Journal of Information Security, 2015, 6, 206-212
Published Online July 2015 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2015.63021

Scientific Research Publishing

Mobile Phishing Attacks and Mitigation Techniques

Hossain Shahriar, Tulin Klintic, Victor Clincy

Kennesaw State University, Marietta, Georgia, USA
Email: hshahria@kennesaw.edu, tkilinc@students.kennesaw.edu, vclincy@kennesaw.edu

Received 24 March 2015; accepted 27 June 2015; published 30 June 2015

Abstract

Mobile devices have taken an essential role in the portable computer world. Portability, small screen size, and lower cost of production make these devices popular replacements for desktop and laptop computers for many daily tasks, such as surfing on the Internet, playing games, and shopping online. The popularity of mobile devices such as tablets and smart phones has made them a frequent target of traditional web-based attacks, especially phishing. Mobile device-based phishing takes its share of the pie to trick users into entering their credentials in fake websites or fake mobile applications. This paper discusses various phishing attacks using mobile devices followed by some discussion on countermeasures. The discussion is intended to bring more awareness to emerging mobile device-based phishing attacks.

Keywords

Mobile Application, Phishing, Smishing, Vishing

1. Introduction

Mobile phishing is an emerging threat in today's connected world. In a mobile phishing attack, an attacker usually sends an SMS message containing links to phishing web pages or applications which, if visited, ask for credential information [1]. Attacks can also be initiated via email messages loaded in the browser of mobile devices.

A report finds that the number of mobile phishing attacks has been increasing over the last few years for various mobile device platforms [2]. For example, the number of unique phishing attempts blocked by Microsoft Windows Phone 8 devices doubled from February to June 2013, and the volume of phishing attempts and online phishing websites doubled in the first half of 2013.

Compared with traditional desktop software users, mobile application users are more vulnerable to phishing

How to cite this paper: Shahriar, H., Klintic, T. and Clincy, V. (2015) Mobile Phishing Attacks and Mitigation Techniques. *Journal of Information Security*, **6**, 206-212. http://dx.doi.org/10.4236/jis.2015.63021

attacks (at least three times [3]). Experts agree on some of the common, well-known reasons for this vulnerability:

1) Within a small devise, it is rather difficult for a user to check whether a page is legitimate, as is confirming the actual pointed hyperlinks, as URLs are not often displayed within mobile browsers.

2) Mobile users are less aware of security options to stop or prevent phishing attacks.

3) Most legitimate mobile applications require users to enter their credentials with very simple user interfaces, making the job of an attacker rather easy to come up with fake apps or plain websites mimicking legitimate user interfaces.

4) Surveys find that 40% of mobile application users enter passwords into their phones at least once.

The information provided by victims is harvested by attackers within the first 60 minutes. A phishing campaign typically takes at least one hour to be identified by IT security administrators before it can take down the phishing site (this is described as the "golden hour") [4]. Phishing attacks target commonly popular financial organizations. A survey found that 71% of phishing attacks were related to spoofed financial organizations, compared with 67% in 2012. Phishing attacks on organizations in the Information Services sector accounted for 22% of phishing attacks in 2013 [5].

The scope of phishing attacks is vast, and the consequences can be severe. On the other hand, there is limited knowledge among users on how to avoid phishing attacks. Symantec's Norton Report shows that 44% of adults are unaware that security solutions exist for mobile devices. This clearly shows not only the lack of awareness, but also the danger posed by mobile application phishing attacks [5].

A phishing (or fraudulent) mobile application potentially can grab victim's account information and data stored on mobile devices [6]. Recently, Google pulled 50 applications from its Android Market app store in response to concerns that they may be malicious. All the apps were uploaded by the same developer and claimed to offer access to bank accounts from a wide variety of institutions such as J. P. Morgan Chase, HSBC, USAA and ING Group. As Google's Android Market relies on its community to flag fraudulent applications, the likelihood of being vulnerable to mobile phishing attacks via fraudulent Android application is more likely than in Apple applications [6].

Given that it is important to be aware of various avenues of mobile phishing attacks and mitigation approaches for Android applications. In this paper, we describe various types of mobile phishing attacks. We also discuss some mitigation approaches and best practices to avoid phishing attacks and future research directions. The work is intended to bring more awareness among mobile application users.

The paper is organized as follows. Section 2 discusses various techniques for phishing attacks. In Section 3, some mitigation approaches are discussed. Finally, Section 4 draws the conclusions and discusses future work.

2. Mobile Phishing Attack Techniques

2.1. Small Screen and Partial Display of URLs

Mobile devices and smart phones mostly have a small screen. Those small screens make it harder to see the full URLs when users click to the links. Also, the companies keep their mobile web sites simple to be able to use the small screen more efficiently. Moreover, some of them cannot even put their own logo due to limited screen size. Therefore, many users are not aware when they are not at official web sites while browsing on the Internet.

When a fake site URL and a legitimate site URL are compared, the differences in URL can be hidden due to small size of the screen and URL bar. **Figure 1** shows a sample of fake PayPal page (left[1]) and its URL address compared to the legitimate one (right[2]) [7]. While legitimate address has secure protocol, HTTPS, the fake site does not. In addition, the fake page has some additional text which may not be visible at all to users at some browsers. Besides the URL address, the fake-site does not display the original PayPal logo. In addition, they pull the attention to the other images to trick the users.

2.2. Accessibility to App Store

Another channel to reach to the end users is via application stores, called application phishing. Android 09*Droid* phishing application is one good example that was intended to gather users' banking credentials [8]. It has been reported that the 09*Droid* phishing application was uploaded to potential victims through the Android market app store, where most of the other apps are legitimate. **Figure 2** shows a snapshot of a set of fake mobile

[1]http://www.xylibox.com/2015/01/captain-barbarossa.html
[2]http://www.sitepoint.com/buy-time-braintree-v-zero-sdk/

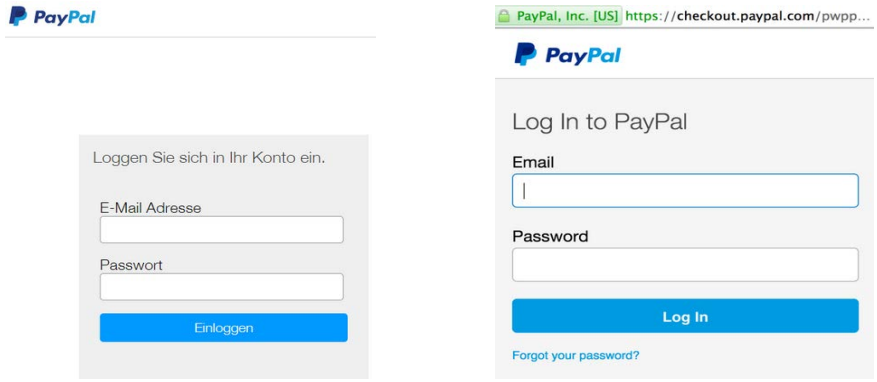


Figure 1. Fake paypal web page and URL (left) vs. real paypal web page and URL (right).

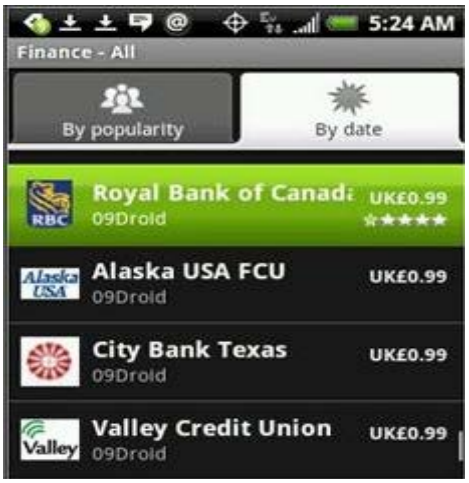


Figure 2. Screenshot of 09Droid banking applications with price information uploaded to Android App market.

banking applications uploaded in Android marketplace (the picture taken from a mobile device) with pricing information. Note that the targeted companies are mostly from North America, and the pricing was in GBP, leaving the prospective North American customers in the dark.

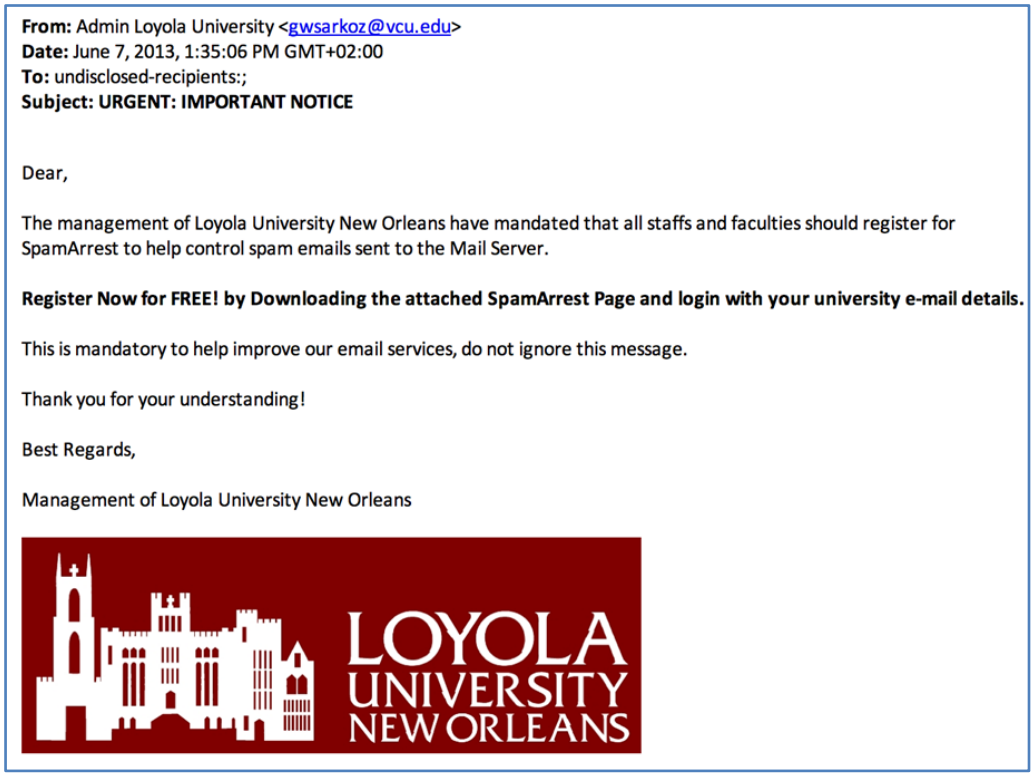
It is unknown what the application performed behind the scene. However, it opens a login web page. It is likely that the application's goal was to steal user credentials. Banking apps that were developed by 09Droid have been pulled from Android market ever since. The targeted companies include Sun Trust, Chase, Wachovia, Bank of America, and Wells Fargo [8].

Phishing attacks are applicable for Apple app that runs on iPad and may have larger screen size. Marble Security implemented a fake iTunes App to show how phishing works on an iOS iPad. First, a phishing email is sent to users informing them they need to install a "mandatory" SpamArrest page and enter university credentials (see **Figure 3** for an example of email) [9].

Once the user follows the instruction, believing that it is legitimate, the application sets a new user profile. iOS allows applications to create unsigned and unverified profiles (as shown in **Figure 4**). Then, a user enters the password of the device if it has been set earlier. The last step is to delete the original iTunes app, and install the new fake one (see **Figure 5**). At this point, the fake iTunes app can be used to steal login credentials to the iTunes store easily.

2.3. Smishing

Another popular phishing method is using SMS messages; this method is called "smishing" [10]. It works the



From: Admin Loyola University <gwsarkoz@vcu.edu>
Date: June 7, 2013, 1:35:06 PM GMT+02:00
To: undisclosed-recipients:;
Subject: URGENT: IMPORTANT NOTICE

Dear,

The management of Loyola University New Orleans have mandated that all staffs and faculties should register for SpamArrest to help control spam emails sent to the Mail Server.

Register Now for FREE! by Downloading the attached SpamArrest Page and login with your university e-mail details.

This is mandatory to help improve our email services, do not ignore this message.

Thank you for your understanding!

Best Regards,

Management of Loyola University New Orleans

LOYOLA UNIVERSITY NEW ORLEANS

Figure 3. Screenshot of a phishing email targeting university employees.

Figure 4. Screenshot of iOS allowing unsigned and unverified profile.

same way as phishing, but instead of an email, a victim receives a text message that asks for banking credentials or to claim a prize. Once the user receives the smishing message from a phone number, it is recommended to inform the cell phone carrier. If the number presents as 5000, it means it has been sent from an email instead of a cell phone. **Figure 6** shows a snapshot of a smishing attack where a spoofed link is provided as part of SMS with an alluring message to a potential victim (winning a lottery).

Figure 5. Original iTunes app removed and fake iTunes app installed.

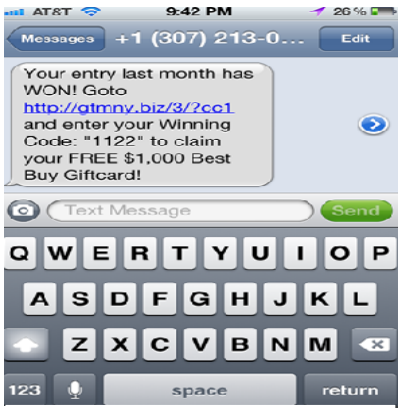


Figure 6. Screenshot of smishing.

2.4. Wi-Fi and Vishing

Wi-Fi phishing occurs when a user connects to the Internet via Wi-Fi hotspots. Evil twin is an example where attackers set up a Wi-Fi to eavesdrop on wireless communications where there is a legitimate Wi-Fi hotspot, such as at a Starbucks [12].

Vishing, voice mail phishing, is a phishing attack on mobile devices into Bluetooth phishing or Voice over IP phishing to reach users' identification or financial information [11]. Other vishing schemes may play a message about a local or regional bank in the area by recording the greeting message of a real bank. Scammers attempt to greet victims and lure them into providing credentials for online banking [12].

3. Mitigation Approaches and Best Practices

3.1. Mitigation Approaches

Common phishing detection systems for mobile devices include content-based filtering, blacklisting, and white-

listing [11]. We discuss them below briefly. We also show the extent to which they can be applied to detect smishing, vishing, and Wi-Fi attacks.

Content Based Filtering: In this technique, content is examined for suspected URLs and matches the context of the URLs [13]-[16]. The approach supplements traditional spam filtering techniques. Content-Based filtering can be performed based on a set of rules or based on identifying statistical differences between benign and suspected phishing contents. It can effectively detect smishing, vishing, and Wi-Fi phishing attacks.

Blacklisting: In this approach, based on human verification, a set of websites is explicitly listed as known phishing URLs [17]. This approach leads to very low false positive rates and is currently supported by various browsers that communicate with trusted servers to obtain a list of blacklisted URLs. Though this approach can possibly identify suspected websites, it may not be able to detect smishing, vishing, and Wi-Fi phishing attacks.

Whitelisting: In this method, users specify websites they trust and access frequently so that other websites are examined for suspected phishing attacks. The approach can be applied to detect smishing where a set of legitimate numbers can be provided to stop receiving unwanted SMS containing fake web addresses [15].

3.2. Best Practices

Although it is hard to detect fake mobile applications, there are several methods to reduce phishing attacks on mobile devices.

a) *Using official apps*: Users should only download official apps from the app stores.

b) *User training*: User training is very important to prevent users clicking unknown links.

c) *Safer browsers*: Browsers with security features installed (such as Chrome mobile) eliminates malware and phishing sites to protect users.

d) *Bookmarks*: Bookmarks eliminate typos when typing URLs. Since it is hard to see the URL bar completely, bookmarking is a good solution to eliminate landing on unwanted pages.

e) *More controls by app stores*: Vendors should take more steps before letting developers uploading their apps for the public.

f) *Security solutions*: Just as security companies have anti-virus programs for desktops, now many also have mobile security solutions. Those programs eliminate malicious activity on mobile devices. An example is COMODO app [18] for Android device available in Google play store.

4. Conclusion

Mobile devices have small screens, so users are not able to see the whole URLs and are very likely to click on the links without enough forethought of possible phishing attacks. Moreover, users download and install applications without realizing that installed applications may not be a copy of legitimate official applications, a problem which overwhelmingly targets financial institutions. This paper provides an overview of various types of mobile phishing attacks. We also discuss some mitigation approaches and their limitations. We suggest some best practices. Our approach would enable users to be more careful when downloading apps and running on their devices to avoid fake interfaces designed by phishers. There is a broad scope of further research to be done to develop novel mitigation approaches, especially considering the variation of devices and accessibility of application market.

References

[1] CAPEC-164: Mobile Phishing. https://capec.mitre.org/data/definitions/164.html

[2] Ashford, W. (2014) Phishing Attacks Track Mobile Adoption, Research Shows. http://www.computerweekly.com/news/2240215873/Phishing-attacks-track-mobile-adoption-research-shows

[3] Kessem, L. (2012) Rogue Mobile Apps, Phishing, Malware and Fraud. https://blogs.rsa.com/rogue-mobile-apps-phishing-malware-and-fraud

[4] Klein, A. (2010) The Golden Hour of Phishing Attacks. http://www.trusteer.com/blog/golden-hour-phishing-attacks

[5] Symantec Internet Security Threat Report 2014, Vol. 19. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[6] Todorova, A. (2010) "Phishing" Scams Cast Net on Mobile Banking. http://online.wsj.com/news/articles/SB10001424052748704343104575033380555965818

[7] Trend Micro eBook (2013) Trend Micro. http://about-threats.trendmicro.com/ebooks/protecting-yourself-against-mobile-phishing/files/assets/downloads/protecting-yourself-against-mobile-phishing.pdf

[8] Morrison, D. (2010) Mobile Phishing Highlights Need for Greater Security. http://www.cutimes.com/2010/01/20/mobile

[9] Jevan, D. (2012) Latest Threats against Mobile Devices. Information Systems Security Association. http://sfbay.issa.org/comm/presentations/2014/ISSA%20Marble%20Security_2014_0114.pptx

[10] Wilson, S. (2014). Smishing, Yes It Is All Bad. http://www.zcorum.com/smishing-yes-its-all-bad/

[11] Foozy, C.F.M., Ahmad, R. and Abdollah, M.F. (2013) Phishing Detection Taxonomy for Mobile Device. *International Journal of Computer Science*, **10**, 338-344.

[12] (2014) Hackers Target Wi-Fi Hotspots in New Phishing Attack. https://johnib.wordpress.com/2007/05/06/hackers-target-wi-fi-hotspots-in-new-phishing-attack

[13] Johnston, S. (2013) How to Protect Yourself from Smishing and Vishing. http://money.usnews.com/money/personal-finance/articles/2013/09/19/how-to-protect-yourself-from-smishing-and-vishing

[14] Yoon, J.W., *et al*. (2010) Hybrid Spam Filtering for Mobile Communication. *Computers & Security*, **29**, 446-459. http://dx.doi.org/10.1016/j.cose.2009.11.003

[15] Mahmoud, T.M. and Mahfouz, A.M. (2012) SMS Spam Filtering Technique Based on Artificial Immune System. *International Journal of Computer Science*, **9**, 589-597.

[16] Zhang, Y., Hong, J. and Cranor, L. (2007) Cantina: A Content-Based Approach to Detecting Phishing Web Sites. *Proceedings of the* 16*th International Conference on World Wide Web*, Banff, May, 639-648. http://dx.doi.org/10.1145/1242572.1242659

[17] Sheng, S., Wardman, B., Warner, G., Cranor, L., Hong, J. and Zhang, C. (2009) An Empirical Analysis of Phishing Blacklists. 6*th Annual Conference on Email and AntiSpam* (*CEAS*), Mountain View.

[18] COMODO Security Solutions. https://play.google.com/store/apps/developer?id=Comodo+Security+Solutions&hl=en