Social Media Security Awareness for Business or Home Computing Users

- The purpose of all social media sites, whether for business or personal use, is communication, sharing, and sometimes collaboration.
- The benefits of the social networking model is that you can put out information you want others to have access to without having to direct that information to a specific individual at a specific time.
- Connecting yourself to others thru social media sites such as Facebook, Twitter, and Linkedin has advantages for the user in terms of staying in touch without much effort.
- Taking advantage of social media to stay connected means that you must know the risks that come with the noted ease of use, and how to protect yourself against bad actors who are interested in things other than your vacation pictures!
- Besides your friends, who else is looking at your information, and how might they be intending to use it!
- The purpose of this short module is to set forth the basic risks and defenses necessary to have a safer experience with social media networking.

**Defensive Computing**

**Be Aware of What Information is Public Thru Social Media**

- Social networking has grown in popularity since being adopted on a large scale in the late 1990’s. Internet users with a social network profile quadrupled between 2004 and 2008 and Facebook claimed a Billion users in 2012.
- Many people are interested in the information all of those users post. Many of those interested parties are not necessarily your friends!
- Identity thieves, scam artists, debt collectors, stalkers, and corporations looking for a market advantage are using social networks to gather information about consumers and competitors.
- Companies that operate social networks are themselves collecting a variety of data about their users, both to personalize the services for the users and to sell to advertisers.
- There are two kinds of information that can be gathered about a user from a social network: information that is shared and information gathered through electronic tracking.
- Once that information is provided and posted, it is going to be there essentially in perpetuity, unless some action is taken by the owner of the information (the user) to take it down.
- Information a user shares may include:
  - Photos, other media, age and gender information, biographical information such as employment history, hometown, and family history information.
  - Posted status updates such as travel, interests, activities.
- Embedded in this seemingly harmless information is a wealth of identity and activity information for a bad actor to mine.
  - Obvious profile information on name, address, age.
  - Relevant identity supporting information such as mother and father’s names, mother’s maiden name, pet’s names, where you like to vacation, when you like to vacation, restaurants you like to eat in, parks your children play in, etc..
• Some of the user Profile information is “hidden” from the public unless the user does not activate privacy settings correctly, or when the privacy settings get reset after an update.
• Social networks can, and do, change their privacy policy without the user’s permission, exposing information formally hidden unless the user understands the change and resets their preferred privacy level.
• Many users are not aware of how to maintain their privacy settings or just choose not to use them.
• Your “friends” may copy and post information from your site, which they had access to, on their own sites, without your permission, bypassing your privacy settings completely.
• You may have third party applications which store and expose some of your profile information which you thought was private.
• Social networks do not guarantee the privacy of their user data and have had numerous failures to protect information:
  o 2010 Facebook - exposure of personal chat logs of users.
  o 2012 Facebook - exposure of old private messages on the “walls” of European users.
  o 2012 LinkedIn - 6.5 million hashed passwords for the business focused social network LinkedIn were published on hacker forums.
• Social networks also benefit from your “public” information by which a profile of your interests may be made so as to direct customized ads to you. They encourage users to post more and more information and are successful in this encouragement!
  o Social networks also gather information thru electronic tracking using cookies to track information such as Websites visited and information associated with websites (ex: shopping cart items)
  o This information goes into a profile of their users which is further useful in their directed advertising

Know the Potential Risks of Social Network Exposure of Your Information

• Identity Theft
  o Identity thieves use an individual’s personal information to pretend to be you.
  o They use the information gathered from public posts, and public information in your profile.
  o They also use information gathered from “social engineering”, by “friending” a user and eliciting information thru messaging and chats over supposed common interests or common friends.
  o Illegitimate third party Apps may gather information from your private profile that you are not aware of thru confusing use statements which you may consent to. This information is used to bolster the false identity.
  o Attacks may also appear in the form of quizzes, questionnaires, or game links on friend sites that you visit that reveal personal information about you if you “play them”.
  o “Phishing” attempts, the offering of a “lure” to hook you into revealing personal information, such as the “fill out the form to qualify to win an iPod” are also a part of the identity theft fraud toolbox. If it seems to be too good, it probably is so don’t click the link!
• “Spear Phishing”, highly directed Phishing aimed at a particular individual, where you receive a legitimate looking message which asks you to click a link and enter your login and password on a site usually known to you, but “spoofed” or falsified in this fraud, tries to elicit your information by making you think you have an account problem or a false billing. Always check by other means directly with the account site. Don’t click the link!
  o Using the information gathered, they then can use the synthetic identity to impersonate you to an extent, the more information they gather, the better the impersonation.

• Introduction of Malware
  o Malware is malicious software that covers a wide range of programs intended to gather information or damage your computer’s software or operating system.
  o Malware can spread thru the social network from contact to contact, as the malware appears to come from a trusted contact, which induces people to download it.
  o Messages supposedly from a “trusted contact” may include malware links when directed to supposedly to view a file or video, which result in infection. Always be wary of unknown links.
  o A shortened URL on a status update, newsfeed, or blog link may lead the user to download a virus or go to a website that will attempt to download a virus to the user’s computer.
  o Email may appear to be from the social network itself asking for information, with a link to click. This is another form of Phishing attack. Always check directly with the site by other means to see if you are being “phished”.
  o Fake security alerts, with the virus posing as anti-virus, or anti-spyware software, offering to “help you” by clicking the link. Never accept an offer to give you free “anti-virus” help!

• Social Engineering Attacks
  o Several of the social engineering methods have been mentioned previously, as all of these fraud attempts have overlapping approaches.
  o Social engineering is the use of information known about a user to elicit additional information from the user. All of the fraudulent methods are part of social engineering.
  o “Phishing” and “Spear Fishing” mentioned previously are social engineering methods. They use a small amount of known information to elicit additional more valuable information.
  o “Misleading Solicitations” is the attempt to make people feel obligated to join a cause or a group because they receive email from a “friend” who has joined. The intent is to solicit the “registration information” from another user. If you are interested, check with the friend by other means, before signing up.
  o “Hijacked Accounts” is the use of compromised legitimate accounts after they are taken over by malware or spyware to defraud other users. The accounts are used to send out spam, malware links, or solicitations to the contacts and friends of the original account.
  o A classic example is the solicitation letter from your friend, “stuck in Honduras” and needing a wire transfer to buy a ticket home, after a robbery.

Avoiding Fraudulent Usage of Your Social Networking Information
o Use a strong password different from the passwords you use to access other sites.
o Never recycle your passwords as you change them periodically.
o Use information that others do not know about you in your security questions, and never post this information on your public information!
o It is best to not provide a work email to a social network. Consider using a specific new email account only for the social network. If the account is compromised, as in the case of the **Linked In** loss of millions of account registrations, your work account will not be compromised.
o Review the privacy policy and how to configure it before you sign up for the account. Make sure you know if there is a change in the privacy policy or terms of service.
o Only provide necessary information you are comfortable with revealing. Leaning to the side of less, is better.
o Never grant access to your contacts or email address book. The network may promise to connect you to people you know who are already on the network, but this exposes your contact list to the whole variety of frauds if it should be compromised. Some networks also use your list, if you do not prohibit them, to solicit your contacts to join.

- Be careful about clicking unknown links in messages from friends on social sites, particularly less well known friends. Links may be fraudulent paths to malware or social engineering attacks. Your friend may not be your friend if they are a stranger. Examine links for oddities, such as misspellings or odd phrasing in the message. If it seems odd, avoid it or check with the friend by other contact means before you “go there”.
- Don’t assume that a message is from who it seems to be from. Hackers break accounts and compromise contacts lists commonly. If you suspect a fraud, contact your friend by alternate means to see if they are compromised.
- Messages from the social network site will not be asking you to confirm personal information or passwords. Such a message is highly likely to be fraud. Do not click any links and report it to the site.
- Know what information you have posted about yourself. This information is the basis of fraud attacks and to help hackers access accounts thru the forgotten password approach. Pet names, Mother’s maiden name, first school, favorite hobby, are all common security questions. Think before you post.
- Don’t post vacation plans for the world to know when you are not going to be home! Physical robbery occurs too, not just cyber theft!
- Turn off geo tagging for your pictures so that the world does not know as much about your physical location.
- Don’t share all the details of your daily routine. Again, bad actors can be physical criminals, not just cyber criminals. Make sure your children understand what information not to share as they participate in social networking as well.
- Don’t make it easy for scammers by posting to the public part of your site your birthdate, age, phone number, and address. This identity information is a gift to scammers. If this information is required for registration, restrict it with your privacy settings.
- Type in the name of your social network link or use a personal bookmark when accessing thru the internet. Never click a link to your social networking site on someone else’s site. You may be giving your user ID and password information to a hacker when you do.
• Be selective about who you accept as “friends”. Identity thieves may create fake, but attractive profiles, to solicit personal information from you and your site. There is no reward for having the most “friends”! The safest strategy is to reject strangers. If you decide to accept a stranger, limit their access thru your privacy settings. Understand your social network’s privacy settings in detail. They are your best protection against scammers.

• Choose your social network carefully. Know the privacy policy and how to configure it. Find out and understand if the site monitors posted material, and what they do with it. You are providing personal information, so know what they are doing with it.

• Assume that everything you put up on the site is permanent and public. Consider if you would want the information on a billboard? The best assumption is that anything you post may become public information.

• Be careful of installing third party apps that let you do more with your site. They may be malware traps. Validate their authenticity and privacy policies carefully before you decide to use them. The best practice is to not use them at all.

• Discuss the risks of social networking with your children relating to home computing. Review their profiles, and postings. Help them configure their sites for proper privacy and to maintain them.

• Make sure they understand what personal information not to post. Make sure they understand what photos not to post, such as embarrassing shots or shots with identifiable location information, such as their house, and including sites away from home such as their school or a favorite playground.

• Make sure they know never to meet with someone they have met on line.

• If house rules are not followed, remove the child’s social site by contacting the social network.

• In the event you feel your account has been compromised, notify the social networking site immediately and alert your contacts. Malware may have been installed on your computer. While not a guarantee of safety, scan your computer immediately with up to date Anti-Virus software.

Useful Links

• Microsoft.Com Safety and Security Center
• Stay Safe Online.Org
• Windows Support-Security, Privacy, and Accounts