Authentification

GUIDE DU FORMATEUR

Le présent document sert de guide de référence et de préparation pour le formateur, ainsi que de complément au plan de leçon.

Les connaissances que l'apprenant doit avoir acquises au terme du module se trouvent dans la section « Objectifs d'apprentissage ».

La section « Contexte et détail pour le formateur » contient quant à elle une description du contenu ainsi que des liens vers des références permettant au formateur d'en apprendre plus sur le sujet. Il pourra ainsi mener les discussions et répondre aux questions avec assurance, sans être limité par la matière. Par ailleurs, chaque élément de la section « Contexte et détail pour le formateur » vient étayer une partie du scénario.

Objectifs d'apprentissage

> Comprendre les aspects de sécurité liés à l'authentification et aux mots de passe.

> Savoir choisir un bon mot de passe.

> Savoir créer un mot de passe fort.

Contexte et détail pour le formateur

1 Authentification (Qui suis-je?)

1.1 En bref

Les mots de passe servent à confirmer votre identité lorsque vous êtes en ligne. Les bons mots de passe permettent de vous identifier en tant qu'individu sans que personne ne puisse se faire passer pour vous. Ils sont uniques, aléatoires, longs et confidentiels tout en étant faciles à mémoriser.

1.2 En détail

- Authentification
  - Il se peut que vous deviez vous identifier en tant que la personne unique que vous êtes, que ce soit pour obtenir des services personnalisés ou pour confirmer que vous êtes la seule personne à avoir accès à un service (comme l'accès à votre compte de banque).
    - Vous pouvez prouver votre identité au moyen d'un élément unique, comme une carte, une clé ou une caractéristique biologique (empreinte digitale), ou en connaissant la réponse à une question secrète.
      - Toutes ces méthodes ont des forces et des faiblesses.
  - Authentification à deux facteurs
    - L'authentification à deux facteurs vise à compenser la faiblesse de l'authentification à un facteur en requérant deux éléments indépendants.
      - Il peut s'agir d'un élément physique et de quelque chose que vous savez.
      - Citons comme exemple les cartes intelligentes et les générateurs de numéros d'utilisateur comme SecurID de RSA et Yubikey[1].
      - Vous devez vous identifier de deux façons avant de vous connecter ou d'utiliser un service.
        - Par exemple, lorsque vous retirez de l'argent d'un guichet automatique, vous devez insérer votre carte, puis entrer votre NIP (numéro d'identification personnel).
        - Sur Internet, votre mot de passe est comme votre NIP. Vous seul le connaissez. La méthode d'authentification à deux facteurs combine le mot de passe à un autre élément qui vous est propre, comme un numéro de téléphone ou un dispositif que vous seul possédez.
      - Ainsi, si quelqu'un veut usurper votre identité, il doit faire de même et entrer les mêmes renseignements.

1 Pour en savoir plus, consulter le site <https://nakedsecurity.sophos.com/2014/11/14/understanding-the-options-2fa/>.

- Code SMS
  - Un code est envoyé à votre appareil mobile par messagerie texte (SMS – service de messages courts). Lorsque vous avez reçu le code, vous l'inscrivez à l'endroit prévu à cet effet, puis vous pouvez vous connecter.
- Applications d'authentification
  - Les applications d'authentification agissent de la même façon que les codes SMS. Toutefois, le code ne vous est pas envoyé : il est plutôt généré directement sur votre téléphone intelligent ou votre tablette.

– Mots de passe

- Actuellement, les mots de passe sont la meilleure option pour la plupart des méthodes d'authentification sur Internet[2].
  - On appelle parfois les mots de passe des ***phrases de passe***.
    - Les phrases de passe sont simplement plus longues que les mots de passe.
      - Les mots de passe sont habituellement courts, soit de 6 à 10 caractères.
      - Les phrases de passe, elles, sont habituellement plus longues; elles ont généralement de 20 à 40 caractères, et parfois plus.
  - Ces dernières sont considérées comme plus fiables pour les éléments chiffrés en raison de leur longueur et du fait qu'elles prennent plus de temps à trouver.
  - Les éléments chiffrés passent souvent par des endroits ouverts à tous où les criminels peuvent les copier et tenter de les déchiffrer.
  - L'utilisation d'un très long mot de passe leur complique assurément la tâche.
- Les criminels peuvent obtenir des mots de passe en :
  - recueillant assez de renseignements sur vous pour deviner votre mot de passe;
  - vous piégeant pour que vous révéliez votre nom d'utilisateur ou votre mot de passe;
  - copiant vos mots de passe, par exemple en regardant par-dessus votre épaule ou à l'aide d'un logiciel espion;
  - devinant votre mot de passe au moyen d'un logiciel automatisé;
  - réutilisant des noms d'utilisateur et des mots passe usurpés pour un autre service.

2 Un examen rigoureux de 35 mots de passe en fonction de 25 critères d'évaluation a démontré que les mots de passe sont la meilleure option sur tous les plans.

- Mauvaises habitudes
  - Réutilisation des mots de passe.
    - Nous avons tous de nombreux comptes, et il peut devenir difficile de se souvenir de tous les mots de passe. Parfois, à vouloir nous simplifier la tâche, nous nous mettons en danger[3].
      - La réutilisation des mots de passe a un effet direct sur la sécurité. En effet, une fuite sur un site Web peut compromettre la sécurité sur un autre.
        - Faites attention de ne pas réutiliser des mots de passe pour les comptes importants (compte de banque, courriels, etc.).
        - Ne vous en faites pas trop pour vos comptes qui ont peu de valeur pour un criminel (aucun renseignement personnel, aucune donnée financière).
  - Oubli de mots de passe
    - Vous pouvez inscrire vos mots de passe sur papier à la maison.
      - En consignant vos mots de passe et en les conservant dans un endroit sûr, vous vous donnez de fortes chances de les protéger de la plupart des moyens habituellement utilisés pour les subtiliser.
      - Ce n'est pas une bonne idée de coller vos mots de passe sur votre ordinateur ou sur votre bureau; toutefois, les placer dans un livre quelconque dans un tiroir s'avère une protection plutôt sûre.
      - Sachez que les banques ou les institutions financières pourraient considérer que si vous couchez sur papier votre mot de passe ou le conservez dans un endroit trop évident, vous contribuez à une possible utilisation non autorisée de leur système. Validez auprès de votre institution avant de garder une copie écrite.
    - Il n'est pas suggéré d'écrire ses mots de passe si l'ordinateur est partagé ou si des inconnus ont accès à l'ordinateur ou au bureau.
  - Mots de passe faibles ou mauvais
    - Les experts en informatique aiment mettre en garde les gens contre les mots de passe faibles ou mauvais.
      - Un mot de passe faible est un mot de passe qu'une personne ou une machine peut facilement deviner.

3 Beaucoup compensent leur grand nombre de comptes en réutilisant le même mot de passe, parfois légèrement modifié. Par exemple, selon une étude de télémesure de 2007, une personne moyenne a 25 comptes protégés par mot de passe, mais seulement 6 mots de passe différents.

- Voici quelques exemples :
    - Noms de membres de la famille ou d'animaux de compagnie, ou des dates significatives.
        - Par exemple, felix56 est un mauvais mot de passe, car tout le monde sait que le nom de votre chat est Félix et que votre année de naissance est 1956.
    - Formulation facile à taper.
        - Par exemple, 1234, 123456, aaaa, qwerty sont tous des mots de passe très évidents; ils figurent sur la liste des mots de passe utilisée par les programmes automatisés des cybercriminels.
    - Courtes phrases ou mots communs.
        - Par exemple, motdepasse, jetaime, Mississippi et anticonstitutionnellement se trouvent tous dans le dictionnaire; ils figurent aussi sur la liste des mots de passe utilisée pour les programmes automatisés des cybercriminels.
    - Mots de passe semblables.
        - Même si vous n'utilisez pas exactement le même mot de passe, les criminels peuvent deviner les petites modifications que vous apportez.
        - Par exemple, changer le numéro à la fin de votre mot de passe n'est pas aussi sécuritaire que d'utiliser un tout nouveau mot de passe.
    - Les mots de passe sont le plus souvent trouvés à l'aide de programmes informatiques. Rappelez-vous qu'il est plus facile de déjouer l'être humain que l'ordinateur, car ce qui semble complexe pour l'un ne l'est pas nécessairement pour l'autre.
    - Les mots difficiles à épeler ne sont pas plus sûrs.
    - Les mots rares ou obscurs ne sont pas plus sûrs eux non plus.
    - Il en va de même pour les mots que personne n'associerait avec vous.
    - Un programme aura plus de difficultés à trouver un mot mal écrit.

- Il sera plus ardu pour un programme de trouver une combinaison aléatoire de mots (sans structure de phrase).
    - Il n'est pas évident de donner un exemple d'un bon mot de passe, car ils sont tous uniques, aléatoires et confidentiels. Une fois qu'un mot de passe est partagé, il n'est plus secret et devient alors un mauvais mot de passe.

- Voici les critères pour avoir un bon mot de passe :
    - Complexité : plus il y a de types de caractères (lettres, majuscules, chiffres, signe de ponctuation), meilleur est le mot de passe.
    - Unicité : la probabilité que la même combinaison de caractères ne soit pas utilisée ailleurs.
    - Caractère aléatoire : la probabilité que la combinaison de caractères ne se reproduise pas ailleurs.
    - Prédictibilité : la difficulté de deviner le mot de passe même en tentant presque toutes les combinaisons possibles (principalement en raison de sa longueur).
    - Mémorabilité : la facilité avec laquelle on se souvient du mot de passe.
    - Convivialité : la capacité d'inscrire le mot de passe au moyen des touches du clavier.
        - Malheureusement, les deux derniers critères sont entravés par les autres.
        - Il faut trouver l'équilibre entre les différents critères pour avoir un mot de passe fort dont on se souvient.

1.3 En pratique

Pensez à l'authentification à deux facteurs.

Pensez sécurité au moment de choisir vos mots de passe.

2 Mots de passe mnémoniques

2.1 En bref

Les phrases peuvent être plus faciles à mémoriser que les mots de passe complexes. Tirez-en avantage en vous servant d'une phrase pour vous souvenir d'un mot de passe.

2.2 En détail

- Mnémonique (aide-mémoire)
    - Choisissez un mot de passe difficile à deviner, mais que vous mémoriserez aisément en abrégeant une phrase facile à retenir.
        - Trouvez une phrase ou un segment de phrase d'au moins 10 mots. Peu importe la phrase, il faut seulement qu'elle soit facile à retenir.
        - Une phrase inconnue ou unique est plus sûre.
        - Choisissez une lettre, un chiffre ou un caractère spécial pour représenter chaque

mot du mot de passe. La méthode la plus fréquente est de prendre la première lettre de chaque mot.

- Idéalement, choisissez un mélange de lettres minuscules et majuscules, de chiffres, de signes de ponctuation et de caractères spéciaux (comme ^ ou %).
- Placez les signes de ponctuation à des endroits stratégiques et faciles à mémoriser. Par exemple, utilisez & plutôt que et ainsi que le signe ? s'il y a une question. Vous pouvez aussi substituer des lettres par des chiffres (E = 3) ou constituer des mots à l'aide de chiffres et de syllabes (1tel).
- Mémorisez la phrase.

– Vous pouvez élaborer votre propre méthode, pourvu que vous ne l'oubliiez pas.

- Exemples :

Phrase	***Mot de passe***
Derek et moi irons skier cet hiver.	D&mis7h.
Heureux d'un printemps qui me chauffe la couenne.	Hd'1pqmClc.
Je ne le dirai pas deux fois.	JnLdp2x.JnLdp2x.

2.3 En pratique

Utilisez la mnémonique pour créer des mots de passe forts faciles à mémoriser.

3 La méthode Diceware

3.1 En bref

La méthode Diceware consiste à créer un mot de passe aléatoire, unique, long et facile à mémoriser à partir de mots tirés d'une liste grâce à des lancers de dés.

3.2 En détail

– Les mots de passe longs sont plus sûrs que les courts.

– Une longue phrase tirée d'un livre ou d'une chanson est facile à mémoriser, mais aussi à deviner, car elle suit certaines règles (grammaire, syntaxe).

– Le mieux serait une très longue suite de lettres aléatoires, mais il serait très difficile de s'en souvenir.

– Une suite de mots aléatoires est aussi très longue et difficile à trouver.

– Les suites de lettres générées par ordinateur ne sont pas totalement aléatoires, car les programmes fonctionnent selon des règles qui peuvent être copiées.

- Les êtres humains ne peuvent pas faire de listes totalement aléatoires non plus, car ils tendent à être prévisibles quand ils essaient de ne pas l'être.
- Les dés, quant à eux, ont été conçus pour être aléatoires, et ils fonctionnent vraiment bien.
- La méthode Diceware permet de créer des phrases de passe de façon totalement aléatoire au moyen de dés et d'une liste de mots.
    - La phrase ainsi obtenue est difficile à deviner, car elle ne suit aucune règle grammaticale ou syntaxique.
    - La liste Diceware associe des mots à des nombres. En voici un extrait :

16655 clause	16656 claw
16661 clay	16662 clean
16663 clear	16664 cleat
16665 cleft	16666 clerk
21111 cliche	21112 click
21113 cliff	21114 climb
21115 clime	21116 cling
21121 clink	21122 clint
21123 clio	21124 clip
21125 clive	21126 cloak
21131 clock	

    - Pour utiliser la méthode Diceware :
        - Téléchargez, puis sauvegardez la liste Diceware[4] ou la liste Beale[5]. Imprimez-la au besoin.
        - Déterminez le nombre de mots qui figureront dans la phrase de passe (quatre, cinq, six ou plus). Plus il y a de mots, meilleure est la phrase.
        - Lancez le dé, puis notez le résultat. Écrivez les chiffres en groupe de cinq.
            - Faites autant de groupes que le nombre de mots voulu.
            - Lancez un dé à la fois ou cinq dés d'un coup, peu importe.
            - Si cinq dés sont lancés en même temps, notez les chiffres de gauche à droite.

4 Sur Internet : <http://world.std.com/%7Ereinhold/dicewarewordlist.pdf>.
5 Sur Internet : <http://world.std.com/%7Ereinhold/beale.wordlist.asc>.

- Recherchez chaque suite de cinq chiffres dans la liste Diceware, puis notez les mots qui y sont associés. Par exemple, la combinaison 21124 donnera le mot clip (voir la liste ci-dessus).

- Les mots ainsi trouvés formeront la phrase de passe.

    - Certaines personnes tentent de faire des liens entre les mots de la phrase pour la mémoriser plus facilement.
    - Il n'y a aucun risque à consigner la phrase de passe et à la conserver dans un endroit sûr[6].

        - Exemples de phrases de passe générées par la méthode Diceware :

            - Les lancers de dés 36424, 51644, 64134, 54236 donnent leekricowhiteskat.
            - Les lancers de dés 33142, 53132, 14323, 65622, 53112, 56456 donnent nscaldblatz64savetardy.

3.3 En pratique

Servez-vous de la méthode Diceware pour créer des mots de passe longs et faciles à mémoriser.

4 Gestionnaires de mots de passe

4.1 En bref

Les gestionnaires de mots de passe sont des programmes informatiques qui servent à retenir vos mots de passe.

4.2 En détail

- Le gestionnaire de mots de passe est l'une des solutions aux problèmes liés aux mots de passe.

    - Il s'agit d'un programme qui gère vos mots de passe pour vous.

        - Il permet de n'avoir qu'un mot de passe pour accéder à tous les autres.
        - Le programme peut fonctionner au moyen d'un mot de passe facile à mémoriser qui en débloque de plus forts.
        - Il peut aussi générer des mots de passe pour un site Web donné en fonction du nom de domaine dudit site (protection contre l'hameçonnage).

- Les gestionnaires de mots de passe se trouvent sous différentes formes d'applications autonomes (mot de passe de site Web, module d'extension de navigateur, signapplets).

- Comme toujours, procurez-vous ces applications sur des sites dignes de confiance comme ceux des fournisseurs connus, l'iTunes Store ou Google Play pour éviter de télécharger des

6 Pour en savoir plus, consulter le site <http://world.std.com/~reinhold/diceware.html>.

logiciels inefficaces ou des programmes malveillants. Certaines banques et institutions financières pourraient considérer que l'utilisation de gestionnaires de mots de passe équivaut à inscrire son mot de passe sur papier et contribue à une utilisation non autorisée de leur système. Validez auprès de votre institution avant d'utiliser un gestionnaire de mots de passe.

- Les gestionnaires de mots de passe ne sont pas très mobiles.
  - Il se pourrait que vous n'y ayez pas accès sur un appareil alors que vous en avez besoin. Le cas échéant, vous devrez tenter de vous souvenir du mot de passe en question ou d'attendre pour vous connecter.
- Il y a cependant une solution à ce problème : les gestionnaires de mots de passe infonuagiques.
  - Ils sont plus accessibles.
  - Ils sont moins sécuritaires, vu que les mots de passe sont stockés dans le nuage.

4.3 En pratique

Servez-vous d'un gestionnaire de mots de passe si vous devez vous connecter à de nombreux comptes fréquemment.

Glossaire

Authentification à deux facteurs	Identification d'une personne au moyen de deux éléments indépendants.
Carte intelligente	Carte dotée d'une puce.
Chiffrement	Processus de conversion de l'information en format illisible par les entités non sécurisées, mais lisible par le destinataire désigné.
Code SMS	Code envoyé par messagerie texte (SMS – service de messages courts) à un appareil mobile dans le cadre d'un processus d'identification.
Gestionnaire de mots de passe	Application facilitant la gestion des mots de passe.
Hameçonnage	Pratique frauduleuse ou procédé consistant à se faire passer pour une entreprise de confiance afin de convaincre une personne de donner ses renseignements personnels.
Méthode Diceware	Méthode consistant à créer de longues phrases de passe aléatoires au moyen de dés et d'une liste de mots.
Mnémonique	Système, agencement d'idées ou associations aidant à se souvenir de quelque chose.
Mot de passe	Mot connu d'une seule personne servant à l'identification de celle-ci.
NIP	Numéro d'identification personnel; code secret servant à identifier une personne, le plus souvent utilisé pour les transactions bancaires.
Nom d'utilisateur	Nom unique donné à un système informatique ou à un utilisateur. Jumelé à un mot de passe, il sert à identifier une personne.
Phrase de passe	Phrase connue d'une seule personne servant à l'identification de celle-ci.