Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 4th, 2012

Social Network Security Issues: Social Engineering and Phishing Attacks

Jeffrey Allen, Leon Gomez, Marlon Green, Phillip Ricciardi, Christian Sanabria, and Steve Kim
Seidenberg School of CSIS, Pace University, White Plains, NY 10606, USA

Abstract

Social Networking sites have grown in popularity with the number of users who utilize the medium to share aspects of their personal lives increasing yearly. Security issues have been of concern to users, site designers, as well as Security specialists who must find ways to defend corporate networks from malicious attacks initiated from these sites. Social engineering attacks can lead to targeted spear phishing attacks, all with a monetary motive at the root. This study describes and discusses some of these security issues.

2.2 1. Introduction

Social engineering is a significant problem in the increasingly vast use of the Internet. Globally, Internet users are being manipulated and coerced through social engineering into compromising sensitive and personal information. The users of social networking sites such as Twitter, Facebook and Tumblr have a greater risk of being targeted for social engineering because of the vast amount personal information that is shared in these environments. Malicious actors may use the information gathered from these sites to craft targeted attacks to further expose and exploit users.

Facebook users are specifically susceptible to social engineering attacks that can lead to more directed attacks such as spear phishing and click jacking. These malicious events often have motives that are rooted in financial gain for the perpetrators. Both awareness and vigilance in the safe practices from both the software and the user perspectives can help protect users from these threats.

2. Fake Social Networking Accounts

The users of social networking sites such at Facebook, Google, and Twitter, have a reasonable expectation that other users on the networks are who they say they are. However, this is not always true. It is very easy to establish fake accounts on these networks. These “fake” accounts can have access to the private data that the users disclose when creating accounts. While these popular social networking sites have policies against creating fake accounts, there is a lack of a real system to determine the validity of the users [1]. Users must be mindful that there are definitive threats associated with online social networking sites. Malicious actors are seeking out and targeting these users for the wealth of information that can be gained and used to further attack.

It is a common tactic of cybercriminals to create fake pages on social networking sites, possibly that of an attractive woman or popular athlete. This “fake” user will then request to be “friends” with targeted users. Users, who are tricked into adding this friend, open their accounts to the mining of personal data, possible malware infection, or both. A fake program might display some form of warning, for example, “Your computer is running slow and may be infected.” Additionally, this scam will coax the user into downloading antispyware software. Once this program is downloaded, the user’s computer is hijacked and the victim is harassed to purchase the software [2].

2.1 Case Study: Robin Sage

Security Consultant Thomas Ryan conducted a case by creating the same fake personal profile on different social networking sites such as Facebook, LinkedIn, and Twitter. His profile consisted of a young woman purporting to be an analyst at the U.S. Navy's Network Warfare Command [3]. The name of this character was “Robin Sage” with a profile possessing photos of a young Asian model from an amateur pornography site. Once this profile was live, it was able to accumulate up to 300 social networking connections including security specialists, military personnel, staff at intelligence agencies, and defense contractors. Not only was this profile able to attract friends, there were invitations to dinner and recommendations to apply within the defense and intelligence sectors [3]. Other information disclosed by friends of the fake user included home addresses, phone numbers, photos, and other personal information.

Another recent tactic used, similar to the Robin Sage case, targeted victims of all networking sites including YouTube, and Twitter. With this scam, links were sent through blogs, emails, and instant messaging. According to EFF (Electronic Frontier Foundation), a fake YouTube site was created in order to target Syrian activists [4]. This fake page attacked users by asking them to enter their YouTube login credentials in order to leave comments on a video. The page proceeded to install malware disguised as an Adobe Flash Player update. Users who clicked "Install" to update Flash allowed a dropper file, setup.exe to run on the local computer. Once installed, the dropper connects back to an address in the Syrian IP space and downloads additional malware, which gives the attacker administrative access to the computer. [4]

2.2 Preventing Social Engineering with Fake Accounts

In order to recover from an attack of this nature, victims should immediately change their passwords. To prevent future attacks, users should pay close attention for signs that may indicate that a site or page may not be authentic. In extreme cases, the safest course of action may be to completely re-install the OS on an infected computer. Additionally, companies need to develop clear policies surrounding the use of social networking sites, up to and including possibly banning the use on corporate owned networks.

3. Phishing Attacks

The FBI defines phishing as a virtual trap set by cyber thieves that use official-looking emails and fake websites that trick users into revealing personal information. A more specific attack, commonly referred to as “spear phishing,” targets individual users that often possess common attributes. For example, all targeted users may be manager level and above at a particular organization. The most common method of delivery for spear phishing attacks is through email messages disguised as a trusted sender. A spear phishing attack can only happen once the hacker gained a sufficient amount of information about his or her victim. This information is readily available on social networking websites. As a result, spear phishing attacks have flooded social networking websites such as Facebook. [6]

The main goal of a phishing attack is to steal personal information from a user by tricking them into believing they are entering information into a legitimate web page. Once a hacker has tricked a Facebook user into giving up their login credentials, the consequences can range from very minor to catastrophic. The attacker may spam advertisements and other phishing attempts to the victim’s friend’s list. He or she may also post hateful or threatening message under the victim’s account, which can be a very serious offense [6]

3.1 Preventing Spear Phishing Attacks

In spite of the apparent phishing threats, there are a plethora of countermeasures a user can set up on their computer. First and foremost, a user surfing any website, not only Facebook, must have a firewall enabled on their computer. Both firewalls and Antivirus can help fend off well-known vulnerabilities and malicious activity. The preventative measure can in turn help prevent spear phishing attempts. [6] The FBI website advises the use of firewalls and antivirus software. PC Magazine recognizes Norton Internet Security and BitDefender Total Security as two of the top security suites used to prevent any kind of phishing attack. [5]

Aside from the user's duty to protect their computer through use of software, it is essential they also keep all software up to date. Software must stay up to date, whether it is security related or not. Many of the phishing attacks, unrelated to Facebook phishing attacks, rely on exploiting outdated software. These attacks can even take advantage of outdated operating systems, such as Windows XP Service Pack 2 or earlier. The less security flaws or “holes” a user has, the smaller chance a user has to fall victim to a phishing scam. [6]

Adequately equipping your computer with the right tools is only the beginning. By using social engineering techniques, hackers can easily bypass firewalls and antivirus filters that would traditionally block such an attack. Even after taking all of the necessary defensive measures, a social networking user can still be at risk for a phishing attack. Users must be aware of the information they post on Facebook and the users they associate with. [6]

By Facebook users sharing sensitive information in their profile and wall posts, they give hackers a chance to collect information about them in order to perform a spear phishing attack. For example, if a user were to post something harmless such as “I love volleyball” a potential hacker could take that information and potentially craft a unique spear phishing attack intended for that user.[6] The hacker can now send a malicious link to the user disguised as a Facebook video of themselves playing volleyball. The hacker could say something along the lines of “Hey Chris, here’s a video of me playing volleyball this summer I uploaded to Facebook. It might need you to sign in before you view it for security reasons, but it’s a cool video!” This seems like a completely legitimate scenario, but the hacker could have set up a Facebook phishing page for the user to sign into in order to steal their login credentials. Another safe browsing practice is associating with the right users on Facebook.

Recognizing fake Facebook accounts is very important in fending off potential spear phishing attempts on Facebook. Once someone is a friend with a particular user on Facebook, they have access to all kinds of personal information related to that specific user. This information can include name, sex, birthdate, hometown, work place, etc. Most fake Facebook accounts are made for the purpose of gathering as much information as possible about a particular person or group of people. This information can be used to conduct a future spear phishing attack or other kind social engineering attempt.

The validity of some Facebook profiles can be more obvious than others. The most suspicious profiles reveal very little information and keep most of the profile information private. These accounts may be operated by hackers who are impersonating people in order to carry out malicious activities. The less information available on a person sending you a friend request, the less trustworthy the account is. A good safe practice would be to validate the identity of the users that are sending you friend requests. If you are unable to validate the identity of the user, you should not accept the friend request.

In addition to users maintaining a constant awareness of who they associate with on Facebook and what they post, users must be especially aware of the media that is being shared with them through the use of hyperlinks. Users do not simply get phished by innocently surfing the Internet. A user falling to a phishing scheme is equally as responsible as the perpetrator. One must be sure to know exactly what they are clicking on. Carelessly clicking on random links sent through Facebook will effectively mitigate the work being done by your security suite software.[6] The number one indicator to tell a site is suspicious is by looking at the URL in the browser's address bar. According to PC Magazine, many phishing sites don't even try to use believable URLs. Some use warped versions of the true URL, such as facebook.net23.com (facebook.com). If the URL looks skeptical you should immediately leave the site and enter the real URL by hand. [6]

4. Click Jacking Background

Social networking users have become a primary target on the web due to the increasing popularity amongst online social networking. Some of these attacks are performed so discretely that users do not even know an attack has been performed until it is too late. These attacks combine social engineering and altering of web pages in order to prey on social networking users. “Clickjacking,” also known as UI redressing is one of the most common attacks on social networking users today. Clickjacking tricks users into clicking on something that performs an action other than what they are intending. This is performed by creating a web page that has multiple transparent, or opaque layers. By making the top layer transparent, we effectively fool the user into only seeing the web page that is underneath the transparent page. It is common for attackers to lure users in by displaying a picture or link that is tempting, or “too good to be true,” to click on. For example, a typical clickjacking attack would bring you to a link that promises a discount from amazon.com, as long as you click on the name of the artist that is being displayed on the page. Once the link is clicked on, it is possible that the user was just tricked into liking someone’s Facebook page. The motivation for this attack could have been to increase the popularity of his or her Facebook page and to better market the page. As demonstrated in the picture below, a clickjacking web page can be very deceiving because the target web page is invisible and the web page underneath it is the web page that is visible to the user. [16]

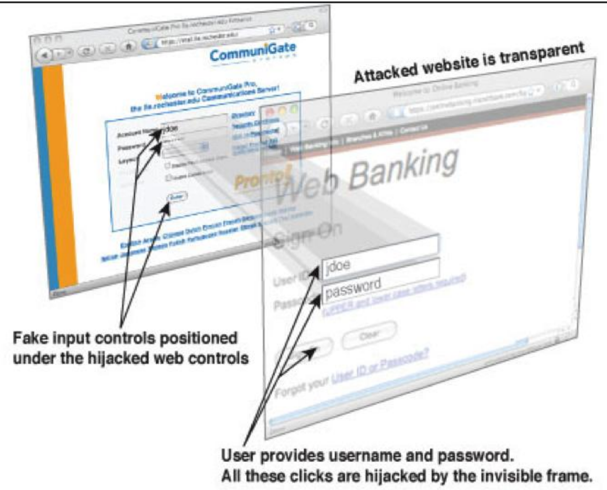

Attacked website is transparent
CommuniGate
Web Banking
Sign On
jdoe
password
Fake input controls positioned under the hijacked web controls
User provides username and password.
All these clicks are hijacked by the invisible frame.

Figure SEQ Figure * ARABIC 1. How a transparent web page can be layered under an existing page to capture private information

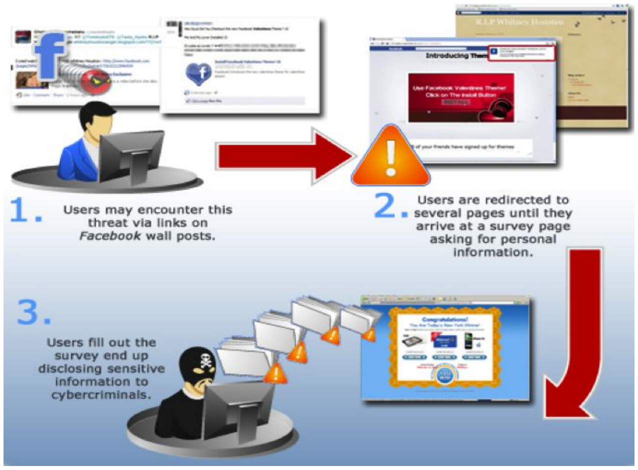

1. Users may encounter this threat via links on Facebook wall posts.
2. Users are redirected to several pages until they arrive at a survey page asking for personal information.
3. Users fill out the survey end up disclosing sensitive information to cybercriminals.

Figure 1. Diagram of how ClickJacking is perpetrated

4.1 Click Jacking Prevention

If performed successfully, clickjacking attacks go unseen by the user. It is extremely difficult to identify a clickjacing web page from a normal web page. Because these links can be freely posted on people's Facebook pages, it is important that users only become friends with people that they know. An important preventative measure is to go through your current friends list and eliminate people you do not know. On social networking websites, you are only as secure as your friends. The friends that you have on Facebook make up your network, and any compromised profiles that sit in your network will put you at risk. The same applies for a network of computers. If one computer is insecurely exposed to attackers, all other computers on the network are now vulnerable to an attack as well. [17]

Clickjacking is one of the most difficult attacks to prevent. As a result, add-ons have been created for some of the most common browsers. These add-ons were developed in order to help spot when there is a transparent web page covering an active page you are visiting. We recommend installing one of these products. They do not interfere with normal browsing and can be very helpful in the prevention of a clickjacking attack. [17]

5. Social Engineering and Social Networks

In today's threat landscape, humans are increasingly becoming the primary target of hackers and criminals searching for the easiest way to compromise corporate networks. Social networking sites such as Facebook and LinkedIn provide a fertile ground for those with malicious intent to seek out, exploit, and then use these network users' computers as pivot points to attack corporate assets. Social engineering is often employed to get users to unwittingly release private information. In fact, reconnaissance is often initially done using these sites to gather information about employees such as names, titles, and email addresses that can be used to make phishing attacks more realistic and effective. Goodchild describes Social engineering as "the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques. [8] For example, a malicious actor wishing to target a defense contractor might identify and research on a social networking site company employees to exploit and use social engineering techniques to compromise data and accounts held by these employees.

Recently, there have been a number of successful high profile attacks that are believed to have used social engineering on Social Networking sites to compromise a network. In her article, Savage describes how attackers gathered information posted by the employees on social networks like Facebook and LinkedIn, set up a Web server hosting a phony photo website, then sent emails containing links that appeared to come from people the employees trusted. Clicking on the links sent them to the website, which downloaded malware and ultimately gave the criminals an opening to infiltrate Google servers. [9] This attack and other like it prove that criminals are actively using social networking sites to develop and commit cyber crime.

The popularity of social networking sites and the millions of users who unknowingly reveal what should be private information is growing yearly. As shown in the diagrams below, 2012 statistics reveal that Facebook currently has 845 million active users registered on its site. The statistics also express that over 50% of the population in North America uses Facebook. [15] Hackers, and nation state backed criminal organizations have taken notice of this popularity, and are actively targeting Facebook users for social engineering attacks, phishing attacks, and data mining attempts. These attacks are not sophisticated, however the data that can be exfiltrated for financial gain or sought out by enemy nation states in espionage attempts.

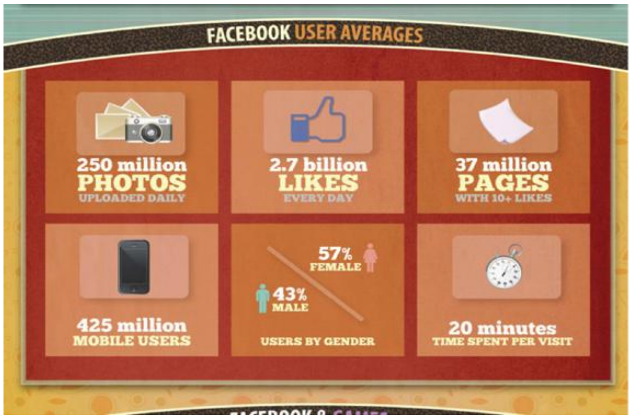

FACEBOOK USER AVERAGES
250 million PHOTOS UPLOADED DAILY
2.7 billion LIKES EVERY DAY
37 million PAGES WITH 10+ LIKES
425 million MOBILE USERS
57% FEMALE
43% MALE
USERS BY GENDER
20 minutes TIME SPENT PER VISIT

Figure 2. Statistical View on the reach of the popular Social Media site Facebook

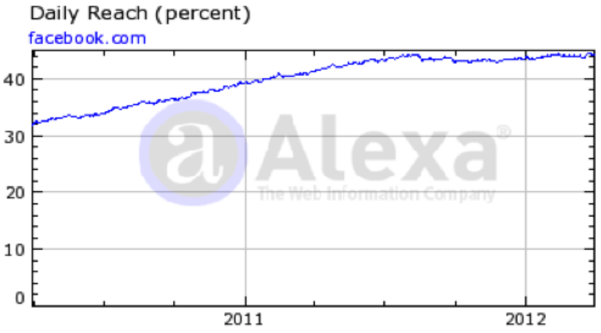


Figure 3. Estimated percentages of US Internet users who visit Facebook.com

5.1 Facebook Applications and Groups

Facebook applications, a large majority of which are games, enhance the user experience during user sessions on the social networking site. These applications often require a user to allow access to all their private data.
This aspect has lead to a proliferation of fake applications that rely on users trust, and even going so far as to have the user recruit new victims for the fake program from their own friends list. Facebook groups are used to allow users to collaborate and communicate with friends with similar interests around a particular topic or community. Users can create groups, post updates, poll users and chat with the entire group at once. [11] Criminals have begun to use fake groups for social engineering and phishing attacks on Facebook users. These groups can contain polls that deceptively attempt to gather user's private information or even have links to malicious sites where credit card information can be captured and sold.

5.2 Preventing Social Engineering using Facebook Applications and Groups

Understanding the threats that social engineering attacks pose are is key to alleviating and avoiding breaches. From a corporate perspective, it is crucial to accept that employees will inevitably use some sort of social networking site at some point, whether during business hours or during off hours and whether allowed or not. Having a strong policy coupled with an awareness-training program will help to mitigate the danger.

Specifically, users can begin with understanding and setting the privacy settings that are built into the social networking site. Facebook has many settings that are turned off by default but allow granular control of private information. Policies must clearly state that users must not post any information that is considered company private or that may disclose privileged information on social networking sites. Information about the user that could be used as a security question, such as mother's maiden name, pet's name, name of high school, etc., should never be posted on a social networking site. These policies and rules must apply to all. Social engineering attacks are not discriminative, and attackers will go after everyone. Users of social networking sites such as Facebook must be sure all potential friends are carefully vetted before being accepted as connections. Due diligence must be performed to ensure friends are who they say they are. [14]

6. Money Laundering

Phishing attacks are forms of organized cyber crimes consisting of accomplices and money launderers. Because phishing attacks are mainly carried out for profit, money laundering is needed "to conceal the coexistence, illegal source, or illegal use of income, and to disguise that income making it appear legitimate". [12] Money laundering consists of three stages:

- Placement easiest method is to "split funds into multiple smaller transactions, such as converting cash into bank money." [12]
- Layering conceals the true origin and owner of the funds. The stage involves "international financial institutes (e.g., offshore banking havens, or other jurisdictions having bank secrecy laws, since the large amounts of daily transfers usually with falsified sender information hinder to trace the source." [12]
- Integration – At this stage illicit funds have sufficiently been layered and can be returned to the mainstream flow.

Accomplices of money laundering are usually separate from the "criminals who committed the actual illicit activity". [12] Money launderers can be broken into three groups: members of organized crime; perpetrators who deliberately collaborate with criminals from such legal positions as, carriers, corrupt bank employees, or accountants; and their "committers doing their regular job, but unaware of their illicit activity, such as financial agents, lawyers, or trustees." [12] Financial agents also called money mules are hired by phishers to transfer funds abroad. Here are some of the strategies employ by phishers to recruit agents.

- Bogus Jobs: Job offerings emailed or printed in newspapers
- Intermediate deals: Using freelancers or members of online-auctions for money laundering.
- Analysis: Fancy web sites built to deceive financial agents.

Money laundering measures:

- Stronger user authentication
- Identification of spoofed sites
- Utilization of trusted computing

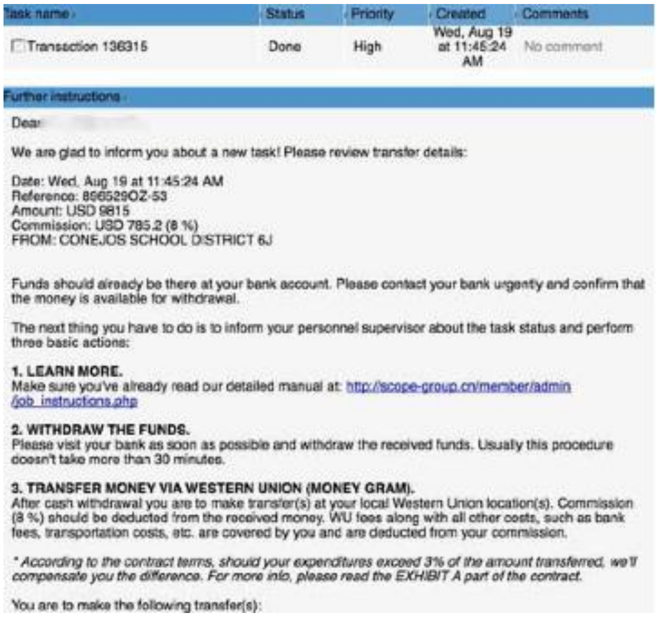
Preventive measure

- Blacklist emails and websites as done with phishing emails and sites

Proactive measure

- Identify and trace financial agents, before they are used by phishers.

Samples of communication between Money
Mules and the phishing attackers:



Task name	Status	Priority	Created	Comments
□ Transaction 136315	Done	High	Wed, Aug 19 at 11:45:24 AM	No comment

Further instructions

Dear [redacted]

We are glad to inform you about a new task! Please review transfer details:

Date: Wed, Aug 19 at 11:45:24 AM
Reference: 896529OZ-53
Amount: USD 9815
Commission: USD 785.2 (8 %)
FROM: CONEJOS SCHOOL DISTRICT 6J

Funds should already be there at your bank account. Please contact your bank urgently and confirm that the money is available for withdrawal.

The next thing you have to do is to inform your personnel supervisor about the task status and perform three basic actions:

1. LEARN MORE.
Make sure you've already read our detailed manual at: http://scope-group.cn/member/admin/job_instructions.php

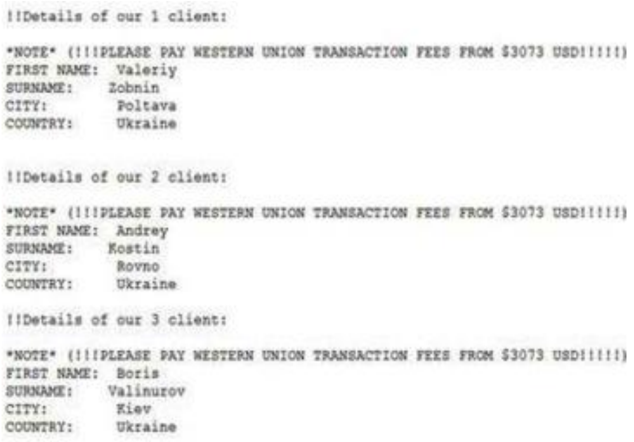
2. WITHDRAW THE FUNDS.
Please visit your bank as soon as possible and withdraw the received funds. Usually this procedure doesn't take more than 30 minutes.

3. TRANSFER MONEY VIA WESTERN UNION (MONEY GRAM).
After cash withdrawal you are to make transfer(s) at your local Western Union location(s). Commission (8 %) should be deducted from the received money. WU fees along with all other costs, such as bank fees, transportation costs, etc. are covered by you and are deducted from your commission.

** According to the contract terms, should your expenditures exceed 3% of the amount transferred, we'll compensate you the difference. For more info, please read the EXHIBIT A part of the contract.*

You are to make the following transfer(s):

Figure SEQ Figure * ARABIC 5. Example of the exchange between victim and perpetrator of a money mule phishing scam



```
!!Details of our 1 client:

*NOTE* (!!!PLEASE PAY WESTERN UNION TRANSACTION FEES FROM $3073 USD!!!!!)
FIRST NAME:  Valeriy
SURNAME:    Zobnin
CITY:        Poltava
COUNTRY:     Ukraine

!!Details of our 2 client:

*NOTE* (!!!PLEASE PAY WESTERN UNION TRANSACTION FEES FROM $3073 USD!!!!!)
FIRST NAME:  Andrey
SURNAME:    Kostin
CITY:        Rovno
COUNTRY:     Ukraine

!!Details of our 3 client:

*NOTE* (!!!PLEASE PAY WESTERN UNION TRANSACTION FEES FROM $3073 USD!!!!!)
FIRST NAME:  Boris
SURNAME:    Valinurov
CITY:        Kiev
COUNTRY:     Ukraine
```

Figure 4. Payment instructions for Money Mule

6.1 Detecting and Preventing Online Money Laundering Attempts

Awareness is a critical ingredient for social network users to be able to identify phishing scams and money laundering attempts. While attackers are improving their skills and in turn getting better at deceiving users, there are basic rules to know and adhere to when interacting via social networks. Users must be diligent and follow these proven deterrents for scams and Internet crimes.

First, and most basically, if a message received in a social media setting looks to good to be true, it almost always is. Users should always seek out and follow independent advice if an offer involves money, time or a commitment. Remember to avoid the temptation of a get rich quick scheme, as the only people who profit in these attacks are the actual scammers. Never send money or give credit card information to anyone the user does not know or trust. Check bank account and credit card statements when received, and immediately report any unexplained transactions. And lastly, report any identified suspected scams to the Internet Crime Complaint Center (IC3) at http://www.ic3.gov . [13]

7. Conclusion

In today's cyber world, users must be aware of the threats associated with online social networking accounts. The users are being targeted by cybercriminals to extract high value information for use in further malicious attacks. Social networking sites have become increasingly popular worldwide. Traditional cyber attacks have shifted toward targeting social networking users. Awareness and following safe browsing practices are critical to preventing cyber attacks such as social engineering, phishing, and click jacking.

8. References

[1] Tom Forenski. (2012, February) ZDNET. Available from http://www.zdnet.com/blog/foremski/the-hollow-emptiness-in-social-media-numbers-most-accounts-are-fake-or-empty/2175?tag=search-results-rivers;item0
[2] Eva Galperin and Morgan Marquis-Boir. (2012, March) InfoSecIsland. Available from http://www.infosecisland.com/blogview/20730-Fake-YouTube-Site-Targets-Activists-with-Malware.html
[3] Matthew Harwood. (2012) Securitymanagment.com. Available from http://www.securitymanagement.com/news/hackers-using-fake-facebook-profiles-peddle-fake-antispyware-006292
[4] (2012, January) FBI Protect Your Computer. Available from http://www.fbi.gov/scams-safety/computer_protect"
[5] Neil Rubenking. (2011, April) PCMag.com. Available from http://www.pcmag.com/article2/0,2817,2384601,00.asp
[6] 2009, April) FBI Spear Phishing. Available from http://www.fbi.gov/news/stories/2009/april/spearphishing_040109
[7] Joseph Straw. (2010, July) SecurityManagement.com. "http://www.securitymanagement.com/news/bombshells-fake-facebook-page-shows-ease-cyberespionage-007409

[8] Joan Goodchild. CSO Online. Available from http://www.csoonline.com/article/514063/Social_Engineering_The_Basics.
[9] Marcia Savage, "TARGET: THE HUMAN Cybercriminals are using social engineering fueled by social media to attack users and break into companies. Information Security, May 2011.
[10] Alexa Website Statistics. Available from http://www.alexa.com/siteinfo/facebook.com
[11] (2012, January) Facebook.com. Available from https://www.facebook.com/about/groups
[12] Sebastian Gajek, Felix Grobert, Ahmad-Reza Sadeghi, Dominik Birk, "Phishing Phishers - Observing and Tracing Organized Cybercrime," in ICMP Second International Conference on Internet Monitoring and Protection , 2007, p. 3.
[13] (2012, January) ScamWatch.gov. Available from http://www.scamwatch.gov.au/content/index.phtml/tag/BankingOnlineAccountScams
[14] (2010, June) Security Awareness Training. Available from http://blog.cosaint.net/2010/06/security-awareness-and-social-networks-why-you-should-care-and-what-you-should-teach/
[15] Infographic Labs. Available from http://infographiclabs.com/news/facebook-2012/
[16] Oscar Celestino Angelo Abendan II. (2012, January) Trendmicro.com.Available from http://about-threats.trendmicro.com/RelatedThreats.aspx?language=uk&name=Think+Before+You+Click%3A+Truth+Behind+Clickjacking+on+Facebook"
[17] Rohan Sharma. (2011, June) ClickJacking. Available from Http://thehackersview.blogspot.com"