

Scam and Pop-up Safety Guide

A scary pop-up or an unexpected phone call can make anyone freeze. Take a breath. You do not have to decide or fix it while someone is pressuring you.



Someone you do not trust is controlling your computer?

Turn the computer off now. If you can, disconnect from the internet/network. Do not keep talking to them. Then call IT Wes for a calm next step.

START HERE

Stop the conversation

- 1 **Do not click, call, download, pay, or share a code.** A real warning does not need you to act under pressure. If you can, disconnect from the internet/network.
- 2 **For a pop-up:** do not use the phone number or link on the screen. If it will not close, press **Ctrl + Alt + Delete**, open Task Manager, and end the browser. Do not restore its old tabs. Turning the computer off is also okay.
- 3 **For a phone call:** hang up. Do not trust caller ID, even if it says Google, FBI, the IRS, or another familiar name. Do not call the number they gave you back.

IF INFORMATION OR ACCESS WAS SHARED

Protect what matters next

- 1 **Stop their access:** turn off the computer and disconnect it from the network.
- 2 **From a different, trusted device,** call your bank or credit card company using the official number on your statement or the back of your credit cards. Review recent transactions and ask what protection steps they recommend, especially if bank-account or credit-card information was shared.
- 3 **Change exposed passwords, starting with email,** and turn on multi-factor authentication. Never give a one-time verification code to anyone who contacted you.

If a scammer had remote access, do not assume the computer is clean just because the pop-up is gone. Have it checked before normal use.

WHAT A SCAM OFTEN LOOKS LIKE

Pressure is the giveaway

- ✗ An unexpected pop-up says your device is infected, locked, or compromised and tells you to call a number.
- ✗ An unsolicited caller claims to be Microsoft, Google, Apple, your bank, antivirus company, internet provider, or the IRS.
- ✗ They create urgency: arrest, account closure, lost files, a "refund," or an immediate security emergency.
- ✗ They ask for **remote control, passwords, one-time codes, gift cards, cryptocurrency, wire transfers, or payment-app transfers (Venmo, Zelle, CashApp).**

VERIFY INDEPENDENTLY

Use your own path

Microsoft, Google, banks, the IRS, and other providers do not make unexpected support calls demanding immediate action or payment.

Do not trust the phone number, link, email, or text that arrived with the message. Type the official website yourself, use the official app, or call the number on your statement or card.

Call someone you trust, like a close family member or friend. A second person can help you slow down and verify what is real.

Not sure? Call before you click.

IT Wes provides patient, no-judgment scam cleanup and computer help. Tell me what happened in plain language, and we will choose the simplest safe next step together.

(520) 261-9201

itwes.com