The E-Informer

1/25/09 Jeffrey Kamovitch Vol 1.

Your Network is Social, Not Secure

Facebook, MySpace, Twitter- it can sometimes be hard to distinguish what is what between these websites, but one thing is for sure; social networks makes cyber-stalking easier than ever.

You can help by making sure your teen's social network profiles are clear of personal information, that the 'friends' they have are legitimate friends that they know well, and each networking site has a feature where they can set their profiles to 'private' so that any passer-by can't see their pictures, comments, or information.

Trust Only Those You Know

Online predators are common, and can be somewhat hard to detect. When instant messaging or participating in a chat room, unless you know the screen name of the person you're talking with, there's always a chance that they can have malicious intent.

To avoid the threat of an online predator, it may be best to avoid public chat rooms as much as possible.

Security…. Certified?

The problem about a professional website is that practically anyone can design one. You might not be able to immediately distinguish whether an e-store, for example, comes from a trustworthy business or if a scammer is waiting for money with no product in return.

The most distinguished way to ensure legitimacy of a website is a SSL (Secure Socket Layer), also known as a 'security certificate'. This little add on, which works by encrypting traffic to and from the user, prevents malicious attacks such as hackers to and from the website. These can be costly, and most scammers avoid these.

To know if a website has a security certificate, there will be a tray at the bottom of your browser that will show a small lock icon if an SSL Certificate is present. Also, if the url begins with **"https"** rather than **"http,"** that is also indicatory of a secure website.

More about SSL Certificates can be found at:

Piracy in Dangerous Waters

Pirating music isn't just illegal; it can be harmful to your computer. When using peer-to-peer software such as Limewire, it is easily to mistake a virus, hidden underneath the guise of nearly any given song.

Online piracy is already risky enough in the legal world, and even if your teen is lucky enough to pirate music without getting caught, a virus may be a little more stealthy than the police and work its way on to the computer and do damage that will require repair.

To avoid getting viruses from peer-to-peer software, it is best to stick to buying your music from a reputable program like Apple's iTunes or Microsoft's Zune software.

Newsletter Resources:

http://www.freepixels.com/Objects/Computers_and_Technology/pic983.html (used with permission)
http://www.facebook.com/help/?safety
http://www.wikihow.com/Avoid-Downloading-a-Virus-from-Limewire
http://info.ssl.com/article.aspx?id=10241
http://www.wiredsafety.org/safety/chat_safety/chatrooms/index.html