Internet Safety for Kids & Families

The Basics of Web Threats

Web Threats:

Web threats are malicious software programs such as spyware, adware, trojan horse programs, bots, viruses, or worms, etc. that are installed on your computer without your knowledge or permission. These programs utilize the Web to spread, hide, update themselves and send stolen data back to criminals. They can also be combined to do the crime — for example, a trojan can download spyware or a worm can be used to infect your computer with a bot.

Here are some basic definitions and safety tips for web threats:

Threat	Definition
Malware	A software program that is secretly placed on your computer to do unexpected or unauthorized, but always malicious actions.
Virus	A program that can copy itself and, like real-life viruses, spread quickly. Viruses are designed to damage your computer, display unexpected messages or images, destroy files, reformat your hard drive, or take up storage space and memory in your computer which may slow it down.
Worm	A self-contained program that can spread copies of itself to other computer systems through network connections, email attachments, instant messages (via file-sharing applications), and by working with other malware. Worms may block you from accessing certain web sites or steal the licenses for applications you have installed on your computer.
Trojan Horse	A program that performs a malicious action but cannot replicate itself. It may arrive as a harmless file or application with hidden, malicious code. When it is executed, you may experience unwanted system problems and might sometimes lose information from your computer.
Spam	Any message sent by email or instant message (IM) that you did not request and—is designed to make money for the sender.
Phishing	Any attempt by phone, email, instant message, or fax to get your personal information in order to steal your identity (and your money). Most phishing attempts look like they are designed for a legitimate purpose, but they are actually intended to be used for criminal activity.
Pharming	The act of hijacking legitimate website addresses or URLs – e.g. "www.mybank.com" – to redirect you to a fake website that looks like the original. The spoofed website secretly collects your personal information after you enter it, and could be used for any number of criminal activities.
Spyware	Software that is installed or executed on your computer (without your knowledge) that monitors, tracks, and reports your electronic movements to the spyware author. It is usually installed on computers through Trojans or as part of legitimate software that you choose to download and install. Spyware collects information using the following: • Keyloggers – software that tracks keyboard strokes for the purposes of logging the Web sites consumers visit, or for recording passwords • Screen-capture technologies – software that periodically gathers screen shots of a desktop and can record information such as login names • Event loggers – software that tracks the Web sites consumers visit or other online behaviors . (The information is generally used for targeting future ads to a user).
Adware	A piece of software that delivers advertisements – such as pop-ups or Web links – to you without your permission. It is usually installed secretly through Trojans or as part of legitimate software that you choose to download and install. Adware can display highly-targeted ads based on data collected by spyware that was already on your computer that tracked your Internet surfing habits.
Bots and Botnets	Short for robots, these are small programs placed secretly on your computer through a Trojan. A criminal "botmaster" can control several bots from a central location, at any time to distribute spam, conduct phishing, or perform a denial of service (DoS) attack and bring down a website so that it cannot be accessed. Botnets are networks of bots. They are typically used to distribute spam and phishing attacks.
Ransomware	Software that encrypts documents for the purposes of extortion. Documents are held ransom until victims buy a decryption key – either by sending payment through a third-party like PayPal, or buying an item online (the receipt includes the key).

Below are some Internet security tips to keep your computer and your family safe from web threats:

General security tips

1. Always keep your security software working and up-to-date. Especially if you use a laptop on unprotected wireless networks in airports, cafes and other locations.
2. Install products and solutions that protect you whether you're surfing the Internet or downloading files directly to your computer. Ensure that Web protection software extends beyond email protection to encompass peer-to-peer networks and the entire range of home computing applications, and can provide warnings about traffic that is incoming and outgoing from your computer in real-time.
3. Employ the latest technologies, such as Web reputation, which can measure the trustworthiness and safety of a Website before you visit it. Use Web reputation technology combined with existing URL filtering and content scanning technologies.
4. Use the latest Web browser version and install security patches when available. Use a web browser that has a no-script plug-in.
5. Check with your Internet Service Provider to see what kind of protection is offered by their network.
6. If you use the Microsoft Windows operating system, enable the "Automatic Update" feature and apply new updates as soon as they are available.
7. Always install, update, and maintain firewalls and intrusion detection software, including those that provide malware/spyware security.

For email

1. Always make sure you are using an anti-spam product for each email address you have.
2. Beware of unexpected or strange-looking emails, regardless of who the sender is. Never open attachments or click on links in these emails.
3. Report suspicious emails to the appropriate authorities.
4. If you trust the sender of the email, scan their email attachments with a security solution before opening them. If they send you a URL and it is short enough, type the URL in your web browser instead of clicking on it from the email.
5. Be alert when receiving emails that request account details (financial institutions almost never request financial details in emails).
6. Never email financial information to **anyone**.

For web surfing and downloading online programs

1. Use a Web reputation service to make sure the website you are going to visit is safe from web threats.
2. Beware of Web pages that require software installation. Scan all programs downloaded from the Internet with an up-to-date security solution.
3. Always read the End User License Agreement and cancel the installation process if other "programs" are going to be installed in addition to the desired program.
4. Do not provide personal information to unsolicited requests for information. Only provide personal information on sites that display a lock icon at the bottom of your browser.

Childnet International commonsense media ConnectSafely Smart Socializing Starts Here™ TREND MICRO™