Volume #4 - Issue #158
May 5th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Recognizing a Tech Support Scam

Some scammers call and claim to be computer techs associated with well-known companies like Microsoft or Apple. Other scammers send pop-up messages that warn about computer problems. They say they've detected viruses or other malware on your computer. They claim to be "tech support" and will ask you to give them remote access to your computer. Eventually, they'll diagnose a non-existent problem and ask you to pay for unnecessary – or even harmful – services.

These scammers may call, place alarming pop-up messages on your computer, **offer free "security" scans**, or set up fake websites – all to convince you that your computer is infected. The scammers try to get you on the phone, and then work to convince you there's a problem. Finally, they ask you to pay them to fix that non-existent problem.

To convince you that both the scammers and the problems are real, the scammers may:

- pretend to be from a well-known company – like Microsoft or Apple
- use lots of technical terms
- ask you to get on your computer and open some files – and then tell you those files show a problem (when they don't)

Then, once they've convinced you that your computer has a problem, the scammers might:

- ask you to give them remote access to your computer – which lets them change your computer settings so your computer is vulnerable to attack
- trick you into installing malware that gives them access to your computer and sensitive data, like user names and passwords
- try to sell you software that's worthless, or that you could get elsewhere for free
- try to enroll you in a worthless computer maintenance or warranty program
- ask for credit card information so they can bill you for phony services, or services you could get elsewhere for free
- direct you to websites and ask you to enter your credit card number and other personal information

The scammers want to get your money, access to your computer, or both. But there are things you can do to stop them.

- If you get an unexpected or urgent call from someone who claims to be tech support, hang up. It's not a real call. And don't rely on caller ID to prove who a caller is. Criminals can make caller ID seem like they're calling from a legitimate company or a local number.

- If you get a pop-up message that tells you to call tech support, ignore it. There are legitimate pop-ups from your security software to do things like update your operating system. But do not call a number that pops up on your screen in a warning about a computer problem.
- If you're concerned about your computer, call your security software company directly – but don't use the phone number in the pop-up or on caller ID. Instead, look for the company's contact information online, or on a software package or your receipt.
- Never share passwords or give control of your computer to anyone who contacts you.

If You Were Scammed

- **Get rid of malware**. Update or download legitimate security software and scan your computer. Delete anything the software says is a problem.
- Change any passwords that you shared with someone. Change the passwords on every account that uses passwords you shared.
- If you paid for bogus services with a credit card, call your credit card company and ask to reverse the charges. Check your statements for any charges you didn't make, and ask to reverse those, too. Report it to **ftc.gov/complaint.**

The bottom line is, if you get an unexpected pop-up, call, spam email or other urgent message about problems with your computer, stop. Don't click on any links, don't give control of your computer and don't send any money.

Thank you for subscribing to our email!