

Spotting a Scam Email

A simple guide to help you stay safe when reading your emails.

Knowing what to look for can help stop scams before they start.

Common Signs of a Scam Email




Look out for emails that:

- Say there's a **problem with your account**
 - Tell you to **act fast** or **click quickly**
 - Ask you to **confirm personal details** like passwords or bank info
 - Include **unexpected attachments or links**
 - Come from a **strange-looking email** address (e.g. info@amaz0n-pay.support)
-

What You Can Do

- **Don't click anything** unless you're sure
 - **Check the sender's address** — not just the name
 - **Ignore the pressure** — real companies won't rush you
 - **Look for spelling mistakes** or strange formatting
 - **Ask someone you trust** if you're unsure
-

If You Think It's a Scam

-  Do not reply
 -  Do not open attachments or click links
 -  Do not forward it
-

Still not sure?

 You can call or text Cyber Shoulder (07440 602 591)

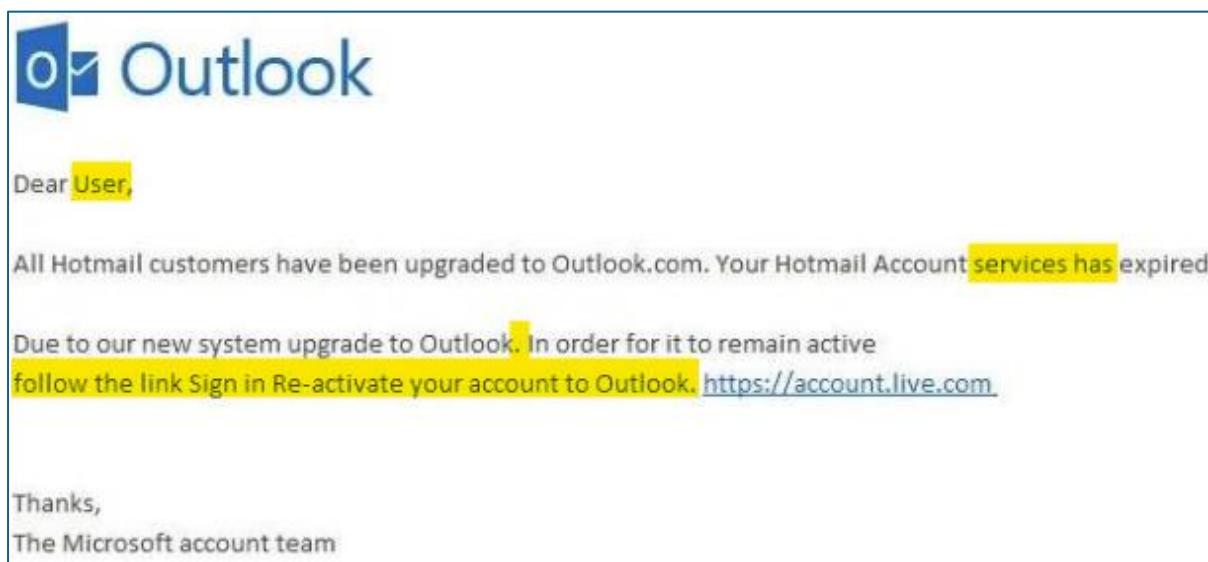
...or speak to someone you trust.

We'll listen without judgment and help you take the next step.

Examples of Scam Emails

Below are examples of scam emails. We've highlighted indicators on each example that are commonly seen within fake emails.

Example 1:



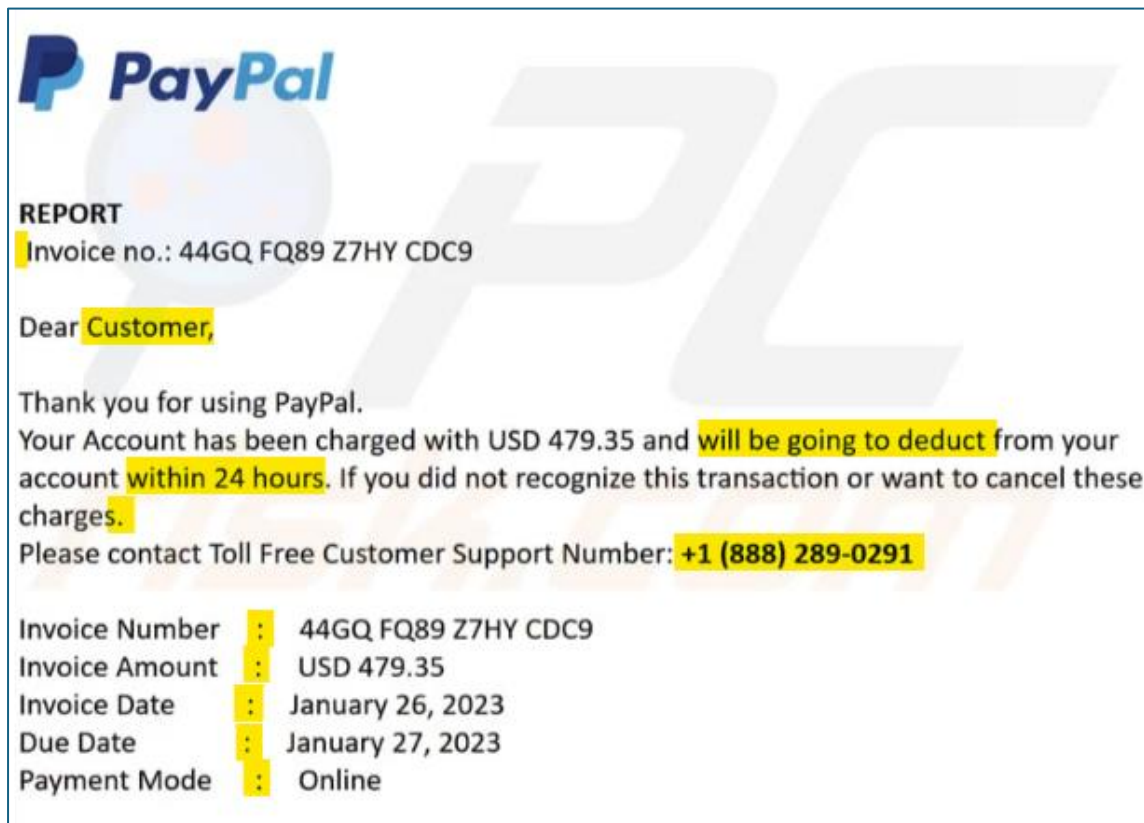
Indicators:

1. The email does not address you by name.
2. The grammar and punctuation of the email is poor.
3. The email includes a call-to-action and a link.

Summary:

Scammers want you to click the link and enter your login details on a fake page. Once they have collected your information, they lock you out, steal your data, sell it, and target your contacts with more scams.

Example 2:



Indicators:

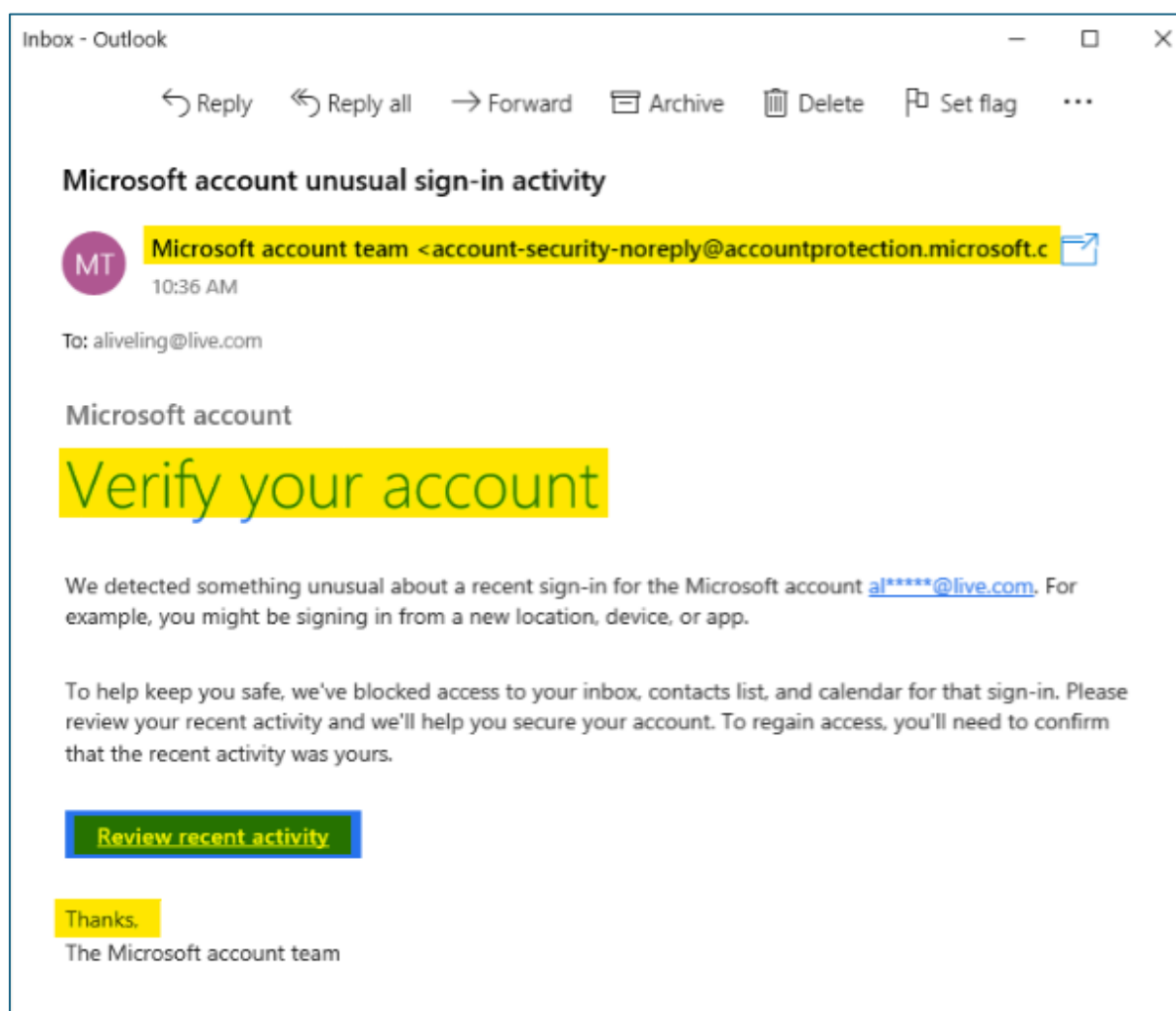
1. The logo may be wrong or low quality.
2. The email does not address you by name.
3. The grammar and punctuation of the email is poor.
4. The email instils fear to the reader such as saying money will be taken.
5. The email instils urgency to the reader such as a deadline.
6. The email provides a contact number. Always look for contact information yourself and do not use the information provided.

Summary:

Scammers know they have a better chance of deceiving you if they can talk to you on the phone and push you to make a quick decision. This scam email is crafted specifically for that.

But if you stay vigilant, you'll spot the key indicators of a PayPal scam. The PayPal logo appears pixelated, suggesting it was lifted from another website. It tries to create urgency by threatening consequences if you delay. There's a fake phone number included to supposedly cancel a fraudulent order.

Example 3:



Indicators:

1. The email uses a generic greeting.
2. The email does not originate from a company or email you expect.
3. The email instils fear to the reader such as saying your account is locked.
4. The links are obfuscated so you do not clearly where you are going.

Summary:

Cybercriminals use fear and urgency to make you act quickly. The email claims there has been suspicious activity on your account and provides a link to a fake login page.

Once you enter your credentials, they capture them. Be cautious of alerts about unusual activity, links to fake login pages, generic greetings and requests for sensitive information.