

How frequently do you use your mailbox ?

- ☐ less than once a week
- ☐ approximately once a week
- ☐ approximately once a day
- ☐ multiple times a day
- ☐ multiple times an hour

How many emails do you receive on an average work day?

- ☐ Less than 5
- ☐ Less than 10
- ☐ 10-50
- ☐ More than 50

How many spam or promotional emails do you receive on an average day?

- ☐ None
- ☐ Less than 10
- ☐ 10-50
- ☐ More than 50
- ☐ I don't know

Do you use a professional mailbox in the context of your job ?

- ☐ Yes
- ☐ No
- ☐ I don't have a job

Have you ever taken part in a security training on phishing?

- ☐ No, never
- ☐ Yes, once
- ☐ Yes, more than once

## How would you rate the following aspects?

	very low	rather low	medium	rather high	very high
your knowledge on phishing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
your ability to detect phishing e-mails	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
your level of alertness for phishing attacks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Well done, the task is done! We will now ask you some questions again.

Some of these questions can be similar to the first form. This is intended, so please try to answer them once more.

What is phishing?

- ☐ A type of online scam where criminals send fraudulent messages to trick people into sharing sensitive information.
- ☐ A type of social engineering used to convince people to buy products they don't need.
- ☐ A type of online advertising that uses deceptive tactics to attract clicks.
- ☐ A type of malware that infects computers and steals personal data.

What are the risks of falling victim to a phishing attack?

- ☐ Computer infected by malware
- ☐ Loss of personal data
- ☐ Financial loss
- ☐ Identity theft
- ☐ All these answers are correct

What is a common type of content found in phishing emails?

- ☐ Threats of account deactivation or legal action if immediate action is not taken
- ☐ Unsolicited job offers
- ☐ Security alert of suspicious login from an unknown location
- ☐ Advertisements for weight loss supplements



Suppose you have received a mail from paypal asking to reset your password, and the email sender address is one of the following. Which one of these mail addresses looks suspicious ?

☐ servicepaypal@gmail.com

☐ support@paypal.com

☐ None

☐ paypal@paypal.com

☐ service@paypal.com

Suppose now you have received a mail from Dropbox saying that a user has shared his dropbox with you. Which one of the following mail addresses looks suspicious ?

☐ no-reply@dropbox.com

☐ None

☐ noreply-dropbox@noreplysupport.com

☐ no-reply@em-s.dropbox.com

The following address is suspicious :  
googleaccountsupport@gsupport.com. Why ?

- ☐ It should contain no-reply
- ☐ It is not suspicious
- ☒ The domain address should contain google.com
- ☐ Company names in email addresses always have capital letters, so « google » should be written « Google »
- ☐ It should be a gmail address



Among the following sentences, which one would you be the most susceptible to find in a phishing mail ?

- ☐ "Your bank account password has been compromised ! If you don't act fast, hackers might steal your money ! Click here to reinitialize your password"
- ☐ "Click here to view the latest collection of our awesome brand !"
- ☐ "Thank you for your registration ! Click here to see your account details"
- ☐ None

What about these?

- ☐ "It was a pleasure having you as a customer. Don't hesitate to come back or contact us to the following link if you need our help again."
- ☐ "Please visit our official website to update your personal account"
- ☐ None
- ☐ "As a valued customer, we're giving you a special discount! -90 % on all our offers, click here to view more!"



## What about these?

☐ None

☐ "This is a notification from the Cybercrime Division of your local police department. Our records indicate that your internet connection was used to access illegal content and distribute malware. To avoid prosecution, you must pay a fine of 500chf within 24 hours. Failure to comply will result in legal action being taken against you."

☐ "We noticed some unusual activity on your account and wanted to confirm whether you made the transaction of 500chf at [Merchant Name] on [Date]. If this was not you, please contact us immediately to resolve the issue."

☐ "As part of our routine account maintenance, we kindly request that you confirm your personal information by visiting our website and completing the validation process accordingly."

## What about these?

☐ None

☐ "Plase update your account information to conitnue using our service, click on the following link"

☐ "Don't forget to submit your report by Friday, April 9th. Submit with the following link"

☐ "We are excited to announce our new website and features. Find more by clicking on the following link"

☐ "Please make sure to verify your account information with the following link"



Suppose you have received an email that can contain one of the following links. Which one looks **legitimate**?

- ☐ <https://cutt.ly/V8rT54mnJ90>
- ☐ <https://www.youtube.com/account>
- ☐ <http://google-file-share.c.com>
- ☐ <https://www.youtube.com/watch?v=dQw4w9WgXcQ&t=3s>
- ☐ None

Suppose attached to a mail you have one of the following files. Which one looks **legitimate**?

- ☐ bank\_account.pdf.exe
- ☐ Important\_doc.docx
- ☐ paypal\_account\_details.exe
- ☐ None
- ☐ bank\_invoice.scr



If you fall for a phishing scam, what should you do to limit the damage?

- ☐ Unplug your computer to get rid of the malware
- ☐ Change any compromised password
- ☐ Delete the phishing email

What should you do as an employee if you suspect a phishing attack?

- ☐ Report it so the organization can investigate
- ☐ Show your coworkers to see what they think
- ☐ Ignore it
- ☐ Open the email and see whether it looks legitimate



Please indicate the degree to which you agree or disagree with each statement. In each case, make your choice in terms of how you feel right now, not what you have felt in the past or would like to feel. There are no wrong answers.

	1 -Strongly Disagree	2	3	4	5- Strongly Agree
I don't always click on links in emails just because they come from someone I know.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It's risky to open an email attachment from an unknown sender.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It can be risky to download files on my work computer.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Nothing bad can happen if I click on a link in an email from an unknown sender.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Just because I can access a website at work, doesn't mean that it's safe.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If an email from an unknown sender looks interesting, I click on a link within it.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When accessing the Internet at work, I visit any website that I want to.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I download any files onto my work computer that will help me get my job done.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

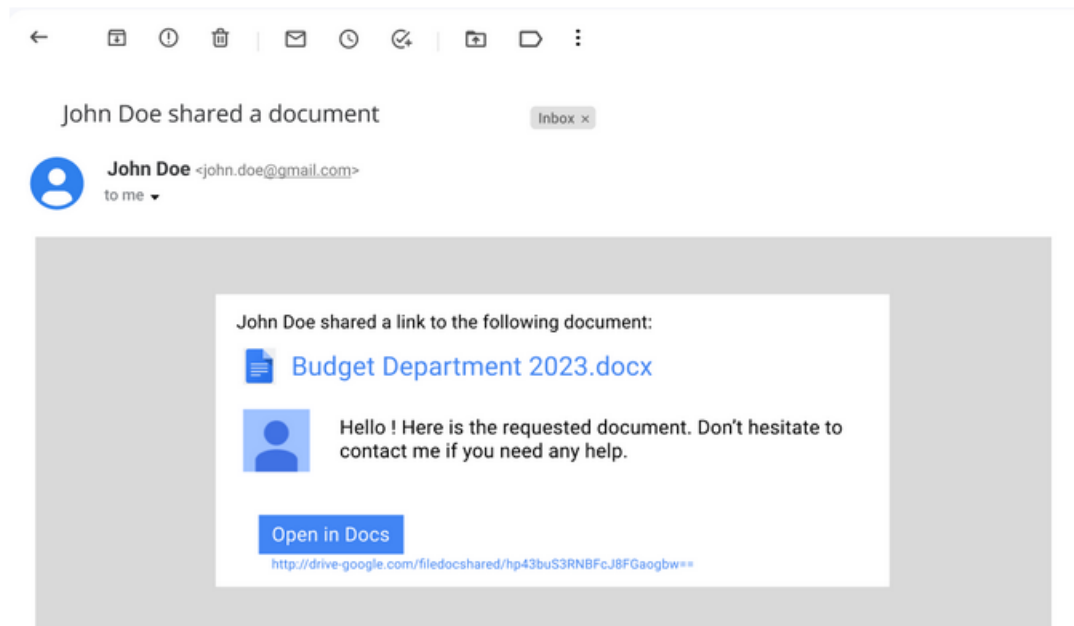
It's always safe to click on links in emails from people I know.



If it helps me to do my job, it doesn't matter what information I put on a website.



Suppose you received the following mail:



Would you classify this mail as phishing?

☐ No

☐ Yes



What about this mail:

Do you remember this photo ??

Inbox x



**John Doe** <john.doe@gmail.com>

to me ▼

Hey :) Do you remember [this photo](#) ??


Would you classify it as phishing?

☐ No

☐ Yes





Now, let's suppose you have received this mail:



[FEDEX] You have **1 PACKAGE** waiting to be delivered

Inbox x

**Fed Ex** <jfed-ex@bandmail.ru>  
to me ▾



Dear Customer,

You have currently **1 package** waiting to be delivered. In order to do so, please complete the delivery information using the following link:

Update delivery info

Package Info

<b>Delivery Reference Number:</b> 29199076US		<b>Delivery expected:</b> 1-2 days	
<b>Product</b>	<b>Name</b>	<b>Quantity</b>	<b>Price</b>
Weight: 550g		1	Unknown

↩ Reply

➦ Forward

Would you classify it as phishing?

☐ No

☐ Yes



New login to Twitter from ChromeMobileAndroid on Android Inbox x



Twitter <verify@twitter.com>  
to me ▾

**We noticed a login to your account from a new device. Was this you ?**



**Location** Texas, USA  
**Device** Android

**If this was you**

You can ignore this message. There's no need to take any action.

**If this wasn't you**

- [Change your password](#). You'll be logged out of all your active Twitter sessions except the one you're using at this time.
- [Review the apps](#) that have access to your account and revoke access to any unfamiliar apps. [Learn more](#).

[Help](#) | [Email security tips](#)

Twitter, Inc. 1355 Market Street, Suite 900 San Francisco, CA 94103

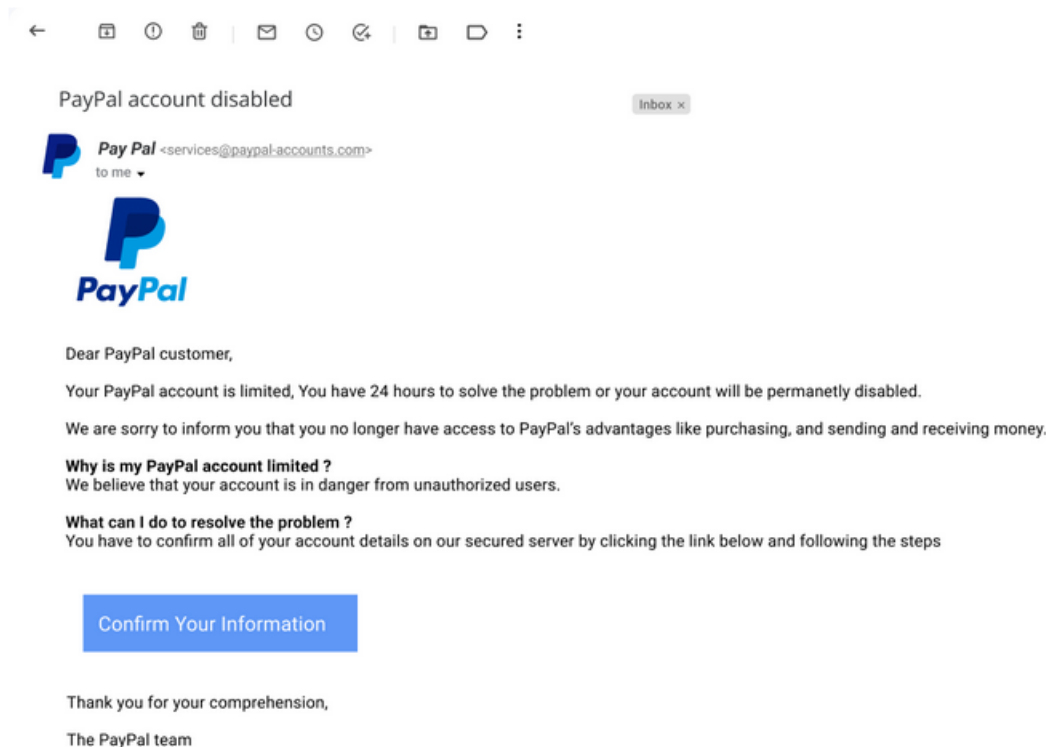
Would you classify it as phishing?

☐ Yes

☐ No



Finally, suppose you received this one:



Would you classify this mail as phishing?

☐ Yes

☐ No

