

How to Recognize and Safely Handle a Random Pop-Up Scam or Spoof Alerts



These types of scam messages can appear suddenly on a computer, tablet, or phone. They may show up while you are visiting a normal website, such as Amazon, your doctor's website, or even right after opening your web browser. Some may include loud audio messages claiming that your computer is compromised and telling you to call a phone number. Do not panic. **DO NOT CALL THE PHONE NUMBER** - Follow the steps below carefully to avoid making the situation worse.

Step 1	Do not react to the message. Do not click anything, type anything, or try to close the message using the keyboard. Do not call the phone number shown on the screen.
Step 2	Take a moment to stay calm. These messages are designed to scare you, but following the steps below will help you respond safely.
Step 3	Press and hold the power button on your computer until it shuts off completely. Do not turn it back on yet.
Step 4	Unplug the power from your modem* and leave it disconnected for at least 10 to 15 minutes or more.
Step 5	While the modem is still disconnected, turn your computer back on. Do not reconnect power to the modem yet. This is especially important if your computer normally connects to Wi-Fi automatically.
Step 6	If the computer starts normally, you reach the login screen, you log in successfully, and everything looks normal, continue to Step 7. If the same pop-ups are still on your screen, go directly to Step 14.
Step 7	Make sure you are not online. Look for the globe icon in the lower-right corner of the screen; if you see the globe, you are offline. Then open the web browser you were using when the scam screen appeared, such as Chrome, Edge, Firefox, or another browser.
Step 8	In the browser window, click the three dots in the upper-right corner. Open History , then open the History page . Click Delete browsing data . Choose All time and leave the four default boxes checked.
Step 9	Click Delete data and wait for the process to finish. When it is complete, close the web browser.

Step 10	If you use any other web browsers, repeat Steps 5 through 9 for each one.
Step 11	Run a full virus and malware scan using Microsoft Defender or your preferred third-party security software. If anything, suspicious is found, remove it. Also check for any unusual or unfamiliar software installed on the computer. If nothing is found, restart the computer and log in normally.
Step 12	Plug the modem back in and allow at least 10 minutes for it to reconnect to your internet service provider.
Step 13	Return to normal use. Make sure Windows updates are current and confirm that any third-party security software you use is also up to date.
Step 14	Power the computer off using the power button. Do not try to keep using the computer or get back online. This could make the problem worse, especially if the modem has been plugged back in and the computer reconnects to Wi-Fi automatically. Leave the computer off and contact a computer technician. The system should be professionally checked and cleaned.
Please note	If you reach Step 14, keep the computer turned off until it has been professionally cleaned. You may plug the modem back in and use other devices on your Wi-Fi network.
*	Disconnecting the modem cuts off the internet connection while you clear the browser data and check the computer.

Image details

Small alert on the side of the screen

This example shows several small warning boxes stacked on the side of the screen.

Scammers often use repeated alerts, urgent language, fake security names, and buttons such as “Renew,” “Ignore,” or “Allow” to pressure you into clicking. Treat this as suspicious: do not select any button, do not call any number shown, and follow the shutdown and cleanup steps in this guide.

Full-screen security warning

This example shows a large fake security warning that appears to block access to the computer and urges you to contact “Windows Support.” It uses Microsoft-style wording and urgent claims to make the message seem official. Do not click “Allow,” “Deny,” or any other prompt, and **do not call the listed phone number**. Power off the computer and continue with the safety steps above.

Ed the Computer Guy – www.edcomputerguy.com – fixit@edcomputerguy.com