CYBERSECURITY, MY FUTURE CAREER

Facilitator's Guide

AN INITIATION TO CYBERSECURITY IN 3 SEQUENCES

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

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

HOW TO USE THIS KIT?

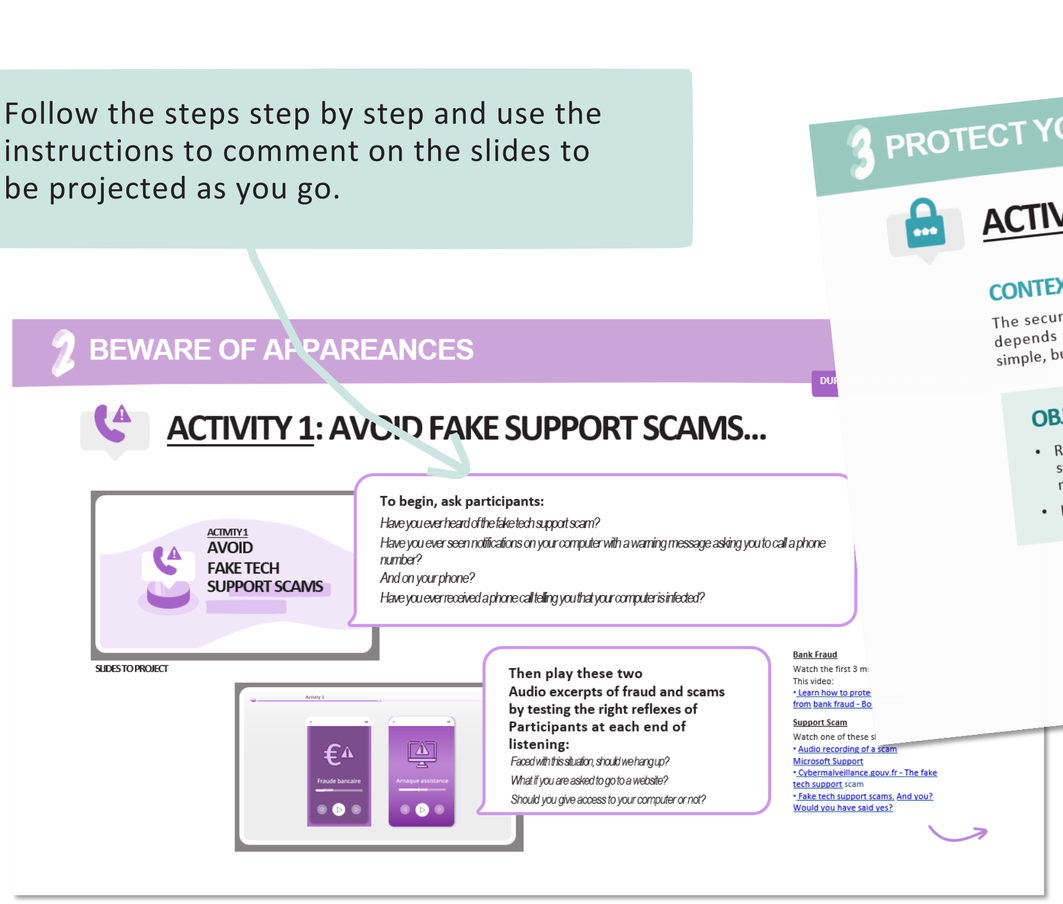
It's up to you to adapt the language to those you want to convince and to choose the words that suit young people by adapting to their concerns!

SUMMARY

BEFORE YOU BEGIN

Get the PDF "**Participant Guide**" to discover the slides to project during your presentation. Check that you will have a screen or a video projector available.

Follow the steps step by step and use the instructions to comment on the slides to be projected as you go.



Background and resources are available to help you delve deeper into the topic and answer questions from participants.

BEFORE YOU BEGIN

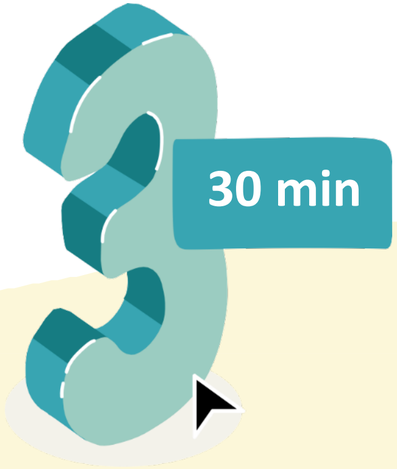
Make sure you have **enough time** to complete the sequences you are interested in (approximate duration).

CYBERSECURITY PROFESSIONS

Discover the diversity of professions

BEWARE OF APPEARANCES

Be vigilant against online scams



PROTECT YOUR ONLINE ACCOUNTS

Learn how to manage passwords

BEFORE YOU BEGIN

Some **golden rules of facilitation** for a serene intervention:

DISTRIBUTE THE FLOOR WELL AMONG THE PARTICIPANTS

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

CONCLUDE BY SUMMARIZING THE IMPORTANT POINTS

1 CAREER IN CYBERSECURITY

Discover the diversity of professions

CONTEXT

There is a **shortage of talent** in the field of cybersecurity with 60,000 positions to be filled in France and, more generally, **several million positions without candidates** worldwide.

The profiles sought are varied: no need to be good at maths or a computer geek, but for those who are, there are of course very technical jobs – everyone can find their way around / no divide. **Math and programming are useful in the field of cybersecurity, but they are not a necessity.**

Cybersecurity jobs cover a **wide range of skills**. Among the most common jobs are the ethical hacker, the cybersecurity consultant, the security incident analyst or the Information Systems Security Manager (CISO), but also the jobs of salespeople, cyber project managers or marketing managers.

There are many recruitment opportunities with an attractive salary (higher than average) and career development (evolution towards different positions throughout one's professional life, etc.).

It is difficult to give an exhaustive list of the qualities required to work in the field of cybersecurity because the positions to be filled are very varied. However, the following qualities are generally observed: **a good knowledge of digital technologies, good analytical and critical thinking skills and intellectual curiosity.**

Cybersecurity jobs are jobs that make **sense:**

- These jobs are important because they allow you **to help others protect themselves from malicious people**, participate in the development of technologies that will contribute to **the protection of health** (avoid blocking hospitals for example), allow **access to reliable information** (by removing fake news) or **raise awareness of cybersecurity gestures**.
- **The sectors of activity are limitless.** You can choose to protect a private company or a public organization.
- Cybersecurity also opens up to **international mobility** because the profession is borderless. We can work on all continents.

CAREER IN CYBERSECURITY

OBJECTIVE OF THE SEQUENCE

This sequence encourages participants to **explore the diversity of cybersecurity professions**, invites them to **familiarize themselves with the vocabulary** of the professions and finally aims to **shake up preconceived ideas**.

At the end of this sequence, Participants will be able to:

- Name some cybersecurity jobs
- Measuring the meaning and challenges of these professions

ACTIVITIES

ACTIVITY 1: THE GESTURES OF CYBER

Practice recognizing good cybersecurity practices.

ACTIVITY 2: I AM NOT A HACKER AND YET I WORK IN CYBERSECURITY!

Challenging certain prejudices about jobs cybersecurity.

ACTIVITY 3: CYBER, ONE OR MORE PROFESSIONS?

Discover some jobs in cybersecurity.

1 CAREER IN CYBERSECURITY

SLIDE TO PROJECT

To start, as an icebreaker, ask participants what they know about cybersecurity using these examples:

Do you know people working in this field? What are the different jobs in cybersecurity?

What does success mean to you?

Do you make a lot of money working in cybersecurity? Why work in cybersecurity?

Do you have to be good at maths to work in cybersecurity? Do you have to be a geek to work in cybersecurity?

What are the qualities to work in the field of cybersecurity?

1 CAREER IN CYBERSECURITY

SLIDES TO PROJECT

Review the 4 key figures illustrated.
To go further, here are some others:

- In 2020, the average cost of a malware attack for a business was more than $2.5 million. This includes the cost of the time it takes to resolve the attack, which is 50 days on average. (source)
- In the second quarter of 2020, the average ransom demanded was over $100,000, and it continues to increase over time. (source)
- The average total cost of a data theft increased by nearly 10% between 2020 and 2021: a level not seen in 7 years. The global average total cost of a data breach in 2021 was $4.24 million. (source)
- The average total cost of an information theft caused by the compromise of a business mailbox is $5.01 million. (source)
- Cybercrime is expected to cost the world $10.5 trillion a year by 2025, up from $3 trillion a decade ago and $6 trillion in 2021. (source)

1 CAREER IN CYBERSECURITY

SLIDE TO PROJECT

Explain to participants that this is a dynamic sector. (source ANSSI / Cybersecurity profiles - Survey 2021)

To find out more about this sector, see also the results of the 2023 survey of the ANSSI Observatory of Professions: https://cyber.gouv.fr/publications/lattractivite-des-metiers-de-la-cybersecurite-vues-par-les-professionnels

LET'S MOVE ON NOW TO ACTIVITIES

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: THE GESTURES OF CYBER

CONTEXT

Cyberattackers often choose **the easiest attacks to carry out.**
For example, a thief will choose to enter a home through a window that is easy to open rather than through an armored door with a surveillance system. The same is true in the digital world. The more **basic security measures** are in place, the lower the risk of cyberattacks.

OBJECTIVE OF THE SEQUENCE

Practice recognizing good cybersecurity practices.

RESOURCES TO GO FURTHER

2021 Activity Report - Cybercrime
ANSSI MOOC

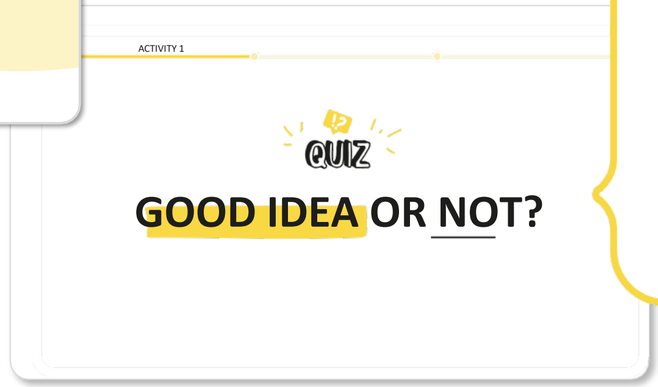
DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: THE GESTURES OF CYBER

To begin, ask participants:

Does a padlock in the browser mean that the site is secure?
Is it riskier to surf with a computer or with a smartphone?

SLIDE S TO PROJECT

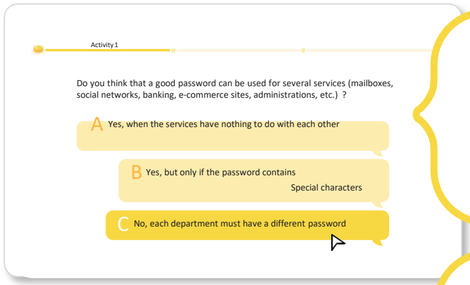


Then, propose the quiz "Good idea or not?" after explaining the context:

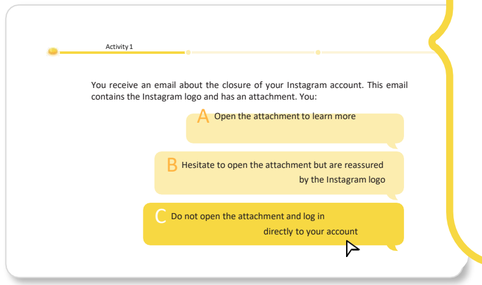
At the end of 2021, 92% of households in France had an internet connection, and you spend an average of 3 hours and 53 minutes every day surfing the internet! (15-24 years old / Médiamétrie 2021)!

DURATION OF THE ACTIVITY: 15MIN

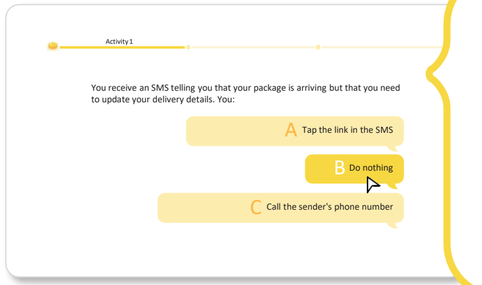
ACTIVITY 1: THE GESTURES OF CYBER



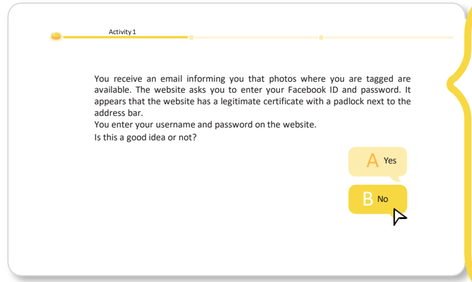
Each service should have a different password to avoid the risk of a cascading compromise.



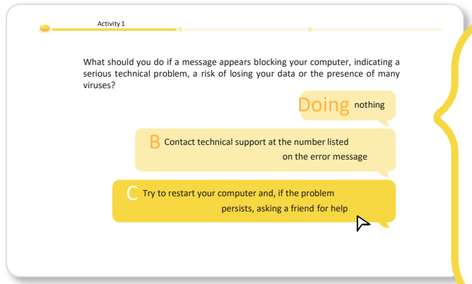
Never click on a link or attachment that seems questionable about its origin or nature. If in doubt, access the website is preferred by typing the address directly into the search bar.



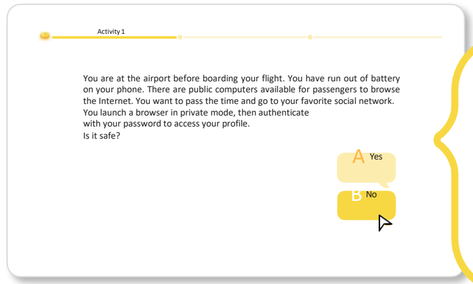
Be careful of messages that seem urgent. If you had ordered something, you would have already entered your postal address. Do not click on these messages or dial the number provided.



A padlock in the address bar does not mean that the site is secure. If in doubt, access the website is preferred by typing the address directly into the search bar. Otherwise, you risk leaking your password to a fraudster.



Fake error messages are usually generated by a malicious or compromised website. These pop-ups may appear to block access to your computer, but restarting your computer may be enough to fix the problem.

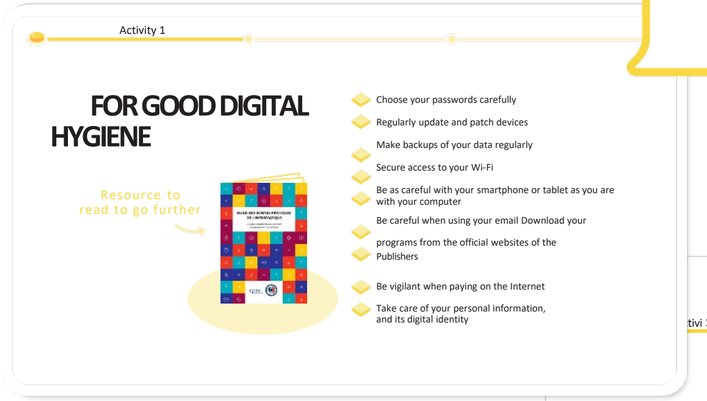


It's risky to log in to your online accounts from a device that you don't own. Keys typed on the keyboard could be recorded or malware could steal your authentication secrets.

DURATION OF THE ACTIVITY: 15MIN

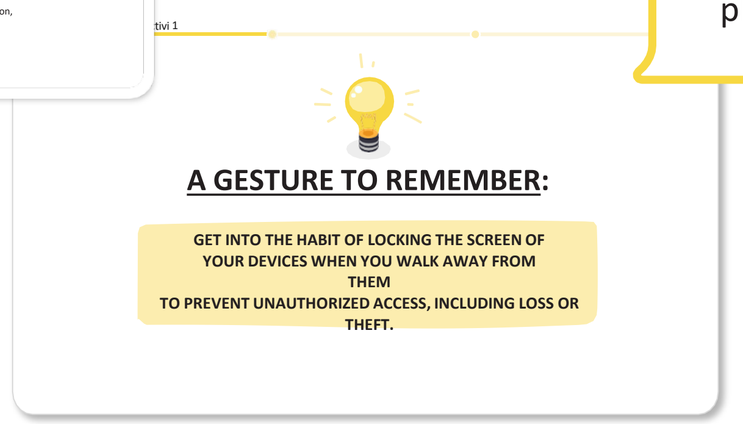
ACTIVITY 1: THE GESTURES OF CYBER

Discover the guide to good IT practices published by the ANSSI and the CPME for small and medium-sized companies, the 9 rules of which can also be applied to individuals. This is called digital hygiene.



SLIDE S TO PROJECT

Take stock of a gesture to remember to protect physical access to their devices.



DURATION OF THE ACTIVITY: 30MIN

ACTIVITY 2: I'M NOT A HACKER AND YET...

CONTEXT

The field of cybersecurity suffers from an **image deficit** where the expert is a solitary, geek-type person who seems to be a little computer genius who spends his time behind his screen coding to get through security systems. **The testimony of a cybersecurity professional** and a **quiz** are there to shake up these preconceived ideas.

OBJECTIVE OF THE SEQUENCE

Challenging certain biases
on cybersecurity professions.

RESOURCE FOR FURTHER

Padlet – Cyber, my future job!

DURATION OF THE ACTIVITY: 30MIN

ACTIVITY 2: I'M NOT A HACKER AND YET...

SLIDE S TO PROJECT

You can present some video testimonials and comment on the different characteristics of the jobs presented (sense of commitment, learning to learn, collaboration) thanks to the [Padlet – Cyber, my future job!]

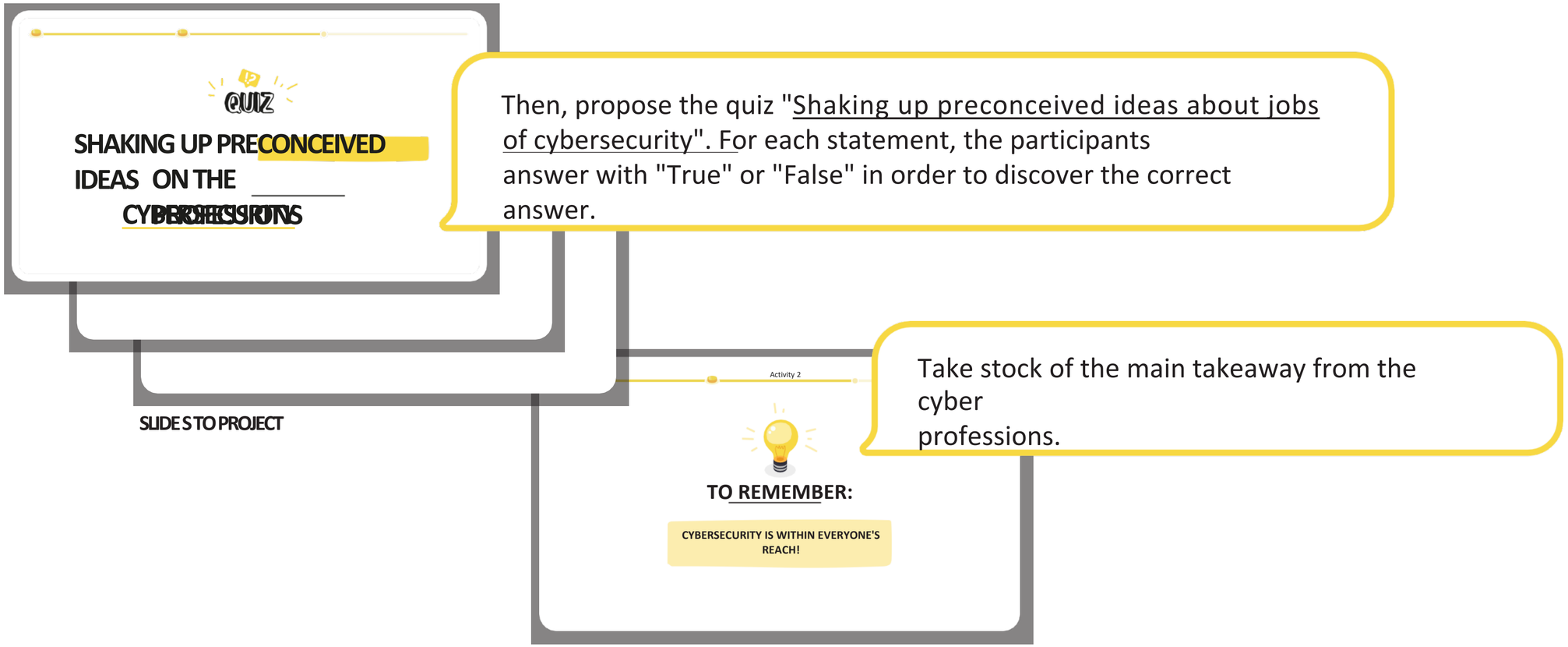
If you are a cybersecurity professional, share your own story and your journey using the questions on the slide or these:

What's your job?
What does the job consist of? What are the different tasks performed?
How big is your company?
What are the workplaces? Do you travel often?
What tools do you need for your job?
How did you get into cybersecurity?
What do you like about your job?
Have you ever been a victim of a virus or phishing?
What are your three cybersecurity tips?

You can also illustrate how the different cybersecurity professions collaborate.

DURATION OF THE ACTIVITY: 30MIN

ACTIVITY 2: I'M NOT A HACKER AND YET...



Then, propose the quiz "Shaking up preconceived ideas about jobs of cybersecurity". For each statement, the participants answer with "True" or "False" in order to discover the correct answer.

Take stock of the main takeaway from the cyber professions.

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 3: CYBER: ONE OR MORE PROFESSIONS?

CONTEXT

Cybersecurity needs are increasing as businesses become more reliant on information and communication technology. Organizations face **increasing risks** of data leakage, fraud, hacking, and intrusion. Cybersecurity professionals have an **important role** to help organizations protect their digital assets (data, computers and networks).

OBJECTIVE OF THE SEQUENCE

Discover some jobs in cybersecurity.

Discover several study paths.

RESOURCES TO GO FURTHER

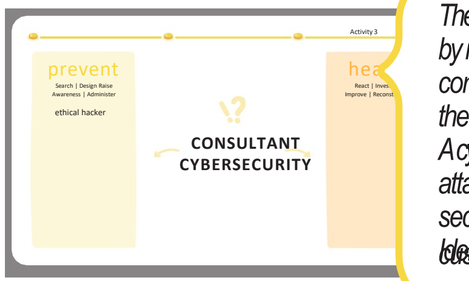
Overview of cybersecurity professions - ANSSI
Mapping of cybersecurity professions - EGE
Cybersecurity professions – Guardia School

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 3: CYBER: ONE OR MORE PROFESSIONS?

Then, propose the game "Prevention or cure ?". For each job proposal, the participants divide it into the two categories: prevention or cure.

The ethical hacker conducts security assessments IT environments, identifies vulnerabilities and proposes remedial actions. It can achieve different types of audits according to its scope of activity (tests , code audit, configuration review, etc.).



The cybersecurity consultant provides solutions to the issues by mobilizing its expertise and experience. It can contribute to the definition of the the organization and implementation of cybersecurity solutions. A cybersecurity consultant's main role is to prevent attacks by helping customers implement security. He can also intervene in a reactive manner and help identify and fix vulnerabilities after an attack.

In the event of suspicion of malicious activity or an attack, the analyst Security incident response analyzes symptoms, performs technical investigations and identifies the operating method of the striker. It qualifies the extent of the compromise and provides recommendations for remediation.

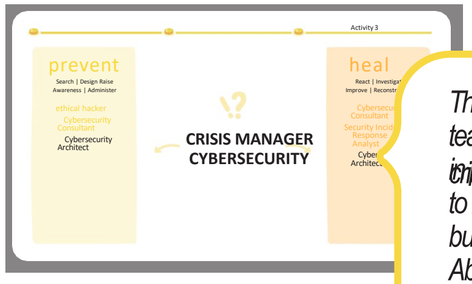
(According to the grouping of the name "Prevention and Cure", from the book: Envie de Cyber, ISSA France Security Tuesday, Ed. Studyrama)

1 CAREER IN CYBERSECURITY

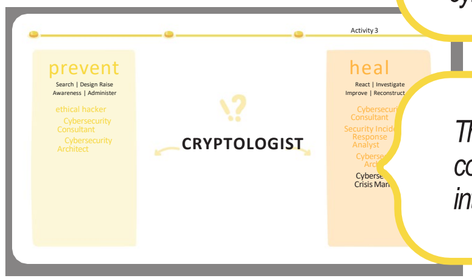
DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 3: CYBER: ONE OR MORE PROFESSIONS?

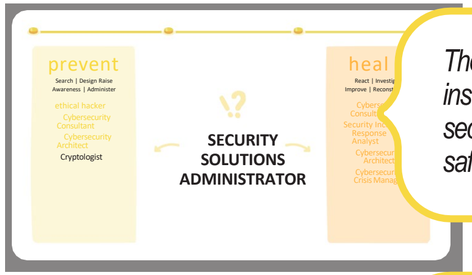
The Data Protection Officer (DPO) ensures that personal data processing practices comply with the legislation in force. He advises and guides the organization to ensure the security and confidentiality of personal information



The cybersecurity crisis manager often intervenes in a team dedicated to crisis management. He analyses the extent of the crisis, puts in place the actions necessary to resolve it and coordinate the teams to implement its recommendations. He advises the management business lines to solve cybersecurity crises. He organizes the Ability of the organization to respond to new cybersecurity.

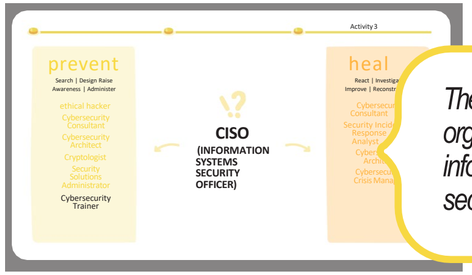


The cryptologist is an expert in cryptography who helps to ensure the confidentiality, integrity and authenticity of data. The cryptologist intervenes in private or public research laboratories.



The Security Solutions Administrator is responsible for installation, management and operation of security. It must ensure the proper functioning of the safety by ensuring that safety conditions are maintained.

The cybersecurity trainer is responsible for training and/or or raising awareness of regulatory and technical aspects or operational cybersecurity operations. He develops training tailored to target audiences and illustrates its through practical work, demonstrations or exercises messages Participatory. It can assess the level of knowledge before after the training.



The CISO is responsible for cybersecurity within organization. It defines the security policy of the systems information, advises business managers, implements security solutions and manages security teams.

(According to the grouping of the name "Prevention and Cure", from the book:

BEWARE OF APPAREANCES

CONTEXT

Fraudsters are everywhere and target everyone: teenagers, grandparents or business leaders. **Online scams** can take many forms, but their goal is always the same: **to steal your passwords, personal data, bank details, access to your devices and online accounts.**

Unsolicited calls and messages are one of the main ways fraudsters operate. Fraudsters are **persuasive** enough to convince you that there is a virus on your computer, that you need to pay a sum of money, that there is fraudulent activity on your bank account. Fraudsters are looking for
Have malware **installed, approve a banking transaction** or authentication request, **disclose personal information,** or your password.

It is important to remain **vigilant** (without becoming
paranoid) by adopting reflexes:

- **Develop your critical thinking and** don't hesitate to **ask yourself questions:** why is this person sending me an attachment by email? Have I ever visited the site pointed to by the link in this SMS? Why is my friend writing me this weird message? etc.
- Use simple gestures such as **locking your computer or phone**, or **avoid typing your credentials on a device that does not belong to you.**

BEWARE OF APPAREANCES

OBJECTIVES OF THE SEQUENCE

This sequence allows participants **to learn about common features of online scams** and **demonstrate their understanding** by putting themselves **in the shoes of an attacker**.

At the end of this sequence, Participants will be able to:

- Recognizing **the Signs of a Scam**
- Explain **the different reflexes** to have against the most common scams
- **Raise awareness by** telling the story of an online scam

ACTIVITIES

ACTIVITY 1: AVOID FAKE TECH SUPPORT SCAMS

Know how to react and report fake tech support scams

ACTIVITY 2: DON'T LET CYBERCRIMINALS STEAL FROM YOU!

Learn to recognize the signs of a scam

BEWARE OF APPAREANCES

To start, as an icebreaker, ask participants what they know about online scams and how to spot them using these questions:

What is an online scam?
Why would someone try to scam you online? How do you know if you are facing a scam?
What to do if you think you've been scammed online?

SLIDE TO PROJECT

LET'S MOVE ON NOW TO ACTIVITIES

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: AVOID FAKE SUPPORT SCAMS...

CONTEXT

This scam is **wreaking havoc** on individuals. While browsing the Internet or after clicking on a malicious link, **a window appears and freezes your computer**. It asks you to urgently call back a technical support number or risk losing access to your data or the use of your computer.
Once contacted, the pseudo technical service asks you to **access your terminal remotely** and **charges** for a fake repair while making you buy useless, even dangerous software.

OBJECTIVE OF THE SEQUENCE

Know how to react and report fake tech support scams.

RESOURCES TO GO FURTHER

How to deal with fake tech support scam? -Cybercrime
Fake Technical Support Scam Fact Sheet – Cybermalicilance Protect yourself from tech support scams (microsoft.com)

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: AVOID FAKE SUPPORT SCAMS...

SLIDES TO PROJECT

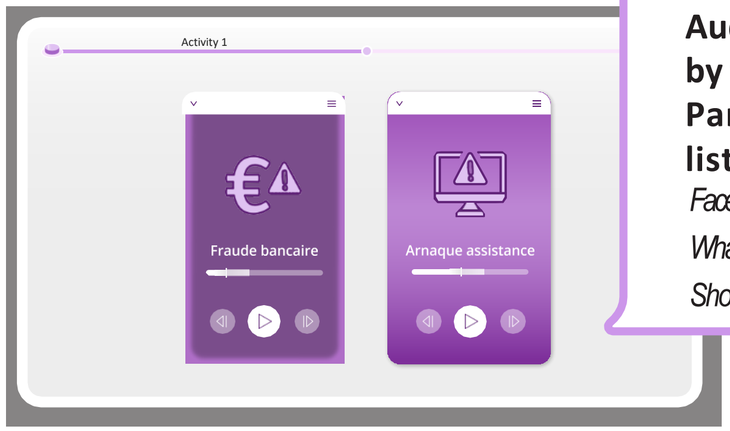
To begin, ask participants:

Have you ever heard of the fake tech support scam?

Have you ever seen notifications on your computer with a warning message asking you to call a phone number?

And on your phone?

Have you ever received a phone call telling you that your computer is infected?



Then play these two Audio excerpts of fraud and scams by testing the right reflexes of Participants at each end of listening:

Faced with this situation, should we hang up?

What if you are asked to go to a website?

Should you give access to your computer or not?

Bank Fraud

Watch the first 3 minutes of This video:

- Learn how to protect yourself from bank fraud - Boursorama

Support Scam

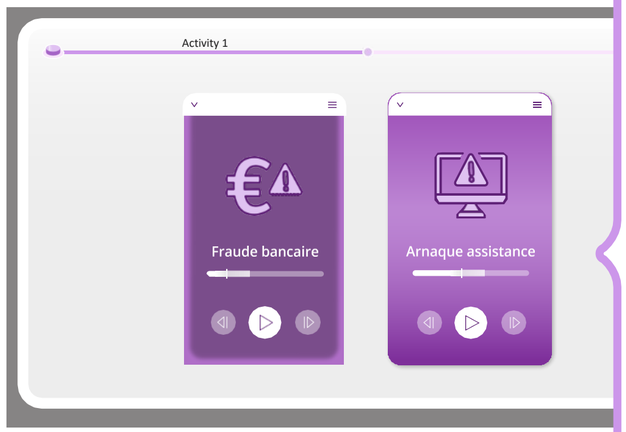
Watch one of these short videos:

- Audio recording of a scam Microsoft Support
- Cybermalveillance.gouv.fr - The fake tech support scam
- Fake tech support scams. And you? Would you have said yes?

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: AVOID FAKE SUPPORT SCAMS...



SLIDE TO PROJECT

Summarize the principle of fake tech support scams:

- *An expert calls you. He claims to work for a well-known company, and tells you that your computer has been infected with a virus. According to him, the only solution is to give him remote access to your computer so that he can repair it directly. It may also attempt to sell you a so-called antivirus. Under pressure, it may seem logical to do what he asks, but beware: it's a scam!*
- *Fraudsters call people randomly, pretending to be legitimate experts. They try to scare you into giving them money or giving them control of your computer by downloading fake software or giving them your passwords. It is important not to give in to the demands of these fraudsters and ignore them.*
- *This scam also takes the form of pop-up messages that appear on your screen, alerting you that your computer has been infected.*
- *Even though the calls and pop-ups are compelling, in reality you risk having your credit card codes and banking credentials stolen, losing access to your computer, becoming a victim of identity theft, and even having your bank account emptied. Do not call the numbers that appear directly in the warning messages.*

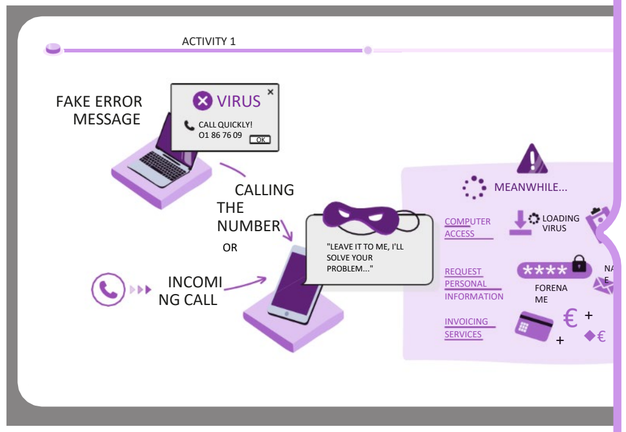
Still taking the example of these 2 cases of scams, explain the first reflexes to have to thwart them:

If someone calls you to verify your personal details as a result of suspicious transactions, or because a transaction needs to be reversed after verifying your identity, don't talk any longer and hang up right away. This person is probably a fraudster who is trying to get you to validate a financial transaction or a connection to your account.

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: AVOID FAKE SUPPORT SCAMS...



SLIDE TO PROJECT

To explain how the scam happens, tell this story using the infographic:

During this attack, the scammer contacts you and tries to convince you that there is a problem on your computer and that you should let them "fix" it for you.

The two most common ways it uses to contact you are by sending you fake error messages on your computer or call you on your phone.

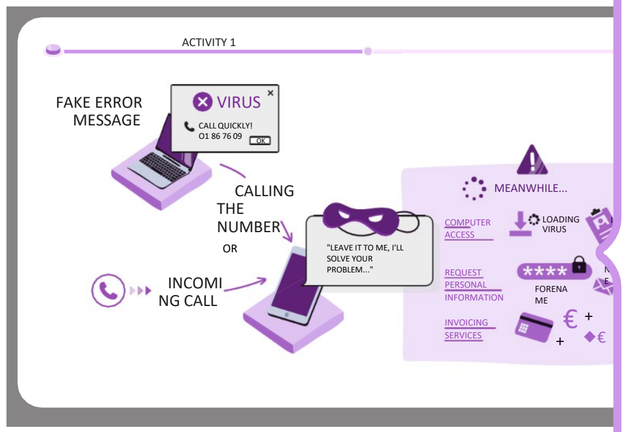
Fake error messages are usually generated by a malicious or compromised website. You use just your web browser. For example, you click on a link in a web or network search and then your screen suddenly displays worrying messages informing you that your computer is experiencing a problem or virus and you should immediately call the phone number provided. These pop-ups may appear to block access to your computer, so you can't close them. Recorded sounds or voices can even accompany these pop-ups to make them even more visible.

Phone calls usually take the form of a "help desk agent" calling you on behalf of a trusted company such as Microsoft or Amazon. These scammers are professionals and are often quite convincing...

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: AVOID FAKE SUPPORT SCAMS...



SLIDE TO PROJECT

It doesn't matter if you call them from a pop-up message or other error message, or if they call you as a help desk agent, the story is always the same. They let you know that they've detected a problem with your computer or account and that they want you to let them fix it.

Here are some things that usually happen at this stage:

- *The scammer will want you to allow them to remotely access your computer so they can "fix" it. When it claims to repair your computer, it will steal your information or install malware.*
- *They may ask for your personal information in order to help you "correct" your account. This information likely includes things like your name, address, username, password, social security number, date of birth, and any other type of personal or financial data it may trick you into revealing.*
- *They will often try to charge you a fee for their services in order to "fix" the non-existent problem. If you gave them your credit card information, they may not have been able to use it and ask if you have another one. He will try to obtain several bank cards.*
- *They may ask you for the credit card payment verification code that you received via SMS.*

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: AVOID FAKE SUPPORT SCAMS...

SLIDE TO PROJECT

Focus on fake Microsoft tech support scams and remind them of these rules:

- *Microsoft will never call you to ask for financial or personal information.*
- *Microsoft will also never call you unsolicited to offer technical support to repair your computer.*
- *Microsoft will never ask you to pay for technical support in the form of cryptocurrency like Bitcoin, or with gift cards.*

If you see an error message or pop-up window with a phone number, don't call it. Microsoft's error and warning messages never include a phone number.

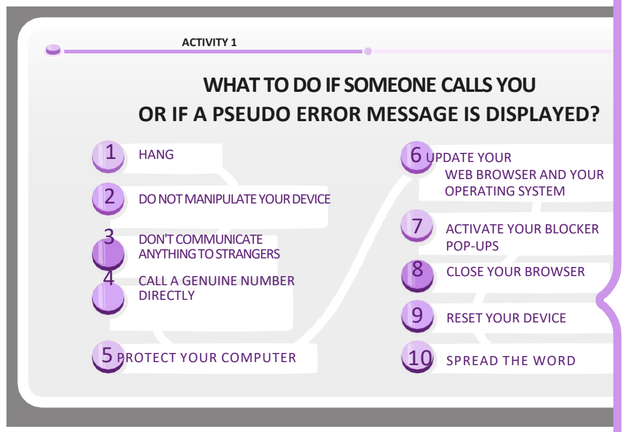
If you've been contacted by someone claiming to be from Microsoft or associated with Microsoft and you think it's a scam, report the incident through the Microsoft online reporting tool "Report support fraud": https://www.microsoft.com/fr-fr/concern/scam?rtc=1

If you are a victim of a fake tech support scam, follow the steps on the cybermalveillance.gouv.fr site: https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/arnaques-au-faux-support-technique

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: AVOID FAKE SUPPORT SCAMS...



SLIDE TO PROJECT

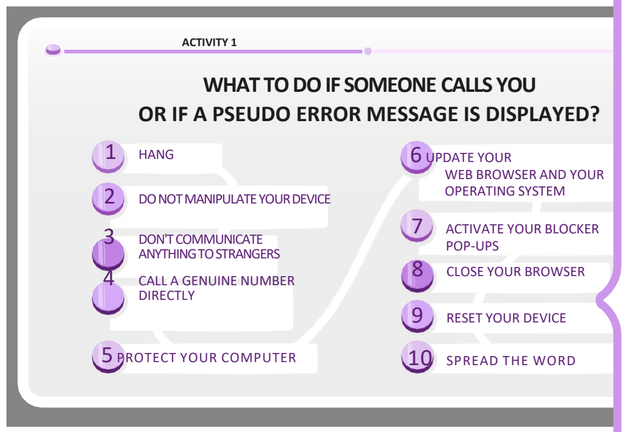
Review what to do if you get a call or if you get a pseudo error message:

- ***Hang up:*** *Most real software companies won't call you to tell you that your computer is compromised. If you are called, it is false.*
- ***Do not manipulate your device:*** *hang up if you are asked by phone to make manipulations on your computer.*
- ***Don't share anything with strangers:*** *Don't give anyone any information about your accounts (any usernames or password) or computer information (IP address). You have no guarantee that the person at the The end of the line tells you the truth about his identity.*
- ***Call a genuine number directly:*** *hang up and call the organization in question using the number obtained from a reliable source, from the organization's website or on invoices or account statements.*
- ***Protect your computer:*** *many products are available to protect your computer: antivirus, anti-spyware and firewalls. In some cases, they can be purchased as a software suite. When you do it Regularly updating them can prevent malware from accessing your computer.*

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: AVOID FAKE SUPPORT SCAMS…



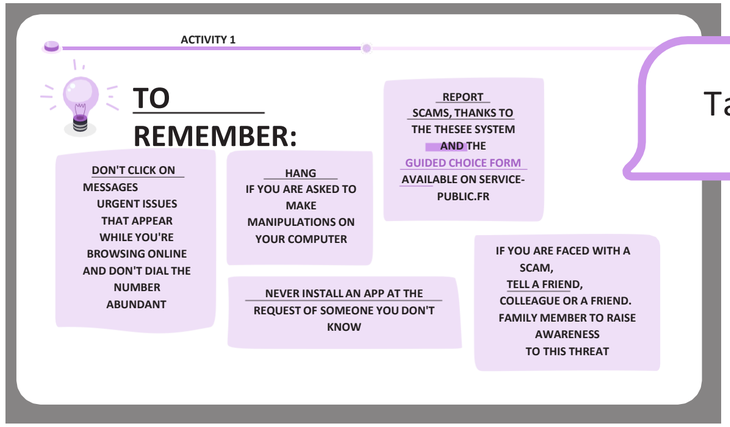
SLIDE TO PROJECT

- ***Update your web browser and operating system:*** *they both have built-in defenses that are regularly updated to keep up with the latest viruses and other malware. By ensuring that your operating system is updated (e.g., Windows, OSX or Ubuntu) and your web browser (eg, Chrome, Firefox, Edge, or Safari), you can stack the chances on your side.*
- ***Turn on your pop-up blocker:*** *Most web browsers have a Built-in pop-ups that prevent pop-ups from appearing on your screen. This could help you protect from fraudulent pop-ups.*
- ***Close your browser:*** *If your screen suddenly fills up with scary messages, close immediately your browser (try pressing Alt+F4 if you can't do it with the mouse). If you can't Close your browser, try restarting your computer.*
- ***Reset your device:*** *If you've granted scammers access to your computer, you can try to get them reset.*
- ***Talk about it around you:*** *share your experience to make those around you aware of this threat. And if you have paid, contact your bank and file a complaint.*

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: AVOID FAKE SUPPORT SCAMS...



SLIDE TO PROJECT

Take stock of the actions to remember to avoid scams.

DURATION OF THE ACTIVITY: 45MIN

ACTIVITY 2: DON'T LET CYBERCRIMINALS...

CONTEXT

The topics of online scams are constantly renewed, but their operation often remains the same: you are sent **false information** and asked to **click on a link** to solve **a situation that does not exist**.

There are many examples:

- You receive an SMS or email from a trusted sender inviting you **to click on a link to update your account, frank a parcel** or **receive money**.
- Someone will contact you by phone or text message to offer you **training based on your rights** and offer to help you create your account.
- An email tells you that **your webcam has been hacked, your browsing on pornographic sites has been recorded** and, of course, a list of all your contacts and passwords has been collected.

All this is false!

OBJECTIVE OF THE SEQUENCE: Learn to recognize the signs of a scam.

RESOURCES TO GO FURTHER

The scourge of phishing in four examples | Youtube Phishing: Detecting a malicious message | CNIL
What to do in case of phishing? | Cybercrime

DURATION OF THE ACTIVITY: 45MIN

ACTIVITY 2: DON'T LET CYBERCRIMINALS...

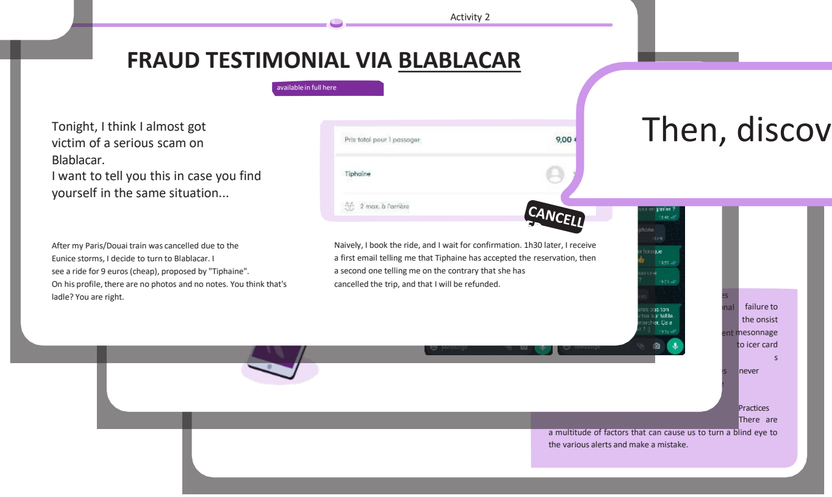
ACTIVITY 2

DON'T LET CYBERCRIMINALS STEAL FROM YOU

SLIDES TO PROJECT

To begin, ask participants:

Have you ever received suspicious messages by email or SMS?
Do you know someone who has ever been a victim of phishing?
What can be the consequences if you click on a link contained in a suspicious message?
What can make you want to click on a link?

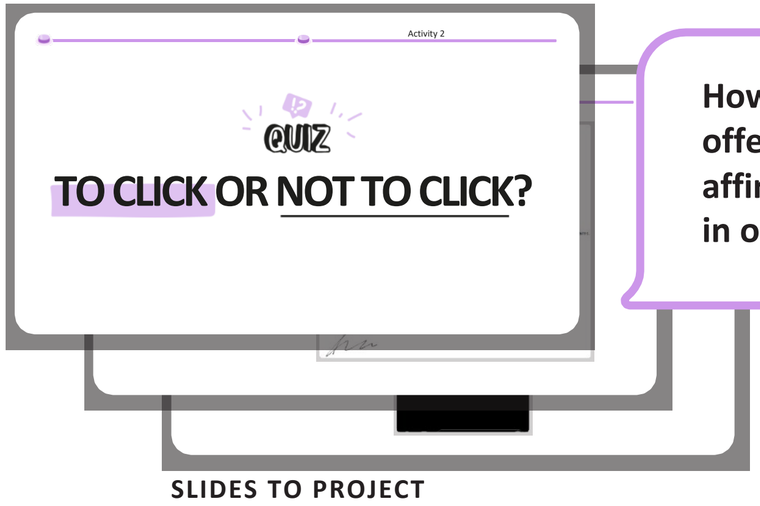


Then, discover Valentin's testimony.

2 BEWARE OF APPAREANCES

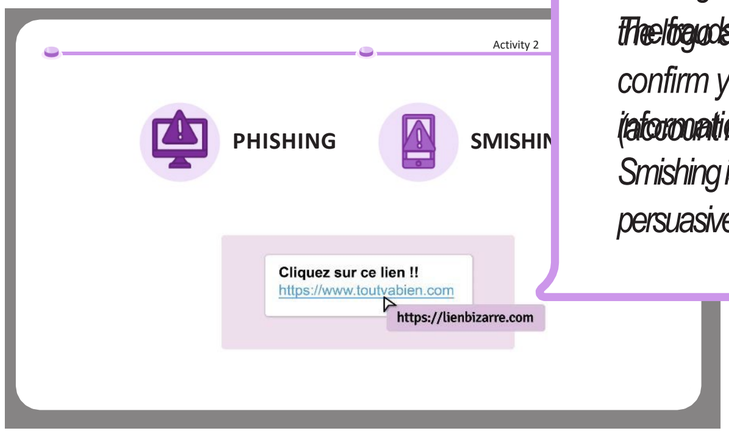
DURATION OF THE ACTIVITY: 45MIN

ACTIVITY 2: DON'T LET CYBERCRIMINALS...



SLIDES TO PROJECT

How can fraudsters go about making their scam credible? To test the participants, offer the "To click or not to click" quiz. For each affirmation, the participants answer the question "*Faced with this message, should we click or not?*" in order to find out the right answer.



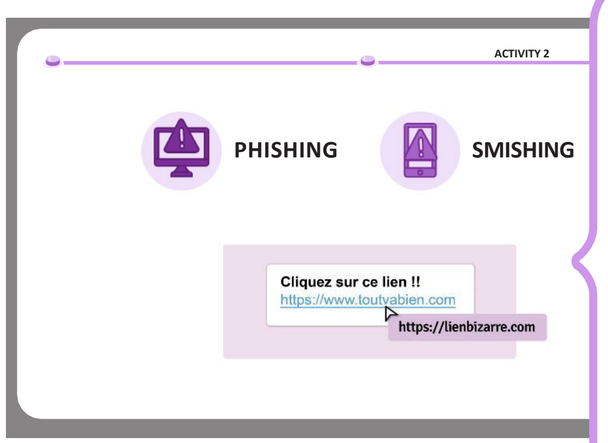
Debrief the exercise by explaining the concepts of phishing and smishing:

Phishing is the most common form of scam on the internet.
The fraudster impersonates a known organization (bank, service provider, etc.) by using the logo and name of this organization. He sends you an email asking you to confirm your information following a technical incident, such as your contact information, account number, personal codes, etc.) or your password.
Smishing is a form of SMS phishing on mobile phones. These messages are also very persuasive and ask you to follow a link.

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 45MIN

ACTIVITY 2: DON'T LET CYBERCRIMINALS...



SLIDE TO PROJECT

Just like barcodes, QR codes are images that contain encoded data, such as a link that can redirect to a website or allow an app to be downloaded. Their use has become widespread in recent years due to their practicality, avoiding laborious link entry on mobile devices. However, as with any technological innovation, QR codes have caught the attention of cybercriminals. Incidents such as fake ticket notices left on car windshields or fake QR codes stuck on parking meters have been reported. These fraudulent QR codes, also known as quishing, started making headlines regularly when it comes to cybercrime as early as 2023. Sending malicious QR codes via email may seem suspicious because it requires a second device to scan, reducing the success rate for cybercriminals. Moreover, the physical distribution of QR codes can only target a limited number of potential victims, thus presenting a low return on investment and a high risk of detection for criminals.

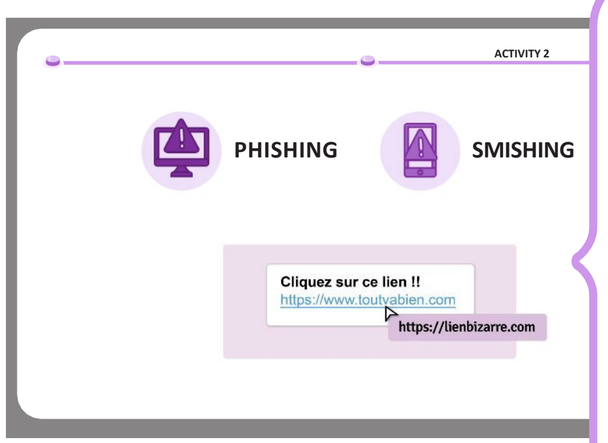
While the threat of malicious QR codes is still limited, it remains real, exploiting victims' difficulty in recognizing fraudulent links, especially when they are masked as a QR code. These malicious QR codes can redirect users to fraudulent sites or trick them into downloading viruses.

Therefore, it is crucial to always check the legitimacy of QR codes before scanning them, just as one would for a link contained in a message, in order to avoid any attempts at scamming or malware infection.

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 45MIN

ACTIVITY 2: DON'T LET CYBERCRIMINALS...



SLIDE TO PROJECT

Continue by giving some advice:

• Be wary of messages that ask you to click on a link, confirm personal information, or Reset a password. These messages can be false alarms and it is best not to follow them.

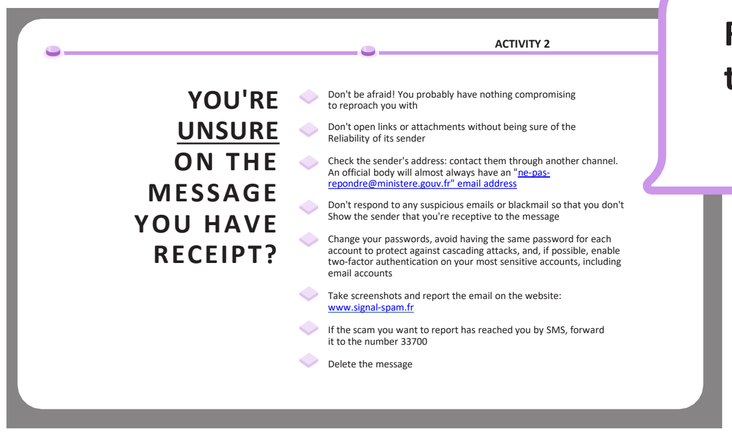
• If you hover over a link with your mouse (on a computer), you'll see where the link takes you. If the address doesn't match the official website address, there's a good chance it's a fake. Often, fraudsters use shortened links to make it look like a link looks like it's safe to click. If you receive a short link, there are free online expander tools that allow you to copy and paste the link, in order to reveal its true destination. Be careful, however, if you don't want to accidentally click on the short link. If you're worried that you won't be able to copy and paste the link correctly, delete the email or text message with the shortened link instead and go to the company's main website to access your account or the offer you're interested in.

• An unknown sender offers you to download "free" applications that are usually paid. This offer is an attempt to steal personal or banking information from you. Download your apps only from official stores and publishers' sites, otherwise you risk downloading malicious software that could compromise your data.

2 BEWARE OF APPAREANCES

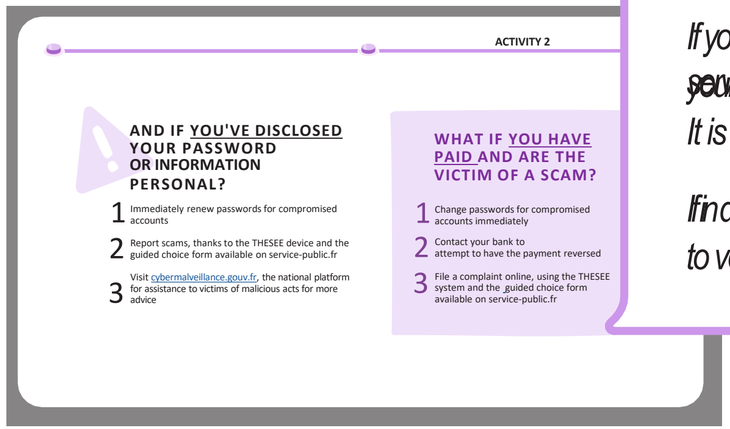
DURATION OF THE ACTIVITY: 45MIN

ACTIVITY 2: DON'T LET CYBERCRIMINALS...



SLIDES TO PROJECT

Review the best practices to have in this situation. You can go live to the www.signal-spam.fr site to show the platform to the participants.



You can go live on cybermalveillance.gouv.fr to show the platform to the participants.

Remind them of the first reflexes to have:

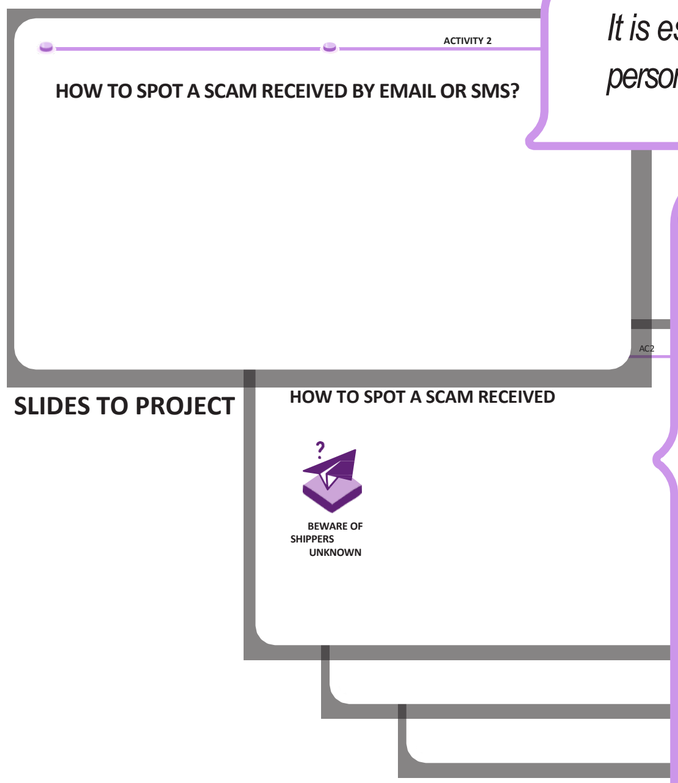
If you receive an email or text message that appears to come from a well-known site such as your bank, the service energy supplier, etc., be vigilant before clicking on the link. He
It is preferable to connect directly to the site on which you have an account.

If in doubt, stop browsing, do not download anything, and call your doctor directly.
to verify the origin of the message!

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 45MIN

ACTIVITY 2: DON'T LET CYBERCRIMINALS...



It is essential to be extra vigilant against cyber-scams and attempts to steal your data personal or banking. Here are some tips to help you spot and avoid pitfalls.

Go on to explain to participants that online scams can be hard to spot: even cybersecurity professionals can be fooled! However, there are a few signs that can identify them.
Comment on the 5 tips:

Beware of unknown senders: *be particularly vigilant if the message comes from an email address or a DSE number,phone that you don't know or that doesn't part of your contact list. Ask yourself who is the sender.*

Pay attention to the writing: *even if it turns out to be less and less true, Some malicious messages are not written correctly. If the message contains typos, spelling or turns of phrase inappropriate sentences, is that it is not authentic and does not originate not a credible organization (administration, major brand, etc.).*

The sender's e-mail address is not a reliable criterion: *If the message seems to be from a friend, contact them on another channel to make sure it's really them. Your contacts' device and mailbox can be hacked and used to send you phishing messages via SMS or email.*

Check the links: *Before clicking on the links, leave your mouse on them. The full link will then appear. Make sure that this link is consistent and points to a legitimate site. This is more difficult to do from a smartphone screen, because you have to press your finger on the link.*

Be wary of strange, urgent and too good to be true requests: *ask yourself the question of the legitimacy of any requests expressed. No organization has the right to ask you for your credit card code, access codes and passwords. Do not transmit anything confidential, even at the request of a person who claims to be part of your entourage.*

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 45MIN

ACTIVITY 2: DON'T LET CYBERCRIMINALS...

SLIDES TO PROJECT

Test your participants' knowledge by offering them a role-playing game "Create your own scam" (after " The School of Social Media "). Print or ask to copy the templates on the following slides.

Ask participants, separately or in pairs, to create their own example of an online scam. They will be able to put themselves in the shoes of a fraudster and think about social engineering attacks.

Encourage participants to think about the following questions when creating their mock scam:

- ***What is your goal?*** *(What do you want to get from your victim(s)?*
- ***How will you make your scam realistic?*** *(If the scam is too weird or obvious, people won't will not fall into the trap)*
- ***How will you use technology to carry out your scam?*** *For example, short URLs like bit.ly and QR codes can make it difficult to spot a fake website address. Fake likes/followers/reviews can also seem genuine or popular when they are not, etc.*

2 BEWARE OF APPAREANCES

DURATION OF THE ACTIVITY: 45MIN

ACTIVITY 2: DON'T LET CYBERCRIMINALS...

SLIDES TO PROJECT

Guide the participants by indicating that, generally speaking, social engineering methods are carried out according to the following pattern:

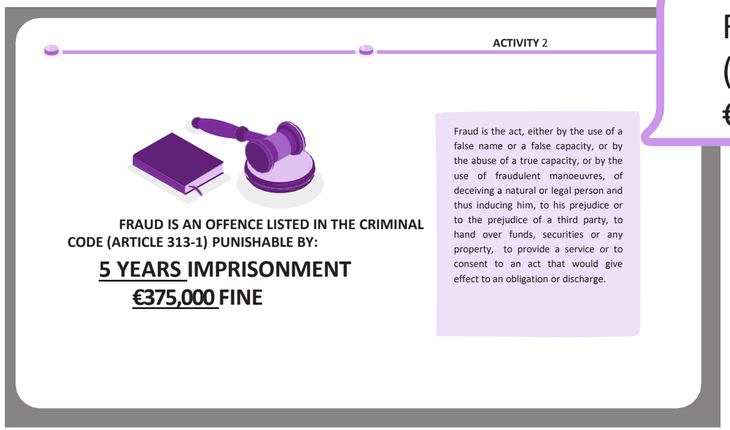
- *An **approach phase** that allows the interlocutor to gain confidence.*
- *An **alert**, in order to destabilize him and ensure the speed of his reaction ("there is a problem on a contract, invoice, etc. »).*
- *A **diversion,** i.e. a sentence or a situation to reassure the user and prevent them from focusing on the alert. For example, a thank you and a reassuring message that everything will be restored if the person cooperates quickly.*

Ask a participant or volunteer group to share their scam: can other people Spot the signs that it is a scam?

2 BEWARE OF APPAREANCES

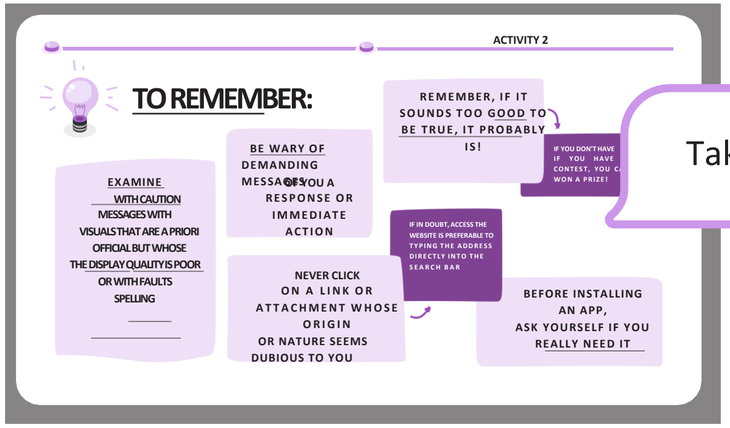
DURATION OF THE ACTIVITY: 45MIN

ACTIVITY 2: DON'T LET CYBERCRIMINALS...

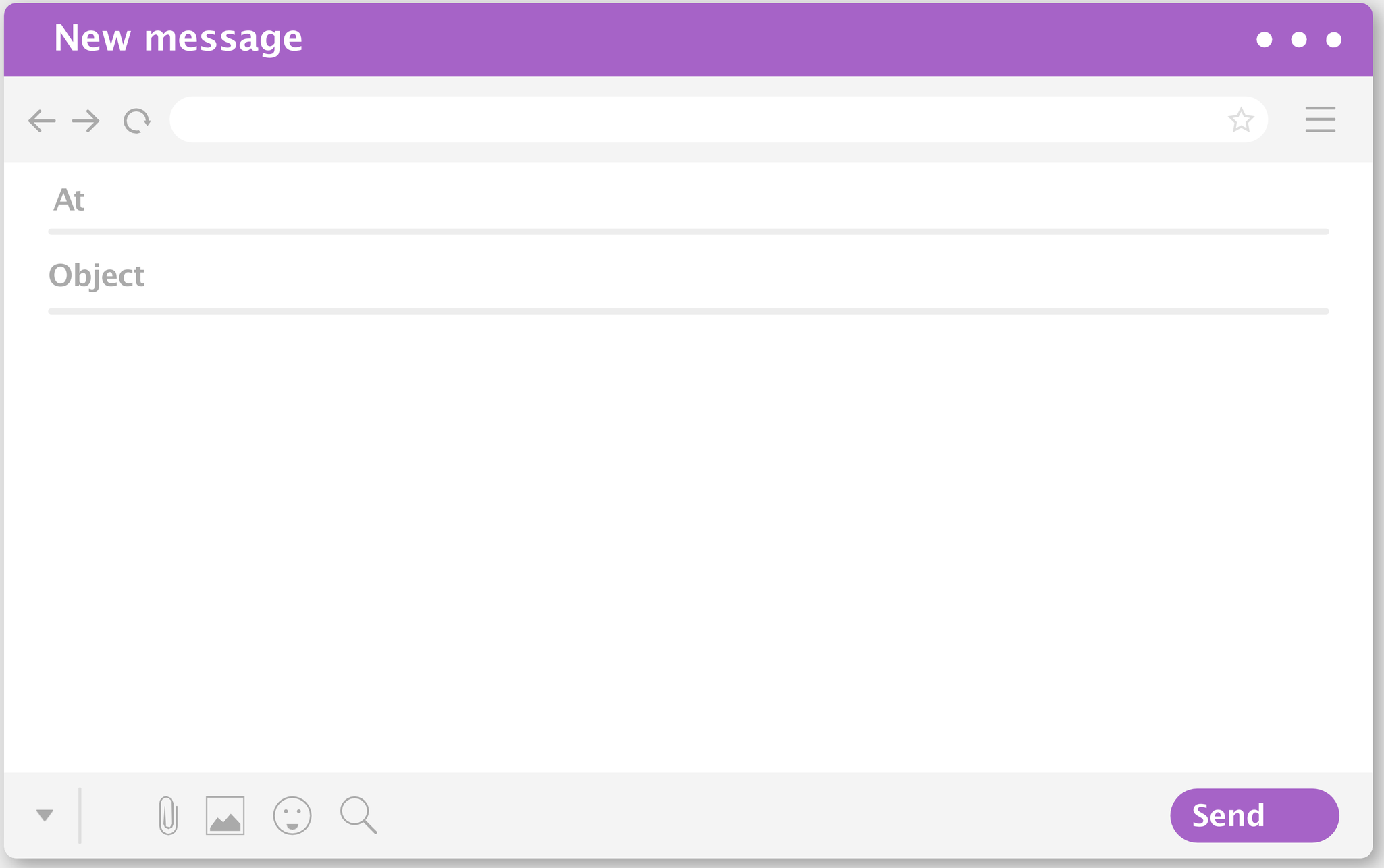


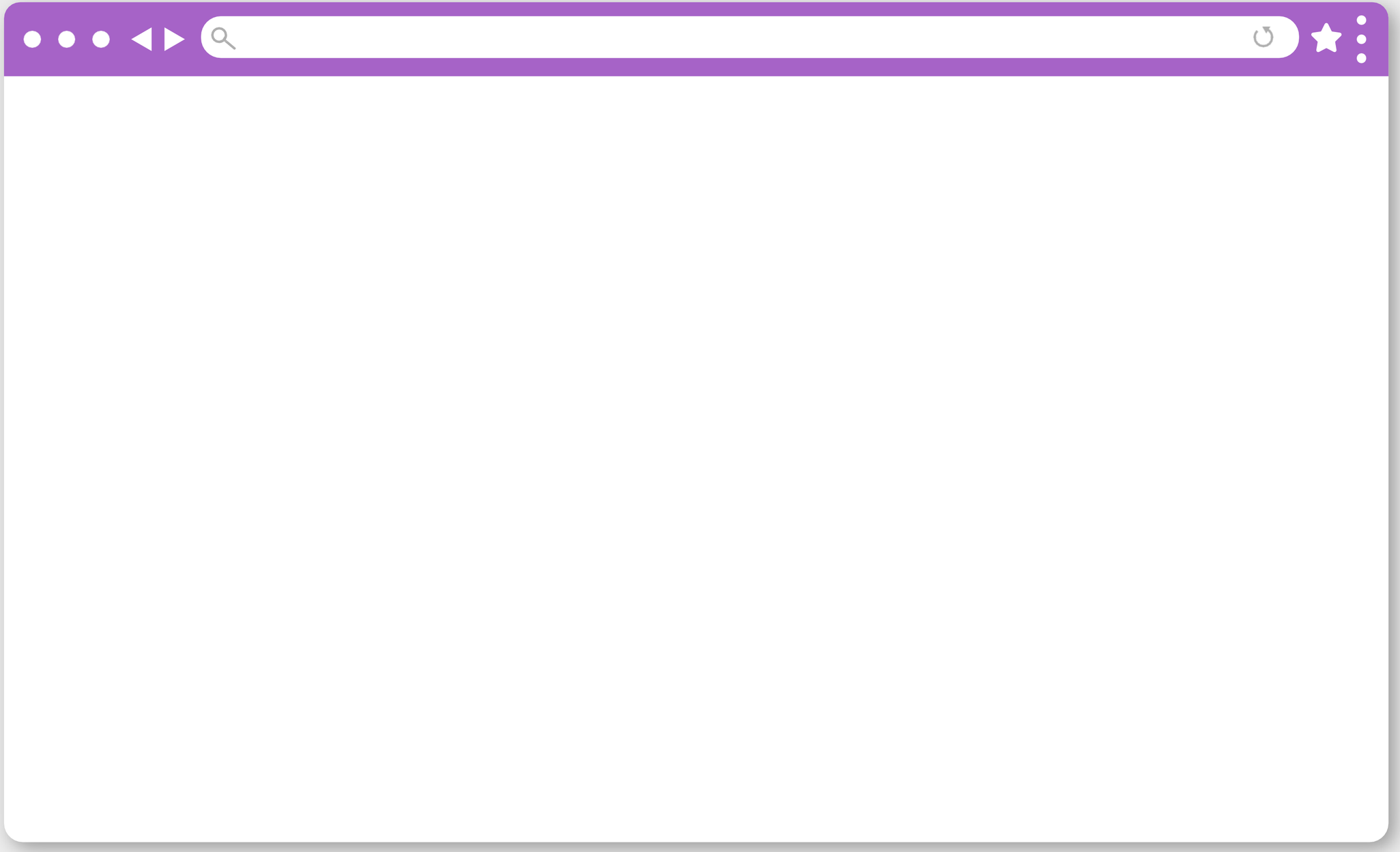
Remember that fraud is an offence listed in the penal code (Article 313-1) punishable by 5 years' imprisonment and a fine of €375,000.

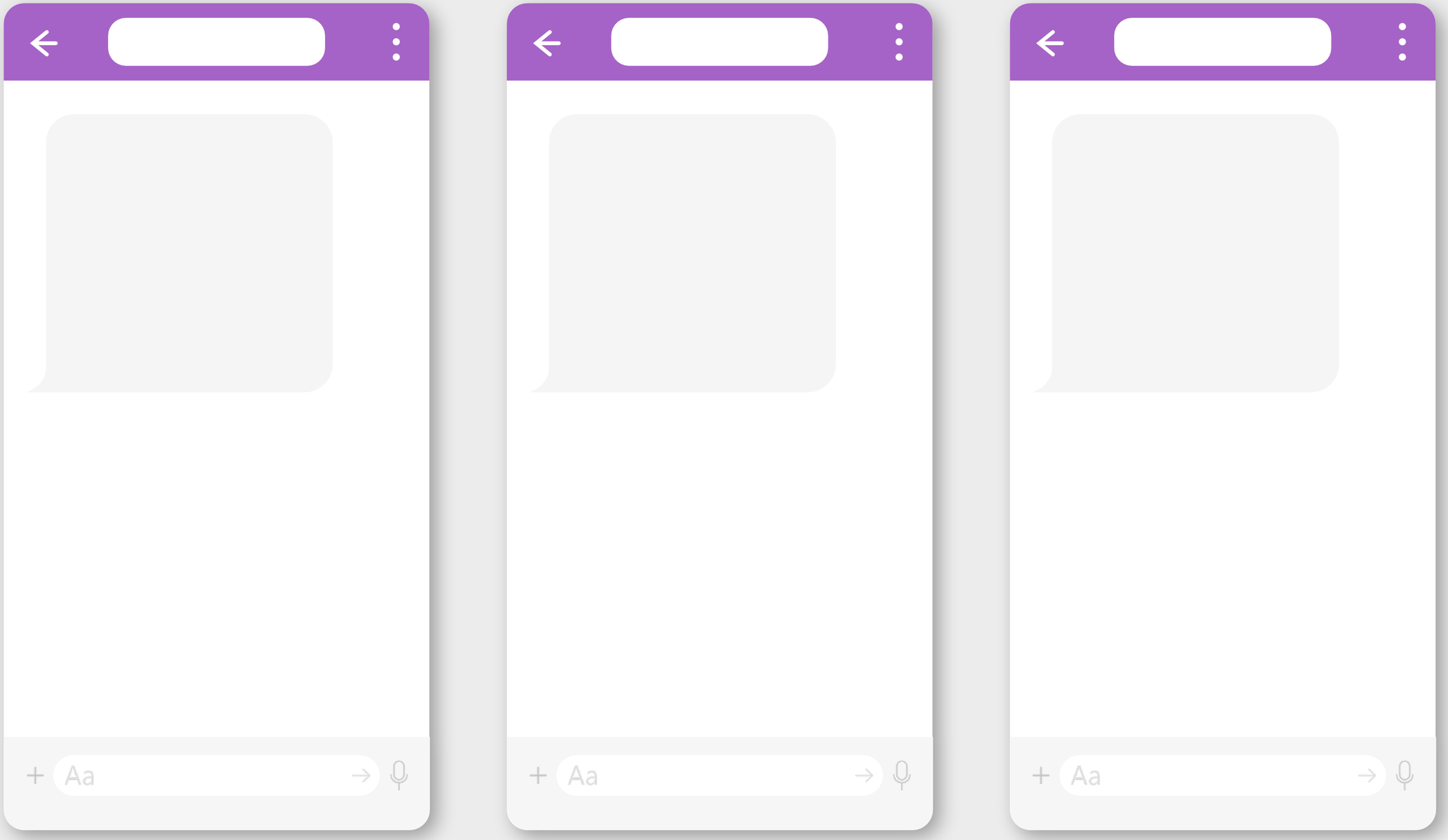
SLIDES TO PROJECT



Take stock of the reflexes to remember to avoid scams.


New message
At
Object
Send




Aa
Aa
Aa

DURATION OF THE ACTIVITY: 10MIN

ACTIVITY 3: SPOT DEEPFAKE CONTENT

CONTEXT

A **deepfake** is an image, video, or audio recording **generated by artificial intelligence (AI),** typically used to spread **false information**. In recent years, advances in artificial intelligence (AI) have made deepfakes seem so realistic that it can be difficult for even the most skilled experts to spot them as fake.

OBJECTIVE OF THE SEQUENCE:

Practice recognizing text or an image generated by an AI.

Check the accuracy of a text before sharing or commenting on it.

RESOURCES TO GO FURTHER

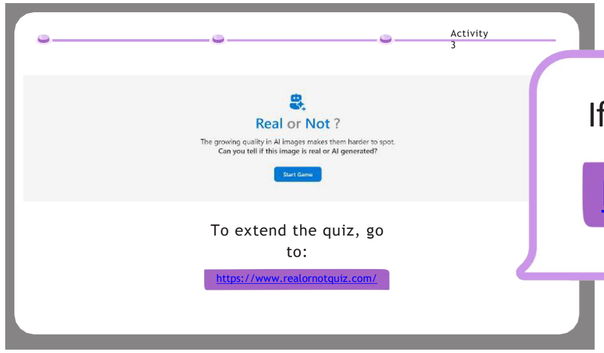
CNIL - artificial intelligence: what are we talking about?

DURATION OF THE ACTIVITY: 10MIN

ACTIVITY 3: SPOT DEEPFAKE CONTENT

SLIDES TO PROJECT

To start, offer the quiz "Real photo or not ?". For each statement, participants must guess whether the proposed image is real or generated by an AI.



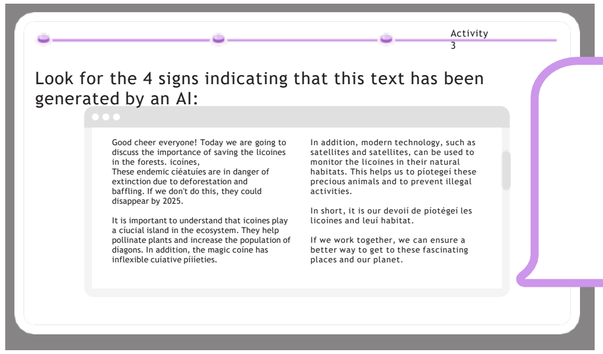
If you want to extend the activity, you can continue the quiz on the website:

https://www.realornotquiz.com/

2 BEWARE OF APPAREANCES

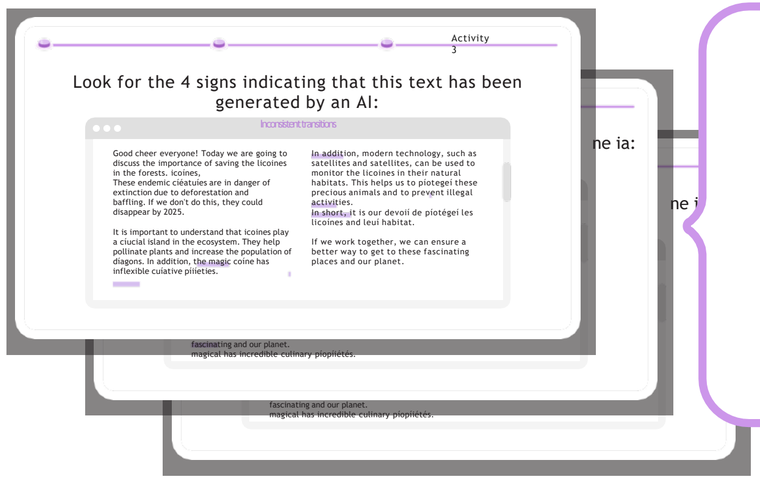
DURATION OF THE ACTIVITY: 10MIN

ACTIVITY 3: SPOT DEEPFAKE CONTENT



How can you spot content generated by artificial intelligence and thus be wary of it? To test the participants, offer to read this fake article and identify the signs betraying it.

SLIDE TO PROJECT

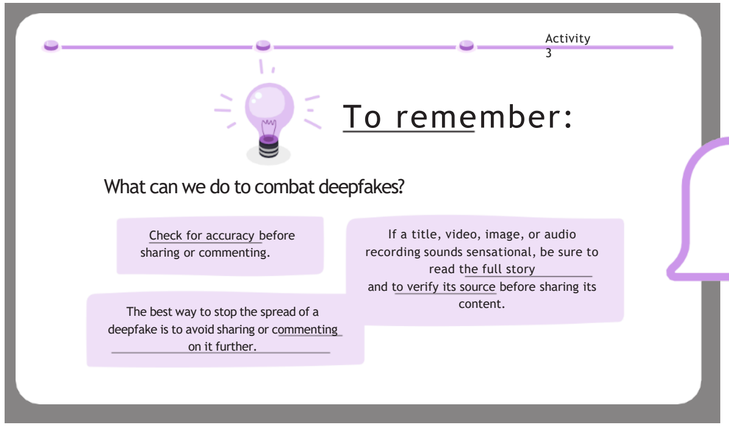


Bring up the clues as you go along by commenting on them:

1. ***Factual inconsistencies:*** *Mention of unicorns and dragons as real creatures with an ecological role.*
2. ***Inconsistent Transitions****: Abrupt transition between points without detailed explanations.*
3. ***Lack of sources:*** *No facts or figures mentioned (such as the disappearance of unicorns by 2025) are sourced.*
4. ***Punctuation errors and turning:*** *Correct punctuation but use of exclamation marks without spaces ("Hello everyone!") which may seem artificial.*

DURATION OF THE ACTIVITY: 10MIN

ACTIVITY 3: SPOT DEEPFAKE CONTENT



SLIDE TO PROJECT

Take stock of the points to remember to spot deepfakes.

3 PROTECT YOUR ACCOUNTS ONLINE

CONTEXT

Like most people, you probably use **the same password for multiple online accounts**. This is a mistake: hackers can easily gain access to your online accounts if your email password is compromised. So, it's important to know how **to manage your passwords** and **protect your online accounts**.

PROTECT YOUR ACCOUNTS ONLINE

OBJECTIVE OF THE SEQUENCE

This sequence encourages participants **to regain control of their passwords** in order to better protect their online accounts through a strategy based on: **choosing a unique password for each account, two-factor authentication for sensitive accounts, using a password manager and creating a strong and easy-to-remember password.**

At the end of this sequence, participants will be able to:

- **Understand the techniques** to create unique and secure passwords (passphrases, random words, password manager).
- Identify the value of two-factor **authentication** for the most sensitive accounts, including the email account.

ACTIVITIES

ACTIVITY 1: A GOOD PASSWORD IS YOUR BEST LINE OF DEFENSE

Raise awareness of the threats to passwords and the need for a unique and strong password per website, application, email, social network.

Learn how to manage your passwords.

ACTIVITY 2: PROTECT YOUR MOST IMPORTANT ONLINE ACCOUNTS

Introduce two-factor authentication for online accounts, especially for email accounts.

3 PROTECT YOUR ACCOUNTS ONLINE

SLIDE TO PROJECT

Before you begin, ask participants what they know about passwords:

Why are passwords important? How do they memorize them?

Can they have a different password for each device and online account? How many online accounts do they have?

Is it a good idea to use a notebook to write down your passwords? Should you let the browser save your passwords?

How can you help a loved one who doesn't know how to manage their passwords?

LET'S MOVE ON NOW TO ACTIVITIES

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: A GOOD PASSWORD IS YOUR...

CONTEXT

The security of online services such as email accounts, social networks, banks, online sales sites depends mainly on passwords. It's easy to succumb to the temptation to choose passwords that are too simple, but this increases the **risk of being hacked**.

OBJECTIVE OF THE SEQUENCE

- Raise awareness of password threats and the need for a strong, unique password per website/app/messaging/social network.
- Learn how to manage your passwords.

RESOURCES TO GO FURTHER

The CNIL's advice for a good password | CNIL
Security: Use multi-factor authentication for your online accounts | CNIL Why and how to manage your passwords - Cybermalveillance Recommendations for multi-factor authentication and passwords | ANSSI

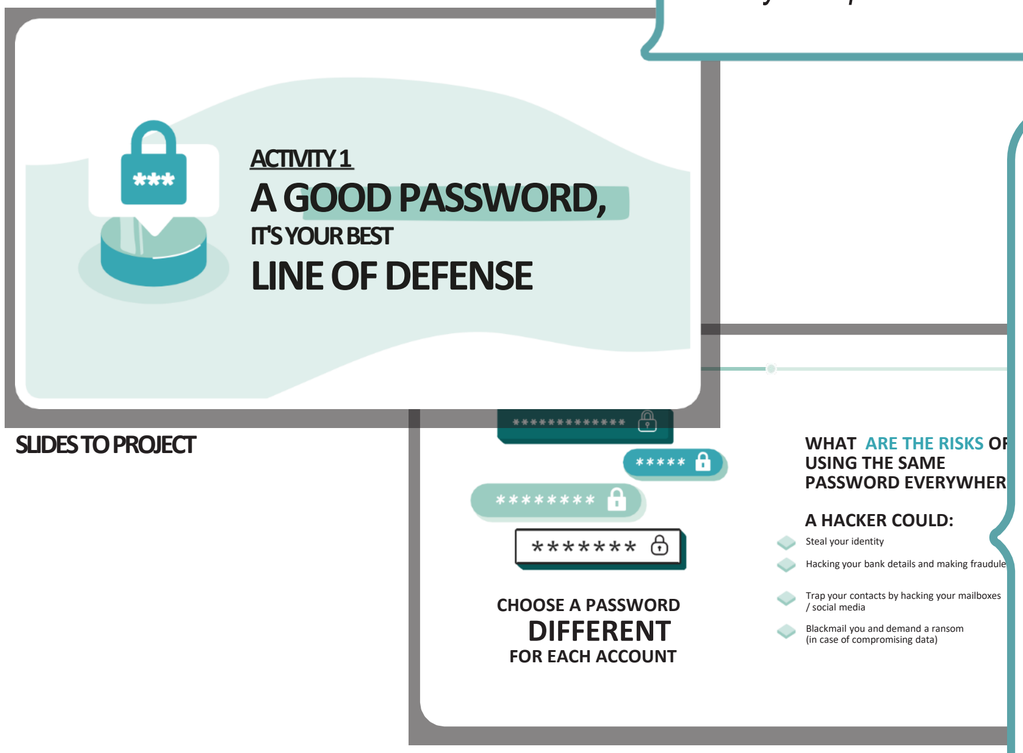
3 PROTECT YOUR ACCOUNTS ONLINE

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: A GOOD PASSWORD IS YOUR...

To begin, ask participants:

Why is it important to choose a good password?



Reusing the same password for all your online accounts is not a good practice at all. By varying passwords and using a strong, unique password per account, the risk of cascading hacks is reduced.

So one of the most effective cybersecurity measures is to have a word from
Different for each of your accounts and devices, but it's not easy to remember each of them.
One solution is to use a password manager:
All you need to do is remember a single strong password.

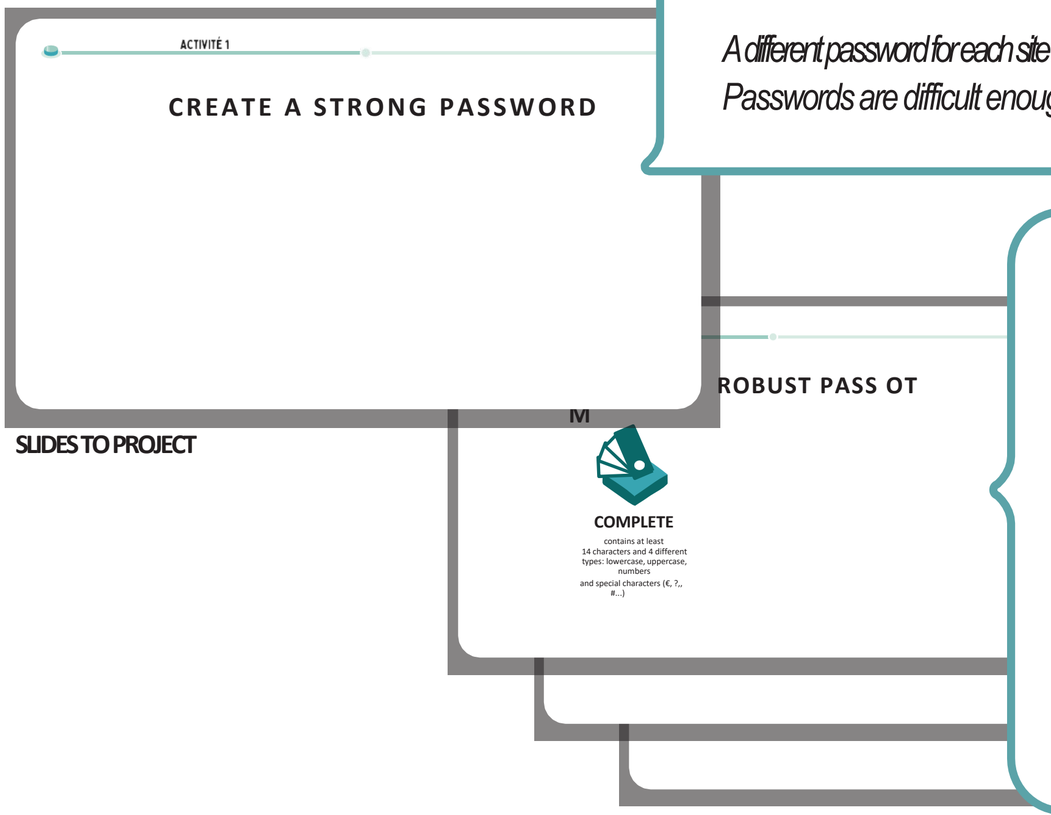
Next, review the risks of using a password unique by specifying:

The main risk of using a single password for all your accounts is to get hack all of their personal data. Because if a hacker manages to find out your authentication methods on a site, it can then use them on all your accounts.

3 PROTECT YOUR ACCOUNTS ONLINE

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: A GOOD PASSWORD IS YOUR...



SLIDES TO PROJECT

To begin, ask participants:

What are the characteristics of a strong password?

A different password for each site is already good but not enough! However, it is necessary that Passwords are difficult enough to guess to discourage some fraudsters.

Review the 3 criteria for a strong password by commenting on them:

A good password is strong if it meets three criteria:

Complete: contains at least 14 characters and 4 different types: lowercase, capitals, numbers, and special characters (punctuation marks or (€, #...)).

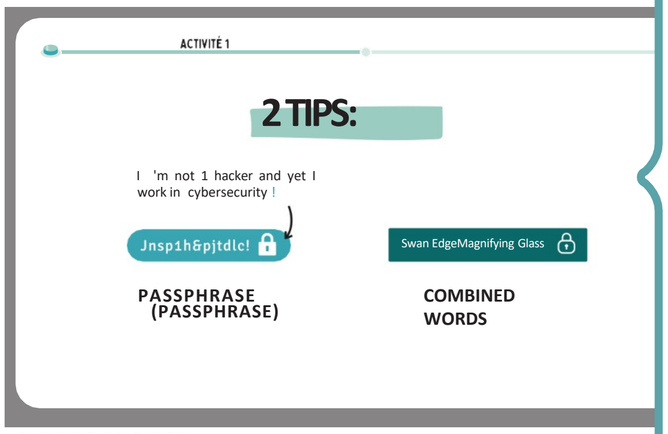
Says nothing about you: no one should guess your password from your date birthday, your nickname or your favorite movie. The same goes for the code of your Smartphone: prefer a random number to a year.

Unique: each of your online accounts (email, social network, etc.) must have its own password and you should not reuse this password for another account.

3 PROTECT YOUR ACCOUNTS ONLINE

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: A GOOD PASSWORD IS YOUR...



SLIDE TO PROJECT

It's not easy to create a strong and easy-to-remember password. However, there is the passphrase technique or combined words.

Memorize a phrase and then use the first letter of each word to create your password. The sentence must contain numbers and special characters! The CNIL provides
A generator that allows you to design your password in seconds! Example: "I'm not 1 hacker and yet I work in cybersecurity!" can become: Jnsp1h&pjtdlc!

Another technique for creating a strong password is to combine random sets of four words. For example, "SwanSongBearerMagnifying Glass" is a password that is very complicated to guess, but easy to remember. The strongest passwords are random sets of three or four words. When you choose words of different lengths and place them in a specific order, it is more difficult to crack your password: the hacker has no idea how long the password is or what types of words/characters it contains.

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 1: A GOOD PASSWORD IS YOUR...

SLIDE TO PROJECT

Explain that another solution is to use a password generator whose main advantage is to create random passwords that are therefore difficult to guess:

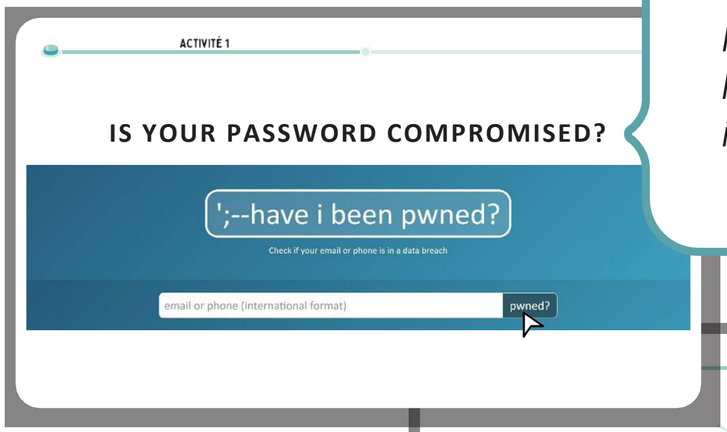
It can be difficult to remember the many passwords, especially if they are strong and randomly generated. That's why password managers were created! It's a convenient solution that allows you to save ALL accounts and passwords with peace of mind.

With a password manager, all usernames and passwords can be stored in a secure database encrypted by a "master" password that has been verified for security. This allows you to have only one password to access all the others. Passwords can be very long, very complex and all different because it is the computer that generates them and remembers them for you. This software also makes it easier to enter passwords without errors and allows you to remember the many usernames and accounts that you accumulate over time.

In practice, there are many solutions on the market. Among the free software products are KeePass (whose security has been evaluated by the ANSSI), Zenyway and Passwordsafe.

DURATION OF THE ACTIVITY: 15MIN

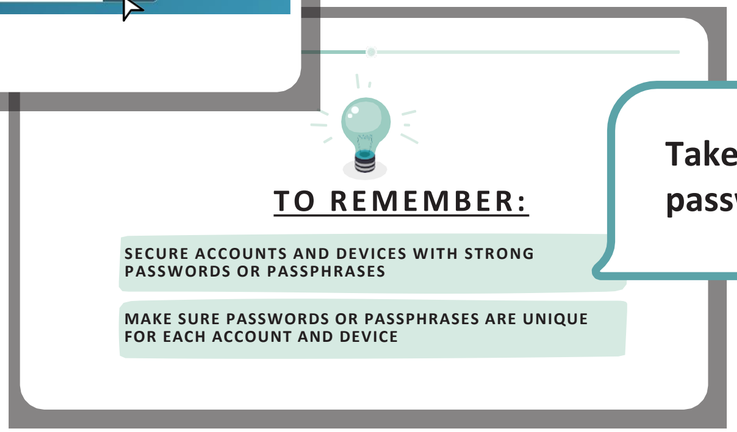
ACTIVITY 1: A GOOD PASSWORD IS YOUR...



SLIDES TO PROJECT

Finally, visit the site to check if a password has been compromise:

haveibeenpwened.com is a site that lists passwords compromised during massive data leaks. The user only has to enter his email address or phone number (often used as an identifier) to find out if he is in a hacked database and if his passwords have been stolen.



Take stock of the actions to remember for good use passwords.

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 2: PROTECT YOUR ONLINE ACCOUNTS...

CONTEXT

Using the same password for all your accounts is a **risky practice**. If you are a victim of **phishing** or if a third-party website is the victim of a data breach that includes your password, a fraudster could use them to not only access that website, but also to access the content of your email.
It is not recommended to use your email account to store sensitive data. In particular, avoid storing credentials such as a scan of your passport, ID card or passwords in a draft.

It is preferable to use a **protected folder**, such as a personal safe, to store encrypted files and make them accessible only after two-factor authentication.

If you don't secure your email account now, this situation could expose you to further dangers. Indeed, a malicious person could use the forgotten password feature to take control of your other online accounts. Be careful with email accounts that you don't use much; They could easily be hijacked without you noticing.

OBJECTIVE OF THE SEQUENCE

Introducing two-factor authentication for online accounts, especially for mailboxes.

RESOURCE FOR FURTHER

Jean-Jacques Latour, Cybermalveillance.gouv.fr, explains the danger of hacking mailboxes

DURATION OF THE ACTIVITY: 15MIN

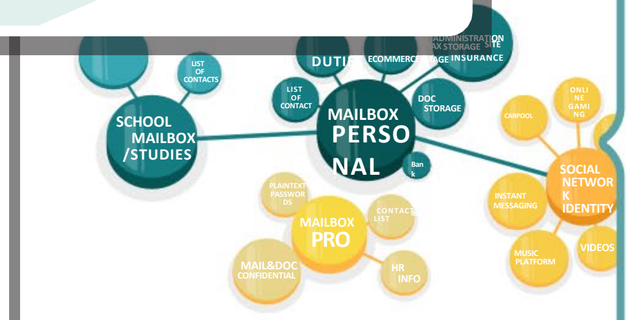
ACTIVITY 2: PROTECT YOUR ONLINE ACCOUNTS...

SLIDES TO PROJECT

To begin, ask participants:

Have you ever used two-factor authentication?

What is the difference between two-factor authentication and passwordless authentication?



(According to the CNIL infographic "Why secure your mailbox password as much as possible? ")

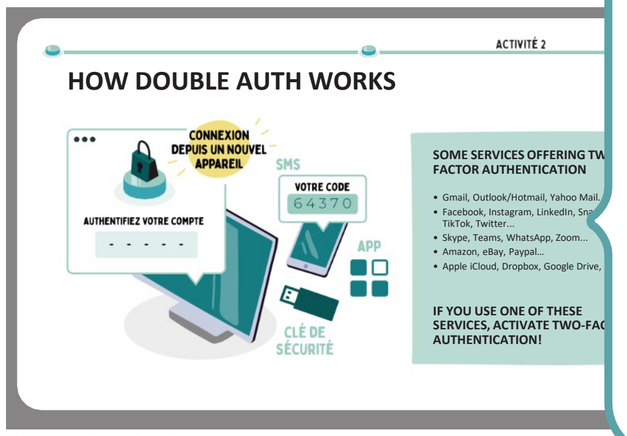
Nowadays, most online services require an email address to register. The security of these services depends on the security of your email account. This means that if someone accesses your account from messaging, it will be able to easily access all other related services by making a reset request password through the link contained in the email received in your inbox. It is therefore necessary to ensure that their email accounts are well secured, enabling all available security options such as two-factor authentication and passwordless authentication. This consideration also applies to social media accounts that are increasingly connected to apps.

A fraudster accessing your email account could do the following:

- ***Identity theft** thanks to the data found in your mailbox (passport copy, card photo) blue, proof of address, etc.).*
- ***Hijacking online accounts** with password reset features.*
- ***Ransom demand** following compromising data found in your mailbox.*
- ***Adding an email forwarding** (often unverified after a mailbox has been compromised): your emails continue to leak despite any subsequent password changes...*

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 2: PROTECT YOUR ONLINE ACCOUNTS...



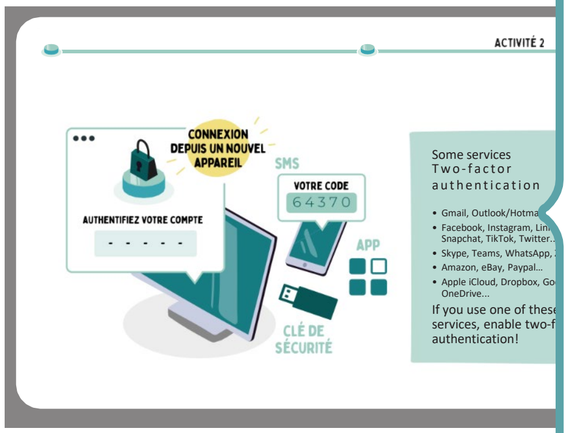
SLIDE TO PROJECT

Use the infographic to explain two-factor authentication and Encourage your contacts to activate it on their accounts whenever possible:

Two-factor authentication, also known as "two-step authentication/verification", is an effective way to keep an online account secure. More and more online services offer this option. In addition to your account name and password, these services ask you for confirmation that you can receive, for example, as a temporary code received by SMS, e-mail (email), via an app or a FIDO2 security key that you keep with you.

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 2: PROTECT YOUR ONLINE ACCOUNTS...



SLIDE TO PROJECT

Apps like Microsoft Authenticator or Google Authenticator allow you to simplify the use of two-factor authentication for your accounts by accepting or not accepting a notification on your phone.

If you sign in to your account from a new device or from a new geographic location, you will receive a notification. You can choose to allow or deny access! This function also informs attempts by others to access their account.

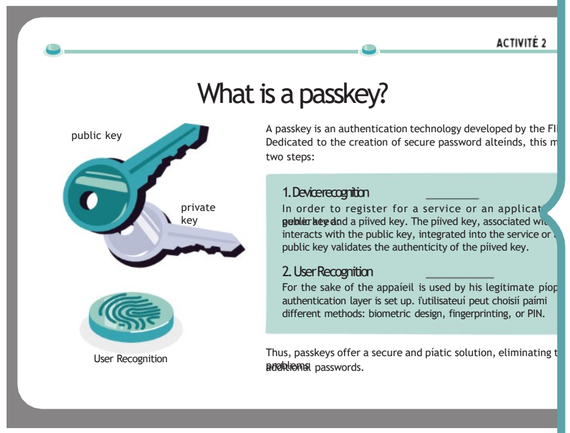
If you receive an authentication code that you didn't ask for (for example, if you didn't just try to sign in to your account), someone else probably knows your password and is trying to access your account. It is advisable to log in to this account as soon as possible and change the password. If this password is used on other accounts, you must change it on those accounts as well.

You can do a demonstration on how to enable the dual authentication on Instagram, Facebook, Gmail, Outlook, Snapchat or TikTok:

Two-factor authentication on Instagram Two-factor authentication on Facebook Two-step authentication on Google account Two-step authentication on Microsoft account Two-factor authentication on Snapchat Two-step authentication on TikTok

DURATION OF THE ACTIVITY: 15MIN

ACTIVITY 2: PROTECT YOUR ONLINE ACCOUNTS...



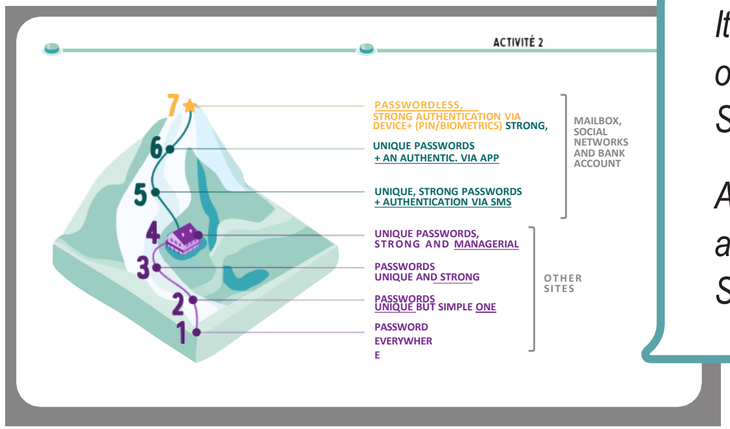
SLIDE TO PROJECT

Now explain the principle of the passkey:

Another more secure and phishing-resistant option is being deployed in the tech world, and that is passkeys. They were designed by the giants of the industry to overcome the weaknesses of passwords. In short, passkeys use encryption technology to secure access. They create a unique key that is stored exclusively on the device. Secondly, they rely on smartphone locking systems, such as biometric recognition or a PIN code, to ensure that it is the owner of the account who is logging in. This makes it more secure and just as easy to use as a password. However, you should know that not all sites are compatible with passkeys yet, but this should accelerate in the coming months.

DURATION OF THE ACTIVITY: 15MIN

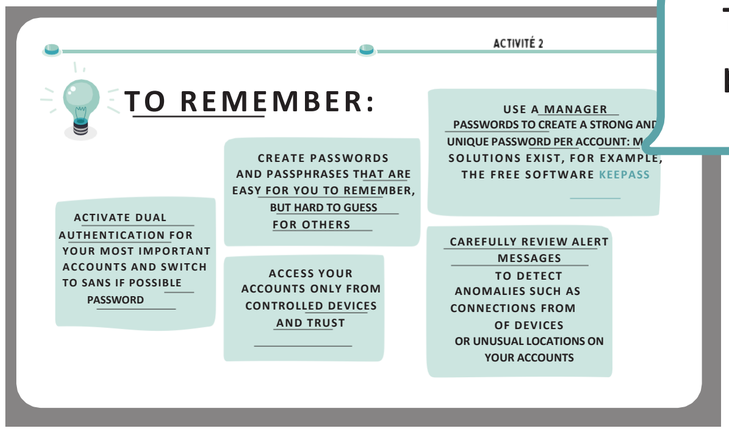
ACTIVITY 2: PROTECT YOUR ONLINE ACCOUNTS...



SLIDES TO PROJECT

It's time to spring clean your digital identities! This means sorting through your online accounts and make sure you have a password manager to manage passwords Strong and unique: this is stage 4!

A passwordless future using a strong authentication mechanism is possible, but there is still a few steps to take before you get there. In the meantime, two-factor authentication is a measure of Security you should set up on your most important online accounts: These are steps 5 and 6.



Take stock of the actions to remember to best protect online accounts.

CYBER IS AN EXCITING JOB OF THE FUTURE!

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

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

REPORTING SCAMS IS ESSENTIAL!

IT IS PREFERABLE TO HAVE SEVERAL PASSWORDS, AS WE HAVE SEVERAL KEYS!

FOR THE MOST IMPORTANT ACCOUNTS, AT LEAST TWO-FACTOR AUTHENTICATION!

SLIDE TO PROJECT

You can conclude by simply reading the conclusion slide.
Then, you can thank the workshop participants by giving them a saying a few words.

THANK YOU!

Version 2.0 - June 2024

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

With contributions from: 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 and Thierry Matusiak.