Phishing Identification Guide

presented by SiparSecure

Learn how to spot and avoid phishing attacks.

1. Check the Sender

- Look closely at the email address — small spelling tricks are common.
- If the name looks familiar but the address looks strange, it's suspicious.

2. Hover Before You Click

- Hover over links to see where they *really* go.
- If the link looks unusual or redirects to a random URL, don't click.

3. Look for Urgent or Threatening Language

Be cautious if the message says things like:

- "Your account will be closed today!"
- "Immediate action required…"
- "You missed a payment — click here."

Attackers use fear to get quick clicks.

4. Never Share Personal or Financial Info

Legitimate companies will **never** ask for:

- Passwords
- Verification codes
- Banking details
- Social Security numbers

…through email or text.

5. Beware of Unexpected Attachments

- Don't open invoices, PDFs, ZIP files, or documents you didn't expect.
- Even if it appears from a coworker — call them to confirm.

6. Check for Grammar or Design Errors

- Strange spacing
- Misspellings
- Off-brand logos
- Low-quality graphics

All of these are red flags.

7. Verify Through Another Channel

If an email seems strange:

- Call the sender
- Message them separately
- Or contact the company directly using their official website

Never trust the contact info inside a suspicious email.

8. Report Immediately

- Notify your IT/security contact
- Delete the email
- Never reply or click anything inside it

Reporting helps protect the whole team.