

## IM the Safe Way

February 19, 2007

### Summary IM the Safe Way

#### Introduction

This has probably happened to you at one time or another: Your computer goes "Ping! Ping! Ping!" while windows pop up on the screen with a string of text messages, as your kid hunches in her chair typing and chuckling. What is she up to? It's called instant messaging and it seems everyone's doing it these days. Instant messaging (also known as IM) lets families and friends chat online as quickly as they can type. To use IM, you need to have one of the popular free programs on your computer — such as AOL Instant Messenger (AIM), Yahoo Instant Messenger or Microsoft Messenger. Then choose a screen name like "soccermom123". Then you just need to get your friends' screen names and add them to your program's Buddy or Friends list (which works just like your email address or phone books).

When you open your IM program, you can see who on your Buddy or Friends list is currently online. To IM a friend, you simply click his or her screen name from your list, type up a quick message (never mind proper grammar when it comes to IMing), and hit Send. Your message pops up on your friend's computer screen faster than an email could travel across the Internet. Now you can chat back and forth. In fact, most IM programs also allow you to talk face-to-face using web cameras.

Convenient as it may be, however, IMing also comes with security risks. Whether you're contemplating joining the instant messaging crowd, or are already an avid IMer, here are a few hazards you — and your kids — need to beware of:

- **Spam/spim** Junk IMs, also known as spim are on the rise. These ads often contain inappropriate images (such as pornographic photos) that can suddenly pop up on your computer screen. Sometimes the messages appear to be from your bank or a contest, for example, but are actually from criminals, who are trying to con you into divulging personal and financial information.
- **Worms, viruses, Trojan horses** Just like with email, malicious programs can infect your IM program, too. If this happens, unbeknownst to you, infected IMs will be sent to those on your Buddy or Friends list. These viruses can make your IM program sluggish, crash your computer, or even take over your computer to surreptitiously use it for hacking or other illegal activities.
- **Predators** Kids are IM's No. 1 fans: 75% of American teens use IM, according to a 2005 report by the Pew Internet & American Life Project. But IM's very personal, one-to-one nature — and the fact that you can close an IM chat window and it's as if the conversation never existed — has attracted child

predators. Experts say these predator use IM to find new victims and try to lure them for offline meetings or to indecently expose themselves via web cams.

#### Safety and privacy tips

There's no cure-all for all IM hazards, but vigilance, common sense and a few basic safety tips can keep your family safe and connected, says Anne Collier, editor, executive director and founder of [NetFamilyNews.com](http://NetFamilyNews.com). To keep your family safe, here are her recommendations:

- 1. Block unwanted or unknown senders**  
Adjust your IM settings so that only those on your Buddy or Friends list can IM you. For example, in Yahoo! Messenger, in the main menu, click on Friends. Choose Edit Ignore List and then select the option: Ignore anyone not on my friends list. Or if you get suspicious or annoying IMs, you can block specific users using the same feature. In AIM, from the main menu you can select My Account Settings, click Privacy and then set the Contact Mode to Allow only users on my Buddy List.
- 2. Don't give out personal information**  
In general, make sure not to post your IM screen name online. It's also a good idea for your family to choose names that don't include personal details like "ZipCode94111" or "ChicagoGirl" or "WestmontHighCheerleader." Many IM programs allow you to create profiles, too. For extra privacy protection, your family should skip this option, or just don't include identifying information or photos.
- 3. Never reply to strangers**  
If you haven't changed your settings to only get IMs from people on your Buddy or Friends list — or you are using a public computer at a library or school — strangers can IM you. Whether an IM is a pornographic advertisement or an IM from someone who seems friendly or like an old friend, the rule is the same: Don't reply. Train your kids to turn off your IM program if this happens, and to tell you or another adult immediately if they receive a scary or disturbing message or image.
- 4. Don't click unsolicited links or attachments**  
Even if a web link appears to be from a friend, it could have been sent by a worm or other malicious program trying to infect your computer. So unless you just asked your friend to IM you a link to her favorite recipe site, for example, don't click any unsolicited links sent via IM. Also, avoid opening files attached to an IM as viruses can spread this way, too.

5. **Don't meet online pals offline**

Sometimes your kids will meet a friend elsewhere on the Internet, such as within an online community site. Then they might give out their IM screen name to have a private conversation. This is bad news and is often how predators find kids. So let your kids know that they should never give out their IM screen name to people they — and you — don't know personally. And they should never agree to meet someone they met online at an offline location. Unfortunately, the "13-year-old girl who also loves soccer," could really be a predator.

6. **Monitor your kids**

Set some house rules for how to use IM appropriately (like no bullying others or using foul language). Sure, kids want their privacy but IM, like your telephone, is a resource that most parents don't want to be abused. So get to know the screen names of your kids' friends. Put your computer in an area of your home which enables you to see if your children are having inappropriate conversations with people you don't know or if they are being harassed.

Also, watch out for trouble signs, such as if your daughter closes message windows quickly or switches screens when you walk in the room. Try to keep an eye out for suspect acronyms, such as POS (parent over shoulder). It's a good idea to allow younger kids to IM only under direct supervision.

Even though IM programs allow you to use webcams to chat face-to-face, this is a major safety issue when it comes to kids. It's simple: Never let kids use webcams without supervision.

7. **Talk to your kids**

Finally, let your kids know all the risks and steps they can take to IM safely. And keep the conversation going. Kids who talk openly about what they do while online are more likely to follow common-sense Internet safety precautions, according to experts. "Our job is to protect and educate first, and then trust that they'll make their own decisions online," Collier says. "You've got to talk to your kids to do that."