Ratcliff IT's Phishing Quiz.

Get better at spotting phishing scams. Boost your cybersecurity instantly.

We'll show you the crafty techniques cybercriminals use to breach your security systems.

Read on to see how good (or bad) your cyber awareness might be.

Why is cybersecurity important?

Because cybercrime costs money and doesn't just happen to big businesses or governments.

Cybercriminals cost the UK an estimated £27 billion a year.

In 2020, phishing attacks rose by 600%.

COVID and the rise of remote work playing a large factor with the 2nd point.

Cyber attacks, be they from phishing attacks or otherwise, cause data losses, reputational damage, revenue losses, and more. This makes preventing cyber attacks much cheaper than recovering from them. It also makes cybersecurity something no business can afford to ignore.

Why you need cybersecurity training

One of the key pillars of good cybersecurity is employee training. Your employees are your first and weakest line of defense against security breaches. It's much easier to fool an employee than it is a firewall.

This is why the government offers its own cyber awareness certification

Cyber Security Essentials is a Government backed scheme to help protect your organisation. When you take part in the program you can:

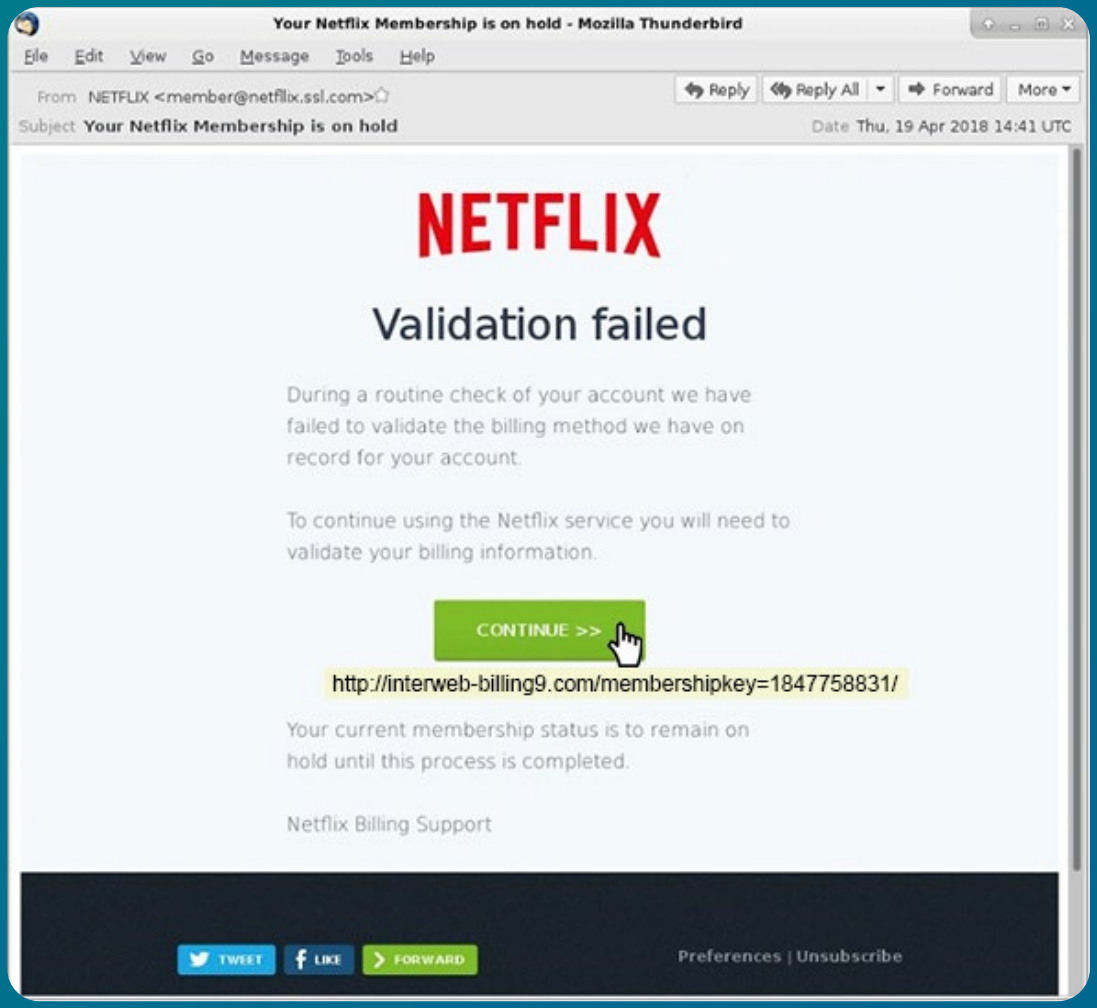
- ✔ Assure your customers that you're doing everything to secure your IT from cyber attacks
- ✔ Attract new business with the promise you have cyber security measures in place
- ✔ Get a clear picture of your organization's cyber security level

Plus, with some organisations, getting Cyber Security Essentials certified is mandatory by law.

Ratcliff IT offers training to help any organisation become more cyber aware and have every chance of becoming certified.

To find out if you'd benefit from cybersecurity training, test you and your team's cybersecurity skills, Ratcliff IT has created a quiz to spot phishing scams; one of the most common forms of cyber attacks. Read on to see just how much – or how little – you know about phishing scams and how at risk you might be to inviting malware into your networks.

1) What looks fishy?

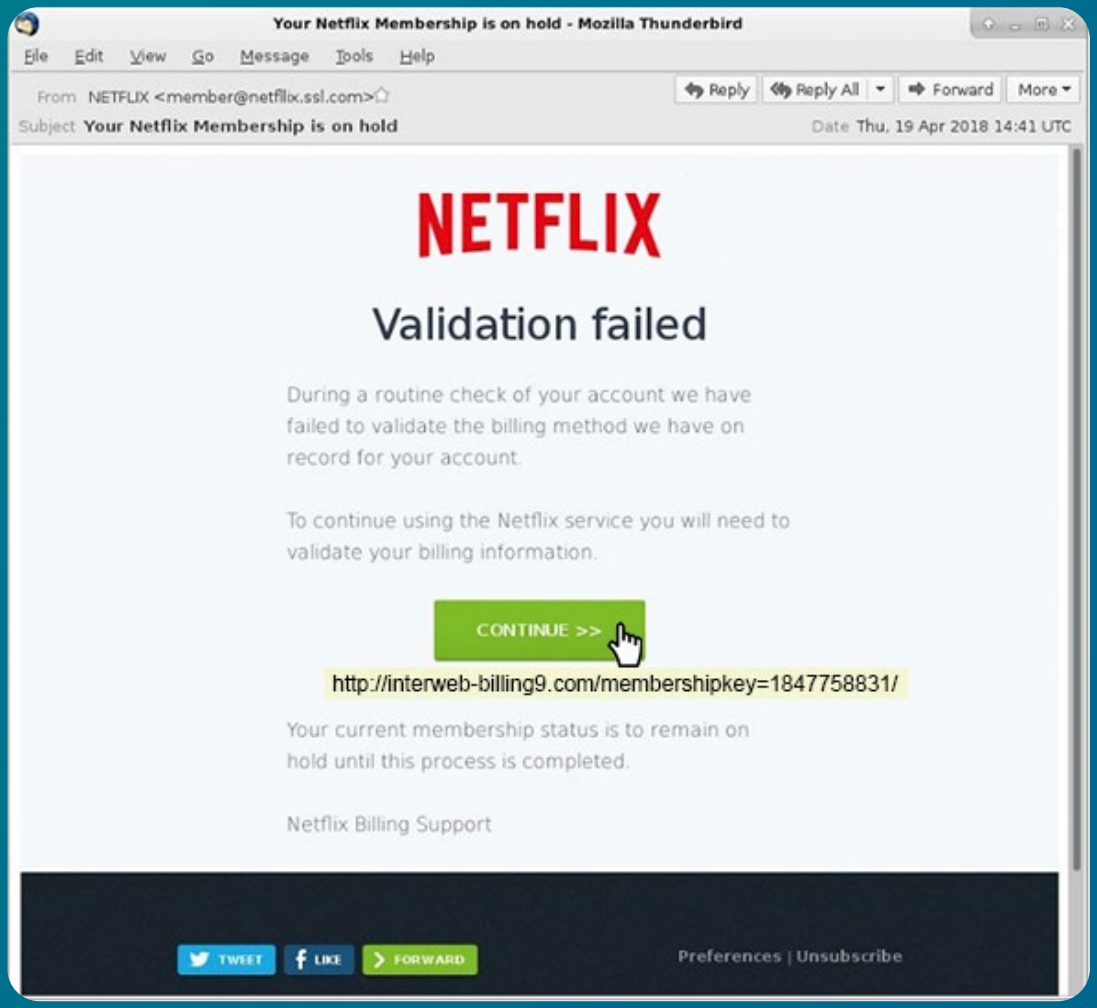


A) Netflix logo is wrong

B) Bad spelling

C) Suspicious link

ANSWER:

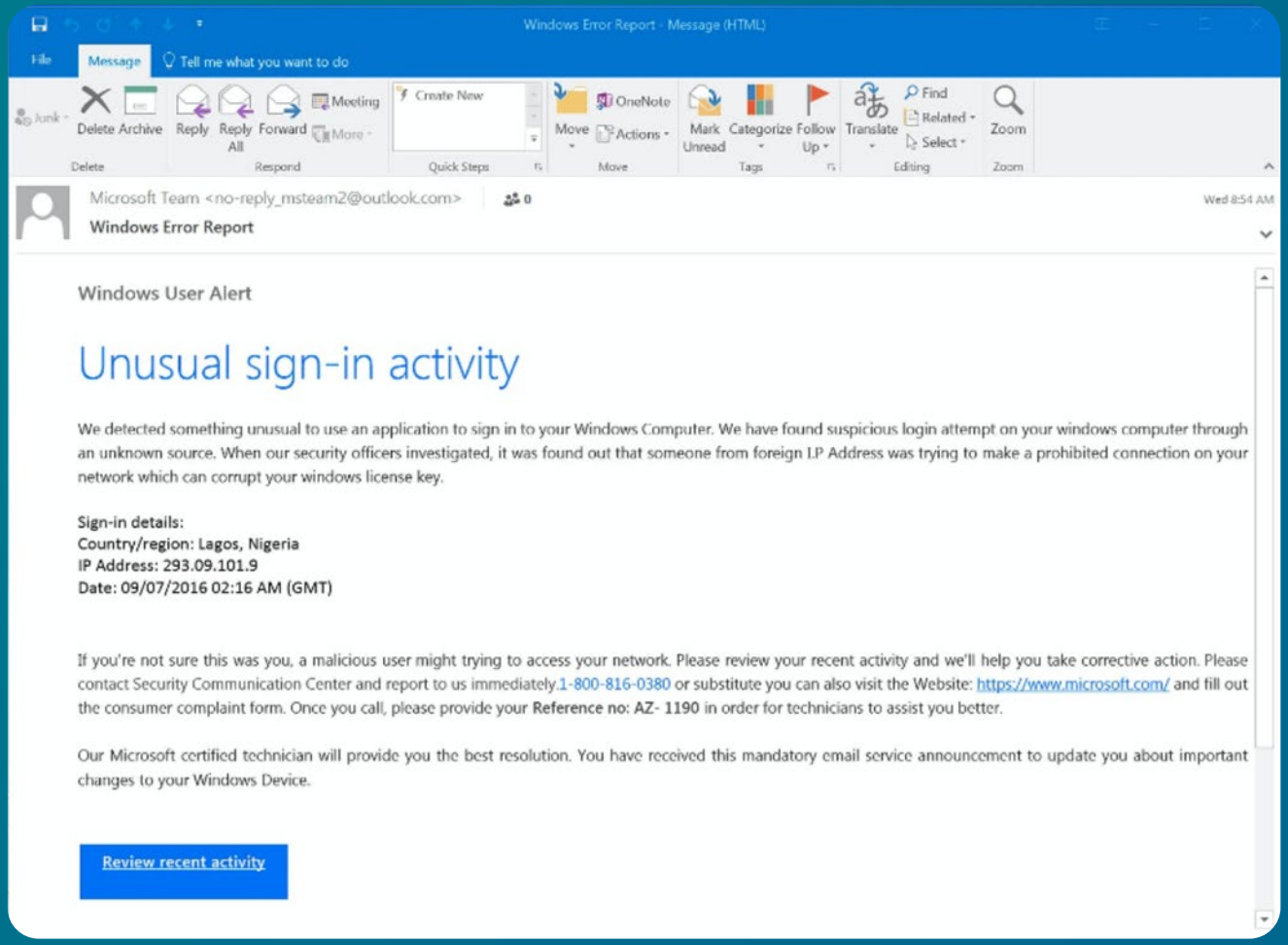


C) Suspicious link

When you get an email from Netflix, you'd expect something like 'netflix.com' to be the link address. Here you can clearly see you're being linked to another destination. In other emails, the scammer may be smart enough to hide a link within a button.

Lesson: never click on a link where the address doesn't seem 100% legitimate.

2) What looks fishy?

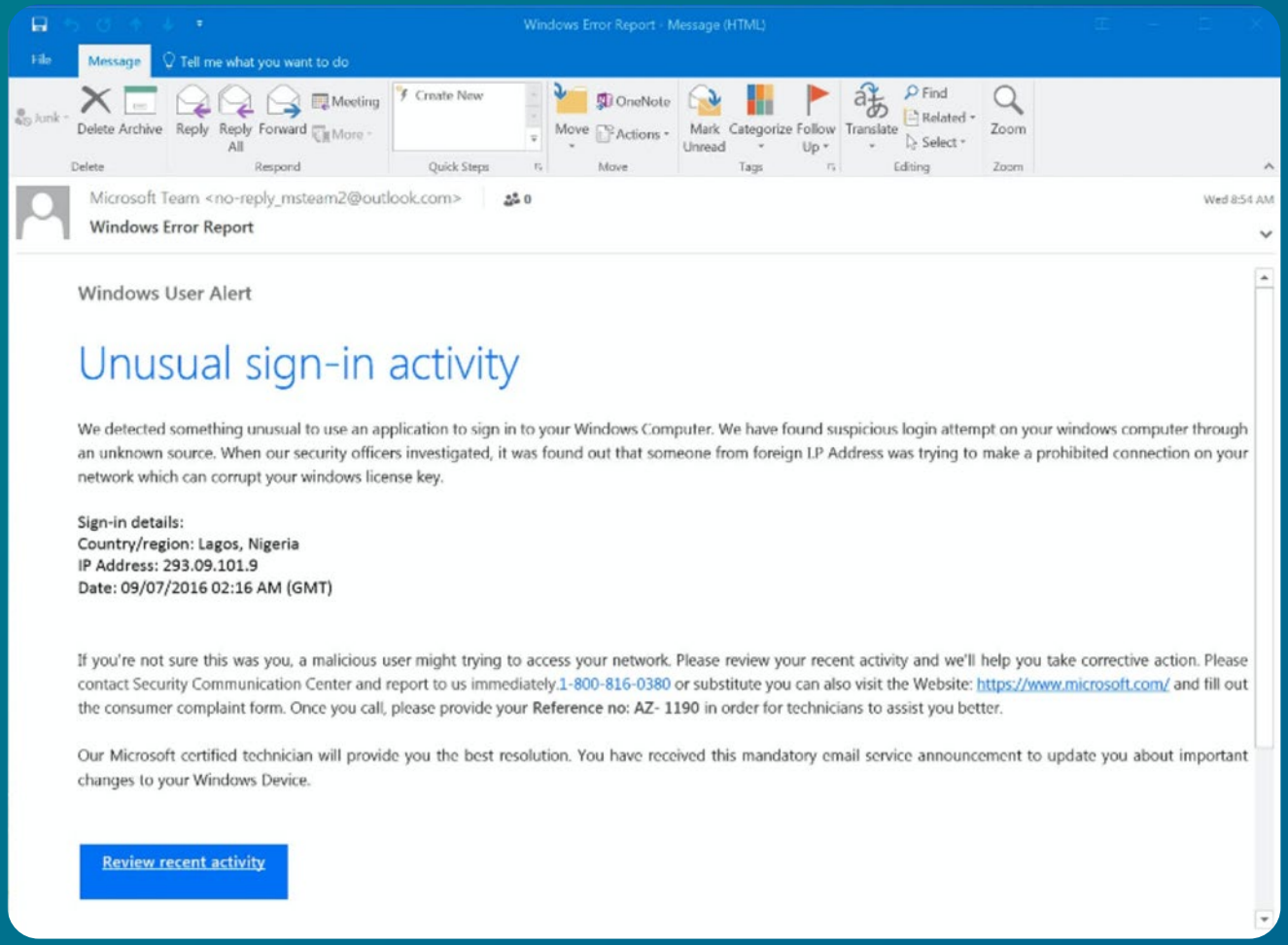


A) Poorly written email

B) No Microsoft logo

C) Not addressing the customer personally

ANSWER:

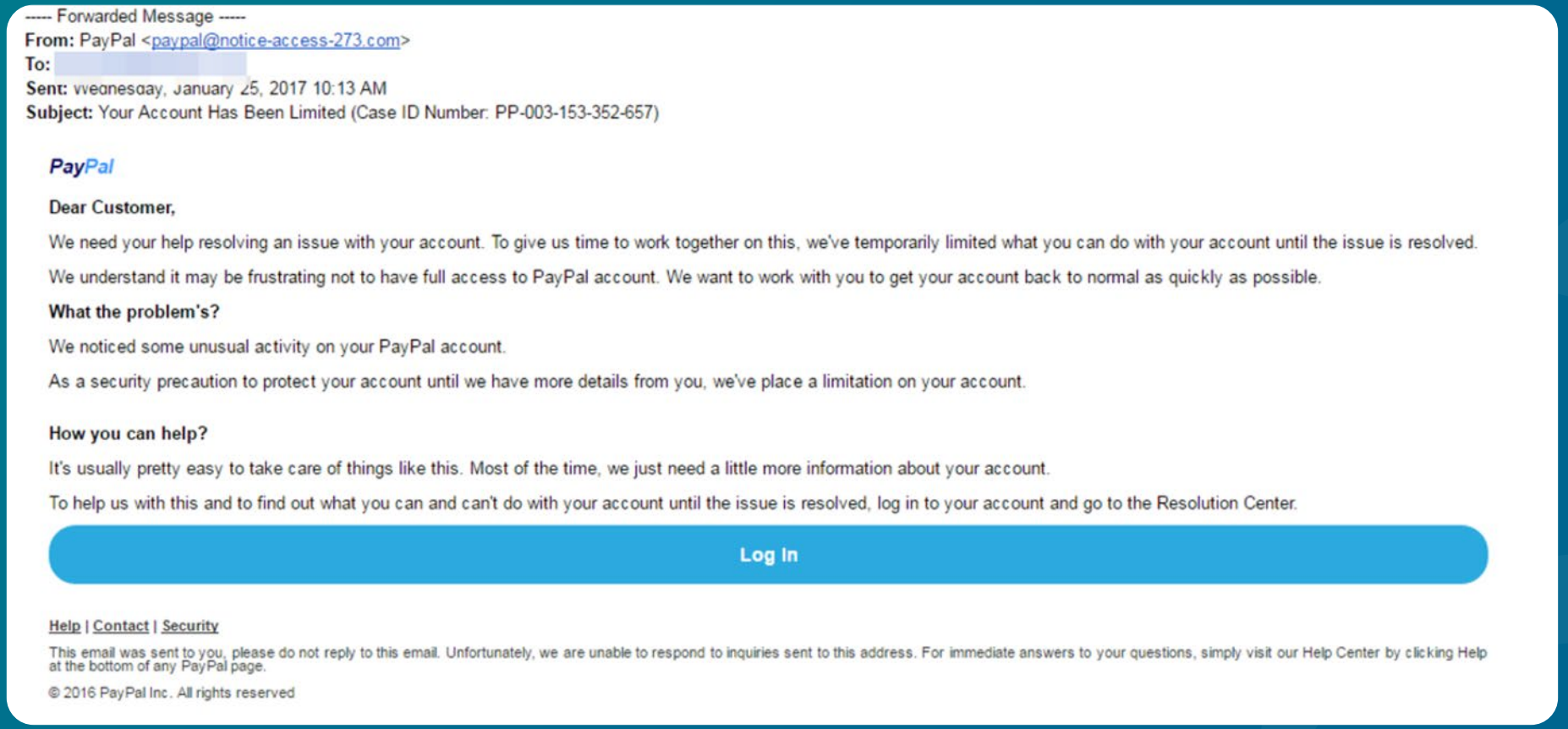


A) Poorly written email

Whilst no individual word is spelled wrong, the message is full of grammatical errors. No native speaker would make these mistakes. There are also strings of missed words, such as in “a malicious user might trying to access” or “please contact security communication center.”

Lesson: if its spelling or grammar is in any way off the mark, delete immediately.

3) What looks fishy?



----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

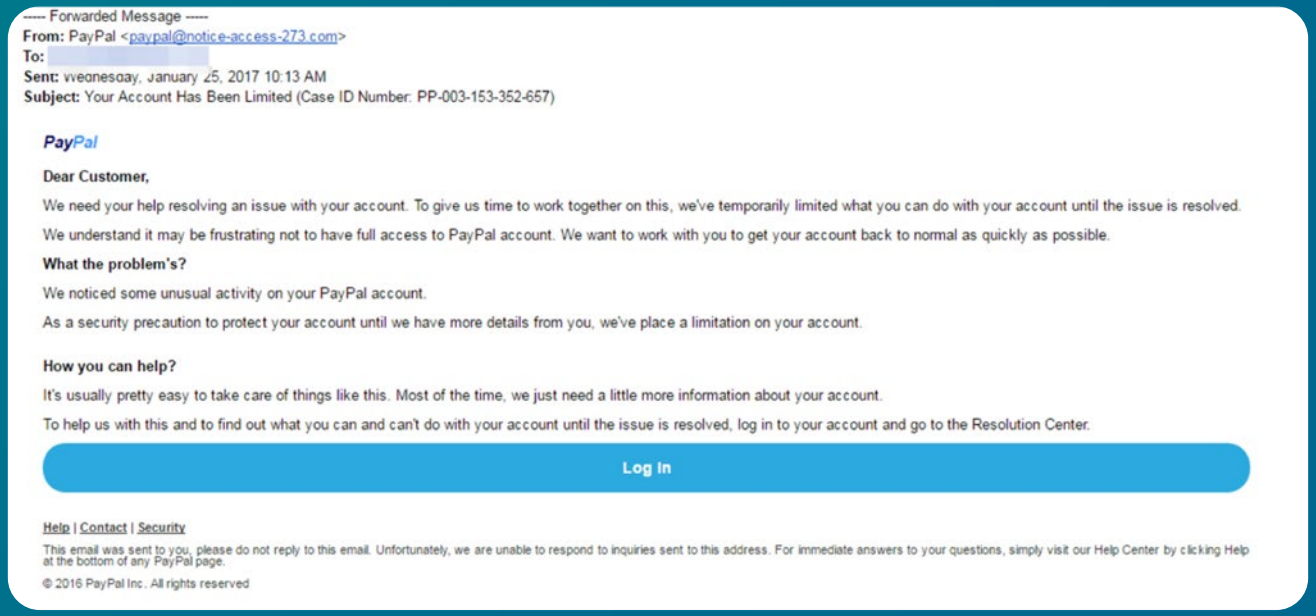
© 2016 PayPal Inc. All rights reserved

A) Wrong email domain

B) Not addressing the customer personally

C) Wrong logo

ANSWER:



----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

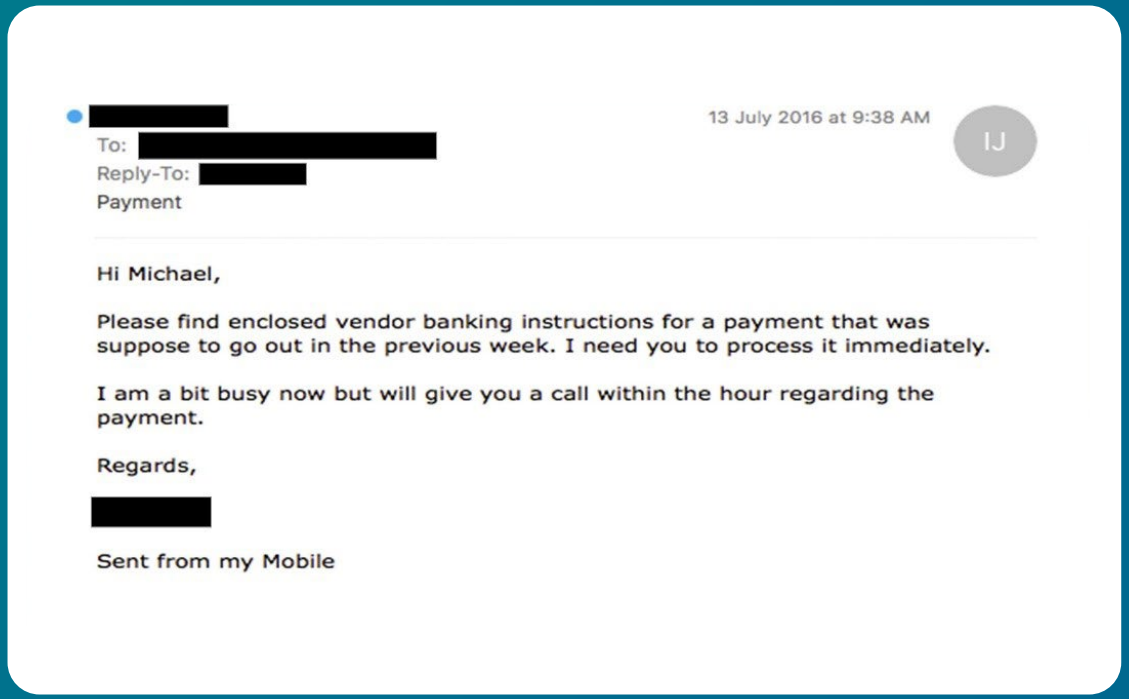
A) Wrong email domain

This is almost a perfect attempt. There's a half-decent logo at the top and there's a believable request. Still, the sender's address is 'payapal@notice-access-273.com.'

A genuine email from PayPal would have the organisation's name in the domain and indicate that it's come from someone @PayPal.

Lesson: if the business isn't in the domain, it's a scam.

4) What looks fishy?



[redacted]

13 July 2016 at 9:38 AM

IJ

To: [redacted]

Reply-To: [redacted]

Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

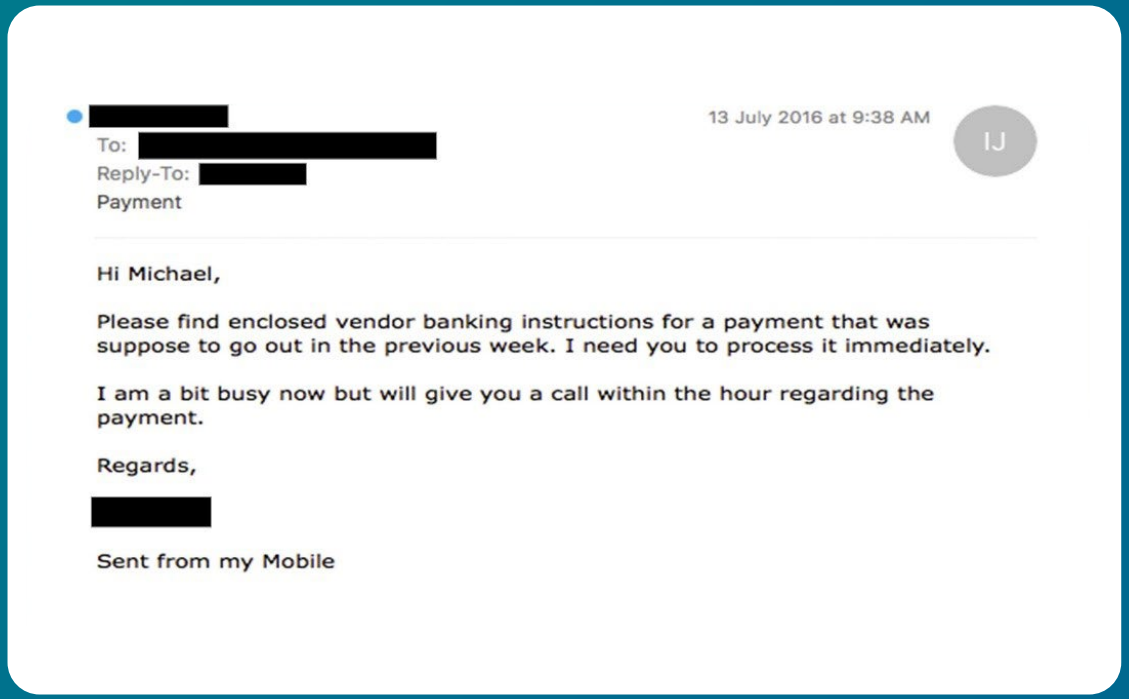
Sent from my Mobile

A) “Sent from my Mobile”

B) Bad grammar

C) A sense of urgency

ANSWER:


[redacted]

13 July 2016 at 9:38 AM

IJ

To: [redacted]

Reply-To: [redacted]

Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

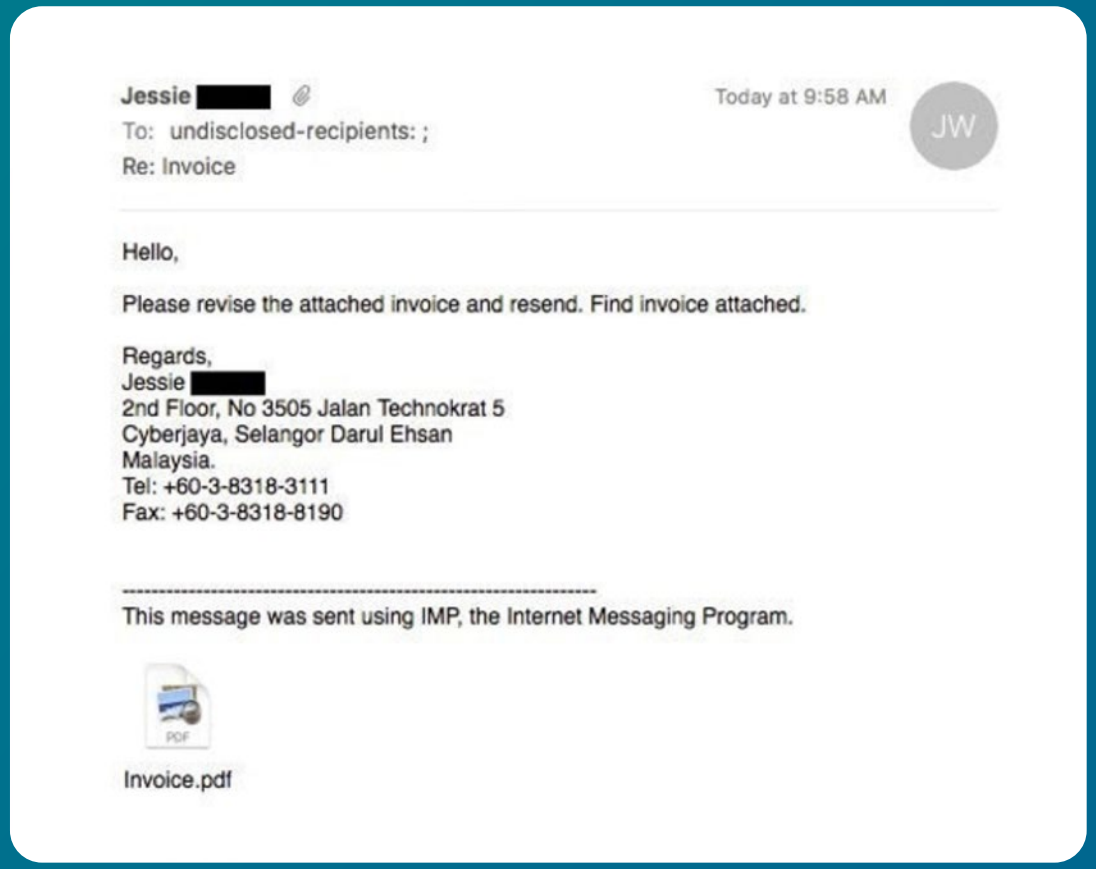
C) A sense of urgency

Scammers want you to act fast without thinking. The longer a victim must think, the more likely they are to notice things that don't seem right.

The command 'process it immediately' is ridiculous. People often don't check their emails for days. No legit outfit will require such a rush.

Lesson: if an email is demanding swift action, it's trying to steal your money.

5) What looks fishy?



Jessie [redacted]

To: undisclosed-recipients: ;

Today at 9:58 AM

JW

Re: Invoice

Hello,

Please revise the attached invoice and resend. Find invoice attached.

Regards,
Jessie [redacted]
2nd Floor, No 3505 Jalan Technokrat 5
Cyberjaya, Selangor Darul Ehsan
Malaysia.
Tel: +60-3-8318-3111
Fax: +60-3-8318-8190

This message was sent using IMP, the Internet Messaging Program.

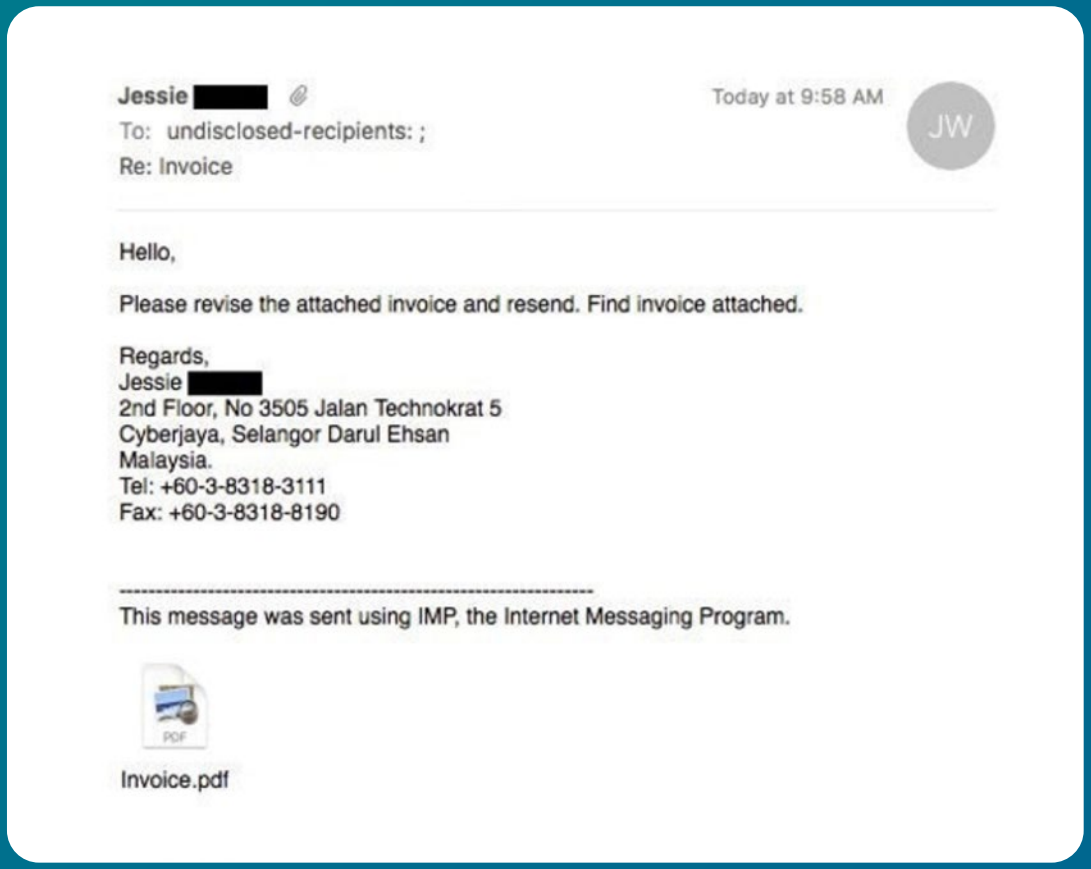
Invoice.pdf

A) Poor subject

B) Suspicious attachment

C) “Undisclosed recipients”

ANSWER:



Jessie [redacted]
To: undisclosed-recipients: ;
Re: Invoice

Today at 9:58 AM

JW

Hello,

Please revise the attached invoice and resend. Find invoice attached.

Regards,
Jessie [redacted]
2nd Floor, No 3505 Jalan Technokrat 5
Cyberjaya, Selangor Darul Ehsan
Malaysia.
Tel: +60-3-8318-3111
Fax: +60-3-8318-8190

This message was sent using IMP, the Internet Messaging Program.

Invoice.pdf

B) Suspicious attachment

It doesn't matter if you expect to receive an invoice from someone or not. Because in most cases, you won't be sure what the message pertains to until it's open.

When you open the attachment, you'll see the invoice isn't intended for you, but it will be too late by then. The document will unleash malware on the victim's computer, which could perform any number of nefarious activities.

Lesson: never open an attachment unless you *know* the message is from a legitimate party. And even then, you should look out for anything suspicious in the attachment.

So, how phishing aware are you?

0-1 out of 5

Oh, dear. Looks like you're exactly the kind of person scammers are after. It's not a matter of if, it's simply a matter of when. You need some serious cybersecurity awareness training if you want to keep your business happy and healthy. That derailing attack is just around the corner!

2-4 out of 5

You got some right. Well done. Unfortunately, if those had been real emails, you could well be looking at thousands of pounds in lost revenue or fines. Phishing emails pull no punches.

5 out of 5

Nice work. You clearly know what phishing scams look like. Still, thousands of scams are being fired at businesses just like yours every second. You may have spotted everything today, but one careless click weeks or months from now could still wreak havoc on your business.

ratcliff
Smarter IT

However well you did, Cyber Security Awareness training is more than worth investigating. One careless moment after a phishing email lands. Or one ill-considered click and your business could be facing lost revenue, fines, and data losses.

Ratcliff IT has years of experience training employees just like yours to spot phishing scams. **Click here** to register for a free training demo and help protect your business from the worst.

020 3551 6262 hello@ratcliff.it ratcliff.it