A Guide To Understanding How Malware Attacks Your Computer

Whenever you connect to the Internet, read your email, or share files with others, you are at risk. Why? Because there are automated attacks against your computer. These attacks can come directly, or indirectly, by malicious software (or malware) designed to harm your computer.

Fortunately, you can protect yourself by taking a few simple precautions. But you need to understand the risks and how to avoid them.

Email Malware

How You Know

- May appear to come from someone you know or trick you into opening
- May not have symptoms of infection but may be silently gathering information
- Some may reduce performance or cause strange behaviors like a spontaneous reboot

What To Do

- Only open email attachments that come from a trusted source and that are expected
- Scan email attachments with Antivirus prior to opening
- Delete all unwanted messages without opening
- Keep security patches up to date

Email SPAM

- Spam is a serious security concern as it can be used to deliver Malware
- Messages that do not include your email address in the TO: or CC: fields are common forms of Spam
- Some Spam can contain offensive language or links to Web sites with inappropriate content

What To Do

- If you suspect an email is spam, do not respond, just delete it
- Consider disabling the email's preview pane and reading emails in plain text

Email Phishing

How You Know

- Requests for confidential information via email are not legitimate
- Phishing attacks may use scare tactics to entice a response
- Fraudulent emails are often not personalized
- Phishing attacks may consist of a group of emails that share similar properties like details in the header and footer

What To Do

- Be extremely wary of emails asking for confidential information
- Confirm the authenticity of a suspicious request before responding in email

Web Phishing

How You Know

- Fraudulent websites are used to steal personal information
- Phishing attacks re-direct victims to a bogus Web site where malicious code is downloaded and used to collect sensitive information

What To Do

- When visiting a website, type the address directly into the browser rather than following a link
- Only provide personal information on sites that have "https" in the web address or have a lock icon at bottom of the browser
- Do not provide personal information to any unsolicited requests for information
- Confirm authenticity of a Web site

Web Spyware

How You Know

- Many "free" programs downloaded from the web install software that tracks your behavior and displays unwanted advertisements
- Some web pages will attempt to install spyware when you visit their page

What To Do

- Allow only authorized programs to connect to the Web
- Do not accept or open suspicious error dialogs from within the browser
- Spyware may come as part of a "free deal" offer - Do not accept free deals

Internet Vulnerabilities

How You Know

- A vulnerability in the web browser may create a weakness in the computer security providing an opportunity for some websites to download malicious code

What To Do

- Install product updates and security patches before using the internet
- Keep web browser up to date with latest patches
- Make sure your computer is configured securely
- Automatically shield newly discovered security holes with your Antivirus software

Instant Messaging Malware

How You Know

- IM attachments, just like email attachments, can carry destructive viruses, Trojan horses, and worms
- Some new worms use IM software to send themselves to every member of your buddy list

What To Do

- Don't open attachments or click on Web links sent by someone you don't know
- Don't send files over IM

- If a person on your Buddy list is sending strange messages, files, or web site links, terminate your IM session
- Remove viruses from IM with your Antivirus software

Instant Messaging SPAM

How You Know

- Some Spam can contain offensive language or links to Web sites with inappropriate content

What To Do

- Reject all Instant Messages from persons who are not on your Buddy list
- Do not click on URL links within IM unless from a known source and expected

Instant Messaging Vulnerabilities

How You Know

- Most instant messages still travel unencrypted across the Internet, exposing private conversations to anyone who can find a way to listen in

What To Do

- Never send personal information through an IM
- Keep your IM software up to date
- Keep your operating system and security software up to date

File Sharing Malware

How You Know

- Malware may spread through common peer-to-peer file sharing applications by placing themselves in shared directories with enticing filenames
- Some Malware threats use peer-to-peer networks to communicate out from an infected system

What To Do

- Scan all files with an Internet Security solution before transferring them to your system
- Only transfer files from a well known source

- Use your Windows Firewall to block all unsolicited outbound communication

File Sharing Spyware

How You Know

- Some adware may be bundled with some "free" versions of popular file-sharing programs

What To Do

- Always read carefully the End User License agreement at Install time and cancel if other "programs" are being installed as part of the desired program

File Sharing Vulnerabilities

How You Know

- Personal information can be extracted from open connections during peer-to-peer connections

What To Do

- Make sure your computer is configured securely
- Use your Windows Firewall to block all unsolicited outbound communication
- Protect personal data by limiting the folders and files that can be shared on the peer-to-peer network

Use Virus Protection

Viruses, worms, and Trojan horses are programs created by hackers that use the Internet to infect vulnerable computers. Viruses and worms can replicate themselves from computer to computer, while Trojan horses enter a computer by hiding inside an apparently legitimate program, such as a screen saver. Destructive viruses, worms, and Trojan horses can erase information from your hard disk or completely disable your computer. Others don't cause direct damage, but worsen your computer's performance and stability.

Antivirus programs scan e-mail and other files on your computer for viruses, worms, and Trojan horses. If one is found, the antivirus program either quarantines (isolates) it or deletes it entirely before it damages your computer and files.

Windows does not have a built-in antivirus program, but your computer manufacturer might have installed one. Check Security Center to find out if your computer has antivirus protection. If not, go to the Microsoft Antivirus Partners webpage to find an antivirus program.

Because new viruses are identified every day, it's important to select an antivirus program with an automatic update capability. When the antivirus software is updated, it adds new viruses to

its list of viruses to check for, helping to protect your computer from new attacks. If the list of viruses is out of date, your computer is vulnerable to new threats. Updates usually require an annual subscription fee. Keep the subscription current to receive regular updates.

Use Spyware Protection

Spyware is software that can display advertisements, collect information about you, or change settings on your computer, generally without appropriately obtaining your consent. For example, spyware can install unwanted toolbars, links, or favorites in your web browser, change your default home page, or display pop-up ads frequently. Some spyware displays no symptoms that you can detect, but it secretly collects sensitive information, such as which websites you visit or text that you type. Most spyware is installed through free software that you download, but in some cases simply visiting a website results in a spyware infection.
