

## Protect yourself in the online, social network community

(ARA) - More people than ever are taking part in social networking sites. Facebook alone has more than 500 million users, according to [Facebook statistics](#). People have a lot to lose if the security of their social networking site is compromised. Their own personal, identifying information, and the information of all those they network with, could be at risk.



In addition, wide usage of mobile devices increases the possibility of virus infection and provides a new gateway to hackers and malicious codes in spam mails and websites around the Internet. Introduction to voice messaging services also provides a new medium for virus infection and hacking of personal data.

"Cell phones and laptops are revolutionizing the way we communicate in today's society," says Lyman Munson, vice president of risk services at [Fireman's Fund Insurance Company](#). "It is imperative to protect your personal information when taking advantage of this wonderful, innovative technology." <http://www.firemansfund.com/individuals-families/welcome/Pages/welcome.aspx>

Here are some top recommendations to help protect yourself and ensure a secure online experience in the world of social networking:

- \* Don't accept pop-ups or prompts for software, unless you're armed with Web scanner software which checks each site for infections prior to access.
- \* Don't provide, post, or submit any confidential personal data (e.g. banking details, medical records, full birth dates, home town, birth place, social security number, etc.). Social networking sites don't require this sort of information to join.
- \* Do change your password at least once a month. Don't change it if you're prompted to. This could be a malicious link.
- \* Avoid letting friends, peers, co-workers or staff access their social networks on your computer, and don't sign into your networks on their machines. Others could introduce infections to your computer through unsafe practices, or your login security could be compromised via cookies saved on your computer.
- \* Never auto save your password information, and clear your history at least once a week.
- \* It's not smart to accept friend requests or request friends who you personally do not know - even if they are mutual friends of others you know.
- \* Talk online about your vacation, whereabouts, etc. after you've returned home, not before you leave. Otherwise, it can be an invitation to thieves to stop by your house while you are away.
- \* Frequently check your privacy settings. Changes in the website/social network may delete your settings, without you knowing. Understand and maintain your desired level of privacy.
- \* Mobile apps are extremely popular. Find out if companies you are a customer of provide applications for you to use that are secure, such as claims or policy information with your [insurance company](#).
- \* Take the time to learn how to use social network sites effectively. Each site has information on privacy settings and "how tos." Many sites help you with details on things such as setting up a variety of friends lists with varying privacy settings and avoiding relationship pitfalls, such as

[www.allfacebook.com](http://www.allfacebook.com).

\* Parents need to be mindful of children's activity and protect computer systems from predators.

\* Be mindful of what you say when responding or posting on your Facebook "wall." Remember, anything you say will be seen by all friends and those out of your control when commenting on a friend's wall.

\* Don't share files on your laptop or mobile device. When you connect at a wireless hotspot, anything that you are sharing on your computer or device may be shared with anyone else connected to that network. Disable the file and printer sharing feature or pick the correct network type on your laptop or mobile device.

\* Secure sites are best. Always look for the https:// and/or padlock symbol on your browser. Most browsers also allow you to hover over the site name to be sure that it is a verified web service.

\* Restrict what you do on Wi-Fi. Don't do anything on Wi-Fi that you wouldn't want to share with anyone else.

**Provided By:**

Fireman's Fund Insurance Company