Tech Support Scams

Tech support scams often begin with a phone call or a pop-up window displaying a fake error message with a number to call. Scammers often impersonate representatives from a tech company—such as Apple, Google or Microsoft—to persuade victims to provide remote access to their computers to "repair" an issue, such as malware.

If the victim provides access to the device, criminals will scan the computer to "troubleshoot the problem" and offer fake solutions. They may install dangerous computer applications or encourage the victim to pay for a phony subscription. In the process, the scammers steal the victim's money and identity.

Don't Be a Victim

- Hang up the phone if you receive an unsolicited call from someone who says 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 passwords to your computer, bank accounts and other sites.
- Scan your computer for viruses and call your security software company for help.
- Report it to the Federal Trade Commission at **ReportFraud.ftc.gov**.