Beat the Bait: A Case Study on Phishing Attack

Neil Russel D. Ayap
School of Information Technology
Mapúa University, Philippines
nrdayap@mymail.mapua.edu.ph

Arfren Ceniel Y. Dabu
School of Information Technology
Mapúa University, Philippines
acydabu@mymail.mapua.edu.ph

Alejandro M. Reyes
School of Information Technology
Mapúa University, Philippines
amreyes@mymail.mapua.edu.ph

Aaron Benedict K. Ventura
School of Information Technology
Mapúa University, Philippines
abkventura@mymail.mapua.edu.ph

Ghibi P. Trinidad
School of Information Technology
Mapúa University, Philippines
gptrinidad@mymail.mapua.edu.ph

Dr. Eric B. Blancaflor
School of Information Technology
Mapúa University, Philippines
ebblancaflor@mapua.edu.ph

Abstract

Every year, cybercriminals become savvier with their phishing attacks and have tried-and-tested methods to deceive and steal from innocent victims. With this, this case study aims to remind all Internet users, especially people who work from home, about the posing threats when browsing or clicking suspicious links, to give warning to those who work in their own homes about the posing threat of keyloggers, and to provide sufficient knowledge to those who confidently work in their home about the threats of phishing. The researchers conducted a survey to its target users through the zoom meeting application. Purpose of the research were discussed in the zoom meeting as well. Research results show that the work from home employees understands the importance of knowing phishing attacks and keyloggers. It is crucial to do a security check-up of personal computers occasionally. Initially, in the researcher's pre-test, only 35% of the respondents strongly agreed that understanding phishing is necessary. However, after demonstrating how keyloggers work and how it may impact their systems, the initial 35% rose to 60%. Only 10% of the respondents think knowing phishing and keyloggers will not make their pc safer nor impact their work from home jobs.

Keywords
keylogger, phishing, cybercriminals, ransomware, malicious links

1. Introduction

According to a 2019 Verizon report, 32% of all data breaches involved phishing in one way or another. In addition, 90% of confirmed phishing email attacks occurred in environments that used Secure Email Gateways (SEGs). Phishing has developed into various highly sophisticated methods since its inception in 1987. As digital technologies advance, this assault will continue to discover new methods to exploit security vulnerabilities (Terranova Worldwide Corporation 2021).

Every year, cybercriminals become savvier with their phishing attacks and have tried-and-tested methods to deceive and steal from innocent victims. Because phishing attacks come in many different forms, differentiating one from a valid email, voice mail, text message, or information request can be difficult. Some links do not need any input from their victims. Once the victim clicks the link and allows it to execute what it intended to do entirely, without any sign, the victim's data is already in the hands of the hackers. This way does not only apply to phishing. It can also cause forced installation of ransomware to the victim's computer (Terranova Worldwide Corporation 2021).

This case study aims to remind all Internet users, especially people who work from home, about the posing threats when browsing or clicking suspicious links. Hackers may see the current lockdown situation as their perfect time to collect more data because users are on the internet, unsuspecting people may already be victims without knowing that they are. More so, it aims to make people understand that some emails may look legitimate, but it may include malicious links with keyloggers. The researchers will conduct a survey in which we will be using a keylogger tool and it will attach it through a link and send it through email. In this manner, it will assess the current condition of the target and identify security issues.

1.1 Objective of the study

- To delivery cautious information to those who work in their own homes about the posing threat of keyloggers.
- To determine the knowledge level of those who confidently work in their home about the threats of phishing.

1.2 Scope and Limitation

The scope and limitation of the study will focus on Work-from-home (WFH) workers. The study will have 15-30 participants, regardless of their type of occupation and age. The limitation is that only Keyloggers that are attached to emails will be used to test the awareness of the participant on the risks of malicious links and file attachments. The applications that will be used on the study will be ensured to be non-harmful for both the participant and researcher. Some of the keyloggers used may be flagged by antivirus software to be infected, but the keyloggers are tested and guaranteed to be safe.

2. Review of Related Literature and Studies

This section presents the related literature and studies after the thorough and in-depth search done by the researchers. Those that were included in this section helps to further the investigation and study that the researchers have done. This chapter shows how phishing and keylogging are making a huge negative impact on those who are not knowledgeable about cyber-attacks.

2.1 Don’t click: towards an effective anti-phishing training. A comparative literature reviews

With different business industries, it is said that emails play a vital role in communication channels. On the other hand, it promotes the act of phishing actively. According to the study conducted, it is mentioned that age can be a one of the determinants of those people who may be victims of phishing. Furthermore, in order for them to minimize their employees from becoming a victim, the business will conduct an anti- phishing training and the employees will agree with the said activity (Jampen et al. 2020).

2.2 A Systematic Literature Review on Phishing and Anti- Phishing Techniques

Using social engineering and technology, phishing technique and attack made end users aggressive in getting restricted and sensitive data. It is said that phishing is the most recorded threat in terms of the internet known in the whole world. With that, users are extremely bothered about the existence of new phishing attackers because as time passes by, they come up with more unique and creative styles in doing the said attack. Moreover, people who do not have enough knowledge about phishing are mostly the victims of it. Usually, phishing attackers send emails that are a scam to different internet users to access their private information (Arshad et al. 2021).

2.3 Phishing Email Detection Using Natural Language Processing Techniques

Due to the increase of internet users, security problems are also rising. Phishing attacks happen mainly for the reason to have the user's personal information as well as the private accounts of an individual. Since Covid-19 happened, attackers thought of making creative ways of attracting different internet users just like the use of different articles involving the topic regarding the pandemic. The articles or different links provided by the attackers seem to appear legitimate and reliable but, in the end, sensitive information is given to the people who are doing phishing techniques (Salloum et al. 2021).

2.4 A Literature Survey of Phishing Attack Technique

The target of most phishing attackers are those people who are unaware and do not have sufficient knowledge about the said attack. It is mentioned that internet users who are usually knowledgeable about phishing or scams are not really the common victims of phishing. The main goal or purpose of phishing is to gather sensitive and personal information from other people through the means of websites, links or different articles that are usually attractive to internet users. In addition, attackers value this information to steal data or money that will be beneficial to them (Pratik and Devale 2016).

2.5 Study on Cybersecurity Challenges of Working from Home during COVID-19 Pandemic

Workforces over the country considering work from home during the Covid-19 pandemic, massively alarmed the knowledge and use of IT infrastructure. With regards the preparedness of every employer, it is doubtful if they can be reliable in terms of cybersecurity. Moreover, cybercriminals take this opportunity to attack different users who are unprepared as well as those users who do not have enough knowledge about phishing or other cyber-attack. In addition to that, social engineering is also known as the cyber-attacks which are performed with those people who are referred to as the weakest link (Sebastian, G. 2021).

2.6 Let's Go Phishing: A Phishing Awareness Campaign Using Smishing, Email Phishing, and Social Media Phishing Tools

The goal of this study is to figure out how many users are more vulnerable to phishing assaults. The researchers will perform the study using an open source phishing toolkit, sending phishing links to various people via email, SMS, and social media to see how many users clicked on or ignored the link. The phishing campaign is carried out by constructing a fake online shop website on which targeted users can register for a chance to win a raffle using scarcity and urgency as motivator strategies. A survey for targeted users who clicked the phishing link will be conducted, followed by a post-survey for all targeted users, regardless of whether they accessed or ignored the phishing campaign (Blancaflor et al. 2021).

3. Methodology

Personal experience, human people, books, journals, and nature are all possible sources of information. A study can result in new knowledge being added to the corpus of knowledge. Research is the only way to make progress in a field. In research, many methods such as study, experiment, observation, analysis, comparison, and reasoning are employed (Ogidiaka et al. 2017). This portion discusses the research method used in the study. It also includes the selection of the respondents that participated in the research and the instruments that were used to gather data. It further discusses the statistical analysis from the responses of the participants. This chapter presents what keyloggers were used and experienced in the study.

3.1 Research Design

This study made use of a pre-experimental design. It was primarily concerned with determining the efficacy of two variables' interrelationships at the same time. To ensure the reliability and trustworthiness of synthesis positive sampling was used by the researchers to choose respondents since it is the greatest fit for the study's survey.

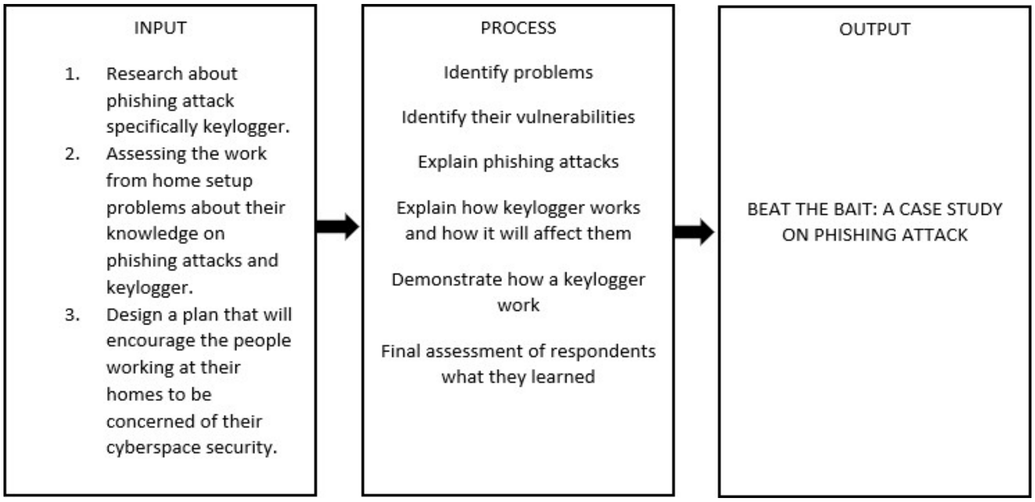
3.2 Research Instrument

The researchers conducted a survey through the help of the Zoom meeting application where the respondents and researchers could properly discuss the purpose of the research. The researchers also used Google Docs as a platform to conduct surveys for the respondents. As the host of the meeting finished discussing and showing the keylogger application. Respondents were given a survey questionnaire to collect data that will then be used to justify the study's objective.

3.3 Data Gathering

The twenty respondents of the study were tasked to answer a questionnaire survey pre-test then have undergone a Zoom batch meeting where they were oriented about how a keylogger works. After being oriented, they were sent an email with a keylogger attached, with their authorization, and it is to experience firsthand how it works running on their own computers. The keylogger used was named "Actual- Keylogger", after experiencing how keyloggers function, the respondents answered the rest of the questionnaire survey to gather their feedback about their awareness and experiences in malicious online baits and keyloggers.

3.4 Conceptual Framework



INPUT

1. Research about phishing attack specifically keylogger.
2. Assessing the work from home setup problems about their knowledge on phishing attacks and keylogger.
3. Design a plan that will encourage the people working at their homes to be concerned of their cyberspace security.

PROCESS

Identify problems

Identify their vulnerabilities

Explain phishing attacks

Explain how keylogger works and how it will affect them

Demonstrate how a keylogger work

Final assessment of respondents what they learned

OUTPUT

BEAT THE BAIT: A CASE STUDY ON PHISHING ATTACK

Figure 1. Conceptual Framework

The activities transcribed in this study is shown in the conceptual framework, see figure 1. Research and assessments on phishing tools, identifying issues in these kinds of attacks were conducted. Demonstrating how a keylogger works were also observed in this study.

4. Results and Key findings

Table 1. Respondents on Understanding phishing is a necessity

1. **Understanding phishing is a necessity**		
Answer	**Frequency**	**Percentage**
Strongly Agree	7	35 %
Agree	11	55 %
Neutral	2	10 %
Disagree	0	0 %

As shown in table 1, most of the respondents strongly agree about checking your personal computers' security occasionally. Some of them are still on the neutral side.

Table 2. Respondents view about the safety of clicking links indiscriminately

2. **It is safe to click random links and ads that offer too good to be true deals and giveaways.**		
ANSWER	**FREQUENCY**	**PERCENTAGE**
Strongly Agree	2	10 %
Agree	1	5 %
Neutral	2	10 %
Disagree	5	25 %
Strongly Disagree	10	50 %
TOTAL	20	100

Presented in table 2 shows that half of the respondents strongly disagree on clicking links indiscriminately, a fourth of them disagree, totaling 75% of the respondents. The rest is on the neutral side, and some say that it is safe to do so.

Table 3. View of the respondents on verification of links that they are accessing

3. **Knowing how to verify if a website is legit, is a must.**		
ANSWER	**FREQUENCY**	**PERCENTA GE**
Strongly Agree	9	45%
Agree	5	25%
Neutral	4	20%
Disagree	2	10%
Strongly Disagree	0	0%
TOTAL	20	100

As shown in table 3, almost half of the respondents strongly agree that verifying that a link or a website is legitimate first before accessing it is essential. A quarter of the respondents agree with it, the rest are neutral, and only 2 of them disagree.

Table 4. Perspective of respondents on vulnerability of work from home personnel compared to those who are working onsite

4. **Working from home makes oneself vulnerable to phishing attacks compared to working onsite**		
ANSWER	**FREQUENCY**	**PERCENTAGE**
Strongly Agree	6	30%
Agree	5	25%
Neutral	6	30%
Disagree	3	15%
Strongly Disagree	0	0%
TOTAL	20	100

As shown in table 4, 30% of the respondents strongly agree that they are more vulnerable than those working on site. They were backed with 25% of the respondents, which also agree with it, totaling 55%. The other 30% belongs to the neutral, which shows that they are either not sure or just on the neutral side. The rest disagrees that they are more vulnerable than those who are working on site.

Table 5. View of respondents on the usage of personal computer in a work from home setup

5. **Using personal computer can make you more vulnerable to phishing attack**		
ANSWER	**FREQUENCY**	**PERCENTAGE**
Strongly Agree	5	25%
Agree	5	25%
Neutral	6	30%
Disagree	4	20%
Strongly Disagree	0	0%
TOTAL	20	100

As shown in table 5, most of the respondents are with the neutral side which totals to 30% of them. In this section, respondents are almost equally distributed to strongly agree, agree and disagree. It shows that respondents have different perspectives about using personal computers for their work from home setup.

Table 6. Respondent's view checking the security of your pc occasionally for the risks of having keyloggers in it.

6. **The risk of having a keylogger in your system is a good enough reason to check your personal computer's security once a while.**		
ANSWER	**FREQUENCY**	**PERCENTAGE**
Strongly Agree	11	55%
Agree	7	35%
Neutral	2	10%
Disagree	0	0%
Strongly Disagree	0	0%

TOTAL	20	100

Most of the respondents strongly agree and agree about the checking of your personal computers' security occasionally, see table 6. Some of them are still on the neutral side.

Table 7. Respondents' post-test's reaction to understanding phishing is a necessity

7. Understanding Phishing Is A Necessity		
ANSWER	FREQUENCY	PERCENTAGE
Strongly Agree	12	60 %
Agree	6	30 %
Neutral	2	10 %
Disagree	0	0 %
Strongly Disagree	0	0 %
TOTAL	20	100

As shown in table 7, the percentage of the respondents that chose strongly agree with shows to be higher than the pre- test. With its percentage of 60% strongly agree and 30% agreeing with the total of 90% which leaves to the neutral side of 10% still.

Based on the survey results, most of the responses agree that the work from home employees understands the importance of knowing phishing attacks and keyloggers. It is crucial to do a security check-up of personal computers occasionally. Initially, in the researcher's pre-test, only 35% of the respondents strongly agreed that understanding phishing is necessary. However, after demonstrating how keyloggers work and how it may impact their systems, the initial 35% rose to 60%. Only 10% of the respondents think knowing phishing and keyloggers will not make their pc safer nor impact their work from home jobs.

5. Conclusion and Recommendation

Phishing is one of the ways hackers can collect data from their victims. One of the tools hackers can use to collect their victim's data is a keylogger. The potential threat of this application can put someone's privacy in danger, such as exposing their password and other security codes. Keylogger is just a simple tool to exploit victims' data, and there are still many ways hackers can gather unsuspecting victims' data that can put someone's life in danger.

The study contributed to the understanding and knowledge of the respondents and there were factors that are highly suggested for future awareness and use. The recommendations are as follows:

- To the people who are working from home, it is recommended that they should find ways to look up if the link that they are logging in or clicking is legitimate.
- To all computer users, it is recommended to check their personal computer's security even occasionally
- To all people who have the potential of using any computer, it is recommended to have sufficient knowledge about phishing attacks as well as the ways on how to avoid being a victim of any fraudulent attacks on the internet.

References

Arshad, Ayesha and Ur Rehman, Attique and Javaid, Sabeen and Ali, Tahir and Sheikh, Javed and Azeem, Muhammad, A Systematic Literature Review on Phishing and Anti-Phishing Techniques. 2021

Blancaflor, E., Alfonso,A., Banganay, K., Dela Cruz, G., Fernandez, K., and Santos S., Let's Go Phishing: A Phishing Awareness Campaign Using Smishing, Email Phishing, and Social Media Phishing Tools. *Proceedings of the International Conference on Industrial Engineering and Operations Management Harbin, China,* July 9-11, 2021.Available: http://www.ieomsociety.org/china2021/papers/108.pdf. 2021.

Jampen, D., Gür, G., Sutter, T. et al. , Don't click: towards an effective anti-phishing training. A comparative literature review. Hum. Cent. Comput. Inf. Sci. 10, 33, August 2020.

Ogidiaka, Emoghene and Ogwueleka, Francisca, Information Gathering Methods and Tools: A Comparative Study, 2017.

Pratik Patil and Prof. P.R. Devale , A Literature Survey of Phishing Attack Technique. Available: https://www.ijarcce.com/upload/2016/april- 16/IJARCCE%2050.pdf, April 2016.

Glorin Sebastian, A Descriptive Study on Cybersecurity Challenges of Working from Home during COVID-19 Pandemic and a Proposed 8 step WFH Cyber- attack Mitigation Plan, February 2021.

Said Salloum, et al., Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey, 2021.

Terranova Worldwide Corporation. 19 examples of common PHISHING Emails: Terranova security.Available: https://terranovasecurity.com/top-examples-of-phishing- emails/, May 2021.

Biography

Eric Blancaflor is an Associate Professor of Mapua University, Philippines. He earned B.S. in Electronics Engineering from Mapua University, master's in engineering major in Computer Engineering in the University of the City of Manila and Doctor of Technology in Technological University of the Philippines. He has published conference papers related to IT systems, network design and security.

Neil Russel D. Ayap is a student of Bachelor of Science in Information Technology in Mapua University, Philippines. His interests are into programming, web development, internet of things, network and systems administration.

Arfren Ceniel Y. Dabu is a student of Bachelor of Science in Information Technology in Mapua University, Philippines. His interests are into programming, web development, internet of things, network and systems administration.

Alejandro M. Reyes is a student of Bachelor of Science in Information Technology in Mapua University, Philippines. His interests are into programming, web development, internet of things, network and systems administration.

Aaron Benedict K. Ventura is a student of Bachelor of Science in Information Technology in Mapua University, Philippines. His interests are into programming, web development, internet of things, network and systems administration.

Ghibi P. Trinidad is a student of Bachelor of Science in Information Technology in Mapua University, Philippines. His interests are into programming, web development, internet of things, network and systems administration.