Avoiding the Phishing Bait: The Need for Conventional Countermeasures for Mobile Users

Said Baadel
Canadian University Dubai &
University of Huddersfield, UK

Fadi Thabtah
Manukau Institute of Technology
New Zealand

Asim Majeed
Birmingham City University
United Kingdom

***Abstract*— According to the international Anti-Phishing Work Group (APWG), phishing activities have significantly risen over the last few years, and users are becoming more susceptible to online and mobile fraud. Machine Learning (ML) techniques have the potential for building technical anti-phishing models, a majority of them have yet to be applied in a real-time environment. ML models also require domain experts to interpret the results. This gives conventional techniques a vital role as supportive tools for a wider audience, especially novice users, in order to reduce the rate of phishing attacks. Our paper aims at raising awareness and educating users on phishing in general and mobile phishing in particular from a conventional perspective, unlike existing reviews that are based on data mining and machine learning. This will equip individuals with knowledge and skills that may prevent phishing on a wider context within the mobile users' community.**

***Index Terms*— Anti-phishing; Cyber Security, Embedded Training; Smishing.**

I. Introduction

Phishing is an attempt to gain sensitive personal and financial information (such as usernames and passwords, account details, and social security numbers) with malicious intent via online deception (Aaron & Rasmussen, 2010; Ramanathan & Wechsler, 2013; Abdelhamid, 2015). Phishing typically employs identity theft and social engineering techniques, such as creating websites that replicate existing authentic ones. Through a seemingly legitimate email that contains a hyperlink, potential users are redirected to the malicious website in order to divulge their private information and credentials (Atkins & Huang, 2013).

Advancements in computer networks and cloud technology in recent years have resulted in an exponential growth of online and mobile commerce, where customers perform substantial online purchases through their mobile devices (Abdelhamid & Thabtah, 2014). This online growth has led to phishing activities reaching unprecedented levels in recent months. The Anti-Phishing Work Group (APWG), which aims to minimize online threats (including pharming, spoofing, phishing, malware, etc.) has recently published a report about phishing activities in February of 2017 (Aaron & Manning, 2017). The report showed that there were approximately 1,220,523 phishing attacks in 2016, an increase of more than 65% from the previous year with an average of more than 92,500 phishing attacks per month in the fourth quarter of 2016. As more and more users become prone to information breaches and identity theft, their trust in e-commerce or mobile commerce platforms will deteriorate, thus resulting in a huge loss of financial gains (Nguyen, et al., 2015). Existing reviews on website and email phishing, such as Mohammad, et al. (2015), Khonji, et al. (2013), Purkait (2012), Aleroud and Zhou (2017), and Jain and Gupta (2017) and Baadel and Lu (2018) have dealt with the problem from a technological solution perspective. Their reviews focused on broad anti-phishing techniques based on data mining, ML, databases, and toolbars, and only briefly discuss solutions such as awareness programs, user education, and training among others. Other recent reviews have dismissed conventional solutions outside ML as ineffective (Varshney, et al., 2016; Abdelhamid, et al., 2017). Therefore, the key objective of this paper is to raise awareness on the challenges of mobile anti-phishing techniques and why it is important to incorporate the traditional conventional techniques such as law enforcement, user training, and online communities in combating phishing attacks on mobile devices.

The remainder of this paper is organized as follows: Section 2 briefly outlines the smishing attacks procedure. In section 3, we outline the classification of mobile attacks. In Section 4, we list some of the challenges in mobile anti-phishing and outline the need for conventional techniques. Section 5 briefly mentions some of the conventional countermeasures. Finally, a brief summary and conclusion are provided in Section 6.

II. Smishing attack procedure

Following the launch of Apple Pay around the world in 2015, Samsung Pay and Android Pay made their debut soon thereafter, making mobile phones very attractive to cybercriminals (ISTR, 2016). A spike in mobile device malware was noted in 2015 and 2016 according to a report by the internet security giant Symantec (ISTR, 2017). The report highlights more than 18 million mobile malware attacks on Android phones alone in the year 2016 compared to 3.4 million attacks just two years prior.

Short Message Service Phishing (Smishing) aims to steal a user's credentials over mobile phones in the form of text messages (Joo, et al., 2017). Phishers send malicious text messages with a link to users that either routes them to a counterfeit website or redirects them to fake app user interfaces (UI) through which the user gets spoofed and discloses their sensitive information (Felt & Wagner, 2011). While a web application keeps session cookies that store the user authentication credentials, a mobile application normally asks for user credentials every time the application is started, thus increasing the chances of a phishing attack to occur (Marforio, et al., 2016).

Figure 1 below shows an example of a Smishing attack.

978-1-5386-7266-2/18/$31.00 ©2018 IEEE

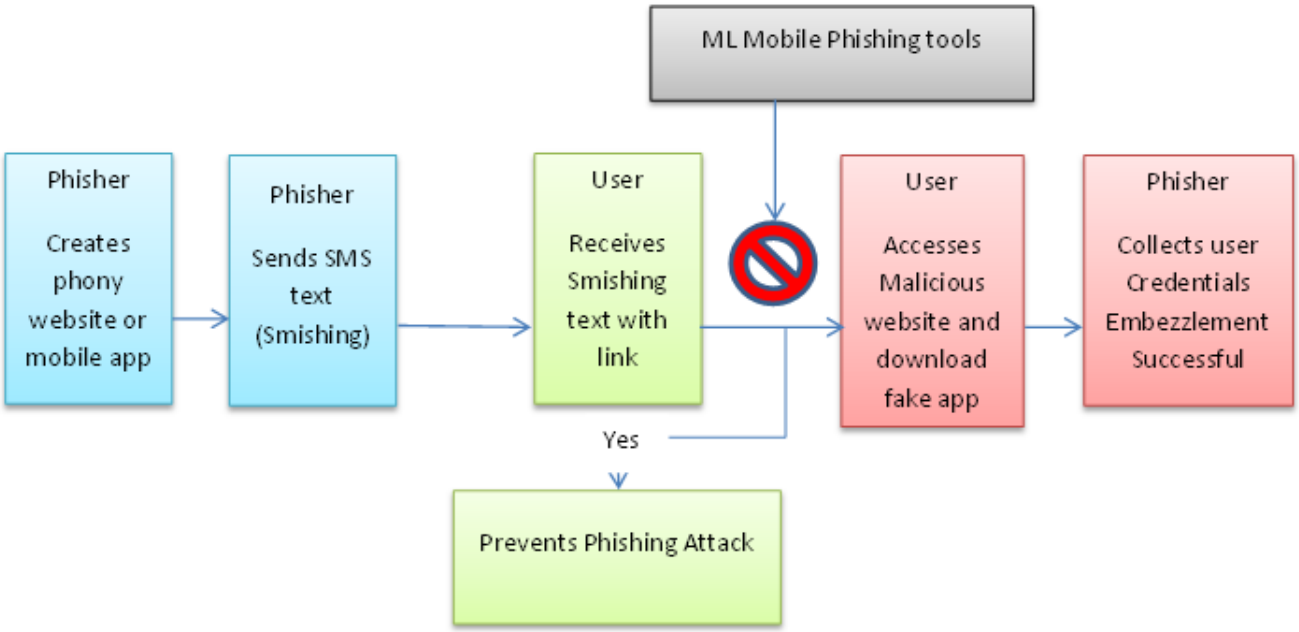

Figure 1. Smishing Attack Life-cycle

The Smishing procedure can be summarized as follows:

a) A phisher creates a website or phony app

b) He/She sends a Smishing text to a mobile phone.

c) User received a text with a link

d) Once the link is clicked, they are routed to a fraudulent phishing website or app.

e) Phisher collects sensitive information from the user.

d) Embezzlement successful.

If successfully detected, ML tools will warn the user of the fraudulent link after step "c" above and prevents the phishing attack from happening if the user ignores the text or does not click the link. However, there are several challenges facing mobile anti-phishing tools that make it difficult for users to distinguish between legitimate and fraudulent links. Some of the challenges are discussed in the next section below.

III. Mobile Anti-phishing Challenges: the Need for Conventional Anti-phishing Techniques

Marforio, et al. (2015), classified and listed five other mobile attacks as follows – similarity, forwarding, background, notification, and floating.

i) Similarity attack – the phishing app has UI features that are similar or identical to the legitimate application. Users are thus spoofed into installing the phishing app as opposed to the legitimate one.

ii) Forwarding attack – phishers take advantage of the forwarding functionality in an app. A user may be prompted to share their online game score or shopping experience with their friends on the social network. As the user clicks the link, the legitimate social network is not launched but rather a phishing screen that collects user credentials used to connect to the social network.

iii) Background attack – the phishing app functions in the background and as the user tries to open a legit application it triggers itself to the foreground and displays the phishing interface.

iv) Notification attack – the attacker generates spoofed notifications similar to that of the legit app and gathers the credentials entered as unsuspecting users click on them.

v) Floating attack – a phishing app can draw a transparent overlaid input field on top of a legitimate password input field and obtain the password entered by the user.

Few intelligent and classical solutions have been dedicated to mobile phishing, perhaps due to the number of resources needed to address the issue in mobile devices. Wu, et al. (2015), has suggested an anti-phish mobile tool for Android called MobiFish. The tool applies the whitelisting concept for phishing detection via mobile apps. It uses a text extraction tool, Tesseract, to verify the legitimacy of a website.

Botazzi, et al. (2015), proposed Mobile Phishing Shield (MP-Sheild) for Android as a proxy service on top of a TCP/IP stack. MP-Shield extracts the URLs from the HTTP get request from the IP packets. The URLs are sent to Google Safe Browsing blacklist repository to check whether the URL is blacklisted or not.

Joo, et al. (2017), suggested a Smishing detection method called S-Detector that collects the logs and timestamp of a smishing attack. The number or URL is run through a blacklist database to see if it exists. The algorithm goes further by detecting if an APK file is downloaded, which will be regarded

as an abnormal path and together with a risk weight value assigned through a Naïve Bayes algorithm flag the text message as a Smishing text attack.

All of these approaches are Android-based only and rely on the data repository techniques of blacklist and whitelist; hence they face similar challenges discussed in table 1 above. Smishing text messages can be changed quickly and use URL shortcut services, enabling them to bypass blacklists and thus are becoming very difficult to detect (Joo, et al., 2017). According to Marforio, et al. (2015), a mobile app can be modified to allow the user to configure a personalized security indicator that will be shown during each login screen. This technique was tested in a study by Malisa, et al. (2017), which concluded that it was more effective on mobile apps. However, the effectiveness of any security indicators for mobile platforms requires user alertness and knowledge to identify spoofing apps from legitimate ones.

Unlike phishing attacks on the PC, the attacks on mobile devices pose additional challenges to detecting and identifying phishing scams. These can be listed mainly as:

a) They are difficult to detect visually by the users since their URLs are normally not displayed in full due to their limited screen sizes (Canova, et al., 2015; Varshney, et al., 2016).

b) Complex anti-phishing solutions cannot run effectively on mobile devices due to hardware and resources limitations (Wu, et al., 2015).

c) Mobile browsers are lightweight and have reduced security capabilities (Varshney, et al., 2016; Wu, et al., 2015).

d) Mobile user habits allow for being easy prey to phishers. For example, shifting to other pages or apps on a mobile phone may be a bit cumbersome compared to a PC. Thus, mobile users will prefer to click on a link from an app instead and easily fall victim to a phishing link (Wu, et al., 2015).

This gives conventional techniques a vital role to play as supportive tools to wider audiences, especially novice users, in reducing phishing attack rates in mobile devices.

IV. Some conventional anti-phishing countermeasures

A) Legislation

Many countries have introduced legislation to combat phishing and cybercrimes. These include the Anti-phishing Act of 2004 (USA), the Fraud Act of 2006 (UK), and Anti-spam Law of 2010 (Canada) among others. Adopting organized crime laws to combat cybercrimes may give law enforcement enhanced investigative powers (Leukfeldt, et al., 2017). According to Larson (2010) and Cassim (2014), legislation should be designed to provide large-scale damage against individual phishers or secondary liability against Internet Service Providers (ISPs) in hopes that ISPs will be motivated to play their role in fighting phishing.

B) Embedded Training and User Education

Many researchers such as (Arachchilage, et al. 2016; Harrison, et al., 2016; Jensen, et al., 2017) have conducted studies on user training for raising phishing awareness. These studies involved either sending users an email with links and monitoring how they responded, or making the participants aware that a simulated phishing experiment was to be conducted and are gauged on their abilities to correctly identify phishing emails. At the end of the training, users were normally given the materials and informed about their vulnerability to phishing.

Mobile game platforms bring an interactive and fun approach to education and training and are somewhat more effective compared to traditional articles or lectures. Users who participated in mobile game studies argued that mobile game based education was fun and gave them immediate feedback so that they were better equipped to identify a phishing attack after completing the game (Sheng, et al., 2007; Arachchilage & Love, 2013). Users trained through mobile application had a higher success rate of identifying phishing sites compared to their counterparts who used traditional mediums (Arachchilage & Cole, 2011).

C) Online User Communities

As users become more aware and are able to identify online scams or fall victim to phishing attacks, they may report their experience in order to prevent others from similar attacks. Users can report fraudulent websites or URL links that can then be stored in online databases. Such accumulated resources can also be used by researchers to study phishing scammers and their evolving ways of devising their scams. This collection of previously identified and detected phishing domain names, or URLs, is commonly referred to as a "blacklist". Some of the widely used and common online communities include Anti-phishing Working Group (APWG), Phishme Blog, Symantec, among others.

The above-listed communities serve as good examples of phishing URL databases available to users. These online communities play an important role in raising anti-phishing awareness and keeping the conversation progressing.

These conventional anti-phishing countermeasures need to be developed and integrated through the mobile platform. Fun games and educational tutorials that educate users on phisher's activities can be easily disseminated through commercial applications, such as banking apps, online transactions apps, popular online stores, and other social media platforms such as Facebook, Snapchat, etc. where it can have an instantaneous global reach and tremendous impact on user awareness.

V. Conclusion and future work

This paper discussed common mobile phishing attacks and some of the challenges in detecting and identifying mobile phishing scams. Unlike phishing attacks on a computer, a mobile scam is hard to identify due to the size of mobile devices,

smartphone resource limitations, and app design for mobile use. Some common conventional anti-phishing prevention techniques, including law enforcement, simulated training, and online communities were briefly discussed. The legislation provides law enforcement officers investigative powers to track cyber criminals. Educational training equips users with the necessary skills to identify a phishing scam. Online phishing communities accumulate data repositories that allow users to share useful information about phishing incidents, creating a knowledge base for online users. These conventional countermeasures need to be developed and integrated through the mobile platform through fun games, tutorials, and through social media platforms for it to have a significant impact and a global reach.

In future work, it is planned to present a classical/conventional anti-phishing framework preventive layer with a thorough analysis and discussion on each of the countermeasures pros and cons to better equip companies, security experts, and researchers in selecting what can work well to equip individuals and stakeholders with knowledge and skills that may prevent phishing attacks on a wider context within the community.

REFERENCES

[1] Aaron, G., and Manning, R. (2017). APWG Phishing Reports. http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf [Accessed August 20th, 2017].

[2] Aaron, G., and Rasmussen, R. (2010). Global phishing survey: trends and domain name used in 2H 2009. Lexington, MA: Anti-Phishing Working Group (APWG).

[3] Ramanathan, V., and Wechsler, H. (2013). Phishing detection and impersonated entity discovery using conditional random field and latent Dirichlet allocation. Computers & Security, 34, 123-139.

[4] Abdehamid, N. (2015). Multi-label rules for phishing classification. Applied Computing and Informatics 11 (1), 29-46.

[5] Atkins, B., and Huang, W. (2013). A study of social engineering in online frauds. Open J Soc Sci, 1(03):23-32.

[6] Abdelhamid, N., and Thabtah F. (2014). Associative Classification Approaches: Review and Comparison. Journal of Information and Knowledge Management (JIKM), 13(3).

[7] Nguyen, L., To, B., and Nguyen H. (2015). An Efficient Approach for Phishing Detection Using Neuro-Fuzzy Model. Journal of Automation and Control Engineering, 3(6).

[8] Mohammad, R., Thabtah, F., and McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. Computer Science Review Journal, 17, 1–24.

[9] Khonji, M., Iraqi, Y., and Jones, A. (2013). Phishing Detection: A Literature Survey. IEEE Surveys and Tutorials, 15(4).

[10] Purkait, S. (2012). Phishing countermeasures and their effectiveness – literature review. Information Management & Computer Security, 20(5): 382-420.

[11] Aleroud, A., and Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. Computer and Security, 68: 160-196.

[12] Jain, A., Gupta, B (2017). Phishing Detection: Analysis of Visual Similarity Based Approaches. Security and Communication Networks, Volume 2017, pp. 1-20.

[13] Baadel, S., Lu, J. (2018). Data Analytics: intelligent anti-phishing techniques based on Machine Learning. Journal of Knowledge and Information Management. In press.

[14] Varshney, G., Misra, M., and Atrey, P. (2016). A survey and classification of web phishing detection schemes. Security and Communication Networks, 6266–6284.

[15] Abdelhamid, N., Thabtah, F., and Abdeljaber, H. (2017). Phishing detection: A recent intelligent machine learning comparison based on models content and features. Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI), China. IEEE.

[16] ISTR (2016). Internet Security Threat Report. Symantec, USA. Volume 21, page 10. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf [Accessed July 18th, 2018]

[17] ISTR (2017). Internet Security Threat Report. Symantec, USA. Volume 22, page 68. https://www.symantec.com/security-center/threat-report?inid=globalnav_scflyout_istr [Accessed July 18th, 2018]

[18] Joo, J., Moon, S., Singh, S., et al. (2017). S-Detector: an enhanced security model for detecting Smishing attack for mobile computing. Telecommunication Systems, 66(1):29-38.

[19] Felt, A., and Wagner, D. (2011). Phishing on mobile devices. Web 2.0 security and privacy workshop, Oakland, CA.

[20] Marforio, C., Masti, R., Soriente, C. et al. (2015). Personalized Security Indicators to Detect Application Phishing Attacks in Mobile Platforms. Cryptography and Security. arXiv:1502.06824 [cs.CR]

[21] Marforio, C., Masti, R., Soriente, C., et al. (2016). Hardened Setup of Personalized Security Indicators to Counter Phishing Attacks in Mobile Banking. Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices, Austria. Pp 83-92. ACM Digital Library.

[22] Wu, M., Miller, R., and Garfinkel, S. (2006). Do security toolbars actually prevent phishing attacks? Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '06, pp. 601–610

[23] Bottazzi, G., Casalichio, E., Cingolani, D., et al. (2015). MP-Shield: A Framework for Phishing Detection in Mobile Devices. Proceedings of the IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM). The UK. IEEE.

[24] Malisa, L., Kostiainen, K., and Capkun, S. (2017). Detecting Mobile Application Spoofing Attacks by Leveraging User Visual Similarity Perception. Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy. Pg 289-300. ACM Digital Library.

[25] Canova, G., Volkamer, M., Bergmann, C., et al. (2015). Learn to spot phishing URLs with the android NoPhish app. Information security education across the curriculum, 87–100. Berlin: Springer.

[26] Leukfeldt, E., Lavorgna, A., and Kleemans, E. (2017). Organized Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. European Journal on Criminal Policy and Research, 23(3):287-300.

[27] Larson, J. (2010). Enforcing intellectual property rights to deter phishing. Intellectual Property & Technology Law Journal, 22(1):1 - 8.

[28] Cassim, F. (2014). Addressing the Spectre of Phishing: Are Adequate Measures in Place to Protect Victims of Phishing. The Comparative and International Law Journal of Southern Africa, 47(3):401-428.

[29] Arachchilage, N., Love, S., and Beznosov, K. (2016). Phishing threat avoidance behavior: an empirical investigation. Computers in Human Behaviour, 60: 185–197.

[30] Harrison, B., Svetieva, E., and Vishwanath, A. (2016). Individual processing of phishing emails. Online Information Review, 40(2):265-281.

[31] Jensen, M. L., Durcikova, A., Write, R. (2017). Combating Phishing Attacks: A Knowledge Management Approach. 50th Hawaii International Conference on System Science. The USA. 4288-4297.

[32] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., et al. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. Proceedings of the 2007 Symposium On Usable Privacy and Security, Pittsburgh, PA.

[33] Arachchilage, N., and Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3): 706-714.

[34] Arachchilage, N., and Cole, M. (2011). Design a mobile game for home computer users to prevent from "phishing attacks". International Conference on Information Society (i-Society), 485-489.