CONTACT:
Research Section
5000 NASA Blvd.
Suite 2400
Fairmont, WV 26554
Ph: 304-367-1994
Fax: 304-366-9095

White Collar Crime (WCC) Issue

Facebook © Privacy and Your Identity
February 2016

Definition

In recent months the issue of personal privacy has been a hot topic in the social networking arena, especially regarding Facebook©, Twitter© and a number of other similar outlets. The problem continues with the recent announcement that a lone individual has compiled a database of vital personal information on more than 500 million users through a web crawler program that harvests public information.[1] With these threats in mind, this document will discuss current privacy gaps encountered during social networking and how people should protect their identity online.

How It Happens

The current state of social networking has reached overwhelming proportions. Recently, Facebook© announced that it had 1.55 billion users in 2015, which means that one out of every 15 people on the planet utilizes the site. Social networking has allowed experimentation with cross-site integration with other media sites.[2] By using the "Like" button, Facebook© users can share their website and content preferences with anyone else in their personal network of friends. The result of this sharing platform could potentially position Facebook© as an integral component of the Internet. It allows any user to distribute web preferences, life situations, and any other relevant information instantly to a potentially massive network with just a click of a mouse. This tool is terrific for keeping up with friends, meeting new people, or trying to network with professionals in a challenging economy, but consideration must be given to potential vulnerabilities and the impending exploitation by scammers.

Costs and Statistics

Cyber Social-Engineering

In a classical sense, social engineering refers to the collective manipulation of large groups to meet political or economic ends. Today, it's taken on an additional meaning in the cyber security world. For our purposes, social engineering refers basically to gaining access to information by exploiting human psychology.[3] A classic example is when a friend on your network messages and asks for a quick loan to get car repairs so he/she can get home for work on Monday. A few days later, you find out that your friend never needed car repairs, and that the person you transferred money to was a scam artist.

This form of social engineering is surprisingly easy to achieve. All the scammer requires is your username and password, and then most scammers would be able to impersonate you sufficiently to defraud at least a minority of your network to come to your aid by transferring money. With over 40% of Facebook© users blindly accepting friend requests, the general scenario is one that has become all too common.[4]

Phishing

Phishing is one of the primary techniques of social engineering that are used to gain password information from your banking or social networking accounts.[5] Scammers send out SPAM emails pretending to be your bank, Facebook©, Twitter©, etc., and state that they need you to verify your information. The email continues with a link to a login screen, which allows you to secure your account. However, the "login" is actually a fake replica of the legitimate site. Once you've entered your username and password, you have literally handed over your private information to scammers. Now their only interest is to access your account or network for financial gain. Considering the aforementioned posting of 100 million user profiles, this could turn out to be a very lucrative bank of information for resourceful criminals. It is entirely too early to determine the consequences of these scams, but it could prove to be a boon for criminally motivated social engineers that would use that information against the victim's friends.

High Profile Examples/Case Studies

- Sarah Phillips runs the website Craftybaking.com. Her account, Food, has more than 379,000 followers, and provides Instagram© users with regularly updated beautifully framed pictures of — you guessed it — food. She was one of the first people to latch onto Instagram, and has used it to build her business ever since. Now, companies like Kraft©, Unilever©, and Starbucks© have multi-thousand dollar deals with the woman to work with her concise and catchy Instagram handle. Once the hackers were able to navigate safeguards correctly with personal information, she said they got full control of her account. They redirected her email so all messages were sent to another hacker-controlled burner account. Simply, hackers were able to indicate to Instagram© they "forgot" the password and reset the account thereby gaining full control of the Instagram© site.[6]

- Harriette Cranfield, a former fashion model from England said that hackers used her social media account to entice young girls into sending in photographs with the promise of highly-paid modeling work. One 18-year-old girl was convinced to send topless photos. When the hackers received the revealing photos, they then sent a message to the victim demanding money in return for NOT posting the photos on social media[8]

- January 11, 2016 - Jeremy Bernard Corbyn is a British politician who is the Leader of the Labour Party and Leader of the Opposition. Mr. Corbyn's Twitter© account was hacked. He has a reputation for being opinionated, however; when his account was hacked a number of messages containing vulgarities were sent out in his name. Apparently, the offending tweets were up for only a few minutes

before they were deleted, yet racked up more than 1000 retweets. For Corbyn, this is not much of a setback; indeed, it's unlikely to have any negative effect on his standing as a politician, or his perceived trustworthiness as a public servant. But for a business Twitter© account, or a Twitter© "hack" where the fake tweeter was careful to make the fraudulent tweets seem legitimate, the results could be very different. Bogus earnings warnings, fake notifications of a bigger hack inside the company; untrue claims about mergers and acquisitions have all been scenarios used to attempt to con victims into revealing their personal information or take other actions they would not normally take.[7]

The Response/Current Efforts

Prevention

While there are some crimes committed online that most individuals cannot prevent, protecting your privacy on Facebook© and any other social networking site will put you miles ahead of other individuals. The following are some basic rules to prevent your account from being susceptible to social engineering or phishing.

1. Review your privacy settings. The standard settings on most accounts are fairly flexible and will require you to tighten them to protect your information. Do not allow anyone, but those close to you to have access to phone numbers, birth date, social security numbers (SSN), etc. Any identifying information should stay close to you and not be a part of your network at large. A good general rule to follow is to never provide a SSN over the internet.
2. Share less social information. This means watch what you post in regard to your photos and social life. Over the past few years, employers and educators have made major decisions based on what they found on Myspace© and Facebook© regarding potential candidates. Keep unflattering or risqué postings to yourself or only with close friends, because once you post, it will always be out there. The easiest way to keep your personal info private is to not share it at all.
3. Reconsider that friend request. More and more studies are suggesting that blindly accepting friends is a major risk factor in being victimized. Consider reviewing your network and only interact with individuals that you know or will be working with in the real world. In fact, there are approximately 83 million fake accounts on Facebook©. It may be very costly keeping all those virtual friends around. Studies suggest that 51% of Facebook© users blindly accept friend requests.[8]
4. Use a dedicated email account. Using an email account that is only used for social networking has many advantages. For example, having an email at facebookaccount@yahoo.com is a great way to separate the rest of your life from your social networking. In case you are victimized, your primary email is protected from potential intruders.

All of the discussed concerns have not gone unnoticed by privacy advocates. There are many privacy groups that are currently lobbying Congress to see that changes will be made in the near future to protect consumers' information.[9] In addition there are currently Congressional committee hearings in progress to assess the seriousness of several data breaches, privacy abuses, and future collection of personal data in an increasingly technological world.[10] Until more permanent solutions have been introduced, the responsibility will fall on the individual to be proactive in protecting their personal information. The steps mentioned above will go a long way to see that you're not a part of a growing problem.

"For More Information" Links

Internet Crime Complaint Center – www.ic3.gov
Identity Theft Resource Center – www.idtheftcenter.org
Looks Too Good to Be True – www.lookstoogoodtobetrue.com

Maintenance and revisions: *NW3C Research Department and Nicole Berdar Research Intern WVU*

Bureau of Justice Assistance
U.S. Department of Justice

This project was supported by Grant No. 2015-BE-BX-0011 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Endnotes

[1] Product Reviews. Facebook Info Leaked: 100m Personal Details on Torrent File? Retrieved from http://www.product-reviews.net/2010/07/29/facebook-info-leaked-100m-personal-details-on-torrent-file/ on January 12, 2016. . http://www.dailymail.co.uk/sciencetech/article-1385863/500m-Facebook-users-information-leaked-advertisers.html

[2] January 12, 2016. (http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/) https://zephoria.com/top-15-valuable-facebook-statistics/

[3] CSO Data Protection. Social Engineering: The Basics. Retrieved from http://www.csoonline.com/article/514063/social-engineering-the-basics on January 12, 2016 .

[4] DownloadSquad. Over 40% of Facebook Users Invite Identity Theft by Blindly Accepting Friend Requests. http://www.downloadsquad.com/2009/12/08/over-40-percent-of-facebook-users-invite-identity-theft-by-blind/ retrieved on . January 12, 2016.

[5] CSO Data Protection. Phishing: The Basics. Retrieved from http://www.csoonline.com/article/221737/phishing-the-basics. on January 12, 2016.

[6] Business Insider Magazine. "A social media star says her account was hacked and Instagram did nothing for five days" in Business Insider Tech. July 2, 2015, located at; http://www.businessinsider.com/food-instagram-account-was-hacked-and-it-took-instagram-five-days-to-respond-2015-7

[7] Hacked Twitter Acount embarrasses UK Labor leader. In Naked Security, January 11, 2016, located at; https://nakedsecurity.sophos.com/2016/01/11/hacked-twitter-account-embarrasses-uk-political-leader/

[8] Glamour model's Facebook page hacked to lure underage girls into sending explicit pictures. (2016, January). Retrieved January 19. 2016, from http://www.dailymail.co.uk/news/article-3390245/Page-Three-model-Facebook-page-hacked-conmen-extort-money-teenage-girls.html

[9] 3 million fake accounts on Facebook. https://zephoria.com/top-15-valuable-facebook-statistics/ on January 12, 2016.

[10] 51% of people blindly accept friend requests on Facebook. http://www.dailymail.co.uk/sciencetech/article-2139424/Half-Facebook-users-accept-friend-requests-strangers-13m-U-S-users-NEVER-opened-privacy-settings.html

[11] CNET News. Privacy Groups Assail Facebook Changes. Retrieved from http://news.cnet.com/8301-13578_3-20006220-38.html January 12, 2016. http://www.zdnet.com/article/privacy-groups-call-on-us-government-to-stop-lobbying-against-eu-data-law-changes/

[12] Mercury News. Senators Grill Facebook, Google, and Apple over Privacy Policies. Retrieved from http://www.mercurynews.com/breaking-news/ci_15615463?nclick_check=1 on January 12, 2016.