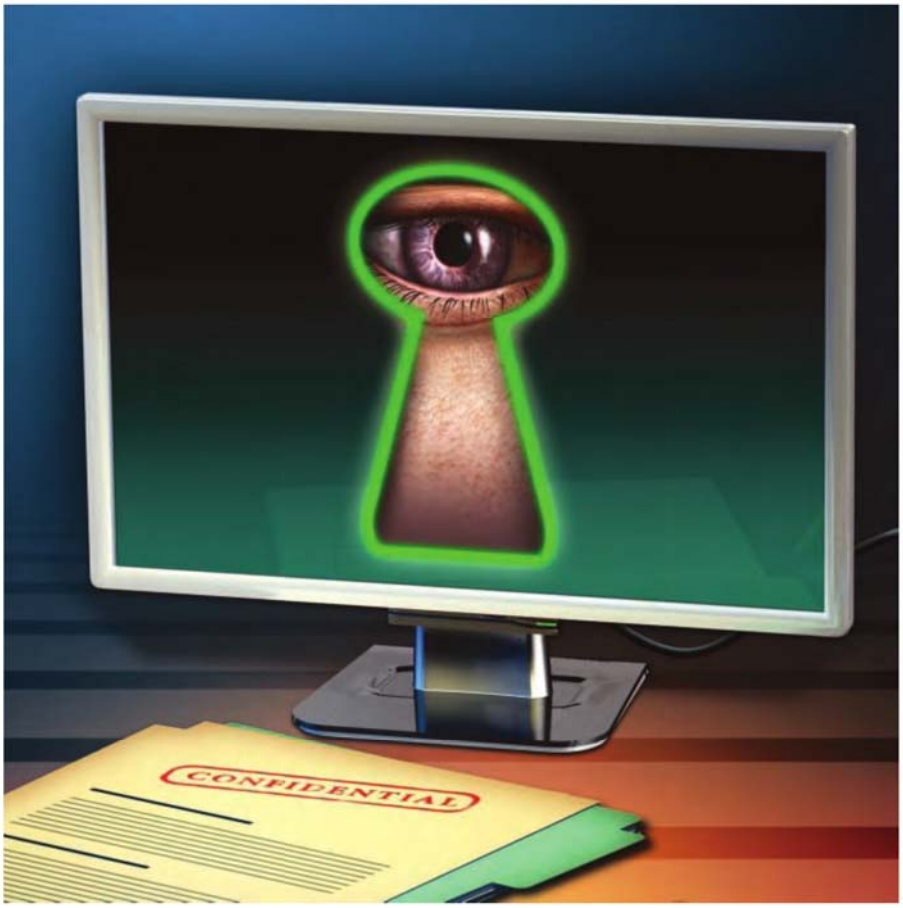
# Protecting Personal Information on Social Networking Sites

By David T. Gallant




*Protect yourself and your information with a few easy steps.*

Facebook boasts more than 500 million registered users around the world; over 700,000 local businesses have Facebook accounts.

I am an avid Facebook user myself, and like approximately 50% of the other users, I log on to my account every day to update my status, post pictures of family members, and see what's going on in the lives of my family and friends. I have been able to reconnect with people whom I have not seen or heard from (or even thought of) in years. I also use my account to promote my business.

But with all that in mind, let's not forget that there are folks on Facebook who may not be my "friends," but rather my "frenemies," and want to take advantage of all the information I provide.

I have taught security awareness seminars for years, and for years I have urged my audience to protect their personal information, not share it with those folks they do not know. Now, lo and behold, social networking sites abound, and everyone, including me, shares some personal information on the Internet with people they know (or believe they know).

**You have no control over what someone else does with your private information once you willingly give it to them.**

But as the adage goes, something is a secret (or private) only when one person knows about it. You have no control over what someone else does with your private information once you willingly give it to them.

Almost everyone uses social networking sites like Facebook, MySpace, and LinkedIn. Since Facebook is the most popular site in the history of the Internet, we will focus on how we can protect our personal information and how that extends to protecting the private information of others we are charged to protect.

## Hidden Hooks

Hackers, burglars, and identity thieves love Facebook because unsuspecting users willingly provide them with valuable information they can use against them. For example, during the account-creation process, you are required to provide a valid email address, as well as your full birthday, which you can choose to display on your profile page. If you are married or in a relationship with another Facebook user, you can link your account to that person's Facebook account. You can also link to the profiles of your mother, father, siblings, friends, coworkers, and groups—indeed to anyone else who has a Facebook account.

**Whatever you do on Facebook remains on your computer.**

So, a would-be identity thief or hacker now has your name, a general idea of where you live, your date of birth, family members' names, affiliations, interests, and other personal information you have posted.

What does a hacker do with that info?

One of the most commonly used security questions online banking accounts require is your mother's maiden name. Think someone can find it? How about your favorite pet's name—another common security question? You've linked your Facebook account to your mom's so the hacker knows who she is, and you've posted a photo of you with your dog and included your pet's name in the photo comments. It's all in your Facebook account. Hackers can use this information to try to make social engineering attacks against your work network.

By gleaning information from Facebook, they can masquerade as you and dupe an unsuspecting information technician into changing your password, sending them your protected information, or granting them physical access to your work network.

Oh, and Facebook has a new feature for mobile users. You can update your physical location and let your "frenemies" know exactly where you are. This is a pretty neat feature, but one you must use with caution. When you post on your status update that you and the family are enjoying a week in Barbados, burglars know it's a good time for a break-in.

## An Ounce of Protection

Does all this mean you should close your social networking accounts? Absolutely not. But you should protect yourself and your information. Here are a few basic tips.

1. **When setting up your Facebook account, use an email address from one of the free sites, such as Gmail or Yahoo.** Don't use the primary email address you use for work, banking, or any other financial site. If you have already set up your account with your primary email address, you can change it in the account settings area.
2. **Never display your entire birth date.** If you want to get those birthday wishes (and who doesn't), simply display the month and day. Keep in mind that even if you don't display your year of birth but belong to a "high school class of 1990" Facebook group, it is simple math to figure out your year of birth, too!
3. **Use the Facebook privacy settings to restrict who can see your profile information.** Do not set it so "everyone" can see your information. Limit your public profile information to the minimum data required to allow your true family and friends to find you by choosing the "Friends" or "Friends of Friends" settings.
4. **Don't become friends with just anyone.** If you don't know them, don't accept their friendship request. If in doubt, make them prove you know each other via email before you accept their friend request.
5. **Always use a strong password and change it frequently**—every 90 days or so.
6. **Be careful of the various applications associated with Facebook.** Many of them ask you for permission to access your personal information. Do you know what they are doing with it? Who else can gain access to it?
7. **Be watchful of changes in Facebook policies.** Security policies that are in effect today may change down the road.
8. **Ensure that your antivirus software is up-to-date.** Heed virus warnings. Viruses spread quickly via Facebook.
9. **Remember that whatever you do on Facebook remains on the computer you are using.** If you use a computer at work, you likely have no expectation of privacy about anything you post or say while using that computer. Make sure your district policy permits using social networking sites.

## User Beware

Facebook is a powerful tool to reconnect and stay connected to family and friends, but all that unprotected information in the hands of a criminal can have catastrophic ramifications. I will continue to use Facebook, but always with an eye toward protecting myself and my family, as well as the personal information under my care. You should as well.

**David T. Gallant** is president of Gallant Computer Investigative Services, LLC, in San Antonio, Texas.  Email: David@GallantCIS.com