

# Malware 101

Listed below is an overview of many different types of malicious software, or malware, on the Internet.

Type	Definition
Adware	Adware is a kind of spyware that generates annoying popup ads.
Drive by download	Malicious code that gets downloaded to your PC without your knowledge when you browse a malicious Website or a "legitimate" Website that's been compromised by a hacker.
Keystroke logger	A program or hardware device that records all keystrokes. They're often used by attackers to obtain passwords or personal information, such as bank account numbers.
Phishing	"Spoofed" e-mails and fraudulent Websites designed to fool you into divulging personal information.
Ransomware	A cyber-extortion scheme in which thieves use malware, like phony security programs, to take control of your computer and demand that you pay a ransom to regain control.
Scareware	A fake warning on your computer system that says you have viruses on your computer and that you need to buy this software to clean your PC. In this case, not only is the software going to disrupt your system, it's going to try and trick you into making a purchase using your credit card.
Spam	Unsolicited "junk" e-mail.
Spyware	Term for malicious software used to track your browsing habits, collect your personal information, or serve you ads.
Trojan horse program	A program that comes into your computer disguised as something else, such as a game or a screen saver. Many Trojans are also keystroke loggers.
Virus	A computer program that's designed to make copies of itself, usually without your knowledge. Usually requires user action to run, such as opening an e-mail attachment.
Virus Hoax	An intentionally deceptive e-mail warning about a nonexistent computer virus.
Worm	Malicious code that requires no specific action on your part to enable infection or to spread. Infects computers by traveling the network looking for devices that have a specific software bug or flaw (called a vulnerability).