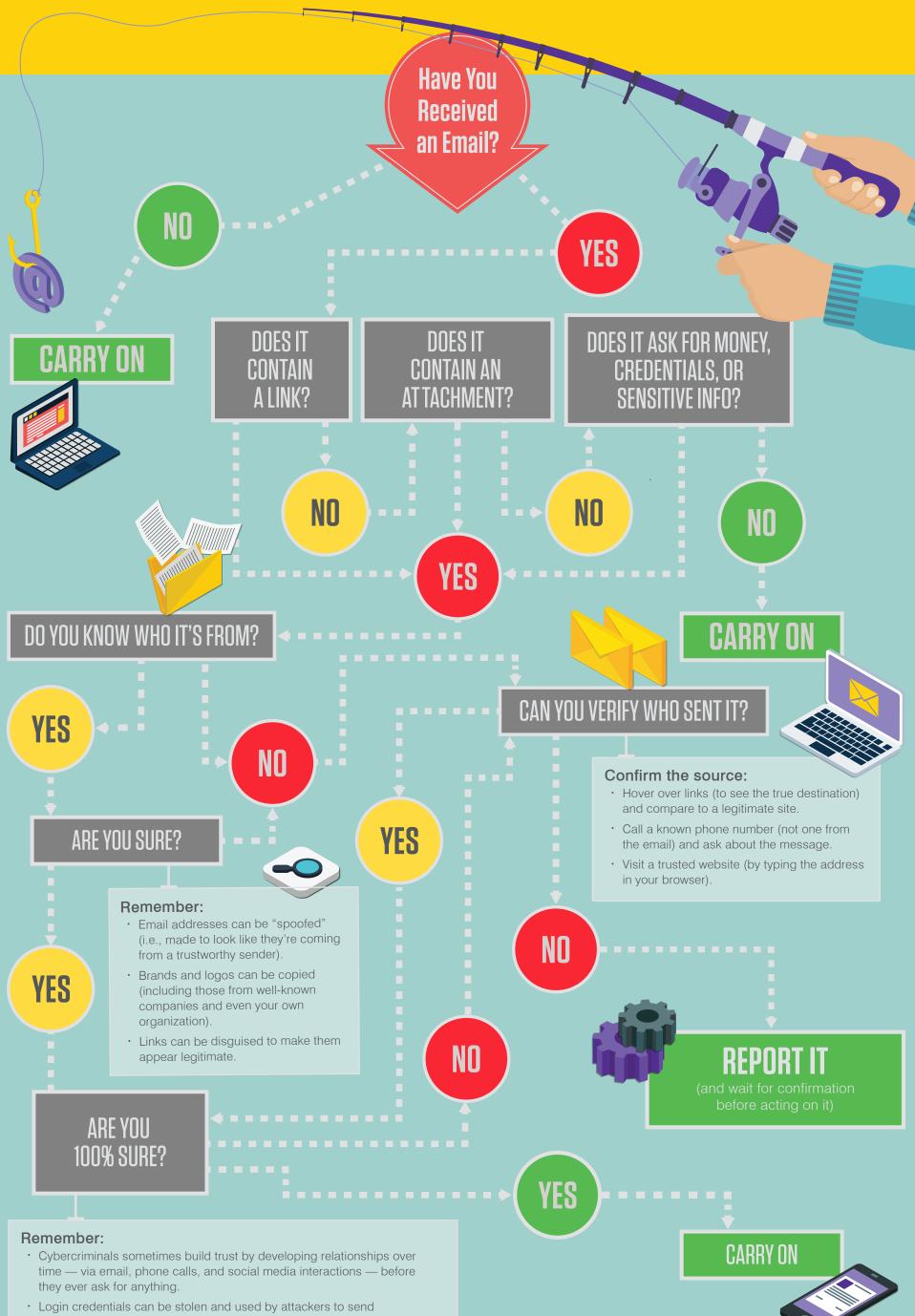# PRACTICAL ADVICE FOR AVOIDING PHISHING EMAILS

Phishing emails require one thing to be successful: For the recipient to take the bait. This "decision tree" is a helpful reminder that verifying unknown emails is an important step in protecting your data and devices.

Have You Received an Email?

NO → **CARRY ON**

YES

DOES IT CONTAIN A LINK?

DOES IT CONTAIN AN ATTACHMENT?

DOES IT ASK FOR MONEY, CREDENTIALS, OR SENSITIVE INFO?

NO — **NO** — **NO** → **CARRY ON**

YES

DO YOU KNOW WHO IT'S FROM?

CAN YOU VERIFY WHO SENT IT?

YES — **NO**

ARE YOU SURE?

YES

Remember:
- Email addresses can be "spoofed" (i.e., 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.

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

YES

NO

REPORT IT
(and wait for confirmation before acting on it)

ARE YOU 100% SURE?

YES → **CARRY ON**

Remember:
- Cybercriminals 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.