GUIDE

If It Already Happened

First steps after someone clicked, shared, or paid.

It is not your fault. Act quickly, but do not panic.

If you clicked a link

Close the page. Enter nothing else. If you typed a password, change it from a device you trust and turn on two-step verification.

If you shared a password or one-time code

Change the password now, in the official app. Then tell the company what happened.

If you sent money or card details

Call your bank on a trusted number now. Say you have been scammed.

If you shared identity documents

Contact your country's identity-fraud service and follow their steps.

If you feel unsafe or are being threatened

Contact emergency or safeguarding services. Ask us and we will help you find the right local number.

Remember

Stop talking to the scammer. Never pay anyone who promises to get your money back.

Local help

Organization, local service, contact	[PARTNER NAME / LOCAL SERVICE / CONTACT]

> This is general safety information. Replace the local placeholders and check the advice against the partner's country before distributing it.

For scam warnings, go to
watchout.report

Cybersecurity Reach Foundation
501(c)(3) nonprofit

YOUR LOGO, NAME AND PHONE