Computer Malware and Phishing Schemes

The Office of the
Minnesota Attorney General
helping people afford their lives and live with dignity and respect

"Phishing" is a scam where thieves attempt to steal personal or financial account information by sending deceptive electronic messages that trick unsuspecting consumers into disclosing personal information. The "bait" may be an email, instant message, or pop-up window in which the sender impersonates a bank or other financial institution, government agency, Internet service provider, or other company. In the past, phishing scams typically directed consumers to a website address linked in the message to verify personal information such as name, bank account number, password, credit card number, ATM PIN number, Social Security number, or home address.

New Bait, Same Scam

Just as fishing lures used to catch fish have grown more sophisticated, so have techniques used to perpetrate phishing. Increasingly, phishing emails do more than just impersonate a bank in the effort to steal consumers' information. Thieves may send a spam email message, instant message, or pop-up message that infects the consumer's PC with spyware or ransomware and gives control of it to the thief. A spam message may infect your computer when you click a link or picture in the spam message, or when you open an attachment to a spam message. If your PC is poorly secured, it may be infected as soon as you open the spam message itself.

Phishing messages are usually provocative. They may attempt to make you irritated, curious, or amused— anything to get you to open the email, click the link, and silently infect your computer! Once your computer is infected, the malicious spyware can lurk there until it finds and sends to the thief your financial and personal information, such as bank account numbers, credit card numbers, or ATM PIN numbers. Infected PCs often become one in a "bot" network of compromised computers used by the scammer (or leased for use of other scammers) to send spam email or to attack other Internet-connected computers.

The Minnesota Attorney General's Office warns Minnesota consumers and businesses to beware of malicious spam emails, instant messages, and pop-up windows designed to steal personal information.

What is Spyware?

Spyware is software that installs itself and sends information from your computer to others without your knowledge or consent. While some spyware programs merely track your web surfing habits in hopes of learning your product preferences for marketing purposes, spyware can also be used by technology-savvy criminals to steal personal and financial information. Modern thieves may use spyware programs, such as "key loggers," system monitors, and trojans to send keystrokes or pictures of your computer's monitor to the thieves in the hope of snagging account numbers, passwords, Social Security numbers, or other confidential information that can be used to steal from you or impersonate you in committing other scams.

What is Ransomware?

Ransomware is software that installs itself on your system and blocks access to data until a ransom is paid to unlock it. Some ransomware encrypts your files, making them inaccessible. You are then coerced to pay for the ransomware to be removed, usually through a difficult to trace payment method such as wire transfer or bitcoin. Often, however, even paying the ransom does not guarantee that you will be able to regain access to your data.

Most Computers are Vulnerable

Studies have found that up to 90 percent of U.S. home computers have been infected with spyware at some time. Unless you are confident that your computer is secured against these hazards, you should not open spam email or click on attachments, images, or links in email messages, instant messages, or pop-up messages.

Protect Yourself

The Minnesota Attorney General's Office urges consumers not to open spam email, or click on attachments, images, or links in email messages, instant messages, and pop-up messages. Unless you have secured your personal computer, spyware can infect it. Instead, delete spam messages without opening them.

You should never click on links or pictures in spam messages, even to unsubscribe. If you never asked to subscribe to a particular organization's messages, but receive a message from that organization, it is possible that a spammer is impersonating that organization, and that clicking on the link to "unsubscribe" may infect your computer. You are safest just deleting these messages without opening them. Email or instant messages from friends' computers can be malicious if that computer has been successfully attacked and is sending spam. If you are not expecting a message with links, images, or attachments, it is safer to call the sender to see if the message is genuine.

For more information on identity theft or other consumer issues, contact the Minnesota Attorney General's Office as follows:

Office of Minnesota Attorney General Keith Ellison
445 Minnesota Street, Suite 1400
St. Paul, MN 55101
(651) 296-3353 (Twin Cities Calling Area)
(800) 657-3787 (Outside the Twin Cities)
(800) 627-3529 (Minnesota Relay)
www.ag.state.mn.us

Additional Tips

1. Keep your computer updated. The operating systems of personal computers and the Internet-connected software (like email programs, web browsers, and music players) should be updated regularly with "critical" security patches.
2. Install a firewall and antivirus software, and keep them up to date.
3. Use anti-spyware programs. There are a variety of reputable anti-spyware products available for free or for a free trial period. Do your research before installing an anti–spyware program. There are many fake programs that may actually infect, rather than clean, your computer.
4. Install pop-up blocking software. If your favorite browser does not have pop-up blocking features, you might also obtain a free pop-up blocking browser toolbar, which is available from some search engines.
5. Make sure the security settings on your Internet-connected applications are strong. Instant messaging settings should prevent unknown persons from sending malicious content, and your search engine (such as Google or Yahoo) can be set such that you do not receive inappropriate or risky search results. Email may be adjusted to receive "text" only, and not "active" content or images, which can be malicious.
6. Don't download free software unless you know and trust the source of the software. Free games, toys, file-sharing applications, and other software can be appealing, but may be bundled with unwanted spyware. Read vendors' privacy policies and end-user license agreements (EULAs) before downloading free software. If these are hard to understand or locate, think twice about installing that software.