CONTACT:
Research Section
5000 NASA Blvd., Suite 2400
Fairmont, WV 26554
Ph: 877-628-7674
Fax: 304-366-9095
Web: www.nw3c.org

Criminal Use of Social Media (2011)

The tremendous rise in popularity of social media over the past five years has led to a drastic change in personal communication, both online and off. The popularity of sites such as Facebook®(750 million active users)[1], YouTube® (nearly 500 million users)[2], and Twitter® (200 million users)[3] has made communication for people not only convenient, but downright instantaneous–allowing users to connect and communicate with anyone using the Internet in seconds. In addition to personal usage, businesses and the public sector use social media to advertise, recruit new employees, and maintain partnerships.[4] In fact, social networking now accounts for 22% of total time spent on the Internet.[5] With social media being adopted by so many in society, it's only fitting that white collar and hi-tech criminals adapt their skill set to the ever-changing landscape of the Internet. This white paper will discuss how criminals are using social media and Web 2.0 technologies to perpetrate new and classic white collar crimes.

Social media is difficult to define at times, but for the purposes of this paper, social media will be defined as any website or software that allows you to receive and disseminate information interactively. This especially includes websites that allow you to read social updates or an informative article and moments later being able to respond with a text update, post a video, or stream audio. There is a variety of different formats of social media that equip users with the ability to share information. The following will discuss these formats and their potential for criminal use.

Crimes for the 21st Century

The most popular form of social media is social networking, which consists of websites that allow users to create an online profile in which users post up-to-the-minute personal and professional information about their lives that can include pictures, videos, and related content. Websites under this category include Facebook®, LinkedIn®, Twitter®, and the now nearly defunct Myspace®. Social networking is a potential gold mine for criminals who leverage the users' personal details into financial opportunity.

Burglary: Simplified

The classic example of exploitation on social networking sites involves the perpetrator perusing users' profiles and looking for potential victims in the vicinity who won't be home. For instance, Facebook® users can post that they will be out for the evening, which gives potential thieves a large time window to burgle the property. Stories of this nature are appearing in the media[6] and serve as a reminder that users are not as cautious as they should be with their personal information. The thieves are sometimes caught by using stolen wares that are unique in some way. For example, a recent investigation in New Hampshire ended when thieves who used Facebook® to profile victims were caught using a very peculiar type of firework that was recently taken in a burglary. An off-duty officer investigated firework explosions he could hear in the distance. The fireworks were stolen in the series of break-ins over the prior month.[7]

Other social networking applications, such as foursquare® and Gowalla®, are primarily location-based networks. Users of these networks are rewarded for posting their locations frequently and are given temporary titles while at their location–for example, posting that you're having a cup of coffee at Starbucks® could make you the "Mayor of Starbucks®."[8] As before, posting your location allows perpetrators the perfect window to commit a burglary, vandalism, or a home invasion.

Social Engineering & Phishing

Not surprisingly, the majority of crimes on social networking sites are cyber based, and many of them use a technique called social engineering. In a classical sense, social engineering refers to the social manipulation of large groups of people 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 to gaining access to information by exploiting human psychology.[9] A classic example of this starts with a friend on your network sending you a message asking for a quick loan to get car repairs so he/she can get home for work on Monday, and ends with you finding out a few days later 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, and because of it, the computer security firm Trend Micro® calls Facebook® a "minefield of scams."[10] All that is needed by the scammer is the username and password of one member of a network and a little practice in writing letters that sound urgent to inspire friends to aid you. All the while the scammer is vague enough not to reveal the impersonation. Even if only a few friends on the list are duped, the return on investment for the scammer is quite high. Social engineering isn't limited to social networking. A recent case involved the software company Oracle®. During a convention, a contest was held to demonstrate the dangers of social engineering. Several hackers posed as IT professionals and asked company employees to hand over data and visit websites as part of "routine IT protocol." Oracle® employees as well as many others were frighteningly compliant in the demonstration.[11]

One popular technique of social engineering is called phishing. Phishing involves making attempts to acquire passwords, account numbers, and related information; this information is often used to commit identity theft. The term phishing is a play on "fishing," in which perpetrators send out many (sometimes millions) of emails with the hopes of getting "bites" in return. The victimization rate that results is usually somewhere in the 0.5% to 1% range.[12] Despite the low success rate, criminals continue to send out emails that look like legitimate concerns over account security or sale reminders from your favorite retailer.[13] Microsoft® has recently reported that phishing attacks are up over 1200% from 8.3% phishing attacks to 84.5% phishing attacks just over the course of 2010.[14]

Malware

Last, social networking offers golden opportunities for virus and malware developers. Users clicking on links, opening attachments, and responding to messages on networks can become victims without knowing it, resulting in adware, viruses, and malware being loaded onto their machines. In December 2010, antivirus developer Sophos® reported that 40% of social network users had encountered malicious attacks.[15] Microsoft® released their own study in the spring of 2011, stating that rogue software was found on 19 million PCs.[16] Additionally, the business world is concerned that their employees' online behavior could be putting their network security at risk. Sophos'® 2010 Security Report surveyed over 500 organizations and found that 72% were concerned that social networking endangered their security.[17]

Cybercasing the Joint

The most recent development in social media technologies is called geotagging, which embeds geographical data (longitude and latitude) into media such as photos, videos, and text messages.[18] Geotagging media allows users' locations to be posted along with their media. The location of users can be found quickly and with frightening precision by combining the geotagging of media-friendly sites, such as YouTube®, Flickr®, Google Maps®, and Craigslist®, with all the aforementioned networking sites to triangulate all positions known.[19]

A recent study from the International Computer Science Institute tested the potential to use all publicly available resources to determine the locations of a variety people on the Internet.[20] In a process called cybercasing, online tools are used to check out details, make inferences from related data, and speculate about real-world locations for questionable purposes. In other words, cybercasing uses the Internet to determine the location of a desired victim using any available resource. The cybercasing study used three different websites in their scenarios.

1. The first scenario used the virtual classified ad site Craigslist® to spot desirable photographs with geotagged data. In most cases, the researchers were able to cross-reference Google Street View® to determine the exact address of the poster. Researchers also determined what times were best to burgle a residence by a poster's ad that would often state "Please call after 5 p.m.," implying that they would be gone at work on most days.
2. The second scenario examined the Twitter® feed of a well-known reality show host. By viewing the pictures posted on TwitPic® with the Firefox® plug-in Exif Viewer[21], the researchers only had to right click on the celebrity's pictures to reveal geographical coordinates. By taking the average of several pictures posted in a similar region, the researchers could determine the location of the user with great precision.
3. Lastly, YouTube® was used to find the home address of someone currently on vacation. By creating a script that collects usernames and downloads the related videos, researchers were able to find a user that lived in the predetermined area of Berkley, CA, and was currently on vacation in the Caribbean, as determined by his most recent YouTube® uploads. The researchers were able to use his real name in a Google® search to determine his address. The entire process took less than 15 minutes.[22]

Later in the paper we will discuss what can be done to protect you against this type of victimization.

Costs and Statistics

The prevalence of criminal activity on social media sites is difficult to determine. In fact, there are currently no comprehensive statistics on social media crimes. This can be due to a number of factors, especially considering the broad nature of social media, anonymity afforded to criminals, and relative unawareness of Internet users, which can create a ripe environment for victimization. However, we can look into related crimes that can involve social media to estimate how often these crimes occur.

Identity Theft

- The 2010 Internet Crime Report from the Internet Crime Complaint Center (IC3) reported that identity theft was the third highest complaint at 9.8% for 2010. In addition, identity theft was the second most referred crime to law enforcement at 16.6%.[23]

- The Consumer Sentinel, a database maintained by the Federal Trade Commission (FTC) that collects information about consumer fraud from the FTC and other reporting agencies, reported that the number one complaint category was identity heft with 247,000 complaints (19%of all complaints) received by the Consumer Sentinel in 2010.[24]

- The identity theft survey released in early 2010 by Javelin Strategy and Research revealed that approximately 3.5% of the U.S. population fell victim to identity theft within the previous year (the survey was conducted in 2010), suggesting that 8.1 million Americans were ID theft victims in 2010. The mean costs to resolve the crime was $631, which was the highest average dollar amount since 2007.[25]

Cyberstalking

- A federal study of offline stalking indicated that one out of every 12 women (8.2 million) and one of every 45 men (2 million) claims to have been stalked at some point.[26] This study also found that 1% of all women and 0.4% of all men were stalked during the 12 months preceding the study.[27] It reported that women are far more likely to be victims of stalking than men, as nearly four out of five stalking victims are women, while men are much more likely to be stalkers–87% of the stalkers identified by victims in the study.[28] Finally, during their lifetimes women are twice as likely as men to be victims of stalking by strangers and eight times as likely to be victims of stalking by intimates.[29]

- In 2010, statistics of cyberstalking victimization compiled by Who@ showed that harassment most often originated through emails, comprising 34% of cases followed by Facebook® with 16.5%. Of all cases reported, 79% escalated in some way. The top two ways in which incidents escalated were through email (28%) and Facebook® (15%). Threats of offline violence occurred in 25% of cases.[30]

- In 2003, the FBI published a descriptive study of NYPD's Computer Investigation and Technology Unit (CITU). The CITU investigates cases in which the offender uses a computer as the primary instrument to commit a crime. Examining 192 closed cases from 1996 to 2000, cyberstalking was the most reported crime to the CITU, comprising 42.8% of the cases investigated by the CITU. The study revealed similar findings to traditional stalking in that 80% of cyberstalkers were male. However, cyberstalkers appear to be younger than offline stalkers. CITU reported an average male age of 24. In addition, 26% of offenders were juveniles, under the age of 16, according to New York State law. Victims were most commonly women (52%), with men being targets in 35% of the cases; other victims included educational institutions and private corporations.[31]

The statistics reviewed suggest that identity theft and stalking/cyberstalking are prevalent and costly crimes. In addition, social media such as Facebook®, Twitter®, YouTube®, and Flickr® all offer an avenue of contact for potential perpetrators. Currently, there is no way to determine the overall occurrence of crimes on social media, but the preceding suggests that social media sites are ideal outlets for fraudsters and stalkers.

Examples/Case Studies

- In 2008, hackers sent messages to Facebook® users stating, "Hey, I got a new Facebook account. I'm going to delete this one, so add my new profile." Upon clicking the hyperlink to add their

friend's new account, the users were sent to a phishing page that was designed to collect their user information. The page looked identical to a Facebook® login page; however, the URL was view-facebookprofiles.com, which is not a subdomain of Facebook® and is one of the telltale signs of a phishing page. However, most people did not recognize this, and potentially thousands of Facebook® users had their accounts compromised by giving away their usernames and passwords. This was not the first attempt at phishing on Facebook®, but it was certainly one of the most coordinated and stands as classic example of phishing.[32]

- In 2007, the dangers of cyberbullying were brought to light when a teenage girl, Megan Meier, committed suicide when it was revealed that a boy she admired on Myspace® was actually a classmate's mother antagonizing the teenager for being different.[33] The mother, Lori Drew, allegedly communicated to Megan as "Josh" for over one month and then abruptly ended the relationship. Megan committed suicide the same day. Lori Drew was convicted of computer fraud and abuse, but was acquitted for Meier's death.[34]

- In 2009, Justin Brown was arrested for impersonating a model named Bree Condon on the dating site Seekingmillionaire.com. Unlike many scams perpetrated on social networking sites, Mr. Brown impersonated a real model and assumed her real name. Ms. Condon hired a private investigator who ultimately alerted police to the fraud that her name, likeness, and professional photographs were being used in the scam until Mr. Brown was arrested. Investigators later learned that Mr. Brown had phone conversations with wealthy men in exchange for money and gifts (iPhone® and $15,000 cash). The scam is an exception considering the care that Mr. Brown took and demonstrates what can be perpetrated by a lone individual. Mr. Brown said that he created a plausible biography of Ms. Condon by using her online biographical information. While the following did not occur on a social media site discussed yet in this paper, the exact scenario could happen on any social networking site.[35]

Prevention Tips

While it's impossible to completely safeguard yourself from being victimized online, the following 10 tips can give you reasonable protection from being victimized on a social media site.[36]

1. **Use caution when you click links** that you receive in messages from your friends on your social website. Treat links in messages on these sites as you would links in email messages.

2. **Know what you've posted about yourself.** A common way that hackers break into financial or other accounts is by clicking the "Forgot your password?" link on the account login page. To break into your account, they search for the answers to your security questions, such as your birthday, home town, high school class, or mother's middle name. If the site allows, make up your own password questions, and don't draw them from material anyone could find with a quick search.

3. **Don't trust that a message is really from who it says it's from.** Hackers can break into accounts and send messages that look like they're from your friends, but aren't. If you suspect that a message is fraudulent, use an alternate method to contact your friend to find out. This includes invitations to join new social networks.

4. **To avoid giving away email addresses of your friends, do not allow social networking services to scan your email address book.** When you join a new social network, you might receive an offer to enter your email address and password to find out if your contacts are on the network. The site might use this information to send email messages to everyone in your contact

list or even everyone you've ever sent an email message to with that email address. Social networking sites should explain that they're going to do this, but some do not.

5. **Type the address of your social networking site directly into your browser or use your personal bookmarks.** If you click a link to your site through email or another website, you might be entering your account name and password into a fake site where your personal information could be stolen.

6. **Be selective about who you accept as a friend on a social network.** Identity thieves might create fake profiles in order to get information from you.

7. **Choose your social network carefully.** Evaluate the site that you plan to use and make sure you understand the privacy policy. Find out if the site monitors content that people post. You will be providing personal information to this website, so use the same criteria that you would to select a site where you enter your credit card information.

8. **Assume that everything you put on a social networking site is permanent.** Even if you can delete your account, anyone on the Internet can easily print photos or text or save images and videos to a computer.

9. **Be careful about installing extras on your site.** Many social networking sites allow you to download third-party applications that let you do more with your personal page. Criminals sometimes use these applications to steal your personal information. To download and use third-party applications safely, take the same safety precautions that you take with any other program or file you download from the Web.

10. **Turn the geotagging feature off.** This is the most direct solution and you can find out how to do this for most phones.[37]

"For More Information" Links

- Internet Crime Complaint Center – http://www.ic3.org
- International Associate of Chiefs of Police Social Media Project – http://www.iacpsocialmeda.org
- National Center for Victims of Crime – http://www.ncvc.org/ncvc/main.aspx?dbName=DocumentViewer&DocumentID=32458
- Privacy Rights Clearinghouse – http://www.privacyrights.org/
- U.S. Department of Justice – http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm
- Working to Halt Online Abuse – http://www.haltabuse.org/index.shtml
- Please Rob Me (Dangers of Over Sharing) – http://www.pleaserobme.com

Primary Author: Jason Boone, NW3C Research Associate

Endnotes

[1] Facebook Statistics. (2011). Facebook. Retrieved on August 8, 2011 from http://www.facebook.com/press/info.php?statistics.

[2] Royal Pingdom. (2011). Facebook, Youtube, Our Collective Time Sinks. Retrieved on August 8, 2011 from http://royal.pingdom.com/2011/02/04/facebook-youtube-our-collective-time-sinks-stats.

[3] BBC. (2011). Twitter co-founder Jack Dorsey, rejoins company. Retrieved on August 8, 2011 from http://www.bbc.co.uk/news/business-12889048.

[4] Business News Daily. (2011) 5 Ways Businesses Will Use Social Media in 2011. Retrieved on August 8, 2011 from http://www.businessnewsdaily.com/five-ways-businesses-will-use-social-media-in-2011-0895/.

[5] Nielsen Wire. (2010). Social Networks/Blogs Now Account for One in every Four and a Half Minutes Online. Retrieved on August 17, 2011 from http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online.

[6] NDTV. (2011). Thieves Use Facebook To Rob Empty Homes. Retrieved on August 9, 2011 from http://www.ndtv.com/article/world/thieves-use-facebook-to-rob-empty-homes-112970.

[7] Escapist Magazine. (2011). Thieves Target Homes Based on Facebook Updates. Retrieved on August 9, 2011 from http://www.escapistmagazine.com/news/view/103419-Thieves-Target-Homes-Based-on-Facebook-Updates.

[8] Time. Please Rob Me: Site Shows Dangers of Foursquare, Twitter. (2010). Retrieved on August 12, 2011 from http://www.time.com/time/business/article/0,8599,1964873,00.html.

[9] CSO Data Protection. Social Engineering: The Basics. Retrieved on August 4, 2010 from http://www.csoonline.com/article/514063/social-engineering-the-basics.

[10] GMA News. (2011). Mobile malware, social network scams top cyber threats. Retrieved on August 9, 2011 from http://www.gmanews.tv/story/228317/technology/mobile-malware-social-network-scams-top-cyber-threats-report.

[11] Computing.co.uk. (2011). Oracle Data Obtained In Social Engineering Attack. Retrieved on August 9, 2011 from http://www.computing.co.uk/ctg/news/2100282/oracle-obtained-social-engineering-attack.

[12] The Register. (2009). One in 200 Success Rate Keeps Phishing Economy Ticking Over. Retrieved on August 9, 2011 from http://www.theregister.co.uk/2009/12/07/phishing_hit_rate.

[13] Phishtank. (2011). What is Phishing? Retrieved on August 9, 2011 from http://www.phishtank.com/what_is_phishing.php?view=website.

[14] Information Week. (2011). Microsoft: Cybercrime Falling into Two Distinct Camps. Retrieved on August 9, 2011 from http://www.informationweek.com/news/security/vulnerabilities/229500284.

[15] Time: Techland. (2011) 40% of Social Network Users Attacked By Malware. Retrieved on August 9, 2011 from http://techland.time.com/2011/03/23/40-of-social-network-users-attacked-by-malware.

[16] Ibid.

[17] Sophos. (2011). 2010 Security Threat Report. Retrieved on August 10, 2011 from http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf.

[18] New York Times. (August 11, 2010). Web Photo Reveal Secrets, Like Where You Live. Retrieved on August 12, 2011 from: http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html.

[19] Read Write Web. (2010). Researchers Warn of Geotagging Dangers: Are You Concerned? Retrieved on August 12, 2011 from http://www.readwriteweb.com/archives/researchers_warn_of_geotagging_dangers_are_you_concerned.php.

[20] Friedland, Gerald & Sommer, Robin. (2010). Cybercasing the Joint: On the Privacy Implications of Geo-Tagging. International Computer Science Institute, August, 2010. Retrievable: http://www.icsi.berkeley.edu/cgi-bin/pubs/publication.pl?ID=002932.

[21] Mozilla Firefox. (2011). Add-Ons - Exif-Viewer. Retrieved on August 15, 2011 from https://addons.mozilla.org/en-US/firefox/addon/exif-viewer/.

[22] Ibid.

[23] Internet Crime Complaint Center. (2011). 2010 Annual Internet Crime Report. Retrieved on August 11, 2011 from http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf.

[24] Federal Trade Commission. (2009). *Consumer Sentinel Network Databook.* Retrieved August 15, 2011 from http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf

[25] Javelin Strategy & Research. (2011). 2011 Identity Fraud Survey: Consumer Version. Retrieved on August 15, 2011 from https://www.javelinstrategy.com/uploads/1103.R_2011%20Identity%20Fraud%20Survey%20Consumer%20Report.pdf

[26] Tjaden, P., & Thoennes, N. (1998, April). Stalking in America: Findings from the national violence against women survey [Electronic version]. Washington, DC: National Institute of Justice & National Center for Injury Prevention and Control. Available at http://www.ncjrs.org/pdffiles/169592.pdf [cited in U.S. Department of Justice. (1999, August). 1999 Report on cyberstalking: A new challenge for law enforcement and industry. A report from the Attorney General to the Vice President. Retrieved January 29, 2003, from http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm].

[27] Tjaden, P., & Thoennes, N. (1998, April). Stalking in America: Findings from the national violence against women survey [Electronic version]. Washington, DC: National Institute of Justice & National Center for Injury Prevention and Control. Available at http://www.ncjrs.org/pdffiles/169592.pdf.

[28] Tjaden, P., & Thoennes, N. (1998, April). Stalking in America: Findings from the national violence against women survey [Electronic version]. Washington, DC: National Institute of Justice & National Center for Injury Prevention and Control. Available at http://www.ncjrs.org/pdffiles/169592.pdf.

[29] Tjaden, P., & Thoennes, N. (1998, April). Stalking in America: Findings from the national violence against women survey [Electronic version]. Washington, DC: National Institute of Justice & National Center for Injury Prevention and Control. Available at http://www.ncjrs.org/pdffiles/169592.pdf.

[30] Who@: Working to Halt Online Abuse. (2009). 2009 Cyber Stalking Statistics.. Retrieved September 15, 2009. From http://www.haltabuse.org/resources/stats/2008Statistics.pdf

[31] FBI Law Enforcement Bulletin. (March 2003). A Study on Cyberstalking. Retrieved on August 9, 2011 from http://findarticles.com/p/articles/mi_m2194/is_3_72/ai_99696472/.

[32] TechCrunch. (2008). Phishing Scam Targeting Facebook Users. Retrieved on August 17, 2011 from http://techcrunch.com/2008/03/26/phishing-scam-targeting-facebook-users.

[33] Fox News. (2007). Mom: Myspace Hoax Led to Daughter's Suicide. Retrieved on August 11, 2011 from http://www.foxnews.com/story/0,2933,312018,00.html.

[34] MSNBC. (2009). Ruling Disappoints Myspace Victim's Mom. Retrieved on August 16, 2011 from http://today.msnbc.msn.com/id/31722986/ns/today_people.

[35] L.A. Times. (2010). Man masquerading as fashion model bilks wealthy men. Retrieved on August 10, 2011 from http://articles.latimes.com/2010/jan/19/entertainment/la-et-bree-condon19-2010jan19.

[36] Microsoft Security Center. (2011). Social Networking Safety. Retrieved on August 15, 2011 from http://www.microsoft.com/security/online-privacy/social-networking.aspx.

[37] Private i. (2011). The Dangers of Geotagging and How to Protect Yourself. Retrieved on August 11, 2011 from http://www.privatewifi.com/the-dangers-of-geotagging-and-what-you-can-do-to-protect-yourself.

This project was supported by Grant No. 2010-BE-BX-K009 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, the Community Capacity Development Office, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. 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.