Digital Literacy:
Gmail Phishing Scams

Laura Gautier

Table of Contents

Introduction

Phishing scams are easy to avoid if you know what to look for, so the following steps will inform you how to identify and report phishing scams in your email's inbox using an example phishing email.

What is a Scam

A *scam* is a dishonest scheme, or fraud.
A *scammer* is a dishonest person, like a thief, who steals from others to benefit themselves.

What are Phishing Emails

A phishing email is a type of scam emailed to you by a scammer to get your personal information. Scammers do this by pretending to be a real company and tricking you into giving away your information.

Phishing Example

Phishing emails may falsely claim that there is an issue with your account or that you have recently won a prize.

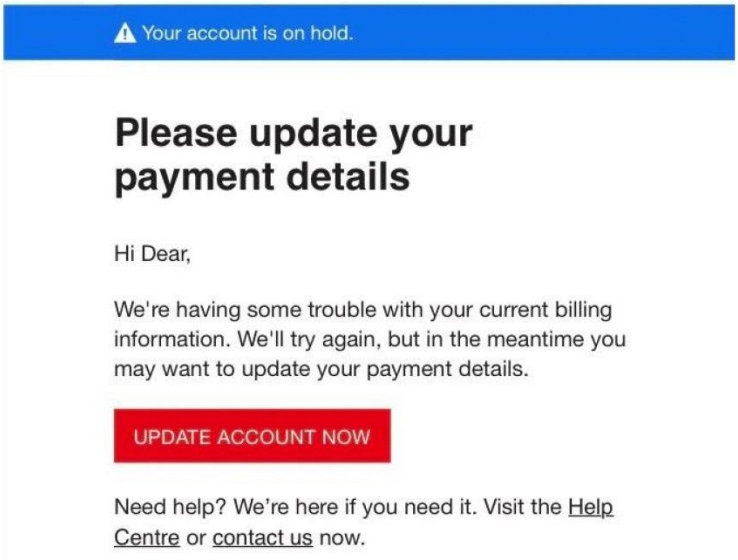


Figure 1. A phishing email pretending to be from Netflix that claims there is an issue with someone's payment information.

Identifying a Phishing Email

1. Go to Your Email Inbox and Open the Email

Go to your email account and click on the suspicious email.

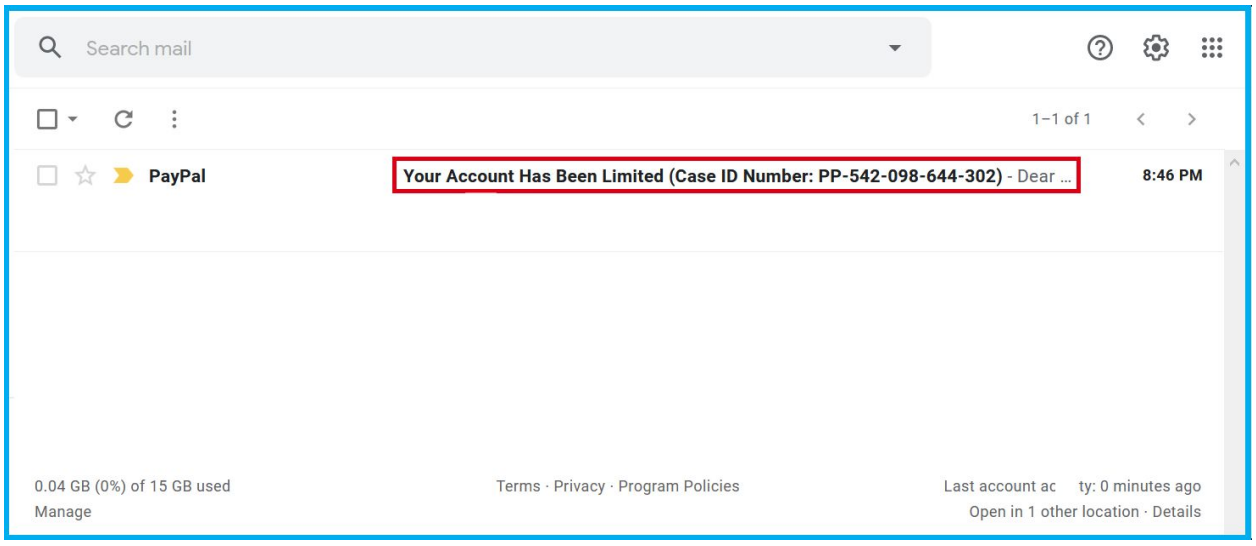


Figure 2. A Gmail inbox with a suspicious email, highlighted in red.

Caution: Do not click any links or attachments

It is important that you only click the email, and not any links or attachments like pictures or PDFs. In the event that you accidentally click one, quickly restart your computer or turn it off and on. This is to disconnect your device from a potentially dangerous website or malware.

2. Check the Sender and Subject Line

Under the sender name, there is a down arrow ▾ under the sender's name that will say "Show details" when hovered over. Clicking the arrow will give you information about who sent you the email.

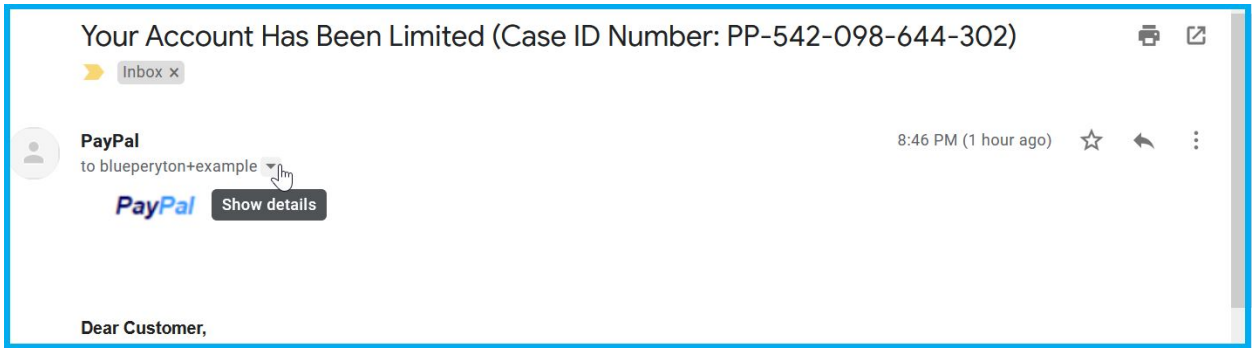


Figure 3: An example phishing email claiming to be PayPal with the cursor hovering over the down arrow.

Often scammers will put their name as a company's name to trick people. After "From:" is the sender's real email address. If it contains random letters or numbers, and you do not recognize it, then it is a phishing email. Similarly, the Subject line may have a "Case ID Number" or a fake invoice number to appear real.

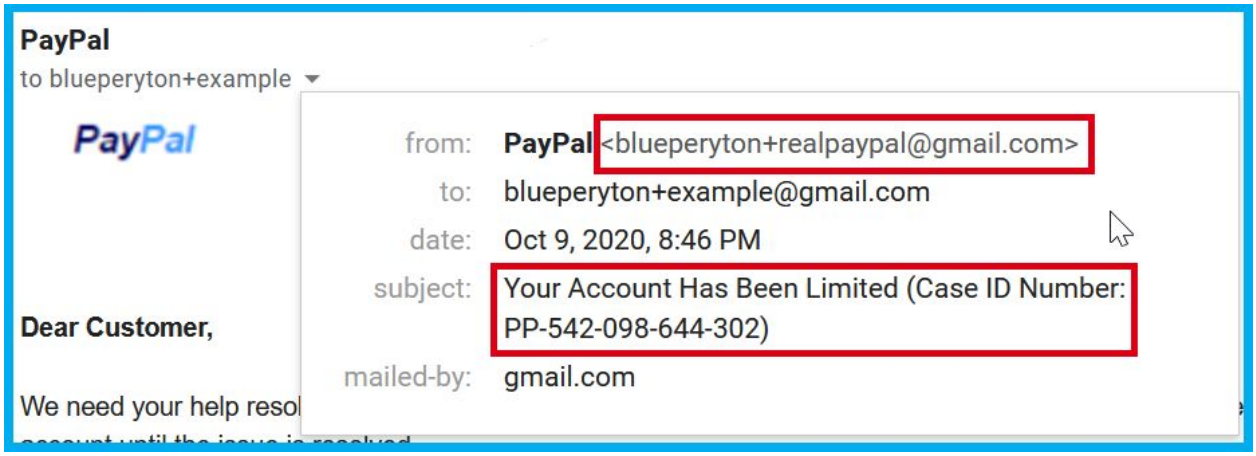


Figure 4: An example of the email's information with the sender's email and the Subject line highlighted in red. The email appears to be from PayPal, but the email address is not PayPal's company address.

3. Check the Email Contents

Read the email and determine if it is suspicious.

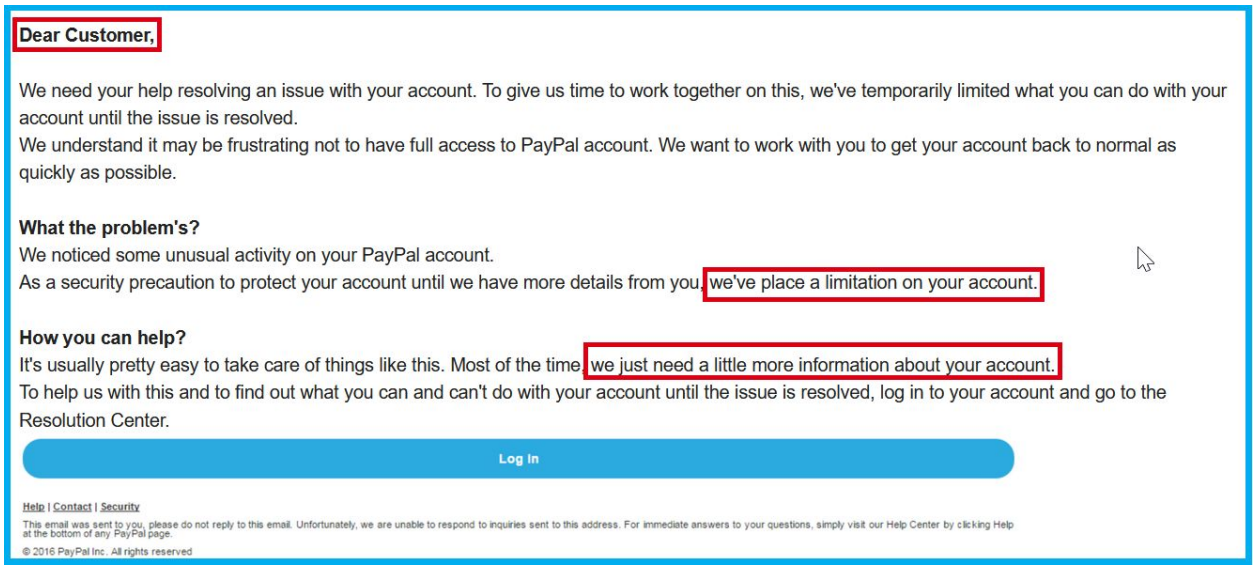
How Do I Know if an Email is Suspicious

Signs of Suspicious Emails

- Asks you for your personal information
    - Login credentials/password
    - Bank account information
    - Payment information

- Says your account is “limited” or “restricted”
- Does not use your name
    - May address you as “Customer” or “Client”
- Contains attachments, such as a Word document or PDF

Companies will never ask for your personal information through email. Additionally, some phishing emails may have suspicious attachments containing malware that can steal your information or cause harm to your computer.



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

Figure 5. The email contents with suspicious parts highlighted in red.

In this email, they address us as “Customer,” claiming they’ve limited our account and need our information. All of these are signs that the email is a phishing scam.

4. Verify Links, If There Are Any

Remember: Do not click suspicious links.

4.1. If the email contains a link, you can hover over it with your mouse. A dark grey box will appear in the bottom left corner of your screen.

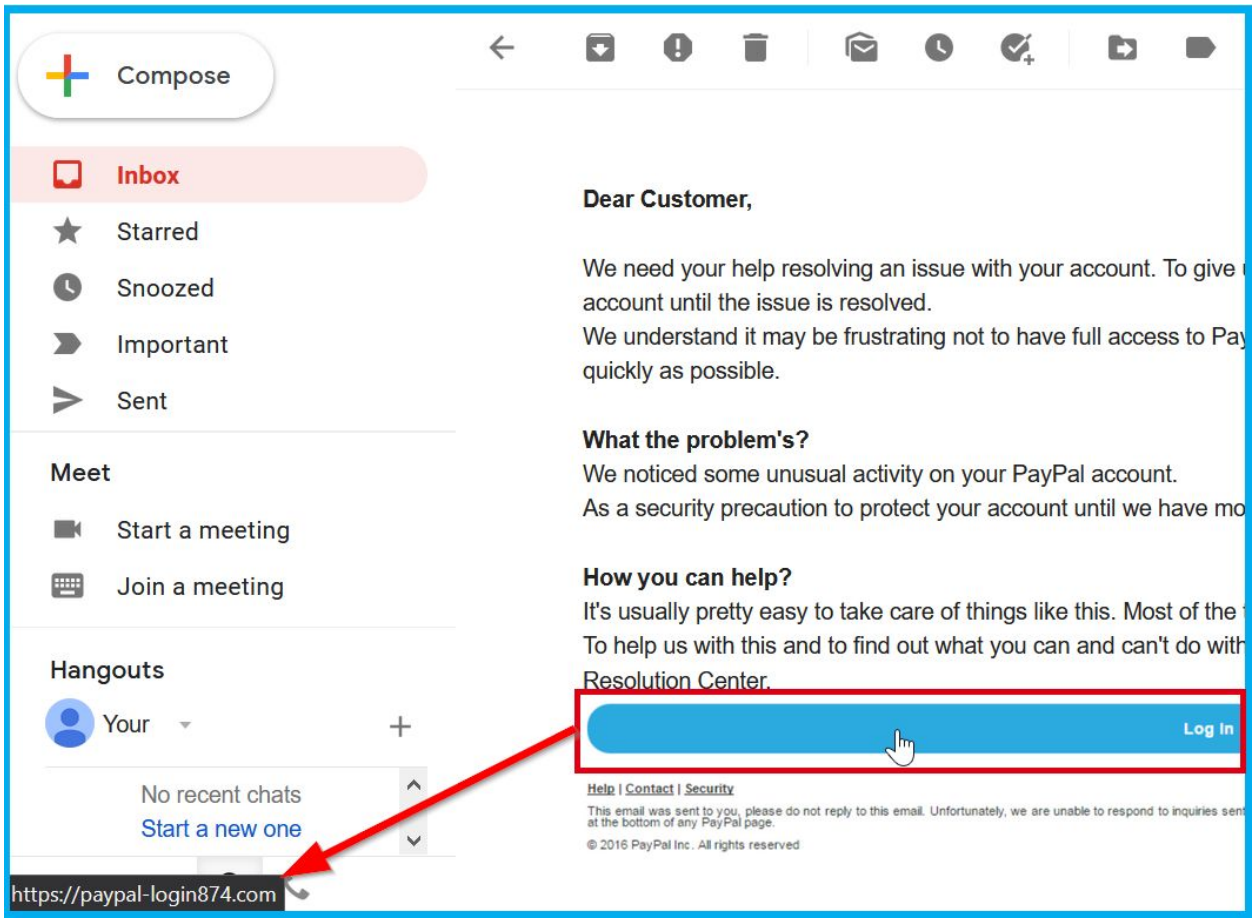


*Figure 6. A screenshot of the mouse hovering over **Log in**, revealing the true website address.*

4.2. If it is a site you do not recognize, then do not click it.

Reporting and Blocking a Phishing Email

1. Click the More Button

1.1. Click the **More** three dots button on the right side of the email next to the **Reply** arrow button.

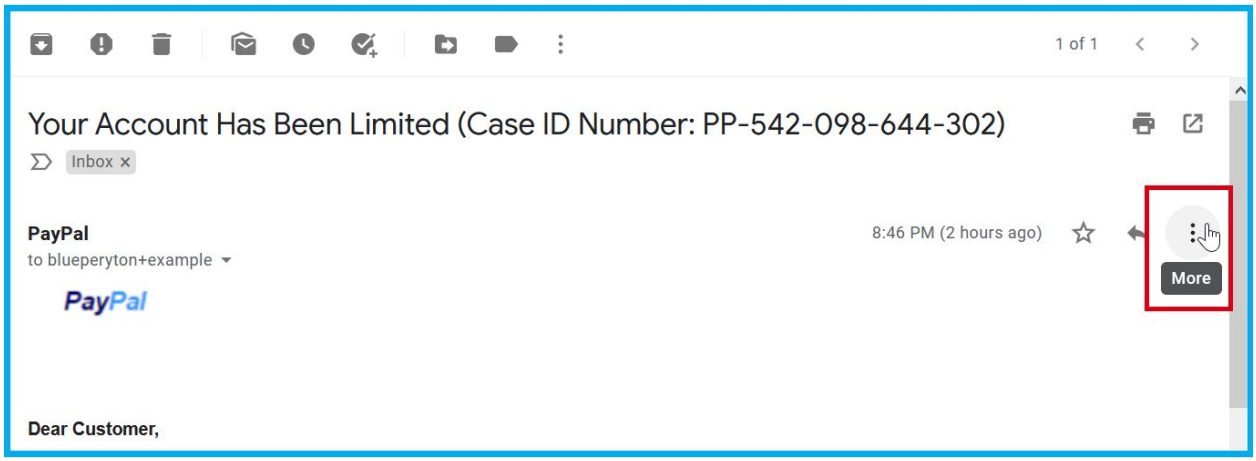


*Figure 7: The location of the **More** button.*

2. Report the Email for Phishing

2.1 Click **Report Phishing**.

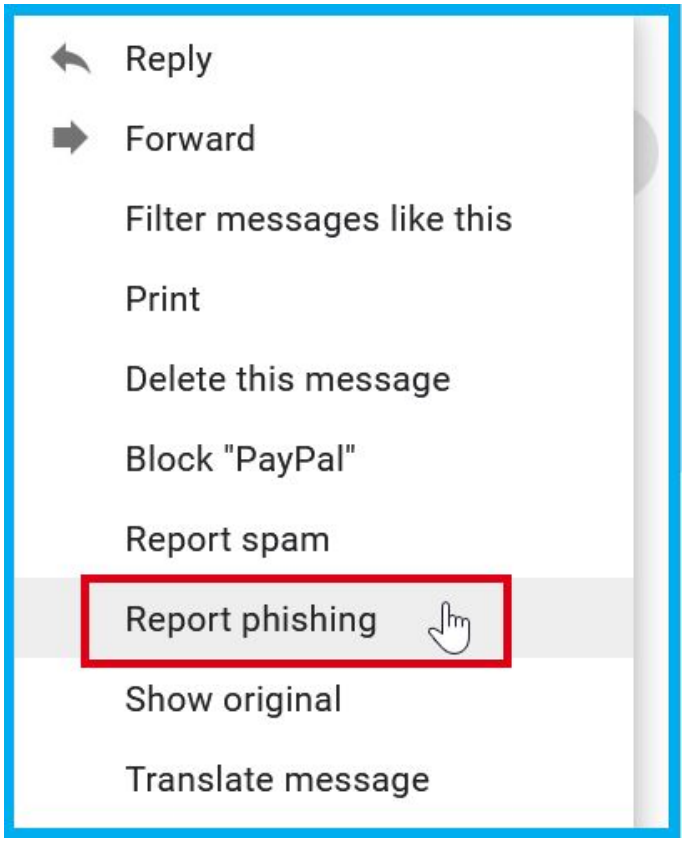


*Figure 8: A screenshot of the **More** options with **Report phishing** highlighted.*

2.2 You may also forward the email to reportphishing@apwg.org.

- Click **More**
- Click **Forward**
- Type reportphishing@apwg.org into the **To** box

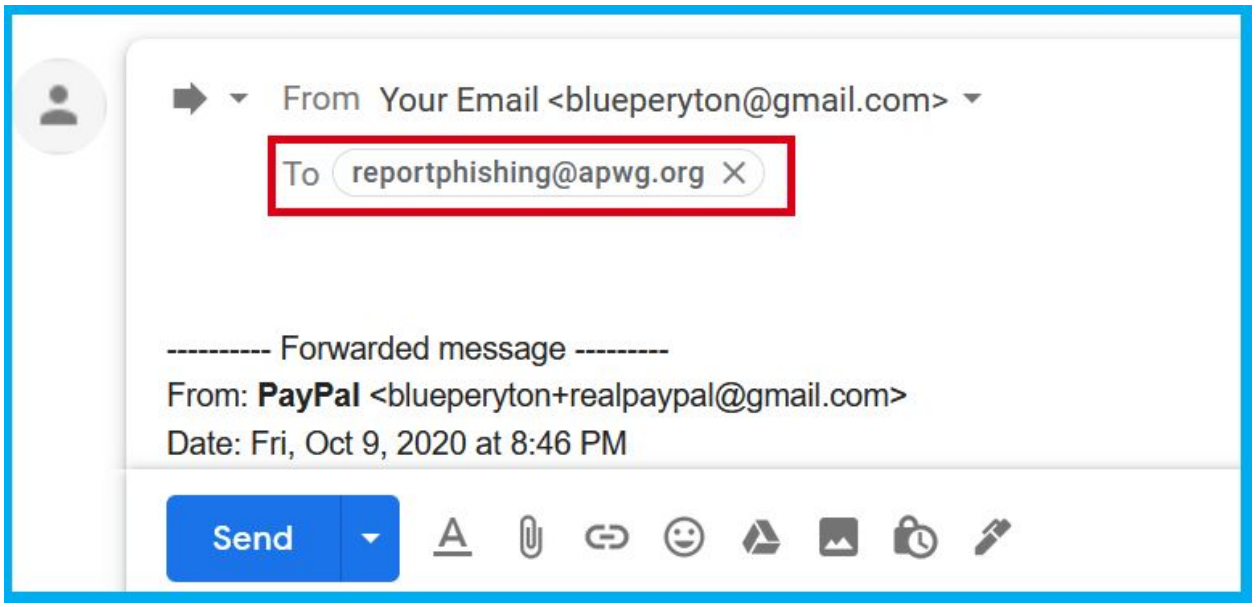


Figure 9. The forwarding box that appears.

- Click **Send**

3. Block the Sender

Click the **More** button again. Then, click **Block 'Sender Name.'**

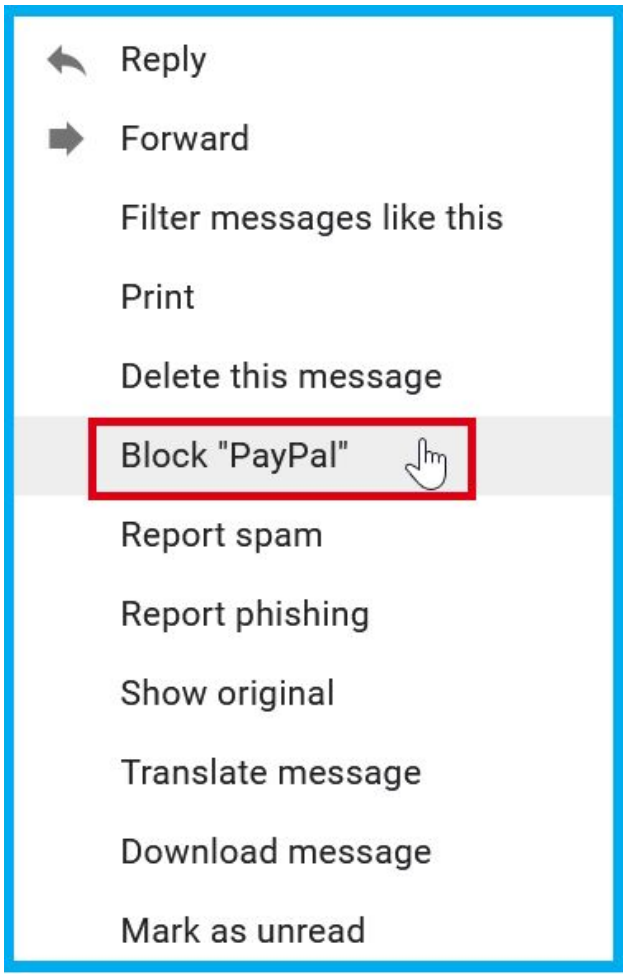


*Figure 10: A screenshot of the **More** options with **Block "PayPal"** highlighted. In this case, "PayPal" refers to the sender of the email for this phishing email example.*

Why Block

This prevents the sender from contacting you from that email address anymore. They will not be able to send you more phishing emails and will have to leave you alone, which protects you from future phishing attempts.