



Web Security and Maintenance Services

## McAfee Security



# Privacy, Security & Virus Information

## Preventing Instant Messaging Crime

One of the newest developments in online communication, Instant messaging (IM) is the fastest and simplest way to communicate online with friends and coworkers. With this new technology come new ways for criminals to distribute worms, viruses, and Trojans into your computer's hard drive. Cybercrime has quickly become an easy way for criminals to hack into your computer and steal your personal information. Hackers like to use an IM clients because they can use network ports that are already open for the IM client – instead of having to open suspicious new ports.

In today's online world, multi-faceted attacks are launched through IM as frequently as they are through e-mail. Hackers like to exploit the operating system and browser vulnerabilities to send malware like Trojan keyloggers and screen scrapers that steal personal information. These hijacked computers turn PC's into 'zombies' used to commit crimes.

Using a man-in-the-middle attack, password-stealing Trojans allow criminals to pilfer a user's logon information and impersonate them. If the instant messaging protocols don't encrypt network traffic, the hacker can slip messages into an existing IM chat session and pretend to be the victim, causing embarrassment and the opportunity for fraud.

There are several rules that you can use to help keep you and your family safe from hackers when using Instant Messaging.

### Be Aware of Criminal's Tactics When Using Instant Messaging

By simply choosing names from an updated directory of buddy lists, cyber criminals exploit IM's user-friendly features. Every time their victim comes online, the cyber criminal will receive a notification on online status. The risks aren't quite finished. Transfer files and peer-to-peer file sharing are supported by Instant Messaging Services, making anyone who uses them vulnerable to malware hiding in files. With these weaknesses in mind, hackers use instant messaging to gain backdoor access to unprotected PCs that run P2P. In this example, a Trojan typically changes a computer's configuration settings to share all files on its hard drive, such as user id's logins, and passwords. Quicken files, banking information, chat information, e-mails, and other sensitive information can all be accessed through IM abuse. This can put the whole family at a great security risk.

Hacker's can also cause denials of service (DoS) on an instant messenger client by flooding a particular user with a large number of messages to crash or slow down their machine. Many IM software packages protect its clients against DoS attacks by allow the victim to block and ignore certain users. However, in the middle of an attack, it may be hard to get away from the flood of messages to ban the sender.

### Top 10 Ways to Defend Against IM Threats

It is easily possible for consumers to protect themselves from worms, Trojans, and viruses delivered through IM. It's easy to keep these threats away by following some of these simple rules:



Web Security and Maintenance Services

## McAfee Security



- 1. Choose a unique IM name with care.** Don't use your real name, e-mail address, or any other personal document that may identify your contact information.
- 2. Only allow people you trust to share your screen name,** and ask them to keep your name private. Only engage in conversation with people from your buddy list. To prevent 'spim' (IM spam), use the IM's different settings to block messages from people you don't know.
- 3. Try to refrain from revealing your screen name or e-mail address** if you plan to work at public internet stations. Some IM services link your screen name to your e-mail address when you login. Consider the possibility of setting up a second e-mail account if this is the case. Your e-mail address could become 'harvested' for phishing attacks.
- 4. While engaged in IM conversations, never give out your passwords** or private information like account numbers or credit card information. Network administrators can actually intercept unencrypted IM traffic. By installing an anti-virus software and firewall protection, you can prevent Trojans and viruses from entering your PC.
- 5. Install strong security software onto your computer** and make sure it is up-to-date as possible. The McAfee Internet Security Suite provides PC protection from all cyber crime including, virus protection, hacker prevention, and spyware. The McAfee Internet Security Suite also includes X-Ray for Windows – which detects and kills rootkits and other malicious applications that have the potential to hide from anti-virus programs. Its integrated anti-spyware, anti-virus, firewall, anti-phishing, anti-spam, and backup technologies work together to fight today's sophisticated, multi-pronged attacks.
- 6. Take the time to install your IM application correctly.** Do not allow it open automatically when you start your computer. If not using your computer, make sure you turn it off and disconnect the DSL or modem line when you're not using it.
- 7. Always allow automatic Windows Updates,** or download Microsoft updates regularly, to keep your PC protected against known vulnerabilities. Whenever other software manufacturers distribute further protection packages, install them immediately. These updates are designed to protect your computer from viruses.
- 8. Change your anti-virus software to scan all e-mail** and instant message attachment and downloaded files. Always refrain from opening attachments from people that you don't know. If you know the person who is the sender, contact them to figure out if the file is trustworthy. Beware of 'phishing' schemes – never click on links in e-mails or IM conversations.
- 9. Be wary when using P2P file-sharing with IM.** Trojans sit within file sharing programs waiting to be downloaded. Avoid files with the extensions .exe, .scr, .lnk, .bat, .vbs, .dll, .bin, and .cmd. Change your file settings to limit the folders that other users can access.



Web Security and Maintenance Services

## McAfee Security



**10. Be aware of your children's use of IM.** Take the time to monitor and limit your children's use of the IM. Locate your home computer in a high traffic, open area – and limit use of your computer at night time. The McAfee security software helps parents control the information and software that children can use.