attack vectors that can be exploited, the consequences of a successful phishing attack and methods of detecting malicious emails. The solutions proposed are; implementing software that investigates the sender, the included URLs and scans the attached files as well as training employees. In order to test the effectiveness of the suggested mitigations FooBar Inc. should send fake phishing emails before and after implementation. In conclusion it was decided that developing phishing-detection software would be too expensive in the short-term for FooBar Inc. but should be considered at a later date. Therefore they should focus on training employees to identify and not follow links or download files from phishing emails.

1. INTRODUCTION

According to the Federal Bureau of Intelligence in the United states, there were 241,342 phishing attacks in 2020. This is an increase of almost 127 thousand from the year prior. Phishing and similar such social engineering attacks were identified as the most common attack type, as well as the fastest growing *(IC3,2020)*.

The company, FooBar Incorporated, has been targeted by malicious hackers. As phishing is so common it can be assumed that those targeting FooBar Inc. may choose to use this method. A successful phishing attack can lead to malware being placed in a network. This malware can launch a Denial of Service (DoS) attack, delete or steal private customer data and send further phishing attacks. The dangers and likelihood of a phishing attack is why mitigations are so important, in order to increase the chance of a fake email being identified. This paper aims to detail what phishing is, suggest a number of ways that FooBar Inc. can reduce their chances of having a successful phishing campaign against them and the methods by which these mitigation s can be evaluated.

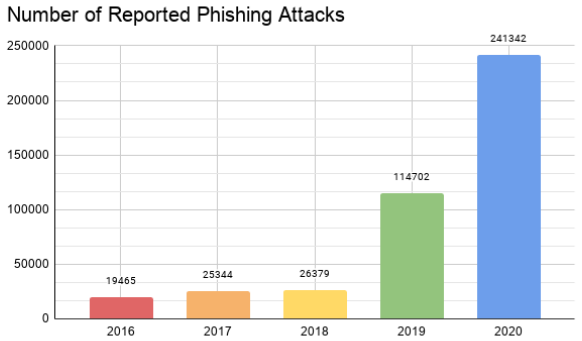

Figure 1: Number of Phishing Attacks Per Year (IC3, 2020)

2. BACKGROUND

PHISHING

Phishing is defined as a semantic attack, where users not software are targeted in order to lure victims into clicking malicious links or installing malware *(Zhang et al,2007)*. This type of attack falls under the category of social engineering. This is where attackers build a trust with the victim in order to encourage them to perform an action they normally would perhaps be unwilling to do.

Classic phising is usually in the form of a scam email. A prince from a distant country has died and decided to leave the recipient of the email all of their money in his will, all they need to do is send their bank details and they will become rich. This is not the only form of phishing however, there now exists a wide array of methods scammers use to try and obtain sensitive information or get malware installed on a device. These are; vishing, smishing, spear phishing, pharming and whaling.

Vishing, or voice phishing, is where a person pretends to be someone they're not over a voice or phone call. A common example of this is where someone would pretend to be from a bank and attempt to persuade a victim into providing their account details in order to prevent a charge or account suspension. Smishing, SMS phishing, is phishing over text. This has gotten increasingly more popular in recent years, a current example would be text messages pretending to be from the NHS offering Covid-19 vaccinations or free tests but instead containing a malicious link *(NHS,2021)*. Spear phishing is when a fraudulent email is sent to a person but the attacker uses information about the victim to personalise the email to them, making it appear more legitimate. *(Kwak et al,2020).* Unlike regular phishing, this form tends to not involve the sending of bulk emails to a wide array of addresses but instead is much more targeted to a single or small group of persons.

A very sophisticated and advanced form of phishing is pharming. This is where a target is tricked into installing malware onto their device, usually via a link in an email, and when they go to websites they are actually redirected to a malicious copy which will contain a keylogger *(Brody et al, 2017).*

3. LITERATURE REVIEW

ATTACK VECTORS

Studies done by the University of Exeter have implied that around 10-20% of adults in the UK are particularly susceptible to scams. These people may be more likely to fall for phishing attempts and attackers may prey on previous victims of such attacks when attempting spear phishing *(OFT,2009).* Further research suggests that the personality trait responsible for this vulnerability towards spear-phishing attacks could be conscientiousness. This personality trait is commonly associated with rational-thinking and traditionally thought to make a person more likely to detect a malicious email. However this second study suggests that users tend to overestimate their ability to detect fraudulent emails, making them in fact more vulnerable, specifically to spear-phishing attacks *(Halevi et al, 2015).* The first study also implied that people who have more knowledge in the subject of the scam email have a greater chance of falling for it. Again suggesting that higher confidence may directly correlate to phishing vulnerability *(OFT,2009).* In the case of FooBar Inc. it could be assumed that the development staff would be more likely than the HR staff to fall for an email surrounding their GitHub account.

Although research suggests that spear-phishing attacks work best with more educated users, other research reveals that more generalised phishing attacks are more successful with those who are less educated on how phishing works and the risks involved. Out of all of the 232 participants, those who demonstrated prior knowledge of phishing were over 20% less likely to click on the malicious links or provide their information to the attacker. It was also found that even if a person had knowledge about more generic cyber security unless they were aware about how phishing worked they were just as vulnerable as those who had no cyber security knowledge *(Downs et al, 2007).*

CONSEQUENCES

Falling for scams can cause distress and mental harm to the victims. This can have a significant negative effect on employees who have accidental clicked a malicious link or downloaded some malware. The distress caused by falling for a phishing attack can cause victims to be more vulnerable to similar events in future, therefore it is of the utmost importance that organisations take steps to prevent successful phishing campaigns in the first place *(OFT,2009).*

The distress and embarrassment as a result of falling victim to a phishing attack may lead the victim to not report the event to their organisation. Research done by Youngsun Kwak et al in 2020 investigated the users perceived ability to detect a phishing email, the likelihood of an individual falling for a spear phishing attack and then their willingness to report it. They found that participants who scored themselves lower on ability to detect fraudulent emails were less likely to report a successful phishing attack. This was suggested to be due to the perception that an employer would respond negatively and therefore distress the employee further *(Kwak et al, 2020).*

Aside from emotional consequences phishing can have financial implications as well. Phishing emails can request personal information from a victim which can be used for identity theft. By utilising pharming an attacker can gather usernames, passwords and bank details from a victim. This allows the malicious user to withdraw money from their bank or buy items online with their money. Usernames and passwords also provide access to their social media and cloud storage accounts *(Brody et al, 2017).*

DETECTION AND PREVENTION

Anti-phishing or phishing detection browser extension's make use of lists of legitimate and fraudulent URLs. They use these in order to verify whether a website is potentially harmful or not and will then alert the user to this fact. These browser extensions will not detect all forms of phishing and will not highlight malware inside of email attachments. Some examples of phishing detecting browser extensions are; Cloudmark Anti-fraud Toolbar, SpoofGuard and Netcraft Anti-phishing Toolbar. Research done in 2007 concludes that these toolbars can be highly inaccurate at detecting false web pages. The results showed that CloudMark successfully detected only 3% of such websites and SpoofGuard had a false positive rate of 42% *(Zhang et al, 2007)*.

For email or SMS phishing attacks most detection softwares take a heuristic-based approach. This is where multiple features of the message are investigated in order to determine whether the source or contents are harmless. There are a number of ways of doing this: Cross checking the email address or phone number to see if they belong to a list of known phishers or if they do belong to whomever they say they are. Looking for spelling or grammar mistakes which may imply that the message was translated badly, a common indicator of phishing emails. Checking SSL certificates and URLs to determine whether the website is legitimate and actually belongs to the organisation that sent the email *(Gupta and Pieprzyk, 2011)*.

One prevention technique, mainly used by financial organisations, is to use a physical device which randomly generates a number that must be entered into the website before a transaction can be approved. This helps to prevent success after a phishing attack, specifically with pharming, as the attacker would require both the user's details and their physical device in order to withdraw or transfer money from their account *(Brody et al, 2017)*.

If a person is warned about the dangers of phishing and how to detect such an email they may be less likely to fall for such an attack again, compared to if they were reprimanded. A study done in 2014 demonstrated that participants who received training after falling for a phishing campaign were less likely to fall for subsequent attacks than those who were just informed about what they had done *(Caputo et al, 2014))*.

4. RECOMMENDATIONS

For FooBar Inc. the author suggests that they implement a phishing detection software that takes a heuristic approach. Since 96% of phishing attacks are sent over email the author believes that the organisation should focus their efforts on this attack vector *(Verizon, 2020)*. The software would be designed to work on three fronts, the email itself, the attached documents and the website that the email links to.

For the email part of this solution the address should first be investigated. A deny or allow list of known addresses would be time consuming and difficult to create but certain email providers could be flagged as potentially suspicious. The contents of the email can then be looked at, are there a large number of spelling or grammar mistakes? This could be indicative of a spam email. Attached files should also be reviewed in order to find malware that may be hidden inside. This can be done by scanning all attachments before they are downloaded in order to prevent them being installed on a company machine and potentially harming the network.

Any hyperlinks embedded should be inspected, a common 'trick' used by malicious users is to change the URL using HTML `<a>` tags. An example would be using `<a href="badwebsite.com/evil"> paypal.com/login </a>` so that the reader of the email thinks they are being directed to the legitimate PayPal login page and not realising that the hyperlink actually sends them elsewhere *(Zhang et al, 2007))*. Even without using HTML tags an attacker can make a URL look like it belongs to the organisation they are pretending to be from. This often done by using unicode characters that look similar or identical to other Latin characters. Using a lowercase 'L' or '1' interchangeably is one example used to trick a user who is just skimming through the email not paying express attention to URLs. Other Greek letters and maths symbols can also be used, as well as adding extra or removing certain letters.

Website domain registry dates should also be looked at, domains younger than a year can be suspicious especially if the organisation is supposed to be much older. As this does not always mean the website is malicious the user should be warned but still permitted to visit the website if the domain has only been registered recently.

No software is infallible and so it is important that FooBar Inc's solution should also include a human centred approach. Training for employees should be developed in order to teach them the dangers of a successful phishing attack and how to identify a malicious email.

It is of great importance that employees should not be reprimanded if they fall victim to such an attack and should be informed that they can report such emails without consequence. As most people do not feel like they can report phishing attacks and those who face negative consequences after reporting are more likely to fall victim again FooBar must be careful to create a positive environment surrounding the reporting of phishing emails.

5. EVALUATION

To test if the suggested anti-phishing techniques would be effective there should be trials done where users are sent fake phishing emails. This should be done before and after the implementation of the aforementioned techniques in order to determine if any difference has been made.

The testing of the training can be done by sending both spear and regular phishing emails with varying amounts of complexity to random employees who have agreed to participate. By complexity the author means the how difficult the email is to identify as spam by a user. This could be using HTML tags to obfuscate the URL, replicating real organisations' email headers/footers or using an email address that looks very similar to the real one. By having different faux-spam emails FooBar Inc. can determine how successful the training was and mitigate the possibility that it is the emails not the training that alerted the user to their intention. These emails should not be sent out all at once but instead staggered over a series of months so that the participants do not expect them. This will better simulate a real-world scenario.

If FooBar Inc. also choose to develop a software solution for this problem then it also must be tested. To test this software the organisation can send it a wide array of spam emails, with varying degrees of complexity, along with real benign emails. The false positive and negative rate are just as important as the success rate because if it is incorrectly flagging or not flagging emails then users can start to ignore the warnings or may not be warned before downloading malicious files. Fortunately unlike the testing of the employee's training this does not have to be done over a series of months and the software can be provided with a large number of emails at once.

Even with the best mitigations in place there is always the risk of a phishing email being received by an employee and them clicking any attached hyperlinks. To help reduce the damage caused by these events FooBar Inc. should consider implementing a multi-factor authentication system to reduce the amount of access a malicious user has to the companies network. As suggested by the British National Cyber Security Center, the company could implement a system where the user is given a physical device that can be used as a login stage before or after their password is entered *(NCSC, 2018)*. Using a randomly generated code from a separate device, such as a phone, would also be a good suggestion as the attacker would need access to both the work computer and mobile phone in order to gain access to the company network.

With any solution there are positive and negative impacts on the company. Providing training will take considerably longer than implementing software, as testing the effectiveness will take months. However, it is much cheaper financially as developing software may require the hiring of external developers or take time away from the current developers as they implement this solution. Third party software can be bought but this again will be very costly, especially as the organisation grows and more employees are hired. Enabling multi-factor authentication can also be expensive, especially if physical devices must be given to each employee but this can prevent the much larger cost of the organisation being hacked.

6. CONCLUSION

The company has a real risk of being targeted by a phishing campaign so needs to implement a solution as soon as possible. It is believed that they should focus on email phishing as they are the most common. Due to resource, time and financial costs the training of employees should be prioritised. A software solution can be implemented at a later date if FooBar Inc. deem it necessary. The environment around reporting an attack is just as important as mitigations to prevent them. Therefor the company should also focus on not creating any hostility when an employee falls for a spam email, to increase the likelihood that they continue to report such incidents. Finally the author would also suggest that they implement a multi-factor authentication system that relies on a physical or seperate device.

7. REFERENCES

Brody, R. et al. (2017). *"PHISHING, PHARMING AND IDENTITY THEFT"* Academy of Accounting and Financial Studies Journal, vol. 11, no. 3, pp. 43-56.

Caputo, D. et al. (2014) *"Going Spear Phishing: Exploring Embedded Training and Awareness."* IEEE Security & Privacy, vol. 12, no. 1, pp. 28–38, doi:10.1109/msp.2013.106.

Downs, J. et al. (2007), *"Behavioral Response to Phishing Risk."* Proceedings of the Anti-Phishing Working Groups 2nd Annual ECrime Researchers Summit on - ECrime '07, vol. 2, pp. 37–44, doi:10.1145/1299015.1299019.

Fette, I. et al. (2006) *"Learning to Detect Phishing Emails."* Research Paper. 16th International Conference on World Wide Web. pp. 649–656, doi, 10.1145/1242572.1242660.

Gupta, G. and Pieprzyk, J. (2011) *"Socio-Technological Phishing Prevention."* Information Security Technical Report, vol. 16, no. 2, pp. 67–73, doi: 10.1016/j.istr.2011.09.003.

Halevi, T. et al. (2015).*"Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks"* University Whitepaper. New York: NYU Polytechnic School of Engineering.

Internet Crime Complaint Center (IC3). (2020) *"Internet Crime Report 2020"*. [online], FBI. Avaialable at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3 Report.pdf [Accessed: 5th May 2021]

Kwak, Y. et al. (2020).*"Why do users not report spear phishing emails?"* Telematics and Informatics, vol. 48, pp. 1–11, doi: 10.1016/j.tele.2020.101343.

National Cyber Security Centre (NCSC). (2018). *"Password administration for system owners"*. [online], NCSC Guidance. Available at: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach [Accessed: 10th May 2021]

National Health Service (NHS). (2021).*"Docs and cops warn on COVID-19 cons"*. [online], NHS England. Available at: https://www.england.nhs.uk/2021/01/docs-and-cops-warn-on-covid-19-cons/ [Accessed: 5th May 2021]

Office of Fair Trading (OFT). (2009). *"The psychology of scams: Provoking and committing errors of judgement"*. Psychological Study. United Kingdom: University of Exeter School of Psychology.

Verizon (2020). *"2020 Data Breach Investigations Report"*. [online], Verizon. Available at: https://enterprise.verizon.com/en-gb/resources/reports/dbir/ [Accessed: 13th May 2021]

Zhang, Y. et al. (2007). *"Phinding Phish: Evaluating Anti-Phishing Tools"*. University Whitepaper. Pennsylvania: Carnegie Mellon University.