Week 4: October 25 - October 31, 2015
Social Media Safety

Social Networking Sites

Online Friendships Can Mean Offline Peril

One thing is for sure: people love the myriad number of social networking sites available. These sites boast hundreds of millions of registered users. But, as with just about any kind of cyberspace communication, there are risks involved. And you should know what they are.

What are social networking sites, exactly? They are websites that encourage people to post profiles of themselves—complete with pictures, interests, and even journals—so they can meet and connect with like-minded people. Most sites also offer messaging capability. Some of these sites restrict membership by age, but many are free.

So what's the problem? Unfortunately, these sites can be appealing to sexual predators, who seek to take advantage of easy and immediate access to information on potential victims, particularly child victims. Even worse, kids want to look cool, so they sometimes post suggestive photos of themselves on these sites.

How pervasive is the problem? Even with all the media attention on the dangers of social networking, the Federal Bureau of Investigation (FBI) still receives hundreds of complaints each year about children who have become victims of criminal incidents on social networks. These incidents of victimization include but are not limited to the following scenarios:

- An adult poses as a child in order to befriend a young victim online, and then later travels to abuse the child.
- An adult poses as a child and convinces the young victim to expose themselves and/or perform sexual acts over webcam, and later extorts the victim to perform additional acts.

Social networking sites encourage users to post a profile listing their age, gender, hobbies, and interests. While these profiles help kids connect and share common interests, individuals who want to victimize kids can use those online profiles to search for potential victims. Kids sometimes compete to see who has the greatest number of contacts and will add new people to their lists even if they do not know them in real life.

Children often don't realize that they cannot "take back" the online text and images they post. They may not know that individuals with access to this information can save and forward these postings to an unlimited number of users. Kids also may not realize the potential ramifications of their online activities. They can face consequences for posting harmful, explicit, dangerous, or demeaning information online, including being humiliated in front of their families and peers, suspended from school, charged criminally, and denied employment or entry into schools.

Be aware of the risks. Once a user posts information to a social networking site, that information is no longer private. The more information posted, the more vulnerable the user may become. Even when using high security settings, friends or websites may inadvertently leak a user's information.

Personal information shared on social networking sites can be used to conduct attacks against a user or their associates. The more information a user shares, the easier it is for someone to impersonate the user and trick one of their friends into sharing personal information, downloading malware, or providing access to restricted sites.

Cyber criminals craft very convincing spear phishing campaigns by leveraging information found on social media. Users should be conscious that information they post could be crafted into a targeting campaign, including spear phishing, which targets select groups of people according to something they have in common. For instance, a cyber criminal may target people who work at the same company, bank at the same financial institution, attend the same college, or order merchandise from the same website.

Predators, hackers, business competitors, and foreign state actors troll social networking sites looking for information or people to target for exploitation. Keep in mind that information gleaned from social networking sites may be used to design a specific attack that does not come by way of the social networking site.

What can you do to keep your children safe, especially if they are visiting social networking sites?

- Monitor your children's use of the Internet; keep your computer in an open, common area of the house.
- Employ two-factor authentication on sites that provide it for free, to avoid the theft of social media accounts or intrusion into those accounts (which means a loss of privacy related to any information that account holds).
- Tell your kids why it's so important not to disclose personal information online.
- Check your kids' profiles and what they post online.
- Read and follow the safety tips provided on the sites.
- Report inappropriate activity to the website or law enforcement immediately.
- Explain to your kids that once they post images online, they lose control of them and can never get them back.
- Only allow your kids to post photos or any type of personally identifying information on websites with your knowledge and consent.
- Instruct your kids to use privacy settings to restrict access to their profiles so only the individuals on their contact lists are able to view them.
- Remind kids to only add people they know in real life to their contact lists.
- Encourage kids to choose appropriate screen names or nicknames.
- Talk to your kids about creating strong passwords.

- Visit social networking sites with your kids, and exchange ideas about acceptable versus potentially risky sites.
- Ask your kids about the people they are communicating with online.
- Make it a rule with your kids that they can never give out personal information or meet anyone in person without your prior knowledge and consent. If you agree to a meeting between your child and someone they met online, talk to the parents or guardians of the other individual first and accompany your kids to the meeting in a public place.
- Encourage your kids to consider whether a message is harmful, dangerous, hurtful, or rude before posting or sending it online. Teach your kids not to respond to any rude or harassing remarks or messages that make them feel scared, uncomfortable, or confused, and to show you the messages instead.
- Keep in mind that most companies, banks, agencies, and other organizations don't request personal information via social media or e-mail. If in doubt, give them a call (but don't use the phone number contained in the message—that's usually phony as well).
- Use a phishing filter. Many of the latest web browsers have them built in or offer them as plug-ins.
- Never follow a link to a secure site from a social media message or e-mail. Always enter the URL manually.
- Educate yourself on the websites, software, and apps that your child uses.
- Don't forget cell phones! They often have almost all the functionality of a computer.