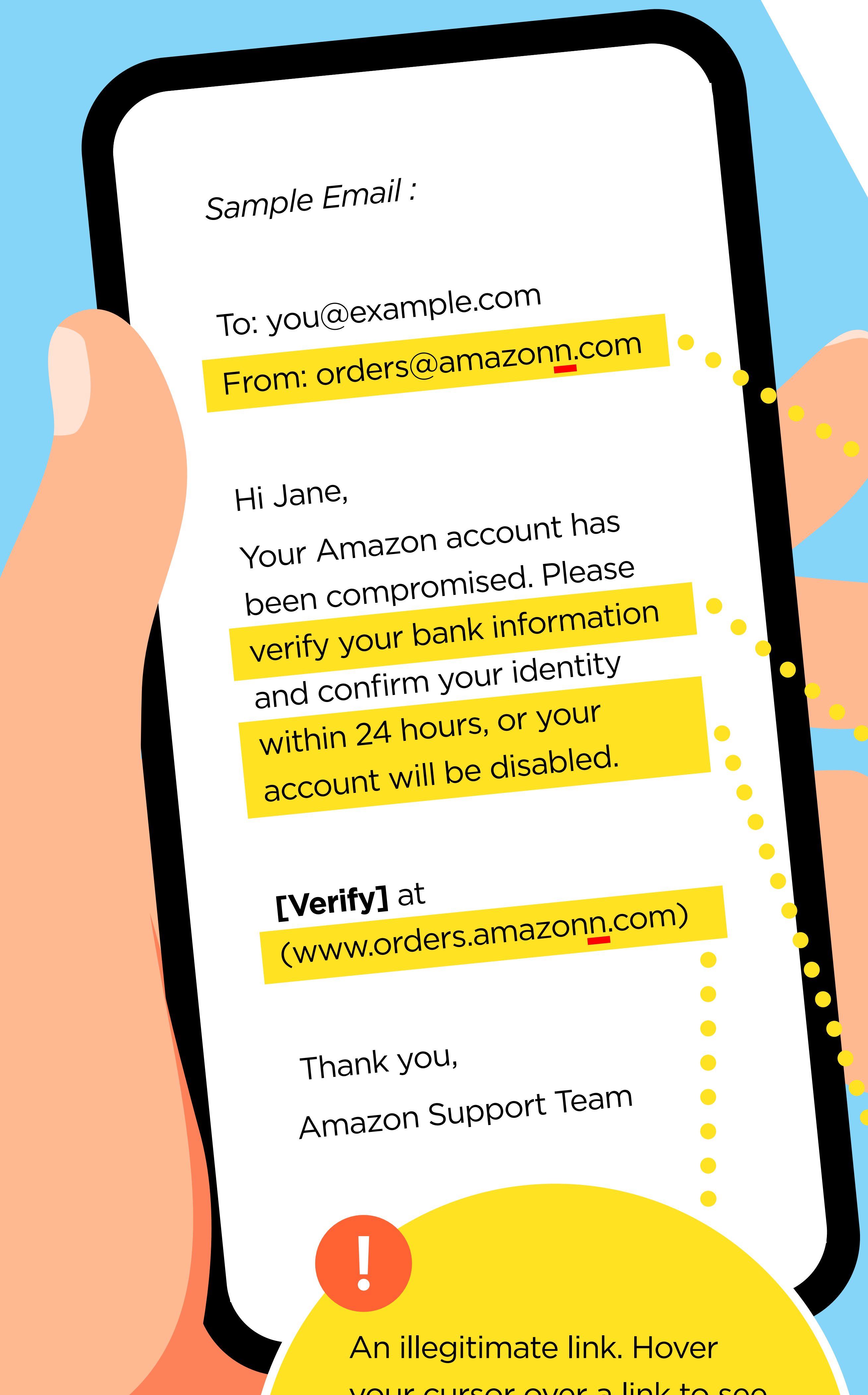
Something's Phishy!

A phishing email is a fake email designed to get the recipient to release sensitive personal information. So how can you tell when a cybercriminal has gone phishing? Check out the red flags below.



Sample Email :

To: you@example.com

From: orders@amazonn.com

Hi Jane,

Your Amazon account has been compromised. Please verify your bank information and confirm your identity within 24 hours, or your account will be disabled.

[Verify] at (www.orders.amazonn.com)

Thank you,
Amazon Support Team

! Misspellings in the email address, subject line or body.

! The sender is asking you to do something they typically never request. Amazon does not ask for personal information via email.

! An illegitimate link. Hover your cursor over a link to see if the URL is recognizable, but never click first. Instead, head to the service's website and log into your account directly to check for notices.

! A demand for immediate action "or else."

Think Before You Click

- ✓ Is this email expected?
- ✓ Does the content make sense?
- ✓ Can this email be verified through another platform?

If you do experience identity theft due to phishing, report it to the Federal Trade Commission (FTC). They have programs and services to help with recovery. Visit: **https://identitytheft.gov/databreach**