

SECURITY

How to spot a phishing email

The five telltale signs of a phishing message, and what to do if you clicked.

Phishing emails try to trick you into giving away passwords or payment details. Check for these signs:

1. **Urgency or threats** — "your account will be closed today", "invoice overdue, pay now".
2. **The sender address doesn't match** — display name says your bank, the address is `security@paypal-alerts.com`.
3. **Generic greeting** — "Dear customer" instead of your name.
4. **Unexpected attachments or links** — hover over a link (don't click): does the URL match where it claims to go?
5. **Requests for credentials** — legitimate services never ask you to "confirm your password" by email.

If you're unsure

Forward the message to us or open a ticket with a screenshot — **never reply to it or click its links**. We'll verify it in minutes.

If you already clicked or entered a password

Don't panic, but act now: **call us or open an urgent ticket immediately**. We'll reset the affected credentials, check the account for unauthorized access, and secure your mailbox. The faster we know, the smaller the damage.