

ANYONE CAN CLICK. SPEED BEATS BLAME.

Clicked a phishing link? Do this.

The faster you speak up, the smaller the problem. Nobody gets in trouble for reporting.

1 Stop. Don't enter anything else.

Close the page. If you haven't typed anything yet, even better.

2 Tell IT right now.

Use the report button or call the help desk. Say what you clicked and when. Minutes matter.

3 Typed a passphrase? Change it.

Do it from a device you trust, on the real site (type the address yourself). Change it anywhere else you reused it, too.

4 Let IT lead on your device.

They may ask you to disconnect from Wi-Fi. Don't wipe, reset, or power it off unless they say so. They may need to look at it.

5 Watch for weird activity.

Surprise MFA prompts, reset emails, login alerts, or money moving. Report anything odd.

Happened on your personal email or phone?

Forward phishing emails to reportphishing@apwg.org · Forward scam texts to 7726 (SPAM) · Report fraud at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud) · Lost money? Call your bank right away and file at [ic3.gov](https://www.ic3.gov).