Tech Support Scams

According to the Federal Trade Commission (FTC), older adults filed more reports indicating a loss on tech support scams between 2015 and 2018 than any other fraud category in the FTC's Consumer Sentinel Network.

These scams often begin with a phone call or a pop-up warning displaying a fake error message with a number to call. Scammers often impersonate representatives from a software company—such as Apple, Google or Microsoft—and try to convince victims to provide remote access to their computers to "repair" an issue, such as malware.

The criminal will then scan the computer and seemingly troubleshoot the "problem," and may install applications to access personal information. After offering fake solutions, the scam artist will ask for payment and may also encourage the victim to sign up for a phony subscription service.

Don't Be a Victim

- Hang-up the phone if you receive an unsolicited call from someone who says that there's something wrong with your computer.
- Be suspicious of pop-up warnings. Security pop-ups from real tech companies will not ask you to call a phone number.
- Do not give access to your computer or share passwords with anyone who contacts you.
- Keep your computer's security software up to date.

If Scammed

- Contact your bank to report fraud and check your statements.
- Change your passwords to your computer, bank accounts and other sites.
- Scan your computer for viruses and call your security software company for help.