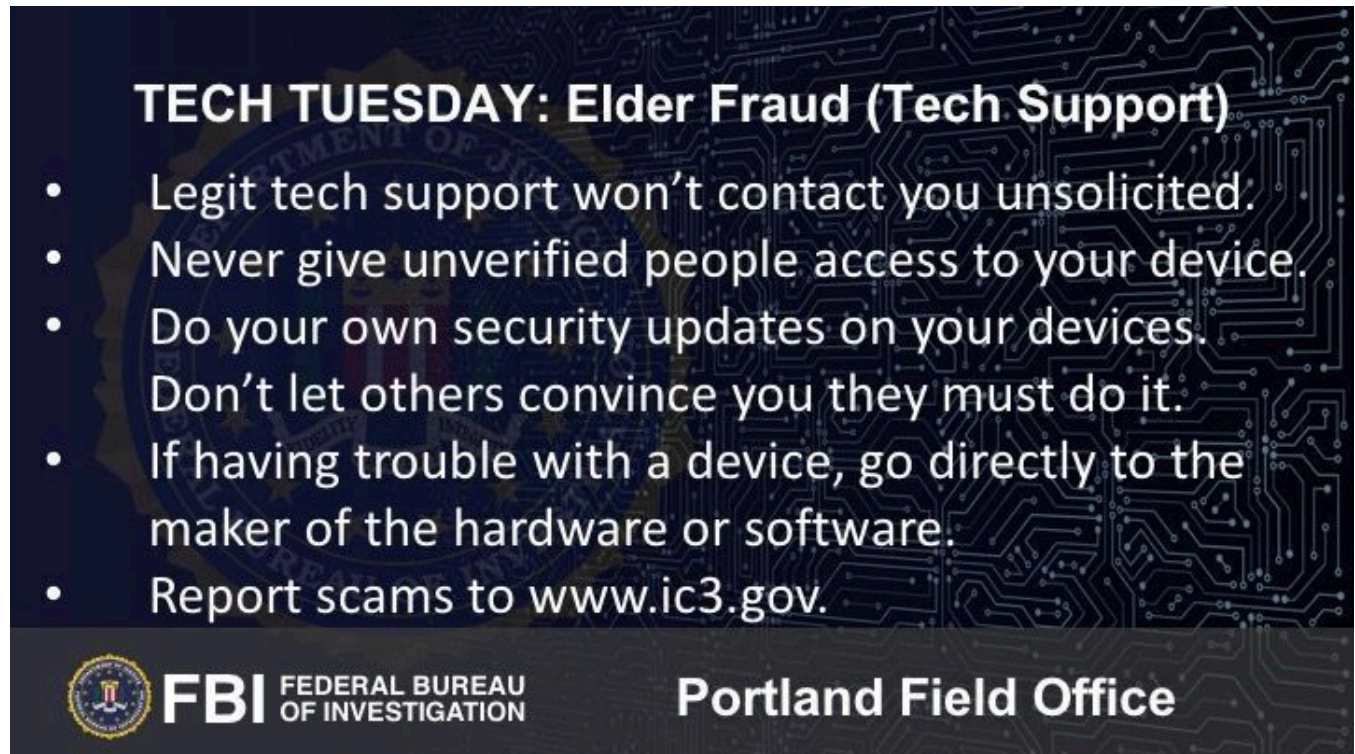


Tech Tuesday: Building a Digital Defense Against Elder Fraud (Part 3 - Tech Support Scams)

June 29, 2021



TECH TUESDAY: Elder Fraud (Tech Support)

- Legit tech support won't contact you unsolicited.
- Never give unverified people access to your device.
- Do your own security updates on your devices. Don't let others convince you they must do it.
- If having trouble with a device, go directly to the maker of the hardware or software.
- Report scams to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

June is Elder Abuse Awareness Month. For more information, go to <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud>. Our series of "Tech Tuesday" reports this month will cover a variety of scams that seniors often face.

Welcome to the Oregon FBI's Tech Tuesday segment. This week: building a digital defense against frauds targeting senior citizens when it comes to technical support scams.

The FBI's Internet Crime Complaint Center says it received almost 10,000 reports from seniors 60 and older about such scams in 2020 – with reported losses of more than \$116 million. That's a 204 percent increase in losses from 2019.

Technical support fraud happens when criminals pose as customer, security or tech support representatives – usually from a well-known company. In one version of the scam – the fraudster contacts the victim by phone, email, or text to tell the victim that there's a problem with the victim's device or financial account. The

fraudster may say the device has a security flaw and has been hacked... or that some unauthorized person is stealing money from a bank account.

In another version of the scam, the senior is experiencing a real technical problem with a device and goes out in search of help. When he pulls up the search engine results, he may inadvertently click on a bad ad instead of a legitimate vendor.

A third common way for a senior to get caught up in this scam is for the fraudster to use malware to cause a pop-up message or lock screen to appear on the senior's device.

No matter how the scam starts, the criminal's goal is to convince the senior to give the fake tech support person remote access to the device. With that access, the fraudster can now potentially have access to all of the victim's personal info, tax returns, and bank accounts.

Criminals target seniors because they are often more trusting, financially stable, and less likely to report the crime out of shame.

Here's how you can protect yourself and family members:

Know that legitimate tech support people will not contact you unsolicited.

Never give unknown, unverified people access to your devices.

Ensure that you update all anti-virus, security, and malware protection on your devices. Don't let an unknown person tell you that he needs to do it for you.

If you receive a concerning pop-up or your screen locks, shut down your device immediately, regardless of the directions you receive from the scammer. Oftentimes, waiting a short time and rebooting will fix the problem.

When doing online searches for technical support, be cautious of listings at the top of the page labeled as "sponsored". If you are having trouble with a particular software or hardware product, go directly to that company's webpage.

If you have been victimized by an online scam, report your suspicious contacts to the FBI. You can file an online report at the FBI's Internet Crime Complaint Center at www.ic3.gov or call your FBI local office.