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

Eric B. Blancaflor, Adrian B. Alfonso, Kevin Nicholas U. Banganay, Gabriel Angelo B. Dela Cruz, Karen E. Fernandez, and Shawn Austin M. Santos
School of Information Technology
Mapua University
Makati City, Philippines
ebblancaflor@mapua.edu.ph, abalfonso@mymail.mapua.edu.ph,
knubanganay@mymail.mapua.edu.ph, gabdelacruz@mymail.mapua.edu.ph,
kefernandez@mymail.mapua.edu.ph, samsantos@mymail.mapua.edu.ph

Abstract

The phishing attacks have been drastically rising in numbers in several platforms such as personal and business emails, short message services (SMS), and the emerging tactic that is through social media accounts. With the vulnerability of social engagement and trust in relationships, the study will show how phishing attacks are easily done with just minimal rapport in comparison to unknown senders and promotional links. The creation of a fake phishing website has been done and sent to 107 people - 46 via email, 37 via social media chat, and 24 via SMS. Data collection has been done through the use of the open-source phishing framework GoPhish for monitoring the links sent via email, Google Analytics for links sent via social media chat, and a link click counter for links sent via SMS. The results have shown that out of the three types of phishing methods used, Social Media Phishing is where the targeted users are most vulnerable on which has a 24 out of 46 (52.17%) success rate, compared to Email Phishing which has 6 out of 37 (16.22%) success rate and Smishing which has a 1 out of 24 (4.17%) success rate.

Keywords

Phishing, Smishing, Email Phishing, and Social Media Phishing.

1. Introduction

Phishing is a social engineering attack that consists of creating spoofed emails to trick people into revealing sensitive information or installation of malicious malware (Hong 2006). Social engineering is the ability of deceiving someone in disclosing sensitive information from their targets. Users and organizations are susceptible to phishing even with vast security measures as it is based on the user's awareness of the risk of phishing attacks. Based on the Verizon Data Breach Investigation Report (2017), 93% of social attacks were phishing related and that 28% of phishing attacks are targeted (PhishingBox 2018).

(Frye 2007) states that Email and Instant Messaging applications are important but vulnerable. Real-time and near real-time communications plays a very significant role in a more efficient functioning of an organization, which makes it a good target for hackers and social engineers. More and more troublesome and criminal minds are looking for more clever ways to trick users into downloading malicious software on their machines, one of these tricks is using a phishing attack (Frye 2007).

Phishing, according to (Jagatic 2007), is a type of deception wherein an attacker acts like a trustworthy person to fraudulently gain sensitive information from a victim (Jagatic et al. 2004). Phishing is an email scam that attempts to steal personal information from users (Yeboah-Boateng and Amanor 2014). Another attack is Smishing, where attacks are conducted using SMS or text messages instead of email which posed risk on mobile device users. Mobile devices are as susceptible to phishing attacks as they are as common as desktops. Statista stated that in 2019, 70.7 million people accessed the internet through their mobile phones in the Philippines (Sanchez 2020).

The aim of this study is to determine the number of users that are more susceptible to phishing attacks. Using an open-source phishing toolkit, the researchers shall conduct the study by sending phishing links to various users through email, SMS, and social media to discover how many users either accessed or ignored the given link. The phishing campaign is done by creating a fake online shop website where targeted users register for a chance to win a raffle using motivation techniques such as scarcity and urgency. The phishing link will have a survey for targeted users that opened the link and then conduct a post-survey for all targeted users whether they accessed or ignored the phishing campaign.

1.1 Objectives

This section discusses the objectives and serves as a guide to achieve the purpose of this case study.

1. To conduct a successful email phishing, smishing, and social media phishing campaign
2. To spread awareness about phishing attacks
3. To determine the type of phishing attack that users are most vulnerable on
4. To identify the presence of security features of devices in mitigating phishing attacks
5. To know the vulnerabilities and awareness of individuals regarding phishing attacks
6. To identify the possible reasons of why users interact with an unfamiliar link
7. To distinguish which platform (social media, email, SMS) is the most vulnerable to phishing

2. Literature Review

Phishing trends have also improved alongside security advancements in terms of its creativity to avoid being detected, which became rampant in this Covid-19 pandemic. According to a recent study, a new phishing attack is being launched every 20 seconds involving the use of HTTPS protocols and SSL/TLS certificates, leading to around 51,000 coronavirus-themed domains in a span of 3 months (Bhardwaj et al. 2020). This number can be explained through a study by Cui et al. (2017), wherein they have determined that some phishing websites are short-lived which lasts for about 10 hours and this resulted in attackers to continuously repeat and republish the same phishing attack with a few modifications. Moreover, 2020 statistics show that 4.54 billion people globally are active internet users, and more than half of this number of people are active on social media (Dwivedi et al. 2020).

Shahriar et al. (2015) described the different types of mobile phishing attacks to bring awareness among mobile users. Mitigation approaches and best practices regarding phishing attacks were also discussed. In their survey, 40% of mobile application users enter their password at least once. 44% of adults are unaware of security solutions in their mobile devices. Chen et al. (2020) examines the online users perceived susceptibility to phishing attacks. An individual's phishing susceptibility is shaped by their recent phishing encounters. The effect of phishing detection failure affects their susceptibility to phishing encounters. Aleroud and Zhou (2020) investigates phishing attacks and anti-phishing techniques in emails, websites, mobile, and social networking sites. They proposed a taxonomy involving attacking techniques and countermeasures that provides effective techniques for phishing detection and prevention in various environments.

An overview of the various types of attack and how to mitigate them were provided (Shahriar et al. 2015), as well as best practices in using mobile devices. The approach would enable users to be aware of phishing attacks and equip users with understanding of how each attack can be prevented. The research was able to show that the effects of perceptions are not constant since users with experience of phishing attacks and users that desensitize themselves from phishing were identified.

In a study conducted by Dupuis and Smith (2020), they described how phishing simulation experiments are conducted wherein participants are either informed about the study beforehand or will be informed after the simulation and provided a survey. They stated that being informed about a phishing attack lead participants to experience the Hawthorne effect which is the change in their behavior as a result of being aware of the study. Out of their 146 participants, only 16 people have interacted with the link sent in their emails with 11% of them becoming a victim of phishing. Moreover, they revealed that gender is related to phishing susceptibility since there are more identified male victims.

Seng et al.(2019) conducted a vignette study that uses verbal details while asking the participants to imagine the corresponding scenario in a Facebook interface regarding a pseudonym that they provided and to obtain a broader understanding of the clicking behavior of social media users. This study considered relationships, location of the post, and the type of post. Based on their findings, the likelihood of a post to be clicked is higher depending on the closeness of their relationship to the participant, if the post is coming from the authors page with the participant tagged, and if it is a post with a media attached. With the use of the gathered data, this study suggests that understanding these instances is important in designing mechanisms to protect users from phishing attacks.

(Silic and Back 2016) conducted an empirical examination to understand how employees respond to phishing attacks on SNS. The researchers created a fake website, conducting qualitative study of employees using interviews. The researchers suggested existing organizations to employ policies and procedures on SNS and have employees gain better understanding of phishing attacks. Insights on the study can serve as a basis on better awareness and security.

3. Methods

3.1 Creating a Fake Gmail Account

The researchers have created a dummy account called Shop Mug Manila which will be used as the sender of the email phishing links to the targeted users.

3.2 Creating a Fake Website

The researchers created 2 fake web pages, the Shop Mug Manila serves as the main Webpage and the Disclaimer page. A Google Forms survey is located within each webpage. The Shop Mug Manila main webpage survey shall ask the user for their contact information to make the web page more convincing, while the disclaimer page survey shall ask the user regarding their awareness about phishing and the security of their devices. Upon submitting the survey in the Shop Mug Manila main Webpage, the targeted user will be automatically redirected to the Disclaimer page.

3.3 Google Tag Manager and Google Analytics for Monitoring Social Media Phishing Clicks

The researchers have used a website tag from Google Tag Manager to monitor the website activity using Google Analytics. The line of code provided by Google Tag Manager is inserted in the Shop Mug Manila webpage's index.html file.

3.4 Deploying Social Media Phishing Campaign

The tagged website is then distributed using Facebook Messenger to the targeted users of the social media phishing campaign.

3.5 GoPhish Setup and Use

Before using GoPhish, a Virtual Private Server (VPS) needs to be set up to host the URL Listener of GoPhish. The researchers have used Amazon Web Services (AWS) for hosting the fake websites and GoPhish server that shall be deployed. After hosting the websites and server, GoPhish has successfully launched.

3.6 Deploying Email Phishing Campaign

A phishing campaign was launched directed to 37 email accounts of the targeted users of the email phishing campaign.

3.7 Link Click Counter and Bitly for Monitoring Smishing Attack

The researchers have registered the URL address of the fake website to an online link click counter (linkclickcounter.com) to monitor the number of clicks it will receive in the smishing campaign. The counter link has been shortened using Bitly URL Shortener to hide its real URL address from the targeted users.

3.8 Deploying Smishing Campaign

The shortened links are then distributed to the 24 targeted users for the smishing campaign.

3.9 Post-Experience Survey Distribution

After sending the phishing links via email, social media, and SMS, a Post-Experience Survey is distributed to the targeted users to see the reason why they clicked the link or why they did not click it.

4. Data Collection

The number of clicks on the site as well as the experience of the user on the phishing website is the required data for the study. Links sent via email have been monitored via GoPhish, which shows the number of emails sent, number of emails opened, the number of links clicked, and the number of users which have submitted their data. Google Analytics has been used to monitor the links sent via social media chat, which shows how many users have clicked the link sent to them by the researchers. An online link click counter is used to monitor the links sent via SMS, which counts the number of users that have clicked the sent link. After the phishing campaign, a post survey has been sent to the participants to ask them about their experience, as well as the reasons why they click or did not click the link sent to them.

5. Results and Discussion

The researchers are able to identify the strengths and vulnerabilities of the devices used for the phishing campaign through various technical and non-technical approaches.

5.1 Social Media Phishing Campaign: The Results of GoPhish

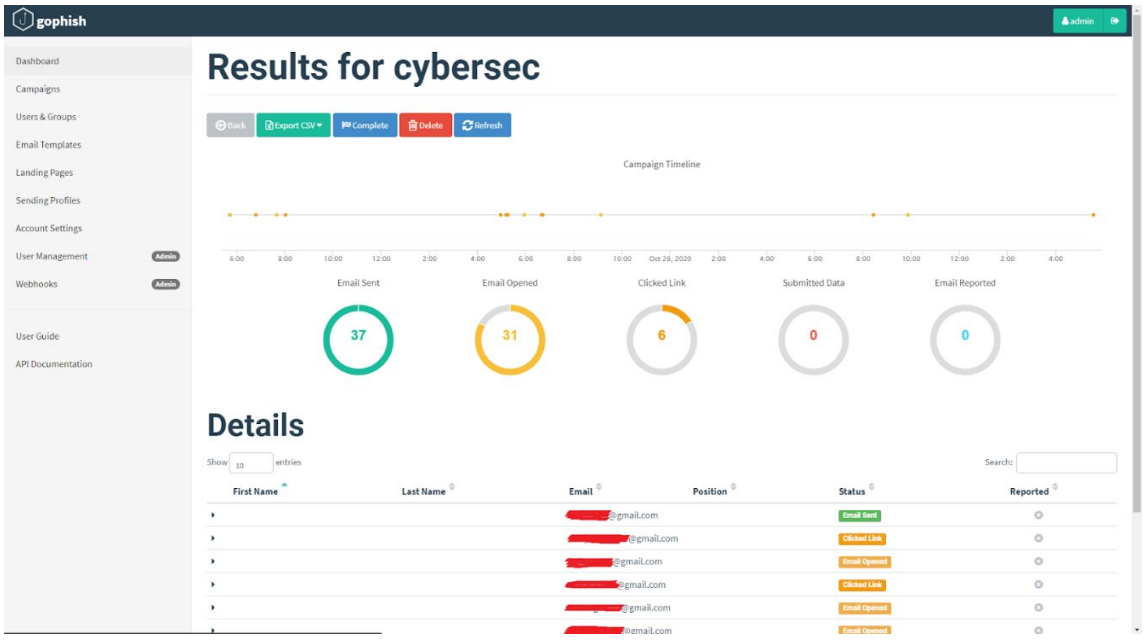

Figure 1. Results in GoPhish

GoPhish details after launching the Email Phishing campaign shown in Figure 1, have revealed that 37 total emails sent to the selected target users, 31 emails have been opened, 26 of them confirmed opened by google - false positive, and 6 phishing links have been clicked. Therefore, 6 out of 37 (16.22%) of the total targeted users for email phishing have clicked the phishing link.

5.2 Smishing Campaign: The Results of Link Click Counter

Monitored URL	Shorten URL		Tag Name	Clicks Counter		
http://3.134.85.123/	https://lcc.click/r5zFbGm	COPY	smishing	8	INFO DELETE	

Figure 2. Results of Link Click Counter

Link click counter details after launching the smishing campaign shown in Figure 2, have revealed that the smishing message and link has been sent to 24 targeted users. 8 users have clicked the link according to the Link Click Counter, but 7 are from group members testing out the effectiveness of the created counter link. Overall, 1 user is recorded to have clicked the smishing campaign link which is 4.17% of the total targeted users.

5.3 Social Media Phishing Campaign: The Results of Google Analytics

	Acquisition		
	Users ↓	New Users	Sessions
2 m.facebook.com / referral	15		
3 l.messenger.com / referral	5		
4 l.facebook.com / referral	4		

Figure 3. Google Analytics Result

The social media phishing message and link was sent to 46 targeted users. The Google Analytics details after launching the Social Media Phishing campaign shown in Figure 3 have revealed that 24 users have interacted with the link under Acquisition>All Traffic>Referrals. This is 52.17% of the 46 target users who have received the link on their social media accounts - Facebook Messenger.

5.3.1 Targeted Users are Vulnerable to Social Engineering Attacks

Table 1. Success Rate of Phishing Campaigns

Smishing	**4.17%**	1 out of 24
Email Phishing	**16.22%**	6 out of 37
Social Media Phishing	**52.17%**	24 out of 46
Total	**67.39%**	**31 out of 107**

As shown in Table 1, Social Media Phishing has a 24 out of 46 (52.17%) success rate, making it the type of phishing attack that the target users are most vulnerable on. Upon the completion of the Post-Experience Survey, we have found out that the targeted users are more vulnerable to phishing attacks upon gaining their trust.

5.3.2 Smishing Results

4.17% of the sent phishing campaigns were opened, 1 of the targeted users tend to ignore suspicious SMS messages from unidentified numbers. One of the targeted users from the post survey said they are not comfortable opening those type of link.

5.3.3 Email Phishing Results

Emails tend to be disregarded by targeted users, 30 out of 37 emails displayed as email opened at the deployment of the phishing campaign which could be a false positive status as mail providers may visit URLs in emails to prevent spam and abuse. 26 out of 30 assumed false positives were found to be opened by google (to look for spam and abuse) and 4 out of 6 clicked links could be one of the emails opened by Google. Also 5 emails were sent and not opened during the phishing campaign and 85.7% of emails deployed where sent through the inbox, the deployed phishing campaign was not marked as spam.

5.4 The Results of the Disclaimer Page Survey

The disclaimer page received 31 redirected users from the initial fake website. Users were asked of their awareness of phishing campaigns, with the majority of 90.3% of users are aware of such campaigns while the rest is not aware of the concept of phishing. 77.4% of the individuals have received the link of the fake website mostly through social media, 19.4% received the links through their emails, and the remaining 3.2% received it through short-message-services. The devices they were using were also asked, with the majority of 64% of the users used their smartphones, and the rest of the 35.6% used their personal computers or laptops.

5.5 The Results of the Post-Experience Survey

After deploying the awareness campaign researchers have selected users to answer a Post-Experience survey. Based on the data received, the most effective way of attack is through social media through Social Media Phishing, the second most vulnerable platform is via Email, and lastly is through smishing. Majority of the targeted users have clicked the link that concludes 65.2% of 23 targets are vulnerable with this attack, while 34.8% of the targeted users refused to click the link. The targeted users are more vulnerable to phishing attacks when you gain their trust. This resulted in 93.3% of 15 targeted users to click the link. While 26.7% of the targeted users are curious about the website which led them to click on the link. Some of the targeted users equivalent to 13.3% responded that they would like to obtain the free item, while other targeted users indicated that they are interested or attracted because of the said raffle. The reasons why the targeted users refused to answer the survey on the ShopMugManila website is shown in this graph, 50% or half of the responses thought that the survey in ShopMugManila website is a scam. While one of them responded that the link has already expired, and an individual also refused to answer due to being forced. Errors and warnings were encountered while accessing the link by users. Most of the targeted users equivalent to 73.3% were unable to detect any errors in the website, 26.7% of the targeted users thought of the disclaimer as a warning, and some of them were alarmed due to the warnings that appeared.

Targeted users were asked for past experience regarding phishing attacks, the common type of phishing attack that the targeted users have encountered. Half or 50% of the targeted users selected scam messages and a link redirecting to a login page. While 25% selected that they have encountered a link which contains a virus. Majority of the users have already experienced scam messages, phishing attacks, and malware attacks.

In conclusion, targeted users are vulnerable to social engineering attacks. Social Media Phishing has a 24 out of 46 (52.17%) success rate, making it the type of phishing attack that the target users are most vulnerable on. Upon the completion of the Post-Experience Survey, targeted users are more vulnerable to phishing attacks upon gaining their trust.

5.6 Proposed Improvements

The researchers formulated the following recommendations based on the findings of this study. These recommendations aim to provide solutions on the vulnerability of targeted users in phishing attacks.

Mobile devices cannot detect malicious links that are sent through SMS. Targeted users should be wary of clicking suspicious links from unknown numbers as there is no error detection present from sending through SMS. In mobile devices, malicious URLs are also displayed partially which could lead into targeted users thinking that the site is genuine. The best thing to do to prevent from being attacked and mitigate risk is to avoid any malicious SMS sent whether it be from trusted contacts or unknown as their contact numbers could be compromised. Targeted users should also be aware and look at the destination URL of the sent link.

The integration of Google Tag Manager and Google Analytics in a fake website can bypass Facebook Messenger's error detection, as well as the Security Standards of Google Mail. Google Analytics can be used as a reconnaissance tool which detects sensitive information of the targeted user. This can be avoided by being wary of links that are being sent in social media. Blacklisting and Whitelisting URLs could also minimize the risk of opening untrusted URLs. Targeted users can allow or block specific URLs in Google Chrome, which prevents them from accessing denied URLs and allow trusted URLs.

Phishing campaigns that were deployed using the phishing tool were not marked as spam or abuse in most of the targeted users. Some of them have been sent through their inbox even by being monitored by Google. Targeted users could not rely on automatically having suspicious email to be marked as spam. Targeted users can modify their settings in Gmail to filter and block addresses that are sending malicious files.

In summary, attacks and vulnerability could always happen. Phishing attacks would find a way to bypass security measures that email providers, social media sites, and SMS have implemented in controlling the suspicious files and links that are being sent to targeted users. Security settings are present in the technology we used today, it is just a matter of utilizing them and avoiding being targeted by preventing attacks from happening. Understanding the concept of phishing as well as mitigating the risk by behaving securely online leads to prevention.

5.7 Validation

Upon asking 15 targeted users on the post survey about their rating on the phishing campaign in spreading awareness about accessing links that can steal people's information, 10 (66.7%) have strongly agreed that the campaign can raise awareness, 4 (26.7%) have agreed, and 1 (6.7%) is neutral about the outcome of the campaign.

Table 2. Likert Scale Range

	Value	Range
Strongly Disagree	**1**	**1.00 - 1.80**
Disagree	**2**	**1.81 - 2.60**
Neutral	**3**	**2.61 - 3.40**
Agree	**4**	**3.41 - 4.20**
Strongly Agree	**5**	**4.21 - 5.00**

By using the formula: [(number of people who selected response 1)*(weighting of response 1) + (number of people who selected response 2)*(weighting of response 2)… (number of people who selected response n)*(weighting of response n)] / (total number of respondents), it yields the equation [(10 * 5) + (4 * 4) + (1 * 3)] / 15 = 4.6 based on the targeted users' answers on the Likert Scale. Based on Table 2 Likert Scale Range, 4.6 falls in the range of Strongly Agree, which states that the phishing campaign is effective in spreading awareness in a targeted user's perspective.

6. Conclusion

A Post-Experience Survey has been distributed to 23 targeted users, 8 Email Phishing targeted users (5 who clicked the link, and 3 who did not click the link), 12 Social Media targeted users (9 who clicked the link, and 3 who did not click the link), and 3 smishing targeted users (1 who clicked the link, and 2 who did not click the link). The results show that trust is the greatest factor in why the targeted users have clicked the link. This shows that even if their devices or browsers have high levels of security, their interaction, closeness, and trust in other people is their greatest vulnerability. Curiosity is the next factor in why the targeted users have clicked the link. This shows that persuading skills can be a significant characteristic of a penetration tester when dealing with other people, because getting their curiosity can be a way for them to disclose their information.

The Post-Experience Survey shows that 13 out of 15 (86.67%) target users did not receive any warning messages upon opening the phishing link. This shows that hosting a fake website on an online hosting application that has a legitimate domain can easily be sent via social media, email, and SMS. If the users trust the sender of the fake website, their sensitive information can easily be gathered. On the other hand, suspicion is one of the ways that a user can be protected from opening a malicious link. The Post-Experience Survey shows that 6 out of 8 (75%) target users have answered that they did not click the link because of their suspicion. This shows that clarifying when suspicion happens can be an additional layer of security for people especially for phishing attacks. 2 out of 15(13.33%) target users had an encounter with a warning webpage upon accessing the link. These users have used Facebook Messenger to access the given link. This shows that Facebook Messenger has a level of security upon sending phishing links.

Conclusively, the target users have a 4.6 Mean Value on the answers on the Likert Scale about their rating on the phishing awareness campaign conducted by the researchers, which falls under the Strongly Agree range. This shows that the target users have an overall positive attitude on the process of the phishing campaign.

References

Aleroud, A., and Zhou, L., Phishing environments, techniques, and countermeasures: A survey. Computers & Security, vol. 68, no. 11, pp. 160-196, 2017.

Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N., and Arthi, S., Why is phishing still successful?. Computer Fraud & Security, vol. 9, no. 9, pp. 14-19, 2020.

Chen, R., Gaia, J., Rao, H. R., An examination of the effect of recent phishing encounters on phishing susceptibility. Decision Support Systems, vol. 133, no. 3,2020.

Cui, Q., Jourdan, G.V., Bochmann, G.V., Couturier, R., and Onut, I.V., Tracking Phishing Attacks Over Time. *Proceedings of the 26th International Conference on World Wide Web (WWW '17)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, pp 667–676, 2017.

Dupuis, M. J. and Smith, S., Clickthrough Testing for Real-World Phishing Simulations. *Proceedings of the 21st Annual Conference on Information Technology Education (SIGITE '20)*. Association for Computing Machinery, New York, NY, USA, pp. 347, 2020.

Dwivedi, Y., Ismagilova, E., Hughes, D., Carlson, J., Filieri, R., Jacobson, J., Jain, V., Karjaluoto, H., Kefi, H., Krishen, A., Kumar, V., Rahman, M., Raman, R., Rauschnabel, P., Rowley, J., Salo, J. Tran, G., and Wang, Y., Setting the future of digital and social media marketing research: Perspectives and research propositions., International Journal of Information Management, 2020.

Frye, D., Email, Instant Messaging and Phishing. Network Security Policies and Procedures. Network Security Policies and Procedures, vol. 32, no. 13, pp. 131-152, 2007.

Hong, J., The state of phishing attacks. Communication of the ACM, vol.55, no.1, pp. 74-81, 2012.

Jagatic, T., Johnson, N., Jakobsson, M., and Menczer, F., Social Phishing. Communications of the ACM, vol. 50, no. 10, pp. 94-100, 2007.

PhishingBox., Phishing and the 2017 Verizon Data Breach Investigation Report. Available: https://www.phishingbox.com/news/phishingnews/phishing-and-the-verizon-data-breachinvestigation-report-dbir, 2018.

Sanchez, M., Number of mobile phone internet users in the Philippines from 2017 to 2019 with a forecast until 2025. Available: https://www.statista.com/statistics/558756/number-of-mobile-internet-user-in-thephilippines/#:~:text=Mobile%20phone%20internet%20users%20Philippines%202017%2D2025&text=In%202019%2C%2070.7%20million%20people,would%20reach%20almost%2090%20million, 2020.

Seng, S., Kocabas, H., Al-Ameen, M.N., and Wright, M. Poster: Understanding User's Decision to Interact with Potential Phishing Posts on Facebook using a Vignette Study. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, pp. 2617–2619.2019.

Shahriar, H., Klintic, T., and Clincy, V., Mobile Phishing Attacks and Mitigation Techniques, Journal of Information Security, vol. 6, no. 3, pp. 206-212, 2015.

Silic, M., and Back, A., The dark side of social networking sites: Understanding phishing risks. Computers in Human Behavior. vol. 60, no. 6, pp. 35-43, 2016.

Biography

Eric B. Blancaflor is an Associate Professor of Mapua University, Philippines. He earned B.S. in Electronics Engineering from Mapua University, Masters in Engineering major in Computer Engineering in the University of the City of Manila and currently working on his dissertation study as a requirement for the degree Doctor of Technology in Technological University of the Philippines. He has published conference papers related to IT systems, network design and security.

Adrian B. Alfonso is an Undergraduate Student of Bachelor of Science in Information Technology, specializing in Cybersecurity in Mapua University. He graduated high school in St. Paul College of Makati under the Science, Technology, Engineering, and Mathematics strand. During the last two years of his secondary education, he took a specialization in Technical Drafting.

Kevin Nicholas U. Banganay is an Undergraduate Student of Bachelor of Science in Information Technology, specializing in Cybersecurity in Mapua University. He graduated high school in Far Eastern University Diliman under the Science, Technology, Engineering, and Mathematics strand. He has participated in Hackfest 2020: Online, organized by Developer Student Clubs Loyola.

Gabriel Angelo B. Dela Cruz is an Undergraduate Student of Bachelor of Science in Information Technology, specializing in Cybersecurity in Mapua University. He graduated high school in Bulacan State University Laboratory Highschool under the Science, Technology, Engineering, and Mathematics strand.

Karen E. Fernandez is an Undergraduate Student of Bachelor of Science in Information Technology, specializing in Cybersecurity in Mapua University. She graduated senior high school in Holy Trinity Academy under the strand Information and Communications Technology, and finished a bridging course for Science, Technology, Engineering, and Mathematics strand in Mapua University. Ms. Fernandez has participated in events and workshops such as the Huawei Developer Day Philippines 2019, organized by Huawei, and Hackfest 2020: Online, organized by Developer Student Clubs Loyola.

Shawn Austin M. Santos is an Undergraduate Student of Bachelor of Science in Information Technology, specializing in Cybersecurity in Mapua University. He graduated high school in St. Anthony School under the Science, Technology, Engineering, and Mathematics strand. He has participated in events and workshops such as the Huawei Developer Day Philippines 2019, organized by Huawei, and Hackfest 2020: Online, organized by Developer Student Clubs Loyola.