

PRINTABLE GUIDE

Handle a suspicious computer warning

Scammers can copy warning screens, logos and caller names. Pause before paying, sharing codes or letting anyone control your computer. Verify unexpected contact independently.

Any computer or phone | 2 min read | 5 steps

Before you start

- ☐ A trusted way to contact your bank or device support
- ☐ A moment to stop before acting

1. Pause the conversation

Do not call a number shown in a frightening pop-up, install a requested remote-control app or share a verification code. Unexpected calls claiming to repair your computer should be checked independently.

- ☐ Done this step

2. Close the page safely

Try closing the browser tab or window. If the page prevents this, use the device's app-switching controls or Task Manager to close the browser. Reopening the same tabs may bring the warning back.

- ☐ Done this step

3. Check through a trusted route

Open your device's built-in security app or support website yourself. Microsoft says its error messages do not contain support phone numbers. Use a contact you obtained independently rather than one supplied by the caller.

- ☐ Done this step

4. Respond to what you shared

If someone controlled the computer, disconnect it from the network and seek trusted help. From a separate trusted device, change affected passwords. If you paid or exposed financial details, contact your bank promptly.

☐ Done this step

5. Report and keep a record

Keep the date, messages and payment information without reopening dangerous links. Report the incident using the relevant service's official scam channel. In the UK, suspicious emails can be forwarded to report@phishing.gov.uk.

☐ Done this step

Try it for yourself

Write your trusted bank and device-support contact routes on your checklist.

☐ I tried the task.

My notes

Does closing the pop-up remove all malware?

No. If you installed software, gave remote access or still see unusual behaviour, further checks with trusted support are needed.

Official help and the online guide

Recognise tech support scams -

<https://support.microsoft.com/en-us/office/protect-yourself-from-tech-support-scams>

Report suspicious emails - <https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-email>

Read online: <https://plaintech-guides.pages.dev/guides/handle-fake-computer-warning/>