

How to Protect Yourself from Malware and Phishing

Phishing

This information is intended to help you protect yourself from a fraudulent form of spam called [phishing](#).

A definition of phishing

- **Phishing** is a prevalent online criminal activity involving **fraudulent e-mail messages** sent in an attempt to obtain your online account information such as **credit card and banking information**. Once phishers have your account information, they might use it to steal your identity or make purchases on your account.

Recognizing phishing

- Phishing e-mails typically purport to be from a **financial institution** such as a bank, credit card company or online payment service. They typically feature **authentic-looking logos** that appear to originate from organizations such as eBay, PayPal, Bank of America, Wells Fargo, TCF Bank, etc.
- Phishing e-mails are usually written under the guise of "**protecting**" you by asking for "**confirmation**" or "**verification**" of personal and/or account information. Providing that information could subject your account to unauthorized access. As the [Federal Trade Commission](#) points out, legitimate businesses don't ask for personal or financial information via e-mail.

Protecting yourself from phishing

- **Never respond** to e-mails that request your personal/account information.
- If the e-mail appears to have been sent from an organization you are affiliated with and you want to look into it further, check for information on that organization's official Web site.

Important: Check the legitimacy of the Web site listed in the phishing e-mail by typing the www-address directly into your browser or call the organization directly. Do NOT click on links in the suspect e-mail.

- Do not call a phone number listed in an e-mail you suspect is phishing. Look up that organization's actual phone number in the phone book or from your official documents.
- Delete e-mails that ask for account or financial information.

Phishing feeds on fear

Why do people get hooked by one of these phishing expeditions? Something called social engineering plays a big role. Consider these scenarios:

- You hear multiple news reports of identity theft, and as a result you are on the alert for anything indicating your own personal information might be at risk of being stolen.

With this heightened level of awareness about the need to protect your personal information, you might more easily fall prey to an e-mail that appears to come from a financial institution you have done business with, especially when the message is asking for "verification" to protect you from the very fraud it is committing. Combine this with a sense of urgency the message reflects in wording such as "...your account with us will be terminated if you don't respond within 24 hours," and it's easy to see why people get hooked.

Understanding Spyware

Spyware, also called adware, is software that is hidden on your computer that gathers personal information about you and your Internet use habits. The software then relays it to advertisers, sponsors and others. Spyware programs also run in the background and can consume significant amounts of memory and cpu. Thus the applications you need to use may not perform at their best.

It is important to understand that not all software that uses ads should be classified as spyware or adware. Some programs use ads and banners as a means to pay for the development of the software and to keep it low-cost or free. If all a program does is rotate ads it may very well be legitimate. It is the software that goes further and is more intrusive that is really spyware.

How Spyware Affects your Computer

Some typical signs of spyware include:

- Computer instability - Slows down or hangs
- Random strange behaviors
- Slow network/Internet performance - even when other users are working just fine
- Advertising popups (including porn) - even when you are not actively surfing the Internet
- New toolbars appear in your browser
- Your browser opens to a different 'home' page on startup

How Spyware gets on your Computer

Most spyware is installed onto your computer without your knowledge and in some cases even without your consent. This typically happens when you install free or shareware programs downloaded from the Internet. Peer-to-peer (P2P) software (like KaZaa or Gnutella), weather monitoring software and even some toolbars are frequent sources of hidden spyware. For the most part, the fine print of license agreements includes information about the spyware that will be installed along with their product, but not always.

Spyware can also get installed when you click on unknown links in e-mails or on some unsavory Web sites. The link may open a Web site that attempts to install spyware onto your computer. This typically is a browser hijacker at work. Browser hijackers can be especially dangerous if hidden from your view. Browser hijackers will change your 'home' page location and even where your search attempts go no matter how many times you reset it back to your own settings. These attacks can range from minor inconvenience of popups to major violations of your privacy. Additionally, some use Internet Explorer to trick users into installing the latest and greatest software from a company via a popup request to install software.

Removing Spyware Already on your Computer

Most spyware is hidden and is difficult to remove without assistance of a removal tool. Antivirus software typically does not detect or remove spyware. A good common practice is to use antivirus software and additionally run a spyware removal tool on a regular basis.

The two recommended tools that can be used to remove spyware are Lavasoft's Ad-Aware and Spybot Search & Destroy. It is recommended that everyone, even if you have not installed suspicious software, use these tools to scan their computer for Spyware on a regular basis.

Lavasoft's Ad-Aware

Available for download at <http://www.lavasoftusa.com/support/download/>

Spybot Search & Destroy

Available for download at <http://www.safer-networking.org/index.php?page=download>.

*****NOTE:** Both Ad-Aware and Search & Destroy use definition files similar to antivirus software. It is important that you have the program check for updates prior to running your scans for spyware.

Avoid being a target for Spyware

There are some simple common sense ways to avoid being a target of spyware. Below are some simple measures you can take to help protect yourself.

- Free software often comes with spyware. While there are very legitimate free software programs out there, make sure you trust the location you download from and are careful not to install free or shareware software from untrusted Internet locations. P2P programs such as KaZaA are notorious for installing spyware as are those such as Bonzi Buddy. In any case it is a good practice to run a spyware removal tool after installing any software downloaded from the Internet.
- If you use Internet Explorer, be careful not to allow just any site to install software on your computer via a popup. These use what are called Active X components. They can be useful when a site requires flash or shockwave installed in order to view the site, but these popups are also

another source of spyware. If a popup appears asking you to install software while surfing the Internet, say no unless you are very sure you need the software to view the site.

- Avoid surfing sites where many spyware installers do business. These sites include illegal software sites, adult sites and sites about hacking or cracking. Many of these sites will attempt to plant spyware or adware on your computer.
- Regardless of how careful you are, you should still run a spyware scanning and removal utility on a regular basis. Make sure you keep the definitions up-to-date. Use personal firewall software on your computer along with antivirus software. The combination of these things will help keep your computer clean and protect your privacy.