Federal Bureau of Investigation

Social Media Guidelines

FIDELITY / BRAVERY / INTEGRITY

Introduction to Social Networking Sites:

»» Social Networking Sites are among the most popular components of Web 2.0, which is the second generation of the World Wide Web that allows individuals to interact and share information online. At various SNS, individuals can create personal profile pages, that may include pictures, video, and postings on personal interests.

»» These sites allow each user to maintain a list of friends who may also post messages on his/her profile page.

»» A user can choose who has access to the information posted on his/her profile page (e.g. users on the same network or group, confirmed friends, the general public).

Global Social Media Trends:

»» According to a February 2012 press release from *ComScore*, Facebook more than tripled its U.S. visitors from 54.5 million in December 2008 to 163.5 million in December 2012. (Worldwide, Facebook draws 845 million monthly active users, and is available in more than 70 languages).

»» According to a June 2010 World Internet Usage Statistics News and Populations Stats, approximately 1.966 billion people use the internet.

»» According to the Department of Homeland Security, cyber attacks against the government and private networks increased from 4,095 in 2005 to 72,065 in 2008.

»» Nearly sixty-three percent of American adults maintain a profile on SNS. Nearly eighty percent have use privacy settings to restrict access by strangers, according to a February 2012 survey by the Pew Research Center.

»» The Federal Trade Commission estimates that as many as 200,000 million Americans had their identities stolen in 2011.

»» According to *Alexa.com,* one of the largest web crawls, Facebook was the second most trafficked site in the world as of March 2011, as well as the top photo-sharing site with 10 billion photos uploaded.

»» A recent study by the National Cyber Security Alliance reported that although 57 percent of individuals on SNS admit to worrying about becoming a victim of cyber crime they still provide information that may put them at risk.

»» According to *Technorati,* a leading blog search engine and directory, there are 112.8million blogs and 250 million pieces of tagged social media online. More than 175,000 new blogs are created each day.

»» Seventy-eight percent of American adults (age 18 and older) use the Internet.

»» Sixty-three percent of all American are part of a wireless, mobile population that participates in digital activities away from home.

»» Facebook and other popular SNS have developed applications that can identity a user's information. Home addresses, for example, can be found and mapped within a matter of seconds. Location services have become extremely popular as more people take advantage of smart phones with GPS and other mapping capabilities. The Facebook application can either be downloaded or viewed via the mobile Facebook page, and its settings can be changed manually to allow 'friends of friends" or the general! public to view a user's personal information.

Guidelines:

The guidelines below have been provided to increase awareness of the potential threats and risks that employees may experience when accessing SNS on personal, non-government systems. SNS, web pages, email accounts, and wireless access points are all vulnerable to identity theft and information aggregation. Adversaries Include hackers, foreign intelligence agents, terrorists, and criminals who may target your family, friends, neighbors, and/or coworkers.

»» SNS are a counterintelligence (CI) and operations security (OPSEC) concern because critical, sensitive, and/or personal information may inadvertently be disclosed. FBI personnel should be careful when providing any information online about themselves, their organization, or their lob. They should refrain from disclosing on any section of their user profiles that they work for the FBI or the Department of Justice. FBI personnel must also consider each word that they post, as these posts will remain indefinitely in cyberspace.
»» FBI personnel shall not promote their personal or professional importance in profile(s) or posting, as this may make them a potential target for adversaries to exploit.
»» FBI personnel should not provide details regarding their work associates, official position, or duties.
»» FBI personnel shall not advertise weaknesses, vulnerabilities, or loopholes within FBI systems or capabilities.
»» FBI personnel shall limit the amount of personal information that they post on SNS. Do not post information that would make you vulnerable, such as your home address or information on your schedule/routine (e.g. on Twitter or LinkedIn). If your friends or connections post information about you, make sure that the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when pasting information on your connections, including photographs (e.g. on Facebook, MySpace, or dating websites).
»» FBI personnel are prohibited from using FBI Information Systems (IS) to access publicly accessible SNS for non-FBI business purposes.
»» FBI personnel who access SNS for personal use from non-FBI IS (e.g., home or publicly available IS) shall not disclose information pertaining to FBI operations or any other information gained by virtue of FBI employment, either during or after their tenure of service with the FBI. This includes photographs or videos involving official FBI related matters and/or FBI facilities.
»» FBI personnel shall not establish any publicly accessible SNS that represents itself as an official FBI site or as affiliated with the FBI.
»» FBI personnel shall not use or associate official FBI email accounts with personal social networking accounts.
»» FBI personnel shall comply with the FBI Seal, Name, Initials and Special Agent Gold Badge Policy, Corporate Policy Directive 0266D, regarding any use of the FBI Seal, Name, Initials or Special Agent Gold Badge, to include use on publicly available SNS.
»» Any suspected or confirmed cases of information spillage and/or disclosure of US Government Protected Information (USGPI) on a publicly accessible SNS shall be immediately reported to the Chief Security Officer.
»» FBI personnel should remember that the internet is a public resource. They should only post information that they are comfortable with anyone accessing. This includes information and photos in profiles, blogs and other forums. Once information is posted online, it cannot be retracted. Even if an individual removes information from a web page, the saved or cached versions of that page may still exist on other users' systems. (This applies to SNS).
»» FBI personnel should evaluate the user settings for their online profiles. It is critical to take advantage of SNS' privacy settings. The default settings for some sites may allow anyone to see a user's profile. Settings can be customized to restrict access to certain people. However, the risk remains that even private information can be exposed. Therefore, caution is necessary when posting any information that may be unsuitable for the public to access, when deciding which applications to enable, and when checking settings to determine what information the applications will be able to access.
»» FBI personnel should protect their accounts by choosing strong passwords that cannot be easily guessed. A strong password is one that uses character classes: uppercase and lowercase letters, numbers, symbols, and/or special characters.
»» FBI personnel should verify the privacy policies on SNS. Some SNS may share information, such as email addresses or user preferences with other companies. This may lead to an increase in spam. FBI personnel should also review

SNS' policies for handling referrals to ensure that their friends are not being unintentionally registered to receive spam. Some SNS will continue to email invitations to everyone referred by account owners until they agree to join.

»» FBI personnel are strongly encouraged to use and maintain anti-virus software. Because attackers are continually writing new viruses, it is important to keep definitions up to date. It is also important to keep all computer applications up to date, as old versions may be exploited by criminals to access the computer.

»» Although most individuals accessing SNS do not pose a threat, there are malicious people being drawn to SNS due to the accessibility and amount of personal information that they make available. The more information that can be learned about an individual, the easier it become for a malicious person to exploit him/her. Predators may form relationships online and then convince unsuspecting individuals to meet them in person, creating a potentially dangerous situation. Malicious people may also use personal information to coerce an individual into providing them with information that they should not be able to access. (For example, social engineering).

»» Any information provided on an individual's location, hobbies, interests, and/or friends can be used by a malicious person to impersonate a trusted friend and convince that individual to disclose other personal or financial data.

»» Children are especial susceptible to the threats that SNS present. Although many sites have age restrictions, children may misrepresent their ages in order to join. Parents can ensure that their children become safe and responsible Internet users by being aware of their children's habits and guiding them to appropriate sites.

»» Parents should talk to their children about not identifying a parent as an FBI employee on SNS.

»» FBI personnel should not post any information on SNS (including photography) that is not already in the public domain and could reasonably be expected to affect the personal security of work associates or the operational security of the FBI and its personnel. This includes such information as the official position(s) of the poster and/or any work associate. To the extent practicable, FBI personnel should take reasonable precautions, including the communication of potential risks of disclosure, to guard against friends and/or relatives posting about their professional affiliations onto SNS.

»» FBI personnel should not post information on SNS that would make them vulnerable to physical harm, emotional distress, other disruptive behavior, or threats thereof. If information about FBI personnel is posted on SNS by friends or connections, then FBI personnel should take all reasonable steps to ensure that the combined information is not more than they would be comfortable with the public knowing.

»» FBI personnel should be wary of strangers. The internet makes it easy for people to misrepresent their identities and motives. FBI personnel should consider limiting the people who can contact them on SNS. If interacting with people they do not know, FBI personnel should be cautious about the amount of information that they reveal, (for example: on MySpace, YAHOO, MSN Messenger, etc.), especially in person.

»» The more letters, numbers, and special characters used, the stronger a password becomes. Compromised passwords may allow malicious people to access SNS accounts and pretend to be their owners.

Guidelines for Popular Sites:

W Wikipedia:

»» Wikipedia is a resource for conducting research and a community of people with similar interests who help shape and guide what is posted under online entries. It has a strong set of rules for editing entries.

»» Wikipedia's *Law of Unintended Consequences* states, "If your write about yourself or your organization in Wikipedia, you have no right to control its content, or delete it, outside of your normal channels.

»» "Content is not deleted just because somebody doesn't like it. If there is anything publicly available on a topic that you would not want included in an article, it will probably find its way their eventually. Therefore, don't create promotional or other articles lightly, especially on subjects you care about."

●● Flickr:

»» Flickr is a popular photo sharing website that allows users to post images that are generally visible and available for download by the general public. It is important to abide by the community guidelines and be cautious when uploading. Always review the Terms of Use.

Operations Security Incidents and Examples:

The following incidents provide several real-world examples that highlight the threats posed by SNS.

Incident:

»» An FBI Intelligence Analyst posted information on LinkedIn that cited his position as an Intelligence Analyst, his work on Russian and Chinese counterintelligence matters, and his specialities and abilities. His postings made him and the FBI susceptible to potential infiltration efforts by foreign counterintelligence officers and may have disclosed or compromised sensitive information.

Suggested Countermeasure:

»» Limit the amount of professional information that you post on SNS, and do not disclose that you are employed or associated with the FBI.

Incident:

»» The *CBS Early Show* reported on the "growing trend' of online auto fraud, detailing the case of Amanda Hanson, a woman with multiple sclerosis who had recently been a victim of a fraudulent online dealer. The dealer's website was made to appeal legitimate by using information from an actual dealership, American Auto Sales, and displaying both Carfax and Better Business Bureau logos. CBS noted, "In 2009 the FBI received more than 6800 consumer complaints about auto fraud. 4300 have already come in so far this year.

Suggested Countermeasure:

»» Verify the legitimacy of any website before providing personal and financial information to make a purchase.

Incident:

»» The wife or the new head of the British Intelligence Agency or MI6 caused a major security breach and left her family exposed after publishing photographs and personal details on Facebook.

Suggested Countermeasure:

»» Limit the amount of personal information you post on SNS, and do not disclose that you are employed or associated with the FBI.

Incident:

»» The FBI is warning parents to be on the lookout for predators who target children on popular SNS. Predator that used to lurk in chat rooms are now frequenting SNS such as Facebook and MySpace.

Suggested Countermeasure:

»» Monitor children’s use of the Internet and take advantage of parental control settings.

Incident:

»» Authorities have reported that criminals are hacking into Facebook and MySpace accounts and messaging the account holder’s friends to report that they have been robbed while vacationing abroad and need money to pay their hotel bills.

Suggested Countermeasure:

»» Verify the information before sending any money. Contact family or other friends of the alleged stranded victim to ensure that he or she is really on vacation in another country.

Conclusion:

»» SNS, webpages, email accounts, and wireless access points are all vulnerable to identity theft and information aggregation. Adversaries include hackers, foreign intelligence agents, terrorists, criminals and pedophiles. They target individuals and their family, friends, neighbors, and coworkers. According to the Bureau of Justice statistics, an estimated 8.6 million households had at lest one person 12 or older who was a victim of identity theft. The Federal Trade Commission estimates that as many as nine million Americans have their identities stolen each year.

»» FBI personnel should protect themselves and the FBI by limiting the amount of personal information posted on SNS. Monitor your children's use of SNS; know who they are talking to and what they are talking about and become familiar with the privacy settings on SNS. Remember that once you post information on the Internet, it will be there forever.

»» Malicious people need only a limited amount of personal information to steal or manipulate their victims' identities. For example, they can use the "Forgot Your Password" feature available on most SNS to gain access to many of their victim's online accounts. This feature typically requires the to answer three security questions before gaining access to the site. If the to these security questions cannot be found on the user's profile, then the perpetrator can use social engineering (via SNS chat) to contact the victim or his or her family members and solicit the desired information.

»» Don't become a victim; protect yourself and your family from online predators. Take advantage of the security and privacy settings on the sights you frequent most. Remember that the adversary is in search of an easy target to exploit.

»» For more information, contact the FBI Operational Security Support Staff.