Relationship Analysis: Phishing Email Success Rates and User Experience Modification

Shannon M. Merchant[1], Aspen Olmsted[2]
[1]*NYU Tandon School of Engineering*
[2]*Simmons University*
USA

Abstract

The number of successful phishing attacks continues to be a common issue amongst users. Falling for one of these attacks can cause identity theft, eventually leading the attacker to easily access your email, social media accounts, banking accounts, and other personal and private information. Current training video methods and automation prove to be beneficial. However, improvements could help keep the number of successful attacks by clicking malicious links lower. In this paper, we investigate whether training amount and long-term memory affect the user's ability to identify malicious website links. We can determine whether current training methods are enough by testing a sample of users at various training levels and comparing the results to the same test with an extension asking top phishing red flag questions. Our hypothesis suggests that users of all training backgrounds would benefit from an easily accessible questionnaire to aid in identifying real emails from malicious ones. The results show that untrained, partially trained, and consistently trained users can determine whether most links are malicious and improve their ability to verify whether these results are accurate. In addition to current and future methods of detecting malicious links, this method helps users to identify malicious links quickly and ensure they are correct when in doubt.

Keywords: Phishing, malicious links, phishing attacks

1. Introduction

Suppose Phishing attacks via email have continued to claim a substantial number of users and organizations around the world. According to Verizon's 2022 Data Breach Investigations Report (DBIR), Phishing is one of the top 5 breaches, with 82% involving the human element [1]. There have been many approaches to reduce the number of successful phishing attacks. These approaches range from training videos about common red flags and password best practices followed by quizzes in hopes the information is retained after that to color-coded toolbars showing the indicated proposed risk of the destination [3]. Automation has also found its place in current anti-phishing solutions in emails and web pages/ URLs. We recognize these methods have not been proven ineffective in reducing the number of phishing emails clicked on. Aspects of these methods will; be replicated in our solution. We believe additional methods and improvements can decrease the overall emails clicked on by each user over time for users with or without previous training.

Our approach is different because by implementing a system where the information is easily accessible, people can reference this tool whenever they open a questionable email. Our approach will focus on the user taking the questionnaire before clicking a link and receiving a percentage of the likelihood that the email is genuine. The rating allows the user to learn to find malicious email red flags without primarily referencing memory. The critical components of our approach will include a short quiz to be given to a sample of individuals of various training backgrounds using fraudulent and non-fraudulent email examples. Once completed, we provide a questionnaire in the form of a Chrome extension written in javascript and formatted using CSS styling for optimal color coding and functionality, containing four top phishing red flags. The extension will output a percentage of the likelihood the email is a phish or not based on the answers to each question. The same users with duplicate emails will use this extension containing the quiz, and the final score will be evaluated.

Our limitation for this experiment will be the small sample size. In addition, while we will be providing noninvasive referencing using a Chrome extension that does not store user data, this limits our use of recorded methods. An example of this is sending test phishing emails to users [4] or writing code to detect potentially malicious emails for them [3] to preserve the security of the test.

The organization of this paper is as follows. Section II describes the related research on this topic. Section III drills into a motivating example behind our study. Section IV explains our hypothesis and evidence based on our experiment. Finally, section V

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0023

concludes our findings and predicts future work.

2. Related Research

Many other methods have been documented to lower phishing email attacks' success rate. Below are a few examples and how our approach differs from theirs.

A. Anti-Phishing Training Experimentation

In the "Does Anti-Phishing Training Work" article, a user study was conducted on 28 participants [3]. These users were asked to identify phishing websites out of 20 total examples. They were split into groups of 10 (5 phishing sites and five legitimate sites) in groups A and B [3]. Each user was randomly assigned a group to start and take the test. They were then asked to take a 15-minute conditional break of either playing a computer game unrelated to Phishing or watching a phishing-related informational video [3]. They then would take the opposite group of tests, and the results were recorded.

Our method is similar to this method with some modifications. Like this method, we will have participation-aware users questioned on the validity of phishing email examples. This questioning will be followed by providing educational tools to the user and having them take a test to see if the results improved. One improvement to this method is using the same test pre- and post-educating the user. This consistency will show improvement related to the original content while keeping the test consistent. Another progress we made is to provide a questionnaire to the user rather than an informational video. This questionnaire is predicted to improve the results because the user will not have to remember each detail and will be provided a percentage of the likelihood that the email is genuine.

B. Using a Phish Scale

In "A Phish Scale: Rating Human Phishing Message Detection Difficulty," a Phish Scale was compiled to rate the difficulty of seven real-world phishing training exercises [4]. These exercises were sent to the users as simulated phishing emails. They included standard phishing emails such as a new voicemail, an unpaid invoice, an order confirmation, Gmail, Weblogs, Valentines, and Security tokens [4]. The difficulty level could be compared to the users' expected and resulting click rates to determine whether the difficulty assessment needed to be adjusted. In addition, the test attempted to categorize these emails and determine their difficulty in tailoring training to users based on their overall results [4].

Our method can also tell us the testing results based on the email category. However, instead of narrowing down the problem area in an organization based on difficulty and class, we will assess the user's overall knowledge.

C. SpoofGuard

SpoofGuard is a project started by Stanford's Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D., and Mitchell, J. C. in the early 2000s [5]. It was created to assess current parameters against past parameters of a user to determine the likelihood that a website is a spoof. Like our method, the implementation will be in the toolbar for easy access. When a new webpage is accessed, SpoofGuard performs a series of checks with Boolean value output to determine whether or not the website is legitimate [5]. Our method is similar but will be checking phishing emails and, at this time, will not be as automated but user interactive. The user interaction, in our opinion from past research, would be beneficial because if the user is answering a series of questions about the email, they are more likely to retain the information on identifying red flags in an email.

SpoofGuard also has an email check we were particularly interested in because it checks whether a URL was clicked on in an email and performs a known address check [5]. In the time given, We will not be implementing such automated checks but see the usefulness of adding them to future versions.

3. Motivating Example

After reviewing the 2022 Cost of Data Breach Report from IBM and the Ponemon Institute indicated that 21% of data breaches resulted from human error. With Phishing being 16% of breaches and costing an average of $4.91 million, helping companies reduce their phishing attack clicks is crucial [2]. Although current methods are not proven ineffective, we began to think that maybe an additional step to current practices could give user awareness the push needed to lower the 21%. Phishing Email Properties [6]:

• Unrealistic Demands
o The email phrasing is intimidating and urgent.

• A Catch
o This type can be a request for money or a "too good to be true" offer

• Poor Grammar
o There are misspellings and grammatical errors within the test or user/company names

• Mismatched URL
o If the hyperlink address is not the same as the embedded link address, it is most likely a phish.

• Requesting Sensitive Information
o You should be cautious if the email asks you for

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0023

sensitive information.

Relevant Breaches

Just this year, we have been impacted by phishing attacks with massive consequences:

i. Acorn Financial Services - is just one example. In August 2022, an employee lost their credentials through a phishing email. The results were catastrophic as the attackers stole sensitive customer and employee information, including names, addresses, identification numbers, bank account numbers, social security numbers, and much more [7]. This attack is an excellent example of how one user can impact an entire organization by clicking the wrong link.

ii. Twilio – Phishing can also take the form of a text message or phone call, as is the case with the Twilio breach of August 2022. Twilio's site had been breached by sending a link to users and redirecting them to a false website resembling the legitimate Twilio website [7]. When entering their credentials on this website, the users unknowingly handed over their accounts to the attackers logging their inputs. This activity resulted in a substantial loss of customer data and affected around 75 million users [7]. The attackers could then steal the user's identity and wreak havoc on the system.

4. Hypothesis

If people have an easily accessible reference to phishing email characteristics, the number of phishing emails clicked on will be reduced.

5. Methodology

To construct the idea of an easily accessible resource to help users identify potentially malicious emails, we decided to use a quiz method. A quiz can be customized to be user-friendly, making it more applicable to users with varying knowledge of phishing emails. The customizations can also be altered to use questions related to the current year's red flag data. To optimize the accuracy of the quiz, we decided to randomize the questions, so they were consistent but in no particular order each time. Color coding of the questions and results ensures a visual understanding of the answers selected and corresponding results. We used green to represent a "good" or low-risk answer while "red" represents a high-risk answer. There are currently four questions in the quiz:

• Are there any typos in the email?
o If there are any grammatical errors in the email, it is a red flag and likely a phishing email.

• Is there a sense of urgency to click the link?
o If there is an urgency to click the link, update information, or perform an action, this is a red flag and likely a phishing email.

• Is the email address from their company website?
o If the email domain name is not what the company website provides, it is a red flag and likely a phishing email.
o Additionally, automation or guided instruction to hover over the link to see if it is the same as the sender could improve this method.

• Are you being asked for sensitive information?
o If you are being asked for sensitive information such as credit card numbers, social security numbers, identification, passwords, etc.…it is likely a phishing email.

We chose these questions based on some of the most common and consistent questions regarding phishing red flags [6]. Of course, there are many other red flags regarding Phishing, but these four were utilized in testing and deemed the most appropriate (see Figure 1).

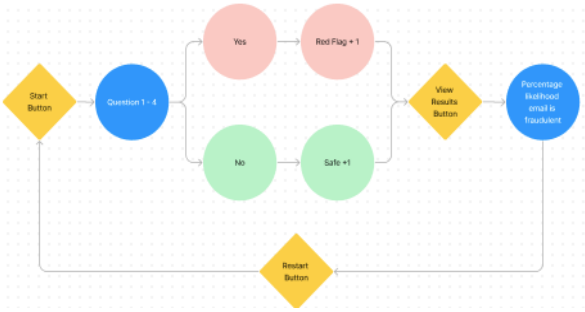

Figure 1. Extension Flow Chart

6. Execution

Phase one

The participant size for this test ended up being ten individuals of varying training backgrounds. They were grouped into categories of no anti-phishing training (A – four participants), some anti-phishing training (B – three participants), and annual/quarterly anti-phishing training (C – three participants). The users were given the three duplicate emails to analyze and decide whether they were fraudulent.

Phase two

The experiment was repeated using the same 10 participants and emails. The chrome extension tool was provided, and the quiz could be taken for each email to assist in their new decisions. Once this was

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0023

complete, the results were captured and compared to the previous results.

We thought the execution of this quiz would be most accessible in a chrome browser extension. Therefore, we used JavaScript to create the functions allowing interaction and viewing the quiz. For the results to be displayed, color coding, and display formatting, we used CSS styling and HTML to create visually stimulating and readable quiz formatting.

Based on the number of questions for each test, we calculated the results in increments of 25% (see Table 1 and Figure 2).

Table 1. Calculated results in increments of 25%

Questions flagged:	Percentage likely to be a phishing email:
1 of 4	25%
2 of 4	50%
3 of 4	75%
4 of 4	100%

Figure 2. Extension Execution

Implementation Difficulties

There are a few problems we encountered while executing this solution. Fitting the extension to the screen exactly enough to be fully visible while also displaying the email in question proved troublesome. There are too many scale adjustments to find the perfect ratio, and it could still be a bit better. We also noticed a flaw where the answer to the selected question is not locked in after clicking it. While using the tool, we see if yes is selected, and no can be chosen immediately until the next is clicked. This check would need to be fixed because selecting multiple answers within one question creates a false red flag and safe variable counters.

7. Evaluation

User Interface

At the opening of the chrome extension, user will see only a Start button for simplicity. Once clicking start, the questions will be shuffled into a random order, and the first will be displayed. When the user clicks an answer, the background and button color will turn green or red based on whether this answer is good or bad. Red indicates that this answer added one to the red flag variable count, while green represents an addition to the safe variable count. Once all four questions are answered, a "View Results" button will be displayed and once clicked, will show the likelihood an email is malicious. This prediction is calculated by dividing the number of red flags by the number of total questions.

Ease of Use

We observed the user interface was not an obstacle for the users who navigated it for the first time. Each button was straightforward, and the area around the questions was cleaned up of any extra data not necessary to the user at that moment in time.

Performance

We did not experience any performance issues with this extension. While using the extension on various machines, it did not show signs of lag with multiple other applications running, display issues such as buttons in the wrong place, or test showing in the background from previous functions.

Difficulties Along The Way

There are a few problems we encountered while executing this solution. Fitting the extension to the screen exactly enough to be fully visible while also displaying the email in question proved troublesome. There are too many scale adjustments to find the perfect ratio, and it could still be a bit better. We also noticed a flaw where the answer to the selected question is not locked in after clicking it. While using the tool, we see if yes is selected, and no can be chosen immediately until the next is clicked. This problem would need to be fixed because selecting multiple answers within one question creates a false red flag and safe variable counters.

8. Empirical Evidence

The results of this project were derived from testing ten users against three emails and giving them the chrome extension tool to compare before and after results (see Table 2 and Figure 3). The results are as follows:

Table 2. Quiz Questions

Questions:	Options:
Are there any typos in this email?	Yes or No
Is there an urgency to click the link?	Yes or No
Is this the email address from their company website?	Yes or No
Are you being asked for sensitive information?	Yes or No

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0023

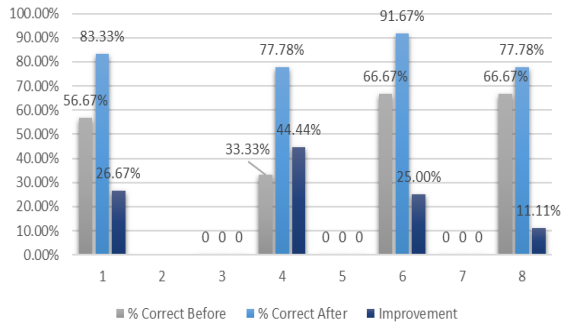

Figure 3. User Results

9. Future Work

Automation

The goal for this solution was to keep automation to a minimum. This goal is to ensure user interaction and predict this would improve the user's long-term memory of the tool. After using this tool for some time, we would add automation to specific areas, including scanning for typos in the test and comparing the hyperlink address value to the embedded link value for equality. Of course, this would come with additional security and privacy measures to be put in place.

More Questions

There are many red flags for an email; it would be wise to add more to the quiz at some point. This addition would ensure each user has covered all their bases regarding how many phishing flags exist in the email in question.

Results to a File

An improvement we found would be helpful after using the extension is to send the data to a file locally after each quiz for auditing reasons. This improvement allowed the user to audit historical activity. This audit would also make it easier to display the results within the tool from a database of entries. Creating the output into a table format from a log entry would make it look more uniform and make it easier to read the data while displaying any additional information to the user.

10. Conclusions

We concluded this process showed a clear improvement between both quizzes. As much of a threat statistically, Phishing involves users clicking malicious links; the group results were relatively high before the tool was given to them. Overall, the method showed improvements in their outcomes as predicted.

Our interactive approach to identifying phishing emails has become a method that we believe can significantly improve the number of clicks and user knowledge over time, especially in conjunction with other methods. The results reveal that users without experience still know which website characteristics to inspect. However, due to the dilemma of users clicking malicious links, perhaps users know what to look for and do not pay close attention at the time regarding some questions to ask themselves. With possible future modifications such as automated detection and improved conventional formatting for the visual references, this has the potential to help users learn what websites are real and which are not.

11. References

[1] Verizon. (2022). 2022 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf. (Access Date 15 November 2022).

[2] IBM. (2022). Ponemon Institute. Cost of a Data Breach Report 2022. IBM Security. https://www.ibm.com/reports/data-breach. (Access Date 15 November 2022).

[3] CS. (23-May-2007). Does Anti-Phishing Training Work? http://www.cs.cmu.edu/~jasonh/publications/apwg-ecrime2007- johnny.pdf. (Access Date 15 November 2022).

[4] Steves,M.P., Greene, K.K.,Theofanos, M. F. (24-Feb-2019). A Phish Scale: Rating Human Phishing Message Detection Difficulty. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/conference-paper/2019/02/24/rating-human-phishing-message-detection-difficulty. (Access Date 15 November 2022).

[5] Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D., and Mitchell, J. C. (2000). Client-side defense against web-based identity theft. https://crypto.stanford.edu/SpoofGuard/web spoof.pdf. (Access Date 20 November 2022).

[6] Milnsbridge. (23-Aug-2022). 5 Characteristics of a Phishing Email. https://www.milnsbridge.com.au/5-characteristics-phishing-email/. (Access Date 24 November 2022).

[7] McCurdy, R. (08-Nov-2022). The biggest phishing breaches of 2022 and how to avoid them for 2023," Security Boulevard. https://securityboulevard.com/2022/11/the-biggest-phishing-breaches-of-2022-and-how-to-avoid-them-for-2023/. (Access Date 16 December 2022).

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0023