proofpoint

PRACTICAL ADVICE FOR AVOIDING PHISHING EMAILS

Phishing emails require one thing to be successful: someone to take the bait. Here's a handy decision tree to help you verify unknown emails, an important step in protecting yourself.

Have you received an unknown email?

Does it contain a link?
- YES → Does it contain an attachment?
- NO → Does it contain an attachment?

Does it contain an attachment?
- YES → Do you know who it's from?
- NO → Does it ask for money, credentials or sensitive info?

Does it ask for money, credentials or sensitive info?
- YES → Do you know who it's from?
- NO → CARRY ON

Do you know who it's from?
- YES → Are you sure?
- NO → Can you verify who sent it?

Are you sure?

Remember:
- Email addresses can be "spoofed" (made to look like they're coming from a trustworthy sender).
- Brands and logos can be copied (including those from well-known companies and even your own organization).
- Links can be disguised to make them appear legitimate.

- YES → Are you really sure?
- YES → Are you really sure?

Are you really sure?

Remember:
- Cyber criminals sometimes build trust by developing relationships over time—via email, phone calls, and social media interactions—before they ever ask for anything.
- Login credentials can be stolen and used by attackers to send malicious emails from known, trusted accounts.
- Before you click a link, download a file, respond with sensitive data, or complete a wire transfer, you must be 100% confident senders are who they say they are and that requests are legitimate.

- NO → Can you verify who sent it?
- YES → CARRY ON

Can you verify who sent it?

Confirm the source:
- Hover over links (to see the true destination) and compare to a legitimate site.
- Call a known phone number (not one from the email) and ask about the message.
- Visit a trusted website (by typing the address in your browser).

- NO → REPORT IT (and wait for confirmation before acting on it)

0519-018