



1. What is a keylogger? Keylogging programs silently copy the keystrokes of computer users and send that information to the crooks. These programs are often hidden inside other software that has been unwittingly downloaded and then infect the PC.

There are at least 12,000 such programs out there, and most computers have them.

2. The way keyloggers get you to unwittingly download their malicious software is to hide the software program in a what appears to be a legitimate program, graphic, music file tec., and then get you to come to the site through an email or instant message that 'makes sense'.
3. **80%** of all keyloggers are not detectable by Anti-Virus software, Anti-Spyware software or Firewalls (Australian Computer Response Team (ausCERT)).
4. Keyloggers have been embedded into the following attachments:
 - MP3 Files
 - Word Documents
 - Excel Documents
 - PowerPoint Documents
 - Email attachments
 - Executable programs and scripts such as games
5. You can get infected by a keylogger by clicking on "**ANY**" faked website link (Google, eBay, Amazon, AOL, Yahoo, etc).
6. You can get infected by a keylogger by clicking on any website picture, photograph or video if they have been subjected to malicious code.
7. An secure Web site or **SSL** session does not protect your keystrokes as you type, since when you type into a browser the keylogger is picking up your strokes.
8. Keyloggers can be pre-embedded onto devices that you plug into your computer. (McDonalds Japan unknowingly shipped infected MP3 devices in Summer 2006)
9. Fraudsters target popular websites i.e. (myspace.com) acting as teenagers to share infected files, with the goal of capturing the parents confidential information (banking passwords, credit card #'s, SSN's, etc).
10. Keyloggers can be purchased for home use at most software stores (e.g. Amazon.com), but there are over 12,000 keyloggers being shared on the internet today, and many are free.

It's no surprise that keyloggers are the hackers favorite tool!