Engineering Resilient Systems (Part 3)

Jonah McElfatrick
1700463

Abstract

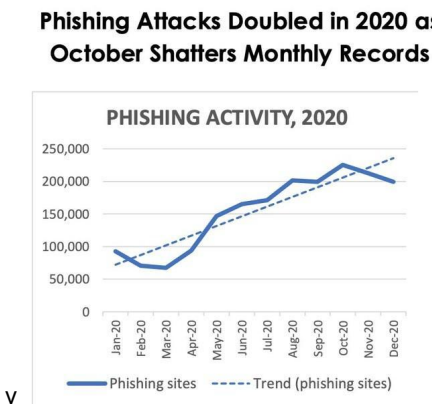
This paper serves to provide the reader with a literature review regarding the subjects of how phishing attacks can compromise security and how irresponsible and uninformed employees are a risk to businesses in this regard. Following this review is a set of recommendations for actions that could be taken place in order to achieve the following objectives:

- Decrease the chances of phishing attacks being received by company employees
- Increase employee's overall awareness of phishing attacks
- Increase the overall strength of a company's password-based authentication system

To further validate the provided recommendations, a practical experiment will be portrayed in which will allow for feedback or confirmation of the effectiveness of the recommendations.

1. Introduction

Phishing is the act in which "an attacker masquerading as a legitimate online entity to steal confidential information from the unsuspecting victims" (Kaur, 2016). Phishing is one of the most common types of cyber-attacks. In 2020, 75% of organizations globally were targeted with phishing attacks amounting to over 240,000 phishing incidents ('Phishing Statistics (Updated 2021) | 50+ Important Phishing Stats', 2021). As can be seen in figure 1 below, these incidents increased month upon month.



v

Figure 1: Phishing Trend 2020 (APWG, 09 February 2021)

The increase in phishing incidents coincides the business and employees having to work remotely and online due to the COVID-19 pandemic. With the increase in companies and services going digital, phishing attacks are only of the many systems created to target not only individuals but also companies.

With the rise in attempted and successful phishing attacks, it is imperative that employees and employers alike gain an understanding of what effects phishing can have on a business, how to prevent the attacks from reaching individuals and how to spot the signs of the attacks.

2. Background

In order to gain an understanding of what can be compromised through a phishing attack and how employees can be possible points of weaknesses, following is a review of literature based on these objectives.

2.1. How Phishing Can Compromise Security

An academic paper (Banday and Qadri, 2007) reviews the different types of phishing attacks and what effects each of these types of attacks can have. Multiple different types of attacks are discussed with their potential effects to a business, included below are some of the attacks discussed and their possible effects:

- Keyloggers and Screen loggers
    - These types of malware can be attached to phishing emails in which are then downloaded to the victim's machine and then send relevant information back to the attacker.
- Data Theft
    - Attacker steals sensitive documents, designs and more in which they may make a profit from but can lead to economic damages for the victim.
    -

An industry journal (*Spear-phishing: how to spot and mitigate the menace | Elsevier Enhanced Reader*, 2013), describes the events that took place in which a London based law firm was targeted by a spear-phishing attack. Through this attack it was found that attached to an email was a document infected with a virus in which compromised the data stored on the computer in which it was opened

upon. This from of attack can have devastating effects on any business in which handles sensitive data in any manner.

This research paper ('International Journal of Advance Research in Computer Science and Management Studies', 2013), discusses the lifecycle of a phishing attack from the reasons behind phishing attacks, to examples and damages caused. Damages caused by phishing attacks include deny user access to their emails and/or systems, identity theft and financial loss. Approximately $929 million was lost due to phishing attack between May 2004 and May 2005.

An academic report (Ragucci and Robila, 2006), discusses the social implications of phishing attacks as well as the damage that can be caused towards businesses through these social implications. Alongside this, a discussion is portrayed regarding the impact on disaster and recovery services during times of need. During the 2004 tsunami and hurricane Katrina, a PayPal phishing email was sent out to 'Contribute to the Tsunami Disaster Relief'. The phisher was arrested and found to have possession of a database with over 800,000 email addresses in which fallen for the scam. Not only does this effect the users who lost their money, it also effects PayPal as their reputation takes a negative impact from it. The public can become wary of the company and their emails and in turn loose trust.

2.2. How Employees Pose a Risk to Companies

This paper (Tian, 2019), discusses the impact that emotional response has on the effectiveness of phishing attacks. A targeted experiment was carried out in order to examine how people reacted to phishing attacks of varying emotional themes. Among the results it is indicated that phishing attacks with an overall positive theme or attitude caused the percentage of click throughs to increase. Also found was individuals who feel uncertain are more likely to act in favor of the attacks and click through the attack.

A 2020 study (Jalali *et al.*, 2020), sets out to investigate the reasons behind why employees at US hospitals click on phishing links. A survey of 397 employees over the course of 2 hospital networks revealed that in spite of previous research, the link between intention to comply and compliance itself is not strongly linked. Through this research, it was noted that there is an association between the amount of work an employee has and the probability of them clicking on a phishing link.

An assessment carried out in 2019 (Gordon *et al.*, 2019), included a study of 6 anonymized US health care institutions. This study included 95 phishing campaigns and 2,971,945 emails sent out to employees. It was found that the click rate of this study was 14.2% in which means that over 400,000 phishing emails were clicked on by employees. This indicates that employees are still a risk as they require more training in which to be able to spot the difference between a legitimate email and a phishing email.

This academic paper (Williams, Hinds and Joinson, 2018), carries out a research experiment in order to analyze the click rate on phishing emails within a company and also what types of phishing emails provide the highest click rate. It was found that the click rate ranged from 6% to 35% with a standard deviation of 11.85% and a mean of 19.44% over the variety of emails sent out. The emails in which provided the highest click rate were those with an authoritative or urgent tone. This indicates that if employees believe that the sender is requiring an action within a certain time frame or that a superior is emailing them, then they are more likely to click the link in the email in order to comply.

3. Recommendation

3.1. Preventing Phishing Attack Spread

A possible mitigation method in which could make it harder for phishing attacks to reach employees is to introduce workplace filters, rules and blacklisting of emails. This can be carried out on multiple organizational workspace suits such as Office365 and GSuite. Included in these forms of organizational workspaces are features and functions such as:

- Email Blacklisting & Whitelisting
- Spam Filtering
- Custom Email Content Filtering
- Quarantine Zones

Using the above features and functions, a custom set of rules can be used to filter any incoming emails into the workspace. Once custom rules are set in place, emails that are caught by these rules can be directed to a quarantine zone to allow for workspace admins to view the contents of the emails in order review how the set rules are working.

3.2. Increasing Awareness

The following methods and actions could be used to increase employee awareness of the risks and consequences of phishing attacks:

- Informational videos

    - Good source of a wide variety of information in a quick and condensed manner
- Leaflets
    - Able to read and understand in their own time
- Demonstrations
    - Give a visualization as to what are the consequences of what can happen.
- Talks
    - Wide variety of information from past and present experiences.

3.3. Strengthen Password Authentication

To increase the base strength of a company's existing password-based authentication, the creation and implementation of a graphical user password system could replace the standardized password-based system. This system would include the use of a pre-determined image or set of images that the user would be required to click pre-determined location points on the image in a specific order in order to authenticate themselves. This would no longer require users to remember long and complex passwords but rather remember locations on an image in a given order. Included in appendix A are wireframes that outline the interface and simple actions for the enrolment interface, selecting image locations and the authentication interface.

4. Experiment

4.1. Validation of Efficacy

To test the effectiveness of the recommendations mentioned above, multiple different evaluation criteria's can be used. Following is example criteria or methods that can be used to verify each of the recommendations made above.

4.1.1. Preventing Phishing Attack Spread

In order to verify the effectiveness of the workspace rules and filters for spam emails, an analysis of the phishing emails coming into the workspace must be analyzed. During analysis, common features and repeated patterns may be found in which can allow for rules and filtering to prevent the emails from reaching employees.

Before the rules have been put in place to catch the features or patterns found in analysis, a count should be made to see how many spam emails are going through to the employees.

This sometimes can rely on employees reporting the email as spam and/or forwarding the email onto the compliance team that will then add the email address tom the blacklist. Another option is to view the quarantine area of the workspace, this will catch any emails that match the current set of rules.

Once the count has been done, the rules can be put in place and then the count process repeated. If the process has been effective, then the number of employee reported spam should drop and the number of emails in the quarantine zone should increase due to the match of features and patterns. Some tweaking may be required in the case that legitimate emails are also being caught in the quarantine zone.

4.1.2. Increasing Awareness

To evaluate the informative training material such as leaflets and videos, quizzes can be developed with a suite of questions that can be randomized for each employee. Taking a quiz before any educational material is handed out and then after the material is handed out allows for a record of results to be taken in order to view the effectiveness of before and after the informative material has been ingested by the employees.

Another method to test if employees can spot phishing emails is to create a phishing testing suite. This testing suite can comprise of a script that uses a created testing email account to send structured HTML formatted emails to a list of emails. Inside the formatted email can be a link that takes the user to a php page that logs who clicked, or to add to a tally in the event of data autonomisation, on the link into a SQL database which then redirects to the page they originally thought they were navigating to. This would allow for a view of how many employees may be susceptible to phishing attacks.

4.1.3. Strengthen Password Authentication

For the image-based password authentication an evaluation can be carried out in order to see if this system would be a suitable replacement for a standardized password-based system. The following criteria could be used to evaluate the proposed image-based password system:

1. Can it be used by those with disabilities?
    a. Would an alternative authentication method be required?
    b. Is the interface simple enough for all users to understand?
2. What should the threshold of images/selection points be?
    a. Finding the balance between usability and security.
3. What is the level of success, once the password is set up?

    a. Can a user repeatedly select the correct locations within the specific threshold?
4. How many touch points should there be?
    a. Finding the balance between security and memorability.

Using the above criteria, in conjunction with user testing and feedback would allow for

4.2. Maximise Acceptance

In order to maximize acceptance of the recommendations above, the five dimensions of usability; Effective, Efficient, Engaging, Error Tolerant, Easy to Learn (Quesenbery, 2003), can be analyzed in reference to each implementation. A short description of each section can be found below.

Effective

Is the user able to carry out the action that they are required to do so? Length or complexity does not matter in this stage, only the success and accuracy of the task at hand.

Efficient

This section involves the speed in which the user can carry out the required action while still maintaining accuracy. This section gives an indication of the task taking too long to complete or being too complex to complete in a timely manner.

Engaging

Is the user having a satisfying or pleasant experience when completing the required action? Is the interface and mechanics working as they should? Could they be improved for aesthetics or function?

Error Tolerant

This section indicates how well the interface reacts to errors. This includes handling, undoing and indicating possible errors that may have occurred while maintaining functionality.

Easy to Learn

This section revolves around how easy the interface is to interpret and if how a new user would come to understand the task at hand when using the interface. Is it clear and concise for what is required?

Using the above sections to evaluate an implemented feature would allow for a higher chance of acceptance from the users who will be using it.

5. Challenges

5.1. Attack Challenges

With the constant development of technology and improved security features, scammers and attackers are forever finding new ways of exploiting a system or improving upon their methods. This not only includes phishing attacks but all other forms of computer attacks. Even with the above recommendations in place, there is a high chance of a new method or tool to be developed in order to get around the implemented security features. In order to help prevent this, regular reviews of the current implemented security system in a company can allow for insight into what could currently be a target and what could be improved upon in the near future in order to attempt to be a step ahead of the attackers.

5.2. Prevention Acceptance Challenges

Although implementing procedures and prevention methods to protect businesses and employees, some of these methods and procedures could have negative side effects that effect the workflow of the employees.

An example of this is the workspace email filtering rules. These rules take time to setup and perfect. During the initial stages of setup, there is time for teething problems in which legitimate emails may be caught in the filter and sent to the quarantine zone. In this case the email may not be noticed to be missing for an extended period of time or until the next time the quarantine zone is checked, and the email passed through to the intended recipient. Another issue that arises from this is privacy concerns. This is apparent as if an email is caught in the quarantine zone, the user that reviews the emails has full access to read the contents of the email and the sender and receiver of the email.

6. References

Tian, C.A. and Jensen, M.L., 2019, December. Effects of emotional appeals on phishing susceptibility. In *Proceedings of the 14th Pre-ICIS workshop on information security and privacy*.

7. Appendix

Appendix A – Image-based Password Authentication System Wireframe

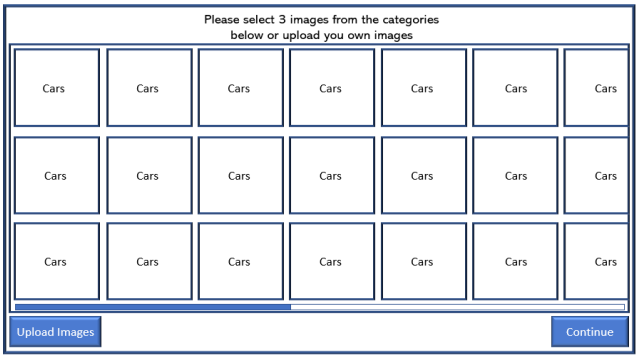


Figure 2: Image Selection

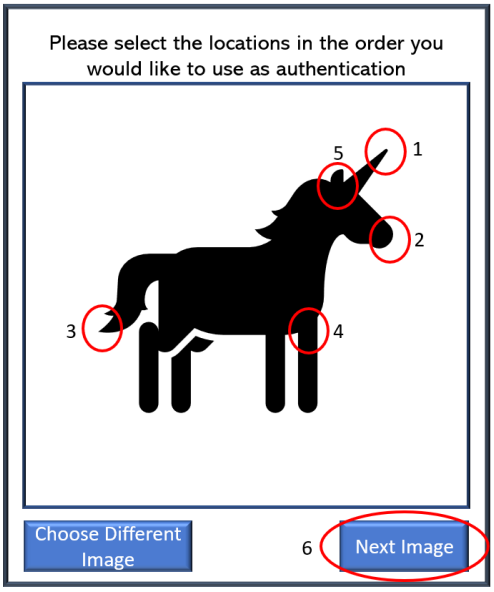


Figure 3: Choosing Locations

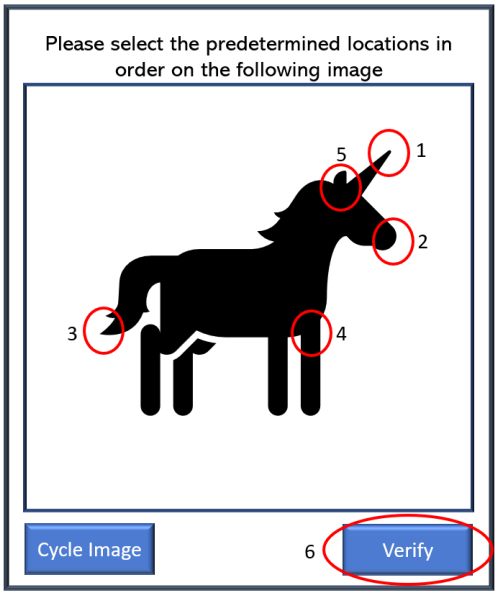


Figure 4: Authentication Interface