Scams Targeting Computer Owners

From the Office of Minnesota Attorney General Lori Swanson

By some estimates, over 85 percent of Americans have a computer in their home. Many computer users do not have the technical know-how to fix their computers when they break or jam. Scammers—many from other countries—seek to exploit these facts.

"Tech Support" Scams.

Tech support scammers make unsolicited phone calls in which they pretend to be a technician for a reputable, well-known computer or software company. The caller claims your computer has been hacked or infected with a virus.

The scam artist may say that your device will crash or that hackers will steal your information if the issue is not immediately resolved. They do this to get you to act quickly, without researching the caller.

The scam artist may ask you to open a program on your computer that logs various activities, such as error and warning messages. While these entries may appear alarming at first glance, they are usually harmless notations that occur during the normal operation of your computer.

After convincing you there is a problem, the scammer claims he can repair your device remotely for a fee. Unsuspecting people may then give the scam artist their credit card or bank account information and remote access to the computer. This is where the trouble begins.

The scammer may use the remote access to perform fake "repairs" or install software that is available for free through other sources. The scammer does this to justify the bogus fee. Other times, scam artists install malware or viruses, which allow them to secretly steal information stored on the computer.

Either way, the end result is this: your device is less secure and the scam artist charges you hundreds or thousands of dollars for services that were unnecessary and useless.

Here's what these scam calls look like:

"Henry" received a call from an individual who claimed to work for Apple and said his computer was infected with viruses that allowed foreign hackers to steal his information. The caller told Henry he could remove the "viruses" for $299. Henry realized that Apple would not call him to warn him about such viruses, so he hung up.

"Ransomware" Scams.

If you are on the Internet, you may receive an unexpected pop-up message that freezes access to your computer. The message will ask you to call a telephone number or follow other instructions to un-jam your computer.

If you call, you will be asked to pay the scam artist a fee to unfreeze your computer. In other words, the scammer who jammed your computer asks you to pay him money to unjam it. Paying him money will usually result in requests for even more money.

It can happen like this:

"Josh" was using his laptop to catch up on the day's news online, when a pop-up froze his computer and instructed him to call a toll-free phone number for tech support. He shut down his computer, but the message was still there after it restarted. Josh knew this was a scam, so he took his laptop to a local computer repair shop to get it fixed.

How to Avoid these Scams.

- If you receive a call from someone who offers technical support, or claims your computer has been hacked or infected with a virus, hang up.
- If you need help with your computer, call the manufacturer or software company at the phone number given to you when you bought the product.
- If your device becomes infected or no longer works, hire a reputable local company to fix it.
- Never give an unknown party remote access to your device.
- Scam artists often identify themselves as representatives of large, national companies to establish credibility. Don't be fooled by such claims.
- If your computer does not have security software, install anti virus, anti spyware and anti malware software on your computer. Keep this software up to date.
- Make sure your device's firewall and pop-up blocker are turned on. This will help prevent intrusions and unsafe pop-ups.
- Do not download software from unknown sources or "click" open links, attachments, or images in unsolicited emails, text messages, or pop up messages. Doing so could lead to a ransomware scam or infect your device with a virus, which may give control of the device (and the information on it) to the scam artist.
- Turn off your computer when it is not in use. This cuts off any connection with attackers or potential attackers.

What to do if You Were Scammed.

- Disconnect your computer from the Internet and turn it off. Take your computer to a reputable technician to have it inspected or repaired. Do not reconnect your device to the Internet until you are sure it is secure and free of spyware or malware. You should then change the password to your device and any online account you accessed from the device.
- If you provided credit card or bank account information to the scam artist, promptly contact your financial institution to make it aware of the incident and dispute any inappropriate charges. It is often easier to get such charges reversed by disputing them with your financial institution, rather than from the scammer that made them. You may also wish to change or close your accounts to protect against unauthorized charges in the future.
- If your personal information has been compromised, consider taking steps to protect yourself against identity theft—including placing a fraud alert in your credit report, freezing your credit report, and monitoring your credit report and financial accounts for unauthorized activity.

Report Scams.

These scams are crimes. You may file a report with the Federal Bureau of Investigation, which may be reached as follows:

Federal Bureau of Investigation
Minneapolis Office
1501 Freeway Boulevard
Brooklyn Center, MN 55430
(763) 569-8000

You may also wish to file a complaint with the Federal Trade Commission as follows:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
Toll free helpline: 1-877-382-4357

For more information tech support scams or consumer issues, contact the Office of Minnesota Attorney General Lori Swanson as follows:

Office of Minnesota Attorney General
Lori Swanson
445 Minnesota Street, Suite 1400
St. Paul, MN 55101
651-296-3353 or 800-657-3787
TTY: 651-297-7206 or 800-366-4812
www.ag.state.mn.us