

## Staying safe online

Social networking websites like MySpace, Facebook, Twitter, and LinkedIn are all services that people can use to connect with others to share information. 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.

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

1. **Use caution when you click links** that you receive in messages from your connections. Treat links in messages on these sites as you would links in email messages.
2. **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.
3. **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 connections, but aren't. If you suspect that a message is fraudulent, use an alternate method to contact your connection to find out. This includes invitations to join new social/online networks.
4. **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.
5. **Always 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. This is known as phishing.

6. **Be selective about who you accept as a connection or friend.** Identity thieves might create fake profiles in order to get information from you.
7. **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.
8. **Assume that everything you put on a social/online networking site is permanent.** Even if you can delete your account, anyone on the Internet can easily print photos or text or save images, content and videos to a computer.
9. **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.
10. **Think twice before you use social networking sites on publicly shared computers.**
11. **Change your password regularly.** And make sure you use different passwords for each of your social networking tools.

## **Manage your reputation online**

If you use social networking sites, tweet or blog, you probably have a reputation online already, even if you don't know it. On the Internet, you create an image of yourself through the information you share in blogs, comments, tweets, snapshots, videos, and links. Others add their own opinions (good or bad) and contribute to your reputation.

Anyone can find this information and use it to make judgments about you. For example, recent research undertaken by Microsoft found that of the US hiring managers and job recruiters surveyed, 79 % routinely review online reputational information when considering job applicants. (This is increasingly the case in the UK also.) Most of them count online reputation as one of their top selection criteria. In fact, 70% of US hiring managers in the study have rejected candidates based on what they found. Top disqualifiers included unsuitable photos and videos, concerns about the applicant's lifestyle, and inappropriate comments.

## **Protect your online reputation**

- Act online in a manner that reflects the reputation you want to earn or maintain.
- Think before you share online. Think about what you are posting, who you are sharing it with, and how this will reflect on your reputation.
- Choose photos and videos thoughtfully, particularly those that might be provocative or make you look irresponsible.
- Talk with your friends about what you do and do not want shared. Ask them to remove anything you don't want disclosed.
- Treat others as you would like to be treated. Be civil in what you say and show on the Web.
- Respect the reputation and privacy of others when you post anything about them (including pictures) on your own pages, on others' pages, or on public sites.
- Stay vigilant. Sign up for personal alerts. Some search engines will automatically notify you of any new mention of your name or other personal info.
- Periodically reassess who has access to your pages. It's okay to remove those who no longer belong.

## **Polish your professional reputation**

- Publish the positive. To be your online best, create what you want others to see.
- Link anything you publish to your name.
- Consider separating professional and personal profiles. Use different e-mail addresses, screen names, blogs, and websites for each profile.
- Don't link your real name (or sensitive personal information such as your home address, phone numbers, or photos) with other profiles that you create.
- Add personal information to your professional profile judiciously and only as it reflects well on that image. Avoid cross references to personal sites.
- Look for Settings or Options to help you manage who can see your profile or photos, how people can search for you, who can comment, and how to block unwanted access.

## **Restore your online reputation**

- If you find information about yourself that does not fit the reputation you want, act quickly.
- In a respectful way, ask the person who posted it to remove it or correct an error.
- If the person does not respond or refuses to help, ask the website administrator to remove the digital damage.
- If you feel a public correction is necessary, present your case simply and politely.