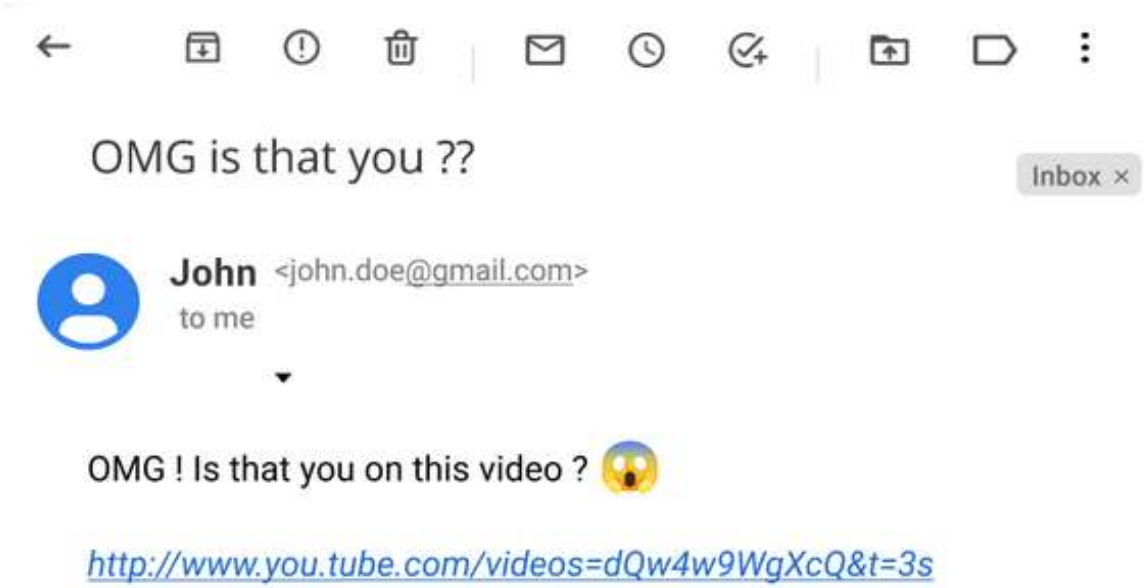
ETH zürich

Welcome to the Training Module! During this session, you will be presented with several emails and asked to determine whether they are phishing attempts or not. To effectively identify a phishing email, pay attention to the small details within the message that may indicate it is not legitimate. We will provide explanations of the techniques used to recognize phishing emails after each example. Best of luck!

→

ETH zürich

Consider the following mail:



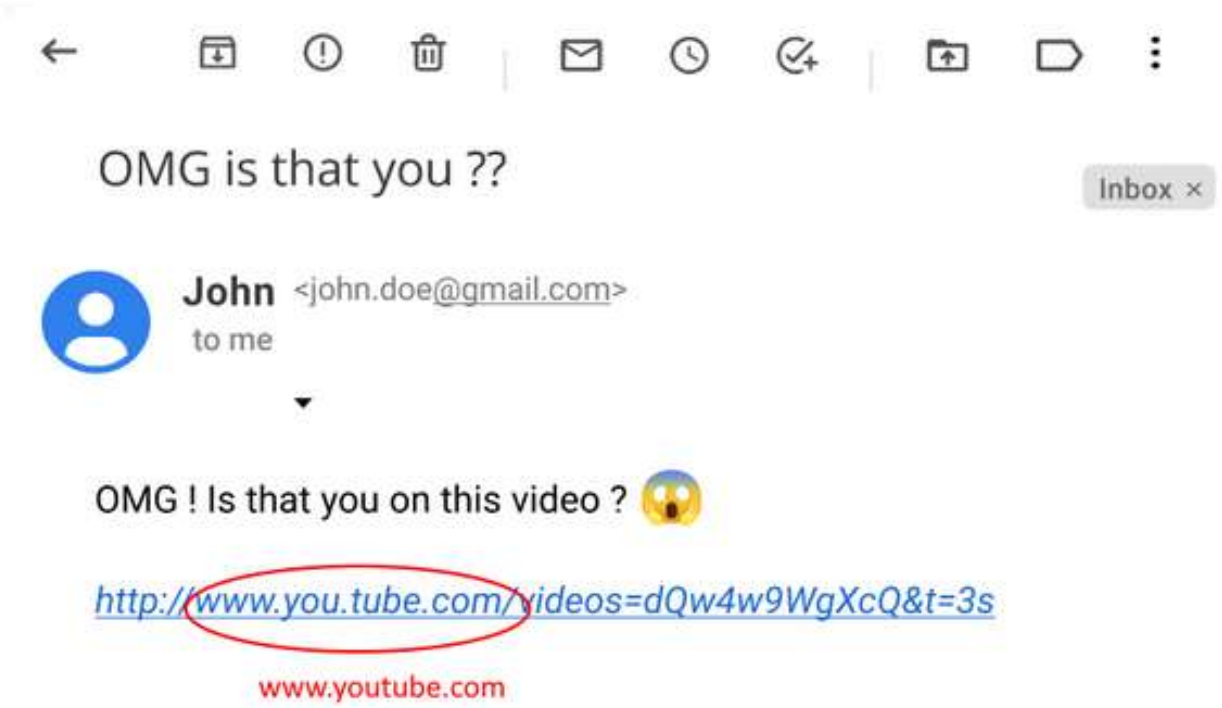
Is this a phishing mail ?

- ◯ Yes
- ◯ No

→

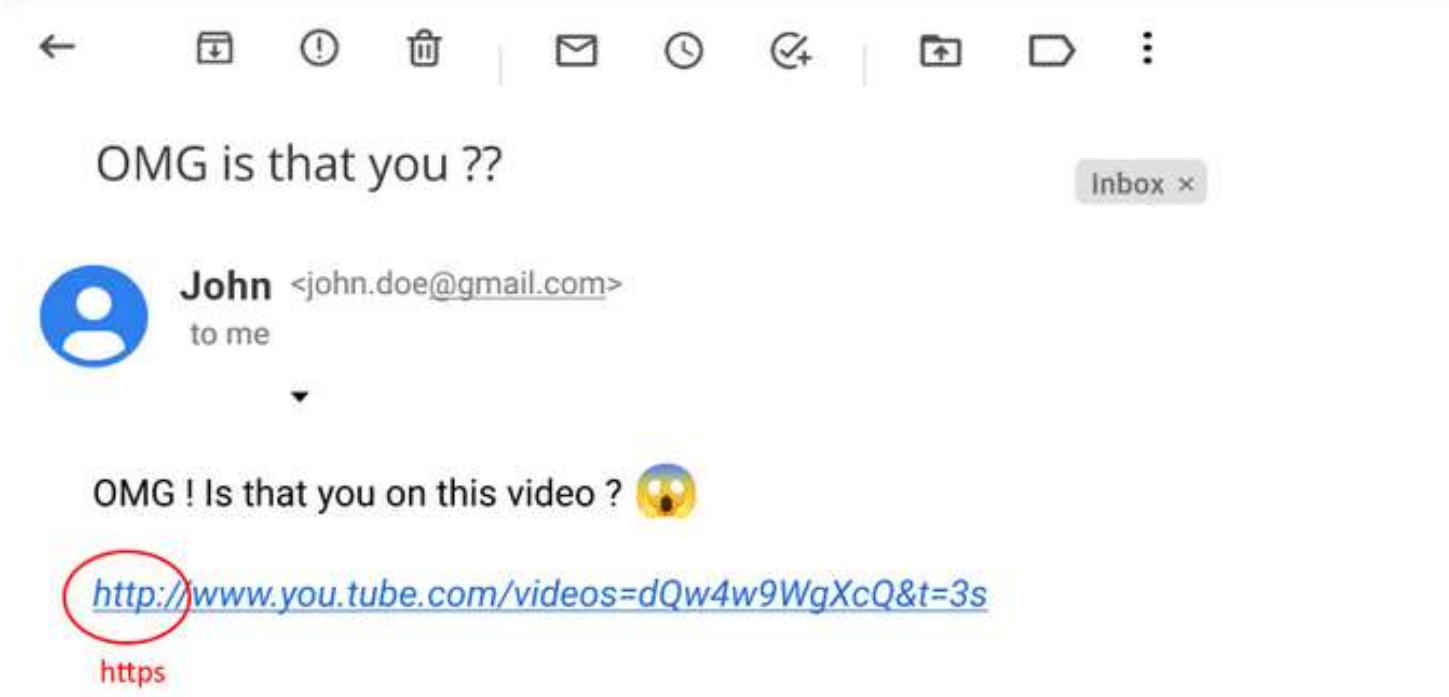
YES! It is a **phishing** mail!

The trick to identify this phishing mail was the URL (the address in the link). One way to do this is to look at the **domain name** (what comes after www). For example, if you see an URL that looks like it's taking you to a **YouTube** video, but the domain name is **you.tube.com** instead of **youtube.com**, that might be suspicious.



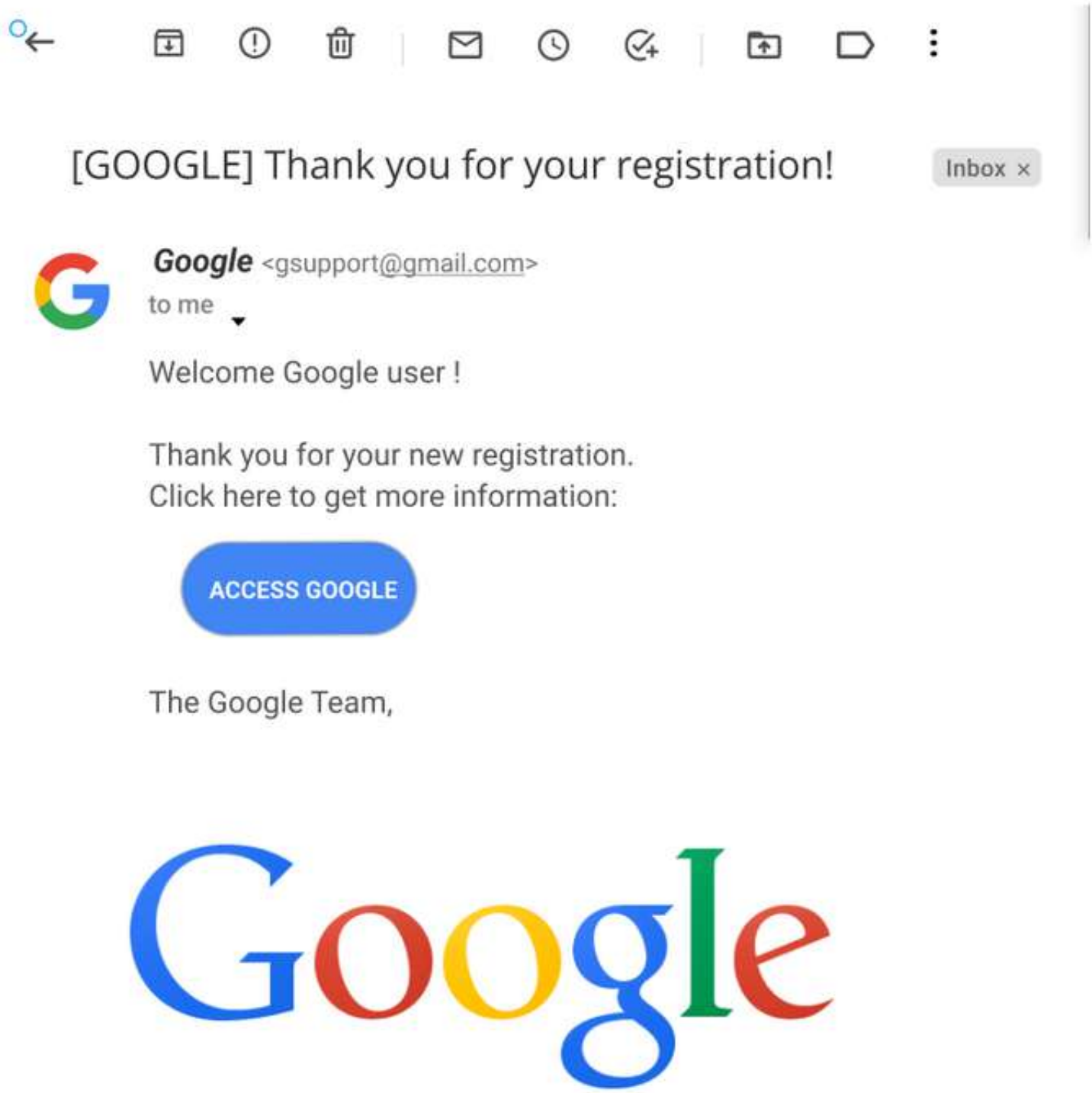
Another thing to check is the **protocol** in the URL (the part before ://www) - make sure it starts with "**https**" instead of "**http**". This means the website is **secure**. Big websites like **YouTube** and **Google** always use "**https**", so it's a good sign that you're not being redirected to a fake website.

Another thing to check is the **protocol** in the URL (the part before ://www) - make sure it starts with "**https**" instead of "**http**". This means the website is **secure**. Big websites like **YouTube** and **Google** always use "**https**", so it's a good sign that you're not being redirected to a fake website.



→

What about this mail ?

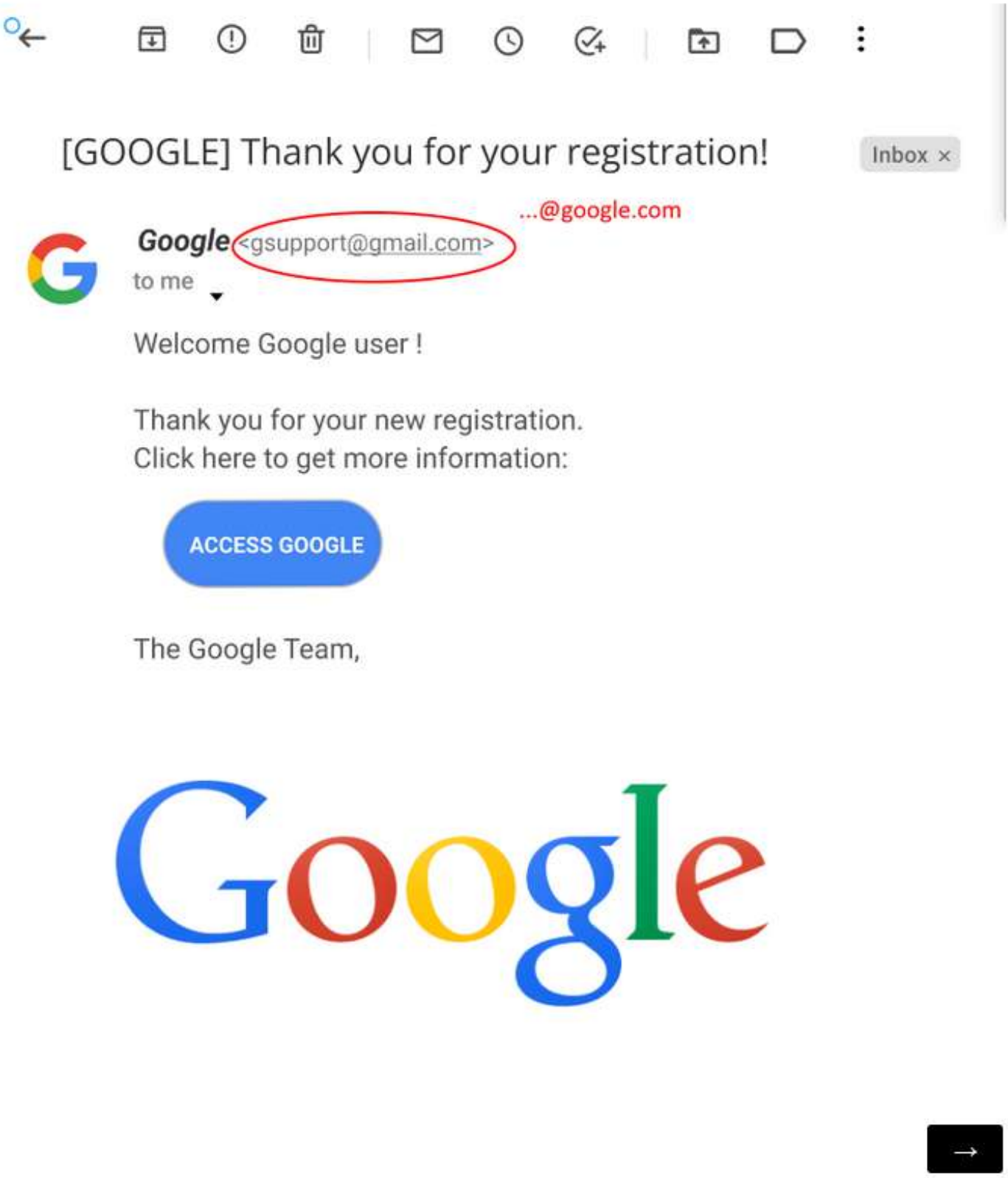


Is it a phishing mail ?

YES! It is a **phishing** mail!

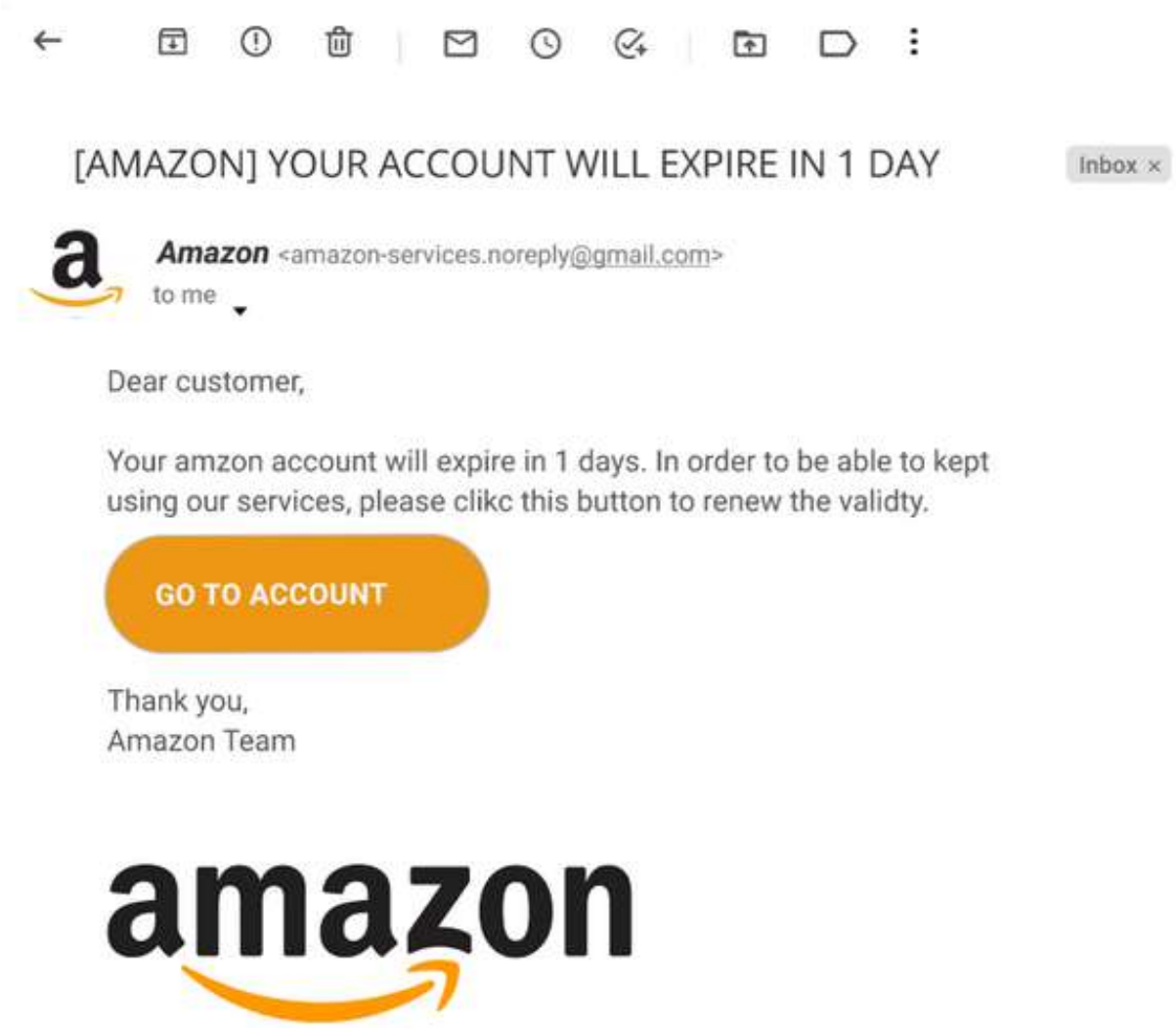
Sometimes scammers use **logos** in their emails to **trick** you into thinking the email is from a legitimate company, like Google. But don't be fooled by logos - anyone can download and use them. Instead, check the **sender's email address** to see if it's really from the company they claim to be.

For example, if you get an email from "**gsupport@gmail.com**" claiming to be from Google, be cautious. Real Google addresses always contain "**google.com**", whereas "gmail.com" is a general mailbox that anyone can use. If you're unsure, search for the email address online to see if it's associated with Google or not. And if you've never received an email from that address before, it's best to assume it's suspicious.


[GOOGLE] Thank you for your registration!
Inbox ×
...@google.com
Google <gsupport@gmail.com>
to me
Welcome Google user !
Thank you for your new registration.
Click here to get more information:
ACCESS GOOGLE
The Google Team,
Google

→

What about this mail?

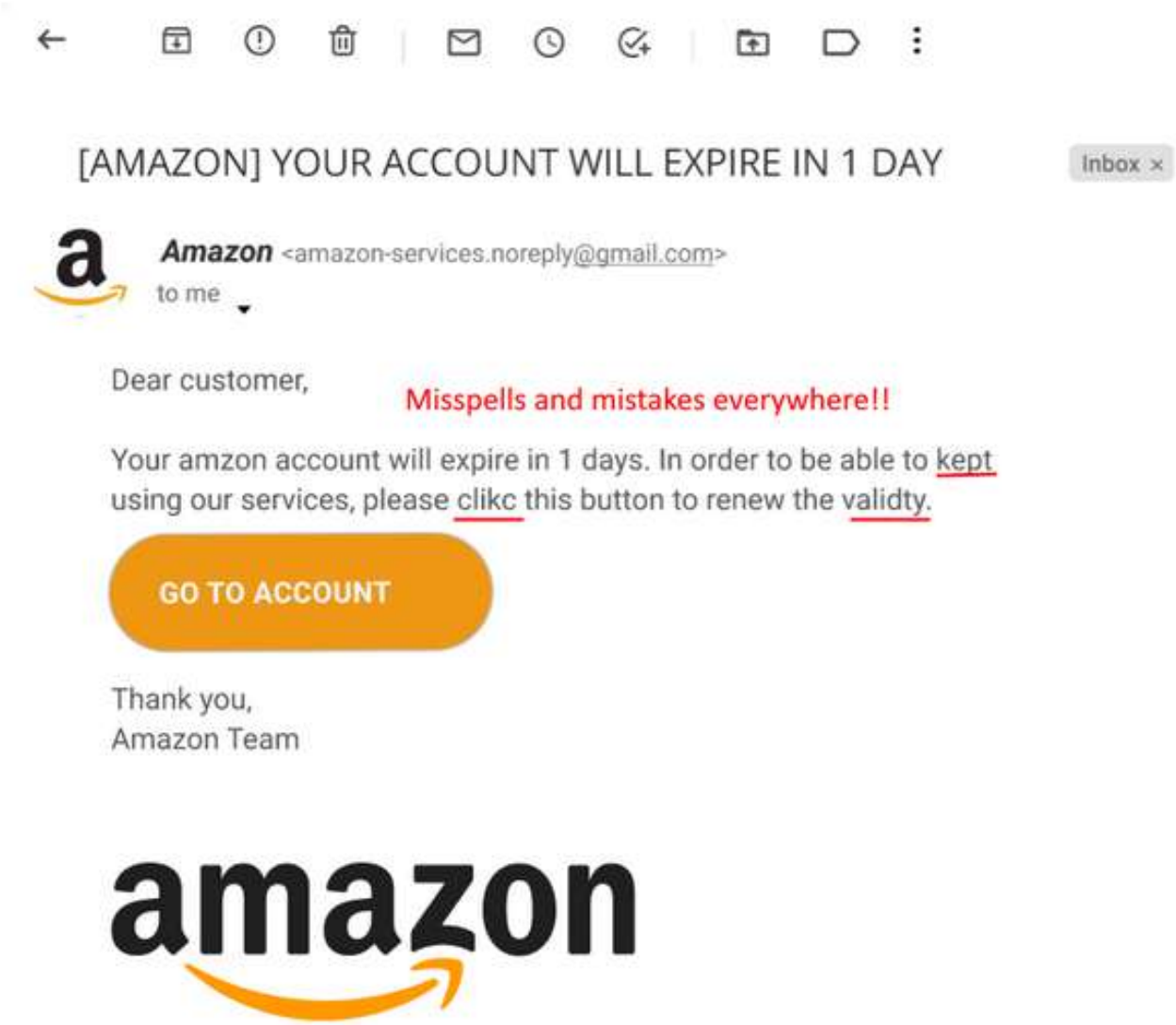


Is it a phishing mail ?

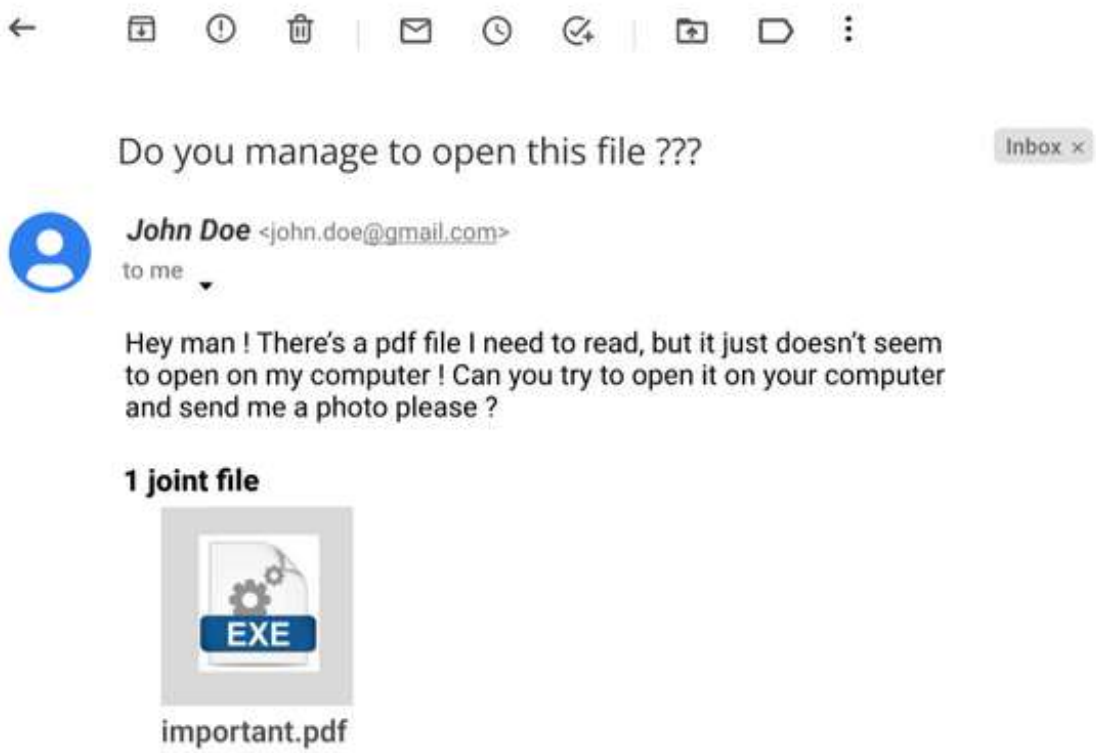
- ○ Yes
- ○ No

YES! It is a **phishing** mail!

Official emails from **large companies** like Amazon go through multiple rounds of review and editing, making it **highly unlikely** that they contain **misspelled words** or other **orthographic mistakes**. Therefore, it's important to be on the lookout for any **spelling errors** in an email that purports to be from a reputable company. If you do spot any misspelled words or other glaring mistakes, it's a red flag that the email might be a **phishing** attempt.



What about this mail?



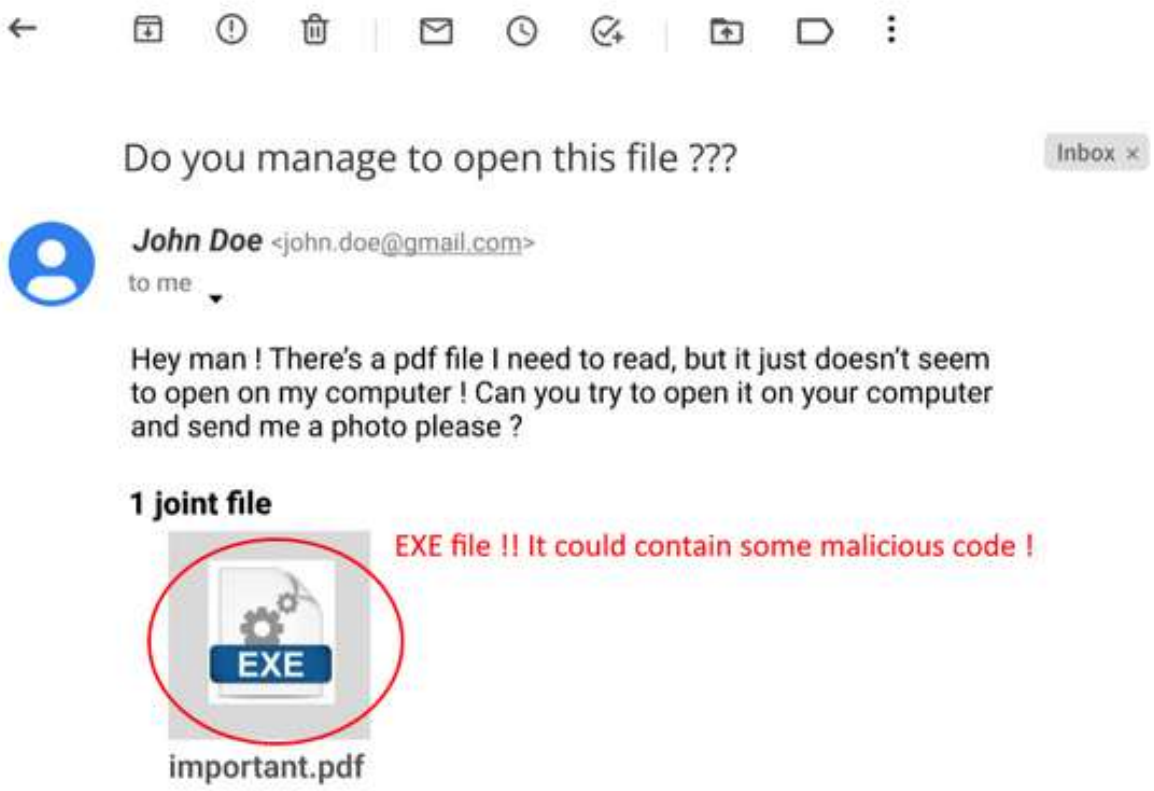
Is it a phishing mail ?

- ◯ Yes
- ◯ No

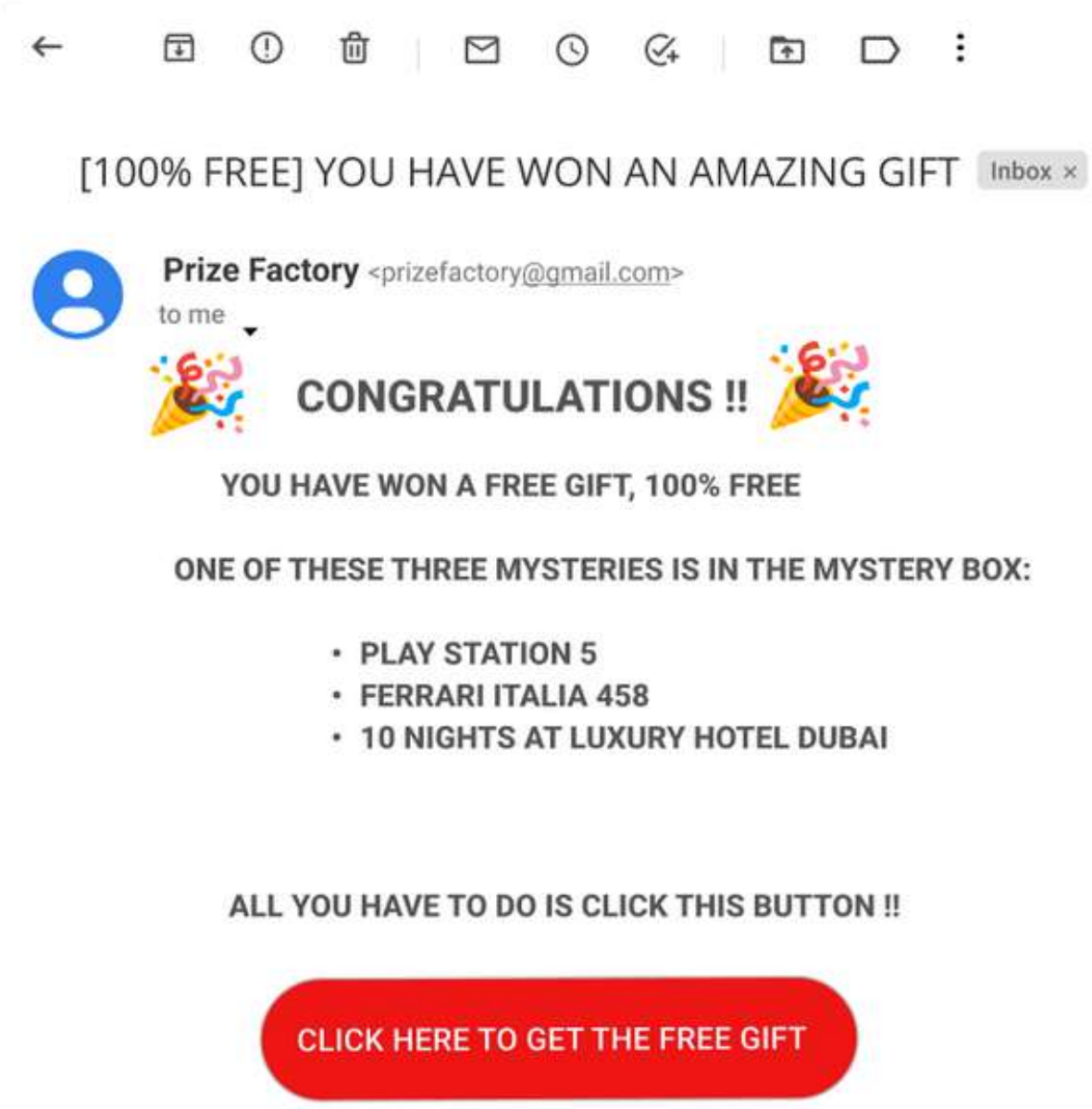
→

YES! It is a **phishing** mail!

Phishing emails often contain attached **files** that appear **harmless** but are actually **malicious** and could endanger your computer and steal your personal data. One way to recognize these types of files is to look at their **extensions** (what comes after the name of the file). For example, a file with a **.exe** extension (file that can execute some malicious code on your computer) may be disguised as a different file type, such as a **.docx** or **.pdf** file. To avoid falling for this trick, hover over the file and look at its properties to see its **full name** and **extension**. If it looks suspicious or unfamiliar, **don't open it**. In this example, we can clearly see that the file is a **exe** (from the file preview of gmail), whereas the sender says it's a pdf, which is suspicious.



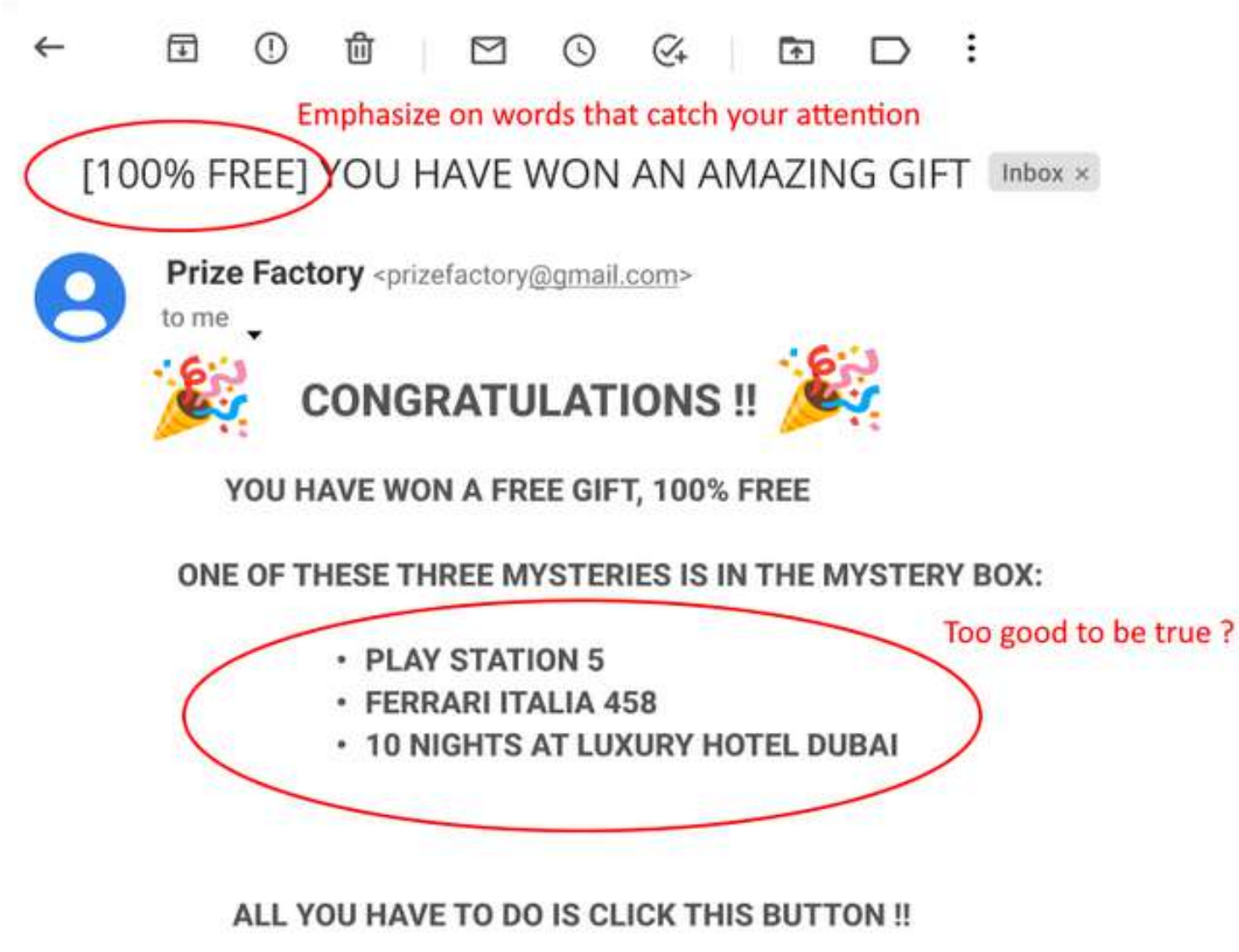
What about this mail?



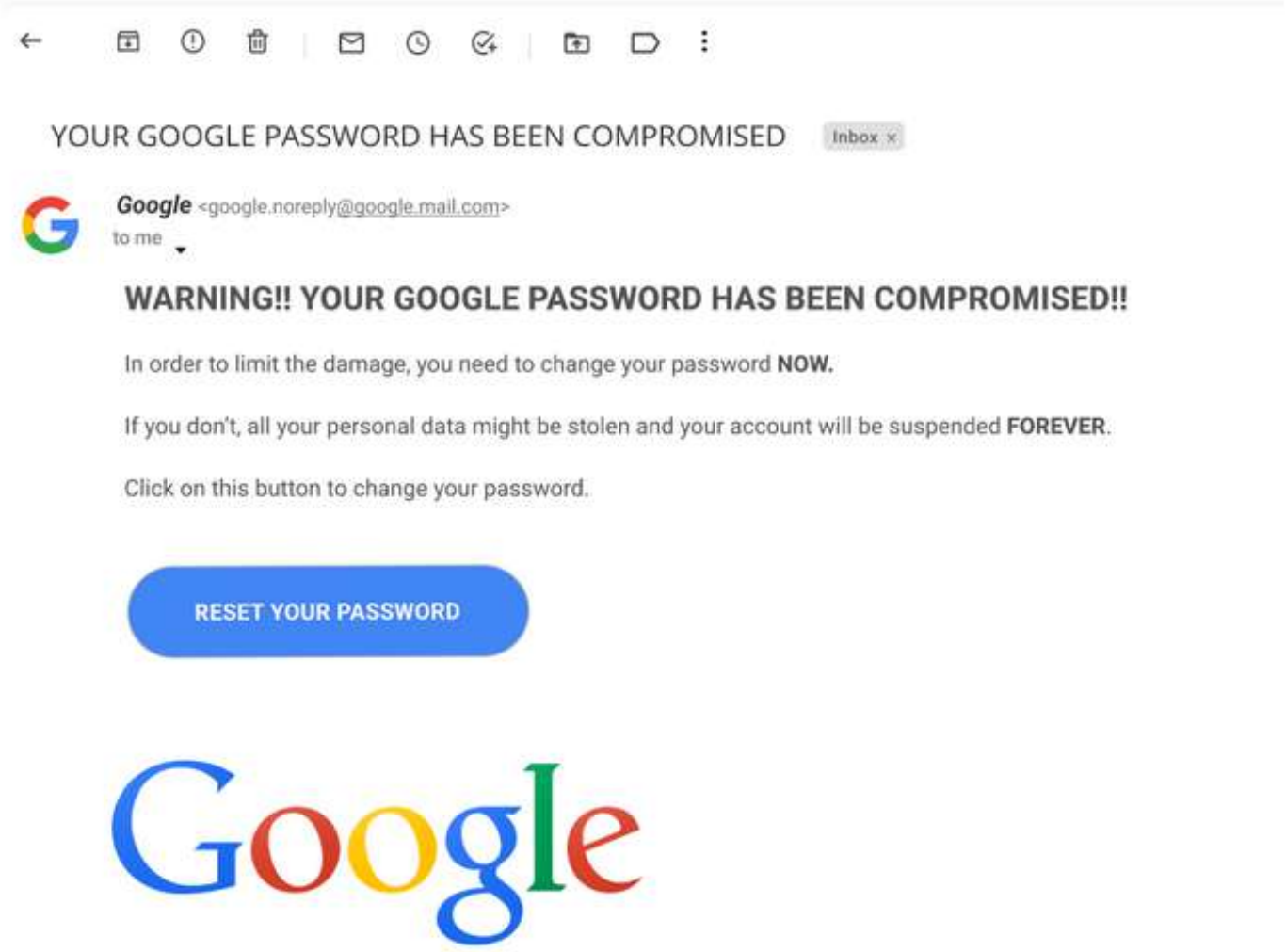
Is it a phishing mail ?

YES! It is a **phishing** mail!

Be careful when you receive emails claiming that you've **won something**. Ask yourself, what did you win? If it sounds **too good to be true**, it probably is. This email might try to **manipulate your emotions** by making you feel excited about **winning a prize**. If the email **heavily emphasizes** the words **"FREE"** and **"GIFT"**, it's a red flag. While it could be a marketing strategy, this type of **aggressive marketing** is usually associated with **scams**, not loyal customer service, so always stay on your guard.



What about this mail?



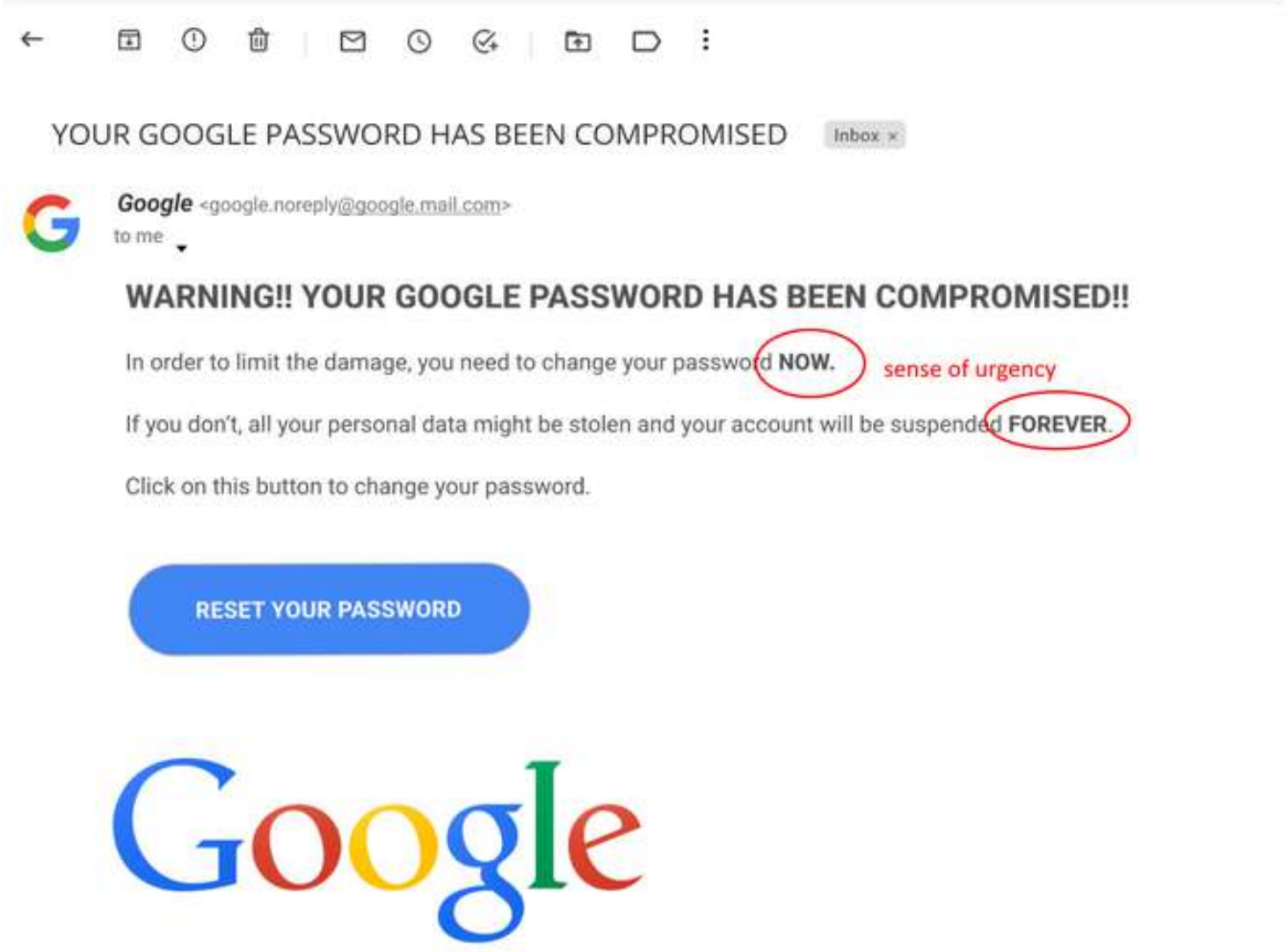
Is it a phishing mail ?

- ◯ No
- ◯ Yes

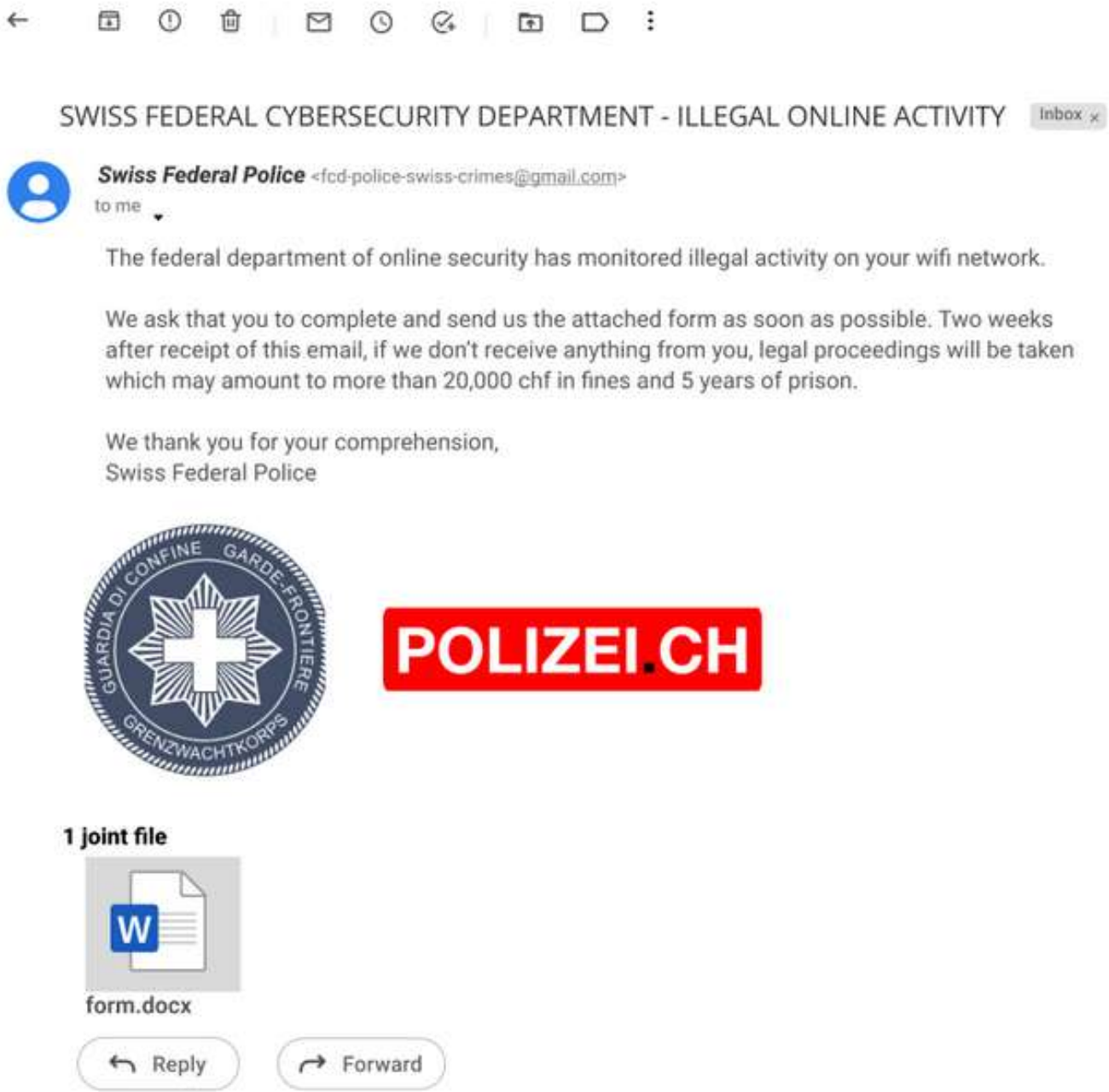
→

YES! It is a **phishing** mail!

Scammers often use **fear** to trick you into clicking on a link or giving them your personal information. They might send you an email claiming that your account has been **compromised** or that your safety is at **risk**. Don't let your **anxiety** take over - instead, take a closer look at the email. If the email seems to be overly insisting on the **urgency** or **danger** of the situation, it's probably a phishing email. Remember, scammers want you to act **quickly without thinking**, so take your time to evaluate the situation **carefully**.



What about this mail ?

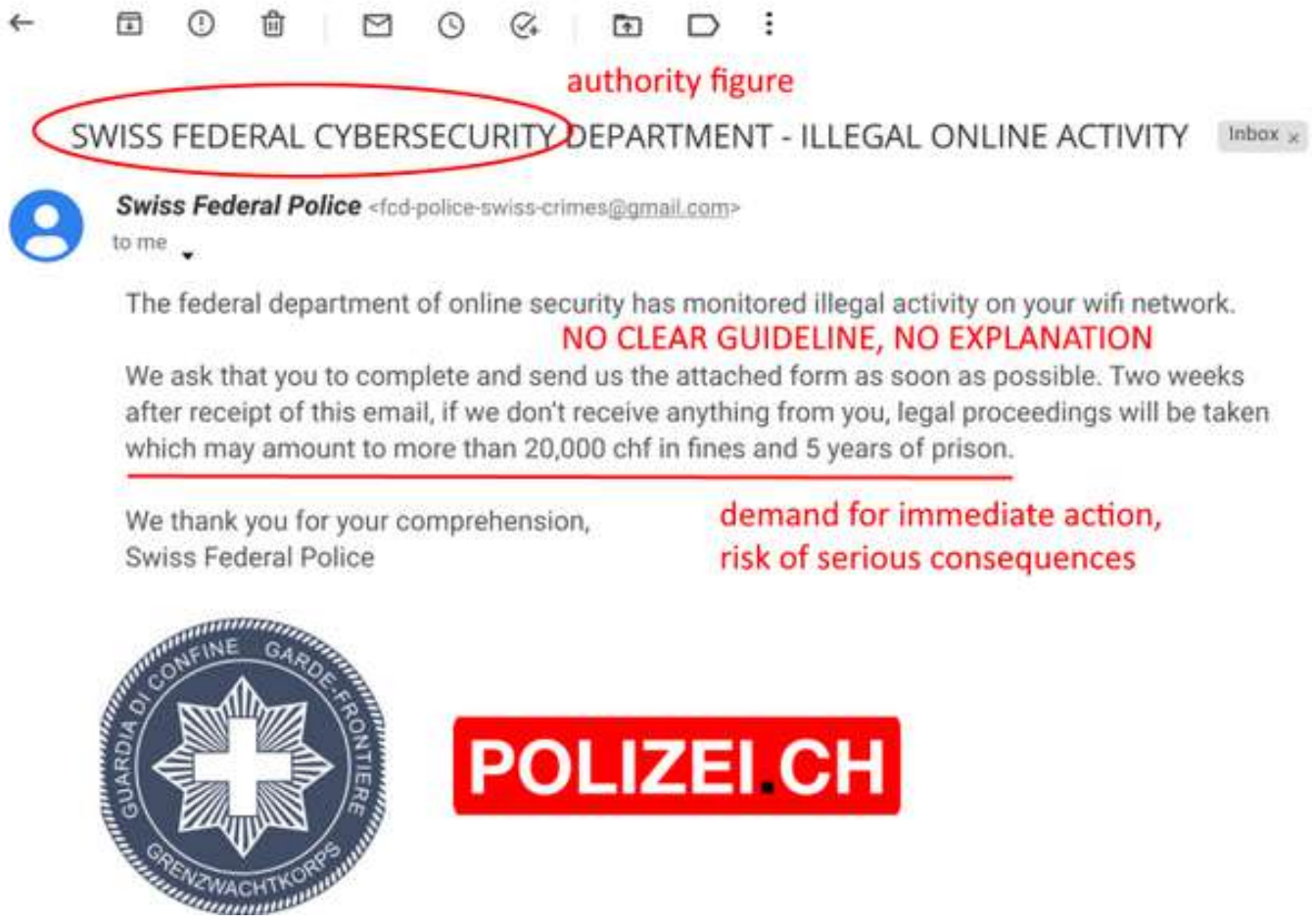


Is it a phishing mail ?

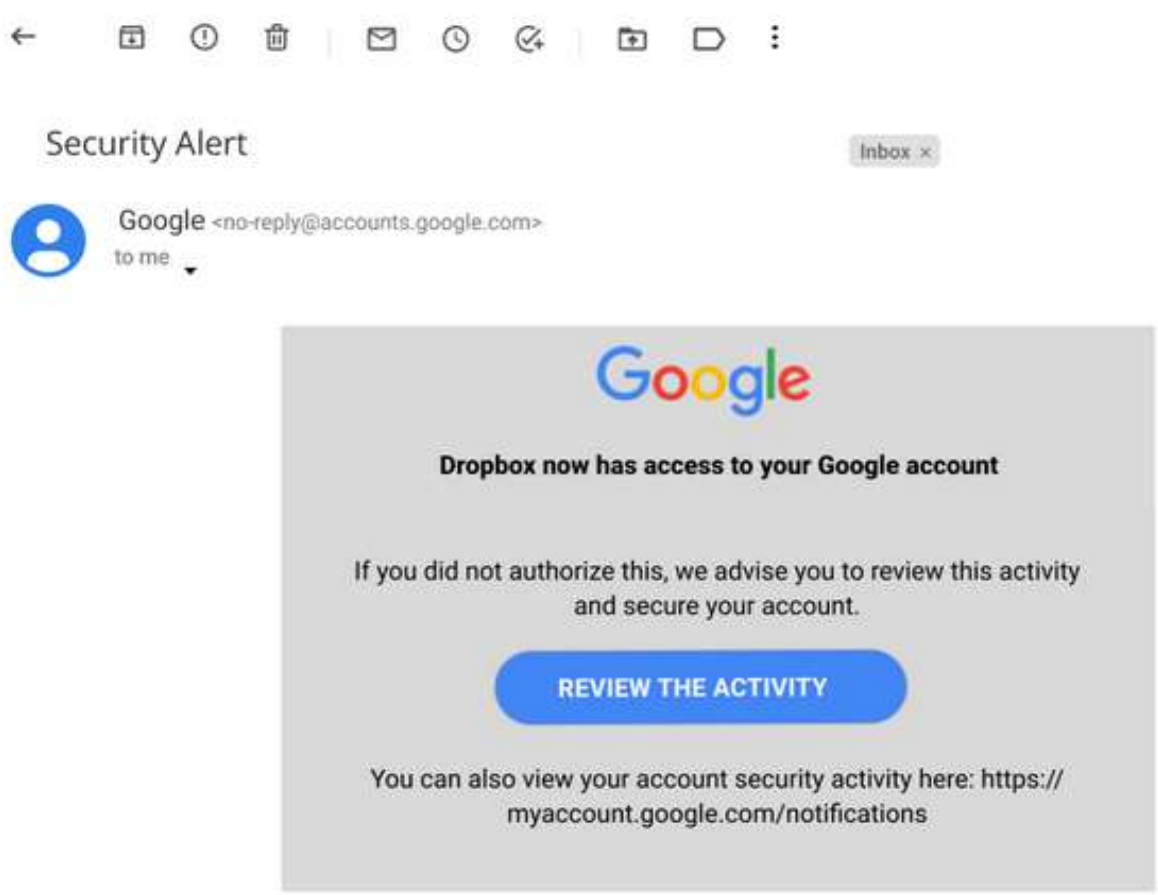
- ◯ Yes
- ◯ No

YES! It is a **phishing** mail!

One common tactic that phishing scammers use is to **impersonate authority** figures, such as law enforcement in this example. They might send you an email accusing you of **illegal online activity** and demand that you take **immediate action** to avoid **serious consequences**. However, these emails are often fake and can be identified by several key factors. First of all, law enforcement would **never** contact you through **unsolicited emails** or demand immediate action without giving you the opportunity to **verify their identity**. Check that all the information they use in their mail **makes sense**, and that they provide **clear guidelines** on what the steps to follow are... anything shady could be the sign of phishing.



What about this mail ?



Is it a phishing mail ?

- ◯ No
- ◯ Yes

→

NO! It is **NOT** a **phishing** mail!

Don't let your guard down, but also don't be **overly suspicious**. Using the techniques we have learned, we can analyze this email and determine that there is nothing immediately suspicious about it. It is well-written with no **misspellings**, **grammatical errors**, or any **urgency**, **authority,** or **promises of rewards**. The email is a security alert, but it does not overly emphasize the **gravity of the situation**. Furthermore, the company accessing the account is Dropbox, a legitimate and well-known company, which adds to its credibility. The sender's domain is **google.com**, which is owned by Google. The link provided in the email is in **https** and the domain of the address, **myaccount.google.com**, is associated with Google. However, it is always important to **double-check** the legitimacy of an email by **searching online** for any information or reviews about the sender or the contents of the email.

ETH zürich

Congratulations, it's the end of the training module!

In order to avoid falling for a phishing mail, always remember to check the following:

- Does the sender's email address look legitimate?
- Does the mail has a sense of urgency?
- Is the sender an authority figure? What are they asking for?
- Is the mail offering huge rewards that seem too good to be true?
- Does the mail contain any misspells?
- Does the mail contain files or URLs that look suspicious?

Thank you for your time, go to the next slide in order to go back to the background task.

→