

LA CYBERSÉCURITÉ, MON FUTUR MÉTIER !

GUIDE DE L'INTERVENANT



UNE INITIATION À LA CYBERSÉCURITÉ EN 3 SÉQUENCES

Ce kit pédagogique comprend **trois séquences**, chacune composée de plusieurs activités.

Les séquences sont **indépendantes** les unes des autres et peuvent être réalisées **selon vos besoins**.

COMMENT UTILISER CE KIT ?

À vous d'adapter le langage à ceux que vous voulez convaincre et de choisir les mots qui conviennent aux jeunes en s'adaptant à leurs préoccupations !

SOMMAIRE

3 AVANT DE COMMENCER

6 1 LES MÉTIERS CYBERSÉCURITÉ

ACTIVITÉ 1 : LES GESTES DE LA CYBER

ACTIVITÉ 2 : JE NE SUIS PAS UN HACKER ET POURTANT
JE TRAVAILLE DANS LA CYBERSÉCURITÉ !

ACTIVITÉ 3 : LA CYBER : UN OU DES MÉTIERS ?

21 2 MÉFIEZ-VOUS DES APPARENCES !

ACTIVITÉ 1 : ÉVITEZ LES ARNAQUES AU FAUX SUPPORT TECHNIQUE

ACTIVITÉ 2 : NE LAISSEZ PAS LES CYBERCRIMINELS VOUS VOLER !

44 3 PROTÉGEZ VOS COMPTES EN LIGNE !

ACTIVITÉ 1 : UN BON MOT DE PASSE, C'EST VOTRE PREMIÈRE LIGNE
DE DÉFENSE !

ACTIVITÉ 2 : PROTÉGEZ VOS COMPTES EN LIGNE LES PLUS IMPORTANTS

59 RESSOURCES POUR BIEN PRÉPARER VOTRE INTERVENTION

AVANT DE COMMENCER

Munissez-vous du PDF “Guide Participant” afin de découvrir les slides à projeter pendant votre intervention. Vérifiez que vous aurez à disposition un écran ou un vidéoprojecteur.

Suivez pas à pas les étapes et aidez-vous des instructions pour commenter les slides à projeter au fur et à mesure.

The diagram illustrates the flow of the presentation. It starts with the 'AVANT DE COMMENCER' slide, which points to the '2 MÉFIEZ-VOUS DES APPARENCES' slide. This slide leads to the 'ACTIVITÉ 1: ÉVITEZ LES ARNAQUES AU FAUX' activity, which then points to the '3 PROTÉGEZ VOS COMPTES EN LIGNE' slide. The '3 PROTÉGEZ VOS COMPTES EN LIGNE' slide contains a summary of the previous slide's content, indicating a cyclical or integrated approach to the topics.

2 MÉFIEZ-VOUS DES APPARENCES

ACTIVITÉ 1: ÉVITEZ LES ARNAQUES AU FAUX

Pour commencer, questionnez les participants :

Avez-vous déjà entendu parler de l'arnaque au faux support téléphonique ?
Sur votre ordinateur, avez-vous déjà vu des notifications avec un message d'avertissement demandant d'appeler un numéro de téléphone ?
Et sur votre téléphone ?
Avez-vous déjà reçu un appel téléphonique vous indiquant que votre ordinateur était infecté ?

Ensuite, faites écouter ces deux extraits audio de fraude et d'arnaque en testant les bons réflexes des participants à chaque fin d'écoute :

Face à cette situation, faut-il raccrocher ?
Et si on vous demande d'aller sur un site web ?
Faut-il donner l'accès ou non à son ordinateur ?

3 PROTÉGEZ VOS COMPTES EN LIGNE

DURÉE DE L'ACTIVITÉ : 15 MIN

ACTIVITÉ 1: UN BON MOT DE PASSE, C'EST VOTRE...

CONTEXTÉ

La sécurité des services en ligne tels que les comptes de messageries, les réseaux sociaux, les banques, les sites de vente en ligne dépend principalement des mots de passe. Il est facile de succomber à la tentation de choisir des mots de passe trop simples mais ceci augmente le risque de se faire pirater.

OBJECTIF DE LA SÉQUENCE

- Faire connaître les menaces qui pèsent sur les mots de passe et la nécessité d'avoir un mot de passe unique et fort par site web/application/messagerie/réseau social.
- Apprendre à gérer ses mots de passe.

RESSOURCES POUR ALLER PLUS LOIN

Les conseils de la CNIL pour un bon mot de passe | CNIL
Sécurité : utilisez l'authentification multifactor pour vos comptes en ligne | CNIL
Pourquoi et comment bien gérer ses mots de passe ? - Cybermalveillance
Recommandations relatives à l'authentification multifactor et aux mots de passe | ANSSI

Des éléments de contexte et des ressources sont là pour vous aider à approfondir le sujet et à répondre aux questions des participants.

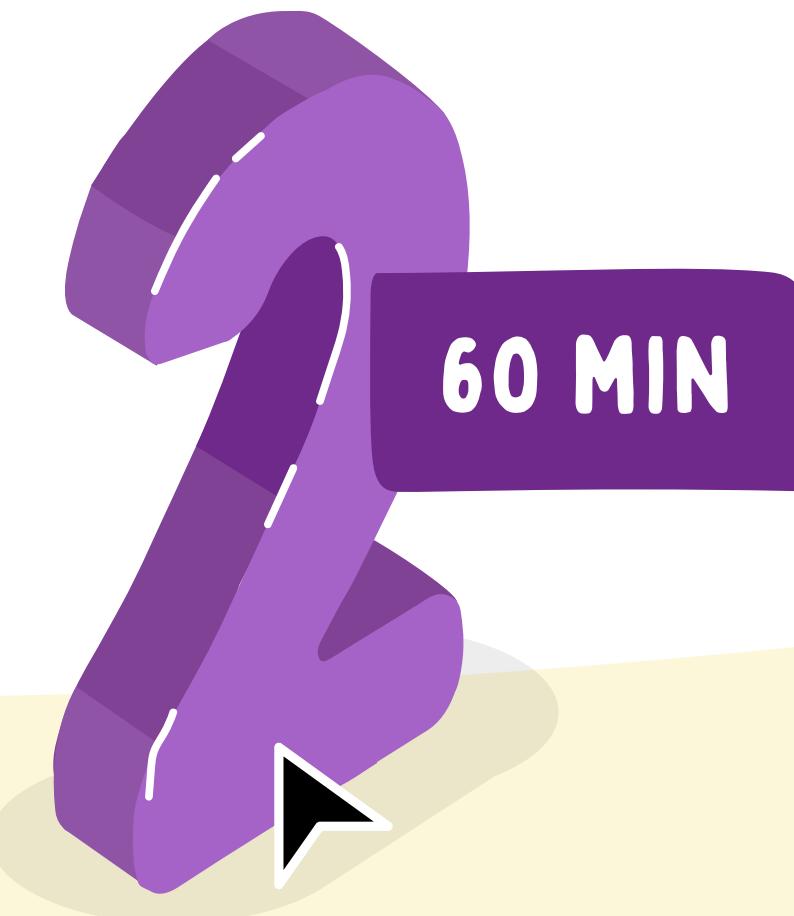
AVANT DE COMMENCER

Assurez-vous de disposer d'assez de temps pour réaliser les séquences qui vous intéressent (durée approximative).



LES MÉTIERS CYBERSÉCURITÉ

Découvrir la diversité
des métiers



MÉFIEZ-VOUS DES APPARENCES

Être vigilants face
aux arnaques en ligne



PROTÉGEZ VOS COMPTES EN LIGNE

Apprendre à gérer
les mots de passe

AVANT DE COMMENCER

Quelques règles d'or de facilitation pour une intervention sereine :

BIEN RÉPARTIR LA PAROLE ENTRE LES PARTICIPANTS

S'ASSURER QUE LES OBJECTIFS SOIENT BIEN COMPRIS À CHAQUE FIN DE SÉQUENCE

CONCLURE EN RÉSUMANT LES POINTS IMPORTANTS



LES MÉTIERS CYBERSÉCURITÉ



CONTEXTE

Il y a une **pénurie de talents** dans le domaine de la cybersécurité avec 15 000 postes à pourvoir en France et, plus globalement, **plusieurs millions de postes sans candidat** dans le monde.

Les profils recherchés sont variés : pas besoin d'être fort en maths ou d'être un geek en informatique, mais pour ceux qui le sont, il existe bien entendu des métiers très techniques – tout le monde peut s'y retrouver/pas de clivage. **Les mathématiques et la programmation sont utiles dans le domaine de la cybersécurité mais ne constituent pas une nécessité.**

Les métiers en cybersécurité couvrent un **large éventail de compétences**. Parmi les métiers les plus courants, on peut citer le hacker éthique, le consultant cybersécurité, l'analyste des incidents de sécurité ou bien encore le Responsable de la Sécurité des Systèmes d'Information (RSSI), mais également les métiers de commerciaux, chef de projets cyber ou responsable marketing.

Les opportunités de recrutement sont nombreuses avec une rémunération attractive (plus importante que la moyenne) et une évolution de carrière (évolution vers des postes différents tout au long de sa vie professionnelle, etc.).

Il est difficile de donner une liste exhaustive de qualités requises pour travailler dans le domaine de la cybersécurité car les postes à pourvoir sont très variés. Toutefois, les qualités suivantes sont généralement observées : **une bonne connaissance des technologies du numérique, une bonne capacité d'analyse et de pensée critique et de la curiosité intellectuelle.**

Les métiers de la cybersécurité sont des métiers qui ont du **sens** :

- Ces métiers sont importants car ils permettent d'**aider son prochain à se protéger des personnes malveillantes**, participer au développement des technologies qui contribueront à la **protection de la santé** (éviter le blocage des hôpitaux par exemple), permettre l'accès à l'**information fiable** (en supprimant les fake news) ou bien **sensibiliser sur les gestes cybersécurité**.
- **Les secteurs d'activité sont sans limite**. On peut choisir de protéger une entreprise privée ou bien une organisation publique.
- La cybersécurité ouvre également à une **mobilité internationale** car le métier est sans frontière. On peut travailler sur l'ensemble des continents.

1

LES MÉTIERS CYBERSÉCURITÉ

OBJECTIF DE LA SÉQUENCE

Cette séquence encourage les participants à **explorer la diversité des métiers de la cybersécurité**, invite à se familiariser avec le **vocabulaire** des métiers et vise enfin à **bousculer les idées reçues**.

À la fin de cette séquence, les participants seront en mesure de :

- citer le nom de quelques métiers en cybersécurité
- mesurer le sens et les enjeux de ces métiers

LES ACTIVITÉS



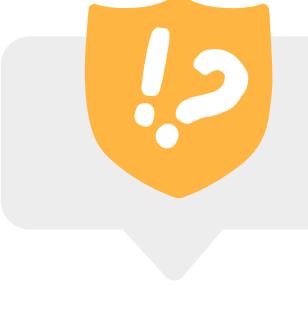
ACTIVITÉ 1 : LES GESTES DE LA CYBER

S'exercer à reconnaître les bonnes pratiques en matière de cybersécurité.



ACTIVITÉ 2 : JE NE SUIS PAS UN HACKER ET POURTANT JE TRAVAILLE DANS LA CYBERSÉCURITÉ !

Remettre en question certains préjugés sur les métiers de la cybersécurité.



ACTIVITÉ 3 : LA CYBER, UN OU DES MÉTIERS ?

Découvrir quelques métiers en cybersécurité.

1

LES MÉTIERS CYBERSÉCURITÉ



SLIDE À PROJETER

Pour commencer, en guise d'icebreaker, demandez aux participants ce qu'ils savent de la cybersécurité en vous aidant de ces exemples :

Connaissez-vous des personnes travaillant dans ce domaine ?

Quels sont les différents métiers en cybersécurité ?

Qu'est-ce que réussir signifie pour vous ?

Gagne-t-on beaucoup d'argent en travaillant dans le domaine de la cybersécurité ?

Pourquoi travailler dans le domaine de la cybersécurité ?

Faut-il être fort en maths pour travailler dans la cybersécurité ?

Faut-il être un geek pour travailler dans la cybersécurité ?

Quelles sont les qualités pour travailler dans le domaine de la cybersécurité ?

1

LES MÉTIERS CYBERSÉCURITÉ

POURQUOI LA CYBERSÉCURITÉ NOUS CONCERNE(RA) TOUTES ET TOUS ?



SOURCE

TOUTES ?

TOUTES ?

TOUTES ?

TOUTES ?

SLIDES À PROJETER

Passez en revue les 4 chiffres-clés illustrés.
Pour aller plus loin, en voici d'autres :

- En 2020, le coût moyen d'une attaque par logiciel malveillant pour une entreprise était de plus de 2,5 millions de dollars. Cela inclut le coût du temps nécessaire à la résolution de l'attaque, qui est de 50 jours en moyenne. [\(source\)](#)
- Au deuxième trimestre de 2020, la rançon moyenne demandée était de plus de 100 000 dollars, et elle continue d'augmenter au fil du temps. [\(source\)](#)
- Le coût total moyen d'un vol de données a augmenté de près de 10 % entre 2020 et 2021 : du jamais vu depuis 7 ans. Le coût total moyen mondial d'une violation de données en 2021 était de 4,24 millions de dollars. [\(source\)](#)
- Le coût total moyen d'un vol d'informations causé par la compromission d'une boîte de messagerie professionnelle est de 5,01 millions de dollars. [\(source\)](#)
- La cybercriminalité devrait coûter au monde 10 500 milliards de dollars par an d'ici à 2025, contre 3 000 milliards de dollars il y a dix ans et 6 000 milliards de dollars en 2021. [\(source\)](#)

1

LES MÉTIERS CYBERSÉCURITÉ



SLIDE À PROJETER

Expliquez aux participants qu'il s'agit d'un secteur dynamique.
(source [ANSSI](#) / Les profils de la cybersécurité - Enquête 2021)

PASSONS MAINTENANT
AUX ACTIVITÉS





ACTIVITÉ 1 : LES GESTES DE LA CYBER

CONTEXTE

Les cyberattaquants choisissent souvent **les attaques les plus faciles à réaliser**.

Par exemple, un voleur choisira d'entrer dans une habitation par une fenêtre facile à ouvrir plutôt que par une porte blindée avec un système de surveillance. Il en est de même dans le monde numérique. Plus les **mesures de sécurité élémentaires** sont en place et moins les risques de cyberattaques sont élevés.

OBJECTIF DE LA SÉQUENCE

S'exercer à reconnaître les bonnes pratiques en matière de cybersécurité.

RESSOURCES POUR ALLER PLUS LOIN

[Rapport d'activité 2021 - Cybermalveillance](#)
[MOOC de l'ANSSI](#)



ACTIVITÉ 1 : LES GESTES DE LA CYBER

ACTIVITÉ 1
**LES GESTES
DE LA CYBER**



SLIDES À PROJETER

Pour commencer, questionnez les participants :

Est-ce qu'un cadenas dans le navigateur signifie que le site est sécurisé ?

Est-il plus risqué de surfer avec un ordinateur ou bien avec un smartphone ?

Ensuite, proposez le quiz “Bonne idée ou pas ?” après avoir exposé le contexte :

Fin 2021, 92 % des foyers en France ont une connexion à Internet, et vous passez en moyenne 3 heures et 53 minutes chaque jour à surfer sur Internet ! (15-24 ans / [Mediametrie](#) 2021) ! Mais savez-vous quels sont les gestes à respecter pour surfer sur internet sans risque ? Pour tester vos connaissances, répondez à ce quiz sur la cybersécurité !

ACTIVITÉ 1

QUIZ

BONNE IDÉE OU PAS ?

ACTIVITÉ 1 : LES GESTES DE LA CYBER

ACTIVITÉ 1

Pensez-vous qu'un bon mot de passe puisse être utilisé pour plusieurs services (boîtes mail, réseaux sociaux, banque, sites de e-commerce, administrations...) ?

A Oui, quand les services n'ont rien à voir les uns avec les autres

B Oui, mais uniquement si le mot de passe contient des caractères spéciaux

C Non, chaque service doit avoir un mot de passe différent

Chaque service doit avoir un mot de passe différent pour éviter les risques d'une compromission en cascade.

Chaque service doit avoir un mot de passe différent pour éviter les risques d'une compromission en cascade.

ACTIVITÉ 1

Vous recevez un mail vous informant que des photos où vous êtes tagué sont disponibles. Le site web vous demande de saisir votre identifiant et votre mot de passe Facebook. Il semble que le site web possède un certificat légitime avec un cadenas à côté de la barre d'adresse.

Vous saisissez votre identifiant et votre mot de passe sur le site web.
Est-ce une bonne idée ou pas ?

A Oui
B Non

Un cadenas s'affichant dans la barre d'adresse ne signifie pas que le site est sécurisé. Au moindre doute, privilégiez l'accès au site web en tapant directement l'adresse dans la barre de recherche. Sinon vous risquez de divulguer votre mot de passe à un fraudeur.

Un cadenas s'affichant dans la barre d'adresse ne signifie pas que le site est sécurisé. Au moindre doute, privilégiez l'accès au site web en tapant directement l'adresse dans la barre de recherche. Sinon vous risquez de divulguer votre mot de passe à un fraudeur.

ACTIVITÉ 1

Vous recevez un mail portant sur la **fermeture de votre compte Instagram**. Ce mail contient le logo Instagram et comporte une pièce jointe. Vous :

- A** Ouvrez la pièce jointe pour en savoir plus
- B** Hésitez à ouvrir la pièce jointe mais êtes rassuré par le logo Instagram
- C** N'ouvrez pas la pièce jointe et vous vous connectez directement sur votre compte

Ne cliquez jamais sur un lien ou une pièce jointe dont l'origine ou la nature vous semblent douteuses. Au moindre doute, privilégiez l'accès au site web en tapant directement l'adresse dans la barre de recherche.

Ne cliquez jamais sur un lien ou une pièce jointe dont l'origine ou la nature vous semblent douteuses. Au moindre doute, privilégiez l'accès au site web en tapant directement l'adresse dans la barre de recherche.

ACTIVITÉ 1

Que faire si un **message bloquant votre ordinateur** apparaît, signalant un problème technique grave, un risque de perte de vos données ou bien la présence de nombreux virus ?

A Ne rien faire

B Contacter le support technique au numéro indiqué sur le message d'erreur

C Tenter de redémarrer votre ordinateur et, si le problème persiste, demander de l'aide à un ami

Les faux messages d'erreur sont généralement générés par un site web malveillant ou compromis. Ces fenêtres pop-up peuvent apparaître pour bloquer l'accès à votre ordinateur, mais le fait de redémarrer votre ordinateur peut suffire à résoudre le problème.

Les faux messages d'erreur sont généralement générés par un site web malveillant ou compromis. Ces fenêtres pop-up peuvent apparaître pour bloquer l'accès à votre ordinateur, mais le fait de redémarrer votre ordinateur peut suffire à résoudre le problème.

Faites attention aux messages qui ont l'air urgents. Si vous avez commandé quelque chose, vous auriez déjà renseigné votre adresse postale. Ne cliquez pas sur ces messages et ne composez pas le numéro fourni.

ACTIVITÉ 1

Vous recevez un SMS vous indiquant que **votre colis arrive** mais qu'il faut **mettre à jour vos coordonnées de livraison**. Vous :

- A Appuyez sur le lien contenu dans le SMS
- B Ne faites rien
- C Appelez le numéro de téléphone de l'expéditeur

Faites attention aux messages qui ont l'air urgents. Si vous aviez commandé quelque chose, vous auriez déjà renseigné votre adresse postale. Ne cliquez pas sur ces messages et ne composez pas le numéro fourni.

ACTIVITÉ 1

Vous êtes à l'aéroport avant d'embarquer pour votre vol. Vous n'avez plus de batterie sur votre téléphone. Il y a des ordinateurs publics à la disposition des passagers pour naviguer sur Internet. Vous voulez passer le temps et aller sur votre réseau social favori.
Vous lancez un navigateur en mode privé, puis vous vous authentifiez avec votre mot de passe pour accéder à votre profil.
Est-ce sans risque ?

A Oui
B Non

Il est risqué de se connecter à vos comptes en ligne depuis un appareil qui ne vous appartient pas. Les touches tapées au clavier pourraient être enregistrées ou bien un logiciel malveillant pourrait vous voler vos secrets d'authentification.

Il est risqué de se connecter à vos comptes en ligne depuis un appareil qui ne vous appartient pas. Les touches tapées au clavier pourraient être enregistrées ou bien un logiciel malveillant pourrait vous voler vos secrets d'authentification.



ACTIVITÉ 1 : LES GESTES DE LA CYBER

ACTIVITÉ 1

POUR UNE BONNE HYGIÈNE NUMÉRIQUE

RESSOURCE À LIRE POUR ALLER PLUS LOIN



- Choisir avec soin ses mots de passe
- Mettre à jour régulièrement et appliquer les correctifs sur les appareils
- Effectuer des sauvegardes de vos données régulièrement
- Sécuriser l'accès à votre Wi-Fi
- Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur
- Être prudent lors de l'utilisation de sa messagerie
- Télécharger ses programmes sur les sites officiels des éditeurs
- Être vigilant lors d'un paiement sur Internet
- Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Faites découvrir le [guide de bonnes pratiques de l'informatique](#) publié par L'ANSSI et la CPME à destination des petites et moyennes entreprises dont les 9 règles peuvent s'appliquer également aux particuliers. C'est ce qui s'appelle l'hygiène numérique.

ACTIVITÉ 1



UN GESTE À RETENIR :

PRENDRE L'HABITUDE DE VERROUILLER L'ÉCRAN DE SES APPAREILS LORSQUE L'ON S'EN ÉLOIGNE POUR ÉVITER TOUT ACCÈS NON AUTORISÉ, NOTAMMENT EN CAS DE PERTE OU DE VOL.

Faites le point sur un geste à retenir pour protéger l'accès physique à ses appareils.



ACTIVITÉ 2 : JE NE SUIS PAS UN HACKER ET POURTANT...

En référence au livre « [Je ne porte pas de sweat à capuche, pourtant je travaille dans la cybersécurité](#) ».

CONTEXTE

Le domaine de la cybersécurité souffre d'un **déficit d'image** où l'expert est une personne solitaire, de type geek, qui semble être un petit génie de l'informatique passant son temps derrière son écran à coder pour franchir les systèmes de sécurité. Le **témoignage d'un professionnel de la cybersécurité** et un **quiz** sont là pour bousculer ces idées reçues.

OBJECTIF DE LA SÉQUENCE

Remettre en question certains préjugés sur les métiers de la cybersécurité.

RESSOURCE POUR ALLER PLUS LOIN
[Padlet – La cyber, mon futur métier !](#)



ACTIVITÉ 2 : JE NE SUIS PAS UN HACKER ET POURTANT...



ACTIVITÉ 2
JE NE SUIS PAS UN HACKER
ET POURTANT JE TRAVAILLE
DANS

ACTIVITÉ 2

**EN QUOI CONSISTE
TON MÉTIER ?**

- Comment es-tu arrivé dans la cybersécurité ?
- Qu'est-ce qui te plaît dans ton métier ?
- À quoi ressemble une journée type dans la cybersécurité ?
- Faut-il savoir parler anglais pour exercer ton métier ?
- As-tu déjà été victime d'un virus ou d'un phishing ?
- Quels sont tes trois conseils cybersécurité ?
- Que dirais-tu aux jeunes qui hésitent à se lancer en cybersécurité ?

▶

SLIDES À PROJETER

Vous pouvez présenter quelques témoignages vidéo et commenter les différentes caractéristiques des métiers présentés (sens de l'engagement, apprendre à apprendre, collaboration) grâce au [Padlet - La cyber, mon futur métier !](#)

Si vous êtes un professionnel de la cybersécurité, partagez votre propre témoignage et votre parcours à l'aide des questions présentes sur la slide ou celles-ci :

C'est quoi ton job ?

En quoi consiste le métier ? Quelles sont les différentes tâches réalisées ?

Quelle est la taille de ton entreprise ?

Quels sont les lieux de travail ? Voyages-tu souvent ?

Quels sont les outils nécessaires à ton travail ?

Comment es-tu arrivé(e) dans la cybersécurité ?

Qu'est-ce qui te plaît dans ton métier ?

À quoi ressemble une journée type dans la cybersécurité ?

Faut-il savoir parler anglais pour exercer ton métier ?

As-tu déjà été victime d'un virus ou d'un phishing ?

Quels sont tes trois conseils cybersécurité ?

Que dirais-tu aux jeunes qui hésitent à se lancer en cybersécurité ?

Vous pouvez également illustrer comment les différents métiers de la cybersécurité collaborent.



ACTIVITÉ 2 : JE NE SUIS PAS UN HACKER ET POURTANT...

ACTIVITÉ 2

QUIZ

BOUSCULER LES IDÉES REÇUES SUR LES MÉTIERS DE LA CYBERSÉCURITÉ

SLIDES À PROJETER

Ensuite, proposez le quiz “Bousculer les idées reçues sur les métiers de la cybersécurité”. Pour chaque affirmation, les participants répondent par “Vrai” ou “Faux” afin de découvrir la bonne réponse.

Faites le point sur l'idée principale à retenir sur les métiers cyber.

À RETENIR :

LA CYBERSÉCURITÉ EST À LA PORTÉE DE TOUTES ET DE TOUS !



ACTIVITÉ 3 : LA CYBER : UN OU DES MÉTIERS ?

CONTEXTE

Les besoins en cybersécurité augmentent à mesure que les entreprises dépendent de plus en plus des technologies de l'information et de la communication. Les organisations font face à des risques de plus en plus élevés en matière de fuites de données, de fraude, de piratage et d'intrusion. Les professionnels de la cybersécurité ont un rôle important à jouer pour aider les organisations à protéger leurs actifs numériques (données, ordinateurs et réseaux).

OBJECTIF DE LA SÉQUENCE

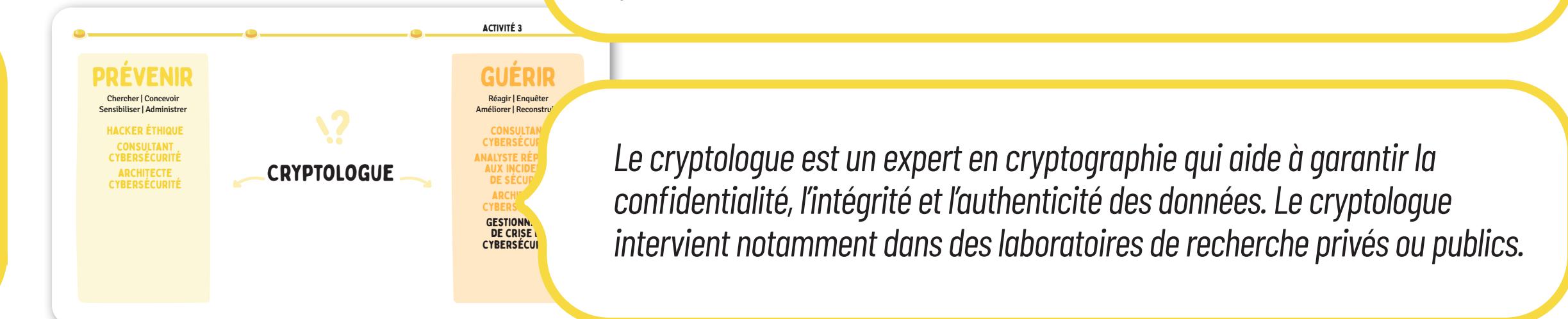
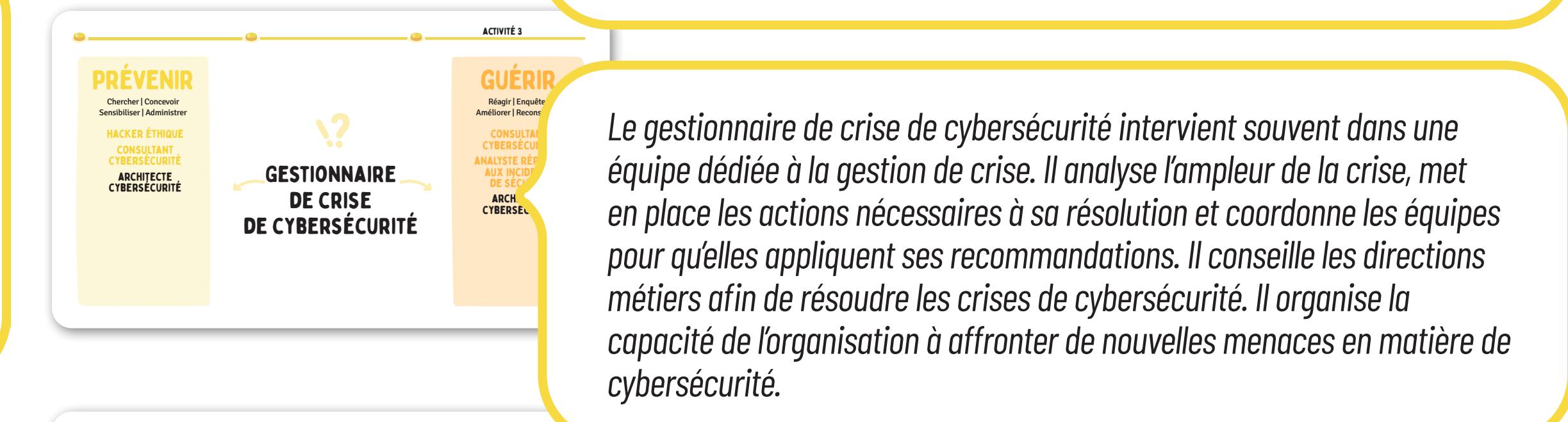
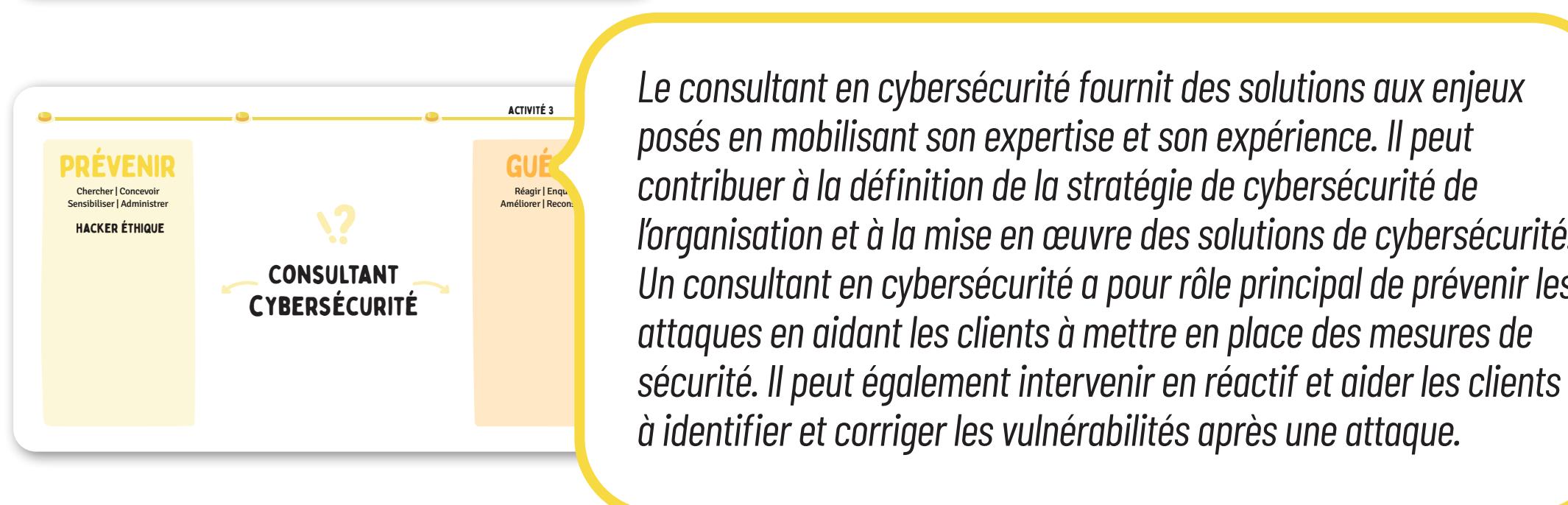
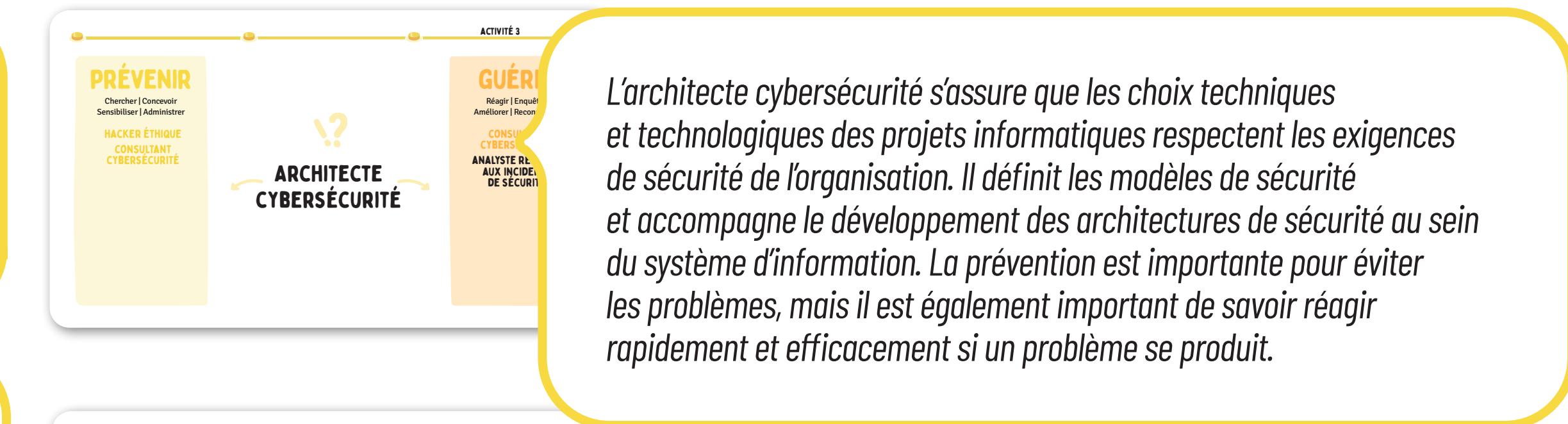
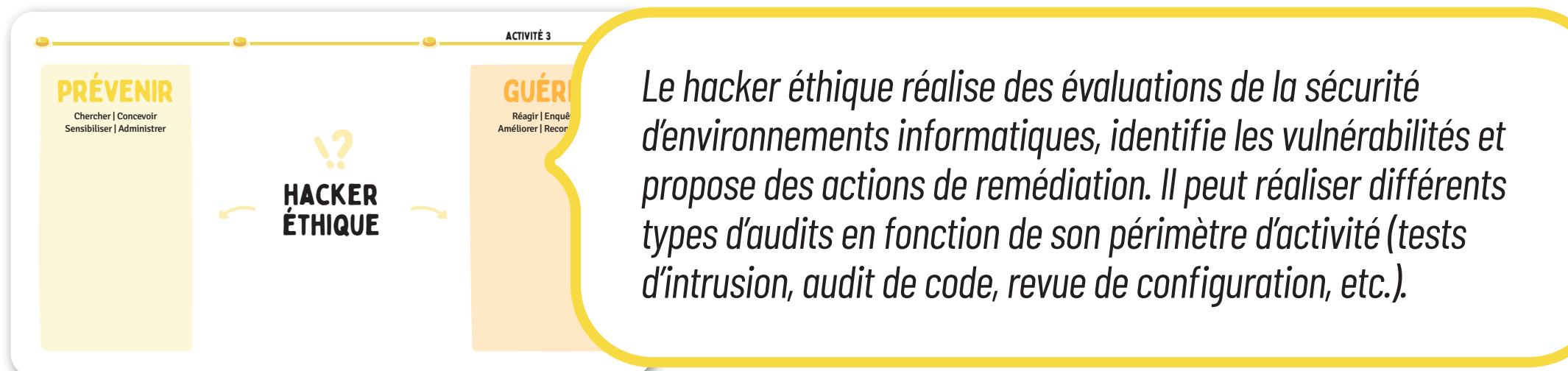
Découvrir quelques métiers en cybersécurité.

RESSOURCES POUR ALLER PLUS LOIN

[Panorama des métiers de la cybersécurité - ANSSI](#)
[Cartographie des métiers de la cybersécurité - EGE](#)
[Les métiers de la cybersécurité – Guardia School](#)



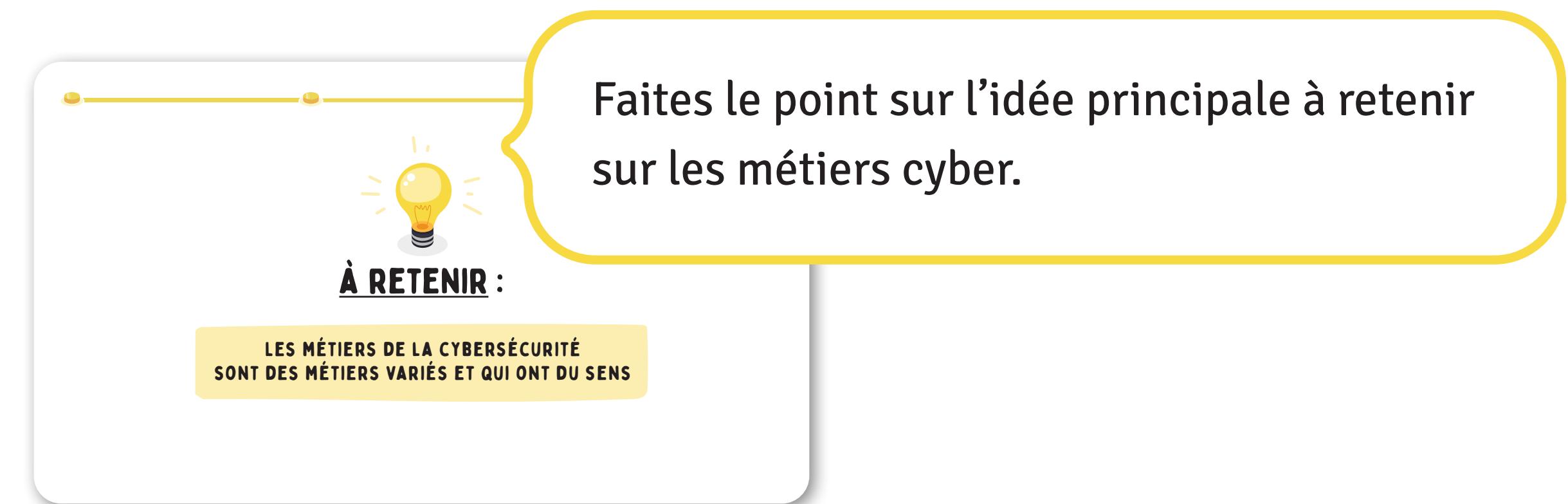
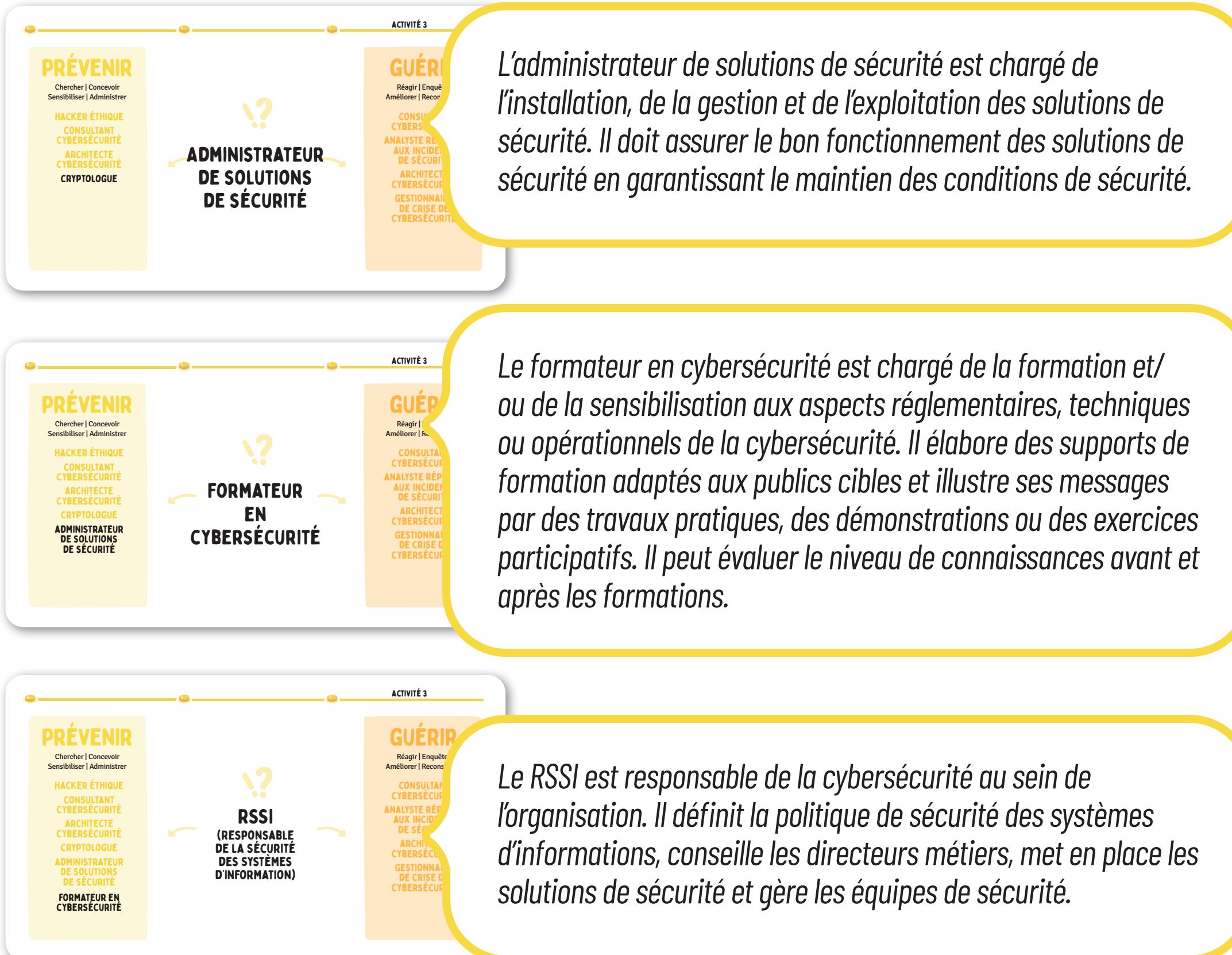
ACTIVITÉ 3 : LA CYBER : UN OU DES MÉTIERS ?



(D'après le regroupement d'appellation "Prévenir et Guérir", du livre :
Envie de Cyber, ISSA France Security Tuesday, Ed. Studyrama)



ACTIVITÉ 3 : LA CYBER : UN OU DES MÉTIERS ?





MÉFIEZ-VOUS DES APPARENCES

CONTEXTE

Les fraudeurs sont partout et ciblent tout le monde : les adolescents, les grands-parents ou bien les dirigeants d'entreprises. Les **escroqueries en ligne** peuvent prendre plusieurs formes mais leur but est toujours le même : **vous voler vos mots de passe, données personnelles, coordonnées bancaires, accès à vos appareils et à vos comptes en ligne**.

Les appels et les messages non sollicités constituent l'un des principaux modes d'actions des fraudeurs. Les fraudeurs sont assez **persuasifs** pour vous convaincre qu'il y a un virus sur votre ordinateur, que vous devez payer une somme d'argent, qu'il y a des activités frauduleuses sur votre compte bancaire. Les fraudeurs cherchent à vous faire **installer un logiciel malveillant**, **approuver une transaction bancaire** ou une demande d'authentification, **divulguer des informations personnelles** ou bien votre mot de passe.

Il est important de rester **vigilant** (sans devenir paranoïaque) en adoptant des réflexes :

- Développer son esprit critique et ne pas hésiter à se poser des questions : pourquoi telle personne m'envoie une pièce jointe par mail ? Ai-je déjà visité le site pointé par le lien dans ce SMS ? Pourquoi mon ami m'écrit ce message bizarre ? etc.
- Utiliser des gestes simples comme verrouiller son ordinateur ou son téléphone, ou encore éviter de taper ses identifiants sur un appareil qui ne nous appartient pas.



MÉFIEZ-VOUS DES APPARENCES

OBJECTIFS DE LA SÉQUENCE

Cette séquence permet aux participants de **découvrir les caractéristiques courantes des arnaques en ligne** et de **démontrer leur compréhension** en se mettant à la place d'un attaquant.

À la fin de cette séquence, les participants seront en mesure de :

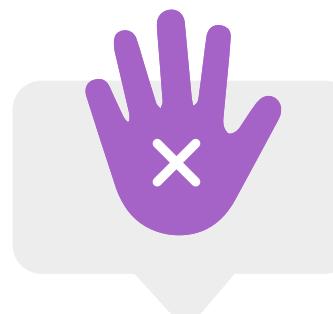
- Reconnaître **les signes d'une arnaque**
- Expliquer **les différents réflexes** à avoir contre les arnaques les plus courantes
- **Sensibiliser les autres** en racontant le déroulement d'une arnaque en ligne

LES ACTIVITÉS



ACTIVITÉ 1 : ÉVITEZ LES ARNAQUES AU FAUX SUPPORT TECHNIQUE

Savoir réagir et signaler les arnaques au faux support technique



ACTIVITÉ 2 : NE LAISSEZ PAS LES CYBERCRIMINELS VOUS VOLER !

Apprendre à reconnaître les signes d'une escroquerie



MÉFIEZ-VOUS DES APPARENCES



SLIDE À PROJETER

Pour commencer, en guise d'icebreaker, demandez aux participants ce qu'ils connaissent des arnaques en ligne et comment les détecter en vous aidant de ces questions :

Qu'est-ce qu'une arnaque en ligne ?

Pourquoi quelqu'un essaierait-il de vous arnaquer en ligne ?

Comment savoir si vous êtes face à une arnaque ?

Que faire si vous pensez avoir été victime d'une arnaque en ligne ?

**PASSONS MAINTENANT
AUX ACTIVITÉS**





ACTIVITÉ 1 : ÉVITEZ LES ARNAQUES AU FAUX SUPPORT...

CONTEXTE

Cette escroquerie fait des **ravages** chez les particuliers. Lors d'une navigation sur Internet ou après avoir cliqué sur un lien malveillant, **une fenêtre apparaît et bloque votre ordinateur**. Elle demande de rappeler **d'urgence** un numéro de support technique sous peine de perdre l'accès à vos données ou à l'usage de votre ordinateur. Une fois contacté, le pseudo service technique vous demande d'**accéder à distance à votre terminal et facture un faux dépannage** tout en vous faisant acheter des logiciels inutiles, voire dangereux.

OBJECTIF DE LA SÉQUENCE

Savoir réagir et signaler les arnaques au faux support technique.

RESSOURCES POUR ALLER PLUS LOIN

[Comment faire face à l'arnaque au faux support technique ? -Cybermalveillance](#)
[Fiche Réflexe arnaque au faux support technique - Cybermalveillance](#)
[Protégez-vous contre les escroqueries au support technique \(microsoft.com\)](#)

2 MÉFIEZ-VOUS DES APPARENCES

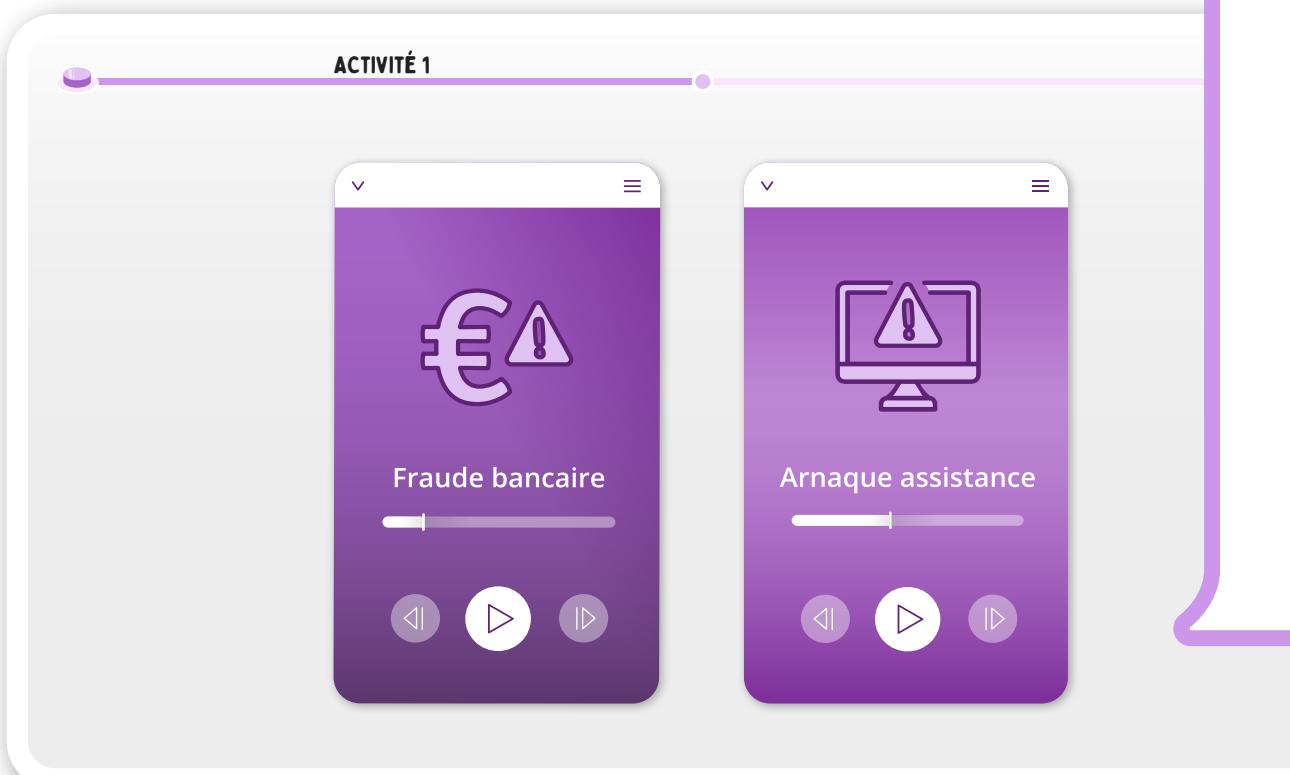
DURÉE DE L'ACTIVITÉ : 15MIN



ACTIVITÉ 1 : ÉVITEZ LES ARNAQUES AU FAUX SUPPORT...

ACTIVITÉ 1 ÉVITEZ LES ARNAQUES AU FAUX SUPPORT TECHNIQUE

SLIDES À PROJETER



Pour commencer, questionnez les participants :

Avez-vous déjà entendu parler de l'arnaque au faux support technique ?

Sur votre ordinateur, avez-vous déjà vu des notifications avec un message d'avertissement vous demandant d'appeler un numéro de téléphone ?

Et sur votre téléphone ?

Avez-vous déjà reçu un appel téléphonique vous indiquant que votre ordinateur était infecté ?

Ensuite, faites écouter ces deux extraits audio de fraude et d'arnaque en testant les bons réflexes des participants à chaque fin d'écoute :

Face à cette situation, faut-il raccrocher ?

Et si on vous demande d'aller sur un site web ?

Faut-il donner l'accès ou non à son ordinateur ?

Fraude bancaire

Visionnez les 3 premières minutes de cette vidéo :

- [Apprenez à vous protéger d'une fraude bancaire - Boursorama](#)

Arnaque assistance

Visionnez l'une de ces vidéos courtes :

- [Enregistrement audio d'une arnaque assistance Microsoft](#)
- [Cybermalveillance.gouv.fr - L'arnaque au faux support technique](#)
- [Arnaques au faux support technique. Et vous ? Vous auriez dit oui ?](#)



ACTIVITÉ 1 : ÉVITEZ LES ARNAQUES AU FAUX SUPPORT...

ACTIVITÉ 1

Fraude bancaire

Arnaque assistance

SLIDE À PROJETER

Résumez le principe des arnaques aux faux support technique :

- Un expert vous appelle. Il affirme travailler pour une entreprise bien connue, et vous dit que votre ordinateur a été infecté par un virus. Selon lui, la seule solution est de lui donner accès à distance à votre ordinateur pour qu'il puisse le réparer directement. Il peut également tenter de vous vendre un soi-disant antivirus. Sous la pression, il peut sembler logique de faire ce qu'il demande, mais attention : il s'agit d'une arnaque !
- Les fraudeurs appellent les personnes de façon aléatoire, en prétendant être des experts légitimes. Ils tentent de vous effrayer pour que vous leur donniez de l'argent ou que vous leur cédez le contrôle de votre ordinateur en téléchargeant un faux logiciel ou en leur donnant vos mots de passe. Il est important de ne pas céder aux requêtes de ces fraudeurs et de les ignorer.
- Cette arnaque prend aussi la forme de messages dans des fenêtres contextuelles qui apparaissent sur votre écran, et qui vous alertent que votre ordinateur a été infecté.
- Même si les appels et les fenêtres contextuelles sont convaincants, en réalité vous risquez de vous faire voler vos codes de cartes bleues et vos identifiants bancaires, de perdre l'accès à votre ordinateur, d'être victime d'un vol d'identité et même de vous faire vider votre compte en banque. Il ne faut pas appeler les numéros qui s'affichent directement dans les messages d'avertissement.

Toujours en prenant exemple sur ces 2 cas d'arnaques, expliquez les premiers réflexes à avoir pour les déjouer :

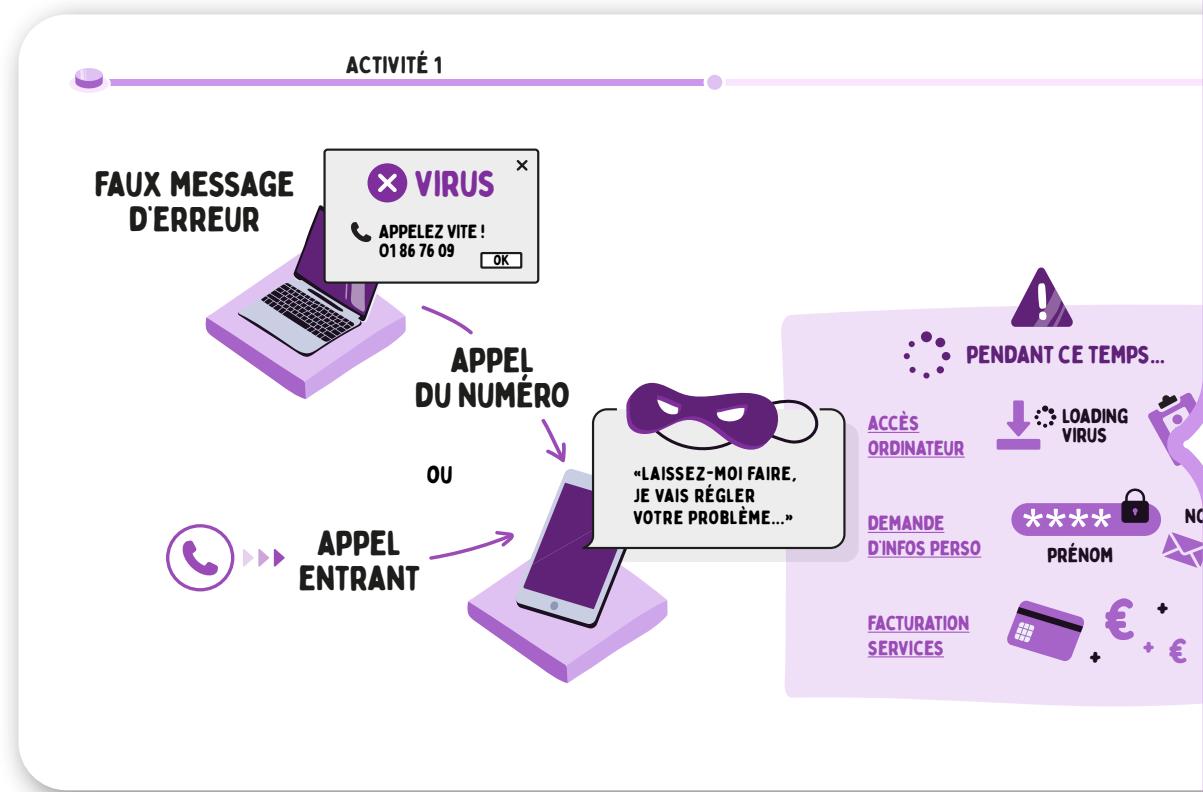
Si quelqu'un vous appelle pour vérifier vos données personnelles à la suite de transactions douteuses, ou parce qu'une transaction doit être annulée après vérification de votre identité, ne parlez pas plus longtemps et raccrochez aussitôt. Cette personne est probablement un fraudeur qui essaye de vous faire valider une transaction financière ou bien une connexion à votre compte.



ACTIVITÉ 1 : ÉVITEZ LES ARNAQUES AU FAUX SUPPORT...

Pour expliquer comment l'arnaque se passe, racontez cette histoire en vous appuyant sur l'infographie :

Au cours de cette attaque, l'escroc vous contacte et tente de vous convaincre qu'il existe un problème sur votre ordinateur et que vous devez le laisser le « résoudre » pour vous.



SLIDE À PROJETER

Les deux moyens les plus courants qu'il utilise pour vous contacter consistent à vous envoyer de faux messages d'erreur sur votre ordinateur ou à vous appeler sur votre téléphone.

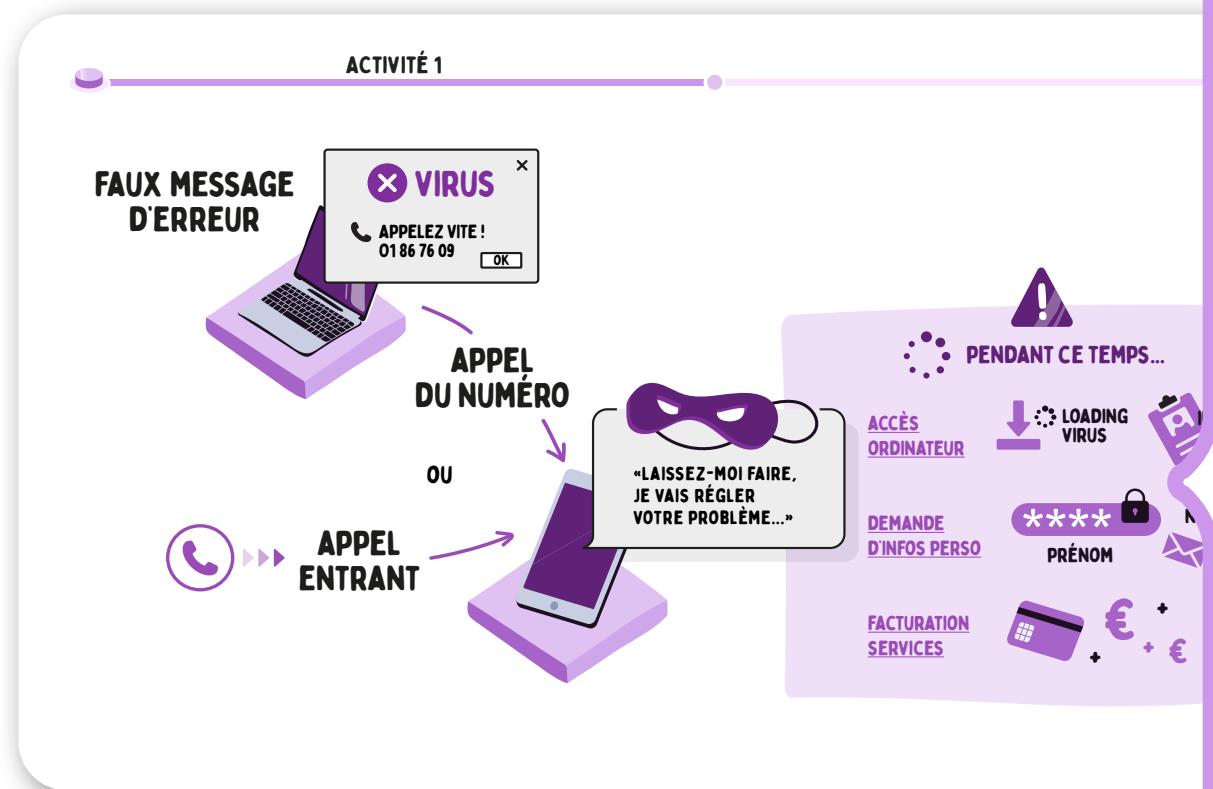
Les faux messages d'erreur sont généralement générés par un site web malveillant ou compromis. Vous utilisez simplement votre navigateur web. Par exemple, vous cliquez sur un lien dans une recherche sur le web ou sur un réseau social, puis votre écran affiche soudain des messages inquiétants vous informant que votre ordinateur rencontre un problème ou un virus et que vous devez immédiatement appeler le numéro de téléphone fourni. Ces fenêtres pop-up peuvent apparaître pour bloquer l'accès à votre ordinateur, de sorte que vous ne pouvez pas les fermer. Des sons ou des voix enregistrées peuvent même accompagner ces fenêtres pop-up pour les rendre encore plus visibles.

Les appels téléphoniques prennent généralement la forme d'un « agent de support technique » qui vous appelle au nom d'une société de confiance telle que Microsoft ou Amazon. Ces escrocs sont des professionnels et sont souvent plutôt convaincants...



ACTIVITÉ 1 : ÉVITEZ LES ARNAQUES AU FAUX SUPPORT...

Peu importe que vous les appeliez à partir d'un message contextuel ou d'un autre message d'erreur, ou qu'ils vous appellent en tant qu'agent du support technique, l'histoire est toujours la même. Ils vous informent qu'ils ont détecté un problème sur votre ordinateur ou votre compte et qu'ils souhaitent que vous les laissiez le résoudre.



SLIDE À PROJETER

Voici quelques éléments qui se produisent généralement à ce stade :

- L'escroc voudra que vous lui permettiez d'accéder à distance à votre ordinateur afin qu'il puisse le «réparer». Lorsqu'il prétendra réparer votre ordinateur, il dérobera vos informations ou installera des programmes malveillants.
- Il peut demander vos informations personnelles afin de vous aider à « corriger » votre compte. Ces informations incluent probablement des éléments tels que votre nom, votre adresse, votre nom d'utilisateur, votre mot de passe, votre numéro de sécurité sociale, votre date de naissance, et tout autre type de données personnelles ou financières qu'il peut vous inciter à révéler.
- Il tentera souvent de vous facturer des frais pour ses services afin de « résoudre » le problème inexistant. Si vous lui avez donné les informations de votre carte de crédit, il est possible qu'il n'ait pas pu l'utiliser et vous demande si vous en avez une autre. Il cherchera à obtenir plusieurs cartes bancaires.
- Il peut vous demander le code de vérification de paiement par carte bancaire que vous avez reçu par SMS.



ACTIVITÉ 1 : ÉVITEZ LES ARNAQUES AU FAUX SUPPORT...

ACTIVITÉ 1

COMMENT RÉAGIR SI ON VOUS APPELLE OU SI UN PSEUDO MESSAGE D'ERREUR S'AFFICHE ?

- 1 RACCROCHEZ
- 2 NE FAITES PAS DE MANIPULATION SUR VOTRE APPAREIL
- 3 NE COMMUNIQUEZ RIEN À DES INCONNUS
- 4 APPElez DIRECTEMENT UN NUMÉRO AUTHENTIQUE
- 5 PROTÉGEZ VOTRE ORDINATEUR
- 6 FAITES LA MISE À JOUR DE VOTRE NAVIGATEUR WEB ET DE VOTRE SYSTÈME D'EXPLOITATION
- 7 ACTIVEZ VOTRE BLOQUEUR DE FENêTRES CONTEXTUELLES
- 8 FERMEZ VOTRE NAVIGATEUR
- 9 RÉINITIALISEZ VOTRE APPAREIL
- 10 PARLEZ-EN AUTOUR DE VOUS

SLIDE À PROJETER

Passez en revue les réactions à avoir si on nous appelle ou si un pseudo message d'erreur s'affiche :

- **Raccrochez** : la plupart des véritables entreprises de logiciels ne vous appelleraient pas pour vous dire que votre ordinateur est compromis. Si l'on vous appelle, c'est faux.
- **Ne faites pas de manipulation sur votre appareil** : raccrochez si l'on vous demande par téléphone de faire des manipulations sur votre ordinateur.
- **Ne communiquez rien à des inconnus** : ne donnez à personne des informations sur vos comptes (tout nom d'utilisateur ou mot de passe) ou des renseignements d'ordinateur (adresse IP). Vous n'avez aucune garantie que la personne au bout du fil vous dit la vérité sur son identité.
- **Appelez directement un numéro authentique** : raccrochez et appelez l'organisme en question en utilisant le numéro obtenu d'une source fiable, à partir du site web de l'organisme ou bien sur des factures ou relevés de compte.
- **Protégez votre ordinateur** : de nombreux produits sont disponibles pour protéger votre ordinateur : antivirus, anti-logiciel espion et pare-feu. Dans certains cas on peut se les procurer comme suite logicielle. Lorsqu'on en fait régulièrement la mise à jour ils peuvent empêcher les programmes malveillants d'accéder à votre ordinateur.



ACTIVITÉ 1 : ÉVITEZ LES ARNAQUES AU FAUX SUPPORT...

ACTIVITÉ 1

COMMENT RÉAGIR SI ON VOUS APPELLE OU SI UN PSEUDO MESSAGE D'ERREUR S'AFFICHE ?

- 1 RACCROCHEZ
- 2 NE FAITES PAS DE MANIPULATION SUR VOTRE APPAREIL
- 3 NE COMMUNIQUEZ RIEN À DES INCONNUX
- 4 APPELEZ DIRECTEMENT UN NUMÉRO AUTHENTIQUE
- 5 PROTÉGEZ VOTRE ORDINATEUR
- 6 FAITES LA MISE À JOUR DE VOTRE NAVIGATEUR WEB ET DE VOTRE SYSTÈME D'EXPLOITATION
- 7 ACTIVEZ VOTRE BLOQUEUR DE FENÊTRES CONTEXTUELLES
- 8 FERMEZ VOTRE NAVIGATEUR
- 9 RÉINITIALISEZ VOTRE APPAREIL
- 10 PARLEZ-EN AUTOUR DE VOUS

SLIDE À PROJETER

- **Faites la mise à jour de votre navigateur web et de votre système d'exploitation :** ils ont tous deux des systèmes de défense intégrés qui sont régulièrement mis à jour pour suivre le rythme d'apparition des derniers virus et d'autres programmes malveillants. En vous assurant de la mise à jour de votre système d'exploitation (par exemple : Windows, OS X ou Ubuntu) et de votre navigateur web (par exemple : Chrome, Firefox, Edge ou Safari), vous mettez toutes les chances de votre côté.
- **Activez votre bloqueur de fenêtres contextuelles :** la plupart des navigateurs web comportent un bloqueur de fenêtres contextuelles intégré qui empêche les fenêtres contextuelles d'apparaître sur votre écran. Cela pourrait vous protéger de fenêtres contextuelles frauduleuses.
- **Fermez votre navigateur :** si votre écran se remplit soudainement de messages effrayants, fermez immédiatement votre navigateur (essayez d'appuyer sur Alt+F4 si vous ne pouvez pas le faire avec la souris). Si vous ne pouvez pas fermer votre navigateur, tentez de redémarrer votre ordinateur.
- **Réinitialisez votre appareil :** si vous avez accordé à des escrocs l'accès à votre ordinateur, vous pouvez tenter de le réinitialiser.
- **Parlez-en autour de vous :** partagez votre expérience pour sensibiliser votre entourage à cette menace. Et si vous avez payé, contactez votre banque et portez plainte.

2 MÉFIEZ-VOUS DES APPARENCES

DURÉE DE L'ACTIVITÉ : 15MIN



ACTIVITÉ 1 : ÉVITEZ LES ARNAQUES AU FAUX SUPPORT...

ACTIVITÉ 1

À RETENIR :

- NE CLIQUEZ PAS SUR LES MESSAGES URGENTS QUI APPARAISSENT PENDANT QUE VOUS NAVIGUÉZ EN LIGNE ET NE COMPOSEZ PAS LE NUMÉRO FOURNI
- RACCROCHEZ SI ON VOUS DEMANDE DE FAIRE DES MANIPULATIONS SUR VOTRE ORDINATEUR
- SIGNALEZ LES ESCROQUERIES, GRÂCE AU DISPOSITIF THESEE ET LE FORMULAIRE DE CHOIX GUIDE DISPONIBLE SUR SERVICE-PUBLIC.FR
- N'INSTALLEZ JAMAIS D'APPLICATION À LA DEMANDE D'UNE PERSONNE QUE VOUS NE CONNAISSEZ PAS
- SI VOUS ÊTES CONFRONTÉ À UNE ARNAQUE, PARLEZ-EN À UN AMI, À UN COLLÈGUE OU À UN MEMBRE DE VOTRE FAMILLE POUR LES SENSIBILISER À CETTE MENACE

SLIDE À PROJETER

Faites le point sur les gestes à retenir pour éviter les arnaques.



ACTIVITÉ 2 : NE LAISSEZ PAS LES CYBERCRIMINELS...

CONTEXTE

Les sujets des arnaques en ligne se renouvellent sans cesse mais leur fonctionnement reste souvent le même : on vous envoie **une fausse information** et on vous demande de **cliquer sur un lien** pour régler **une situation qui n'existe pas**.

Les exemples sont nombreux :

- Vous recevez un SMS ou un mail provenant d'un expéditeur de confiance vous invitant à **cliquer sur un lien pour mettre à jour votre compte, affranchir un colis ou recevoir de l'argent.**

- Quelqu'un vous contacte par téléphone ou par SMS pour vous proposer une **formation grâce à vos droits** et se propose de vous accompagner dans la création de votre compte.
- Un mail vous indique qu'on a **piraté votre webcam, enregistré votre navigation sur des sites pornographiques** et, bien entendu, recueilli la liste de tous vos contacts et mots de passe.

Tout cela est faux !

OBJECTIF DE LA SÉQUENCE : Apprendre à reconnaître les signes d'une escroquerie.

RESSOURCES POUR ALLER PLUS LOIN

[Le fléau du “phishing” en quatre exemples | Youtube](#)

[Phishing : détecter un message malveillant | CNIL](#)

[Que faire en cas de phishing ou hameçonnage ? | Cybermalveillance](#)



ACTIVITÉ 2 : NE LAISSEZ PAS LES CYBERCRIMINELS...



**ACTIVITÉ 2
NE LAISSEZ PAS
LES CYBERCRIMINELS
VOUS VOLER**

SLIDES À PROJETER

Pour commencer, questionnez les participants :

Avez-vous déjà reçu des messages suspects par mail ou SMS ?

Connaissez-vous quelqu'un qui a déjà été victime de phishing ?

Quelles peuvent être les conséquences si l'on clique sur un lien contenu dans un message suspect ?

Qu'est-ce qui peut donner envie de cliquer sur un lien ?

TÉMOIGNAGE DE FRAUDE VIA BLABLACAR

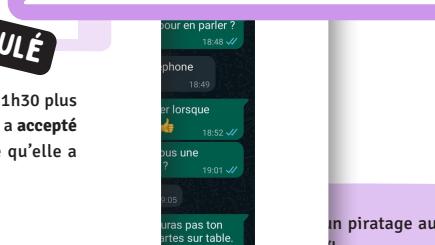
DISPONIBLE EN INTÉGRALITÉ ICI

Ce soir, je pense que j'ai failli être victime d'une grave arnaque sur Blablacar.
J'ai envie de vous raconter ça au cas vous vous retrouveriez dans la même situation...

Après que mon train Paris/Douai a été annulé en raison de la tempête Eunice, je décide de me tourner vers Blablacar. Je vois un trajet pour 9 euros (pas cher), proposé par "Tiphaine". Sur son profil, aucune photo et aucune note. Vous trouvez ça louche ? Vous avez raison.



Naivement, je réserve le trajet, et j'attends confirmation. 1h30 plus tard, je reçois un premier mail qui m'indique que Tiphaine a accepté la réservation, puis un second qui me dit au contraire qu'elle a annulé le voyage, et que je vais être remboursé.



Sur les réseaux sociaux, on nous donne des astuces pratiques, je me suis fait avoir. Stress, fatigue, inattention... Il existe une multitude de facteurs qui peuvent nous pousser à fermer les yeux sur les différentes alertes et à commettre une erreur.

Ensuite, faites découvrir le témoignage de Valentin.



ACTIVITÉ 2 : NE LAISSEZ PAS LES CYBERCRIMINELS...

ACTIVITÉ 2

QUIZ

TO CLICK OR NOT TO CLICK ?

SLIDES À PROJETER

Comment les fraudeurs peuvent-ils s'y prendre pour rendre leur arnaque crédible ? Pour tester les participants, proposez le quiz “To click or not to click”. Pour chaque affirmation, les participants répondent à la question “*Face à ce message, faut-il cliquer ou non ?*” afin de découvrir la bonne réponse.

ACTIVITÉ 2

PHISHING SMISHING

Cliquez sur ce lien !!
<https://www.toutvabien.com>
→ <https://lienbizarre.com>

Débriez l'exercice en expliquant les notions de phishing et smishing :
Le phishing (hameçonnage) est la forme d'arnaque la plus courante sur internet. Le fraudeur se fait passer pour un organisme ou une entreprise connue en utilisant le logo et le nom de cette organisation. Il vous envoie un mail vous demandant de confirmer vos informations à la suite d'un incident technique, comme vos coordonnées bancaires (numéro de compte, codes personnels, etc.) ou bien votre mot de passe.
Le smishing est une forme d'hameçonnage par SMS sur les téléphones portables. Ces messages sont aussi très persuasifs et demandent de suivre un lien.



ACTIVITÉ 2 : NE LAISSEZ PAS LES CYBERCRIMINELS...

ACTIVITÉ 2

PHISHING SMISHING

Cliquez sur ce lien !!
<https://www.toutvabien.com>

https://lienbizarre.com

SLIDE À PROJETER

Continuez en donnant quelques conseils :

- Faites attention aux messages qui demandent de cliquer sur un lien, de confirmer des informations personnelles ou de réinitialiser un mot de passe. Ces messages peuvent être des fausses alertes et il est préférable de ne pas les suivre.
- Si vous survolez un lien avec votre souris (sur un ordinateur), vous verrez où le lien vous redirige. Si l'adresse ne correspond pas à l'adresse du site officiel, il y a de fortes chances pour qu'il s'agisse d'un faux. Souvent, les fraudeurs utilisent des liens raccourcis pour faire croire qu'un lien semble pouvoir être cliqué sans danger. Si vous recevez un lien court, il existe des outils en ligne gratuits de type expander qui vous permettent de copier et de coller le lien, afin de révéler sa véritable destination. Soyez toutefois prudent, si vous ne voulez pas cliquer accidentellement sur le lien court. Si vous craignez de ne pas réussir à correctement copier et coller le lien, supprimez plutôt le mail ou le SMS contenant le lien raccourci et rendez-vous sur le site principal de l'entreprise pour accéder à votre compte ou à l'offre qui vous intéresse.
- Un expéditeur inconnu vous propose de télécharger « gratuitement » des applications habituellement payantes. Cette offre est une tentative pour vous dérober des informations personnelles ou bancaires. Téléchargez vos applications uniquement depuis les stores officiels et les sites des éditeurs sinon vous risqueriez de télécharger un logiciel malveillant susceptible de compromettre vos données.



ACTIVITÉ 2 : NE LAISSEZ PAS LES CYBERCRIMINELS...

ACTIVITÉ 2
VOUS AVEZ
UN DOUTE
SUR LE MESSAGE
QUE VOUS AVEZ
REÇU ?

- N'ayez pas peur ! Vous n'avez sans doute rien de compromettant à vous reprocher
- N'ouvrez pas de liens ou de pièces jointes sans être sûr de la fiabilité de son expéditeur
- Vérifiez l'adresse de l'expéditeur : contactez-le par un autre canal. Un organisme officiel aura presque systématiquement une adresse mail de type "ne-pas-repondre@ministere.gouv.fr"
- Ne répondez à aucun mail suspect ou à du chantage pour ne pas montrer à l'expéditeur que vous êtes réceptif au message
- Changez vos mots de passe, évitez d'avoir le même mot de passe pour chaque compte pour vous prémunir d'attaques en cascade et, si possible, activez la double authentification sur vos comptes les plus sensibles, dont vos comptes de messagerie
- Faites des captures d'écran et signalez le mail sur le site : www.signal-spam.fr
- Si l'escroquerie que vous souhaitez signaler vous est parvenue par SMS, transférez-le au numéro 33700
- Supprimez le message

Passez en revue les bonnes pratiques à avoir face à cette situation. Vous pouvez vous rendre en direct sur le site www.signal-spam.fr pour montrer la plateforme aux participants.

SLIDES À PROJETER

ET SI VOUS AVEZ DIVULGUÉ
VOTRE MOT DE PASSE
OU DES INFORMATIONS
PERSONNELLES ?

- 1 Renouvez immédiatement les mots de passe des comptes compromis
- 2 Signalez les escroqueries, grâce au dispositif THESEE et le formulaire de choix guidé disponible sur service-public.fr
- 3 Rendez-vous sur cybermalveillance.gouv.fr, la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance pour obtenir plus de conseils

ET SI VOUS AVEZ PAYÉ
ET ÊTES VICTIME
D'UNE ESCROQUERIE ?

- 1 Changez immédiatement les mots de passe des comptes compromis
- 2 Adressez-vous à votre banque pour tenter de faire annuler le paiement
- 3 Portez plainte en ligne, grâce au dispositif THESEE et le formulaire de choix guidé disponible sur service-public.fr

Vous pouvez vous rendre en direct sur cybermalveillance.gouv.fr pour montrer la plateforme aux participants.

Rappelez les premiers réflexes à avoir :

Si vous recevez un mail ou SMS qui semble provenir d'un site connu comme votre banque, le service des impôts, votre fournisseur d'énergie, etc., faites preuve de vigilance avant de cliquer sur le lien. Il est préférable de se connecter directement soi-même sur le site sur lequel on possède un compte.

Au moindre doute, stoppez votre navigation, ne téléchargez rien, et appelez directement votre correspondant pour vérifier l'origine du message !



ACTIVITÉ 2 : NE LAISSEZ PAS LES CYBERCRIMINELS...

ACTIVITÉ 2

COMMENT REPÉRER UNE ARNAQUE REÇUE PAR MAIL OU

SLIDES À PROJETER

COMMENT REPÉRER UNE ARNAQUE REÇUE PAR M



Il est essentiel de redoubler de vigilance face aux cyber-arnaques et tentatives de vol de vos données personnelles ou bancaires. Voici quelques conseils pour mieux repérer et éviter les pièges.

Continuez en expliquant aux participants que les arnaques en ligne peuvent être difficiles à repérer : même les professionnels de la cybersécurité peuvent se faire avoir ! Cependant, il existe quelques signes qui permettent de les identifier. Commentez les 5 conseils :

Attention aux expéditeurs inconnus : soyez particulièrement vigilants si le message provient d'une adresse électronique ou d'un numéro de téléphone que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact. Posez-vous la question de qui est l'expéditeur.

Soyez attentif à l'écriture : même si cela s'avère de moins en moins vrai, certains messages malveillants ne sont pas correctement écrits. Si le message comporte des fautes de frappe, d'orthographe ou des tournures de phrases inappropriées, c'est qu'il n'est pas authentique et ne provient pas d'un organisme crédible (administration, grande marque ...).

L'adresse de messagerie de l'émetteur n'est pas un critère fiable : si le message semble provenir d'un ami, contactez-le sur un autre canal pour vous assurer qu'il s'agit bien de lui. L'appareil et la boîte mail de vos contacts peuvent être piratés et utilisés pour vous envoyer des messages de phishing par SMS ou mail.

Vérifiez les liens : avant de cliquer sur les liens, laissez votre souris dessus. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime. Cette manipulation est plus délicate à effectuer depuis un écran de smartphone, car il faut laisser appuyer son doigt sur le lien.

Méfiez-vous des demandes étranges, urgentes et trop belles pour être vraies : posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n'a le droit de vous demander votre code de carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.



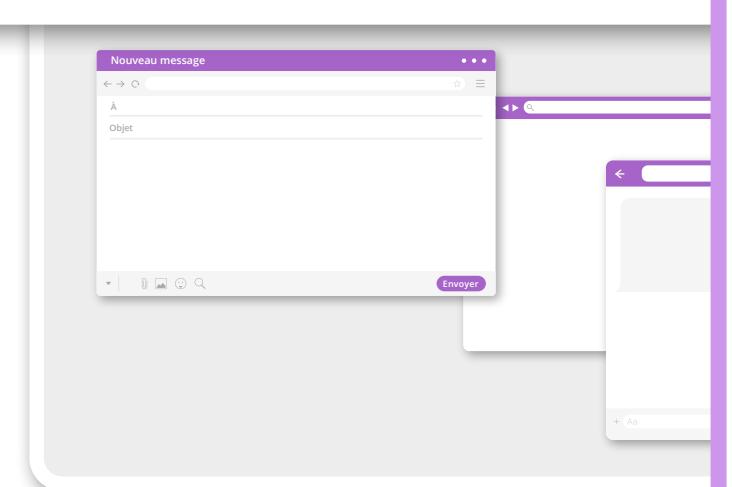
ACTIVITÉ 2 : NE LAISSEZ PAS LES CYBERCRIMINELS...

ACTIVITÉ 2

JEU DE RÔLE

CRÉEZ VOTRE PROPRE ARNAQUE

SLIDES À PROJETER



Testez les connaissances de vos participants en leur proposant un jeu de rôle “Créez votre propre arnaque” (d’après « [L’école des réseaux sociaux](#) »). Imprimez ou demandez de recopier les modèles présents sur les slides suivantes.

Demandez aux participants, séparément ou en binômes, de créer leur propre exemple d’arnaque en ligne. Ils pourront se mettre à la place d’un fraudeur et réfléchir aux attaques d’ingénierie sociale.

Invitez les participants à réfléchir aux questions suivantes lorsqu’ils créent leur arnaque fictive :

- **Quel est votre objectif ?** (Que voulez-vous obtenir de votre ou de vos victimes ?)
- **Comment ferez-vous pour que votre arnaque soit réaliste ?** (Si l’arnaque est trop bizarre ou évidente, les gens ne tomberont pas dans le piège)
- **Comment utiliserez-vous la technologie pour réaliser votre arnaque ?** Par exemple, les URL courtes comme bit.ly et les QR codes peuvent empêcher de repérer une fausse adresse de site web. Les faux likes/abonnés/avis peuvent aussi sembler authentiques ou populaires alors qu’ils ne le sont pas, etc.



ACTIVITÉ 2 : NE LAISSEZ PAS LES CYBERCRIMINELS...

ACTIVITÉ 2

JEU DE RÔLE

CRÉEZ VOTRE PROPRE ARNAQUE

SLIDES À PROJETER

Nouveau message
Objet:

Guidez les participants en indiquant que d'une manière générale les méthodes d'ingénierie sociale se déroulent selon le schéma suivant :

- Une **phase d'approche** permettant de mettre l'interlocuteur en confiance.
- Une **mise en alerte**, afin de le déstabiliser et de s'assurer de la rapidité de sa réaction (« il y a un problème sur un contrat, une facture, etc. »).
- Une **diversion**, c'est-à-dire une phrase ou une situation permettant de rassurer l'utilisateur et d'éviter qu'il se focalise sur l'alerte. Par exemple, un remerciement et un message rassurant indiquant que tout sera rétabli si la personne coopère rapidement.

Demandez à un participant ou à un groupe volontaire de partager son arnaque : les autres personnes peuvent-elles repérer les signes qu'il s'agit d'une arnaque ?



ACTIVITÉ 2 : NE LAISSEZ PAS LES CYBERCRIMINELS...

ACTIVITÉ 2

L'ESCROQUERIE EST UNE INFRACTION
INSCRITE AU CODE PÉNAL (ARTICLE 313-1) PUNIE DE :

5 ANS D'EMPRISONNEMENT
375 000€ D'AMENDE

L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

Rappelez que l'escroquerie est une infraction inscrite au code pénal (Article 313-1) punie de 5 ans d'emprisonnement et 375 000€ d'amende.

SLIDES À PROJETER

ACTIVITÉ 2

À RETENIR :

- EXAMINEZ AVEC PRUDENCE LES MESSAGES COMPORANT DES VISUELS À PRIORI OFFICIELS MAIS DONT LA QUALITÉ D'AFFICHAGE EST MAUVAISE OU COMPORTANT DES FAUTES D'ORTHOGRAPHE
- MÉFIEZ-VOUS DES MESSAGES EXIGEANT DE VOUS UNE RÉPONSE OU UNE ACTION IMMÉDIATE
- NE CLIQUEZ JAMAIS SUR UN LIEN OU UNE PIÈCE JOINTE DONT L'ORIGINE OU LA NATURE VOUS SEMBLENTE DOUTEUSES
- RAPPELEZ-VOUS QUE SI CELA SEMBLE TROP BEAU POUR ÊTRE VRAI, C'EST PROBABLEMENT LE CAS !
- SI VOUS N'AVEZ PAS PARTICIPÉ À UN CONCOURS, VOUS NE POUVEZ PAS GAGNER DE PRIX !
- AU MOINDRE DOUTE, PRIVILEGIEZ L'ACCÈS AU SITE WEB EN TAPANT DIRECTEMENT L'ADRESSE DANS LA BARRE DE RECHERCHE
- AVANT D'INSTALLER UNE APPLICATION, DEMANDEZ-VOUS SI VOUS EN AVEZ VRAIMENT BESOIN

Faites le point sur les réflexes à retenir pour éviter les arnaques.

Nouveau message

• • •



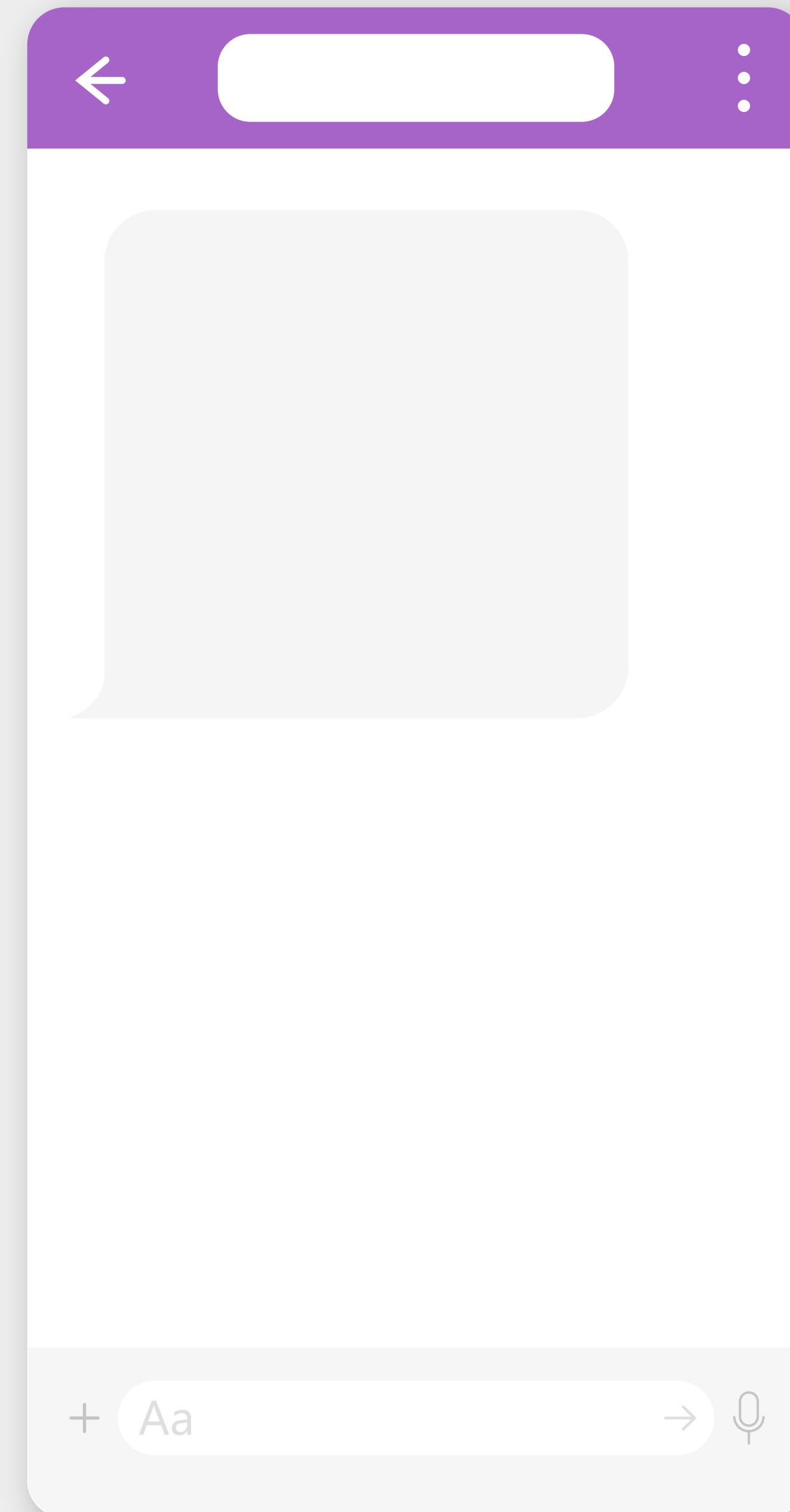
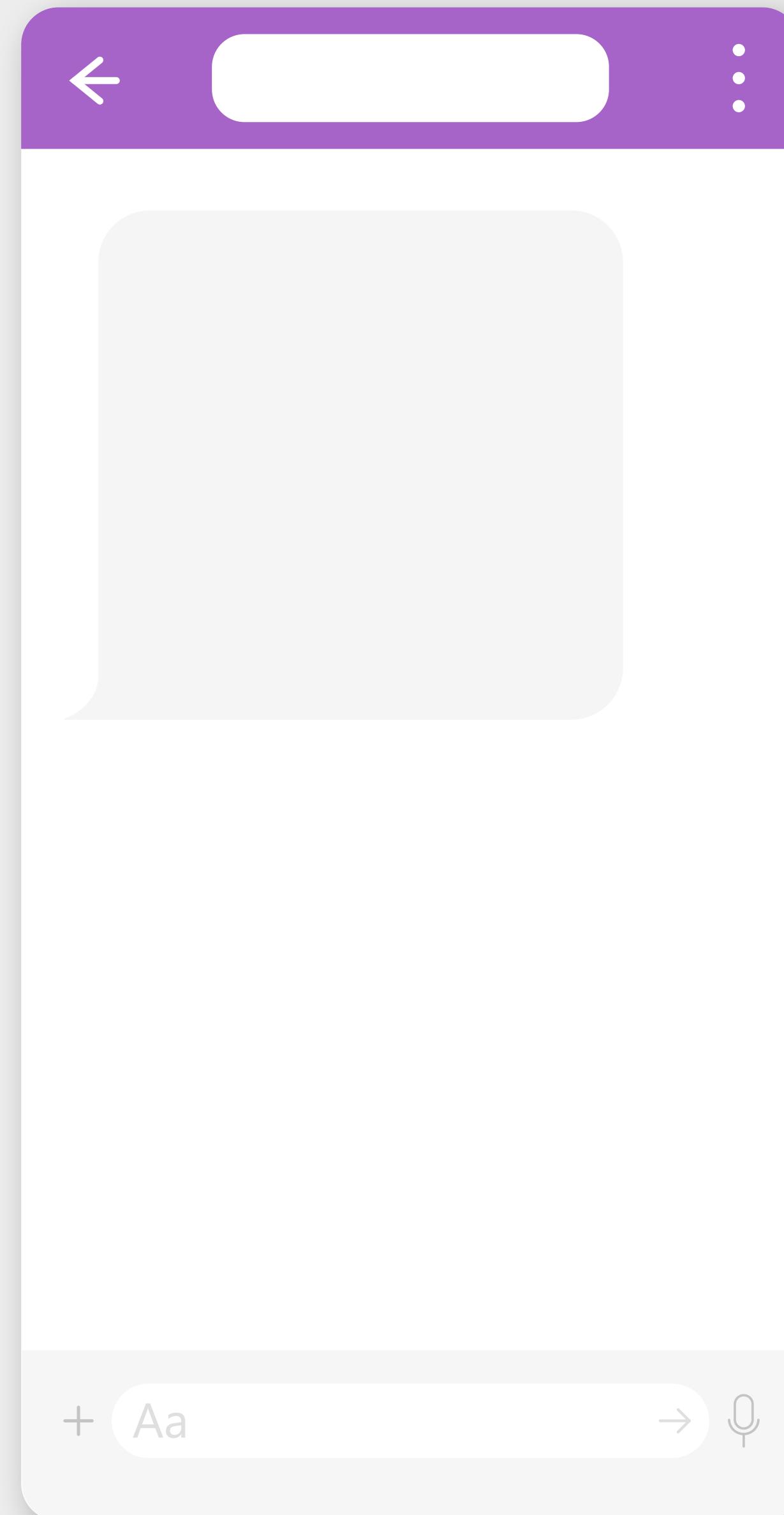
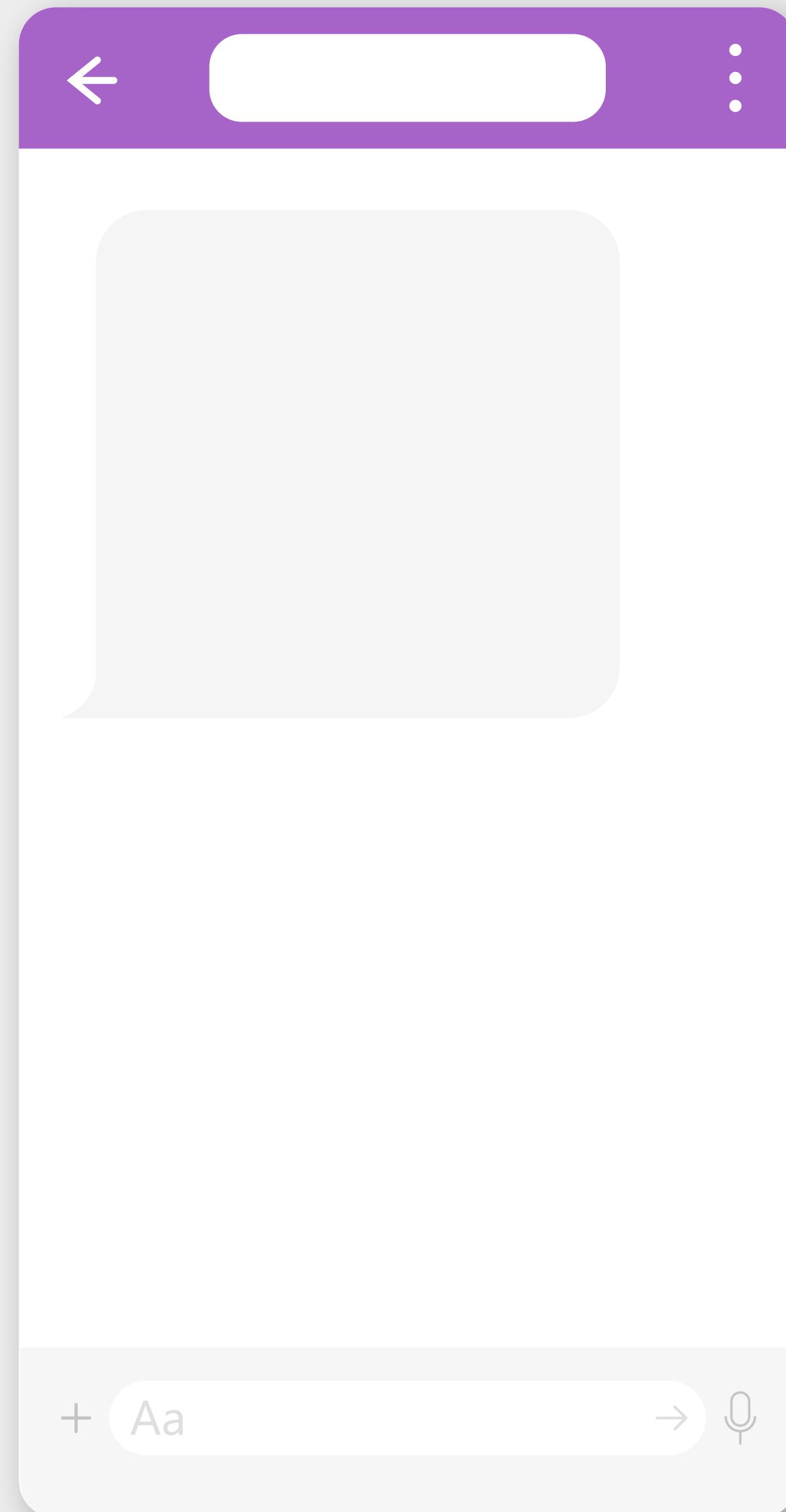
À

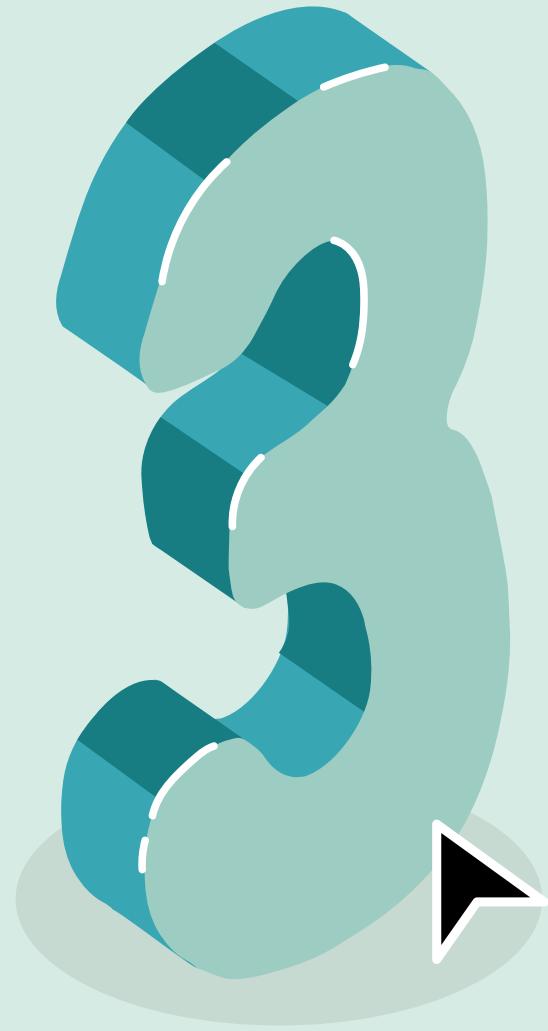
Objet



Envoyer





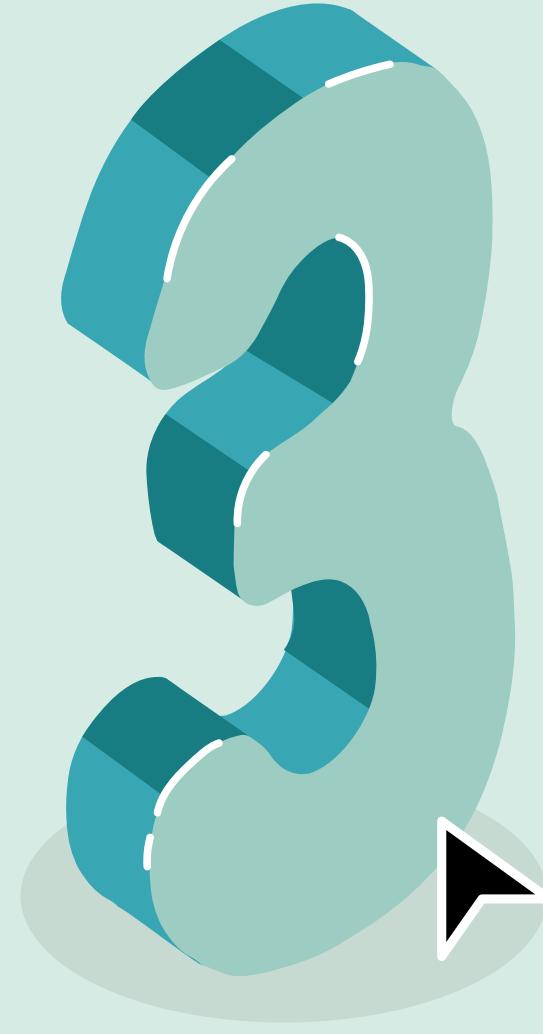


PROTÉGEZ VOS COMPTES EN LIGNE



CONTEXTE

Comme la plupart des gens, vous utilisez certainement **le même mot de passe pour plusieurs comptes en ligne**. C'est une erreur : les pirates informatiques peuvent facilement obtenir un accès à vos comptes en ligne si votre mot de passe de messagerie est compromis. Il est donc important de savoir comment **gérer vos mots de passe et de protéger vos comptes en ligne**.



PROTÉGEZ VOS COMPTES EN LIGNE

OBJECTIF DE LA SÉQUENCE

Cette séquence encourage les participants à **reprendre le contrôle de leurs mots de passe** afin de mieux protéger leurs comptes en ligne à travers une stratégie reposant sur : **le choix d'un mot de passe unique pour chaque compte, la double authentification pour les comptes sensibles, l'utilisation d'un gestionnaire de mots de passe et la création d'un mot de passe fort et facile à mémoriser.**

À la fin de cette séquence, les participants seront en mesure de :

- **Comprendre les techniques** pour créer des mots de passe uniques et sécurisés (phrases de passe, les mots aléatoires, gestionnaire de mots de passe).
- Identifier l'intérêt de la **double authentification** pour les comptes les plus sensibles, dont le compte de messagerie.



LES ACTIVITÉS

ACTIVITÉ 1 : UN BON MOT DE PASSE, C'EST VOTRE MEILLEURE LIGNE DE DÉFENSE

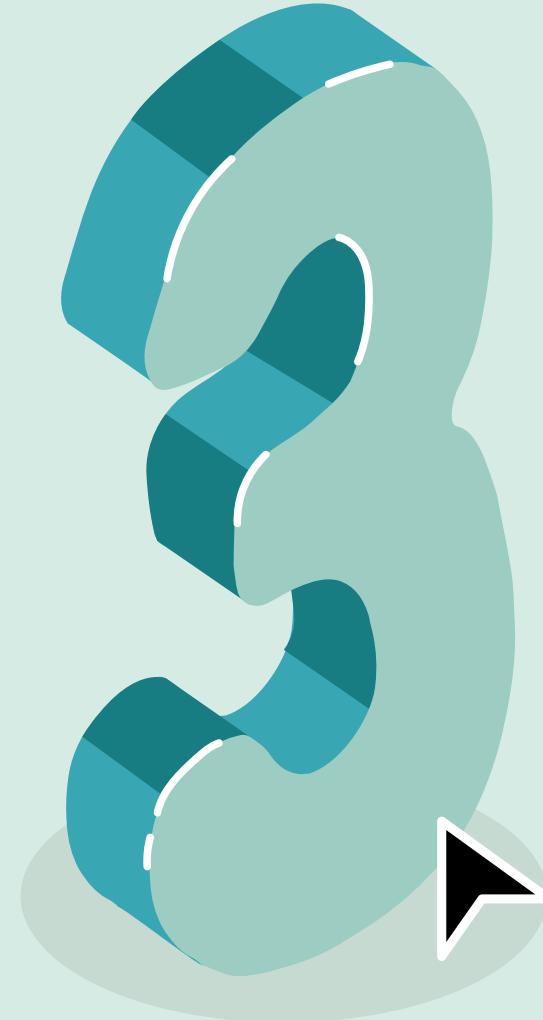
Faire connaître les menaces qui pèsent sur les mots de passe et la nécessité d'avoir un mot de passe unique et fort par site web, par application, par messagerie, par réseau social.

Apprendre à gérer ses mots de passe.



ACTIVITÉ 2 : PROTÉGEZ VOS COMPTES EN LIGNE LES PLUS IMPORTANTS

Faire découvrir la double authentification pour les comptes en ligne notamment pour les comptes de messagerie.



PROTÉGEZ VOS COMPTES EN LIGNE



SLIDE À PROJETER

Avant de commencer, demandez aux participants ce qu'ils savent sur les mots de passe :

Pourquoi les mots de passe sont importants ?

Comment font-ils pour les mémoriser ?

Arrivent-ils à avoir un mot de passe différent pour chaque appareil et chaque compte en ligne ?

Combien de comptes en ligne ont-ils ?

Est-ce une bonne idée d'utiliser un carnet pour noter ses mots de passe ?

Faut-il laisser le navigateur sauvegarder ses mots de passe ?

Comment aider un proche qui ne sait pas gérer ses mots de passe ?

**PASSONS MAINTENANT
AUX ACTIVITÉS**



3 PROTÉGEZ VOS COMPTES EN LIGNE

DURÉE DE L'ACTIVITÉ : 15MIN



ACTIVITÉ 1 : UN BON MOT DE PASSE, C'EST VOTRE...

CONTEXTE

La sécurité des services en ligne tels que les comptes de messageries, les réseaux sociaux, les banques, les sites de vente en ligne dépend principalement des **mots de passe**. Il est facile de succomber à la tentation de choisir des mots de passe trop simples mais ceci augmente le **risque de se faire pirater**.

OBJECTIF DE LA SÉQUENCE

- Faire connaître les menaces qui pèsent sur les mots de passe et la nécessité d'avoir un mot de passe unique et fort par site web/application/messagerie/réseau social.
- Apprendre à gérer ses mots de passe.

RESSOURCES POUR ALLER PLUS LOIN

[Les conseils de la CNIL pour un bon mot de passe | CNIL](#)

[Sécurité : utilisez l'authentification multifacteur pour vos comptes en ligne | CNIL](#)

[Pourquoi et comment bien gérer ses mots de passe ? - Cybermalveillance](#)

[Recommandations relatives à l'authentification multifacteur et aux mots de passe | ANSSI](#)

3 PROTÉGEZ VOS COMPTES EN LIGNE

DURÉE DE L'ACTIVITÉ : 15MIN



ACTIVITÉ 1 : UN BON MOT DE PASSE, C'EST VOTRE...

Pour commencer, questionnez les participants :

Pourquoi est-il important de choisir un bon mot de passe ?

**ACTIVITÉ 1
UN BON MOT DE PASSE,
C'EST VOTRE MEILLEURE
LIGNE DE DÉFENSE**

SLIDES À PROJETER



CHOISIR UN MOT DE PASSE
DIFFÉRENT
POUR CHAQUE COMPTE

QUELS RISQUES COURT-ON
À UTILISER LE MÊME MOT D'
PASSE PARTOUT ?

UN PIRATE POURRAIT :

- ◆ Usurper votre identité
- ◆ Pirater vos données bancaires et réaliser des frauduleux
- ◆ Piéger vos contacts en piratant vos boîtes m / réseaux sociaux
- ◆ Vous faire chanter et demander une rançon (en cas de données compromettantes)

Réutiliser le même mot de passe pour tous ses comptes en ligne, cela n'est pas du tout une bonne pratique. En variant les mots de passe et en utilisant un mot de passe fort et unique par compte, on diminue d'autant le risque de piratages en cascade.

L'une des mesures les plus efficaces en matière de cybersécurité est donc d'avoir un mot de passe différent pour chacun de vos comptes et appareils mais il n'est alors pas évident de se rappeler de chacun d'eux. L'une des solutions est d'utiliser un gestionnaire de mots de passe : il suffit alors de se rappeler d'un seul mot de passe robuste.

Ensuite, passez en revue les risques à utiliser un mot de passe unique en précisant :

Le principal risque d'utiliser un seul mot de passe pour tous ses comptes est de se faire pirater l'intégralité de ses données personnelles. Car si un pirate réussit à connaître vos moyens d'authentification sur un site, il peut ensuite les utiliser sur tous vos comptes.

3 PROTÉGEZ VOS COMPTES EN LIGNE

DURÉE DE L'ACTIVITÉ : 15MIN



ACTIVITÉ 1 : UN BON MOT DE PASSE, C'EST VOTRE...

ACTIVITÉ 1

CRÉER UN MOT DE PASSE ROBUSTE

SLIDES À PROJETER

Pour commencer, questionnez les participants :

Quelles sont les caractéristiques d'un mot de passe fort ?

Un mot de passe différent pour chaque site c'est déjà bien mais pas suffisant ! Encore faut-il que les mots de passe soient suffisamment difficiles à deviner pour décourager certains fraudeurs.

MOT DE PASSE ROBUSTE



COMPLET

contient au moins
14 caractères et 4 types
différents : des minuscules,
des majuscules, des chiffres
et des caractères spéciaux
(!, ?, €, #...)

(!, ?, €, #...)

(!, ?, €, #...)

Passez en revue les 3 critères pour un mot de passe robuste en les commentant :

Un bon mot de passe est robuste s'il répond à trois critères :

Complet : contient au moins 14 caractères et 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux (signes de ponctuation ou caractères spéciaux (!, ?, €, #...)).

Ne dit rien sur vous : personne ne doit deviner votre mot de passe à partir de votre date d'anniversaire, de votre surnom ou bien de votre film préféré. Idem pour le code de votre smartphone : préférez un nombre aléatoire à une année.

Unique : chacun de vos comptes en ligne (messagerie, réseau social, etc.) doit disposer de son propre mot de passe et il ne faut surtout pas réutiliser ce mot de passe pour un autre compte.

3 PROTÉGEZ VOS COMPTES EN LIGNE

DURÉE DE L'ACTIVITÉ : 15MIN



ACTIVITÉ 1 : UN BON MOT DE PASSE, C'EST VOTRE...

ACTIVITÉ 1

2 ASTUCES :

Je ne suis pas 1 hacker & pourtant je travaille dans la cybersécurité !

Jnsp1h&pjtdlc! 🔒

PHRASE DE PASSE (PASSPHRASE)

PorteChantCygneLoupe 🔒

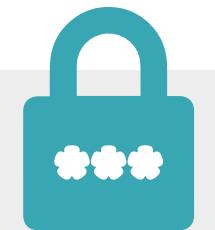
MOTS COMBINÉS

SLIDE À PROJETER

Pas simple de créer un mot de passe robuste et facile à mémoriser. Il existe pourtant la technique de la phrase de passe (passphrase en anglais) ou bien des mots combinés.

Mémorisez une phrase puis utilisez la première lettre de chaque mot pour créer votre mot de passe. La phrase doit contenir des chiffres et des caractères spéciaux ! La CNIL met à disposition un générateur qui permet de concevoir votre mot de passe en quelques secondes ! Exemple : « Je ne suis pas 1 hacker et pourtant je travaille dans la cybersécurité ! » peut devenir : Jnsp1h&pjtdlc!

Une autre technique pour créer un mot de passe fort est de combiner des ensembles aléatoires de quatre mots. Par exemple, « PorteChantCygneLoupe » est un mot de passe très compliqué à deviner, mais facile à mémoriser. Les mots de passe les plus forts sont des ensembles aléatoires de trois ou quatre mots. Quand vous choisissez des mots de différentes longueurs et que vous les placez dans un ordre précis, il est plus difficile de pirater votre mot de passe : le pirate n'a aucune idée de la longueur du mot de passe ou des types de mots/caractères qu'il contient.



ACTIVITÉ 1 : UN BON MOT DE PASSE, C'EST VOTRE...

ACTIVITÉ 1

UTILISER UN GESTIONNAIRE DE MOTS DE PASSE

PASSWORDSAFE ZENWAY KEEPASS

SLIDE À PROJETER

Expliquez qu'une autre solution est d'utiliser un générateur de mot de passe dont le principal avantage est de créer des mots de passe aléatoires donc difficiles à deviner :

Il est parfois difficile de se souvenir des nombreux mots de passe, surtout s'ils sont robustes et générés aléatoirement. C'est pourquoi les gestionnaires de mots de passe ont été créés ! C'est une solution pratique qui permet d'enregistrer en toute sérénité TOUS les comptes et mots de passe.

Avec un gestionnaire de mots de passe, on peut enregistrer tous les identifiants et mots de passe dans une base de données sécurisée et chiffrée par un mot de passe « principal » dont la sécurité a été vérifiée. Cela permet de n'avoir qu'un seul mot de passe pour accéder à tous les autres. Les mots de passe pourront être très longs, très complexes et tous différents car c'est l'ordinateur qui les génère et les retient à votre place. Ces logiciels facilitent par ailleurs la saisie, sans erreur, des mots de passe et permettent de retenir les nombreux identifiants et comptes que l'on accumule avec le temps.

En pratique, il existe de nombreuses solutions sur le marché. On peut citer, entre autres, parmi les logiciels libres [KeePass](#) (dont la sécurité a été évaluée par l'ANSSI), [Zenyway](#) ou [Passwordsafe](#).

3 PROTÉGEZ VOS COMPTES EN LIGNE

DURÉE DE L'ACTIVITÉ : 15MIN



ACTIVITÉ 1 : UN BON MOT DE PASSE, C'EST VOTRE...

ACTIVITÉ 1

VOTRE MOT DE PASSE EST-IL COMPROMIS ?

';-have i been pwned?

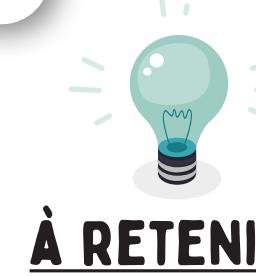
Check if your email or phone is in a data breach

email or phone (international format) pwned?

Enfin, faites découvrir le site pour vérifier si un mot de passe a été compromis :

haveibeenpwned.com est un site qui recense les mots de passe compromis à l'occasion de fuites de données massives. L'utilisateur n'a qu'à entrer son adresse mail ou son numéro de téléphone (utilisé très souvent comme identifiant) pour savoir s'il figure dans une base de données piratée et si ses mots de passe ont été volés.

SLIDES À PROJETER



À RETENIR :

SÉCURISEZ LES COMPTES ET LES APPAREILS AVEC DES MOTS DE PASSE ROBUSTES OU DES PHRASES DE PASSE

ASSUREZ-VOUS QUE LES MOTS DE PASSE OU PHRASES DE PASSE SONT UNIQUES POUR CHAQUE COMPTE ET CHAQUE APPAREIL

Faites le point sur les gestes à retenir pour un bon usage des mots de passe.



ACTIVITÉ 2 : PROTÉGEZ VOS COMPTES EN LIGNE...

CONTEXTE

Utiliser le même mot de passe pour tous vos comptes est une **pratique risquée**. Si vous êtes victime de **phishing** ou bien si un site web tiers est victime d'une **fuite de données** comprenant votre mot de passe, un fraudeur pourrait les utiliser pour, non seulement accéder à ce site web, mais aussi pour accéder au contenu de votre messagerie. Il est déconseillé d'utiliser son compte de messagerie pour stocker des données sensibles. En particulier, évitez d'y stocker des justificatifs d'identité comme un scan de votre passeport, votre carte d'identité ou bien vos mots de passe dans un brouillon.

Il est préférable d'utiliser un **dossier protégé**, de type coffre-fort personnel, pour stocker des fichiers chiffrés et les rendre accessibles seulement après une double authentification.

Si vous ne sécurisez pas dès maintenant votre compte de messagerie, cette situation pourrait vous exposer à d'autres dangers. En effet, une personne mal intentionnée pourrait utiliser la fonction d'oubli de mots de passe pour prendre le contrôle de vos autres comptes en ligne. Faites attention aux comptes mails que vous utilisez peu ; ils pourraient facilement être détournés sans que vous vous en rendiez compte.

OBJECTIF DE LA SÉQUENCE

Faire découvrir la double authentification pour les comptes en ligne notamment pour les boîtes mails.

RESSOURCE POUR ALLER PLUS LOIN

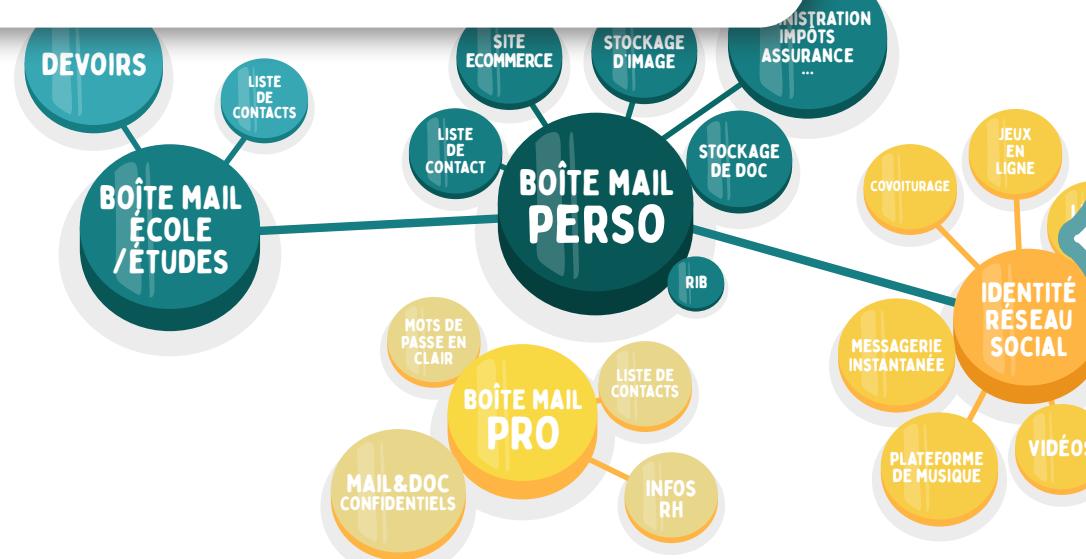
[Jean-Jacques Latour, Cybermalveillance.gouv.fr, explique le danger des piratages des boites mails](#)



ACTIVITÉ 2 : PROTÉGEZ VOS COMPTES EN LIGNE...

ACTIVITÉ 2 PROTÉGEZ VOS COMPTES EN LIGNE LES PLUS IMPORTANTS

SLIDES À PROJETER



(D'après l'infographie CNIL « [Pourquoi sécuriser au maximum le mot de passe de votre boîte mail ?](#) »)

Pour commencer, questionnez les participants :

Avez-vous déjà utilisé la double authentification ?

Quelle différence entre la double authentification et l'authentification sans mot de passe ?

De nos jours, la plupart des services en ligne demandent une adresse mail pour s'inscrire. La sécurité de ces services dépend de la sécurité de votre compte de messagerie. Cela signifie que si quelqu'un accède à votre compte de messagerie, il pourra facilement accéder à tous les autres services liés en faisant une demande de réinitialisation de mot de passe à travers le lien contenu dans le mail reçu dans votre boîte de réception. Il faut donc s'assurer que ses comptes de messagerie soient bien sécurisés, en activant toutes les options de sécurité disponibles comme la double authentification et l'authentification sans mot de passe. Cette considération s'applique également aux comptes de réseaux sociaux de plus en plus connectés aux applications.

Un fraudeur qui accéderait à votre compte de messagerie pourrait effectuer les actions suivantes :

- **Usurpation d'identité** grâce aux données retrouvées dans votre boîte mail (copie de passeport, photo de carte bleue, justificatif de domicile...).
- **Détournement de comptes en ligne** grâce aux fonctions de réinitialisation de mot de passe.
- **Demande de rançon** à la suite de données compromettantes retrouvées dans votre boîte mail.
- **Ajout d'une redirection de mail** (souvent non vérifiée après la compromission d'une boîte mail) : vos mails continuent de fuiter malgré tout changement de mot de passe ultérieur...

3 PROTÉGEZ VOS COMPTES EN LIGNE

DURÉE DE L'ACTIVITÉ : 15MIN



ACTIVITÉ 2 : PROTÉGEZ VOS COMPTES EN LIGNE...

ACTIVITÉ 2

COMMENT FONCTIONNE LA DOUBLE AUTHENTIFICATION

CONNEXION DÉPUIS UN NOUVEL APPAREIL

SMS

VOTRE CODE 64370

APP

CLÉ DE SÉCURITÉ

QUELQUES SERVICES PROPOSANT LA DOUBLE AUTHENTIFICATION

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

SI VOUS UTILISEZ L'UN DE CES SERVICES, ACTIVEZ LA DOUBLE AUTHENTIFICATION !

SLIDE À PROJETER

Grâce à l'infographie, expliquez l'authentification à deux facteurs et encouragez vos interlocuteurs à l'activer sur leurs comptes dans la mesure du possible :

La double authentification également appelée "authentification/vérification en deux étapes", est un moyen efficace de préserver la sécurité d'un compte en ligne.

De plus en plus de services en ligne proposent cette option. En plus de votre nom de compte et de votre mot de passe, ces services vous demandent une confirmation que vous pouvez recevoir, par exemple, sous forme de code provisoire reçu par SMS, par courrier électronique (mail), via une application ou bien une clé de sécurité FIDO2 que vous gardez avec vous.



ACTIVITÉ 2 : PROTÉGEZ VOS COMPTES EN LIGNE...

ACTIVITÉ 2

COMMENT FONCTIONNE LA DOUBLE AUTHENTIFICATION ?

SLIDE À PROJETER

Des applications comme [Microsoft Authenticator](#) ou encore [Google Authenticator](#) vous permettent de simplifier l'utilisation de la double authentification pour vos comptes en acceptant ou non une notification s'affichant sur votre téléphone.

Si vous vous connectez à votre compte depuis un nouvel appareil ou depuis un nouvel emplacement géographique, vous recevrez une notification. Vous pouvez choisir d'autoriser ou de refuser l'accès ! Cette fonction informe aussi l'utilisateur des tentatives d'accès à son compte par d'autres personnes.

Si vous recevez un code d'authentification que vous n'avez pas demandé (par exemple, si vous ne venez pas de tenter de vous connecter à votre compte), quelqu'un d'autre connaît sans doute votre mot de passe et tente d'accéder à votre compte. Il est conseillé de se connecter à ce compte dès que possible et de modifier le mot de passe. Si ce mot de passe est utilisé sur d'autres comptes, vous devez le changer sur ces comptes également.

Vous pouvez faire une démonstration sur comment activer la double authentification sur Instagram, Facebook, Gmail, Outlook, Snapchat ou TikTok :

[Authentification à deux facteurs sur Instagram](#)

[Authentification à deux facteurs sur Facebook](#)

[Authentification en deux étapes sur compte Google](#)

[Authentification en deux étapes sur compte Microsoft](#)

[Authentification à deux facteurs sur Snapchat](#)

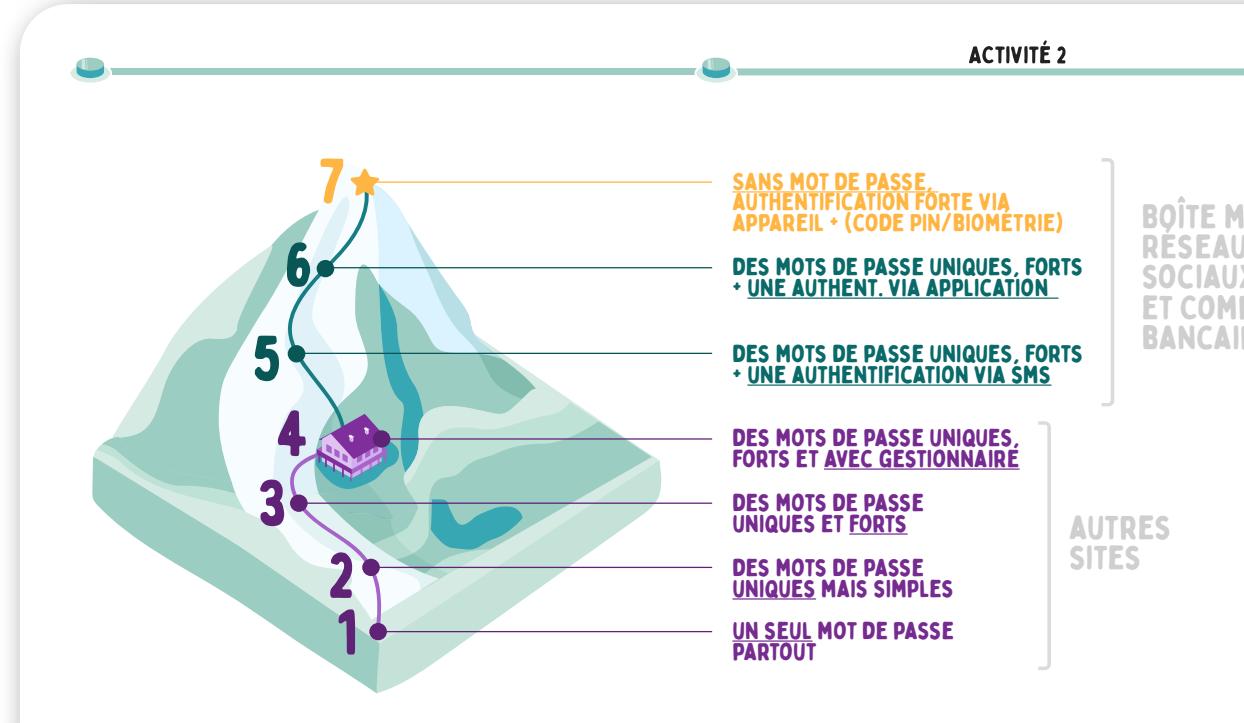
[Authentification en deux étapes sur TikTok](#)

3 PROTÉGEZ VOS COMPTES EN LIGNE

DURÉE DE L'ACTIVITÉ : 15MIN



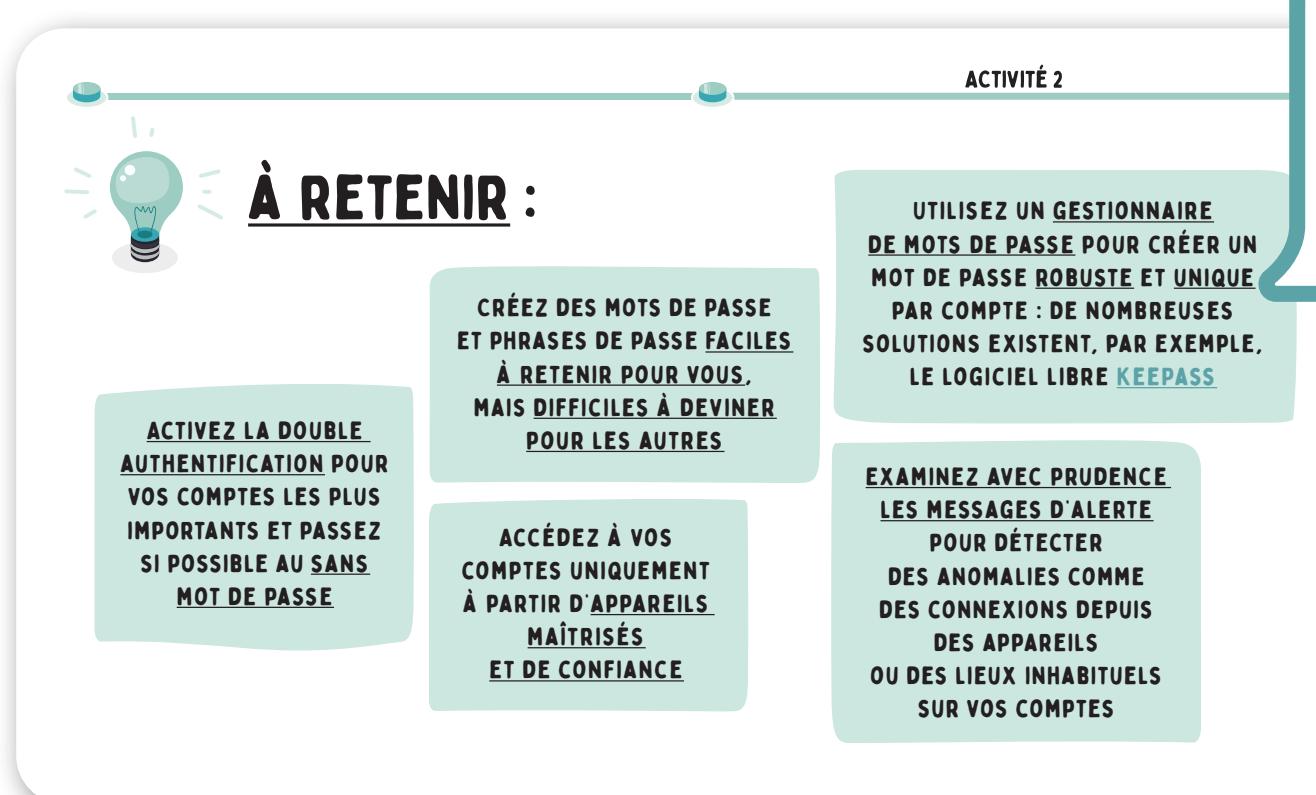
ACTIVITÉ 2 : PROTÉGEZ VOS COMPTES EN LIGNE...



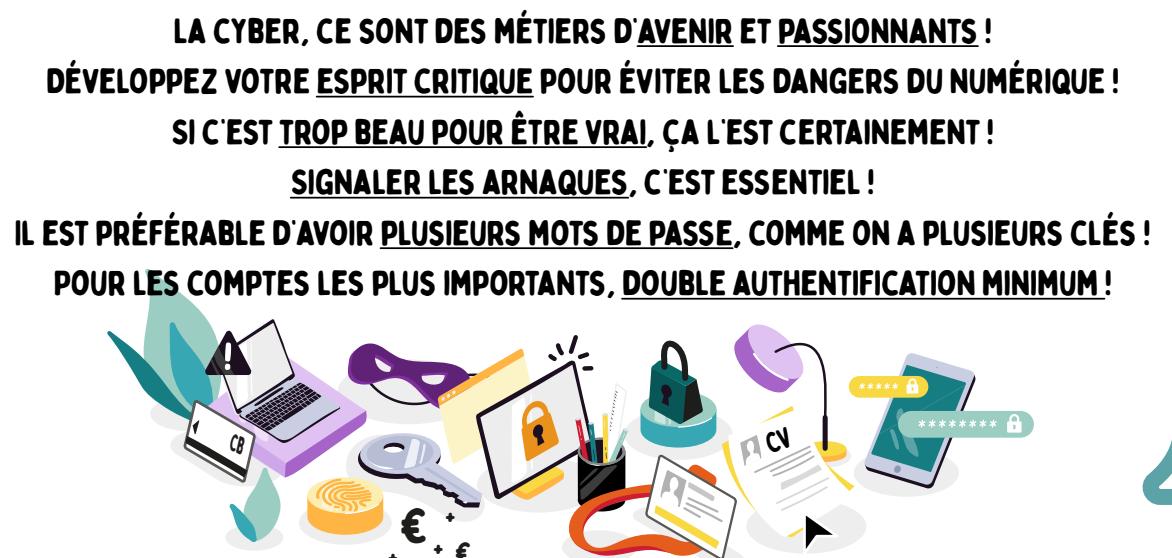
Il est temps de faire le ménage de printemps de vos identités numériques ! Cela signifie faire un tri dans vos comptes en ligne et vous assurer que vous avez un gestionnaire de mot de passe pour gérer des mots de passe forts et uniques : il s'agit ici de l'étape 4 !

Un futur sans mot de passe à l'aide d'un mécanisme d'authentification forte est possible, mais il y a encore quelques étapes à franchir avant d'y parvenir. En attendant, la double authentification est une mesure de sécurité que vous devriez configurer sur vos comptes en ligne les plus importants : il s'agit des étapes 5 et 6.

SLIDES À PROJETER

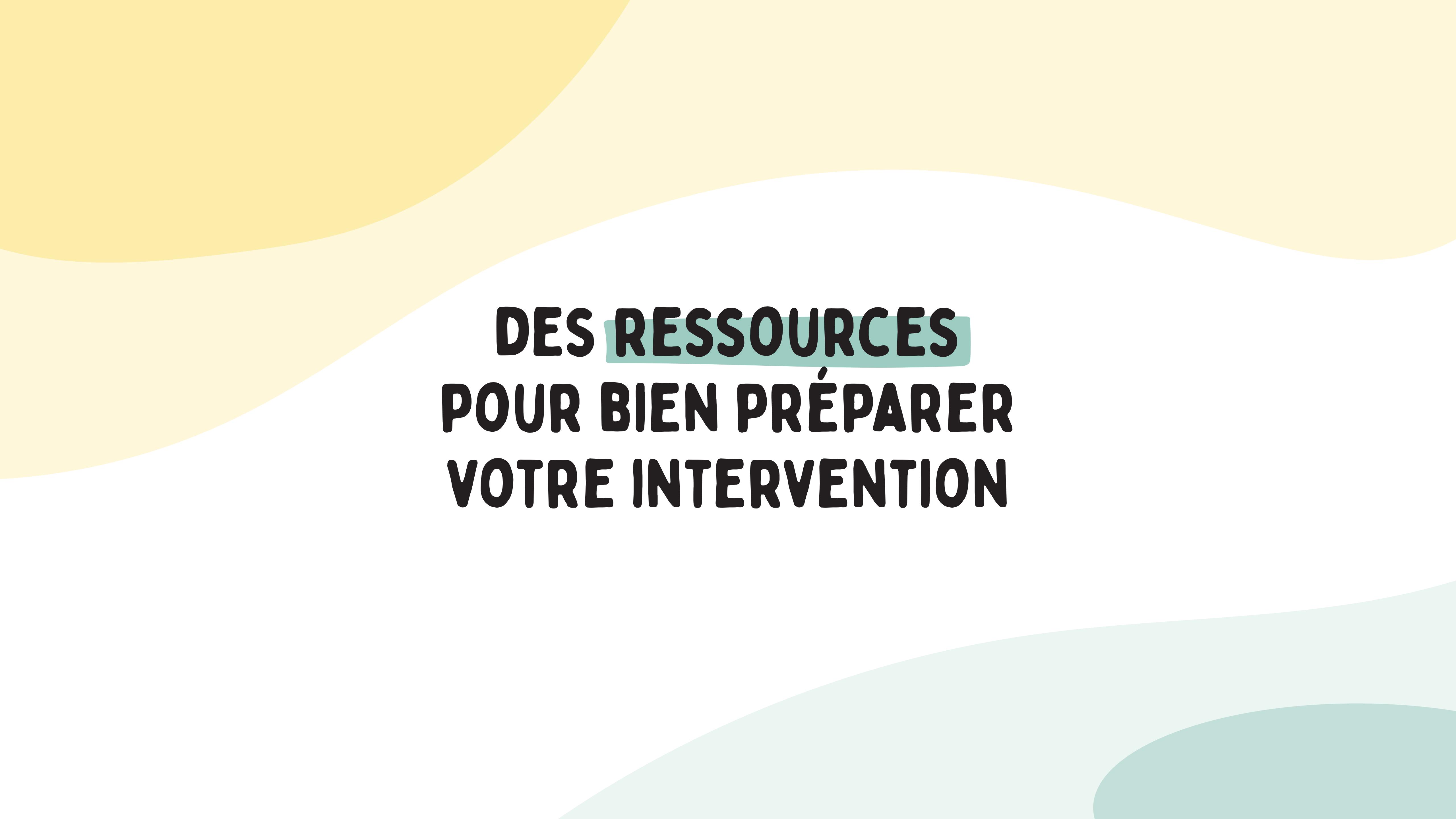


Faites le point sur les gestes à retenir pour protéger au mieux les comptes en ligne.



SLIDE À PROJETER

You pouvez conclure en lisant simplement la slide conclusion.
Puis, vous pouvez remercier les participants de l'atelier en leur disant quelques mots.



DES RESSOURCES
POUR BIEN PRÉPARER
VOTRE INTERVENTION

LES ACTEURS A CONNAITRE POUR REPÉRER ET ÉVITER LES DANGERS SUR INTERNET

Source : Application du Ministère de l'intérieur « [Ma sécurité](#) »

Percev@l : Cette plateforme vise à lutter contre la fraude à la carte bancaire sur Internet. Elle permet à tout internaute de signaler aux forces de l'ordre un ou plusieurs usages frauduleux de sa carte bancaire. Pour signaler une fraude si vous êtes toujours en possession de la carte, recherchez « [Signaler une fraude à la carte bancaire](#) » à l'aide de votre navigateur Internet ou directement sur [Percev@l](#).

L'ANSSI : L'[agence nationale de sécurité des systèmes d'information](#) (ANSSI) est l'autorité nationale en matière de défense et de sécurité cyber. Elle est plus spécialement chargée des opérateurs d'importance vitale, mais propose également des documentations destinées aux particuliers et aux professionnels.

Cybermalveillance.gouv.fr : Cette [plateforme nationale d'assistance aux victimes de cybermalveillance](#) propose un parcours diagnostique pour identifier la cybermalveillance à laquelle la victime est confrontée. En outre, elle distille des conseils et fiches pratiques sur divers phénomènes et propose la mise en relation avec un réseau de professionnels référencés en mesure de réaliser des actions de remédiation en cas de cybermalveillance.

Pharos : La [Plateforme d'harmonisation, d'analyse, de recouplement et d'orientation des signalements](#) (Pharos) du ministère de l'Intérieur procède prioritairement au traitement des signalements de contenus illicites mis en ligne. Tout un chacun peut effectuer un signalement depuis son portail dédié dès lors que le contenu incriminé est public. Arnaques, discriminations, menaces d'atteintes aux personnes, faits liés au terrorisme, urgences vitales, pédopornographie, peuvent notamment être portées à la connaissance des autorités grâce à ce dispositif. Pharos initie des enquêtes judiciaires chaque fois que nécessaire.

Signal Spam : Partenariat public/privé, [Signal Spam](#) permet aux internautes de signaler tout ce qu'ils considèrent comme étant du spam dans leur messagerie. La structure a pour vocation d'améliorer la lutte contre le spam en France.

E-enfance : L'[association e-Enfance](#) propose aux jeunes, à leurs parents et aux professionnels des interventions en milieu scolaire et des formations sur les usages responsables d'internet et les risques éventuels comme le cyberharcèlement, le cybersexisme et les autres formes de cyberviolence. Elle opère le 3018, numéro national pour les victimes de violences numériques (6 jours sur 7).

Info Escroqueries : Composé de policiers et de gendarmes, le téléservice Info Escroquerie est chargé d'informer, de conseiller et d'orienter les personnes victimes d'une escroquerie. Composez le 0 805 805 817 (du lundi au vendredi de 9h à 18h30).

France victimes : [France Victimes](#) est une association loi de 1901, créée en 1986. Elle fédère un réseau de 132 associations d'aide aux victimes d'infractions pénales, qui ont pour missions l'écoute, l'information juridique, le soutien psychologique et l'accompagnement des victimes d'infractions pénales en France. Contactez l'association en composant le 116 006 (7 jours sur 7 de 9h à 19h) ou par mail : victimes@france-victimes.fr

Phishing initiative : Initiative française privée, [Phishing Initiative](#) offre à tout internaute la possibilité de lutter contre les attaques de phishing.

Nomoreransom : Initiative européenne à laquelle participe Europol, [nomoreransom.org](#) collecte toutes les ressources disponibles permettant de mettre au clair les fichiers chiffrés par de nombreuses souches de ransomware.

LEXIQUE

Antivirus : logiciel informatique destiné à identifier, neutraliser et effacer des logiciels malveillants.

Authentification multifacteur : méthode d'authentification plus robuste qu'un simple identifiant et mot de passe et qui requiert la présentation de plusieurs types de preuves, appelées « facteurs ». Ces facteurs peuvent être des éléments d'information connus seulement par l'utilisateur (comme un mot de passe), un élément physique en sa possession (comme une carte à puce, un téléphone ou une clé USB) ou bien un élément biométrique.

Authentification forte : méthode d'authentification jugée la plus sécurisée, car elle repose sur des techniques de cryptographie qui sont jugées très difficiles à contourner.

Chiffrement : procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'une donnée impossible à toute personne qui ne possède pas la clé de (dé)chiffrement.

Code d'exploitation (exploit) : tout ou partie d'un programme permettant d'utiliser une vulnérabilité ou un ensemble de vulnérabilités d'un logiciel (du système ou d'une application) à des fins malveillantes.

Compte d'administrateur : compte permettant d'effectuer des modifications affectant les utilisateurs (modification des paramètres de sécurité, installation des logiciels...).

Logiciel espion : logiciel malveillant qui s'installe dans un ordinateur afin de collecter et transférer des données et des informations, souvent à l'insu de l'utilisateur.

Pare-feu (firewall) : logiciel et/ou matériel permettant de protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet, protection d'un réseau d'entreprise) en filtrant les entrées et en contrôlant les sorties selon les règles définies par son utilisateur.

Prime aux bogues (Bug Bounty) : programme de récompenses proposé par des sites web et entreprises qui offre des récompenses aux personnes qui rapportent des bogues, surtout ceux associés à des vulnérabilités. Ce programme a pour but de trouver et de corriger les bogues avant des cybercriminels.

Rançongiciel (Ransomware) : logiciel malveillant qui chiffre les données d'un appareil, ce qui les rend inaccessibles. Une rançon est réclamée, le plus souvent en cryptomonnaies, avec la promesse de restaurer l'accès aux données. Une fois exécuté sur son « hôte », le rançongiciel va progressivement chiffrer tous les fichiers qui lui sont accessibles, rendant leur consultation ou l'utilisation de l'appareil impossible. Dans le cas d'un réseau d'entreprise, le logiciel malveillant va également chercher à se propager sur toutes les ressources accessibles, y compris les ordinateurs partagés et les serveurs.

SOC (Security Operation Center) : division dans une entreprise qui assure la supervision, la détection et le traitement des incidents de sécurité.



MERCI!

Version 1.1 - Juin 2022

Ce document a été rédigé par des professionnels de la cybersécurité et sous la direction artistique de Claire Lacroix.

Ce document est mis à disposition sous licence [Creative Commons Attribution 4.0 International – \(CC BY 4.0\)](#).
Il est consultable à l'adresse suivante : <https://aka.ms/infoseckit>

Avec la contribution de : 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 et Thierry Matusiak.