

PHISHING

HOW TO STAY SAFE

1. Don't trust unexpected links or attachments

If you weren't expecting it, don't click it—even if it looks like it came from a company or someone you know.



“You must fix a problem in your account.”

Don't click. Instead, open your browser and type the website address yourself.

2. Don't give out passwords or codes

No real company will ever ask for your password or a code from your phone.

3. If you're unsure, stop and check

Call the person or company directly using a number you trust—never use a phone number or link.

