



Fraud Watch Network

TECH SCAMMERS KNOW YOU ARE HOME . . . AND ONLINE

Two things have been certain during this pandemic: People have been home more than ever, and they've been using technology more than ever to stay connected to the outside world. Scammers are keyed into these facts and are taking advantage. It's the classic tech-support scam, and it is running rampant right now.

HOW IT WORKS

- You receive a phone call from what appears to be Microsoft or another big tech company, claiming they detected a virus on your device that requires your immediate attention.
- Or you sit down to your device to find a pop-up message warning that your device is infected and you need to call the number in the message or click a link right away.
- A "technician" explains the severity of the issue, requests remote access to your device and then shows you "the problem."
- The "technician" can fix your problem for a fee, and then may offer you a monthly subscription to keep your device safe.
- The "technician" often calls back months later, offers you a refund and asks for your bank account information to deposit the money.

WHAT YOU SHOULD KNOW

- Big tech companies say they don't call customers to warn of problems on their devices.
- The supposedly problematic files the "technician" shows you on your device are completely benign.
- The scammer may ask you to pay by credit card or may direct you to purchase a gift or reloadable card and provide the account number and PIN (this is always a red flag).
- The "technician" may install malware on your device while they have access to harvest usernames and passwords to exploit your accounts.

WHAT YOU SHOULD DO

- Screen phone calls with an answering machine or voicemail, and once you listen to the message, decide if it warrants a callback.
- If the caller claims you have a problem with your device, don't believe it.
- If you think your device is infected, get it checked out by a reputable source; most big-box electronics retailers offer tech-support services.
- If you get a pop-up that freezes your screen, shut down your computer and restart it to make it go away.
- If you realize you've fallen victim to this scam and paid by credit card, contact your financial institution to dispute the charge and cancel any monthly fees you may have agreed to.

When it comes to fraud, vigilance is our number one weapon. You have the power to protect yourself and your loved ones from scams. Please share this alert with friends and family and visit the [Fraud Watch Network](#).