TECH4 ME2

TECH ISN'T A 4-LETTER WORD

Tech4Me2 Quick Guide

Phishing Emails Quick Reference Guide

What to look for, what to do, and how to protect yourself

JOHN CLITES

What are "phishing emails"?

Phishing emails are specifically designed to obtain information from you, most often credit card information or login credentials for an account. They represent the largest threat when using email, and are possibly your biggest online threat, period. The good news is that, although phishing emails, are increasingly sophisticated, you can generally spot them—if you know what to look for.

How to Spot Phishing Emails

Phishing emails virtually always exhibit one or more "tells". Look for the following:

•Urgent or threatening language ("Act now," "Your account will be closed")

• Requests for personal or financial information

• Suspicious links or unexpected attachments

• Email address that doesn't match the company

• Generic greetings ("Dear Customer")

• Spelling or grammar mistakes

• Messages that just don't feel right

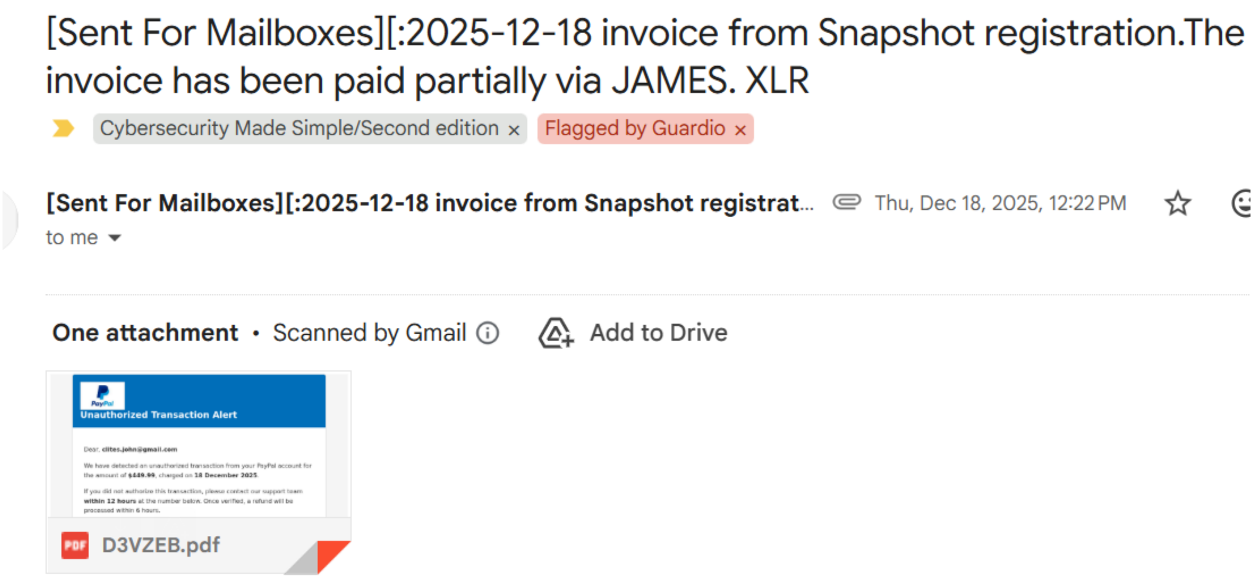
→ ***When in doubt, don't click.***

On the following pages, you'll see examples of some of the most common types of phishing emails used today.

1. "Your Account Is Delinquent"

You're told you must pay immediately or your account will be closed. A link or phone number is provided.

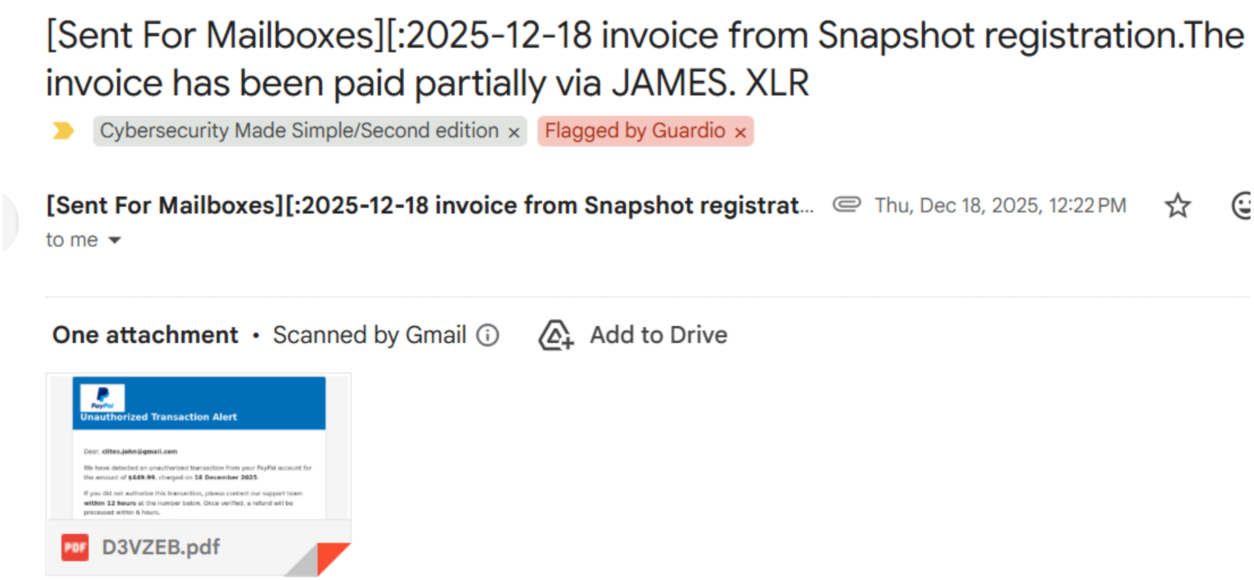
Watch for: Urgency, threats, and unfamiliar links.



2. “Invoice Attached” (Malware Trap)

An email claims you owe money and includes an attachment. Opening it may install harmful software.

Watch for: Unexpected invoices or attachments you weren’t expecting. Never open any attachment in these suspect emails.



3. "Your Account Was Compromised"

You're warned about a data breach and told to log in right away using a provided link.

Watch for: Messages that push you to "secure your account" immediately.

🚨 YOUR ACCOUNT IS ON LOCKDOWN Phishing ×

Your Wallet <info@signalheadline.com> Sun, Mar 15, 6:02 AM (2 days a

to me

Hey John,

Security breach attempt detected on your profile linked to clites.john@gmail.com.

Systems have auto-locked the account.

Restore full control before the 24-hour window closes or all files and settings will be archived indefinitely.

Immediate verification required.

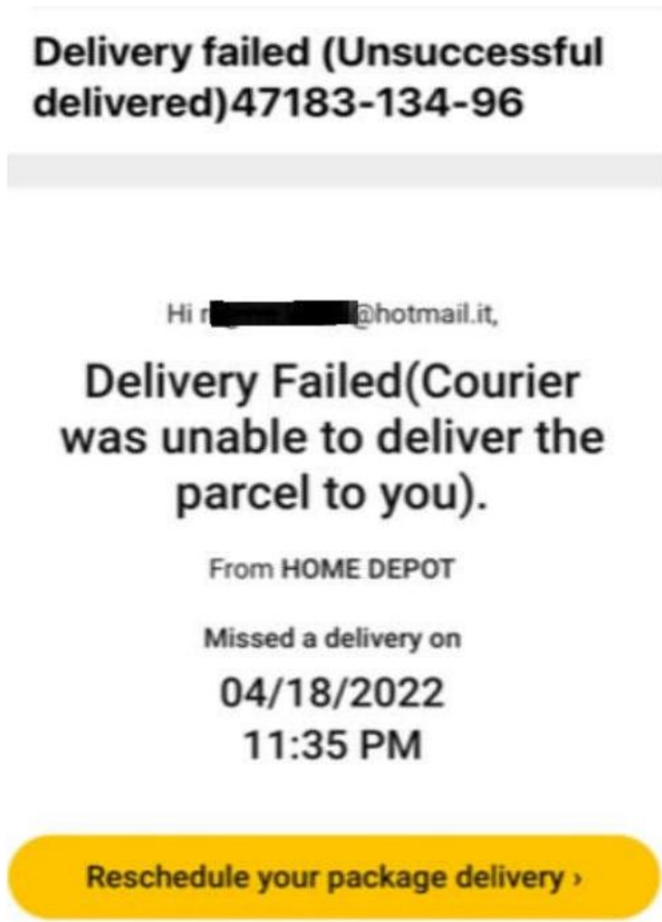
Thanks,

Your Wallet

4. "Delivery Problem"

A message says a package couldn't be delivered and asks you to click a link or pay a small fee.

Watch for: Messages about packages you weren't expecting.

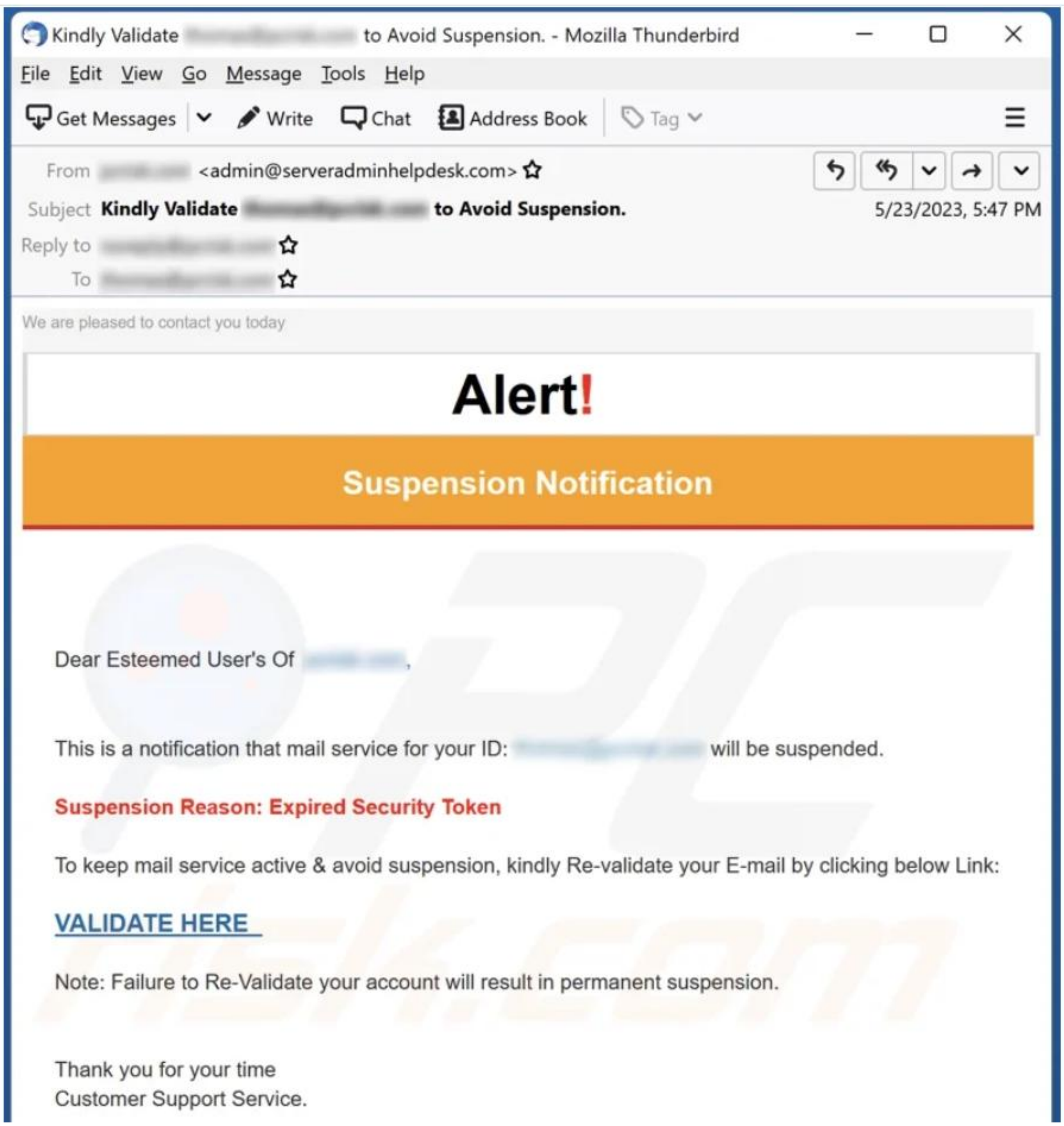


If you click on the button, you'll be requested to pay a fee.

5. "Password Expiring / Account Suspension"

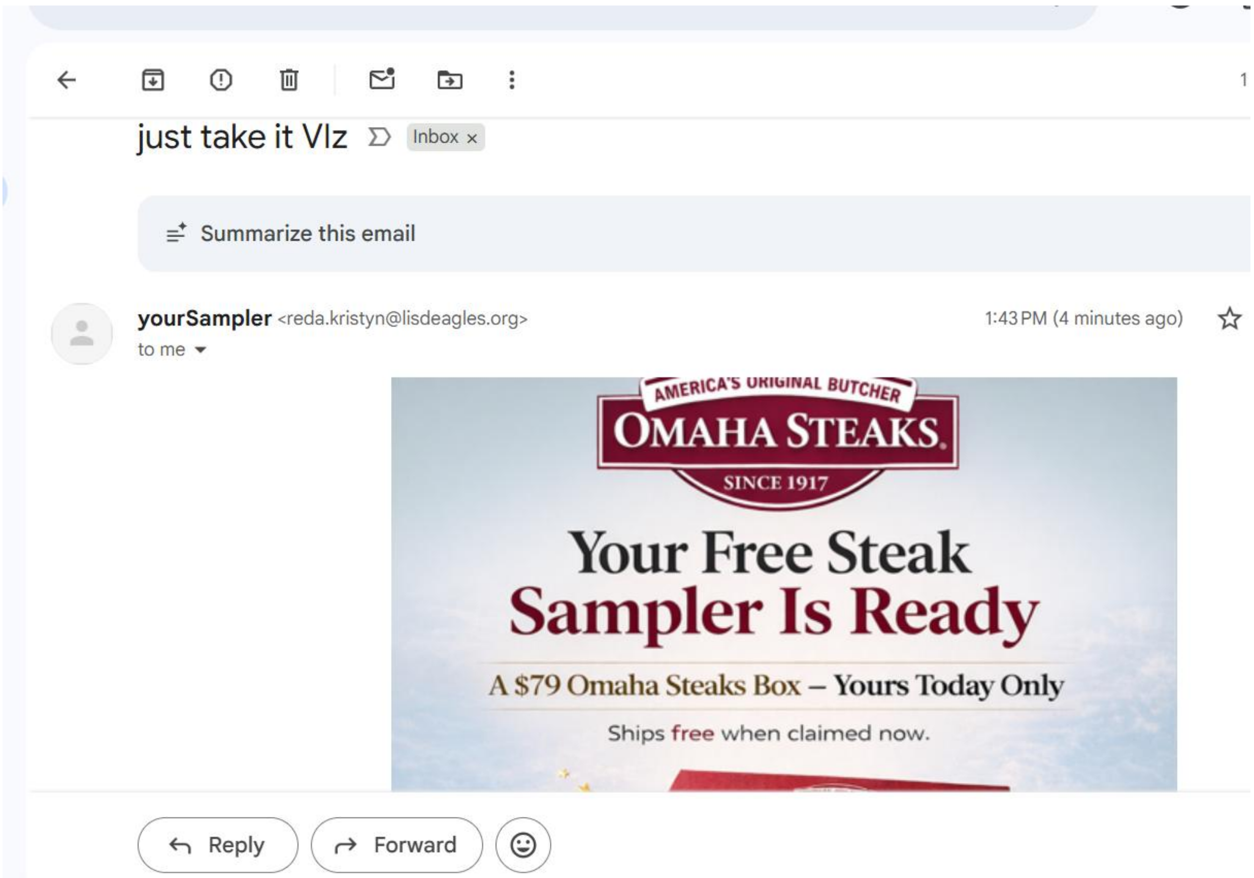
You're told your email or account will be locked unless you update your password now.

Watch for: Generic greetings and urgent instructions to click a link.



6. "Refund or Reward"

You're offered money, a rebate, or a prize—but must "verify your information" first.
Watch for: Offers that seem unexpected or too good to be true.



One Rule That Will Protect You Most of the Time

Never click links or open attachments in unexpected emails.

Links may redirect you to a "spoof" site (scam site designed to look authentic). Clicking an attachment may release malware onto your computer.

Instead:
- Go directly to the company's official website
- Or use your saved bookmark
- Or call the company using a known phone number

Quick Safety Checklist

Before you click anything, pause and ask:
- Was I expecting this message?
- Is there pressure to act quickly?
- Does the sender's email look slightly off?
- Does the message contain spelling or grammar mistakes?
- Am I being asked for personal or financial information?

If something feels off, trust that instinct.

A Quick Note

If this guide helped you, you may also enjoy the Tech4Me2 courses and additional guides available at **www.tech4me2.com** on the Products Library and Freebies pages.

Have a topic you'd like explained in plain English? Email me at **john@tech4me2.com**