Computer Scams

From the Office of Minnesota Attorney General Keith Ellison

Over $21 million dollars. That is the amount of money consumers reported as lost to tech-support scams in the first nine months of 2017. In one variation of this scam, computer users receive a pop-up message on their screens telling them their computer has been hacked or infected with a virus and directing them to call a toll-free number for assistance. In another variation, people receive phone calls from scammers who say that their computer has a serious problem and offer to help them fix it. Either way, your computer is not really at risk, and the person on the other end is a scammer waiting to trick you into paying for computer support services you don't need, empty your bank account, or even steal your identity.

How the Scheme Works

Scammers make unsolicited phone calls or place misleading pop-up Internet advertisements to try to convince unsuspecting computer users that something is seriously wrong with their computers that must be fixed immediately. Scammers often pose as representatives of reputable, well-known computer or software companies.

Once a scammer has a person on the phone, the scammer often asks to remotely access the person's computer. Once inside, the scammer can download malware, steal passwords, or try to sell unnecessary services or products—including products that are available elsewhere for free—for non-existent problems.

Scammers often try to trick people into paying for services they don't need by opening a program on their computer that logs various activities, like error and warning messages. The scammers use these messages, which are usually harmless notations that occur when a computer is functioning normally, to convince people that something is seriously wrong with their computer.

Tips to Avoid Computer Scams

- If someone calls you offering technical computer support or claiming your computer has been infected with a virus or hacked, hang up.
- If you receive a pop-up message directing you to call a telephone number for assistance with your computer, take a picture of your entire screen, including, if possible, the universal resource locator (URL) of the web page, and include it in any reports you make to the Minnesota Attorney General's Office or other law enforcement agencies. Then press the "control" and "F4" keys to get rid of the pop-up. Do not click on the "x" in the upper right-hand corner of the window. If the pop-up remains after doing this, restart your computer.
- Be wary if a person asks for payment in an unusual form, such as through gift cards, wire transfers, or a check to be picked up by a courier.
- If your device has been infected by a computer virus or does not work, take it to a reputable local company to fix it.
- Make sure your computer has up-to-date antivirus, anti-malware, and anti-spyware software.

What to Do if You've Been Scammed

- If an unknown person remotely accessed your computer, disconnect your computer from the Internet immediately, turn it off, and take it to a reputable computer technician for inspection.
- If you provided a credit card or bank account information to the scammer, contact your financial institution right away to notify it of the incident and dispute any inappropriate charges.

- If your personal information was compromised, consider taking steps to protect yourself from identity theft—such as placing a fraud alert on your credit report, freezing your credit report, and monitoring your credit report and financial accounts for unauthorized activity.

If you have been contacted by a computer scammer, you may report the matter to 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)
www.ag.state.mn.us