

Social Networking — Protect Your Space

February 19, 2007

Summary Social Networking — Protect Your Space

Introduction

Social networking Web sites are among the fastest growing phenomena on the Internet. And it is tweens (kids 8-12) and teens (kids 13-18) who are driving that growth. Among the most popular social networking sites are MySpace, Friendster, Xanga, YouTube, and Facebook. All of them provide a place for kids to get together online with existing and new friends. When used cautiously, these sites are great ways for kids to communicate and share their experiences. When used carelessly, however, they can expose your children to identity theft and predators.

Tell us about yourself

All social networking Web sites entice kids to join, post personal profiles, pictures and, in some cases, video that can be accessed by their friends or, usually, anyone else who joins the Web site. For example, MySpace, the most popular of the sites, encourages kids to "Create Your Profile! Tell us about yourself, upload your pictures, and start adding friends to your network."

But don't tell too much

Your job as a parent is to make sure your children tell you before they join a site or create a profile, then ensure that their profile doesn't reveal too much about them. As MySpace advises in its "Safety Tips" -

"Don't forget that your profile and MySpace forums are public spaces. Don't post anything you wouldn't want the world to know (e.g., your phone number, address, IM screen name, or specific whereabouts). Avoid posting anything that would make it easy for a stranger to find you, such as where you hang out every day after school."

Privacy is a good policy

Make sure you know who has access to your child's information. Federal law requires social networking Web sites, like all Web sites, to post their privacy policy. You'll find a link to it on the home page, usually at the bottom. Make sure you read and understand who has access to your child's information before they post it. If your child is under 13, you will be asked to give your permission before the site can share your child's information. Also, you should know that children often lie about their age to gain access to these sites, and the sites themselves don't enforce their minimum age policies. So don't assume that just because your child is not yet 13 that they haven't joined a site. Failure to protect your child's

privacy may result in them receiving unwanted or objectionable email that may entice or trick them into giving out personal or financial information.

Hi, I'm Cindy, a friend of Bob's

Is she really Cindy? How much does Bob really know about her? Social networking sites allow members to create private networks that include only their friends. Problems occur when network members invite new friends to the network, especially "friends" that they have met only online. Even if your children are careful about who they invite into a private network, their friends may not be. Before responding to Cindy, they should ask Bob what he knows about Cindy. And you should make sure your children understand that the people they meet on a social networking site may not be who they say they are - and who they really are could be a predator.

A good rule is to not give out too much real information - including phone number, email address, home address, city or school - to anyone.

Beware of surveys

On social networking Web sites, kids are often asked to participate in opinion surveys. Many of these are harmless, asking questions about their favorite music or sports. Others are more probing and may ask inappropriate questions about dating or sex. Some may ask your child to provide personal information in order to participate in the survey. Set guidelines about surveys for your children. Ask them to tell you before they participate. Make sure they understand what personal information they should not reveal.

Protect passwords

Social networking sites allow users to protect their private networks with passwords. Problems may occur when a member of the private network passes along the password to new friends, including those they don't really know. That can give outsiders access to your child's personal conversations, information and pictures. Also, hackers recently have broken into personal networking sites and created fake popup windows that ask users to provide a name and password before they can access videos or profiles on the site. The hacker then uses that information either to hack into your computer or your child's online information. Remind your child that the purpose of a password is to protect themselves and their information. When they give it to someone they don't know or trust, they lose that protection.

Be informed

Whether your child is a tween or a teen, make sure you know where they go and what they do online. Ask them to show you any social networking site they want

to join or have joined. Ask them to show you their profile and who their network friends are. Read and understand the privacy policies of the sites they visit or join. And, again, remind them to not reveal too much about themselves. Today, socializing online is extremely popular among kids. With your involvement, direction, and supervision, it can be as safe as it is popular.

In This Article