

Scareware & Malware

DON'T PANIC · DON'T CLICK · THINK FIRST

5 min
read

Learn how to recognize fake security warnings, respond confidently, and protect yourself before a scam becomes a real problem.

★ RGE TIP

Scammers don't hack your computer first — they hack your emotions first. A warning demanding immediate action is your signal to slow down.

📱 ON ANY DEVICE

Windows PCs, Macs, iPhones, iPads, and Android devices can all display scareware. The look changes — the scam doesn't.

1 Everyone Uses These

Essentials · Everyday Tasks

-  **Learn the Warning Signs**
Scareware pretends to be Microsoft, Apple, or your antivirus.
-  **Never Call the Number**
Real companies don't place support phone numbers inside browser warnings.
-  **Don't Click Anything**
Buttons like OK, Cancel, and Scan Now may all trigger the scam.
-  **Close the Browser**
Close the tab or force-close the browser if necessary.
-  **Keep Everything Updated**
Updates close security holes before scammers can exploit them.
-  **When in Doubt...**
Pause first. Fear is the scammer's favorite tool.

2 Useful Skills

Good to Know · Do More

-  **Force-Close the Browser**
Task Manager (Windows) or Force Quit (Mac).
-  **Clear Browser Cache**
Removes leftover scareware pages.
-  **Run Windows Security**
Or your antivirus — verify whether anything actually installed.
-  **Restart the Computer**
Many fake warnings disappear after restarting.
-  **Know Who You'll Call**
Find a trusted technician before you need one.

★ **Flyswatter before bazookas:** not every warning means malware. Closing the browser, restarting, and running a scan clears most scareware.

3 Advanced Topics

Use with Caution · Take Control

-  **If You Called the Number**
Stop immediately if you realize it's a scam.
-  **Disconnect from the Internet**
If remote access was given, disconnect Wi-Fi or unplug Ethernet.
-  **Remove Remote Access Software**
AnyDesk, TeamViewer, UltraViewer, etc.
-  **Change Passwords**
Use a different trusted device.
-  **Contact Financial Institutions**
If banking or credit card information was shared.
-  **Have the Computer Checked**
Especially if software was installed or remote access occurred.

KNOW THE DIFFERENCE

😊 Scareware

-  **Fake warning** — usually just a webpage
-  **Wants you to panic** — an emotional attack

🚫 Malware

-  **Real infection** — installs software
-  **Wants to stay hidden** — a technical attack

HOW TO GET STARTED



STOP



Don't Click



Close Browser



Restart



Run Security



Back in Control

SAFETY REMINDERS

-  Microsoft and Apple do not display browser pop-ups telling you to call support.
-  Gift cards are never legitimate tech-support payments.
-  Never allow remote access unless you initiated the support session.
-  If something feels wrong, stop before doing anything.
-  It's always easier to prevent a scam than recover from one.

★ RGE GOLDEN RULE

If a computer tries to scare you into acting immediately... **slow down.** The scammer is in a hurry. You don't have to be.

"Teacher first. Technician second. People always."