



## Social Networking Security Tips: Steps You Can Take Now to Protect Your Online Information

Are social networking and individual privacy mutually exclusive? It may seem that way – after all, the risk of identity theft through social networking can be high. Additionally, many sites are frequently in the midst of some type of privacy controversy, with individual consumer privacy hanging in the balance. And yet, for many people, social networking sites are significant because they keep us connected to family and friends, allow us to interact with others professionally, and enable us to tap into communities with similar interests and activities. How to keep the balance between convenience and privacy? Fortunately, there are certain steps that every consumer can take to minimize the risks to their sensitive information. Here the Investigators of the Fraud Solutions division of Kroll offer some tips and tactics consumers can use to interact safely on social networking websites.

- » **Use the website's security features.** Default settings generally offer no privacy. That's why it is important to thoroughly explore the privacy settings available on the website and use them to control who gets to see the information you post. Check these settings periodically, as they can be reset by site administrators if there is a change to the website.
- » **Share personal information sparingly:**
  - **In your profile** - You don't have to fill in every blank in the profile just because the blank exists. Sharing too much can increase your risk of falling victim to identity theft. If you are using the site to reconnect with friends or family, you will have to put a certain amount of information on the site so a long-lost someone can find you, but be prudent. If you are using a social networking site to interact only with certain people and aren't interested in being "found," don't include information like location, previous names, etc.
  - **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. Is the quiz asking for information typically used in security or challenge questions, as with a bank or credit card account? Identity thieves are known to sometimes collect bits and pieces of information through applications like this.
- » **Consider how your friends' privacy settings might affect your privacy.** Be aware that if your friends use privacy settings that are less stringent than yours, then your information/photos might be seen by others to whom you are not connected.
- » **Use caution when adding applications.** While you should be cautious with the information you provide within the application itself or to the company that's selling the app, there are other security considerations. 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 friend or organization. The message often contains a link to a site where you are asked to share information or to perform some other task. One attack that has gained notoriety relays a dramatic story about the need for money because the sender is stuck in a foreign country. Think about what you are reading before you respond to such an urgent message. You put your personal identifiers, your computer "health" and your money in jeopardy when you react before thinking about what might really be happening.



- » Don't be lulled into a false sense of security by the "nothing to hide" argument. Unfortunately, privacy in the digital age has little to do with hiding facts and more to do with protecting your information. Sometimes people don't realize that seemingly innocuous bits of information can be combined by a perpetrator of identity theft to commit a variety of fraudulent acts, such as taking over an existing credit card or bank account, hijacking your social networking or email account, opening new accounts, or committing crime under the guise of your personal identity.

You hold the primary responsibility for protecting your own information. The best way to protect it is not to post sensitive personal information and control who has access to what you do post to the extent that you can.