Malware – What Is It and How To Avoid It

CONSUMER ALERT

BILL SCHUETTE
ATTORNEY GENERAL

The Attorney General provides Consumer Alerts to inform the public of unfair, misleading, or deceptive business practices, and to provide information and guidance on other issues of concern. Consumer Alerts are not legal advice, legal authority, or a binding legal opinion from the Department of Attorney General.

Malware – What Is It and How To Avoid It

Scam artists and criminals can sit anywhere in the world and target computers and smart phones. Unfortunately, there are a seemingly infinite number of ways you may encounter malware. Because of this, it is difficult to provide information on how to handle each and every situation you might experience. However, understanding more about malware and what to watch out for is a good first step in limiting the heartache malware can cause.

What is Malware?

"Malware" is a broad term that refers to malicious software. This software can take many forms including viruses and spyware. Depending on the purpose of the malicious software, it may simply be a nuisance causing your computer or device to repeatedly crash. Malware could also be a type of spyware designed to monitor computer use, steal personal information, or commit other types of fraud. With the emergence of smart phones and other web enabled devices, personal computers are no longer the only targets. Malware can also infect phones, tablets, and other mobile devices.

How to Avoid Malware?

E-mail has made a lot of things easier. You can send pictures, documents, and links to others in the blink of an eye. This also means scam artists and criminals can send you malware quickly, easily, and cheaply through e-mail. Sometimes, scam artists design innocent looking e-mails promising to link to a funny story or viral video. It may even look like it is from someone you know. Other times, scam artists may try to use fear, intimidation, or sorrow. They create official looking e-mails to trick people to download malware. Because scam artists seem to develop new scams daily, it is difficult to compile a list of every scam e-mail. However, two types of official looking e-mail scams seem to be common and effective.

Scam artists send e-mails claiming to be from a court. It states that you have been summoned to appear for a hearing. The e-mail often contains a link or an attachment that promises to provide further information. Unfortunately, clicking on the link or attachment can download malware onto your computer or device. More information from the FTC about this specific scam can be found here.[1]

Scam artists have also been sending e-mails claiming to be funeral homes. The e-mail appears to provide information about a funeral service. Similar to the scam above, the e-mail will contain a link or an attachment that promises to provide further information. Instead, clicking on the link results in malware

[1] http://www.consumer.ftc.gov/blog/its-not-your-day-court

being downloaded onto your computer. More information from the FTC about this specific scam can be found here.[2]

Besides staying abreast of the current or popular scams, following these tips can also help avoid malware problems..

- **Be cautious about opening any attachment or downloading *any* file from e-mails** you receive, regardless who sent them. These files can contain viruses or other software that can weaken your computer's security.

- **If you get an e-mail or pop-up message that asks for personal or financial information, do not reply. And don't click on the link in the message, either.** Legitimate companies don't ask for this information via e-mail.

- **If you receive an e-mail from a familiar online merchant, make sure that before opening, you compare the order number in the subject line of the e-mail to the receipt you printed from the merchant's website when you completed your order.** Also, look for a digital signature. If the order number in the subject line does not match the order number on your receipt, do not open the e-mail! Delete it immediately.

- **If you are concerned about unauthorized activity in your account, contact the organization mentioned in the e-mail using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself.** Don't cut and paste the link from the message into your Internet browser - phishers can make links look like they lead to a familiar Web page when in reality they point to a fraudulent look-alike site.

- **Install protective anti-virus, anti-spyware, and firewall software, and keep them up-to-date.** Some phishing e-mails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes both current and older viruses, can effectively reverse the damage, and updates automatically.

  A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Operating systems or browsers also may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

- **Check your browser (Firefox, Internet Explorer, Chrome, Opera, Safari, etc.) to see if it has anti-phishing features**. Such features may include a toolbar that compares websites you attempt to visit with known phishing sites.

- **Don't e-mail personal or financial information.** E-mail is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "httpS://" (the "s" stands for

[2] http://www.consumer.ftc.gov/blog/fake-funeral-notice-can-be-deadly-your-computer

"secure"). Unfortunately, no indicator is foolproof; some phishers have forged ("spoofed") security icons and "https" sites.

- **Backup, Backup, Backup.** Regularly backup your files and keep these backups in an offline location that is not connected to the internet. This will help protect you if you lose access to your data due to malware.

More information about malware and protecting yourself can be found at http://www.onguardonline.gov/articles/0011-malware. For additional information about fraudulent e-mails, please see “Fraudulent E-mail Thieves Intend to Steal Your Personal Information” located here: http://www.michigan.gov/ag/0,4534,7-164-17337_20942-151331--,00.html

Contact The Attorney General’s Consumer Protection Division

Consumers may contact the Attorney General's Consumer Protection Division at:

Consumer Protection Division
P.O. Box 30213
Lansing, MI 48909
517-373-1140
Fax: 517-241-3771
Toll free: 877-765-8388
www.michigan.gov/ag (online complaint form)