California Department of Justice
Attorney General Xavier Becerra

May 2017

Consumer Alert
Beware of Tech Scams

What to Look Out For

A scam artist posing as a tech support person will often attempt to gain access to the unwary consumer's computer or credit card with variations of the following statements:

- Viruses or malware have been found on your computer and need to be eliminated immediately.
- Your computer will suffer imminent harm if you do not buy the software, allow tech support to fix the problem, or provide remote access to your computer.
- You must search for particular files on your computer. When you find the files, which are usually harmless or related to legitimate programs, the scammer may try to trick you into believing that you need to buy useless software to delete them.

As part of the scheme to "save" your computer, the scammer may direct you to a fraudulent website and ask you to enter credit card information, or other sensitive financial information, that he or she can then steal. Or, the scammer may take control of your computer and refuse to return it to you unless you agree to purchase computer services.

Helpful Resources

If you believe that you are a victim of a tech support scam, or if tech support scammers have called you, file a complaint with the California Attorney General's Office by visiting: *www.oag.ca.gov/contact/consumer-complaint-against-business-or-company.* Complaint forms are available in English, Spanish, Chinese and Vietnamese.

You may also call (800) 952-5225 or send a letter to:

California Department of Justice
Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550

You may also file a report with the Federal Trade Commission (FTC) at 1-877-FTC HELP, or online at *www.ftc.gov/complaint*

Additional consumer tips and resources on privacy and cybersecurity are available from the California Attorney General at: *www.oag.ca.gov/privacy/consumer-privacy-resources*

California Department of Justice
Attorney General Xavier Becerra

10 Ways to Protect Yourself From Tech Support Scams

1. If you get a call from someone claiming to be a tech support person, hang up.
2. If you get an unfamiliar pop-up window, close it.
3. If you receive a suspicious email or text message, delete it.
4. If you are asked to provide remote access to your computer, hang up. Never give control of your computer or provide payment or sensitive information to someone whom you do not know.
5. Be aware of links and avoid suspicious websites.
6. Do not be pressured into purchasing software or computer services. Do your own research.
7. Run current versions of anti-virus software on your computer. Purchase consumer software from known and trusted sources.
8. Do not rely on caller ID alone to authenticate a caller. Criminals know how to manipulate caller ID systems to make it appear they are calling from a local or legitimate number.
9. Never give out any of your passwords. No legitimate company requests your password.
10. Change your browser settings to block pop-ups from unfamiliar websites. If you see a pop-up alert, don't click on it and don't call any of the phone numbers listed on the pop-up. If you encounter an unwanted pop-up window, you can close your internet browser by following these steps:
    - **Apple:** you can close your browser by using Force Quit: (1) either access Force Quit from the Apple icon menu or press Command+Option+Escape simultaneously to open the Force Quit Applications window; (2) select your web browser; and (3) click on "Force Quit."
    - **Windows:** you can close your browser by using the Task Manager: (1) press Ctrl+Alt+Del and click on Task Manager or simply press on Ctrl+Shift+Esc; (2) select your web browser; and (3) click on "End Task."

What to Do if You Are a Victim of a Tech Scam

- If you have given a scammer remote access to your computer, revoke it verbally. If he or she does not immediately return control of your computer to you, shut down or restart your computer. That should cut off the remote session. The next time your computer is turned on, use your anti-virus software to scan your computer.
- Report the fraud by calling our office or filing a complaint online.
- Change your passwords – including those linked with your computer, email, and any financial accounts.
- If you paid for fake tech support services or software with a credit card, call your credit card company to reverse the charges.
- If you have given any other financial information to a scammer, or if you think the scammer might have gained access to such information, contact your bank to report the fraud immediately.