TECH4 ME2
TECH ISN'T A 4-LETTER WORD

Tech4Me2 Action Guide

Phishing Emails: What to Look for- and What to Do

Real-world examples and simple steps to help you recognize scams and stay safe

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

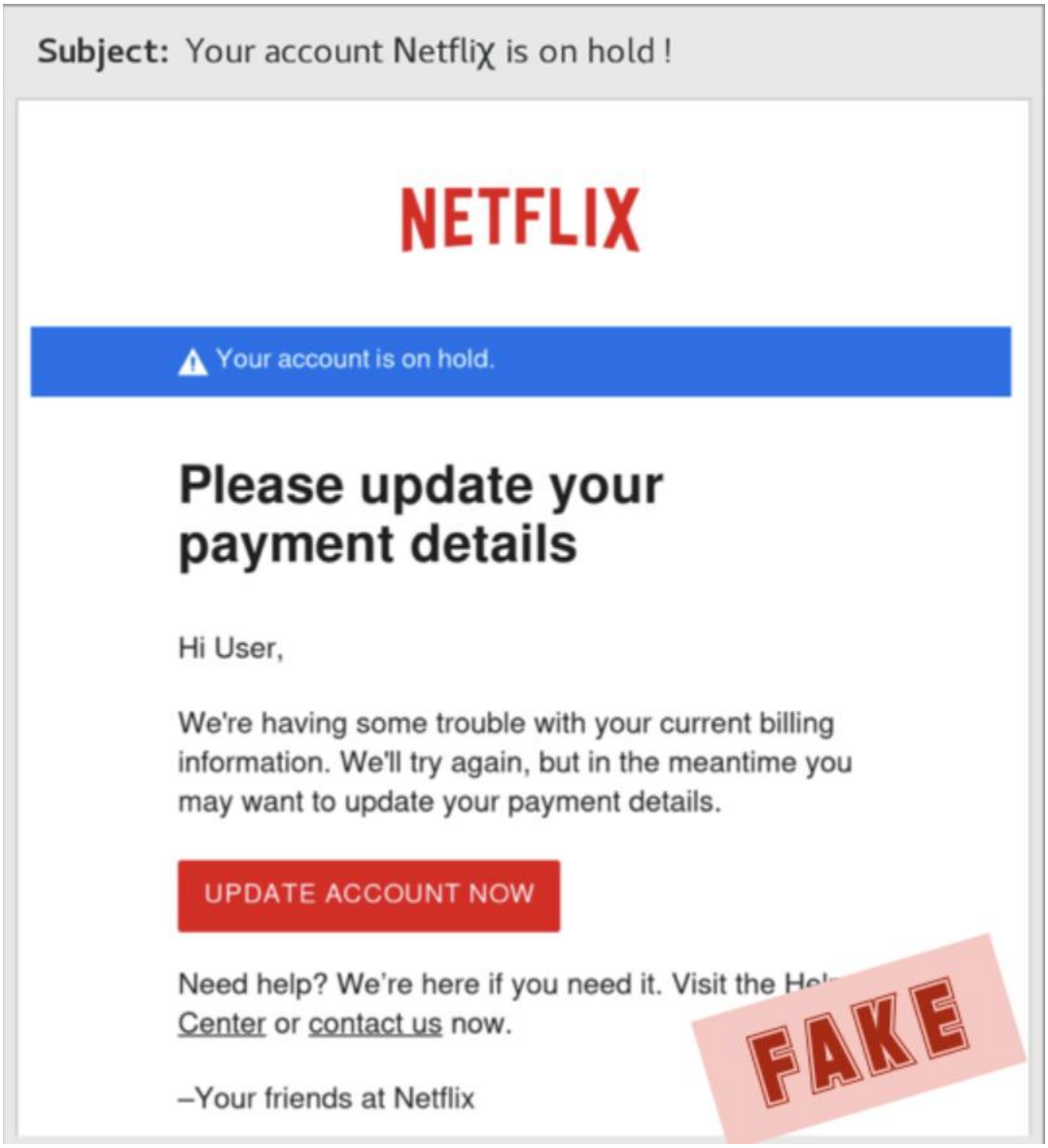
→ ***When in doubt, don't click.***

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

1. "Your Account Hase Been Suspended/Will Be Closed"

You're told your account will be closed because payment failed.

Watch for: Urgency, threats, and unfamiliar links.

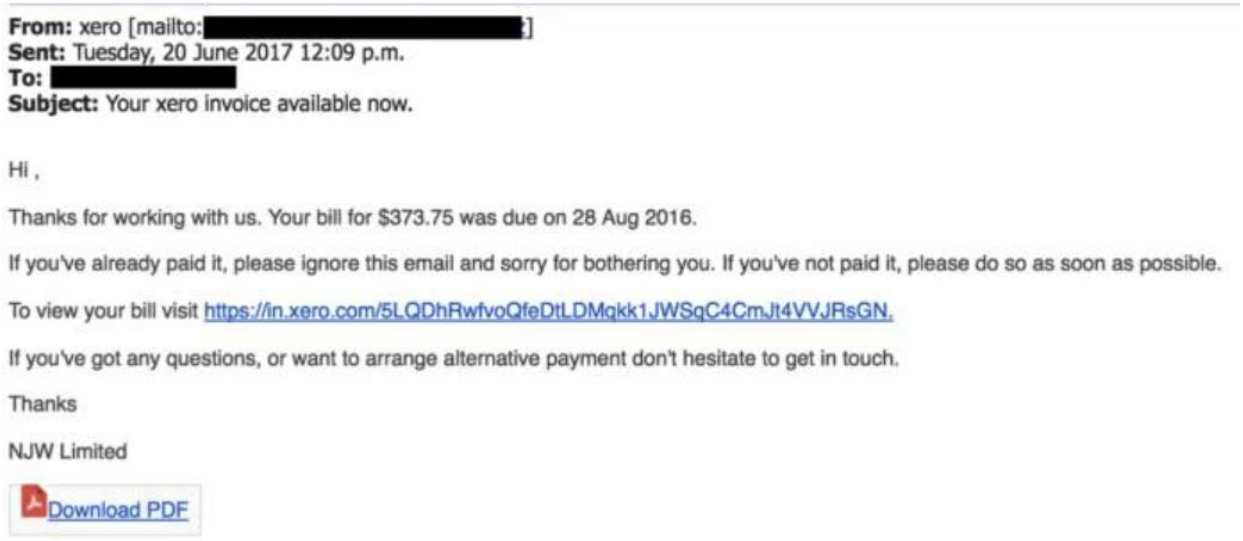


There are many variations of this common scam. In this version, the recipient is notified that their payment failed and they must update their payment information. Clicking the button in fact redirects to a spoof site designed to look like the actual Netflix site.

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. Often these emails purport to come from Netflix, PayPal, or other big-name companies which many people have accounts with.



From: xero [mailto:[redacted]]
Sent: Tuesday, 20 June 2017 12:09 p.m.
To: [redacted]
Subject: Your xero invoice available now.

Hi ,

Thanks for working with us. Your bill for $373.75 was due on 28 Aug 2016.

If you've already paid it, please ignore this email and sorry for bothering you. If you've not paid it, please do so as soon as possible.

To view your bill visit https://in.xero.com/5LQDhRwfvoQfeDtLDMqkk1JWSqC4CmJt4VVJRsGN.

If you've got any questions, or want to arrange alternative payment don't hesitate to get in touch.

Thanks

NJW Limited

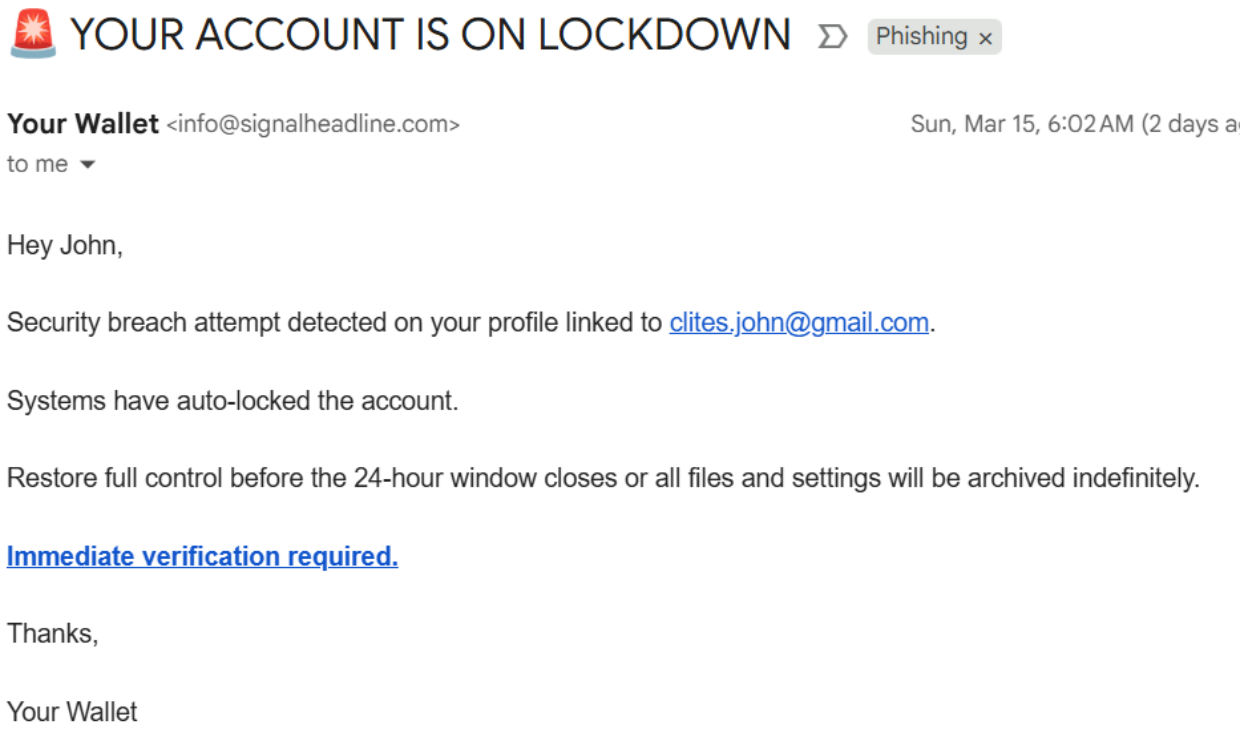
Download PDF

First ask yourself if the email is unexpected. Do you even have an account with this company? Note that this email includes both a link and a PDF attachment, increasing the odds of catching someone.

3. "Your Account Was Compromised"

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

Watch for: Messages that push you to "secure your account" or "verify your information" 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,

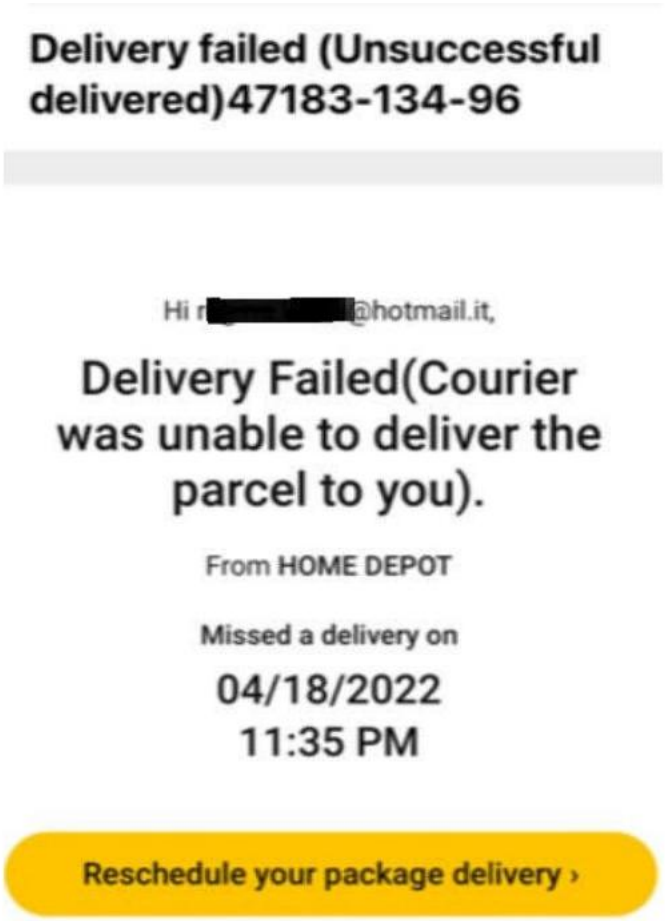
Your Wallet

This is a clever email. Note the subject line is all caps in a large font. Also, the reason that the reason has been locked the account is due to a data breach, which unfortunately are common these days. Many people have received notifications that their data may have been compromised, making this email seem more credible.

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.

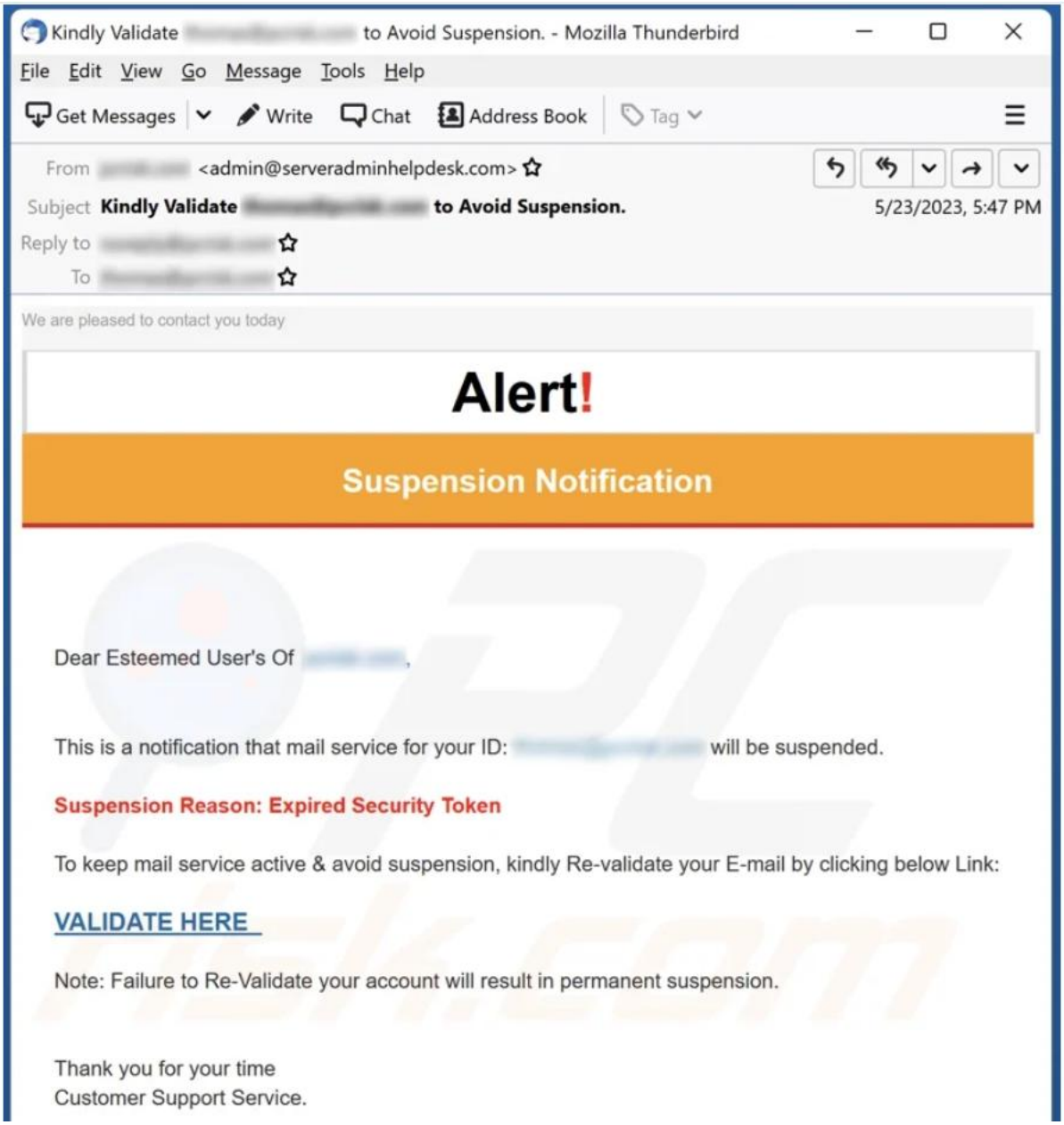


If the recipient clicks on the button, they will be requested to pay a fee. This message purports to come from Home Depot. Walmart, Fedex, UPS, and USPS are also common "senders".

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.

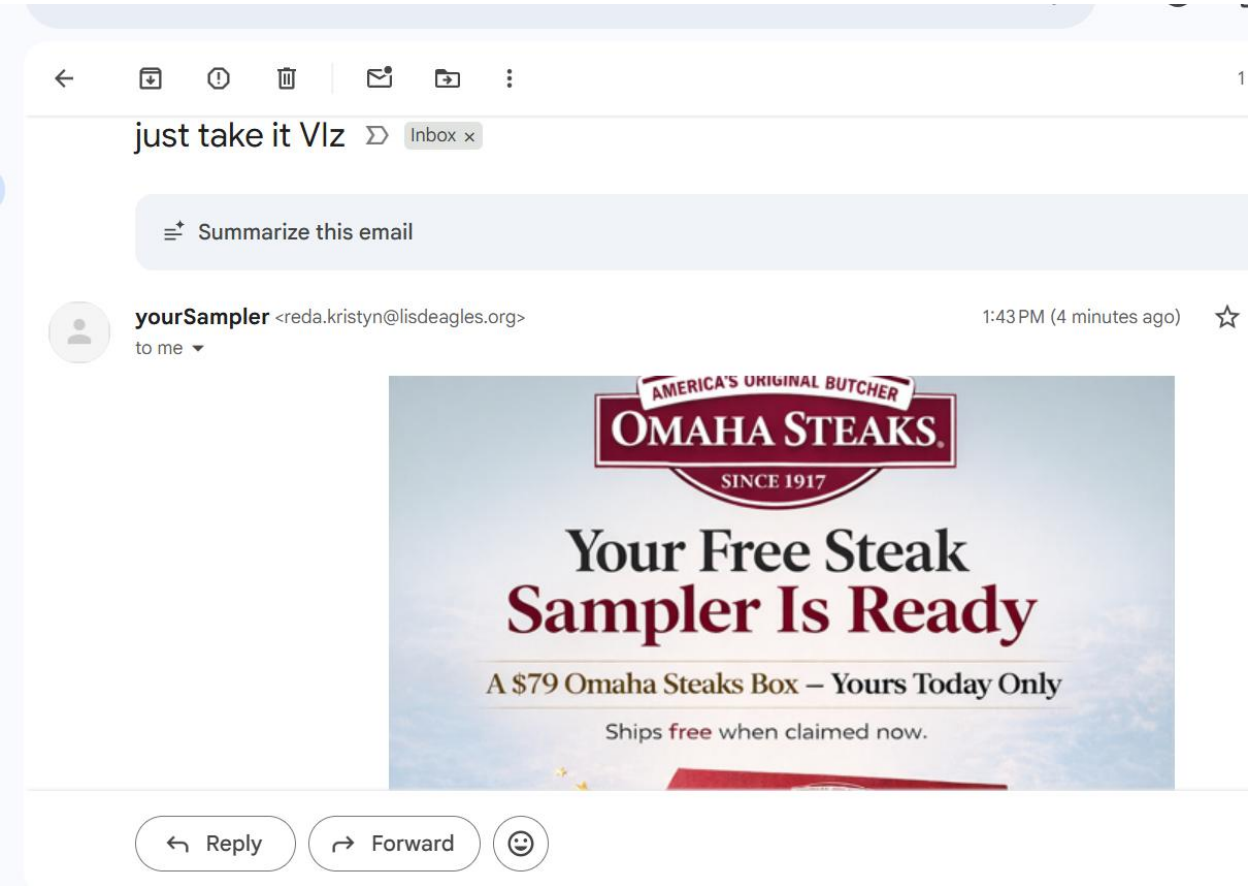


Note the generic – and grammatically incorrect – greeting. No reason is given. The supposed sender is not even clearly identified. Also note the threat of "permanent suspension".

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.



Note the odd subject line. And the sender's email address doesn't relate to Omaha Steaks. Omaha Steaks is a well-known brand, and the image might at first appear to be genuine, but in the actual email it appears a bit less sharp than it should.

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 directly at **john@tech4me2.com**