What To Do If You Get Tricked By a Hacking Phone Call

> **Stop. Breathe. Do Not Panic. Scammers are professionals at making you feel rushed or terrified. If you realize you are on the phone with a scammer, or if you just gave them information or access to your computer, follow these steps immediately.**

1 Disconnect Everything Immediately

- **Hang up the phone.** Do not explain yourself, do not apologize, and do not say goodbye. Just press "End Call."
- **Turn off your computer.** Do not just close the lid or put it to sleep. Press and hold the physical power button on your computer for 10 seconds until the screen goes completely black and the machine shuts down. This instantly cuts off their remote access.
- **Turn off your WiFi router.** Unplug the power cord from the wall. This completely severs the connection between your home and the scammer.

2 Secure Your Money

- **Call your bank and credit card companies immediately.** Use the phone number printed on the back of your physical card. Never use a number the caller gave you or search for one on Google right now.
- **Tell them:** "I gave a phone scammer access to my computer and banking information. Please freeze my accounts and watch for fraudulent charges."
- **Change your banking passwords.** Use a different, safe device (like your smartphone on cellular data, not WiFi) to change your passwords.

3 Secure Your Identity and Accounts

- **Check your email.** Scammers often try to break into your primary email (like Gmail or Yahoo) first, because that is where password reset links are sent. Change your email password immediately.
- **Place a fraud alert.** Contact one of the three major credit bureaus (Equifax, Experian, or TransUnion) to place a free fraud alert on your credit file. This makes it harder for scammers to open new accounts in your name.

4 Clean Your Devices

- **Do not turn your computer back on yet.** If the scammer installed remote access software (like AnyDesk, TeamViewer, or LogMeIn), they might still have a backdoor.
- **Seek professional help.** Take your computer to a trusted local repair shop or the Geek Squad. Tell them: "A scammer had remote access to this machine. I need you to remove all remote access tools and scan for malware."