Instant messaging 101

Instant messaging is what kids do online more than anything else. There are many different kinds of instant messaging technology, and most are free. AIM (AOL's instant messenger free application) is the most popular, but MSN's free instant messenger application and Yahoo's free instant messenger application are also very popular.

IM is more like talking than e-mail is. You can do it while playing games, or doing homework or even while talking on the telephone to the same people you are IMing. Some kids IM certain kinds of things while talking about others in the same conversation. IMs are used to emphasize certain points, or to add additional thoughts or information.

Text messaging devices, like mobile phones and mobile text-messengers, are very popular with kids as well. They are used to chat, send messages and communicate with their friends and, increasingly, parents. Many schools have banned these devices, as kids have learned to use them to cheat on tests (IMing each other for the answers) or to pass messages in class.

Some of the newer applications allow voice IM, and photo or video IMs too.

Attachments, including malicious code and viruses, can be sent by IM too. And spam has moved over the IM, being renamed SPIM to differentiate it from its e-mail counterpart.

Most IM safety tips mirror e-mail and chat safety tips. Not sharing personal information with strangers, making sure you really know the person you are IMing, checking all attachments with an updated anti-virus program are all at the top of the lists. Knowing how to use the privacy and security settings for your IM application is essential, as well. Blocking any person who bothers you, or who sends you unwanted or inappropriate messages or attachments is very important. And blocking anyone not on your approved or buddy list is too.

Cyberbullying, cyberstalking and harassment often occur using IM applications. Trojan horse hacking and virus programs are often sent that way too. Since many screens are open at once, kids are not as careful when opening IMs as they are with e-mails.

When things go wrong, it's harder to trace an IM than an e-mail. They don't use the traditional headers used by e-mail applications, so spotting the IM source isn't easy. And finding who is behind the IM message is much harder with IM as well. Many e-mail accounts require a paid subscription and can be traced to the sender easily. IM accounts, like many free web-based e-mail accounts, can be opened by anyone and shut down as fast. No proof of who you really are is required. And, while chat rooms often receive the biggest blame for online sexual predators, in the U.S. at least most cases involve IM, not chat. That's why using a logging or monitoring product that will capture IMs is important in case anything goes wrong. Otherwise, the message is lost in the ether and taking any disciplinary actions or legal action is difficult, if not impossible.

Many kids use more than one IM application, since with the exception of Trillian, they only communicate with others using the same IM platform. And having eight or nine IM communications open at the same time isn't unusual at all, when kids are IMing. Because it is more like talking than writing, kids find themselves breaking the privacy and safety rules when using IM more than in other applications, except

chat. And IMing with strangers is much more dangerous than chatting with strangers. I always explain that most of us would prefer that our children are approached on a full playground, rather than one-on-one, if they encounter a sexual predator. There is strength and safety in groups. When approached one-to-one our children are often easier prey.

But banning IM is not an option. The kids would feel and be isolated if their friends communicate using IM. They wouldn't know what social events are planned and wouldn't be informed when everyone else learns about things. It's much better to screen out strangers and teach ourselves and others not to respond when a stranger sends an IM with "hi!" and tries to make us "guess" who they are. If they are really someone you know, they will find a way to let you know. Block and report any misuse as well.

The only way to monitor IMs and to capture them for any future reporting or prosecution needs is to use a monitoring software, like Spectorsoft.