

Social Networking Security

Social networking websites such as Facebook and MySpace allow you to reconnect with old friends and make new ones. They allow you to share ideas and the events of your life with the people in your network. However, the ease with which people can obtain the personal information you make available can be cause for security concerns. If you use social networking sites, you can protect yourself by following a few simple guidelines.

Limit your available personal information

Be wary of making too much personal information available online. Online banking and e-commerce sites frequently use “challenge questions” to help you recover a forgotten password, or for other security purposes. Often, your online profile will contain enough information to answer these questions. If a hacker has access to this information, he may be able to break into your online banking account. In fact, some online quizzes are nothing more than veiled attempts to gather answers to challenge questions.

Use privacy settings to restrict who can access your information...

Most social networking websites provide a way to limit what information is available and who can see it. Familiarize yourself with how the privacy settings work, and set them to limit your exposure as much as possible. If your social networking website has no privacy settings, consider taking your online socializing elsewhere.

... But don't rely on them

E-commerce websites are held to a higher security standard than most other websites. Social networking sites have a spotty track record when it comes to protecting personal information. Even if your favorite website provides privacy settings, it may not enforce them as well as advertized.

Vary your password

Use a password for social networking websites that is different from the ones for your e-mail, e-commerce and financial websites. Ideally, you should use a different password on each website.

Know who you are “friending”

Consider refusing friend requests from people you don't know. They may be interested in more than your friendship.

Beware of following links

Links sent in messages sometimes lead to websites that distribute malware. Consider the source of the message: is it from someone who never sends you messages? Does the message sound like something your friend would send? If it looks suspicious, ask your friend if they really sent it. If they didn't, their computer may be infected with malware which actually sent you the message.

Talk to your kids about security

If you have children, talk to them frequently about how to remain safe online:

- Help your kids understand what information should be private.
- Explain that kids should post only information that you – and they – are comfortable with others seeing.
- Use privacy settings to restrict who can access and post on your child's social networking website.
- Remind your kids that once they post information online, they can't take it back.
- Tell your kids to trust their gut if they have suspicions. If they ever feel uncomfortable or threatened by anything online, encourage them to tell you.
- Consider using the social networking website your kids do, and become part of their network.