

FAKE VIRUS WARNINGS

Scareware and adware: what they are and what to do

A web page cannot scan your computer. If a pop-up says you are infected or hacked, treat it as a scam until our team says otherwise.

SECURITY ALERT



Your PC is infected with 5 viruses.

Do not restart. Call support now:

1-8XX-XXX-XXXX

SCAN NOW

FAKE

WHAT IT IS

Scareware

Fake warnings built to look like Windows, Microsoft, or antivirus alerts. They claim your computer is infected or hacked and push you to call a number, download a fix, or pay.

Adware

Unwanted software or browser notifications that flood your screen with ads and pop-ups. Many of those pop-ups are scareware, and they lead to scam or malicious sites.

HOW IT USUALLY STARTS

1. Clicking Allow on notifications

A site asks to show notifications, often with a prompt like "Click Allow to verify you are not a robot." Clicking Allow lets that site send pop-ups to your desktop even after you close the tab. Those pop-ups look like system alerts.

2. Landing on a fake alert page

A mistyped address, a bad ad, or a search result opens a full-screen page with alarms, flashing red text, a fake scan, and a phone number. The browser may seem locked. The page is only a web page, and it has not scanned or accessed anything on your computer.

WARNING SIGNS

- It says your computer is infected, hacked, or locked.
- It lists a phone number for "Microsoft Support" or another help desk. Microsoft does not put phone numbers in its error or warning messages.
- It uses countdown timers, alarm sounds, or flashing text to rush you.
- It asks you to install remote access software, enter your password, or pay by card, gift card, or cryptocurrency.
- Pop-ups appear in the corner of your screen from a website name you do not recognize.

WHAT TO DO

1. Do not call the number, click any buttons, or download anything.
2. Close the browser. If it will not close, press **Ctrl + Shift + Esc** to open Task Manager, select the browser, and click **End task**.
3. When you reopen the browser, do not restore the previous pages.
4. Contact our security team. We will check the computer and remove any notification permissions the site was given.
5. If you already called, allowed remote access, entered a password, or paid, contact us right away. Do not wait to see what happens.

HAVE YOU SEEN SOMETHING LIKE THIS? CONTACT OUR SECURITY TEAM.

When in doubt, reach out.

EMAIL

security@karhucyber.com

SECURITY HOTLINE

(888) 438-1168