International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 10 , October 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

A STUDY OF SOCIAL ENGINEERING BY USING SMART PHONE SAMSUNG GALAXY S4 WITH NOKIA LUMIA 1520

Mohammed Farook Bin Rafiuddin

Bachelor of Forensics Computing, Asia Pacific University, Malaysia

ABSTRACT

This paper dealt about the importance of social engineering and the methods to perform social engineering by using smart phones. Here the smart phones used for the social engineering incorporated with Samsung Galaxy S4 and Nokia Lumia 1520. The attacker phone in this paper used Samsung and the Victim phone used is Nokia. Also some descriptions been explained about how to carry out phishing provided with example of facebook phishing attack. The examples of preventive measures and attacks in social engineering also discussed in this study.

Keywords: *Social Engineering, Samsumg, Nokia Lumia, Facebook, Hacking, Phishing*

I. INTRODUCTION

In terms of information technology, contextualizing social engineering means manipulating people into performing actions without them realizing in order to get the information you need or want. At most situations, social engineering is usually done to gain information on confidential information. In the digital world, it is also defined as a non-technical method of intrusion hacker's use that relies heavily on human interaction and communication that so often involves tricking people into breaking normal security procedures and this has been a major threat most organizations today encounter [1].

1.1 Why Is It Performed?

The main reason behind many social engineering attempts are to convince the user to open files and to leak information and most of the times are without them realizing. Hackers use social engineering to convince people to open certain malware or viruses through email attachments. Besides that, phishers also use social engineering to convince people to leak sensitive information usually done in banking's. Also, this method is performed to convince people that you work in a building, to get inside of places, to lure people into doing certain actions and trapping them and many other reasons. Apart from the above, social engineering became increasingly vital ever since software products became more secure and passwords are harder to crack. A hacker can spend days trying to brute force attack on a password or just turn to exercising social engineering and get the information needed in about 5 minutes [2].

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

1.2 How is it performed?

The person who performs social engineering is usually referred to as a social engineer. A social engineer often runs something like a con game to get his manipulation game started. For instance, a person who wants to break into a computer network may try to engineer the confidence of an authorized user of the computer to get himself into the network. Social engineers usually rely and hope heavily on the surrounding people to help out without knowing. The better the person is at social engineering the easier he or she tricks people into giving information out and the faster you get what you need. Besides that, often information gets leaked in situations where an organizations authorized employee gets a call regarding some kind of urgent problem that requires immediate attention. They usually call and drop a situation at the help desk whereby network access grant maybe needed and during that time, a typical social engineer goes all old-fashioned eaves dropping to get information [1]. Often the methods used are called phishing, vishing and impersonation. The whole idea is to trick the victim in doing something he or she have no idea about the consequences. It is easier to deal with human error than to find errors in a computer system because most often, errors are presented easily due to human lack of knowledge, and other attributes that makes us human which is to make mistakes and to misuse trust.

II. METHODS TO PERFORMING SOCIAL ENGINEERING

Among the most frequently used methods in the field of social engineering is phishing and speared phishing. Both are similar to the act of fishing because both are started by baiting. Phishing is when a party send a malicious email disguised as a legit official email often looking like it's from a trusted source. The email is meant to trick the user into installing malwares on their device and sharing personal information sometimes through remote access. Meanwhile speared phishing is also the same as phishing but it is tailored to a particular individual or organization. In better words, it is designed or focused on just one context or party. In such situations, the attackers are usually trying to gather financial data or confidential trade information from the particular organization. Besides that, Baiting is among the methods often used in this field of study. Baiting is also known as the real world Trojan horse that uses physical media and relies entirely on the curiosity and the greed of the victim. In better words, it is the process when the attacker leaves behind a malware infected physical device such as a USB flash drive or a CD in a place sure to be found on purpose in attempt to lure people to use it and when it is loaded into the computer, the malware is automatically installed [3]. Tailgating is a fairly old school method of intrusion. It is also the process when an unauthorized party follows an authorized person into a secured location. Usually in buildings guarded with RFID security and many more. Usually done in attempt to steal valuable property or information. Usually involve having key card access to a secure building area. Example, attacker simply walks behind a person who has legitimate access to the building, Due to common courtesy, the person with the authorized access usually hold the door for the person behind to enter as well without asking for his security card [1].

Apart from that, another method frequently used to aid social engineering is the idea of caller id spoofing. The method is achieved by getting a spoofcard or downloading an app on your phone such as incognito caller ID. In this app, it allows the user to change their mobile number and call the targeted ID. During the call, the number

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

that appears on the target will be the desired number set by the attacker. Hence, the attacker can impersonate as the owner of someone else's belongings and gather information from organizations. For hackers who are trying to gain access to someone's online accounts, spoofing is just first step in social engineering play to convince the target that they are legitimate [4].

III. HOW TO CARRY OUT SOCIAL ENGINEERING IN SMART PHONES?

Here the phones used Samsung Galaxy S4 using FakeId application and Nokia Lumia 1520 under Windows 10. There are various types of persuasion, the most common one is phone calls with the aid of a callerIDspoofer to change the number that appears on the victim's phone also known as a spoofing card. Here what the attacker does is that, he or she tries to convince to win the heart of the victim by gaining trust. The first step to this technique is to have good foundation in psychology and communication skills. The attacker has to be calm and able to put up a legit drama to make the opposite side (victim) to think that, the person behind the call is the real deal. Typically, social engineers first design their play and settings such as the situation, what the idea is about, whom they are going to be speaking on the phone with and who are they representing as. The objective of social engineering on phone call is usually to get user information details such as ID card number, personal emails, Facebook, full name, age, the surrounding, and the computers, system and OS and many others. Sometimes, a social engineer needs to take it slow and not ask too many information at a time on the phone. It has to be a slow and simple relationship with trust on the phone. For example, the attackers can call you in the middle of the night and drop a dilemma on you such as your phone bill has been increasing and that you have a call charges to Egypt or United Kingdom about USD 2000. This automatically creates a panic situation and victims buy that. Hence in that situation, whatever information the attackers ask is given easily [5].

3.1 Attacker's Phone: Samsung Galaxy S4

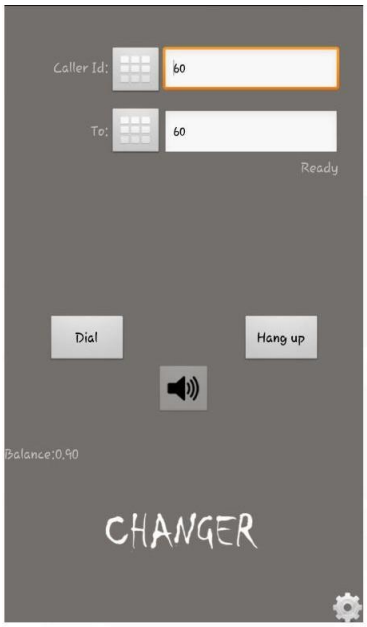


Figure.1 Android app

International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 10 , October 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The above “Fig.1” shows the android app used. The home screen is shown above where the desired caller ID can be manually placed according to your own desire and wish. The number placed in the caller ID will be displayed on the target phone during the call. The following app was used to display on the target machine as a private call. The credit balance is displayed at the bottom right of the screen shown in “Fig.2”.

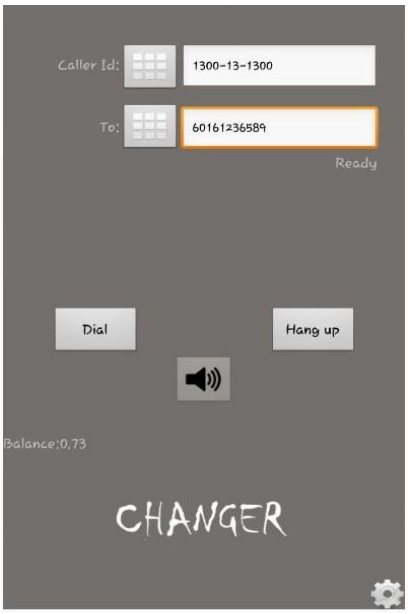


Figure.2 Target machine

The above image shows the caller ID used and the target number.

Figure.3 Call Progress

International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 10 , October 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The above image “Fig.3” is taken when the attacker has hit the dial button. Upon hitting the dial button, the target number will be highlighted around the box to indicate that the call is live. As shown, the call is in progress for 00.05. The attacker can wait till the target answer the phone.

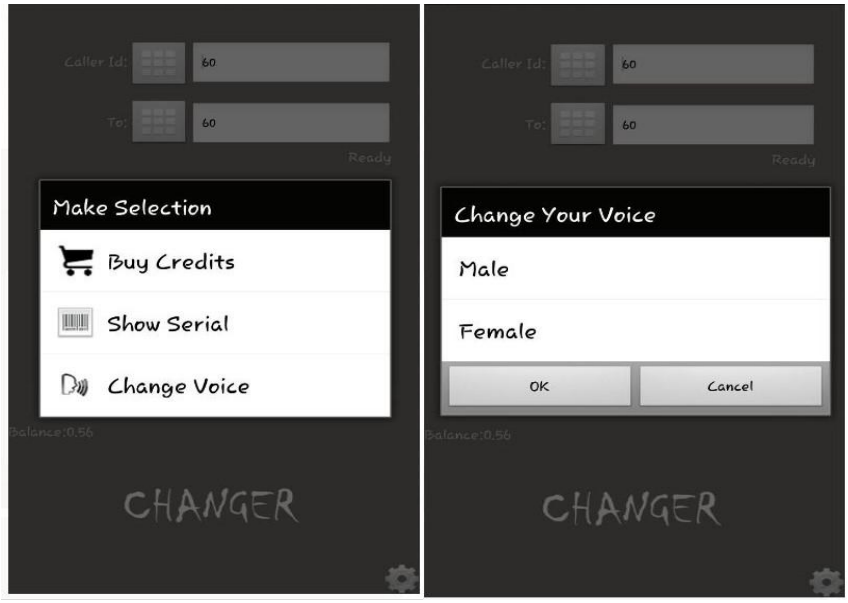


Figure.4 Attackers Options

The above two images “Fig.4” shown the other attacker options to change voice from male to female. This would come in handy during situations such as trying to forward calls to the boss or higher ups. With just one touch, you can change the actor from male to female.

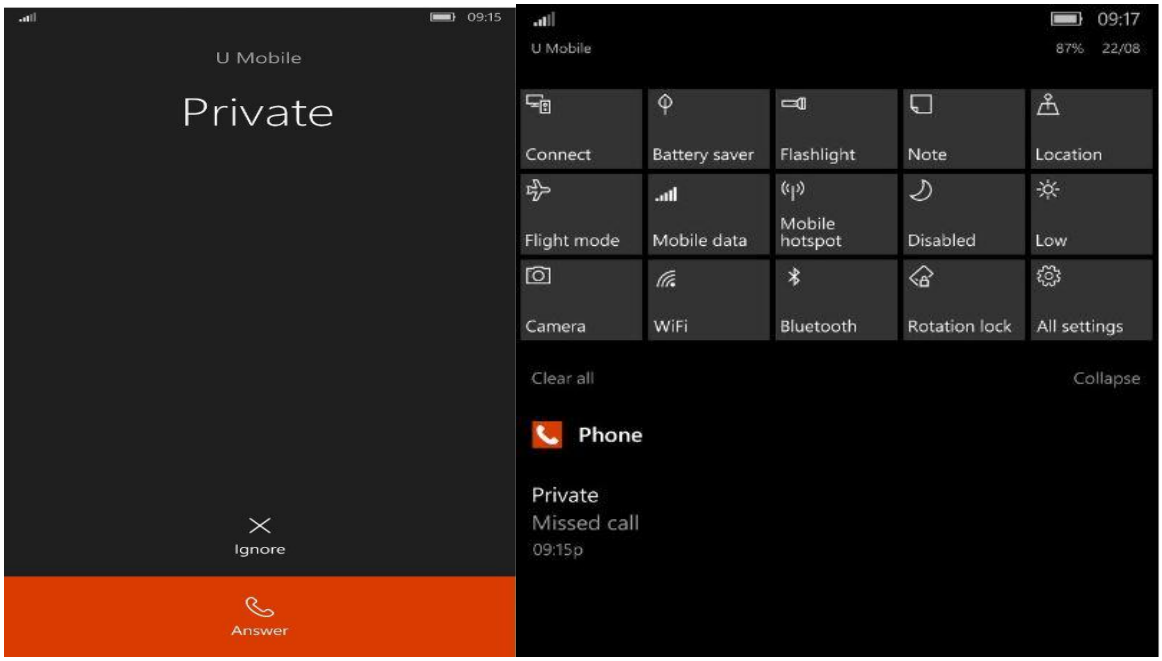


Figure.5 Victim phone: Nokia Lumia 1520

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The above two images “Fig.5” shown the phone screen during the phone call through the victim’s point of view. When the attacker called the victim phone, the caller ID displayed on the victim phone was private giving an impression that it’s from a private number maybe from an organization. When the victim did not answer the call, the notification bar displayed a private missed call.

IV. HOW TO CARRY OUT PHISHING?

Phishing is usually done to gather information such as typically username and passwords. Usually in phishing, the attacker creates a fake page and redirects the victim to that page or sends it in an email to the victim and gets him to click it. When Phishing is done, it is usually carried out by e-mail spoofing and instant messaging [6]. For beginners, in this tutorial, it will be shown how to phish Facebook accounts. Typically two files are needed. First file would be Phishing.php and the second is Index.html. To create a Phishing.html, first we need a php script which will collect all form of data.

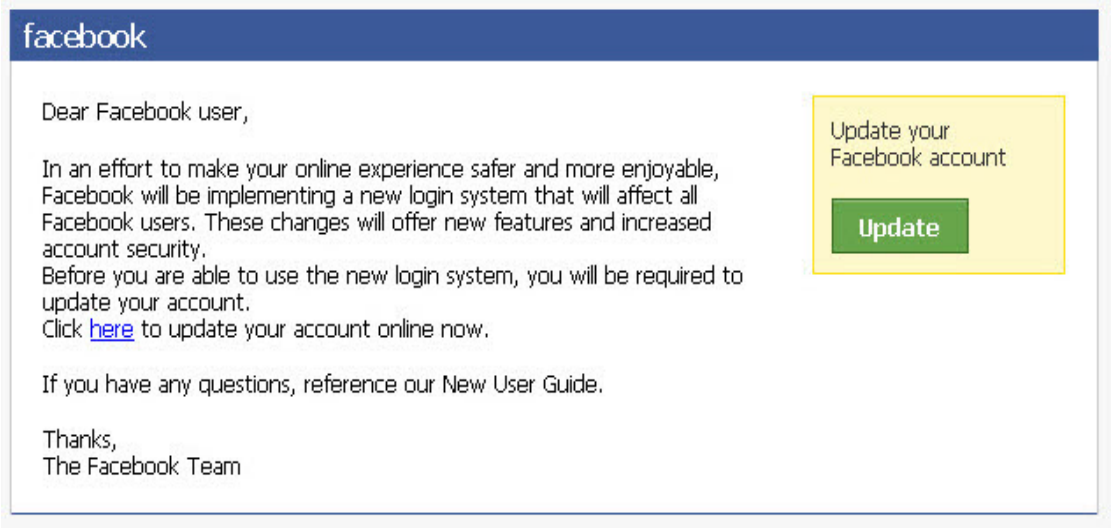
```
< ?php header("Location: http://www.facebook.com");
$handle = fopen("log.txt", "a");
foreach($_GET as $variable => $value)
 {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

The above code is the execution code to create a php script for a fake Facebook page. Copying the code and saving it in a text editor notepad and save it as phishing.php will give you the first file which is phishing.php file. For the second file, go to the Facebook page without logging in, right click on the browser empty spaces and click on view page source and open the source code in a text editor notepad. Next, after opening it, a new window will pop-up where you can see all the html coding. All you need to do is find the text “https://www.facebook.com/login.php?login_attempt=1”. Upon finding the link, replace the link with “phishing.php” and save this page as index.html. After that, navigate to any free hosting websites such as “www.t35.com” or “www.freehostia.com” and create a free account and create a folder in the account name it Facebook.Lastly, upload both the files created which is named “phishing.php” and “index.html” to the Facebook folder you created inside the free hosting websites. Therefore once you are done with creating it, the link to your phisher will be for example “www.yourname.t35.com/facebook/index.htm”. Move on to sending this link to

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

your targeted victims with any message attach to it. So, when someone logs in to the link sent, their username details and password will be sent over to your free hosting website account in a log.txt file [6].

The above picture shown is an example of Phishing attack [9]



Hackers can attach the link in a similar text like this to lure the victim into blindly following it. Phishing is often associated with an emails or phone calls or both.

4.1 Example of Social Engineering Attacks and Preventive Measures to Counter Them

Important aspect on social engineering is that it relies heavily on human's inability to keep up with the rapid growth of culture that focuses primarily on technology. Social engineers relies and harps on the fact that humans are not aware of the value that information they have and are often careless in holding precautionary methods in protecting it. So frequent, social engineers would harvest dumpsters in attempt to gain valuable information, memorize access codes by shoulder surfing or by taking advantage of peoples natural inability to choose for a secure password for their accounts and that can be easily guessed.

In attempt to stay safe from being socially engineered by attackers are by having more awareness campaigns and security awareness training programs. This can go a long way in protecting people and organizations from

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

getting important confidential information leaked. If people are aware the ways and methods as to how social engineering is primarily done, there will be more awareness among the common public. This also gives security officers a higher chance in detecting those who perform such acts because the public are well aware and educated regarding such attempts and can further assess the crime unit department in aims of hunting them down. The people should also get themselves attached to the knowledge of the fast growing technology just so that one will not easily fall behind the fast growing knowledge [7].

When it comes to phishing, best way to protect yourself or an organization from phishing attacks is to guard against spam, communicate personal information through a phone or a secured website, do not click on any unnecessary links or download files or open attachments that come in emails without knowing what it is actually. Protect the computer with antivirus and online internet security. Also never fill up details in any popups or download without knowing any extensions or popups plugin and always remember to be aware in giving out personal information online [8].

V.CONCLUSION

In conclusion, Social Engineering is a very interesting field of study that goes hand in hand with the study of human psychology and human thinking. A person who is very logical and critical in thinking is very unlikely to fall for the trap of social engineering but still possible whereas one that is not critical and not logical, it would be extremely easy to make him or her to fall for the trap. Knowledge is the key element here on trapping someone or avoiding oneself from being trapped. The Above short summary and documentation sums briefly in context the inand outs of social engineering. Mind hack can only be stopped by gaining more information and knowledge, being extremely aware and spreading massive awareness regarding the situation.

VI. ACKNOWLEDGMENT

Author would like to thank Mr Umapathy Eaganathan, Faculty in Computing, Asia Pacific University, Malaysia for his constant support and encouragement to publish and attend this international conference in India.

REFERENCES

[1] Rouse, M., 2014. *social engineering.* [Online] Available at: http://searchsecurity.techtarget.com/definition/social-engineering

[2] Henry, A., 2014. *Why Social Engineering Should Be Your Biggest Security Concern.* [Online] Available at: http://lifehacker.com/why-social-engineering-should-be-your-biggest-security-1630321227

[3] Bisson, D., 2015. *5 Social Engineering Attacks to Watch Out For.* [Online] Available at: http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for

[4] Szoldra, P., 2016. *It's surprisingly easy for a hacker to call anyone from your personal phone number.* [Online] Available at: http://www.techinsider.io/phone-number-spoofing-2016-2

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[5] Granger, S., 2010. *Social Engineering Fundamentals, Part I: Hacker Tactics.* [Online] Available at: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics [Accessed 15 8 2016].

[6] hackersocean, 2014. *Phishing Attack Step by step tutorial.* [Online] Available at: http://www.hackersocean.com/2012/01/phishing-attack-step-by-step-tutorial.html [Accessed 14 8 2016].

[7] Pinola, M., 2012. *How Can I Protect Against Social Engineering Hacks?.* [Online] Available at: http://lifehacker.com/5933296/how-can-i-protect-against-hackers-who-use-sneaky-social-engineering-techniques-to-get-into-my-accounts

[8] identitytheftkiller, 2008. *Are You Phishing For Trouble?.* [Online] Available at: http://www.identitytheftkiller.com/prevent-phishing-scams.php

[9]Thebulldogetstate, 2012. PHISHING. [Online] Available at: https://thebulldogestate.wordpress.com/2012/01/07/repost-facebook-phishing-scam-alert/