

# CYBERSECURITY, MY FUTURE CAREER



# AN INITIATION TO CYBERSECURITY IN 3 SEQUENCES

This kit includes three sequences, each composed of several activities.

The sequences are **independent** of each other and can be made **to suit your needs**.

## HOW TO USE THIS KIT?

It is up to you to adapt the language to those you want to convince and to choose the right words for young people by adapting to their concerns!

# SUMMARY

3 BEFORE YOU START

## 5 1 CAREER IN CYBERSECURITY

ACTIVITY 1: CYBER GESTURES

ACTIVITY 2: I AM NOT A HACKER AND YET I WORK IN CYBER SECURITY

ACTIVITY 3: CYBER: A SINGLE JOB OR MULTIPLE?

58 2

## BEWARE OF APPEARANCES!

ACTIVITY 1: AVOID FAKE TECHNICAL SUPPORT SCAMS

ACTIVITY 2: DO NOT LET CYBERCRIMINALS STEAL FROM YOU

87 3

## PROTECT YOUR ACCOUNTS ONLINE!

ACTIVITY 1: A STRONG PASSWORD IS YOUR BEST DEFENCE

ACTIVITY 2: PROTECT YOUR MOST IMPORTANT ACCOUNTS ONLINE

# BEFORE STARTING

Make sure you **have enough time** to complete the sequences you are interested in (approximate duration).



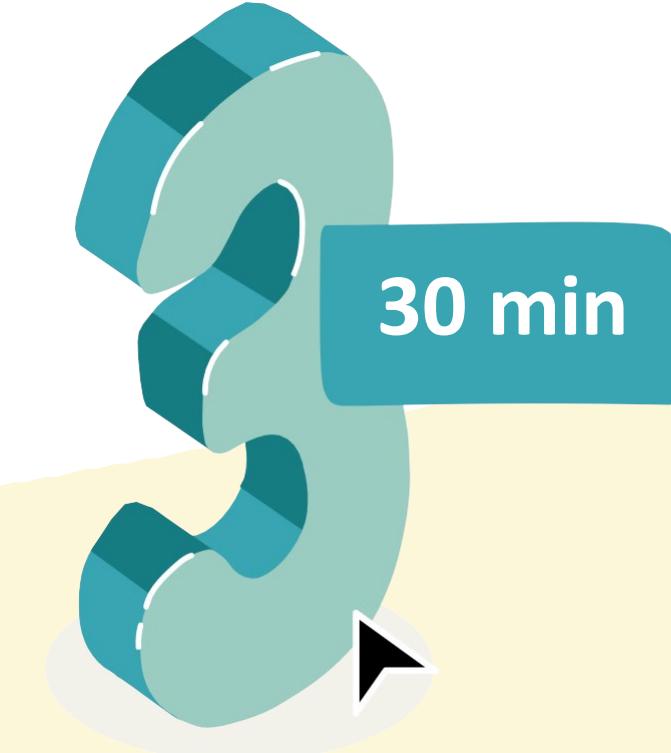
## CAREER IN CYBERSECURITY

Discover the diversity  
of professions



## BEWARE OF APPEARANCES

Be vigilant against online  
scams



## PROTECT YOUR ACCOUNTS ONLINE

Learn how to manage  
passwords

# BEFORE STARTING

Some **golden rules** for a smooth intervention:

**DISTRIBUTE THE FLOOR AMONG THE PARTICIPANTS**

**ENSURE THAT THE OBJECTIVES ARE  
UNDERSTOOD AT THE END OF EACH SEQUENCE**

**CONCLUDE BY SUMMARISING THE IMPORTANT POINTS**



# CAREER in CYBERSECURITY

# WHY DOES CYBERSECURITY CONCERN US ALL?



[SOURCE](#)

# WHY DOES CYBERSECURITY CONCERN US ALL?



SOURCE



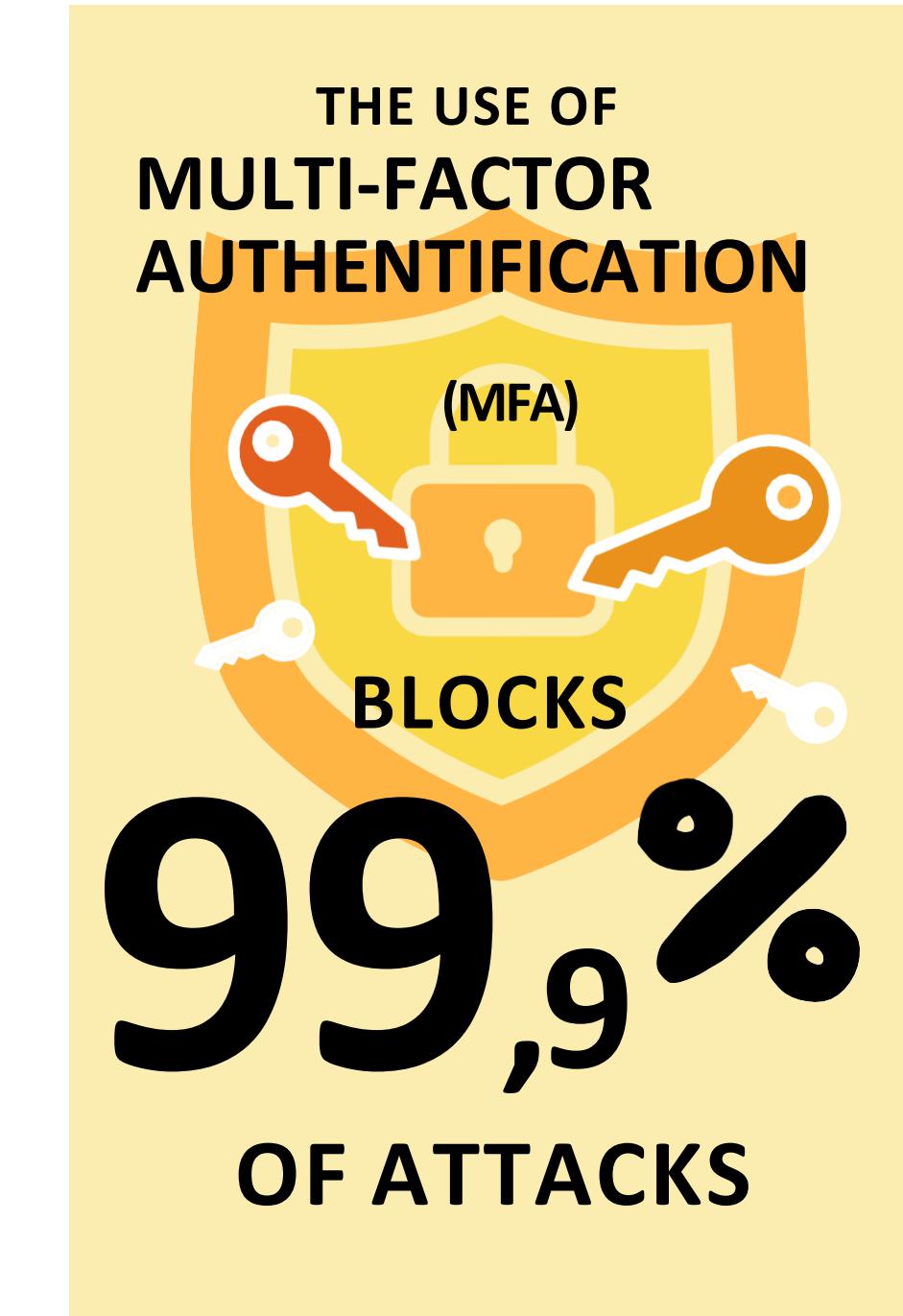
# WHY DOES CYBERSECURITY CONCERN US ALL?



**SOURCE**

**93%** OF ALL SECURITY INCIDENTS COULD HAVE BEEN **AVOIDED** IF BASIC RULES CONCERNING **CYBER HYGIENE** HAD BEEN PUT IN PLACE

This section emphasizes the preventability of many security incidents through better cybersecurity practices.

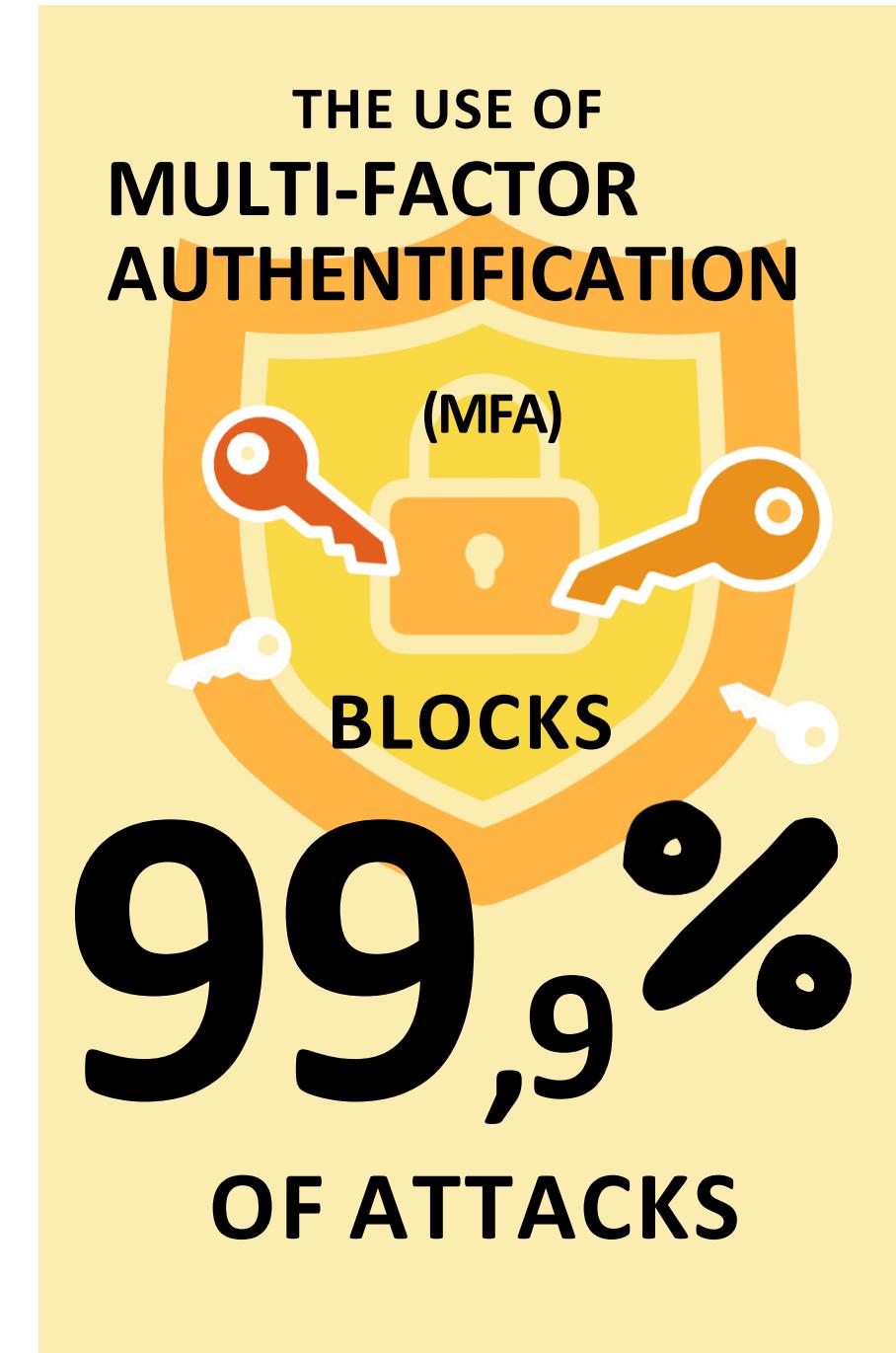


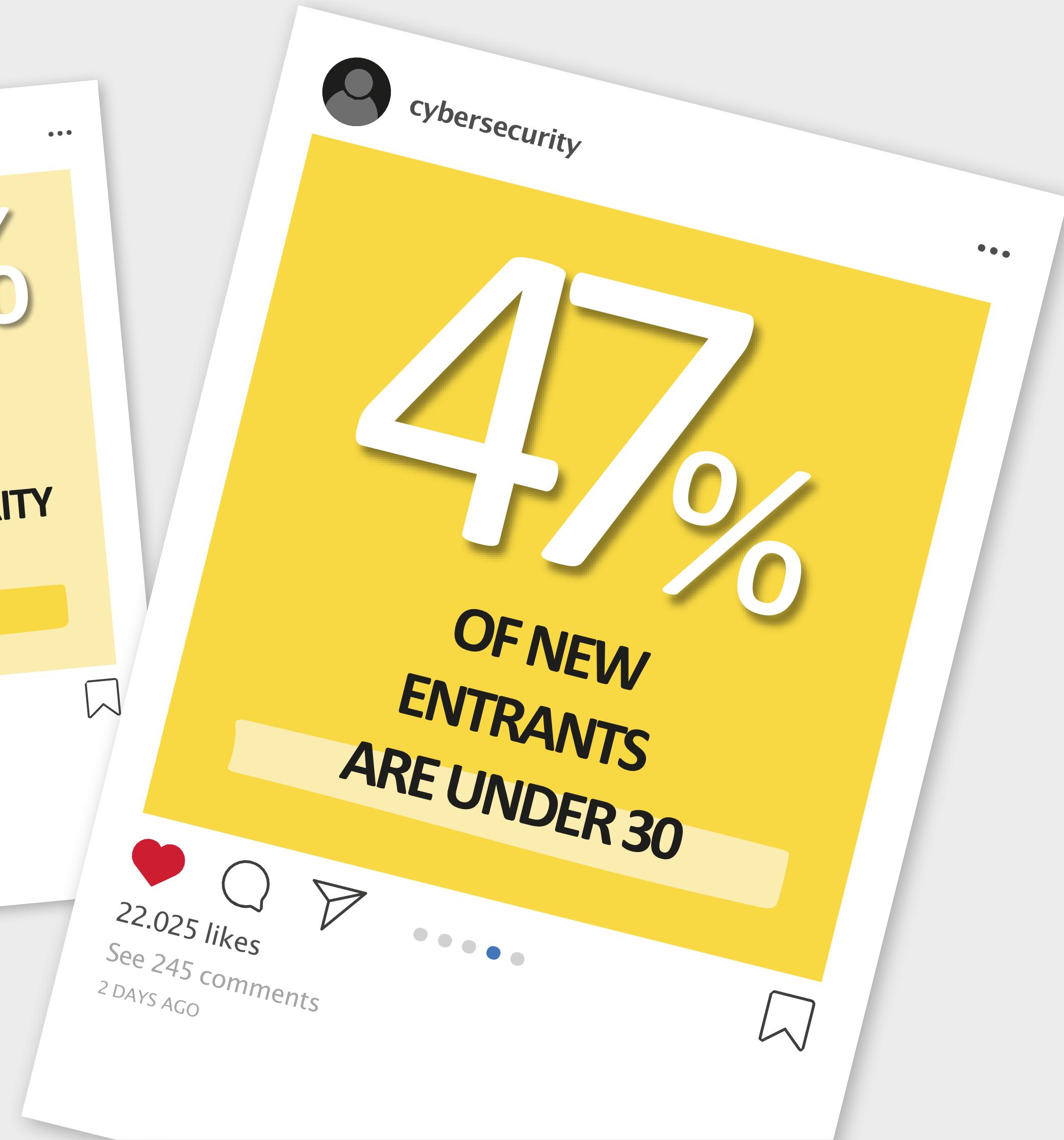
# WHY DOES CYBERSECURITY CONCERN US ALL?

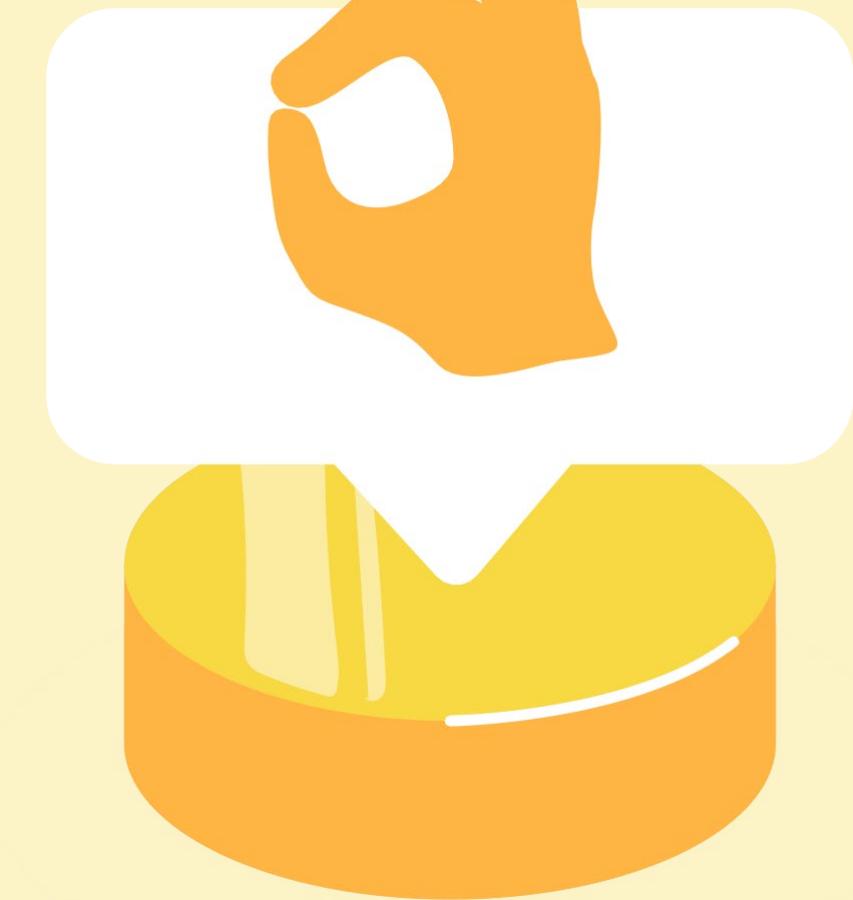


**SOURCE**

**93%** OF ALL SECURITY INCIDENTS COULD HAVE BEEN **AVOIDED** IF BASIC RULES CONCERNING **CYBER HYGIRNE** HAD BEEN PUT IN PLACE







**ACTIVITY 1**  
**CYBER  
GESTURES**

ACTIVITY 1



**GOOD IDEA OR NOT?**

## ACTIVITY 1



Do you think that a good password can be used for several services (mailboxes, social networks, bank, e-commerce sites, administrations...)?

A Yes, when the services have nothing to do with each other

B Yes, but only if the password contains special characters

C No, each service must have a different password

## ACTIVITY 1

Do you think that a good password can be used for several services (mailboxes, social networks, bank, e-commerce sites, administrations...)?

A Yes, when the services have nothing to do with each other

B Yes, but only if the password contains special characters

C No, each service must have a different password



## ACTIVITY 1

You receive an email about the **closure of your Instagram account**. This email contains the Instagram logo and an attachment. You:

A Open the attachment to learn more

B Hesitate to open the attachment but be reassured  
by the Instagram logo

C Do not open the attachment and you log in  
directly to your account

## ACTIVITY 1

You receive an email about the **closure of your Instagram account**. This email contains the Instagram logo and an attachment. You:

A Open the attachment to learn more

B Hesitate to open the attachment but be reassured  
by the Instagram logo

C Do not open the attachment and you log in  
directly to your account

## ACTIVITY 1



You receive a text message telling you that **your package is arriving but that you need to update your delivery details**. You:

**A** Click on the link contained in the SMS

**B** Do nothing

**C** Call the shipper's phone number

## ACTIVITY 1

You receive a text message telling you that **your package is arriving but that you need to update your delivery details**. You:

A Click on the link contained in the SMS

B Do nothing

C Call the shipper's phone number

## ACTIVITY 1

---

You receive an email informing you that photos in which you are tagged are available. The website asks you to enter your Facebook username and password. It seems that the website has a legitimate certificate with a padlock next to the address bar.

**You enter your username and password on the website.**

Is this a good idea or not?

A Yes

B No

## ACTIVITY 1

You receive an email informing you that photos in which you are tagged are available. The website asks you to enter your Facebook username and password. It seems that the website has a legitimate certificate with a padlock next to the address bar.

**You enter your username and password on the website.**

Is this a good idea or not?

A Yes

B No



## ACTIVITY 1

What should you do if a **message appears on your screen blocking your computer**, indicating a serious technical problem, a risk of losing your data or the presence of numerous viruses?

**A** Do nothing

**B** Contact technical support at the number indicated  
on the error message

**C** Attempt to restart your computer and, if the problem  
persists, ask a friend for help

## ACTIVITY 1

What should you do if a **message appears on your screen blocking your computer**, indicating a serious technical problem, a risk of losing your data or the presence of numerous viruses?

**A** Do nothing

**B** Contact technical support at the number indicated  
on the error message

**C** Attempt to restart your computer and, if the problem  
persists, ask a friend for help

## ACTIVITY 1

---

You are at the airport before boarding your flight. You have no battery on your phone. There are public computers available for passengers to surf the Internet. You want to pass the time and go on your favourite social network.

**You launch a browser in private mode, then you authenticate yourself with your password to access your profile.  
Is it safe?**

A Yes

B No

## ACTIVITY 1

You are at the airport before boarding your flight. You have no battery on your phone. There are public computers available for passengers to surf the Internet. You want to pass the time and go on your favourite social network.

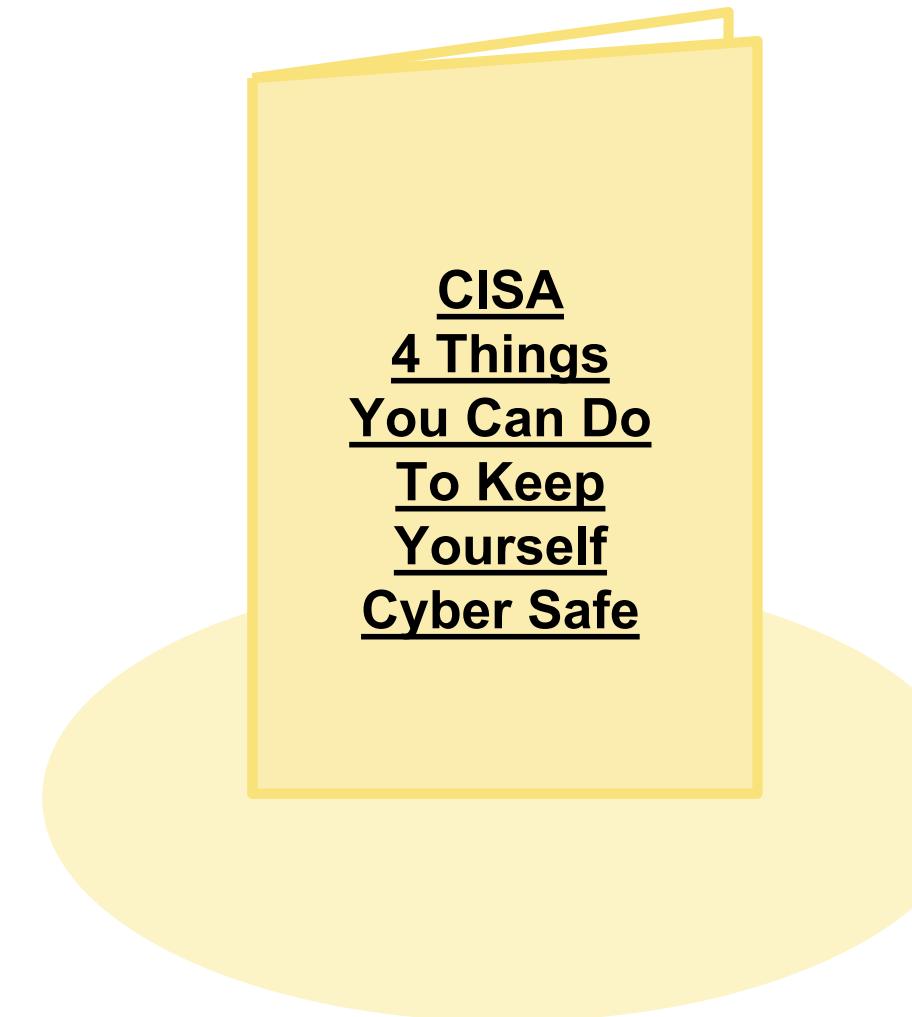
**You launch a browser in private mode, then you authenticate yourself with your password to access your profile.  
Is it safe?**

A Yes

B No



# FOR GOOD DIGITAL HYGIENE



- ◆ Choose your passwords carefully
- ◆ Regularly install updates on your devices
- ◆ Make **regular** backups of your data
- ◆ **Securing** your Wi-Fi access
- ◆ Be as **careful** with your smartphone or tablet as with your computer
- ◆ Be **careful** when using your email
- ◆ Download your apps from the **official websites**
- ◆ Be **vigilant** when paying on the Internet
- ◆ **Taking care of your personal and professional** information and your digital identity



## **A GESTURE TO REMEMBER**

**GET INTO THE HABIT OF LOCKING THE SCREEN OF  
YOUR DEVICES WHEN YOU ARE AWAY FROM THEM TO  
PREVENT UNAUTHORISED ACCESS, ESPECIALLY TO  
PREVENT IN CASE THEY ARE LOST OR STOLEN.**

## ACTIVITY 2



I AM NOT A HACKER AND  
YET I WORK IN CYBER  
SECURITY

## ACTIVITY 2

# WHAT DOES YOUR JOB INVOLVE?

- How did you get into cybersecurity?
- What do you like about your job?
- What is a typical day in cybersecurity like?
- Do you need to speak English to do your job?
- Have you ever been a victim of a virus or phishing attack?
- What are your three cybersecurity tips?
- What would you say to young people who are hesitating to get into cybersecurity?



A collection of 20 YouTube video thumbnails arranged in a grid, each with a yellow border. The thumbnails show various cybersecurity professionals, such as a woman in a black top, a man in a suit, and a person in a lab coat, along with titles like "Zoom sur les métiers de la Cybersécurité", "Des femmes dans la cyber", and "Le bug bounty: quand les hackers volent au secours des entreprises". A red plus sign is located in the bottom right corner of the grid.



# SHAKING UP PRECONCEIVED IDEAS ABOUT THE CYBERSECURITY PROFESSION

ACTIVITY 2

A horizontal yellow bar with three small circular markers at regular intervals. The first marker is a yellow circle with a black outline. The second marker is a yellow circle with a black outline. The third marker is a light yellow circle with a black outline.

**TRUE OR FALSE?**

**IT'S A SECTOR THAT RECRUITS A  
LOT**

ACTIVITY 2



# IT'S A SECTOR THAT RECRUITS A LOT

Yes, the cybersecurity sector is recruiting a lot and around the world. There is a shortage of talent in the cybersecurity field with several million vacancies worldwide.



## ACTIVITY 2

**TRUE OR FALSE?**

**TO WORK IN  
CYBERSECURITY YOU NEED  
TO BE AN ENGINEER**

ACTIVITY 2

TRUE **FALSE** SE?

**TO WORK IN  
CYBERSECURITY YOU NEED  
TO BE AN ENGINEER**

No, working in cybersecurity does not necessarily mean being an engineer. There are also non-technical jobs, such as awareness-raising and all the cybersecurity jobs involving commercial and legal aspects.

ACTIVITY 2



**TRUE OR FALSE?**

**CYBERSECURITY  
MEANS BEING GOOD  
AT MATH**

ACTIVITY 2

**TRUE FALSE ?**

**CYBERSECURITY  
MEANS BEING GOOD  
AT MATH**

Cybersecurity is all about common sense, critical thinking and knowledge. This does not mean that you should not be good at maths!



## ACTIVITY 2

**TRUE OR FALSE?**

**THESE ARE JOBS WHERE  
YOU HAVE TO KNOW  
HOW TO CODE**

ACTIVITY 2

TRUE **FALSE** TRUE?

# THESE ARE JOBS WHERE YOU HAVE TO KNOW HOW TO CODE

Cybersecurity encompasses many fields, and it is therefore difficult to give a general answer. Some cybersecurity jobs do require the ability to code, such as security solutions developer or technical security auditor. Others, on the other hand, do not, such as cybersecurity consultant or Information Systems Security Manager (ISSM).

ACTIVITY 2



TRUE OR FALSE?

**THESE ARE NOT JOBS  
FOR WOMEN**

**ACTIVITY 2**

**FALSE**  
TRUE OR FALSE?

**THESE ARE NOT JOBS  
FOR WOMEN**

There is no reason why cybersecurity jobs should not be for women.  
Cybersecurity jobs are open to women, but they are often underrepresented in this industry.

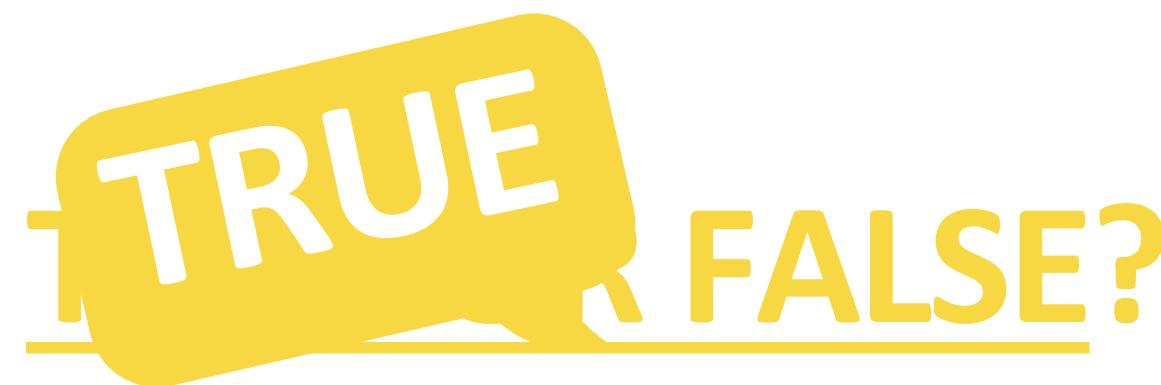


## ACTIVITY 2

TRUE OR FALSE?

**YOU DON'T NEED TO STUDY A  
LONG CAREER**

**ACTIVITY 2**



# **YOU DON'T NEED TO STUDY A LONG CAREER**

You do not need to study for a long time to work in cyber security,  
but it is important to have a good understanding of the basic  
concepts of computer security.

ACTIVITY 2

A horizontal yellow bar with three small circular markers at regular intervals. The first marker is larger and has a yellow gradient background with a white circle in the center. The second marker is smaller and has a white gradient background with a yellow circle in the center. The third marker is a small yellow dot.

TRUE OR FALSE?

**CYBERSECURITY JOBS  
ARE NOT WELL PAID**

ACTIVITY 2



**FALSE**  
TRUE OR FALSE?

# CYBERSECURITY JOBS ARE NOT WELL PAID

Cybersecurity jobs are rather well paid.  
They pay an average of \$105,800 per year. ([Source](#))

ACTIVITY 2



## TO REMEMBER:

CYBERSECURITY JOBS ARE  
AVAILABLE TO EVERYONE!



**ACTIVITY 3**

**CYBER, A  
SINGLE JOB OR  
MULTIPLE  
JOBS?**



# PREVENT OR CURE?

# PREVENT

Research | Design

Raise awareness | Manage

# CURE

React | Investigate

Improve | Rebuild



# ETHICAL HACKER



# PREVENT

Research | Design

Raise awareness | Manage

ETHICAL HACKER

# CURE

React | Investigate

Improve | Rebuild



# CYBERSECURITY CONSULTANT



# PREVENT

Research | Design

Raise awareness | Manage

**ETHICAL HACKER**  
**CYBERSECURITY**  
**CONSULTANT**



# CURE

React | Investigate

Improve | Rebuild

**CYBERSECURITY**  
**CONSULTANT**

# PREVENT

Research | Design

Raise awareness | Manage

**ETHICAL HACKER**  
**CYBERSECURITY**  
**CONSULTANT**



# CURE

React | Investigate

Improve | Rebuild

**CYBERSECURITY**  
**CONSULTANT**  
**INCIDENT**  
**RESPONSE**  
**ANALYST**

# PREVENT

Research | Design

Raise awareness | Manage

ETHICAL HACKER

CYBERSECURITY  
CONSULTANT

CYBERSECURITY  
ARCHITECT



# CYBERSECURITY CRISIS MANAGER



# CURE

React | Investigate

Improve | Rebuild

CYBERSECURITY  
CONSULTANT

INCIDENT  
RESPONSE  
ANALYST

CYBERSECURITY  
ARCHITECT

# PREVENT

Research | Design

Raise awareness | Manage

**ETHICAL HACKER**

**CYBERSECURITY  
CONSULTANT**

**CYBERSECURITY  
ARCHITECT**

# CURE

React | Investigate

Improve | Rebuild

**CYBERSECURITY  
CONSULTANT**

**INCIDENT  
RESPONSE  
ANALYST**

**CYBERSECURITY  
ARCHITECT**

**CYBERSECURITY  
CRISIS MANAGER**



# PREVENT

Research | Design

Raise awareness | Manage

**ETHICAL HACKER**

**CYBERSECURITY  
CONSULTANT**

**CYBERSECURITY  
ARCHITECT**

**CRYPTOLOGIST**



# SECURITY SYSTEMS ADMINISTRATOR



# CURE

React | Investigate

Improve | Rebuild

**CYBERSECURITY  
CONSULTANT**

**INCIDENT  
RESPONSE  
ANALYST**

**CYBERSECURITY  
ARCHITECT**

**CYBERSECURITY  
CRISIS MANAGER**

# PREVENT

Research | Design

Raise awareness | Manage

ETHICAL HACKER

CYBERSECURITY  
CONSULTANT

CYBERSECURITY  
ARCHITECT

CRYPTOLOGIST

SECURITY  
SYSTEMS

ADMINISTRATOR

# CURE

React | Investigate

Improve | Rebuild

CYBERSECURITY  
CONSULTANT

INCIDENT  
RESPONSE  
ANALYST

CYBERSECURITY  
ARCHITECT

CYBERSECURITY  
CRISIS MANAGER



# CYBERSECURITY TRAINER

# PREVENT

Research | Design

Raise awareness | Manage

ETHICAL HACKER

CYBERSECURITY  
CONSULTANT

CYBERSECURITY  
ARCHITECT

CRYPTOLOGIST

SECURITY  
SYSTEM

ADMINISTRATOR

CYBERSECURITY  
TRAINER

ISSM

# CURE

React | Investigate

Improve | Rebuild

CYBERSECURITY  
CONSULTANT

INCIDENT  
RESPONSE  
ANALYST

CYBERSECURITY  
ARCHITECT

CYBERSECURITY  
CRISIS MANAGER

# INFORMATION SYSTEMS SECURITY MANAGER (ISSM)

# PREVENT

Research | Design

Raise awareness | Manage

**ETHICAL HACKER**

**CYBERSECURITY  
CONSULTANT**

**CYBERSECURITY  
ARCHITECT**

**CRYPTOLOGIST**

**SECURITY  
SYSTEM**

**ADMINISTRATOR**

**CYBERSECURITY  
TRAINER**

**ISSM**

# CURE

React | Investigate

Improve | Rebuild

**CYBERSECURITY  
CONSULTANT**

**INCIDENT  
RESPONSE  
ANALYST**

**CYBERSECURITY  
ARCHITECT**

**CYBERSECURITY  
CRISIS MANAGER**





## TO REMEMBER:

CYBERSECURITY JOBS ARE VARIED AND MEANINGFUL



**BEWARE OF  
APPAREANCES**

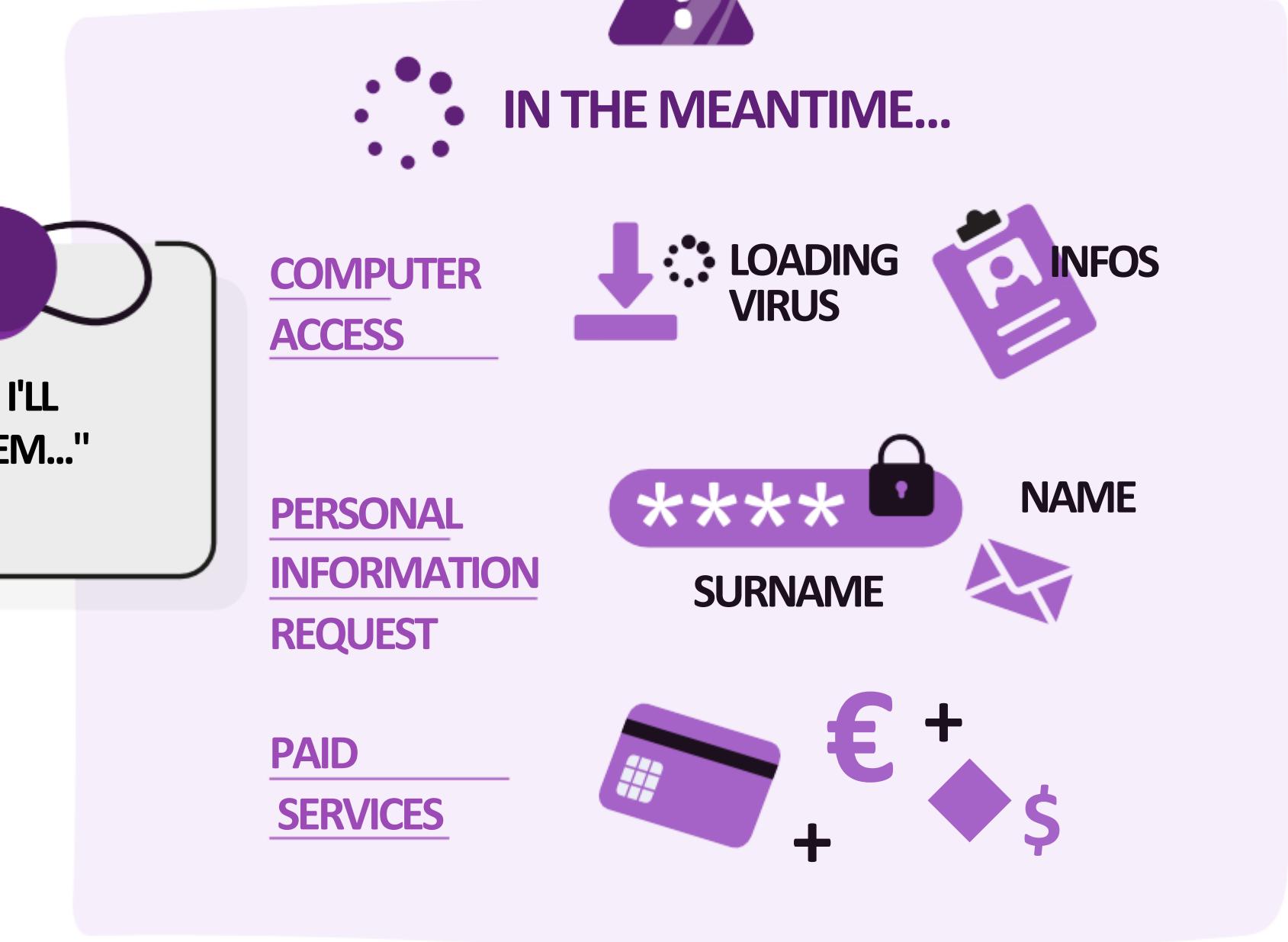
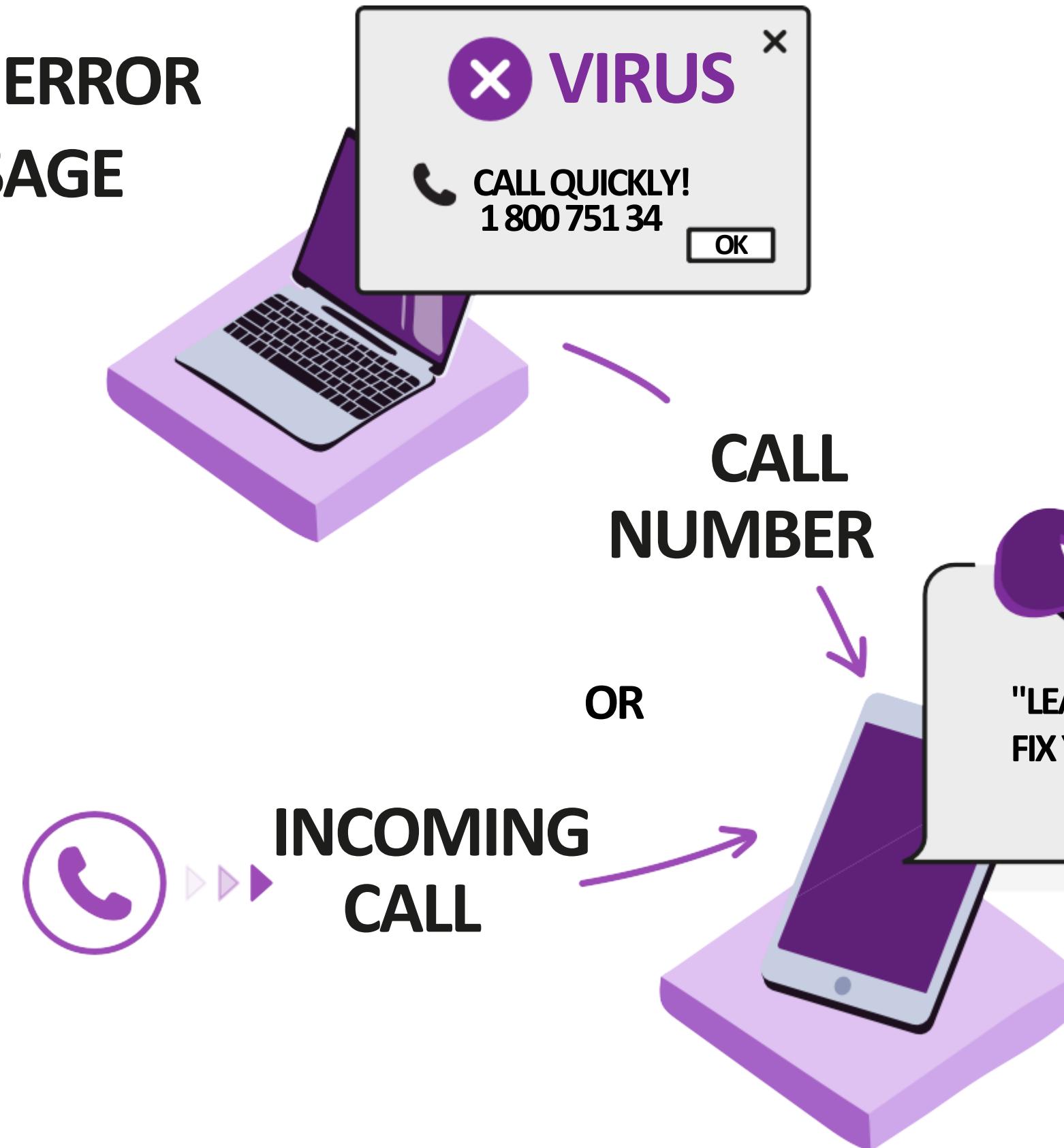


## **ACTIVITY 1**

# **AVOID FAKE TECHNICAL SUPPORT SCAMS**

## ACTIVITY 1

### FAKE ERROR MESSAGE



# HOW TO REACT IF SOMEONE CALLS YOU OR IF A FAKE ERROR MESSAGE IS DISPLAYED?

- 1 HANG UP**
- 2 DO NOT PERFORM ANY MANIPULATION ON YOUR DEVICE**
- 3 DO NOT COMMUNICATE WITH STRANGERS**
- 4 CALL AN AUTHENTIC NUMBER DIRECTLY**
- 5 PROTECT YOUR COMPUTER**
- 6 UPDATE YOUR WEB BROWSER AND OPERATING SYSTEM**
- 7 ENABLE YOUR POP-UP BLOCKER**
- 8 CLOSE YOUR BROWSER**
- 9 RESTART YOUR DEVICE**
- 10 TALK ABOUT IT**



## TO REMEMBER:

**DO NOT CLICK ON URGENT MESSAGES THAT APPEAR WHILE YOU ARE ONLINE AND DO NOT DIAL THE NUMBER PROVIDED**

**HANG UP IF YOU ARE ASKED TO DO SOMETHING ON YOUR COMPUTER**

**NEVER DOWNLOAD AN APPLICATION AT THE REQUEST OF SOMEONE YOU DON'T KNOW**

**REPORT SCAMS TO THE POLICE**

**IF YOU COME ACROSS A SCAM, TELL A FRIEND, COLLEAGUE OR FAMILY MEMBER TO MAKE THEM AWARE OF THIS ABOUT THIS THREAT**



**ACTIVITY 2**  
**DO NOT LET  
CYBERCRIMINALS  
STEAL FROM YOU**



**TO CLICK OR NOT TO CLICK?**

# TO CLICK OR NOT TO CLICK?

The screenshot shows a Google Mail inbox with a single email from "World Health Organization <eeeeekrodou@sch.gr>". The subject is "(no subject)". The email body contains a message from Timmy Bridges, Health Communications Manager at the United Nations Foundation, regarding a COVID-19 relief grant. It includes fields for Full Names, Contact Address, Occupation, Phone Number, and Valid Identification, and ends with a signature.

https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=i7iyx0m0rxgx&cat=INBOX%2FPhising&sear...

(no subject) ➤ INBOX/Phising X

World Health Organization <eeeeekrodou@sch.gr> Fri, 1 May 2020, 13:26

to

--

World Health Organization(WHO) and United Nations(UN) swings into action.

You are Entitled to \$50,000 USD per week relief grant, in a bid to control the spread of the COVID-19 pandemic. Respond with the below details for claims.

Full Names:  
Contact Address:  
Occupation:  
Phone Number:  
Valid Identification:

Thanks and my best regards to your family,

Timmy Bridges  
Health Communications Manager  
United Nations Foundation

Reply Forward

# TO CLICK OR NOT TO CLICK?

The email address sending the email does not correspond to the official website address. Also, be careful with e-mails offering money or goods. When it is too good to be true, it's because it is!



https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=i7iyx0m0rxgx&cat=INBOX%2FPhising&sear...

(no subject) ➤ INBOX/Phising X

World Health Organization <eeeeekrodou@sch.gr> Fri, 1 May 2020, 13:26 ☆ ↶ :

✉ to ▾

--

World Health Organization(WHO) and United Nations(UN) swings into action.

You are Entitled to \$50,000 USD per week relief grant, in a bid to control the spread of the COVID-19 pandemic. Respond with the below details for claims.

Full Names:  
Contact Address:  
Occupation:  
Phone Number:  
Valid Identification:

Thanks and my best regards to your family,

Timmy Bridges  
Health Communications Manager  
United Nations Foundation

Reply Forward

# TO CLICK OR NOT TO CLICK?

Notice: your package will be returned to the sender: <https://yesdetail.com/d/?pn4cqiha70>

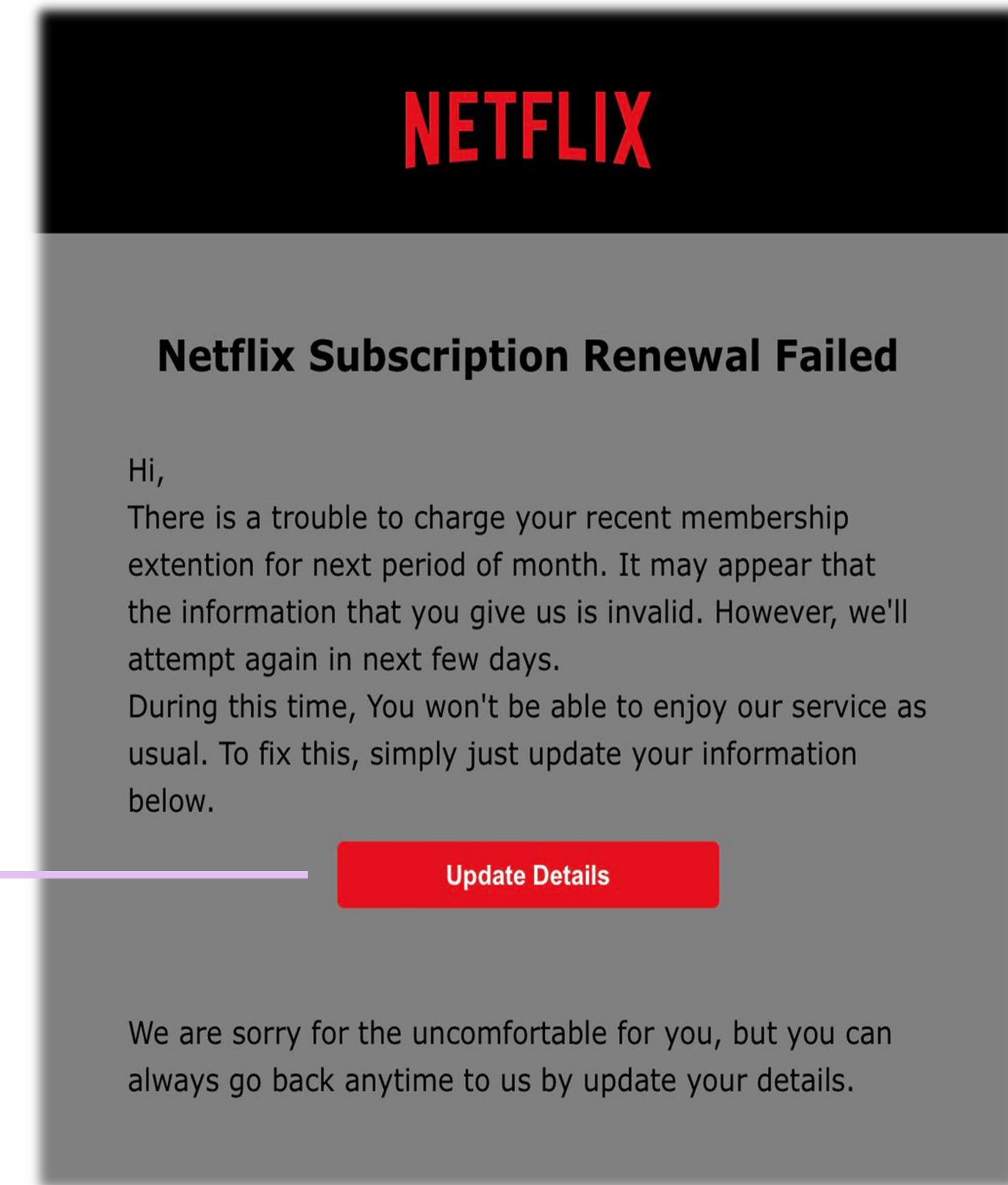
# TO CLICK OR NOT TO CLICK?



Beware of messages that require an immediate response or action. There is a good chance that this destination address is a scam, as it does not correspond to the official website address.

Notice: your package will be returned to the sender: <https://yesdetail.com/d/?pn4cqiha70>

# TO CLICK OR NOT TO CLICK?



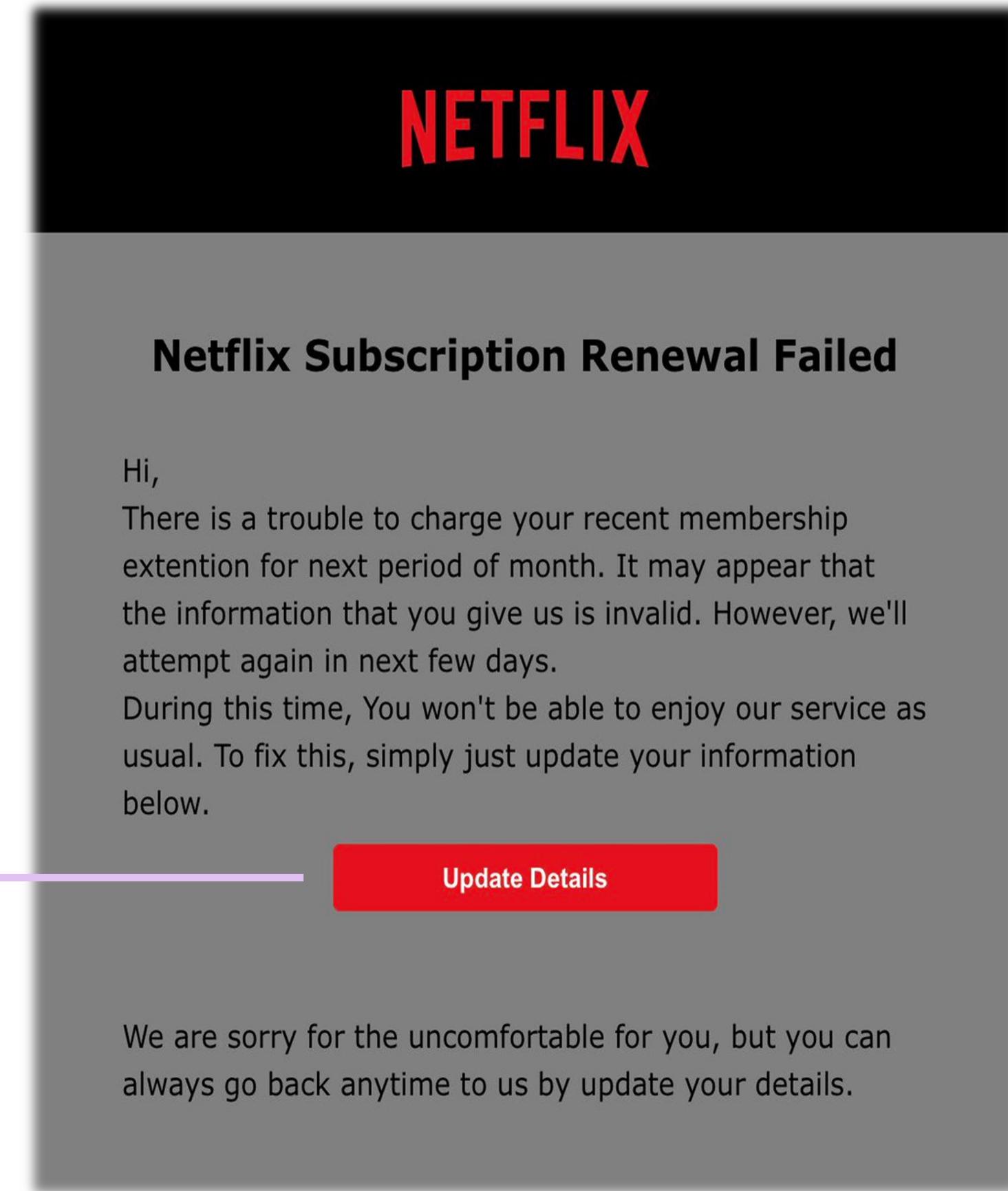
<http://impresasavoldelli.it>

# TO CLICK OR NOT TO CLICK?

There is a good chance that this destination address is a scam. It does not correspond to the official website address, and the "http:" link indicates that the connection is not secure, which should make you suspicious.

NO

<http://impresasavoldelli.it>





# TO CLICK OR NOT TO CLICK?

Attn: Your-150 Dollar Prime Credit Expires on 12/28. Shopper: [REDACTED] Spam x



Amazon Update <AmazonUpdate@efficaciousrbays.xyz>  
to me

**A** Why is this message in Spam? It's similar to messages that were detected by our spam filters. [Learn more](#)



The Amazon Marketplace

-----SHOPPER/MEMBER:4726  
-----DATE-OF-NOTICE: 12/22/2015

Hello Shopper! @gmail.com! To show you how much we truly value your years of business with us and to celebrate the continued success of our Prime membership program, we're rewarding you with-\$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)

In order to use this-\$100 reward, simply go below to get your-coupon-card and then just use it during checkout on your next purchase. That's all there is to it!

[Please visit-here now to get your reward](#)

\*\*\*DON'T WAIT! The Link Above Expires on 12/28!

# TO CLICK OR NOT TO CLICK?

The email address sending the email does not correspond to the official website address. Beware of messages that require an immediate response or action. Also, be careful with e-mails offering money or goods. When it is too good to be true, it because it is!



Attn: Your-150 Dollar Prime Credit Expires on 12/28. Shopper: [REDACTED] Spam x



Amazon Update <AmazonUpdate@efficaciousrbays.xyz>  
to me

**A** Why is this message in Spam? It's similar to messages that were detected by our spam filters. [Learn more](#)



The Amazon Marketplace

-----SHOPPER/MEMBER:4726  
-----DATE-OF-NOTICE: 12/22/2015

Hello Shopper: [REDACTED] @gmail.com! To show you how much we truly value your years of business with us and to celebrate the continued success of our Prime membership program, we're rewarding you with-\$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)

In order to use this-\$100 reward, simply go below to get your-coupon-card and then just use it during checkout on your next purchase. That's all there is to it!

[Please visit-here now to get your reward](#)

\*\*\*DON'T WAIT! The Link Above Expires on 12/28!



# TO CLICK OR NOT TO CLICK?

**Microsoft offers you an  
XBOX One.**

Congratulations, you've  
won! Get your console:

<https://www.microsoft.com/>



# TO CLICK OR NOT TO CLICK?

NO

**Microsoft offers you an  
XBOX One.**

Congratulations, you've  
won! Get your console:

<https://www. microsoft.com/>



The destination domain name is  
not exactly the same as the to the  
official website address.

Attention: a small dot appears  
below the first "o" in the word  
microsoft.

This type of scam is called typosquatting,  
i.e., using a letter that is graphically close  
to another one to make people think they  
are on an official website.

# YOU HAVE A DOUBT ABOUT THE MESSAGE YOU RECEIVED?

- ❖ **Don't be afraid!** You probably don't have anything incriminating to blame yourself for
- ❖ **Do not open links or attachments** without being sure of the reliability of the sender
- ❖ **Check the sender's address:** contact him through another channel.
- ❖ **Do not respond to any suspicious or blackmail emails** to avoid show the sender that you are receptive to the message
- ❖ **Change your passwords, avoid having the same password** for each account to protect yourself from cascading attacks and, if possible, **activate double authentication on your most sensitive accounts**, including your email accounts
- ❖ **Delete the message**



## AND IF YOU HAVE DISCLOSED YOUR PASSWORD OR PERSONAL INFORMATION?

- 1** Immediately change passwords for compromised accounts
- 2** Report the scams, by contacting the local authorities
- 3** Visit your national platforms or helplines for assistance to victims of cyberbullying for more advice

## AND IF YOU HAVE PAID AND ARE A VICTIM OF A SCAM?

- 1** Change passwords for compromised accounts immediately
- 2** Contact your bank to try to get the payment reversed
- 3** File a complaint with your local authorities

## HOW TO SPOT A SCAM RECEIVED BY EMAIL OR SMS?

## HOW TO SPOT A SCAM RECEIVED BY EMAIL OR SMS?



**BEWARE OF  
UNKNOWN  
SENDERS**

## HOW TO SPOT A SCAM RECEIVED BY EMAIL OR SMS?



**BEWARE OF  
UNKNOWN  
SENDERS**



**PAY ATTENTION  
TO THE  
WORDING OF  
THE  
EMAIL/TEXT**

## HOW TO SPOT A SCAM RECEIVED BY EMAIL OR SMS?



BEWARE OF  
UNKNOWN  
SENDERS



PAY ATTENTION  
TO THE  
WORDING OF  
THE  
EMAIL/TEXT



THE SENDER'S  
EMAIL ADDRESS  
IS NOT A  
RELIABLE  
CRITERION

## HOW TO SPOT A SCAM RECEIVED BY EMAIL OR SMS?



BEWARE OF  
UNKNOWN  
SENDERS



PAY ATTENTION  
TO THE  
WORDING OF  
THE  
EMAIL/TEXT



THE SENDER'S  
EMAIL ADDRESS  
IS NOT A  
RELIABLE  
CRITERION



CHECK  
THE LINKS

## HOW TO SPOT A SCAM RECEIVED BY EMAIL OR SMS?



BEWARE OF  
UNKNOWN  
SENDERS



PAY ATTENTION  
TO THE  
WORDING OF  
THE  
EMAIL/TEXT



THE SENDER'S  
EMAIL ADDRESS  
IS NOT A  
RELIABLE  
CRITERION



CHECK  
THE LINKS



BEWARE OF  
STRANGE,  
URGENT AND  
TOO GOOD TO  
BE TRUE  
REQUESTS



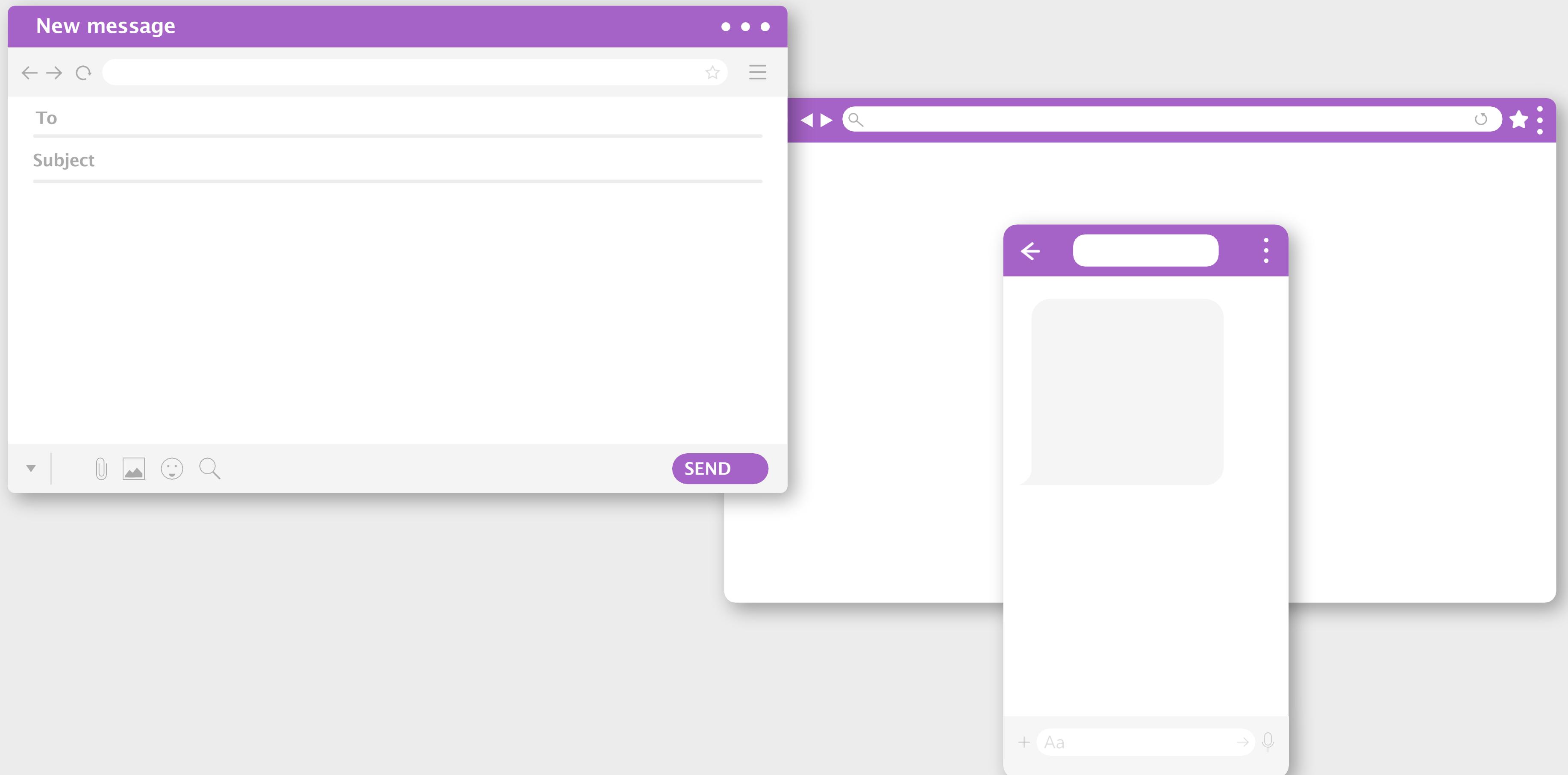
# **CREATE YOUR OWN**

---



## **SCAM**

## ACTIVITY 2





**ONLINE FRAUD IS A CRIMINAL OFFENCE WHICH  
MAY BE PUNISHED BY JAIL TIME AND PENALTIES**



## TO REMEMBER:

BE CAUTIOUS ABOUT  
MESSAGES WITH VISUALS  
THAT LOOK OFFICIAL BUT  
ARE POORLY DISPLAYED OR  
HAVE SPELLING MISTAKES

BEWARE OF  
MESSAGES THAT  
REQUIRE YOU TO  
RESPOND OR TAKE  
IMMEDIATE ACTION

NEVER CLICK ON A LINK OR AN  
ATTACHMENT WHOSE ORIGIN  
OR NATURE SEEMS DOUBTFUL

REMEMBER THAT IF IT  
SOUNDS TOO GOOD TO BE  
TRUE, IT PROBABLY IS!

IF IN DOUBT, YOU SHOULD  
ACCESS THE WEBSITE BY  
TYPING THE ADDRESS  
DIRECTLY INTO THE  
SEARCH BAR

BEFORE INSTALLING  
AN APPLICATION,  
ASK YOURSELF IF YOU  
REALLY NEED IT!



IF YOU HAVE NOT ENTERED A  
COMPETITION, YOU CANNOT  
HAVE WON A PRIZE!





**PROTECT  
YOUR  
ACCOUNTS  
ONLINE**



## ACTIVITY 1

# A STRONG PASSWORD, IS YOUR BEST DEFENCE

## ACTIVITY 1

\*\*\*\*\*



\*\*\*\*



\*\*\*\*\*



\*\*\*\*\*



**CHOOSE A PASSWORD THAT  
IS DIFFERENT  
FOR EACH ACCOUNT**

### WHAT ARE THE RISKS OF USING THE SAME PASSWORD EVERYWHERE?

#### A HACKER COULD:

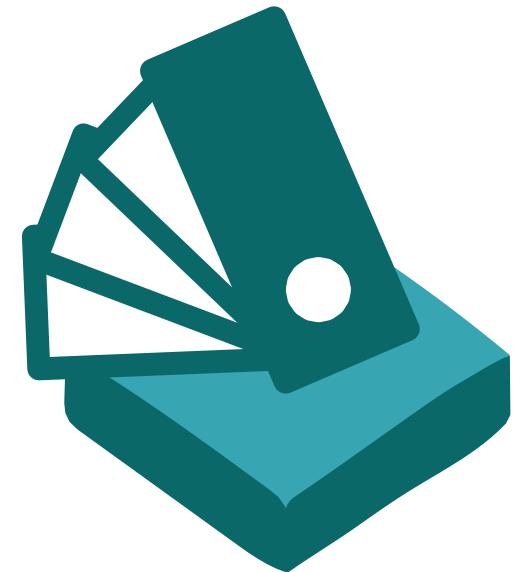
- ❖ Steal your identity
- ❖ Hack into your bank details and make fraudulent purchases
- ❖ Steal your contacts by hacking into your mailboxes/social networks
- ❖ Blackmail you and demand a ransom (in case of compromising data)

**ACTIVITY 1**

---

# **CREATE A STRONG PASSWORD**

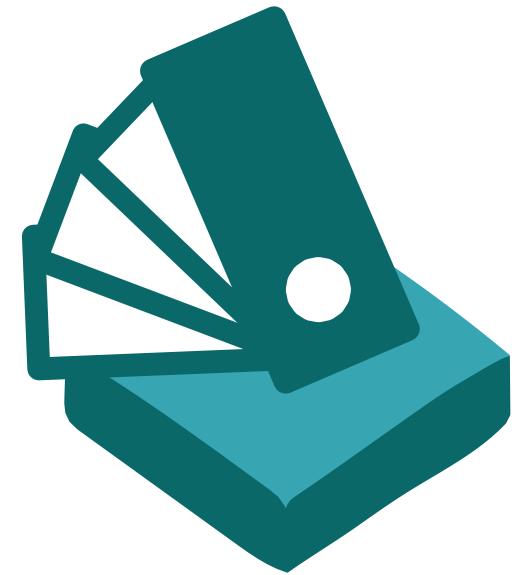
# CREATE A STRONG PASSWORD



## COMPLETE

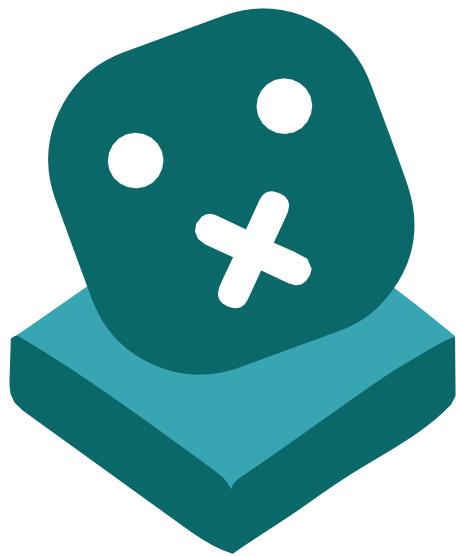
contains at least **14**  
**characters** and **4 different**  
**types**: lower case, upper  
case, numbers and special  
characters (!, ?, €, #...)

# CREATE A STRONG PASSWORD



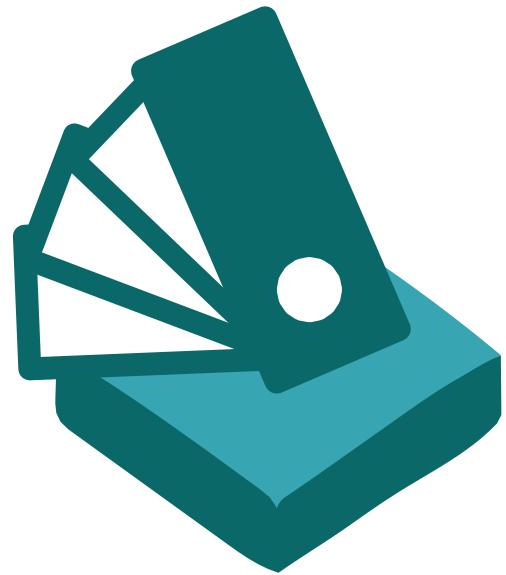
## COMPLETE

contains at least **14** characters and **4 different types**: lower case, upper case, numbers and special characters (!, ?, €, #...)



## SAYS NOTHING ABOUT YOU

# CREATE A STRONG PASSWORD



## COMPLETE

contains at least 14  
**characters** and **4 different types**: lower case, upper case, numbers and special characters (!, ?, €, #...)



## SAYS NOTHING ABOUT YOU



## UNIQUE

ACTIVITY 1

## 2 TIPS:

I am **not a hacker & yet I work in cybersecurity!**

lanah&ylwic!



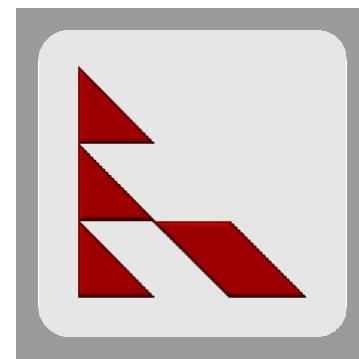
SwanEdgeDoorWork



PASSPHRASE

COMBINED WORDS

# USE A PASSWORD MANAGER



PASSWORDSAFE



ZENWAY



KEEPASS

The screenshot shows the KeePass application window titled "My KeePass.kdbx - KeePass". The interface includes a toolbar with various icons, a search bar, and a context menu on the right side. The main area displays a table of saved entries:

Title	User Name	Password	URL	Notes
Airbnb	*****	*****	https://www.airbnb.fr/	
Amazon	*****	*****	https://www.amazon.fr/	
Booking	*****	*****	https://www.booking.com/	
Deezer	*****	*****	https://www.deezer.com/	
Discord	*****	*****	https://discord.com/	
DropBox	*****	*****	https://www.dropbox.com/	
Facebook	*****	*****	https://www.facebook.com/	
Gmail	*****	*****	https://mail.google.com/	
Hotmail	*****	*****	https://outlook.live.com/	
Instagram	*****	*****	https://www.instagram.com	
LinkedIn	*****	*****	https://www.linkedin.com/	
Netflix	*****	*****	https://www.netflix.com	
Outlook	*****	*****	https://www.outlook.com	
Paypal	*****	*****	https://www.paypal.com	
Steam	*****	*****	https://store.steampowered.com	
Twitter	*****	*****	https://twitter.com/	
Uber	*****	*****	https://www.uber.com	

At the bottom of the window, there is a status bar with the text "Group: Perso, Title: LinkedIn, User Name: \*\*\*\*\*, Password: \*\*\*\*\*, URL: https://www.linkedin.com/, Creation Time: 9/1/2014 9:27:21 PM, Last Modification Time: 3/30/2022 8:58:56 AM".

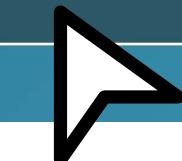
# IS YOUR PASSWORD COMPROMISED?

';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format)

pwned?



ACTIVITY 1



## **TO REMEMBER:**

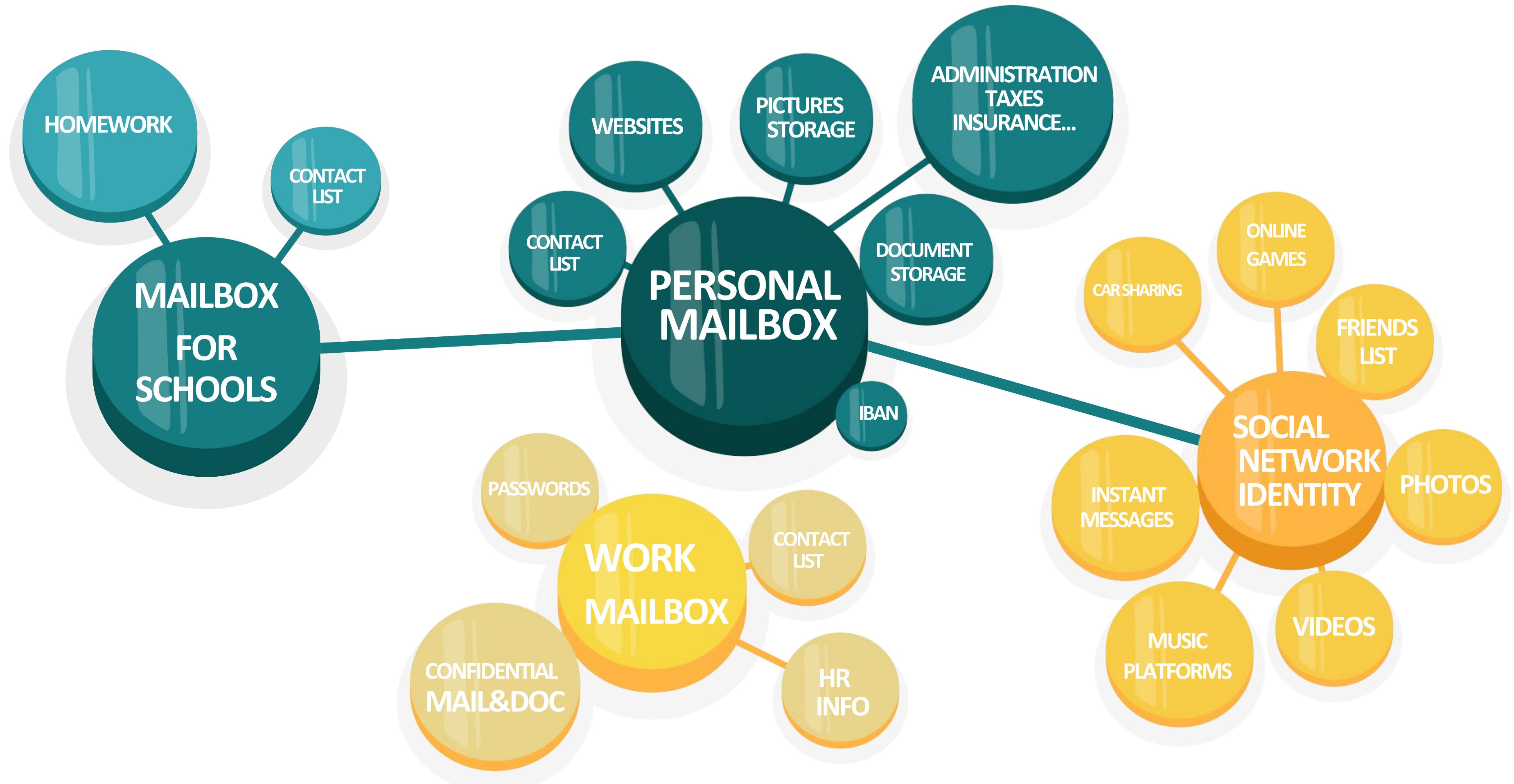
**SECURE ACCOUNTS AND DEVICES WITH STRONG PASSWORDS  
OR PASSPHRASES**

**ENSURE THAT PASSWORDS OR PASSPHRASES ARE UNIQUE FOR  
EACH ACCOUNT AND DEVICE**

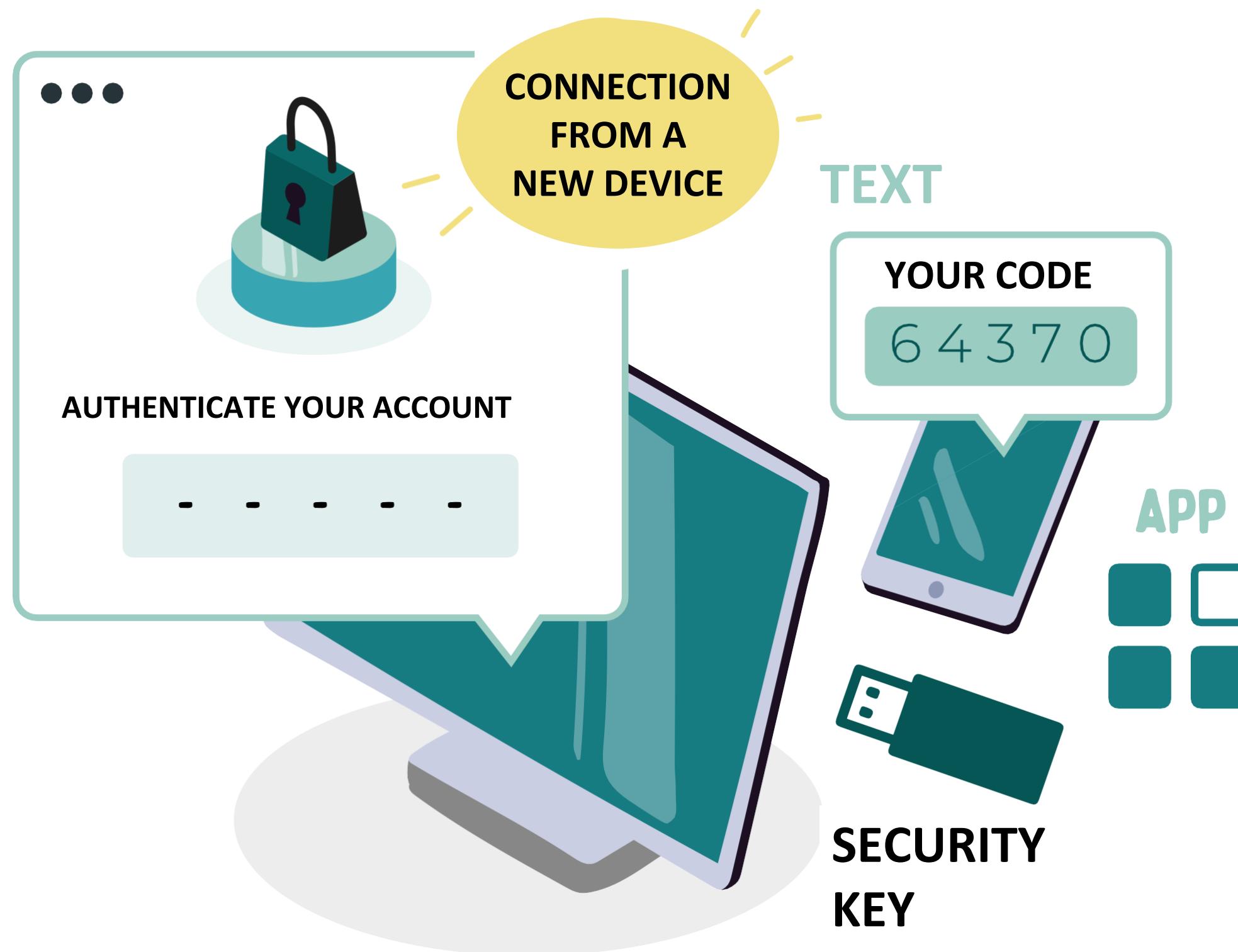


## **ACTIVITY 2**

# **PROTECT YOUR MOST IMPORTANT ACCOUNTS ONLINE**



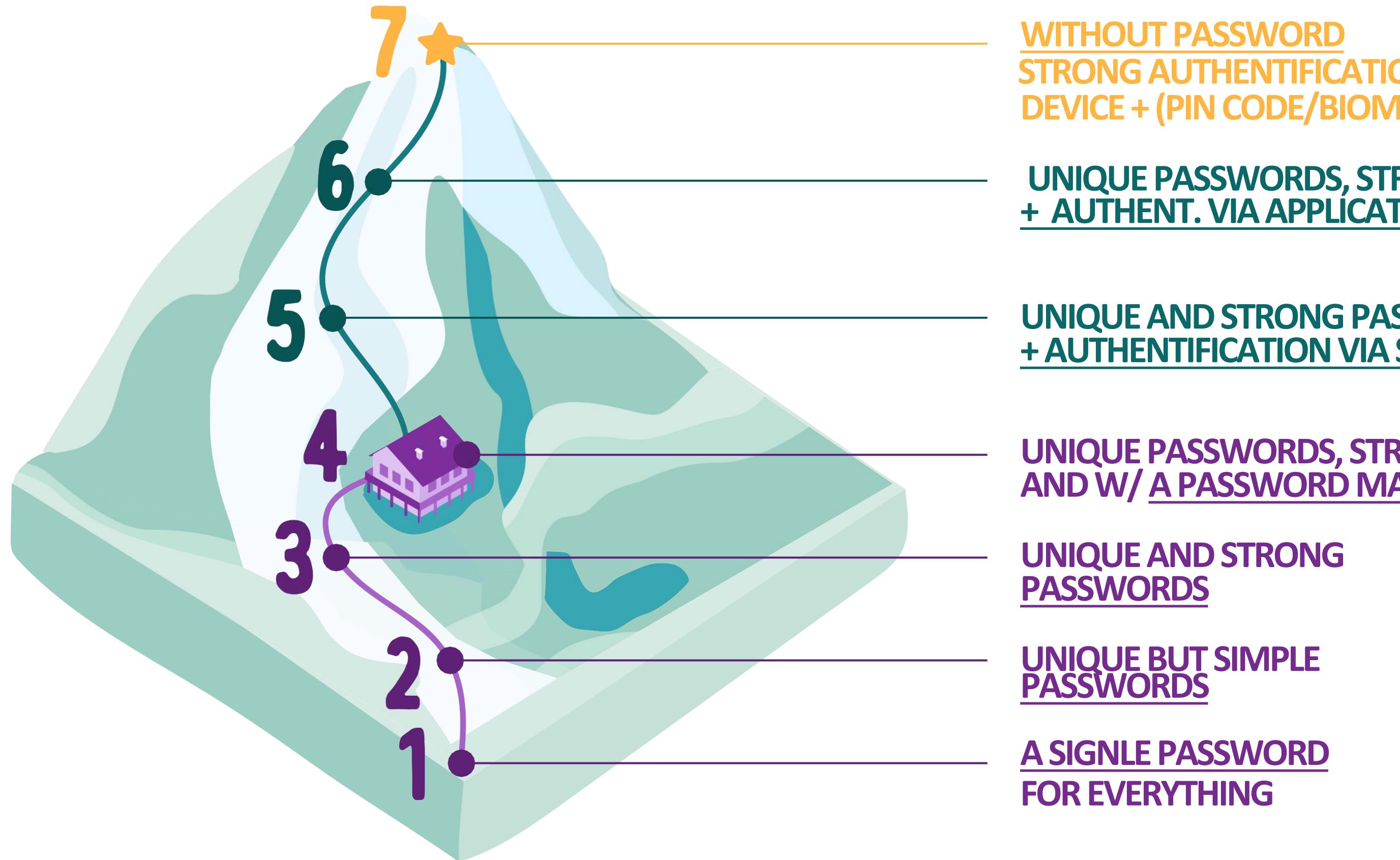
# HOW DOES TWO-FACTOR AUTHENTICATION WORK?



## SOME SERVICES OFFERING TWO-FACTOR AUTHENTICATION

- Gmail, Outlook/Hotmail, Yahoo Mail...
- Facebook, Instagram, LinkedIn, Snapchat, TikTok, Twitter...
- Skype, Teams, WhatsApp, Zoom...
- Amazon, eBay, Paypal...
- Apple iCloud, Dropbox, Google Drive, OneDrive...

**IF YOU USE ONE OF THESE SERVICES, ACTIVATE THE TWO-FACTOR AUTHENTICATION!**



MAILBOX,  
SOCIAL  
NETWORKS  
AND BANK  
ACCOUNT

OTHER  
WEBSITES



## TO REMEMBER:

ENABLE TWO FACTOR AUTHENTICATION FOR YOUR MOST IMPORTANT ACCOUNTS AND SWITCH TO PASSWORD-FREE IF POSSIBLE

CREATE PASSWORDS AND PASSPHRASES THAT ARE EASY FOR YOU TO REMEMBER, BUT DIFFICULT FOR OTHERS TO GUESS

ACCESS YOUR ACCOUNTS ONLY FROM CONTROLLED AND TRUSTED DEVICES

USE A PASSWORD MANAGER TO CREATE A STRONG AND UNIQUE PASSWORD PER ACCOUNT: MANY SOLUTIONS EXIST, FOR EXAMPLE, THE FREE SOFTWARE: [KEEPASS](#)

CAUTIOUSLY REVIEW ALERT MESSAGES TO DETECT ANOMALIES SUCH AS LOGINS FROM UNUSUAL DEVICES OR LOCATIONS ON YOUR ACCOUNTS

**JOB<sup>S</sup> IN CYBERSECURITY ARE JOBS OF THE FUTURE AND EXCITING!**

**DEVELOP YOUR CRITICAL THINKING SKILLS TO AVOID THE DANGERS OF TECHNOLOGY!**

**IF IT'S TOO GOOD TO BE TRUE, IT CERTAINLY IS!**

**REPORTING SCAMS IS ESSENTIAL!**

**IT IS BETTER TO HAVE SEVERAL PASSWORDS, AS ONE HAS SEVERAL KEYS!**

**FOR THE MOST IMPORTANT ACCOUNTS, DOUBLE AUTHENTICATION IS REQUIRED!**



# THANK YOU!

**Version 1.1 - October 2022**

This document was written by cybersecurity professionals and under the artistic direction of Claire Lacroix.

This document is made available under license [Creative Commons Attribution 4.0 International – \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/). It is available at the following URL:  
<https://aka.ms/infoseckit>

With the contribution of: Alexandre Lafargue, Arnaud Jumelet, Céline Corno, Grégory Schiro, Guillaume Aubert, Haifa Bouraoui, Helena Pons-Charlet, India Giblain, Jean-Marie Letort, Manuel Bissey, Sabine Royant, Samuel Gaston-Raoul, Sara Fialho Esposito and Thierry Matusiak.