

Séance “Sécuriser mes usages numériques”

Les trois situations suivantes permettent aux élèves de régler leurs paramètres, d'identifier les tentatives de phishing, et d'apprendre à créer des mots de passe robustes pour sécuriser leurs usages numériques.

Objectifs pédagogiques

Objectifs pédagogiques
Reconnaître les données personnelles que je transmets lorsque je m'identifie sur un service.
Reconnaître si un mail ou un sms est une tentative de phishing.
Créer des mots de passe forts et variés.

Liens avec le CRCN

Domaine	Compétence
Protection et sécurité	Protéger les données personnelles et la vie privée
Protection et sécurité	Sécuriser l'environnement numérique

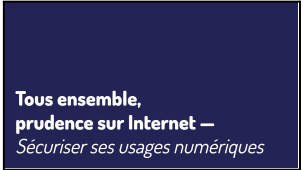
Déroulé synthétique

Séquence	Temps
Introduction de la séance	2 minutes
Activité : Traces d'identification Dans cette activité, chaque binôme d'élèves se voit attribuer une donnée personnelle. Au travers d'exemples sur des sites marchands ou réseaux sociaux, les élèves devront déterminer si la donnée personnelle qui leur est attribuée est collectée, ou non. Ils analysent également si cette collecte s'effectue automatiquement et si elle est essentielle pour le service en question.	15 minutes
Activité : Arnaque ou réel ? Dans cette activité, chaque binôme d'élèves dispose d'un exemple de message ou de mail. Ils doivent collectivement analyser ces exemples, afin de déterminer les bons réflexes qui permettent de se protéger des tentatives de phishing et apprennent ainsi à déterminer si un message est légitime ou non.	15 minutes
Analyse vidéo : Fuite de données Dans cette activité, les élèves identifient comment des mots de passe forts et variés permettent de sécuriser l'accès à un service, mais également quelles peuvent être les faiblesses des mots de passe suite au visionnage d'une vidéo traitant de la sécurité des services numériques. Ils saisissent ainsi les stratégies qui leur permettront de créer des mots de passe forts et efficaces.	15 minutes
Conclusion de la séance	3 minutes

Matériel

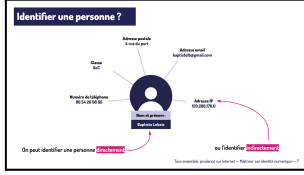
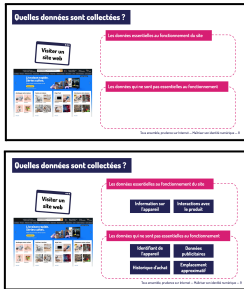

Matériel	
20 fiches données personnelles à découper	
16 fiches "Exemples de messages" à découper	

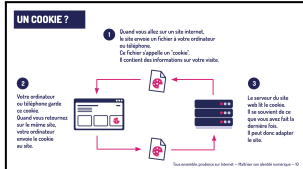
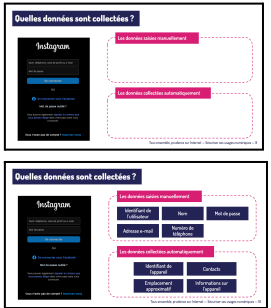

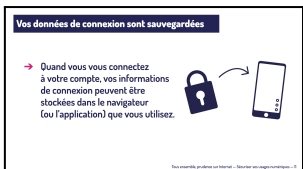

Introduction de la séance – 2 minutes

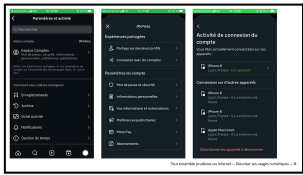
Actions des participants	Matériel
<p>Accueil</p> <p>L'animateur ou l'animatrice se présente et accueille le groupe.</p> <p>Il pose le cadre de l'intervention. Il explique le programme de la séance et invite à la participation et à la bienveillance de chacun.</p>	 <p>Support de présentation p.1</p>

Activité : Traces d'identification – 15 minutes



Actions des participants	Matériel
<p>L'animateur ou l'animatrice projette la situation.</p> <p><i>"Le compte instagram d'Emma était enregistré sur le téléphone de son amie Camille. Mais après une dispute, Camille est allée sur le compte d'Emma pour fouiller dans ses messages."</i></p> <p>L'animateur ou l'animatrice demande ;</p> <p><i>"Ça vous arrive de vous connecter avec un appareil qui n'est pas à vous ? Quelqu'un a déjà utilisé votre compte à votre place ? C'est déjà arrivé à quelqu'un que vous connaissez ?"</i></p>	 <p>Support de présentation p.2</p>
<p>"Pour comprendre cette situation, je vous distribue des fiches. Vous allez lire ce qui est écrit dessus. Nous allons essayer de comprendre quel est le point commun entre toutes ces fiches."</p> <p>L'animateur ou l'animatrice distribue les fiches aux groupes d'élèves, puis affiche la slide avec toutes les données personnelles. Il demande aux élèves qui ont les fiches de données compliquées de lire les définitions à voix haute pour tout le monde : <i>emplacement approximatif, identifiant de l'appareil, ou interactions avec le site ou l'appli.</i></p> <p>L'animateur ou l'animatrice demande ensuite aux élèves</p> <p><i>"Quel est le point commun entre toutes ces données ? – Toutes ces données sont des données personnelles"</i></p>	 <p>Fiches données personnelles à découper</p> <p>Support de présentation p.3</p>

Actions des participants	Matériel
<p>C'est quoi une donnée personnelle ?</p> <p>L'animateur ou l'animatrice lit ensuite les définitions inscrites sur la slide.</p> <p>D'abord la définition "officielle" de la CNIL, puis la version résumée / simplifiée.</p> <p>L'animateur ou l'animatrice demande ensuite ; <i>"qu'est ce que ça veut dire, "identifier quelqu'un ?"</i></p>	 <p>Support de présentation p.4</p>
<p>Identifier une personne ?</p> <p>L'animateur ou l'animatrice désigne certaines des données présentées sur l'image : certaines permettent d'identifier une personne directement (nom, prénom) et d'autres permettent d'identifier une personne indirectement (adresse postale, numéro de téléphone...).</p> <p>L'animateur ou l'animatrice peut utiliser cet exemple :</p> <p><i>"On sait que cette adresse mail appartient à Baptiste. Donc si je reçois un mail depuis cette adresse, c'est que c'est Baptiste qui m'a envoyé un email."</i></p> <p>L'animateur ou l'animatrice explique</p> <p><i>"on peut identifier une personne avec une seule donnée, comme avec son numéro de téléphone.</i></p> <p><i>Mais on peut également identifier une personne en croisant des données qui, seules, ne seraient pas suffisantes : le prénom et la classe, par exemple."</i></p> <p>L'animateur ou l'animatrice explique que ces données personnelles, nous en donnons constamment sur internet.</p>	 <p>Support de présentation p.5</p>
<p>L'animateur ou l'animatrice explique la consigne de la slide suivante :</p> <p><i>"D'après-vous, quelles données sont collectées lorsque nous arrivons sur un site internet où nous n'avons pas besoin de compte ?"</i></p> <p><i>"Parmi les données qui figurent sur les fiches que je vous ai distribuées, certaines sont indispensables, d'autres ne le sont pas."</i></p> <p><i>"Regardez la fiche que vous avez dans les mains. À votre avis, est-ce que le site web collecte cette donnée ?"</i></p> <p>Les élèves lèvent la main s'ils pensent que le site web collecte la donnée qu'ils ont entre les mains.</p> <p>Ensuite, l'animateur ou l'animatrice affiche la correction. Il explique :</p> <p><i>"certaines données sont indispensables. La donnée personnelle "type d'appareil" permet au site d'afficher une version compatible avec l'appareil. Vous avez déjà remarqué qu'un site paraît différent selon que vous le visitez avec un ordinateur ou un smartphone..."</i></p> <p><i>D'autres données ne sont pas nécessaires : la donnée personnelle "données publicitaires" permet au site de faire des recommandations personnalisées, ou de montrer des publicités ciblées. Ça ne vous apporte rien, à vous !</i></p> <p><i>Indispensables ou pas, toutes les données collectées quand on visite un site web sont</i></p>	 <p>Support de présentation p.6-7</p>  <p>Fiches données personnelles à découper</p>

Actions des participants	Matériel
collectées grâce aux cookies”.	
<p>C'est quoi les cookies ?</p> <p><i>“Les cookies, ce sont des fichiers que les sites internet enregistrent sur ton ordinateur ou ton téléphone quand tu les visites. Ces fichiers contiennent la liste des choses que tu as fait sur le site : les pages regardées, les liens sur lesquels tu as cliqué, les recherches, les choses que tu as mises dans un panier d'achat. Certaines des données des cookies permettent de faire fonctionner le site, comme le “type d'appareil.” D'autres ne servent qu'à te recommander des contenus, ou à te montrer des publicités ciblées.”</i></p>	 <p>Support de présentation p.8</p>
<p>L'animateur ou l'animatrice passe à l'exemple suivant.</p> <p>“Maintenant nous allons essayer de comprendre, ce que collecte un site ou une application lorsqu'on se crée un compte, ou qu'on se connecte à son compte. Certaines données personnelles, vous allez les fournir volontairement, et certaines seront collectées automatiquement.</p> <p><i>“Ici, nous sommes sur une page de connexion de réseau social. D'après-vous, quelles données vont être collectées ? Regardez la fiche que vous avez dans les mains. À votre avis, est-ce que dans ce cas, vous fournissez cette donnée personnelle ? Si oui, est-ce manuel ou automatique ?”</i></p> <p>L'animateur ou l'animatrice affiche la correction, et explique</p> <p><i>“quand on se connecte à un site ou une application, nous fournissons nous-mêmes notre identifiant, mais aussi une adresse e-mail, ou notre n° de téléphone*. Mais il y a également des données qui sont collectées sans que nous ayons à les saisir nous-mêmes... L'identifiant de l'appareil, l'emplacement où vous êtes, les contacts dans votre téléphone : tout cela va être fourni au réseau social sans que vous n'ayez rien à faire...”</i></p> <p><i>[* s'il en a le temps, l'animateur peut expliquer qu'il vaut mieux utiliser une adresse mail pour se créer un compte, car c'est plus facile d'en changer que de changer de n° de téléphone]</i></p>	 <p>Support de présentation p.9-10</p>  <p>Fiches données personnelles à découper</p>
<p><i>“Et comme c'est assez ennuyeux de devoir s'identifier à chaque fois qu'on se connecte à un site ou qu'on ouvre une application, vos données de connexion (votre identifiant, votre mot de passe...) sont stockées dans un cookie enregistré sur votre ordinateur ou votre smartphone. Vous n'avez pas à les redonner à chaque fois que vous voulez ouvrir votre application !</i></p> <p><i>Du coup, c'est bien pratique, mais ça peut aussi poser des problèmes...”</i></p>	 <p>Support de présentation p.11</p>
<p>L'animateur ou l'animatrice reprend la situation d'Emma.</p> <p>“Le compte instagram d'Emma était enregistré sur le téléphone de son amie Camille. Mais après une dispute, Camille est allée sur le compte d'Emma pour fouiller dans ses messages.”</p> <p>L'animateur ou l'animatrice demande</p> <p><i>“Alors, à votre avis, comment Camille a-t-elle pu accéder au compte d'Emma ?</i></p>	 <p>Support de présentation p.12</p>

Actions des participants	Matériel
<p>→ Emma s'était connectée sur le téléphone de Camille, et les identifiants de connexion de Camille étaient donc enregistrés. Camille n'avait plus qu'à sélectionner le profil d'Emma pour accéder à son compte.</p>	
<p>Qu'aurait dû faire Emma pour éviter que ça n'arrive ?</p> <ul style="list-style-type: none"> → Déconnecter son compte Instagram sur le téléphone de Camille après l'avoir utilisé → Déconnecter à distance les appareils sur lesquels son compte est enregistré <p>L'animateur ou l'animatrice explique ensuite comment faire en prenant l'exemple d'Instagram. Il faut aller dans les paramètres > Dans l'espace comptes > Dans l'onglet Sécurité > Et déconnecter les sessions actives sur d'autres appareils.</p> <p><i>"La plupart des applications proposent cette fonctionnalité, pour permettre aux utilisateurs de garder la main sur la sécurité de leurs comptes. Si vous ne savez pas comment faire, vous pouvez chercher simplement sur internet [nom de l'appli] déconnecter tous les appareils."</i></p>	<p>QUE PEUT FAIRE EMMA DANS SA SITUATION ?</p> <ul style="list-style-type: none"> → Quand Emma se connecte sur un appareil qui ne lui appartient pas, il faut qu'elle se déconnecte quand elle a fini. → Elle peut aussi déconnecter à distance les appareils sur lesquels son compte est enregistré.  <p>Support de présentation p.13-14</p>

Activité : Arnaque ou réel ? — 15 minutes

Actions des participants	Matériel
<p>Introduction</p> <p>L'animateur ou l'animatrice présente la situation :</p> <p><i>"Marco a reçu un SMS avec un lien qui lui dit de confirmer les informations de paiement de son compte Netflix. Et que s'il ne le fait pas, son compte sera suspendu. Il ne sait pas s'il doit cliquer sur ce lien."</i></p> <p>L'animateur ou l'animatrice demande ;</p> <p><i>"ça vous est déjà arrivé ? vous avez déjà reçu ce type de messages ?" est-ce arrivé à quelqu'un dans votre famille ? qu'avez-vous fait ? Pensez-vous que Marco devrait cliquer sur le lien ?"</i></p> <p>Puis :</p> <p><i>"En effet, ce message est une arnaque. Certaines personnes, les pirates, peuvent chercher à voler vos données personnelles. Pour ça, une technique très répandue est celle du hameçonnage (ou phishing)."</i></p>	<p>LA SITUATION DE MARCO</p>   <p>Support de présentation p.15-16</p>

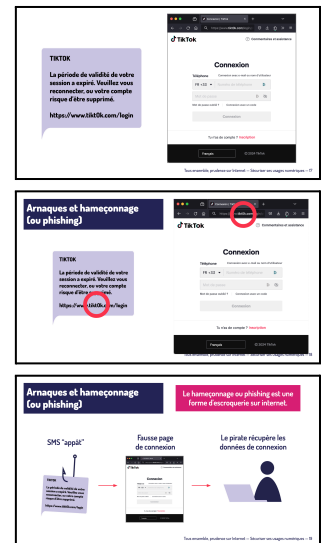
Actions des participants

L'intervenant utilise l'exemple "TikTok" pour expliquer au public quel est l'objectif de cet exemple d'arnaque.

"En créant une fausse page web, identique à celle de tiktok, le diffuseur de ce message cherche à récupérer les identifiants de connexion d'un utilisateur."

Le hameçonnage, c'est ça : une escroquerie sur internet. Quelqu'un se fait passer pour un organisme ou une plateforme que vous connaissez, pour que vous fournissiez vos identifiants et d'autres données personnelles. Ils essaieront ensuite d'exploiter vos identifiants et données personnelles sur d'autres sites pour obtenir de l'argent ou faire des achats qu'ils ne paieraient pas, puisque c'est votre compte en banque qui serait facturé."

Matériel



Support de présentation
p.17-19

L'animateur ou l'animatrice explique la consigne de l'activité.

"Je vais distribuer une fiche à chaque binôme. Sur ces fiches, il y a des captures d'écran de messages, de mails, ou de sites web. Je vous demande d'identifier lesquels de ces exemples sont des arnaques, et lesquels sont des messages réels. Chacun son tour, chaque binôme expliquera à la classe pourquoi cet exemple est ou n'est pas une arnaque."

L'animateur ou l'animatrice fait défiler les exemples au tableau. Pour chaque exemple, il demande au binôme correspondant de déterminer s'il s'agit d'une arnaque ou pas, et d'expliquer pourquoi.

Les exemples à traiter :

Disney+ — ARNAQUE — Le lien ne renvoie pas vers le site de Disney

Bonjour, c'est le livreur — ARNAQUE — Le lien ne renvoie pas vers le site de chronopost (seul le sous-domaine s'appelle chronopost, ici le nom de domaine est pickup-suivi.com)

Salut Marine, — PAS UNE ARNAQUE — Aucun lien, contact enregistré

INFO SFR : une esim — ARNAQUE — le lien n'est pas le bon, ne renvoie pas sur le site de SFR

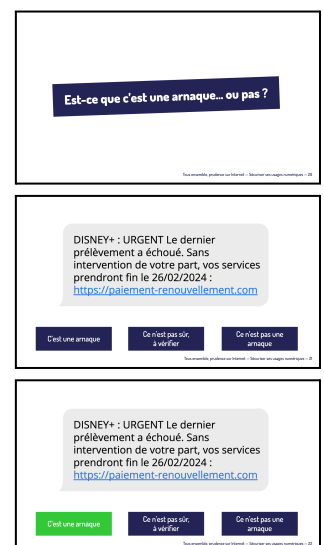
Votre code de connexion Twitter — PAS UNE ARNAQUE — c'est un code de confirmation

MONDIALRELAY : Votre première livraison — ARNAQUE — pas le bon site

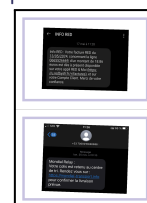
INFO-ANTAI : Dernier rappelle — ARNAQUE — Lien compressé pour cacher la destination, et fautes d'orthographe dans le message

Votre colis 49801681 à été livré — PAS UNE ARNAQUE — Informations précises, c'est un code de retrait


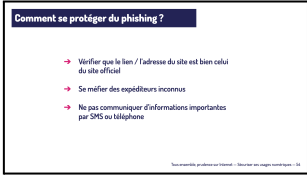


INFO RED : Votre facture — PAS UNE ARNAQUE — Informations précises, le lien est le




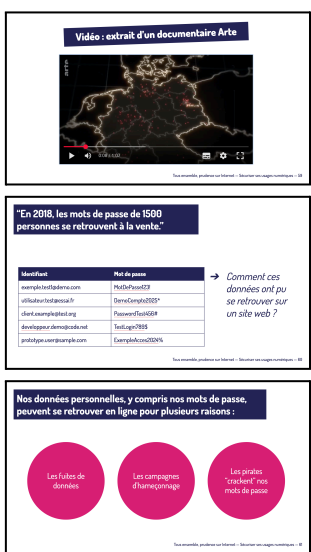
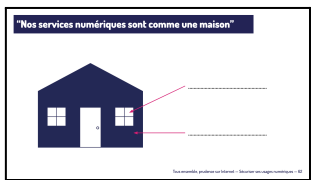
Support de présentation
p.20-52



Fiches "Exemples de
messages" à découper

Actions des participants	Matériel
<p>bon</p> <p>La créativité est un métier — PAS SÛR — Le lien est compressé, mais cela semble être un message promotionnel classique. À vérifier.</p> <p>SFR espace Client — ARNAQUE — l'url n'est pas celle du site de SFR</p> <p>CC papa, — ARNAQUE — Schéma classique des arnaques (tenter de rediriger vers un autre service, ce genre de message cible par exemple particulièrement les personnes âgées)</p> <p>SFR attire votre attention — ARNAQUE — c'est un lien compressé</p> <p>INFO RED : vous avez consommé — PAS UNE ARNAQUE — les informations sont précises, le lien redirige bien vers le site de SFR</p> <p>Mondial Relay : Votre colis — ARNAQUE — le lien n'est pas le bon</p> <p>Netflix : votre compte sera suspendu — ARNAQUE — le lien n'est pas le bon, et le message joue sur l'urgence pour faire paniquer</p>	
<p>Débrief :</p> <p>L'animateur ou l'animatrice projette la slide de débrief, qui récapitule les différents éléments à observer afin de se protéger des tentatives de hameçonnage. Il ou elle explique :</p> <p><i>"Il faut faire attention aux liens qui sont dans les messages. Il faut aussi faire attention aux expéditeurs inconnus, et il ne faut pas communiquer d'informations importantes par SMS ou téléphone. Ce genre de tentative de hameçonnage va souvent jouer sur les émotions : la peur de perdre l'accès à votre compte sur votre réseau social préféré, ou l'impatience de recevoir un colis... L'important est de bien prendre le temps d'observer pour ne pas se faire avoir. Ne jamais se précipiter."</i></p>	  <p>Support de présentation p.53-54</p>
<p>Résolution de la situation :</p> <p>L'animateur ou l'animatrice revient à la situation de Marco. Il demande aux élèves ce que doit faire Marco dans sa situation.</p> <p><i>"En effet, il ne doit pas répondre à ce message, car il s'agit très clairement d'une tentative d'hameçonnage."</i></p> <p>Transition vers activité sur les mots de passe :</p> <p><i>"Être vigilant à tous ces signes permet de se protéger de ce type d'arnaque. Mais pour bien protéger ses données personnelles, il faut également faire d'autres choses. Parce que nous pouvons toutes et tous nous faire avoir par ce genre d'arnaque un jour."</i></p>	  <p>Support de présentation p.55-57</p>

Analyse vidéo : Fuite de données – 15 minutes

Actions des participants	Matériel
<p>Introduction</p> <p>L'animateur ou l'animatrice demande aux élèves :</p> <p><i>“Pour vous, à part éviter de cliquer sur les liens qu'on vous envoie par mail ou SMS, qu'est-ce qui est important pour bien protéger ses comptes et ses données personnelles ?”</i></p> <p>Les élèves répondent, jusqu'à ce qu'un ou une élève parle des mots de passe.</p> <p><i>“Les mots de passe sont très importants pour protéger nos comptes et sessions. Pour mieux comprendre en quoi c'est important, nous allons nous appuyer sur la situation de Elya.”</i></p> <p>L'animateur ou l'animatrice lit la situation :</p> <p><i>“Elya a été dupée par une page d'hameçonnage. Elle a donné son identifiant et son mot de passe. Elle a changé son mot de passe sur le vrai site, mais elle se demande si ses autres comptes sont en danger.”</i></p>	<p></p> <p>Support de présentation p.58</p>
<p>L'animateur ou l'animatrice montre la vidéo au groupe et revient ensuite avec les publics, sur ce qu'ils ont vu dans la vidéo :</p> <p><i>“Au début de la vidéo, il est dit qu'en 2018, les mots de passe de 1500 utilisateurs se sont retrouvés en vente sur le web. À votre avis, comment c'est possible ?”</i></p> <p><i>Voici à quoi ressemble une liste d'identifiants volés :</i></p> <p><i>un gros tableau, avec des adresses mails et le mot qui y est associé”</i></p> <p>“Ces listes peuvent être faites de plusieurs façons :</p> <ul style="list-style-type: none"> - les fuites de données : des pirates attaquent les entreprises, et volent sur leurs serveurs la liste des utilisateurs et leurs mots de passe - les campagnes d'hameçonnage : les pirates envoient des messages avec des liens, comme nous venons de le voir, et vont récupérer les identifiants de connexion des utilisateurs imprudents - cracker nos mots de passe : les pirates utilisent parfois des logiciels qui vont tester un par un, et à toute vitesse, tous les mots de passe possibles, jusqu'à trouver le bon. <p><i>“Il est très important de faire attention à nos données personnelles, surtout nos mots de passe. Mais il est toujours possible qu'un de nos mots de passe se retrouve dans la nature.”</i></p>	<p></p> <p>Support de présentation p.59-61</p>
<p>Mais du coup, à quel point est-ce grave, qu'un mot de passe soit ainsi accessible ?</p> <p>L'animateur ou l'animatrice reprend l'image de la maison utilisée dans la vidéo et rappelle les différents éléments :</p> <ul style="list-style-type: none"> - Les murs et le toit : ce sont les logiciels et applications que nous utilisons, qui contiennent différentes données personnelles sur nous 	<p></p>

Actions des participants

- **Les portes et les fenêtres, protégées par des serrures** : les connexions, protégées par des mots de passe

L'animateur ou l'animatrice utilise cet exemple pour illustrer le fait de perdre un mot de passe :

"Imaginons, vous perdez votre clé de la porte d'entrée de chez vous. Ou vous vous demandez si quelqu'un vous l'a volée. Qu'allez-vous devoir faire ? Changer la serrure, pour rester en sécurité, bien sûr.

Quelle serrure ?

Celle de la porte d'entrée bien sûr.

Mais si c'est la même clé que pour la boîte aux lettres ?

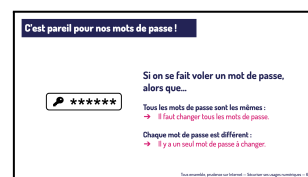
Et si la même clé ouvre la porte d'entrée, la porte du garage, la boîte aux lettres et la porte-fenêtre qui donne sur le jardin ?

Il faudra changer toutes les serrures qui correspondent à la clé perdue ou volée.

Pour les mots de passe, c'est la même chose ; lorsqu'un de vos mots de passe a été volé ou rendu public, vous allez devoir en faire un nouveau pour tous les sites où vous l'utilisez, et donc :

- si vous utilisez toujours le même mot de passe : Il faut changer sur tous comptes.
- si vous utilisez un mot de passe différent pour chaque compte : Il y a un seul mot de passe à changer.

Matériel



Support de présentation
p.62-65

L'animateur ou l'animatrice explique :

"Utiliser un mot de passe différent pour chaque site, c'est donc important. Mais il y a autre chose de très important en ce qui concerne les mots de passe. C'est qu'ils soient assez forts.

"Pour vous, parmi les deux mots de passe affichés à l'écran, quel est le mot de passe le plus fort ? Et pourquoi ? Qu'est-ce qui fait un mot de passe fort ?"

L'animateur ou l'animatrice demande :

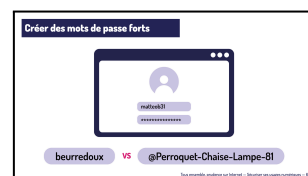
"mais pourquoi c'est important d'avoir un mot de passe fort ?"

En fonction des réponses des publics, il ou elle explique :

"Certains pirates peuvent "cracker" un mot de passe. Pour ça ils vont utiliser un logiciel, qui va essayer, un par un, tous les mots de passe possibles ! Si votre mot de passe est trop simple, il le trouvera instantanément ! Surtout si comme "beurreddoux" il est composé uniquement de mots connus. Par exemple pour ces deux mots de passe, combien de temps ça prend ?"

La réponse pour l'exemple "beurreddoux" : 3 secondes

La réponse pour l'exemple "@Perroquet-Chaise-Lampe-81" : Au moins 26 trillions d'années



Support de présentation p.62

Actions des participants

Quiz sur les mots de passe, et la durée nécessaire pour les craquer à l'aide d'un logiciel d'attaque en force brute*.

L'intervenant utilise le support de présentation pour animer un quiz, dans lequel les participants doivent deviner le temps nécessaire pour craquer un mot de passe. Plus les exemples avancent, plus la durée est longue parce que les mots de passe se complexifient.

[* un logiciel qui va automatiquement tester toutes les combinaisons possibles, en débutant par les plus "faciles" : les mots qui existent, les suites de chiffres ou de lettres prévisibles (azerty, abcd, 1234, 4321, etc)]

L'animateur ou l'animatrice présente l'infographie de gauche "Combien de temps faut-il à un pirate pour trouver votre mot de passe en 2023 ?".

Il explique qu'à l'aide de logiciels spécialisés, les pirates peuvent tester plusieurs milliers de combinaisons à la seconde. Donc un mot de passe très court pourra être trouvé quasiment instantanément.

L'animateur ou l'animatrice utilise ensuite le tableau, en donnant des exemples, pour illustrer en quoi le temps nécessaire pour cracker un mot de passe est différent en fonction de la complexité du mot de passe.

Création de système de mot de passe

L'animateur ou l'animatrice enchaîne :

"Mais comment faire pour avoir un mot de passe long, compliqué, et en même temps différent pour chaque site ? Et ensuite s'en souvenir ou être capable de le retrouver ? Vous pouvez utiliser ce qu'on appelle un système de mots de passe. L'idée, c'est de créer une logique, toujours la même, qui changera légèrement en fonction de chaque site."

L'animateur ou l'animatrice explique les étapes par lesquelles passer pour créer son système de mot de passe, et invite ensuite les élèves à essayer au tableau.

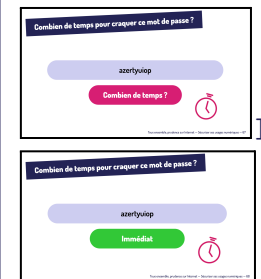
L'animateur ou l'animatrice précise que, évidemment, il ne faut pas qu'ils réutilisent les exemples montrés au tableau.

L'animateur ou l'animatrice revient sur la situation de Elya.

Il demande aux élèves ce que doit faire Elya dans sa situation :

- Si elle utilisait des mots de passe différents partout, alors avoir changé un mot de passe est suffisant. Elle doit s'assurer que ses mots de passe sont forts.
- Si elle utilisait le même mot de passe partout, elle doit changer tous ses mots de passe, sur tous ses comptes, et les remplacer par des mots de passe forts.

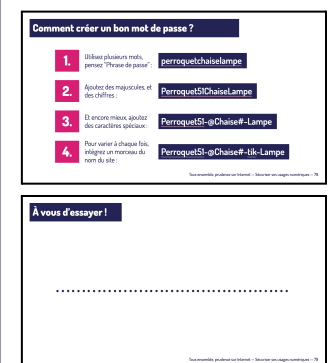
Matériel



Support de présentation p.67-76



Support de présentation p.77



Support de présentation p.78-79



Support de présentation p.80-81

Conclusion de la séance — 3 minutes

Actions des participants	Matériel
<p>Conclusion</p> <p>L'animateur ou l'animatrice demande aux publics de résumer ce qu'il s'est passé au cours de ces séances, ce que les élèves ont retenu.</p> <p>L'animateur ou l'animatrice donne la parole aux publics, et pour chaque point abordé, demande aux publics à quoi ils pensent que cela leur servira, aujourd'hui, demain, plus tard...</p>	