

Top 5 Instant Phishing Checks

A quick-reference cheat sheet to spot scams fast.

1. Check the Sender Address

If the email domain looks weird, misspelled, or unfamiliar — don't trust it.

2. Look for Urgency or Threats

If they tell you "act now" or "your account will close," pause before doing anything.

3. Hover Over Links Before Clicking

If the link preview doesn't match the company's real website, it's a scam.

4. Never Share Personal Information

Banks and companies NEVER ask for passwords, codes, or Social Security numbers by email.

5. Trust Your Gut

If something feels "off," do not click. Go directly to the official website instead.