

Social networking websites like MySpace, Facebook, Twitter, and Windows Live Spaces are services people can use to connect with others to share information like photos, videos, and personal messages.

As the popularity of these social sites grows, so do the risks of using them. Hackers, spammers, virus writers, identity thieves, and other criminals follow the traffic.

Read these tips to help protect yourself when you use social networks:

- **Use caution when you click links that you receive in messages from your friends on your social website.** Treat links in messages on these sites as you would links in email messages.
- **Know what you've posted about yourself.** A common way that hackers break into financial or other accounts is by clicking the "Forgot your password?" link on the account login page. To break into your account, they search for the answers to your security questions, such as your birthday, home town, high school class, or mother's middle name. If the site allows, make up your own password questions, and don't draw them from material anyone could find with a quick search. For more information, visit these links:
 - [What was the name of your first pet?](#)
 - [What is screen scraping?](#)
 - [Take charge of your online reputation](#)
- **Don't trust that a message is really from who it says it's from.** Hackers can break into accounts and send messages that look like they're from your friends, but aren't. If you suspect that a message is fraudulent, use an alternate method to contact your friend to find out. This includes invitations to join new social networks.
- **To avoid giving away email addresses of your friends, do not allow social networking services to scan your email address book.** When you join a new social network, you might receive an offer to enter your email address and password to find out if your contacts are on the network. The site might use this information to send email messages to everyone in your contact list or even everyone you've ever sent an email message to with that email address. Social networking sites should explain that they're going to do this, but some do not.
- **Type the address of your social networking site directly into your browser or use your personal bookmarks.** If you click a link to your site through email or another website, you might be entering your account name and password into a fake site where your personal information could be stolen. Be selective about who you accept as a friend on a social network. Identity thieves might create fake profiles in order to get information from you.

- **Choose your social network carefully.** Evaluate the site that you plan to use and make sure you understand the privacy policy. Find out if the site monitors content that people post. You will be providing personal information to this website, so use the same criteria that you would to select a site where you enter your credit card.
- **Assume that everything you put on a social networking site is permanent.** Even if you can delete your account, anyone on the Internet can easily print photos or text or save images and videos to a computer.
- **Be careful about installing extras on your site.** Many social networking sites allow you to download third-party applications that let you do more with your personal page. Criminals sometimes use these applications to steal your personal information. To download and use third-party applications safely, take the same safety precautions that you take with any other program or file you download from the web.
- **Think twice before you use social networking sites at work.** For more information, see below.

Be careful with social networking sites, especially at work

Some employees have replaced the daily computer solitaire break with a daily check of Facebook, LinkedIn, Twitter, MySpace, Windows Live Spaces, or other favorite social networking site, many workplaces report.

Online social networking might be a more interactive distraction for employees than playing cards, but it's a lot more dangerous to the health of the corporate network.

Several recent reports attest that phishing scams, viruses, spyware, and other unwanted software are spreading through social networks and into workplace networks. These outbreaks can damage computer systems and might even steal sensitive information from your company.

Some workplaces block social networking Web sites, but because these sites can also be a valuable tool at work, you still might have access.

If you do, here are some ways to use that access more safely:

- Find out if your company has a policy about visiting certain Web sites using your corporate network.
- When you sign up for a social networking site, use your personal e-mail address, not your company e-mail address.

- Use caution when you click links that you receive in messages from your friends on your social networking site. Treat links in messages on these sites as you would links in e-mail messages.
- Be choosy about who you accept as a “friend” on a social network. Identity thieves may create fake profiles in order to glean information from you. This is known as social engineering.
- Be careful about the information you reveal about your workplace or company on your social networking site. (This is a good rule to follow for blogs too.)

Content provided by Microsoft Safety & Security Centre.