

Keyloggers

Definition

A keylogger is a small software program that can sit on your computer and send anything you type to a third party. Keylogger programs circumvent encryption security. Instead of capturing information that has already been encrypted, the keylogger captures information as you type it. As an example, when you type in your credit card information for a purchase, such as your billing address, security code and actual credit card number, this information is easily captured and sent to a third party if a keylogger program exists on the computer you are using.

Interaction with keyloggers:

1) Public computers

Any public computers could have keyloggers installed without the administrators of the computers being aware of the threat. When you use one of these computers to perform some sensitive task, your bank information, debit / credit card info, papal info, etc. would be sent to an anonymous thief.

Solution:

To be safe, always assume any computer that is not your own has a keylogger installed and avoid performing any sensitive tasks that would be attractive to a thief.

2) Your personal computers

a) Other computers on your network: keyloggers can install onto your own personal computer through other computers that use your network. People in your office may connect to your network to send a quick e-mail, lookup information, or any other number of reasons. Guests at your house may use your Internet access. Any keylogger on these computers has a strong chance of moving to your computer.

Solution:

Establish a separate network for casual users in your office and for your guests at home, all while using only one Internet connection.

b) Internet scam or insecure software:

A **scam** leads you to click on something that allows the keylogger to download undetected. A scam can take the appearance of a legitimate computer alert. For example, you may receive an alert saying that you have a virus when, in fact, the alert may have been prompted by a web site you visited and clicking anywhere on that alert window, even the "close" button, would prompt a download of malware that could include a keylogger.

Solution:

Use the keyboard to close any of these windows instead of clicking. Closing a window with the keyboard can generally be done by pressing alt+f4 when the window is displayed.

Insecure software examples currently are two web browsers: Internet Explorer and Safari. If you use either of these programs, it is actually possible for a malicious third-party to install software on your computer without you doing anything other than browsing to a web site. You don't even have to click anything or download anything.

Solution: Upgrade to Opera or Firefox for your web browsing.

c) Lack of a good hardware firewall: this is not to be confused with software applications that are called "firewalls". Instead, these are physical devices that protect your computers from outside threats.

Solution: Firewalls from Cisco and Nortel offer the most robust protection.