Mots de passe

Les participants apprendront à mieux protéger leurs informations en ligne en utilisant et en maintenant des mots de passe forts. Ils prendront connaissance des principes de création d'un mot de passe fort et des problèmes pouvant être engendrés par le partage de mots de passe. Ils apprendront également à protéger leurs mots de passe et à prendre des mesures afin d'éviter que quiconque n'y ayant pas été autorisé accède à leurs comptes.

Documentation

Fiche Formation sur les mots de passe

Notions de base sur les mots de passe

Première partie

Informations aux élèves

Nous ne réfléchissons pas souvent aux mots de passe que nous utilisons sur les sites web, applications et services. Toutefois, plus votre mot de passe sera bien choisi, plus vos informations seront protégées.

Interaction dans la classe

Encouragez les participants à débattre sur les questions suivantes. Veuillez rappeler aux participants qu'il est important de ne pas partager leurs véritables mots de passe au cours de cet exercice ou de tout autre exercice.

Questions aux élèves

Combien de mots de passe possédez-vous ?

> Utilisez-vous un mot de passe différent pour votre boîte e-mail et pour chacun de vos comptes sur les réseaux sociaux ?
>
> Sont-ils très différents, ou sont-ils une variante d'un seul mot de passe ?

Si vous avez plusieurs mots de passe, comment faites-vous pour vous souvenir que tel mot de passe appartient à tel compte ?

Questions aux élèves

Combien de fois vous est-il arrivé d'oublier un mot de passe important ?

> Qu'avez-vous fait lorsque vous avez oublié votre mot de passe ?
>
> Comment faites-vous pour que vos mots de passe soient faciles à retenir ?

Y a-t-il un mot de passe que vous utilisez tous les jours ?

Que se passerait-il si quelqu'un trouvait votre mot de passe sans que vous ne le sachiez ?

> Est-ce que cela dépendrait de qui il s'agit ?

Quel genre d'informations quelqu'un pourrait-il apprendre sur vous s'il utilisait votre mot de passe pour accéder à votre compte ?

Deuxième partie

Interaction dans la classe

Mettez les participants deux par deux.

Informations aux élèves

Discutez avec votre binôme de ce qu'il pourrait se passer si quelqu'un voulant vous causer du tort découvrait le mot de passe que vous utilisez pour accéder à votre plate-forme de réseau social préférée.

Interaction dans la classe

Donnez 5 minutes aux participants pour discuter. Demandez ensuite aux groupes de partager leur avis.

Informations aux élèves

À présent, discutez avec votre binôme de ce qu'il se passerait si un pirate informatique découvrait le mot de passe qu'utilisent vos parents/tuteurs pour accéder à leurs comptes bancaires en ligne.

Interaction dans la classe

Donnez 5 minutes aux participants pour discuter. Demandez ensuite aux groupes de partager ce dont ils ont discuté.

Troisième partie

Informations aux élèves

Vous vous demandez peut-être comment un pirate informatique peut découvrir un mot de passe privé. Il existe plusieurs façons de le faire ; l'une d'entre elles consiste à utiliser l'ingénierie sociale, c'est-à-dire à piéger quelqu'un afin qu'il partage son mot de passe. Un pirate informatique peut le faire en envoyant un e-mail qui semble provenir d'une plate-forme ou d'un site web sur lequel la personne a un compte. L'e-mail peut inviter la personne à cliquer sur un lien et à se connecter avec son nom d'utilisateur et son mot de passe et, dès lors que la personne se connecte, le pirate informatique a accès à ces informations.

Les pirates informatiques tentent souvent de deviner des mots de passe en utilisant des expressions fréquentes telles que « motdepasse123 », « test » ou encore votre

nom ou prénom.

Une autre façon utilisée par les pirates informatiques pour découvrir un mot de passe privé est ce que l'on appelle l'attaque « par force brute ». Une attaque par force brute a lieu lorsqu'un pirate informatique essaie de se connecter à votre compte en essayant de façon répétitive plusieurs mots de passe. Bien qu'un pirate informatique soit en mesure de manuellement perpétrer une attaque par force brute, c'est souvent un programme informatique qui réalise l'opération, de façon rapide et automatique, en essayant toutes les combinaisons de mots de passe possibles. Par exemple, une liste de mots de passe possibles ou un ensemble de mots de passe consistant en une combinaison de plusieurs lettres et chiffres, jusqu'à ce qu'ils découvrent le bon code d'accès.

Évidemment, certaines attaques par force brute sont plus complexes. Si votre mot de passe fait partie de la liste des mots de passe probables, tels que « médor123 » ou « motdepasse », certains programmes pourront le deviner plus rapidement en essayant ces mots de passe en priorité, avant d'en essayer des moins probables ou d'essayer différentes possibilités aléatoires. L'attaque peut être également plus précise si le pirate informatique dispose d'informations vous concernant. Par exemple, s'il sait que votre animal de compagnie s'appelle Toby, il peut essayer « Toby » avec différents chiffres à la fin (ex. : « Toby629 » ou « Toby3020 »)

Principes de création

Première partie

Questions aux élèves

Qui sait ce que veut dire avoir un mot de passe « fort » ou un mot de passe « plus fort » ? En quoi est-ce une bonne idée ?

Informations aux élèves

Un mot de passe fort permet de protéger vos informations. Alors qu'un mot de passe fort ne garantit pas que votre compte ne soit jamais piraté, avec un mot de passe faible, il est beaucoup plus facile pour une personne d'accéder à vos informations.

Exercice sur les mots de passe

Questions aux élèves

Donnez quelques exemples de mots de passe faibles.

1. Quelques exemples : Motdepasse, 12345, salut!, une date de naissance, un surnom.

Selon vous, pourquoi sont-ils faibles ?

1. Ils peuvent être facilement devinés par une autre personne et/ou un ordinateur qui effectue une attaque « par force brute ».

Citez quelques façons de rendre un mot de passe plus fort.

1. Ajouter des chiffres, des lettres majuscules et minuscules, des symboles, utiliser un mot de passe plus long et éviter les expressions communes et les mots seuls.

Interaction dans la classe

Une fois que les participants auront donné leurs avis, écrivez ces consignes au tableau :

Comprend au moins un chiffre.

Comprend au moins un symbole.

Comprend au moins une lettre majuscule et une lettre minuscule.

Les mots de passe doivent contenir au moins 7 caractères.

Les mots de passe doivent être faciles à retenir (sauf si vous utilisez un gestionnaire de mots de passe).

Un gestionnaire de mots de passe est un site web/une application aidant les utilisateurs à enregistrer et à organiser leurs mots de passe.

Les mots de passe ne doivent pas contenir un mot fréquent seul ou des informations personnelles (date de naissance, nom d'un parent, etc.).

Un même mot de passe ne doit pas être utilisé pour plusieurs sites web.

Informations aux élèves

Il existe deux approches afin de créer des mots de passe forts. La première consiste à suivre une « recette du bon mot de passe », comme celle inscrite au tableau. Suivre cette « recette » vous encourage à inclure des éléments plus difficiles à deviner à votre mot de passe texte/numérique afin de le rendre plus fort. L'inconvénient de cette approche est que le mot de passe devient plus difficile à retenir.

Les mots de passe forts

Informations aux élèves

Une autre approche pour créer des mots de passe forts concerne la longueur du mot de passe. Parce que la force d'un mot de passe réside dans sa longueur, utiliser une suite de 4 mots ou plus sans aucun rapport le rend beaucoup plus difficile à deviner tant pour les personnes que pour les attaques par force brute. Cette méthode a l'avantage supplémentaire de créer des mots de passe plus faciles à retenir que ceux créés en utilisant la « recette du bon mot de passe ».

Enfin, on peut utiliser un mélange de ces deux méthodes en créant une suite de 4 mots ou plus qui n'ont aucun rapport, et en y ajoutant des symboles et des chiffres.

Le but de ces différentes méthode est le même : créer des mots de passe uniques et difficiles à deviner par d'autres personnes.

Informations aux élèves

Mettez les participants deux par deux

Par deux, essayer de créer un mot de passe fort en utilisant les consignes que vous avez écrites plus tôt au tableau. Pensez qu'un mot de passe difficile à trouver de façon aléatoire par un ordinateur peut tout de même être facile à deviner pour un humain ou pour un ordinateur qui dispose d'une liste de mots de passe longs et fréquents. La feuille sur laquelle vous avez écrit votre mot de passe ne sera pas ramassée à la fin de l'activité. De ce fait, nous vous encourageons à ne pas utiliser ce mot de passe pour l'un de vos comptes puisque les membres du groupe le connaîtront.

Donnez 5 minutes aux participants pour faire cela. Ensuite, parcourez la salle et demandez aux participants de donner des exemples de mots de passe qui sont, selon eux, très forts. Demandez aux participants s'ils peuvent se souvenir des mots de passe qu'ils ont créés sans les regarder.

Certains sites web demanderont que vos mots de passe remplissent quelques-unes de ces conditions (voire toutes), et d'autres ne les soumettront à aucune restriction. Vous pouvez également créer des mots de passe contenant une suite de mots fréquents et aléatoires.

Interaction dans la classe

Toujours deux par deux, demandez aux participants de créer de nouveaux mots de passe en utilisant des suites de mots. Dites-leur d'utiliser au moins quatre mots afin que le mot de passe soit à la fois fort et facile à retenir. Donnez 5 minutes aux participants pour faire cela. Ensuite, parcourez la salle et demandez aux participants de vous donner leurs exemples de mots de passe. Une fois de plus, rappelez aux participants que leurs feuilles ne seront pas ramassées à la fin de l'activité et de ne pas utiliser ce mot de passe pour l'un de leurs comptes.

Informations aux élèves

Certains sites web utilisent un système appelé identification à facteurs multiples (ou à deux facteurs) afin de vérifier votre identité. Ces sites web utilisent souvent un texto, une app ou un e-mail comportant un code à utilisation unique qui doit être saisi avec le mot de passe.

Cette méthode protège davantage vos comptes en ajoutant un niveau de sécurité supplémentaire qui est beaucoup plus difficile à pirater. À titre d'exemple, pour se connecter à votre compte, une personne doit connaître votre mot de passe et accéder à l'application, à l'appareil ou à l'adresse e-mail associée à votre compte.

Protéger les mots de passe

Première partie

Informations aux élèves

Même si vous créez un mot de passe difficile à pirater par un ordinateur ou une personne, il existe d'autres raisons pour lesquelles un mot de passe peut être faible.

Questions aux élèves

Quelles sont les autres raisons pour lesquelles un mot de passe peut être faible ?

1. Quelques exemples : utiliser un même mot de passe pour plusieurs comptes, utiliser un mot de passe qui contient des informations personnelles, utiliser le même mot de passe pendant des années, oublier votre mot de passe.

Selon vous, à quelle fréquence devriez-vous changer vos mots de passe ?

Informations aux élèves

Même les bons mots de passe peuvent être mis en danger ou volés, mais il existe des moyens pour vous protéger. Si une brèche de données a lieu sur un site où vous possédez un compte, assurez-vous de changer votre mot de passe sur ce site, mais également sur tous les sites web où vous utilisez un mot de passe similaire.

Il peut être difficile de se souvenir de nombreux mots de passe longs et compliqués.

Questions aux élèves

Selon vous, est-ce une bonne idée d'écrire vos mots de passe sur une feuille ou dans un document de votre ordinateur ? Pourquoi ? Si non, pourquoi ?

Interaction dans la classe

Évoquez plusieurs possibilités, par exemple si quelqu'un trouve la feuille ou le fichier contenant les mots de passe. Expliquez qu'il existe une approche consistant à utiliser un gestionnaire de mots de passe. Le gestionnaire de mots de passe est une application qui aide les utilisateurs à enregistrer et organiser leurs mots de passe.

Deuxième partie

Informations aux élèves

Chaque jour, nous utilisons différents comptes sur différents sites web. Il peut être

compliqué de se connecter et de se déconnecter de chaque site à chaque fois.

Questions aux élèves

Avez-vous déjà utilisé la fonctionnalité « enregistrer le mot de passe » de votre navigateur pour qu'il soit sauvegardé pour un site web ? Pourquoi ? Si non, pourquoi ?

Comprenez-vous comment le site web se souvient de vous ?

1. Demandez aux participants de vous expliquer. Expliquez ensuite que les sites web peuvent se souvenir que vous vous êtes connecté en stockant un cookie. Les cookies sont de petits fichiers stockés sur votre ordinateur qui aident un site web à savoir qui vous êtes, vous et votre ordinateur, sans que vous n'ayez à vous connecter une nouvelle fois lors de vos prochaines visites. Toutefois, ces cookies peuvent également être utilisés pour suivre vos activités lorsque vous naviguez de site web en site web. C'est l'un des moyens utilisés par les publicités pour vous cibler.

Peut-on enregistrer un mot de passe en toute sécurité si l'on est sur notre propre ordinateur ?

Questions aux élèves

Utilisez-vous un identifiant et un mot de passe sur votre ordinateur ?

Que pourrait-il se passer si vous partagiez votre ordinateur avec d'autres personnes ?

1. Dans ce cas, même si dans le champ « Mot de passe », votre mot de passe est sans doute caché par des points noirs ou des astérisques, d'autres personnes utilisant votre ordinateur peuvent potentiellement le découvrir. Ce n'est pas parce que vous ne voyez pas le mot de passe sur votre écran qu'il n'est pas stocké quelque part.

Questions aux élèves

Existe-t-il des situations dans lesquelles il est possible de partager un mot de passe en toute sécurité ? Quand ? Pourquoi ?

1. Par exemple, si leurs parents veulent connaître leurs mots de passe, ou bien s'ils disposent d'un compte joint/compte familial sur un service tel que Netflix.

Partagez-vous vos mots de passe avec quelqu'un ? Si oui, avec qui et pourquoi ?

Si l'un de vos amis les plus proches vous disait « Si je compte pour toi... », est-ce que cela vous inciterait à partager votre mot de passe avec lui ? Pourquoi ? Si non, pourquoi ?

Informations aux élèves

Vous pouvez décider de partager votre mot de passe avec quelqu'un d'important pour vous, mais le fait que cette personne soit importante pour vous ne signifie qu'elle mérite d'avoir un accès complet à vos comptes en ligne.

Réfléchissez bien à la relation que vous entretenez avec cette personne avant de partager vos mots de passe, et notamment à comment votre relation pourrait évoluer dans le temps. Par exemple, ce n'est pas la même chose de partager un mot de passe avec vos parents/tuteurs que de partager un mot de passe avec votre meilleur(e) ami(e).

Questions aux élèves

Que pourrait-il vous arriver si vous partagez un mot de passe ?

1. Quelqu'un pourrait pirater vos comptes bancaires, se faire passer pour vous en ligne ou apprendre certaines choses que vous préfèreriez garder secrètes.

Si vous partagiez le mot de passe d'un compte, utiliseriez-vous ce compte différemment ?

Questions aux élèves

Y a-t-il des choses que vous ne regarderiez pas sur Netflix ou que vous n'écririez pas dans un e-mail si quelqu'un pouvait voir ce que vous faisiez ?

Interaction dans la classe

Les participants doivent réfléchir à leur propre comportement quant à l'utilisation d'un compte partagé. Ils doivent tenir compte du fait que, sur ce compte partagé, leur activité en ligne est à la vue d'autres utilisateurs du compte.

Questions aux élèves

Si votre compte est une représentation virtuelle de vous-même, comme un profil sur un réseau social, est-il bon de permettre à d'autres personnes d'utiliser ce compte ?

Interaction dans la classe

Discutez de la possibilité que quelqu'un se fasse passer pour vous et envoie des messages à vos amis.

Questions aux élèves

Autorisez-vous un de vos appareils à stocker vos mots de passe ? Pourquoi ? Si non, pourquoi ? Cela veut-il dire qu'il est prudent d'enregistrer vos mots de passe sur votre téléphone ou ordinateur personnel ? Que se passerait-il si vous laissiez un ami emprunter votre téléphone ou votre ordinateur ?

Partagez-vous certains appareils avec d'autres personnes, telles que votre famille ou vos amis ? Partagez-vous un compte sur cet appareil, ou chaque personne en possède-t-elle un ?

Vous arrive-t-il d'utiliser un appareil « public », comme ceux présents dans les bibliothèques, les écoles ou autres ? Utilisez-vous cet appareil de la même façon que si vous utilisiez un autre appareil ?

Troisième partie

Interaction dans la classe

Mettez les participants deux par deux.

Informations aux élèves

Discutez avec votre binôme, et racontez s'il vous est déjà arrivé d'utiliser un ordinateur dans votre établissement scolaire, à la bibliothèque ou autre, et de vous apercevoir qu'une personne était toujours connectée sur un réseau social ou sur une adresse e-mail. Demandez aux participants si, dans une telle situation, ils regarderaient le compte ou s'ils feraient autre chose.

Interaction dans la classe

Donnez 5 minutes aux participants pour qu'ils discutent puis demandez-leur de partager leurs réflexions. Encouragez le groupe à discuter de cette utilisation non autorisée.

Accès non autorisé à un compte

Première partie

Interaction dans la classe

Remarque : une partie du contenu de cette activité a été abordée dans l'« Activité n° 1 : Notions de base sur les mots de passe ». À vous de décider si vous souhaitez ou non revoir cette partie.

Informations aux élèves

D'autres personnes peuvent avoir accès à votre compte, et ce, sans même connaître votre mot de passe et sans même avoir réussi à le trouver de façon aléatoire. Si une personne connaît suffisamment d'informations personnelles vous concernant, elle pourrait être en mesure de découvrir votre mot de passe ou de convaincre quelqu'un dans une entreprise de transmettre vos informations. Étant donné que la technologie n'est pas utilisée pour pirater vos comptes, ce genre d'attaques est appelé ingénierie sociale

Questions aux élèves

Levez la main s'il vous est déjà arrivé d'oublier le mot de passe que vous utilisiez sur un site web.

Que se passe-t-il si vous cliquez sur « J'ai oublié mon mot de passe » ?

1. En général, le site web vous demande de répondre à des questions de sécurité ou essaie de vous contacter à l'aide de votre numéro de téléphone ou de votre adresse e-mail.

Citez quelques-unes des questions de sécurité que pose le site web.

1. Expliquez comment des amis ou des connaissances peuvent deviner ces réponses ou répondre à ces questions. Par exemple : le nom de votre animal de compagnie, le nom de jeune fille de votre mère, le nom de votre professeur préféré, le nom de votre meilleur(e) ami(e), le nom de votre équipe sportive préférée.

Qui d'autre pourrait connaître ces informations vous concernant ?

De quelle façon un site web vous contacte-t-il lorsque vous avez oublié un mot de passe ?

Qui pourrait avoir accès à vos points de contact ?

Questions aux élèves

Comment un inconnu pourrait-il découvrir les informations personnelles associées aux réponses des questions de sécurité ?

1. Publications sur les réseaux sociaux, recherches d'informations publiques en ligne, plusieurs tentatives, contacter vos amis, etc.

Citez des exemples de publications sur les réseaux sociaux contenant des informations personnelles.

1. Par exemple, une photo Instagram de votre chat avec son nom en légende, une photo sur laquelle vous avez ajouté un lieu, ou des publications d'anniversaire publiques.

Comment pouvez-vous utiliser Google pour en apprendre plus sur quelqu'un et pirater son mot de passe ?

1. Si un moteur de recherche affiche la photo de classe de troisième de quelqu'un dans le journal en ligne d'un collège, vous pouvez trouver le nom de son professeur.

Deuxième partie

Informations aux élèves

Publier des informations contenant les réponses à vos questions de sécurité peut s'avérer très dangereux. Assurez-vous de choisir des questions de sécurité dont vous êtes le seul à connaître les réponses. Vous pouvez également inventer des réponses aux questions de sécurité, du moment que vous les enregistrez dans un gestionnaire de mots de passe ou qu'elles sont faciles à retenir.

Les sites web peuvent contacter les utilisateurs en utilisant leur numéro de téléphone ou l'adresse e-mail associée à leur compte d'utilisateur. Si un utilisateur oublie son mot de passe, les sites web fournissent souvent un mot de passe temporaire ou un lien hypertexte que l'utilisateur peut utiliser pour réinitialiser leur mot de passe.

Questions aux élèves

Est-ce une façon sécurisée de s'assurer que la personne formulant la demande d'un nouveau mot de passe est bien l'utilisateur ?

Que se passerait-il si vous partagiez l'adresse e-mail associée au compte ?

1. La méthode du lien hypertexte pour réinitialiser le mot de passe est la plupart du temps sans risque. Toutefois, partager un compte ou un mot de passe avec une autre personne vous expose à un risque.

Informations aux élèves

L'ingénierie sociale peut être réalisée par des personnes qui vous contactent directement et qui essaient de vous piéger afin que vous leur communiquiez vos informations. Parfois, elles vous enverront un e-mail en prétendant être quelqu'un d'autre (ex. : un ami, un membre de votre famille ou un employé de banque) et vous demanderont de partager avec eux des informations importantes (telles que votre date de naissance) afin de vérifier votre identité. Elles peuvent également agir de manière plus subtile, par exemple si quelqu'un piratait le compte d'un réseau social de l'un de vos amis et vous envoyait un message (à vous et potentiellement à de nombreuses autres personnes) en vous demandant votre date de naissance ou le lieu où vous avez grandi. Si vous recevez quelconque message étrange de la part d'un ami, essayez d'abord de le contacter (en dehors de cette plate-forme de réseau social) afin de vous assurer que c'est bien lui qui vous a envoyé ce message.

Les attaques qui utilisent des e-mails semblant authentiques sont appelées hameçonnage et vous exposent au risque que quelqu'un usurpe votre identité. Par exemple, un usurpateur d'identité peut obtenir une carte de crédit à votre nom et l'utiliser. Vous pourriez ensuite avoir des difficultés à en obtenir une plus tard.

L'hameçonnage permet au voleur d'usurper votre identité et d'accéder à d'autres informations. Ainsi, il pourrait fouiller dans votre boîte e-mail, envoyer des messages à vos amis en se faisant passer pour vous ou voler votre argent. Ce procédé peut également permettre à l'usurpateur de vous bloquer l'accès au compte en créant un nouveau mot de passe que vous ne connaissez pas.

Exercice

Fiche

Devoir

Demandez aux participants de répondre aux questions suivantes et d'ajouter leurs réponses, sous la forme de textes ou d'illustrations, à la fiche Formation sur les mots de passe.

1. Citez 3 choses que vous avez apprises lors de cette session et que vous appliquerez la prochaine fois que vous créerez un mot de passe.

2. Donnez un exemple de situation où il est n'est pas dangereux de partager votre mot de passe avec quelqu'un d'autre.

3. Citez 3 stratégies que vous pouvez utiliser afin de partager votre mot de passe avec quelqu'un d'autre en toute sécurité.

4. Citez 3 exemples de ce qui pourrait arriver de mal si un mot de passe tombait entre de mauvaises mains.