IDENTIFYING PHISHING EMAILS: STAY ALERT, STAY SECURE

SPOT THE PHISH BEFORE IT HOOKS YOU!

LEGITIMATE EMAIL
Key Features

- **Company logo** is high-quality and properly placed
- **Clear and Professional Language** (No urgency or threats)
- **Personalized Greeting** (e.g., Dear John,)
- **Safe Link** e.g.,(https://company.com/security)
- **Sender Email is Official** (e.g., support@company.com)

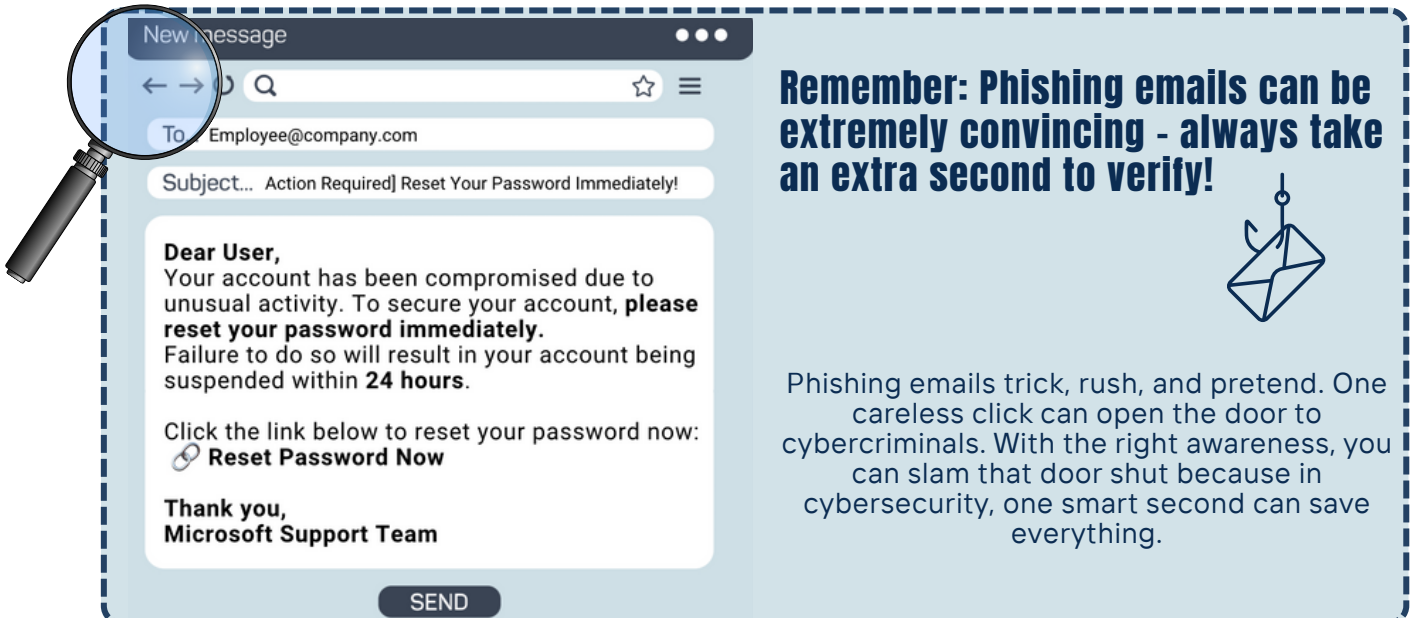
PHISHING EMAIL
Red Flags

- **Fake Company Logo** (off-brand, distorted, or pixelated)
- **Suspicious Sender Email (e.g., security-alert@companyxyz.com)**
- **Generic Greeting** (Dear User instead of a real name)
- **Urgent & Threatening Language** ("Your account will be locked in 24 hours!")
- **Mismatched Hyperlink** (Hovering over the link reveals a fake URL)

Spot that PHISH!

Can You Spot the Phishing Red Flags?

Look closely! There are at least 5 warning signs that this email is fake. Can you find them before clicking?

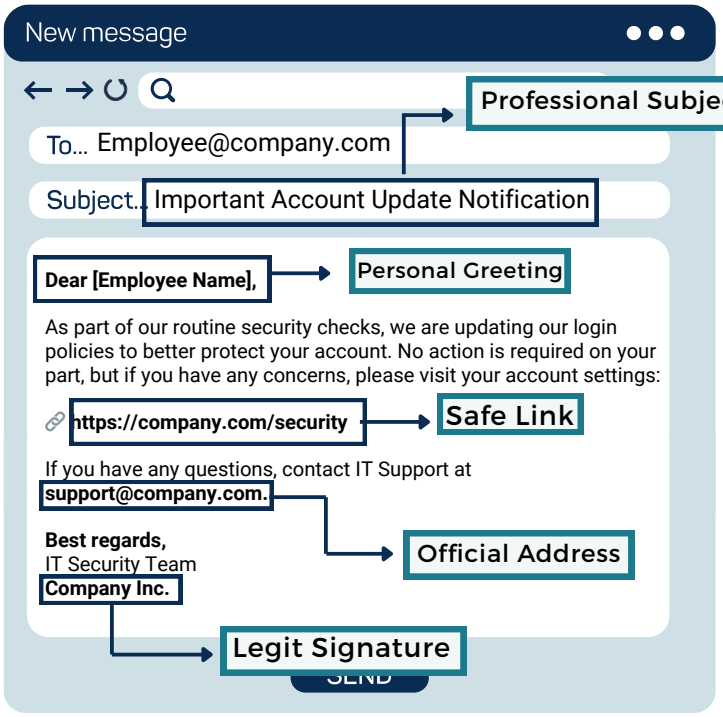


Remember: Phishing emails can be extremely convincing - always take an extra second to verify!

Phishing emails trick, rush, and pretend. One careless click can open the door to cybercriminals. With the right awareness, you can slam that door shut because in cybersecurity, one smart second can save everything.

Didn't Ace the Game? No Worries—Now's Your Chance to Level Up!

If you didn't spot all the red flags in the phishing email game, don't stress—this section is here to help. Take a closer look at this real email breakdown to understand what you might've missed and why it matters. Learning to recognize phishing tactics takes practice, and the more you know, the better protected you'll be. Use this as your quick guide to sharpen your eye and stay one step ahead of cyber threats.



Even the most well-meaning employees can fall for phishing emails, especially when messages appear urgent, official, or emotionally triggering. Cybercriminals count on human error — a quick click, a rushed decision, or a missed red flag. That's why continuous awareness, training, and a strong culture of caution are essential to keeping your organization secure.

Answer Key - 5 Red Flags in the Email

1. **Fake Sender Address** – security@microsoff-support.com (Notice the typo: "microsoff" instead of "microsoft").
2. **Misspelled Company Name** – Microsoft is misspelled in the sender email and the link.
3. **Urgent Call to Action** – "Your account will be suspended in 24 hours!" (Phishing emails often create a sense of panic).
4. **Suspicious Link** – Hover over the "Reset Password Now" link. It does not lead to Microsoft's official website but to a fake URL (microsoff-security-update.com).
5. **Poor Grammar & Formatting** – The greeting is generic ("Dear User" instead of addressing you by name), and the email has odd sentence structures that a real Microsoft email wouldn't use.

DON'T TAKE THE BAIT — THINK BEFORE YOU CLICK!