Facebook: A Comprehensive Analysis of Phishing on a Social System

December 7, 2010

Tarek Amin, Oseghale Okhiria, James Lu and James An

Department of Electrical and Computer Engineering
University of British Columbia
Vancouver, Canada

tarekamin89@gmail.com, sega.okhiria@gmail.com, jameslu1027@gmail.com, jamesanse@gmail.com

Abstract— Phishing is one of the most common Internet scams on the Internet today and with the introduction of interactive social websites, it has the potential to become more effective. Thus, the project analyzes phishing on the Facebook social website. In order to accomplish this, we set up a fake Facebook login page and simulated a simple phishing scam to gain insight on social systems and the techniques they implement to deal with phishing. From the analysis done, it was found that approximately 1 in 3 Facebook user's fell for the simulated scam. The results show that users interacting on a social networking website are more likely to fall for phishing scam due to its social nature. Furthermore, tests have shown that the Facebook social system does not provide effective means in dealing with phishing attacks. Out of the many solutions suggested, a possible resolution to combat phishing on Facebook could be to implement a restriction on the number of devices the user can use to access their accounts without additional authentication.

I. INTRODUCTION

With over $1.2 billion dollars in direct loss in 2003, internet phishing has become one of the most common and powerful attacks present on the web [1]. Phishing is a form of social engineering in which the adversary attempts to steal personal information such as usernames, passwords and credit card information by emulating a legitimate source. Emails have been the center of attention for phishing attacks. Users would receive mail that visually imitates a trusted service or company, using convincing rationalizations to steal personal information. Many solutions have been proposed and implemented for these types of phishing attacks in which awareness and education have played a crucial role [2]. However, the introduction of the Web 2.0 has provided new techniques in which scammers can successfully increase the effectiveness of phishing attacks [3]. By its very nature, this new web phenomenon encourages interactive information sharing and user oriented web designs which make social engineering a more influential process. In the heart of this new trend is the emergence of social websites such as Facebook, MySpace, hi5 and YouTube. Facebook for instance has over 30 billion objects such as web links and blog posts that are shared every month [4].

Along with real social interactions, interactive interfaces, such as the one provided by Facebook, can prove to be very vulnerable to social engineering attacks. Thus, we attempt to analyze to what extent this is true in two major steps. We study how Facebook's user interface encourages, or more accurately, lacks a system that can effectively reduce the amount of phishing on the growing trend of social websites. Furthermore, we look at how users, usually known to be the weakest link in a secure system, can impact the integrity and confidentiality of the social experience. The fundamental importance of the analysis is to understand what needs to be done to reduce such risks.

Analysis and solutions on phishing have been very extensive and have been carried out by researchers on topics like fake emails, web sites and web forms [5]. However, little has been done on the risks and solutions for social websites. There has been some work, but not to the extent provided in this report. Thus, part of our analysis attempts to simulate real phishing attacks on Facebook through various interactive methods. This assists in effectively understanding how Facebook deals with phishing attacks, as well as, how and why users fall for simple scams.

From our simulated attacks, we found out that Facebook does not provide a comprehensive system in reducing the amount of phishing scams. Furthermore, our results show that roughly 1 in 3 people fall for very simple attacks, in which their username and password could have been easily retrieved. One of the major implications of such vulnerability is the ability for adversaries to use this personal information to exploit the relationship entrusted between friends to gain financial benefits. Due to this social interaction between users in the context of social websites, it is difficult for Facebook to implement a psychologically acceptable design that does not hinder the user friendliness of the system. Defense in depth and securing the weakest links have not been achieved either. In order to reduce the risks involved with phishing attacks some countermeasures have been proposed including user authentication and URL detection.

II. ANALYZING THE FACEBOOK SYSTEM

As mentioned in the introduction, the analysis of the Facebook system is broken down into two essential components. The first component attempts to analyze how the system, in this case the website, encourages or prevents phishing attacks. Thus, we study various aspects of the system such as the login procedure, the layout of the interface and the services provided to the user. This will give important insight on what does or doesn't increase the effectiveness of social engineering attacks. A list of the elements is described below.

I. The Facebook System Interface

A. Account Creation

An analysis needs to be made on the account creation procedures that Facebook employ. The ease or difficulty in the process of successfully creating a Facebook account is essential. This plays an important role in analyzing how phishers would be capable of creating an account in which phishing attacks can occur from. A question related to this interface could be how does Facebook ensure that the user creating the account is a real person and has true intentions to socialize over the system?

B. Login Process

Studies on how the Facebook system deals with log in process is also a crucial point of analysis. Thus, we have to look at how the system deals with usernames and passwords and the ways, if any, it deals with suspicious login variations. This investigation is important as it determines how the system would react to someone other than the real user logging into their accounts. A question related to this element would be, if an adversary had access to a user's personal information, would the system be able to detect changes such as a change in geographical location? This assumes that the adversary is located in a different part of the globe.

C. Exploitation of Services

Services provided by the Facebook system such as wall posting, group creation, in-system messaging and instant chat play an essential role in social engineering attacks. If an adversary can exploit the user friendliness of the system, then he/she can effectively encapsulate the phishing scam into a service that the typical user expects to be normal. A question that can be raised is how can the adversary exploit the services of a basic wall post to convince the victim that the scam is actually trustworthy?

D. Account Activity

An obvious element of inspection is how the Facebook system deals with suspicious account activity. Having a system that does not incorporate this can lead to mass phishing attacks. But a more important question could be how does the Facebook system detect narrow targeted phishing attacks? i.e attacks that do not trigger account suspension. When is there a limit?

II. The Human Aspect

Humans are usually known to be the weakest link of a secure system. Phishing in essence attempts to exploit this link. It is always easier to get a user to give you their personal information rather than exploit the cryptographic algorithms of the system. Thus a major part of our analysis focuses on how easy it is to deceive a user into providing their personal information. We attempt to find out if users of the social system and any internet user in general, do pay attention to the URL of a phishing scam that attempts to redirect them. Gathering such information is essential as an understanding of what makes phishing successful will be beneficial to the proposal of counter-measures.

III. RELATED WORK

Phishing has been around for a while and, as stated in the introduction, is one of the most common attacks on the Internet. So it comes as no surprise that there have been many analyses on the topic. However, many of the previous analyses on Internet phishing deal with capturing the essence of phishing attacks by analyzing the components and processes which attackers use to collect sensitive or confidential information [6]. Very few researchers simulate actual phishing on social networks in order to acquire information about both the system and the users that fall for the scam.

One previous work to note would be that of Check Point Software's Security Research & Response team. This team conducted a phishing simulation using Facebook in order to evaluate the dangers social network sites expose us to. In their analysis, the team created a fake Facebook profile. Using this profile they then sent out 200 private messages to complete strangers. The message was the same for all 200 recipients. It consisted of a short message which read, “Check out my latest pictures”, accompanied with an external URL link to a potentially dangerous site, which could contain worms, Trojans or viruses that could attempt to gain information from your computer [7]. The results were obtained by keeping track of the number of people who clicked on the potentially dangerous link.

From their analysis, they found that approximately 35% of the recipients attempted to visit the URL link provided in the message. This is a substantial finding, as a previous study done on traditional phishing without the use of social networks done by Gartner in April, 2004 showed that only 3% of randomly surveyed participants reported to falling for a phishing scam [6].

While this analysis provides substantial findings, we believe it may be insufficient because visiting a suspicious URL link does not necessarily mean that the scam is successful. In our analysis we approached the victims in a different manner as well as going one step further to gaining more accurate results, which will be discussed in the following section.

IV. ANALYSIS METHODOLOGY

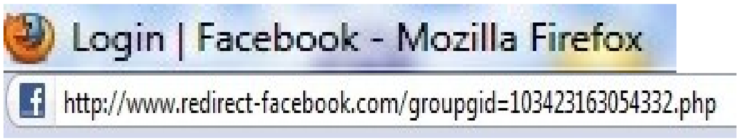
In order to effectively analyze the Facebook system, the set of tasks and methodologies are split into two major components. First, the mechanisms for analysis must be setup and effectively designed to successfully simulate a real phishing attack. This is an important factor in the overall achievement of the investigation and must be described in some detail to ensure this analysis can be repeatable. Secondly, the system must be attacked in specific ways in order to effectively analyze the elements mentioned in section number II. A good integration of these two major components will aid in the achievement of crucial results.

I. SETTING UP A FACEBOOK PHISHING ATTACK

The essence of phishing is to attempt to steal a user’s personal information. In this case, the personal information mainly relates to the user’s username and password. Thus, a common method in doing so is by redirecting the user to a fake websites that effectively imitates the trustworthy source. In the case of our analysis, we intended in directing the user to a fake Facebook login page that would ask them to re-enter their personal information. It is important to reiterate from the previous section that such attacks occur from both the legitimate source itself (Facebook) and through external means such as other social websites. This is one of the aspects that differentiate this analysis from previously carried ones.

A. Creating the Fake Login Page

To setup our analysis, we obtained a domain name through a provider. Thus, we were able to manipulate the webpages on the domain to simulate a Facebook phishing attack. By adding webpages with names such as the one shown in **fig 1**, we attempt to deceive the user into thinking that this page originates from Facebook.



Login | Facebook - Mozilla Firefox

http://www.redirect-facebook.com/groupgid=103423163054332.php

Figure 1: Fake Facebook Web Page

The webpages part of redirect-facebook.com indicates that the user is accessing a Facebook group and thus tricks them into believing the source of the content. This signifies the importance that not all internet users can parse and understand the content of the URL, which has been identified in research [5]. Paying close attention to the images shown above we see that visual cues such as the small Facebook logo at the beginning of the URL along with the name of the website provide false indication that the webpage is trustworthy. All of these small details play an important role in the simulation of a real attack.

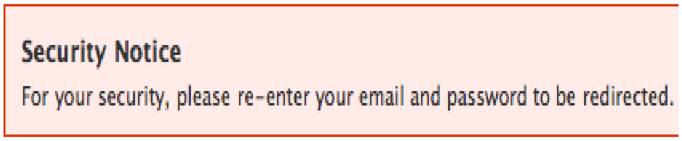
B. Replicating the Facebook Login Page

The next vital step in the setup was to convincingly replicate the Facebook login page. Surprisingly, this was not too difficult. By accessing the source code through any web browser, the Cascading Style Sheets (CSS)[1] and other information can be obtained. Thus, it was easy to create a website that accurately replicated the login page and was identical to Facebook. Furthermore, the fake login page had a security notice such as the one shown in **fig 2**. This justifies the user’s requirement to re-enter their username and password in order to be redirect to the Facebook group.

C. Collecting Information

The only major difference between the two login pages was that the fake one did not actually obtain the user’s username and password. Furthermore, the fake page would redirect the user to a carefully thought survey in order to collect maximum information regarding their phished accounts. This information was useful in determining why users fall for such scams and provided insight to some of the counter-measures.

[1] The CSS is a set of rules that govern the structure and format of a web page.



Security Notice

For your security, please re-enter your email and password to be redirected.

Figure 2: Fake Security Notice

It is important to mention that the number of phished users was obtained by implementing two “unique IP counters”, one at the login page and the other was at the survey. By looking at the number of IP addresses on the survey page, we could infer that these users actually fell for the scam. Furthermore, looking at the IP counter difference between the survey page and the login page, we could deduce that these users followed the link but did not provide their personal information. It is vital to mention that we assumed the users who were redirected to this survey have actually provided their real username and password and not meaningless information.

II. SIMULATING THE ATTACK

Once the essentials have been setup, we proceeded with the actual analysis of the Facebook social system. By making use of the fake website that we have created, we attempted to simulate the process a phisher would go through in order to successfully steal personal information from the users. Therefore, we tested how the Facebook system would deal with such attacks and how it would encourage it. At the same time, we found out if the techniques employed have been successful by looking at the collected information from the IP counters and surveys.

A. Creating Fake Accounts

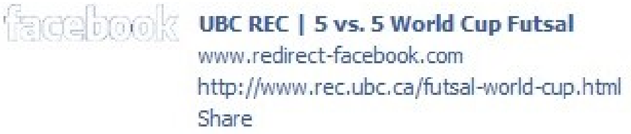
The initial step a phisher would take is to create several fake Facebook accounts. This was simply accomplished by going through the account creation procedures and filling in the required information. After the account was setup, all that was left was to personalize the account to mimic one of a typical Facebook user. We tested the account creation procedure by attempting to create around 10 new Facebook accounts within a very short period of time. Furthermore we repeated this process with both the same IP address and a different IP address each time. This simulates the idea that the adversary would attempt to spoof their IP address in order to go undetected by Facebook. This was accomplished by an IP proxy.

B. Logging into User’s Accounts

This simulation was done assuming one obtained a user’s username and password through a phishing scam similar to the one we describe. There is little one can do with such a simulation, however, we attempted to find out whether the Facebook system could identify whether multiple users can access the same account from different IP addresses. This relates to the scenario that an adversary can log on to an account at the same time as the actual user. This was accomplished by logging into the same account from two different computers. Furthermore, we analyzed the possible situation in which the adversary can log onto an account from a different region of the world within a short time frame. This was achieved through an IP proxy.

C. Exploiting Facebook Interactive Services

We attempted to exploit some of the features Facebook provide such as adding links to wall posts. Once links were added, their metadata would be displayed and the user would have command over the type of information that is shown. An example is provided in **fig 3** below.



UBC REC | 5 vs. 5 World Cup Futsal
www.redirect-facebook.com
http://www.rec.ubc.ca/futsal-world-cup.html
Share

Figure 3: Encapsulated Phishing Scam

The user has the ability to change the title of the link as well as the content that describes it. For instance, the figure above encapsulates the URL that was shown in **fig 1** with the “UBC REC” title and a non-existing link as shown by the last URL. Even though the fake Facebook link was still present, as seen in the middle of the figure, the other data would provide a means of distraction.

D. Flooding Facebook

The last scenario we attempted to simulate was the idea that phishers would attempt to send many phishing scams within a short period of time. Thus, this was accomplished by posting many messages through different groups within a matter of minutes. The concept of this analysis was whether Facebook could determine this action to be suspicious or not. If so, we wanted to find out how long it would take.

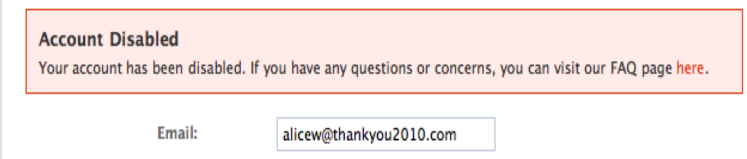
V. RESULTS

The results collected from this analysis provide some interesting and concerning outcomes. Thus to effectively describe them, the same headings used for the analysis methodology will be applied.

A. Problems and Results from Creating Fake Accounts

The first problem that was encountered was the requirement for a valid email to sign up. This was easily solved by the use of widely available online services that provide internet users a temporary email address for a short period of time. Thus any email account will work; even if they end up expiring within 10 minutes.

When attempting to create multiple accounts from the same IP address, Facebook was clever enough to detect this. Within a couple of account creations, a box appeared requesting phone verification to ensure the user was real. However, attempting to sign in with an IP proxy was successful as long the IP was changed every few accounts. Within a few days of account creation, some accounts were disabled as shown in **fig 4**. It was revealed that the ones that were not disabled were due to uncommon names; suggesting Facebook pay close attention to names that are commonly used such as "Alice", "Trudy" and "Bob. However, this is not a major concern.



Account Disabled

Your account has been disabled. If you have any questions or concerns, you can visit our FAQ page here.

Email: alicew@thankyou2010.com

Figure 4: Disabled Account

B. Accessing User Accounts

After some testing and analyzing, it was found that irrespective of the IP address used to access an account using the user's personal information; Facebook would allow the "authorized" person to login. Furthermore, multiple accesses are also allowable; indicating a user and an adversary could be logged in at the same time without detection.

C. Send Many Message on Facebook

After carrying out the analysis, it was discovered that Facebook has already taken care of users sending too many messages within the system. However, when posting messages on groups at a decent frequency (roughly 10 per hour), Facebook was unable to detect messages at this rate.

D. Success of Phishing Scam

The phishing scam that was implemented showed some very interesting results. Out of a sample space of around 60 total users, 31% of them were deceived by the simple scam. This shows that roughly one in three people are likely to give their username and password to the phisher through a social website. Furthermore, 71% of the people who carried out the survey (roughly half of the people who were deceived) mentioned that they did not check the URL before the provided their personal information. In addition, 75% stated that logging onto the Facebook website was second nature to them. These results provide very useful information.

VI. DISCUSSION

The results that were collected from the analysis of phishing on the Facebook social system must be evaluated in order to achieve insights in their meaning.

A. Findings and Implications

From the collected results we realized that one major factor that contributed to the success rate of our simulated phishing scam was due to the human being's habit capture errors. Some tasks become second nature to an individual as a result of having preformed the task so frequently e.g. logging in to Facebook. This is a key factor which attackers could easily exploit with a commonly used network such as Facebook.

Another equally prominent contribution to the success of the simulated phishing scam is the level of trust created due to the constant interaction with people over the Internet (social network). Users tend to trust those who they perceive as being real people and share similar interests and hobbies. It becomes impossible to differentiate between legitimate users and users who have ill intentions.

Despite attempts to increase security the fact that it is difficult to create mutual authentication between Facebook and the user, makes phishing a little easier. Facebook attempts to authenticate the user with the use of several tools (such as phone verification). Nonetheless, these means of authentication are insufficient and do not consistently ensure the legitimacy of the user. Furthermore, there is no fail-safe means for the user to authenticate Facebook besides the URL in the address bar and the common visual interface, which can easily be replicated (such as the login page). This relies on the knowledge of the user, which in most cases is not sufficient.

Moreover, it is important to note that besides the already known implications of a successful phishing scam, users tend to use the same password for multiple accounts throughout the Internet. Access to ones email address and password could be the gateway to successfully impersonating the individual on a variety of other websites (since many allow users to login with their email address). Even worse, if the user uses the same password for their email accounts, the adversary could possibly have access to sensitive information such as financial matters.

B. Principles of Secure Design

Often web 2.0 platforms are faced with the decision of ensuring user accessibility and ease of use or ensuring a more secure system. Many try to find a balance between the two, making security as invisible to the user as much as possible. As this is not easy, more often than not, system designers tend to sacrifice a little on security for user accessibility. Such is the case with many social networks. For instance, Facebook could ask for verification from the user every time the user's account is accessed from a different computer or location but they choose not to. This hinders the user's social experience. Therefore, it is a result of attempting to make the Facebook social system more psychologically acceptable to the user that phishing security was not up to par.

The principal of defense in depth could be further explored in this scenario. By providing more countermeasures such as the ones suggested below, a great deal of attackers could be dissuaded from performing scams as it would take greater effort and more advanced techniques. Another aspect of security design principles that Facebook could benefit from is to assume that human behavior introduces vulnerability. Facebook must design the system with the idea that the average user is either attempting to break it, or has no knowledge of how to be safe on the Internet. A very straightforward example of this principle would be to draw the user's attention to the URL prior to every login.

C. Limitations

Certain limitations we faced in carrying out this analysis caused us to make some assumptions. To preserve user's confidentiality we could not verify that the right information had been entered on the login page. To do this we would have been forced to illegally obtain their information and verify this by logging into their accounts. So we made the assumption that users who arrived at the survey page had entered their real email address and password on the fake login page.

Another limitation we faced was that of the unique IP counter. While it is a lot more accurate and superior to the page hit counter, it provides room for error. Many Internet user's use laptops and connect to networks via a Dynamic Host Configuration Protocol (DHCP). This means that if such a user should revisit the site after having been assigned a new IP address by the Host we would count the new IP address as another visitor.

D. Suggestions

To combat the idea of Habit Capture Errors, we decided to design a very simple prototype to accompany this suggestion. To ensure users did not login to a Facebook account that was not real, we designed a web browser prototype that would compare the URL of the “fake” Facebook page with the real one. By using a simple algorithm, the tool would detect parts of the URL and attempt to determine if it is similar to the URL “facebook.com”. Once a match is found, the tool would assess the location of the server and compare it with the real Facebook multiple IP addresses. If they are equivalent, the URL can be assumed safe and part of Facebook. If not, the tool would warn the user. This method can be applied to a list of commonly attacked websites. The idea behind the tool is to provide some defense in depth (on the browser side) to better help users parse URLs.

The ability that users can use temporary emails (that can be setup in a matter of seconds) should be prevented. Facebook could implement a system that blacklists email domains that provide such service ensuring legitimate email accounts are used. This does not necessarily stop adversaries from creating fake accounts; however, it does slow down the process as they have to undergo various email creation steps.

In terms of the user being able to authenticate Facebook, an SSL connection could be established for the login page. This will provide the visual cues that are well known to secure sites, thus, fake login page replication can be reduced. Along with the SSL, the user should be made aware to look for such indications upon login.

Despite sacrificing a little bit of user accessibility we believe that, with such the size of network Facebook has, it is vital to implement a means to deny access to accounts from a device different from those commonly used by the user without proper authentication. For instance a user should have three registered commonly used devices for accessing Facebook; two computers and one mobile device (similar to apple's 5 computer policy for iTunes content). Access to the users account from all other devices should require additional user authentication unless the user changes their commonly used device and register it with Facebook. Such additional authentication could be in the form of a second password, an email message, a secret question or perhaps one pertaining to information about you that is stored on their server. This will prevent unauthorized access by people who manage to obtain the username and password.

VII. CONCLUSION

Our analysis of phishing on a social system, using Facebook as our stage, provided us with a lot of information regarding both the Facebook system and how users interact with it. We were able to analyze why social networks make phishing scams much harder to detect by the average user. While it is difficult to ensure all users are knowledgeable and use the system correctly, there are several options Facebook can explore in terms of protecting their users.

VIII. REFERENCES

[1] R. Dhamija and J. Tygar, "The Battle Against Phishing: Dynamic Security Skins," University of California, Berkeley,

[2] "Report on Phishing," Binational Working Group on Cross-Border Mass Marketing Fraud, Oct 2006. URL:www.justice.gov/opa/report_on_phishing.pdf

[3] Lawton, G.; , "Web 2.0 Creates Security Challenges," *Computer* , vol.40, no.10, pp.13-16, Oct. 2007doi: 10.1109/MC.2007.367

[4] Facebook [Online]. Available: http://www.facebook.com/press/info.php?statistics

[5] J. Chen and C. Guo, "Online Detection and Prevention of Phishing Attacks," Institute of Communications Engineering,

[6] M. Jakobsson, "Modeling and Preventing Phishing Attacks," Indiana University, Bloomington,

[7] (2010, December 6) 35% of Facebook Users Could Be Victims of Phishing Scams. [Online]. Available: http://blog.zonealarm.com/blog/2010/01/35-of-facebook-users-could-be-victims-of-phishing-scams.html