



Social Networking Sites under Attack

Social networking sites like Facebook.com and MySpace.com have been used by students since their inception to connect to friends and meet new people. Though social networking sites have been incredibly successful, their popularity has made their users vulnerable, most recently to hackers and virtual scam artists. Since June 2006, the increasingly more common internet scam known as “phishing” has made its way to these sites. Phishing is the practice of using false Web sites to lure users into providing sensitive personal information.

In June 2006, it was reported that many users of the popular MySpace.com site fell victim to a phishing scam. Instant messages were sent to MySpace users that lured them into signing into a fake MySpace.com look-alike Web page. This page transmitted the personal information of these users to hackers who could then use the information to gain access to MySpace accounts and thus steal more personal information. Similarly, Orkut, a social site run by Google, became the victim of a worm that was running through its system collecting information from its users.

As the “stratospheric ascent” of social networking sites continues — market research firm ComScore Media Metrix reported huge gains in visitors to MySpace.com during the past year — incidences of identity theft and online scams may also be expected to rise. The many social benefits provided by these sites may be negated by the drawbacks if users are not careful about what information they divulge and how they access these sites.

The following are some tips for students who use these sites to keep themselves safe:

1. Check official Web sites for the published policies and practices on asking for personal information from clients. The Facebook.com officially states that they will never ask for users’ usernames or passwords through e-mail. If you see an e-mail asking for this information, it is most likely a phishing scam looking for victims who will respond with their personal information so that hackers can gain access to their accounts.
2. Make sure you have correctly typed in the URL of a social site before logging into your account. Many fake Web sites are set up using spellings similar to the official sites. The Washington Post reported that one man was sent to “MySpase.com” (as opposed to MySpace.com) but luckily realized this was a fake site before signing in (see article: <http://www.washingtonpost.com/wp-dyn/content/article/2006/07/15/AR2006071500119.html?sub=AR>)
3. Limit the amount of personal information you place in your profiles on these sites. Not everyone on social networking Web sites has positive intentions. Sexual harassment, “cyber-bullying,” identity theft, and other scams are just some of the risks of these sites. The most important thing you can do is make sure that you have protected yourself in as many ways as possible. If the information on your page is not something you would tell a perfect stranger on the street, why put it on the internet for the world to see?

As the phrase popularized by Spiderman goes, “With great power, comes great responsibility.” Use these sites freely to communicate and make new friends around the world, but just make sure you are safe in doing so.