Phishing with a License: Measuring the Susceptibility of Students to Phishing Attacks by Developing a Phishing Simulation

Joseph Dreese
Pennsylvania College of Technology
One College Avenue
Williamsport, PA 17701
(717) 756-3840
jmd27@pct.edu

ABSTRACT

Phishing attacks continue to be one of the biggest security risks for organizations. A report published by PhishMe found that in 2016, 91% of cyber-attacks and data breaches began with a spear phishing email.[15] Phishing is a cybercrime that involves an attacker attempting to collect confidential or sensitive credentials through electronic communication by impersonating a trustworthy organization or individual. This paper outlines the significance of phishing attacks and the steps that organizations can take to defend against them. This study can be used as a reference by organizations to develop and execute successful phishing simulations at a relatively low cost. The phishing simulation outlined in this paper covers the random selection of 600 college students and the methods used to gauge their susceptibility to phishing attacks. Of the 600 emails that were sent during this phishing simulation, 196 emails were opened and 139 phishing links were clicked. Overall there was a click-rate of approximately 23.18% however, of the emails that were opened and view, approximately 71.9% of them resulted in a clicked phishing link. Phishing simulations provide an excellent foundation for understanding an organizations susceptibility to phishing attacks. This study proves that an effective phishing simulation can be developed and executed for the low cost of $60.58

CCS Concepts

• **Information systems** • Information systems~Hypertext languages • **Security and privacy~Spoofing attacks** • **Security and privacy~Phishing** • **Security and privacy~Penetration testing** • Security and privacy~Trusted computing • Security and privacy~Social aspects of security and privacy • Security and privacy~Usability in security and privacy • **Human-centered computing~Web-based interaction** • **Applied computing~Education** • General and reference~Measurement • General and reference~Metrics • Computing methodologies

Keywords

Phishing; Phishing Simulation; Security Awareness; Cybercrime, Penetration Testing; Gophish;

1. INTRODUCTION

Phishing attacks continue to be one of the biggest security risks organizations face. A report published by PhishMe found that in 2016, 91% of cyber-attacks and data breaches began with a spear phishing email.[15] According to State of the Phish 2018, a survey of information security professionals indicated that 76% reported experiencing phishing attacks in 2017.[7] Phishing attacks play a major role in the security of organizational information and systems. Phishing attacks can also lead to identity theft which continue to be a wide-spread issue. To defend against phishing attacks individuals and organizations need to develop a better understanding of what phishing is, who conducts phishing attacks and what makes phishing attacks so successful.

It has become popular among organizations to conduct phishing simulations in order to better understand the susceptibility of the members of the organization and to gauge the specific risk that phishing attacks pose to the organization. By conducting a phishing simulation, an organization can create a baseline of the its susceptibility to phishing attack and use this data as a reference for future simulations. This paper will cover steps that were involved in the creation and deployment of a phishing simulation which targeted students attending Pennsylvania College of Technology. This paper will present the results of the simulation as well as provide lessons learned and recommendations based off of the results.

2. PHISHING ATTACKS

2.1 What is Phishing?

2.1.1 Definition

Phishing is a cybercrime that involves an attacker attempting to collect confidential or sensitive credentials of an individual through electronic communication by impersonating a trustworthy organization or individual. The majority of phishing attacks begin with a spoofed emailed that appears to originate from a legitimate organization making it difficult for users to find any difference based on appearances.[5]

2.1.2 History of phishing

Figure 1 is a timeline of the evolution of phishing attacks between 1996 and 2006.[3] It was in 1996 that the term phishing was first used publicly to describe the theft of AOL access credentials. The following year was when customers were warned of the threat of phishing by media publications. After the year 2000, the pace of phishing activity rapidly increased. In the year 2000, keyloggers became a prevalent way to gather credentials by phishers. The next year, phishers began to obfuscate URLs to direct victims to spoofed websites.[3] This evolution of phishing over the decade between 1996 and 2006 was rapidly progressing and not many were aware of the risk which made it very difficult to defend against. In 2018, though the majority of individuals know that phishing exists, phishing attacks continue to be one of more prominent risks to an organization.

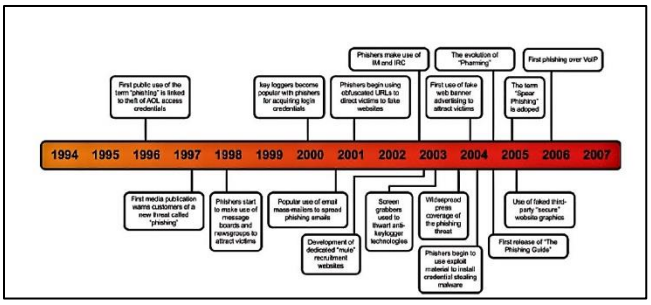

Figure 1. The evolution of phishing timeline, 1996-2006.[3]

2.2 What is the Significance of Phishing Attacks?

A study was conducted between March 2016 and March 2016 by individuals from Google, the University of California, Berkeley and the International Computer Science Institute. The purpose of the study was to provide longitudinal measurements of underground credential theft and analyze the risk it poses to public users.[8] Using Google as a case study, they observed that only 7% of victims have their current Google password exposed by data breaches of third parties. Comparatively, it was observed that 12% of keylogger victims have their current Google passwords exposed and the rate is much higher with 25% of phishing victims having the password exposed.[8] The study found that phishing victims are 400 times more likely to have their accounts hijacked compared to random Google users. This rate is much lower for data breach and keylogger victims with a rate of 10 times as likely for breach victims and 40 times as likely for keylogger victims.[8]

This study was developed around Google accounts with the significance of exposed Google credentials leading to other accounts being compromised because of password reuse. By using data from 7 of the largest data inverted credential[8] leaks between 2012 and 2014, they observed that 17% of the 22 million email addresses re-used the password at least once. In a study performed by Das et al. 10 fully inverted leaks from 2006-2012 were analyzed and they discovered that for 6,077 accounts 43% of them reused the password.[8] This fact that a high percentage of individuals reuse passwords means that if one account is compromised by a phishing attack, then there is a significant chance that other accounts can be hijacked using the same credentials.

2.3 Who Conducts Phishing Attacks?

2.3.1 Cyber criminals

Cyber criminals are individuals who conduct various attacks such as phishing to collect and profit from user data and credentials. They identify and exploit vulnerabilities for malicious purposes. The goals of cyber criminals can vary but they are usually looking to steal user credentials, collect data of individuals or organizations for sale, or gaining and maintaining access of systems to create zombie systems or botnets.

Cyber criminals use various influencing techniques to manipulate targets into clicking the malicious link. The email needs to appear to be genuine and should influence the target to take action with minimal consideration. These actions could include clicking a link, opening an attachment or providing the sender sensitive information.[9] In regards to phishing attacks, there are five techniques that are often used by cyber criminals. The first technique is to instill a sense of urgency in the victim.[9] This can be something as simple as requiring a response to an email in a limited amount of time. The second technique is "providing information of interest or use to the user".[9] This involves attention grabbing information to a user to create curiosity. The third technique used is encouraging an emotion response from the user.[9] This can be similar to the sense of urgency technique or it can create a positive emotional response such as winning a prize or receiving large discounts. The fourth technique commonly used by cyber criminals is "exploiting compliance with authority".[9] This occurs when a cyber-criminal impersonates a high ranking individual or person of authority and instructs the user to perform a task or provide certain information. The final technique that is commonly used by cyber criminals is focusing on contextual or work-related communication norms". [9] This could include using a spoofed email invitation to a holiday celebration or using an email involving a newly updated policy. There are many other techniques used by cyber-criminals but these are the most common.

2.3.2 Penetration testers and cyber professionals

Penetration testers are individuals who conduct, identify, and exploit vulnerabilities of organization just as cyber criminals do. The difference, however, is that penetration testers are given permission by the organization to do so. The goal of a penetration tester or cyber professional is to identify vulnerabilities and exploit them at the request of organizations. There is no malicious intent when conducting a penetration test. The purpose is to test the security of an organization and identify any risks. Penetration testers will document all their findings and present them to the organization as well as provide recommendations and possible solutions. Penetration testers may use many of the same techniques that cyber criminals do, but the important difference is the techniques they use must be approved by the organization.

2.4 Why are Phishing Attacks So Successful?

One of the main reasons phishing attacks are so successful is the lack of awareness individuals have about phishing attacks.[1] Many individuals do not know how to identify phishing attacks and do not understand the different techniques attackers will use to deceive them. This is why having a Security Awareness Training and Education (ATE) program is crucial for organizations. Another reason phishing attacks are so successful is that attacks will take advantage of psyche factors of individuals to manipulate their emotions and create a sense of urgency or panic. Creating an emotional response leads the user to act without critical thought and, ultimately, leads the user to click a malicious link.

3. THE PURPOSE OF THIS SIMULATION

Phishing simulations can significantly help an organization improve its security posture by providing baseline measurements for the susceptibility of users to phishing attacks. One potential benefit of phishing simulations is that they can be used to raise employee awareness of the risks of phishing emails. Phishing simulations "not only provide a means to educate users but also allows the organization to understand its relative risk from phishing".[9] Phishing simulations can also be used to create a proportional baseline of the amount of staff that are likely to fall for phishing email. Click-rates are commonly used as the main statistic for phishing simulations.

By using phishing simulations to create a baseline, organizations give themselves a starting point on which to improve their security posture. This improvement happens through the use of Security Awareness, Training, and Education. ATE is commonly seen as the best defense against phishing attacks. ATE has been defined as "educational program that aims to reduce security breaches cause by lack of employees' security awareness".[1] Phishing attacks

exploit human vulnerabilities of an organization. no matter how many firewalls, encryption software, and authentication methods are implemented, none of that will matter if individuals continue to fall for phishing attacks.[6]

4. SETTING UP A PHISHING SIMULATION

4.1 Requesting Permission

The Pennsylvania College of Technology was contacted to request permission to conduct this phishing simulation on students. This involved asking permission to work outside of the Acceptable Use Policy. There are no federal laws that specifically identify phishing as an illegal act but there were actions taken to create these laws. A bill introduced in 2005 known as the Anti-Phishing Act of 2005. sought to criminalize Internet scams that involve fraudulently obtaining personal information, commonly known as phishing.[6] The bill also proposed a five-year prison sentence and/or fine for any individuals who committed identify theft or spoofed any corporate websites or emails.[6] The Anti-Phishing Act was never written into law at the federal level. Currently, however, currently 23 states and Guam have laws that specifically target phishing.[4]

Requesting permission should always be done before conducting a phishing simulation, any type of penetration testing, or related activity. It is important to be completely transparent and identify the intentions of the simulation as well as to research different policies and laws that may be associated.

4.2 Creating a Target List

An outside actor would not usually have access to student directories with student names and emails. This particular phishing simulation was not conducted from the perspective of an a outside actor. The purpose of this simulation was to create a baseline of the students' phishing awareness, so certain internal resources could be used. Since this simulation was not conducted from the perspective of an outside actor internal student directory and email resources were used to develop a target list.

The Pennsylvania College of Technology has six distinct schools with multiple majors under each. 100 students were selected randomly from each of these schools. All of the majors were listed and searched in the student directory to find the total number of students in each major for each school. Each student was assigned a number and the random number generator selected the student out of the total amount. It was a tedious process but it was the only way to truly select random targets.

4.3 Choosing a Phishing Platform

The first step in setting up a phishing simulation is choosing a platform. There are several open source phishing simulations available. The Infosec Institute provides a list of the top 9 free phishing simulators that are available. Some higher ranked phishing simulators on the list were SecurityIQ PhishSim, Gophish, Lucy, and Simple Phishing Toolkit (sptoolkit).[2] Gophish was selected as the phishing platform for this simulation. Gophish had just released a new version Gophish v0.5.0 on January 27, 2018. Gophish is a phishing framework developed by Jordon Wright. It is completely free open-source software that is written in the Go programming language. It is simple to use and it is well documented.[10]

4.4 Installing the Platform

Much of the installation process was relatively simple. Gophish provides a user guide that walks users through the installation and configuration process. The user guide not only outlines the installation and configuration process, it provides step by step instructions on how to build a campaign.[10] The developer, Jordon Wright, can be contacted on GitHub. He provides timely support for any questions or issues that users may have. Installing Gophish is as simple as downloading the zip file for your operating system from the web site, extracting the contents and running the application.[10] The application can be accessed by opening a web browser and typing the local IP and port of the admin server, 127.0.0.1:3333.[10]

4.5 Purchasing a Domain

Amazon provides discounts to students when they sign up for Amazon Prime using their college email address. It was because of this reason that Amazon was chosen to be the organization that the emails would appear to be originating from. A combination of domain names was searched but eventually it was decided that amazonaccounts.info would be the domain. This domain was relatively inexpensive and seemed like a legitimate domain from which an amazon email might originate. For a small fee an Office 365 email was purchased from GoDaddy that incorporates using the new domain.

4.6 Hosting a Landing Page

The hosting services were also purchased from GoDaddy. The purpose of this phishing simulation was only to collect a baseline of click rates. It was necessary to deceive the students only to the point of clicking the phishing link. For this particular simulation, there was no need to spoof or clone a website because no credentials were going to be harvested. GoDaddy's hosting services are broken into 3 tiers and 5 accounts types. For the landing page for this project, the Economy Tier was chosen and the account type was Linux Hosting with cPanel.[11] The landing page was developed using WordPress which is free when using GoDaddy hosting services.

The landing page was developed to inform the student that the email they received was only part of a simulation and that is was a project approved by the Pennsylvania College of Technology. Figure 2 is the landing page that students would be directed to after they clicked the phishing link/button. The landing pages explains the scope of the project to the students and provides 3 additional links on a navigation bar for them. The first link directs them to a survey created on surveymonkey.com. The second link is a phishing awareness video for them to watch at their convenience. The last link on the navigation bar goes to a page with a link to a phishing awareness game Anti-Phishing Phil. Anti-Phishing Phil is a game that was created by the CMU Usable Privacy and Security Laboratory (CUPS) at Carnegie Mellon University. The game can be found at http://www.ucl.ac.uk/cert/antiphishing/.

Overall, the landing page was created to inform the students that the phishing email was not malicious and was only a simulation. The landing page was also meant to improve the phishing awareness of the students through the use of a phishing awareness video and game. The survey was created to capture basic data of the students who clicked the link such as age ranges, year in college (freshman, sophomore, etc.) and major they were studying at the college. The survey also included questions asking if the students think the college should require phishing awareness training and if they think the college should have a button added to the college email client to report phishing emails.

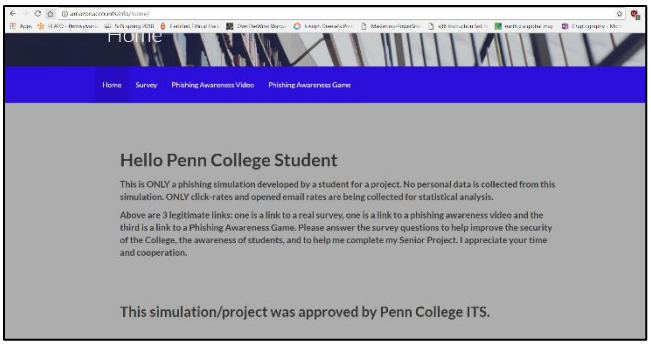

Figure 2. Landing page.

4.7 Creating an Email Template

The template was created using HTML in Brackets. The code was then transferred to the Gophish platform so that it could be stored and used for the campaign. Figure 3 is the template that was used for the phishing simulation. It is a fairly simple template that creates a sense of urgency for the recipient by informing them that their request to have their billing address changed has been successfully completed. The address in the template was randomly chosen using a tool at http://www.fakepersongenerator.com/random-address. The variables {{FirstName}} and{{LastName}} are used by Gophish to add the first and last names of the recipient, making the email more personable and legitimate. Gophish also adds a tracking variable {{.Tracker}} that represents an image that will be added to the email that is not visible to the recipient. It is also necessary to use the {{.URL}} variable to link any buttons or links you want the targets to click on. This variable creates a link that will direct users to the established landing page and record the activity.

Figure 3. The email template used for this simulation.

4.8 Building a Server

Amazon Web Services AWS has a 12-month trial of their services. One of the services included in the free trial is the creation of cloud-based servers. A server was created using AWS free tier trial for the purpose of hosting the phishing platform so that when targets opened the email or clicked the phishing link the activity would be accurately recorded. One issue with hosting the phishing platform on AWS is that there is a specific policy in place against using their services for penetration testing or simulations without first requesting permission.

During a meeting with members of the Pennsylvania College of Technology Information Technology Services (ITS), it was suggested that if a response was not provided in a timely manner from AWS, a server could be created internally. AWS responded within a few days but due to time constraints it was decided to have a create a server internally. The Pennsylvania College of Technology's ITS created the server and ensured it was isolated from the data center by creating Access Control Lists.

4.9 Configuring the Platform

Once the internal server was created all that need to be done was to download and install GoPhish on the Sever and import the target lists, email template and the landing page. The only change from the configuration process this time was the json file within the GoPhish folder. Figure 4 is the original json file for Gophish. The only item that needed to be changed is the listen_url for the admin_server. The IP address for the listen_url needs to be the IP address of the server Gophish is being hosted on. This is the new IP address will be entered in the browser following the launch of the GoPhish application with the same port of 3333. There is not much more configuration needed to use GoPhish once the target list, email template, and landing page are imported. There are, however, a few things to consider creating a sending profile and creating a campaign.

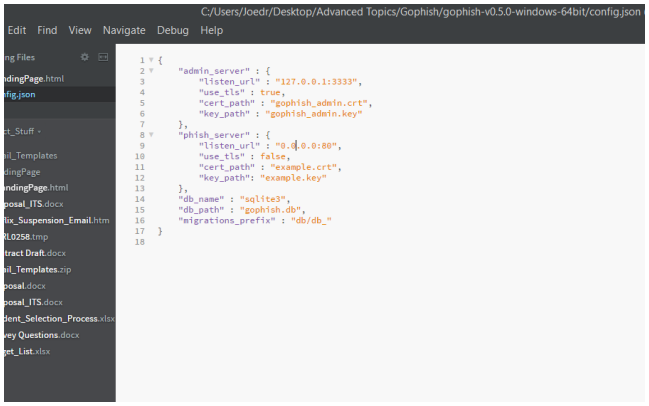

Figure 4. GoPhish json file.

Figure 5 is the displays the different textboxes where information input is needed for the sending profile. The first box simply requires a name for the sending profile. For the From, Username, and Password boxes, the email address the phishing email will be sent from needs to be entered as well as the credentials associated with that account (Username and Password). The most significant information needed for the user profile is the Host information. The information needed for the Host section is the SMTP relay server the associated port number. The SMTP server and port combination for Gmail services is what was used for this simulation. The server is smtp.gmail.com and the port being utilized is 587.

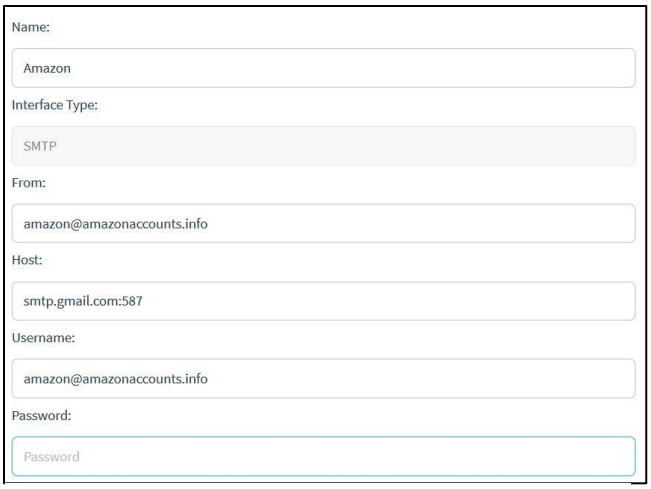

Figure 5. Sending Profile.

The next thing that needed to be considered when configuring the platform was the requirements for a new campaign. Figure 6 displays the different requirements for creating a new campaign. The first requirement is the name given to the campaign. For this particular the simulation, there were 10 different waves of targets, deathstar, deathstar2, etc. The next two options are the email template and the landing page. For these requirements, there are dropdowns to select the email template and landing page that have already been imported. The URL requirement is a very important consideration. In the user guide for GoPhish, the instructions say that 127.0.0.1:3333 should be entered. This is only the case when testing the platform on a local machine. For the platform to host the landing page properly and to record opens and click-rate activity the URL must be the IP address of the Server on which it is being hosted. The Schedule requirement is very beneficial because it allows for campaigns to be launched at a specific date and time. For this particular phishing simulation, there were 600 selected targets separated into 10 different waves. This requirement allowed for the waves to be launched at different times at random intervals to decrease suspicion and prevent the email source from being flagged.

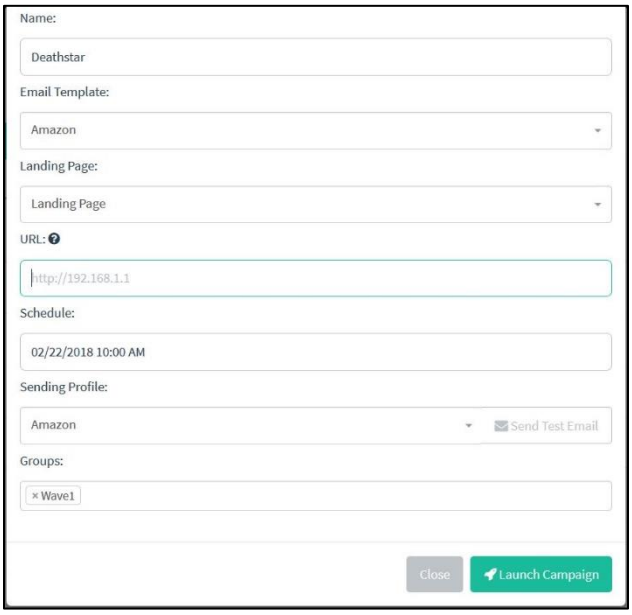

Figure 6. Campaign Options.

4.10 Using GSuite

Following some research, it was discovered that the email provided by GoDaddy only had a limit of 250 messages sent a day.[12] If more relays are needed for a GoDaddy account they can be purchased in packs of 50. Since this simulation involved sending 600 emails in a day, an alternative was needed. GSuite can be used to send up to 2000 emails a day per user and it allows for an existing business email domain to be used. This was important because the spoofed email was vital in deceiving the students during this simulation. Setting up GSuite to use an existing email domain is fairly simple. It involves adding an MX record to the domain's DNS records table.[14] When GSuite account is initially set up it is on a free 14-day trial. During the free trial only 500 emails per account can be sent.[13] The trial needed to be waived to allow the number of emails for this simulation to be sent.

4.11 Cost of the Simulation

Setting up this simulation involved many different services and tools but it was relatively inexpensive to perform. The most expensive service was the monthly cost for using Survey Monkey. Survey Monkey's basic plan is free but it only allows up to 100 responses. For the simulation, there was a chance that there would be more than 100 individuals clicking the phishing link and being directed to the landing page where the survey link resides. By upgrading to the standard plan for $37/month, surveys can have up to 1000 responses. Fortunately, Survey Monkey does have a discount for students, educators, and nonprofits which reduces the cost to $25/month. The second most expensive service was the GoDaddy hosing service. The Economy Tire Linux Hosting with cPanel was $15.82. The domain and email account were purchased together with the domain cost of $3.17 and email account cost of $5.29. An additional feature was chosen to make the register the domain as a private domain so that tools like WHOIS could not be used to identify who owns the domain. An additional cost of $5.27 was paid in order to register the domain privately. Collectively the cost of the domain, the Office 365 email account, and the private registration cost a total of $13.73. The final cost for the simulation was the cost of the GSuite services. GSuite was only used for roughly a week and had a cost of $6.03. The total cost of setting up and performing this phishing simulation was $60.58

5. ANALYZING THE COLLECTED DATA

5.1 Simulation Results

Following the week-long simulation, the results indicated that out of the 600 emails that were sent, 196 were opened and 139 individuals clicked the phishing link. Figure 7 is the visual representation of these results provided by Gophish. Of the total 600 emails sent, approximately 32.66% were opened. Overall there was a click-rate of approximately 23.18% however, out of the total opened emails, there was approximately a 71.9% click-rate. This means that of the 196 individuals who opened the email 71.9% clicked the phishing link that redirected them to the landing page.

Figure 7. Visual Results of Emails Sent, Emails Opened, and Clicked Links

Gophish provides the capability to export the raw results to a CVS file. The results that Gophish produces provides the user agent of the individual who clicked the phishing link. This user agent includes the device and operating system used by the individual when they clicked the phishing link. To better understand the habits of those who clicked the links, PowerShell scripts were written and executed on the results to identify what devices were used when individuals opened the phishing email and clicked the link.

The results indicated that there were 71 iPhones, 2 iPads, 10 Macs, 36 Android devices, and 24 Windows devices used to click the phishing link. A total of 143 devices were used to click the phishing link. There were a total 139 students who clicked the link using 143 different devices. This means that a few users clicked the link using multiple devices.

5.2 Survey Results

Unfortunately, there was a relatively low response rate for the surveys. During the simulation there were a total of 139 students who clicked the phishing link but only 14 individuals took the survey. Due to the lack of responses, an email was sent out to those individuals who clicked requesting them to take the survey. This time 23 students responded to the survey. Both of these samples are relatively small when compared to the number of students that clicked the phishing email. Additionally, there was no clear way to tell if there were repeating respondents between the two samples

For the first group of 14 respondents, 85.51% were between the ages of 18-24 and 14.29% were between the ages of 25-34. Of the individuals in group 1, 21.43% were juniors, 50% were sophomores, 28.57% were freshman, and there were no seniors. When asked if they think the college should require phishing awareness training for the students, 57.14% selected yes and 42.86% selected no. When asked if they think the college should implement a button in Outlook to report suspected phishing emails, 92.86% selected yes and 7.14% selected no.

For the second group of 23 respondents, 82.61% were 18-24 years old, 13.04% were 25-34 years old, and 4.35% were 35-44 years old. Of the individuals in group two 30.43% were seniors, 26.09% were juniors, 26.09% were sophomores, and 17.39% were freshman. When asked if they think the college should require phishing awareness training for the students, 73.91% selected yes and 26.09% selected no. When asked if they think the college should implement a button in Outlook to report suspected phishing emails, 91.30% selected yes and 8.70% selected no.

Although there was a relatively low response rate for the surveys, demographic results for which of the six schools the students belonged to was still able to be produced. A PowerShell script was run on the user agents to create a list of all the students who clicked the phishing email. This list was compared to the original target list that was create that had information about the major and school the students belonged to. Of the students who clicked the phishing link, 18.7% were in the school of Business & Hospitality, 18.7% were in the school of Construction & Design Technologies, and 10.7% were in the school of Health Sciences. Additionally, 18.7% of the students were in the school of Industrial, Computing, & Engineering Technologies, 14.4% were in the school of Sciences, Humanities & Visual Communications, and 18.7% were in the school of Transportation & Natural Resources Technologies.

6. RECOMMENDATIONS

Based on the results of this simulation it is recommended that the Pennsylvania College of Technology begin to explore different ways to help students before develop a better awareness of phishing attacks. Based on the statistical information that was gathered from the simulation, it was determined that the students of the Pennsylvania College of Technology have a high level of susceptibility to phishing attacks. It is recommended that the Pennsylvania College of Technology find or develop an effective method to educate students on how to identify phishing emails and how to understand the types of techniques attackers will use to try to deceive them. It is also recommended that the Pennsylvania College of Technology implement an effective process or mechanism for students to report suspected phishing emails. This could include implementing a button into Outlook 365 for students to use. These recommendations are based on the statically analysis of the simulation results and on the results of the surveys.

7. LESSONS LEARNED

When conducting a study or experimental project, it is generally a good idea to reflect on what went well and what did not. There was a lot that went really well in this phishing simulation. The platform was successfully set up and hosted on a server. All the emails were sent and the results of opened emails and clicks of the phishing links were accurately recorded. There was a lot success when executing this phishing simulation but there were a few items that were overlooked.

One issue that was discovered was that those who clicked on the phishing link were not able to access the landing page. The landing page is hosted virtually by GoPhish and the link was directed to Gophish on the internal server. Those who clicked the link while on the campus network were able to reach the landing page that explained that the email was part of a simulation. Unfortunately, those who clicked it off campus did not reach the landing page that supplied information about the simulation project. This was either an issue with the College firewall or a configuration issue with the internal server. This led to a lack of survey responses on the landing page and a few unhappy emails responses from participants of the phishing simulation. This detail was overlooked because, to remotely access, the server an individual needed to be on the campus network. Therefore, all test emails that were sent to test accounts were accessed while on campus. It was an item that was overlooked for this simulation and that needs to be tested in future simulations to prevent the possibility of confusion and panic.

A second issue that was identified was the lack of survey responses. This lack of responses caused limited demographic analysis of the students who clicked the phishing link. For a better response rate for surveys in the future, an incentive of some sort needs to be implemented to make it worth the time for individuals to respond. For example, those who respond will be entered to win a gift card or some kind of prize. It may seem like individuals are being rewarded for not having security awareness but this is something that can produce better response results for surveys.

8. CONCLUSION

There is no solution that will completely protect an organization from phishing attacks. Phishing attacks will continue to be a risk to individuals and organizations, but there are steps that can be taken to limit susceptibility to phishing attacks. One way organizations can improve their defenses against phishing attacks is to conduct their own phishing simulation. This study has proven that an organization can perform an effective phishing simulation at a relatively low cost. A week-long phishing simulation was conducted for a low cost of $60.58. Conducting simulations can allow an organization to gauge the susceptibility of its employees to phishing attacks. This study found that, out of 600 emails that were sent, 196 were opened and 139 individuals clicked the phishing link. This result indicates that approximately 23.18% of emails sent resulted in the link being clicked. Of the students who opened the phishing email, approximately a 71.9% viewed it as a legitimate email and clicked the phishing link.

The best way to defend against phishing attacks is to have an effective Security Awareness, Training, and Education (ATE) program in place. The data collected from phishing simulations can be used to create a baseline to be compared to for future simulations. By comparing newly collected data to the baseline, an organization can identify if their ATE programs are effective. Based on the data collected in this study, it is recommended that the Pennsylvania College of Technology implement phishing awareness training for students and conduct a simulation in the future to weigh the effectiveness of the training. This study and report can be used by the Pennsylvania College of Technology and other organizations as evidence of the importance of phishing awareness and to develop inexpensive phishing simulations to measure their susceptibility to phishing attacks.

9. ACKNOWLEDGMENTS

Special Thanks to ACM SIGCHI for allowing us to modify templates they had developed.

Special thanks to the Pennsylvania College of Technology for allowing this phishing simulation to be conducted and for allowing the use of their internal server.

Special thanks to Dr. Sandra Gorka for reviewing and facilitating this project.

10. REFERENCES

[1] Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security Awareness Training: A Review. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 5-7).

[2] Antipov, A. (2017, September 26). Top 9 Free Phishing Simulators. Retrieved March 10, 2018, from http://resources.infosecinstitute.com/top-9-free-phishing-simulators/

[3] Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing Attacks and Defenses. International Journal of Security and Its Applications,10(1), 247-256. doi:10.14257/ijsia.2016.10.1.23

[4] Ncsl.org. (2018). *State Phishing Laws*. [online] Available at: http://www.ncsl.org/research/telecommunications-and-information-technology/state-phishing-laws.aspx [Accessed 10 Mar. 2018].

[5] Sankhwar, S., & Pandey, D. (2017). Defending Against Phishing: Case Studies. *International journal*, *8*(5).

[6] Shi, J., & Saleem, S. (2012). Computer Security Research Reports: Phishing. *University of Arizona*.

[7] Technologies, W. S. (n.d.). 2018 State of the Phish™. Retrieved March 10, 2018, from https://www.wombatsecurity.com/state-of-the-phish

[8] Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., ... & Margolis, D. (2017, October). Data Breaches, Phishing, or Malware?: Understanding the Risks of Stolen Credentials. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1421-1434). ACM.

[9] WILLIAMS, E. J., & JOINSON, A. (2017). Understanding Employee Susceptibility to Phishing: A Systematic Approach to Phishing Simulations. *ndm*, 265.

[10] WRIGHT, J. (2018). *Introduction · Gophish User Guide*. [online] Gophish.gitbooks.io. Available at: https://gophish.gitbooks.io/user-guide/content/ [Accessed 18 Feb. 2018].

[11] Godaddy.com. (2018). What type of hosting account do I have? | GoDaddy Help GB. [online] Available at: https://www.godaddy.com/help/what-type-of-hosting-account-do-i-have-6971 [Accessed 11 Mar. 2018].

[12] Godaddy.com. (2018). How many email messages can I send per day? | Workspace Email - GoDaddy Help GB. [online] Available at: https://www.godaddy.com/help/how-many-email-messages-can-i-send-per-day-313 [Accessed 11 Mar. 2018].

[13] Support.google.com. (2018). Gmail sending limits in G Suite - G Suite Administrator Help. [online] Available at: https://support.google.com/a/answer/166852?hl=en [Accessed 11 Mar. 2018].

[14] Support.google.com. (2018). GoDaddy: Set up G Suite MX records - G Suite Administrator Help. [online] Available at: https://support.google.com/a/answer/33353?hl=en [Accessed 11 Mar. 2018].

[15] Dark Reading. (2018). 91% Of Cyberattacks Start with A Phishing Email. [online] Available at: https://www.darkreading.com/endpoint/91%E2%80%93of-cyberattacks-start-with-aphishing-email/d/d-id/1327704 [Accessed 12 Mar. 2018].