INVESTIGATOR TIPS

Social Networking Security Tips

Protect your information when being "social"

There are certain steps that every consumer can take to minimize the risks to their sensitive information when they participate in social networking. Here Kroll's Investigators offer tips consumers can use to be social more safely.

- **Use the website's security features.** Default settings generally offer no privacy. Explore the privacy settings available on the website and use them to control who gets to see the information you post.
- **Share personal information sparingly:**
  - **In your profile.** You don't have to fill in every blank in the profile just because the blank exists.
  - **On your wall or page.** Even with privacy settings employed, the best practice is to not post anything that you wouldn't say in public.
  - **Within third-party applications.** Some popular applications, like quizzes, ask for a lot of information about you, your life, and your interests. Before you provide information, think about how the answers you give can potentially be used elsewhere.
- **Consider how your friends' privacy settings can affect your privacy.** If your friends use less stringent privacy settings, then your information/photos might be seen by others to whom you are not connected.
- **Use caution when adding applications.** Some apps are vehicles for malware that can affect your computer or capture information. Refrain from downloading anything to your computer if you cannot verify the app's security or do not recognize the developer.
- **Understand social engineering attacks.** These attacks arrive in the form of a message that appears to be from a trusted contact. The message often contains a link to a site where you are asked to share information or to perform some other task. One attack relays a dramatic story about the need for money because the sender is stuck in a foreign country. Think before you respond to such an urgent message and try to reach the apparent sender to verify or dispel the story.
- **Don't be lulled into a false sense of security by the "nothing to hide" argument.** Seemingly innocuous bits of information can be combined by an identity thief to commit various fraudulent acts, such as taking over an existing credit card or bank account, hijacking your social networking or email account or opening new accounts.

MEM-063-2013-05-10