Sécurité et confidentialité

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

> Savoir ce qu'est un logiciel de sécurité.

> Comprendre pourquoi il faut couvrir la caméra de l'ordinateur.

> Savoir configurer les paramètres de sécurité et de confidentialité des différents appareils.

Contexte et détail pour le formateur

1 Configuration des paramètres de sécurité et de confidentialité

1.1 En bref

Par mesure de sécurité, il est important de configurer les mots de passe, d'activer les pare-feu et de vérifier les paramètres de confidentialité de votre ordinateur.

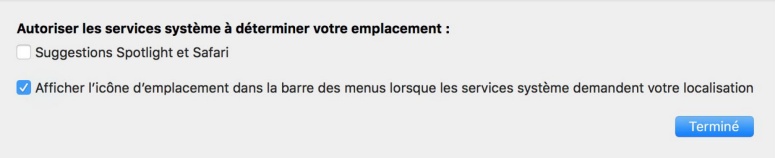
1.2 En détail

- Mot de passe
  - Verrouillez votre ordinateur par un mot de passe, même si vous êtes le seul à l'utiliser.
    - Les mots de passe fournissent un degré minimal d'imputabilité et peuvent empêcher les autres de voir et d'utiliser vos données si votre ordinateur était perdu ou volé.
    - Un bon mot de passe doit être complexe, long, unique et aussi facile à mémoriser que possible. Pour en savoir plus sur les mots de passe, reportez-vous à la leçon sur l'authentification.
  - Modification du mot de passe
    - Apple: Go to ***Apple menu*** at the top left of screen, then ***System Preferences*** > ***Users & groups*** > Click ***Change password.***
    - Windows: Go to ***Control panel*** > ***user accounts and family safety*** > ***Change password.***
- Pare-feu (barrière de sécurité entre l'ordinateur et le réseau, aussi appelée « coupe-feu »)
  - Activation du pare-feu de l'ordinateur[1]
    - Apple : Ouvrez le menu ***Apple*** dans le coin supérieur gauche de l'écran, puis sélectionnez ***Préférences Système*** > ***Utilisateurs et groupes*** > ***Modifier le mot de passe***.
    - Windows : Dans le ***Panneau de configuration***, sélectionnez ***Comptes d'utilisateurs et contrôle parental*** > ***Modifier le mot de passe***[2].
- Paramètres de confidentialité
  - Souvent, les appareils connectés à Internet communiquent avec des services externes.
    - Dans certains cas, la communication peut prendre des proportions imprévues ou inutiles.

1 Pour en savoir plus sur les pare-feu de Windows, consulter le site : <http://windows.microsoft.com/fr-ca/windows-8/Windows-Firewall-from-start-to-finish>.

2 Sur Internet : <http://windows.microsoft.com/fr-ca/windows-10/turn-windows-firewall-on-or-off>.

- Vérifiez si le système d'exploitation transmet plus de données que vous le souhaiteriez.
- Il s'agit d'un équilibre entre fonctionnalités et vie privée. Vous êtes la seule personne à savoir ce que vous êtes à l'aise de partager ou sacrifier en échange de fonctionnalités. Il est important de faire vos propres choix et de ne pas simplement vous fier aux paramètres par défaut du fabricant.
  - Tous les ordinateurs Apple et Windows possèdent des paramètres réglables qui contrôlent la quantité de données transmises par Internet.
  - Pour renforcer les paramètres de confidentialité (tout en perdant certaines fonctionnalités) :
    - Apple
      - Ouvrez le menu ***Apple*** dans le coin supérieur gauche de l'écran, puis sélectionnez ***Préférences Système*** > ***Spotlight*** > ***Résultats de la recherche***, et décochez les cases ***Suggestions Spotlight*** et ***Résultats Bing***.
      - Retournez dans ***Préférences Système*** > ***Sécurité et confidentialité***, puis cliquez sur ***Confidentialité***.
      - Ouvrez les services de localisation.
      - Sélectionnez les applications qui peuvent accéder à vos données de localisation.
        - Si vous ne voulez pas que l'information s'ajuste automatiquement selon votre emplacement, décochez-les toutes.
        - Vous pouvez préciser votre emplacement manuellement pour les applications météo.
        - Si vous choisissez de laisser certaines applications utiliser vos données de localisation automatiquement, décochez les autres cases, cliquez sur ***Services système*** et décochez l'option ***Suggestions Safari et Spotlight***.



      - Désactivez les recherches Web automatiques.
        - Rendez-vous dans ***Préférences Système*** > ***Spotlight*** > ***Résultats de la recherche***, et décochez les cases ***Suggestions Spotlight et Résultats Bing***.

- Windows[3]
  - Rendez-vous dans ***Paramètres*** > ***Confidentialité*** > ***Général***.
    - Désactivez l'option ***Laisser les applications utiliser mon identifiant de publicité***.
    - Activez le filtre ***SmartScreen*** (fonction permettant de bloquer certains sites malveillants connus).
    - Désactivez l'option d'envoi des données d'écriture à Microsoft.
    - Si vous parlez d'autres langues, vous pouvez autoriser les sites Web à accéder à votre liste de langues pour fournir du contenu local. Sinon, désactivez cette option.
  - Désactivez Cortana.
    - Dans le menu ***Démarrer***, commencez à entrer un mot, puis cliquez sur le carnet dans le volet gauche et sélectionnez ***Paramètres***. Désactivez Cortana.
    - Lorsque vous désactivez Cortana, l'option ***Rechercher en ligne et inclure les résultats web*** s'affiche. Désactivez-la.
  - Rendez-vous dans ***Paramètres*** > ***Confidentialité*** > ***Voix, entrée manuscrite et frappe***.
    - Cliquez sur ***Arrêter*** de me connaître pour désactiver l'option ***Apprendre à me connaître***.
- Microsoft Edge (nouveau navigateur de Windows 10)
  - Comme la plupart des navigateurs modernes (notamment Chrome et Firefox), Edge comprend des fonctions de rappel périodique. Vous les trouverez dans ***Paramètres*** > ***Paramètres avancés*** :
    - ***Autoriser Cortana à m'aider dans Microsoft Edge*** enregistre votre historique de navigation pour pouvoir s'y référer lorsque vous posez des questions à Cortana. Vous pouvez désactiver cette fonction dans les paramètres avancés de Microsoft Edge.
    - ***Afficher les suggestions de recherche à mesure que je tape*** permet à Microsoft Edge d'enregistrer vos frappes pour vous suggérer des recherches à mesure que vous tapez. Vous pouvez aussi ***désactiver*** cette fonction.
    - ***Me protéger contre les sites et téléchargements malveillants avec le filtre SmartScreen***. Laissez cette fonction activée.
  - Dans ***Paramètres*** > ***Confidentialité*** > ***Commentaires & diagnostics***, il y a deux paramètres :

3 Pour en savoir plus sur les paramètres de confidentialité de Windows, consulter le site : <https://www.microsoft.com/fr-fr/security/default.aspx>.

- **_Fréquence des commentaires_** : Changez-le pour **_Jamais_**.
- **_Données de diagnostic et d'utilisation_** : Changez-le pour **_De Base_**.

- Localisation
  - Rendez-vous dans **_Paramètres_** > **_Confidentialité_** > **_Emplacement_**. Si vous prévoyez vous déplacer souvent avec votre ordinateur et désirez que certaines applications se mettent à jour automatiquement, comme la météo, sélectionnez-les. Autrement, décochez-les.

- Verrouillage de l'écran des appareils mobiles
  - Il est très important de verrouiller l'écran des appareils mobiles. Cette mesure fournit un degré minimal d'imputabilité. Si vous perdez votre téléphone, il sera plus difficile pour les autres d'accéder à vos données et à vos services.
  - Si possible, utilisez un mot de passe composé de lettres et de chiffres.
  - Il peut aussi être avisé d'utiliser la fonction de balayage des empreintes digitales. Si vous choisissez un schéma, évitez les formes simples, comme les L, les triangles et les carrés. Nettoyez souvent l'écran pour effacer les traces de votre schéma sur l'écran. Si vous utilisez un code à quatre chiffres, évitez les séquences évidentes, comme 1234, 0000, 2580, 1111, 5555, 5683, 0852, 1212 ou votre date de naissance. Ce ne sont pas de bons mots de passe[4].

- iPhone
  - Sur les appareils dotés de Touch ID (un capteur d'empreinte digitale), rendez-vous dans **_Réglages_** > **_Touch ID et code_** et configurez votre code. Il peut aussi être pratique de configurer Touch ID pour le déverrouillage du téléphone. Vous n'avez qu'à suivre les instructions après avoir sélectionné l'option.
  - Sur les appareils qui ne sont pas dotés de Touch ID, rendez-vous dans **_Réglages_** > **_Code_** et sélectionnez **_Activer le code_**[5].

- Android
  - Ouvrez les **_Paramètres_** de votre appareil, puis faites défiler les options et sélectionnez **_Sécurité_** > **_Verrouillage de l'écran_**.
    - Si vous avez déjà configuré le verrouillage, entrez le schéma, le NIP ou le mot de passe avant de choisir un verrouillage différent.
    - Sélectionnez le type de verrouillage que vous désirez et suivez les instructions[6].

4 Pour obtenir une explication technique, consulter le site : <http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes>.
5 Sur Internet : <https://support.apple.com/fr-ca/HT204060>.
6 Sur Internet : <https://support.google.com/nexus/answer/2819522?hl=fr>.

1.3 En pratique

Configurez les mots de passe, activez les paramètres de sécurité et vérifiez les paramètres de confidentialité de votre ordinateur et de vos appareils mobiles.

2 Logiciels de sécurité

2.1 En bref

Comme leur nom l'indique, les logiciels de sécurité aident à gérer la sécurité. Ils sont vendus sous forme d'abonnements renouvelables régulièrement. Il est recommandé d'opter pour un antivirus combiné à un logiciel de surveillance active.

2.2 En détail

- Les logiciels de sécurité sont conçus pour vous protéger des programmes malveillants.
  - Mais comme le verrou sur la porte ou les barreaux à la fenêtre, ils ne peuvent garantir votre sécurité.
  - Aucun logiciel de sécurité n'offre une protection absolue.
    - Ils ne remplacent pas non plus la prudence. Le sac gonflable de votre voiture ne vous empêchera pas d'avoir un accident, et il ne vous sera d'aucune utilité si vous ne portez pas votre ceinture.
    - Il peut toutefois empêcher un petit incident de dégénérer en accident grave.
  - Les logiciels de sécurité sont très importants, mais ne doivent représenter qu'une partie de votre plan de sécurité.
- Les détaillants d'appareils électroniques et de fournitures de bureau offrent souvent un grand choix de logiciels de sécurité.
  - Il n'est pas possible de recommander un produit spécifique, mais il existe une liste de ce qu'il ne faut pas acheter. De nombreuses applications prétendent être des antivirus, mais ne sont en réalité que des arnaques ou des virus eux-mêmes[7].
  - Lorsque vous achetez un logiciel de sécurité, vous achetez à la fois un produit et un service.
    - Sur Internet, les menaces et les programmes malveillants changent sans cesse. Votre logiciel de sécurité doit donc être capable de s'adapter pour bien vous protéger.
      - L'entreprise qui vous vend le logiciel de sécurité doit le mettre à jour constamment.
    - Les modalités d'abonnement varient d'un produit à l'autre.

7 La liste complète est accessible sur le site : <http://asafercomputer.co.uk/?q=Library>.

- Informez-vous de la durée de l'abonnement et du nombre d'appareils protégés.
  - Souvent, l'abonnement doit être renouvelé chaque année.
  - Tenez votre abonnement à jour pour rester protégé contre les menaces courantes.

- Les logiciels de sécurité peuvent nuire à la performance de votre ordinateur.
  - La raison est simple : ils lisent tous les fichiers que vous ouvrez pour vérifier qu'ils sont sécuritaires.
    - Il n'y a aucun moyen d'éviter cette réduction de la performance.
      - Les fournisseurs de logiciels travaillent très fort pour réduire l'effet de leurs logiciels sur la performance.
      - La plupart des logiciels de sécurité populaires (ceux qui sont vendus en magasin) ne réduisent que légèrement la performance[8].
      - Si votre ordinateur est beaucoup plus lent après l'installation d'un nouveau logiciel de sécurité, ce peut être pour l'une des raisons suivantes :
        - l'ancien logiciel n'a pas été désinstallé;
        - il n'y a pas suffisamment d'espace libre sur le disque dur (l'ordinateur a besoin d'environ 20 % d'espace libre pour fonctionner);
        - le logiciel doit être mis à jour;
        - il y a trop de logiciels ouverts simultanément;
        - l'ordinateur est simplement trop vieux pour exécuter les logiciels modernes (vérifiez toujours les exigences système avant d'acheter un logiciel).
- « Plus » n'est pas nécessairement synonyme de « meilleur ».
  - Il ne devrait toujours y avoir qu'un seul logiciel de sécurité installé sur votre ordinateur.
    - L'exécution simultanée de plusieurs logiciels peut causer des conflits entraînant un ralentissement ou un dysfonctionnement de l'ordinateur.
- Évaluez le degré d'intrusion du logiciel.
  - Certains logiciels passent leur temps à confirmer qu'ils fonctionnent; d'autres travaillent discrètement en arrière-plan sans jamais se manifester. Il s'agit d'un choix personnel.
    - Cet aspect peut être personnalisé sur la plupart des logiciels de sécurité populaires.
- Évaluez les fonctions du logiciel.

8 Pour voir une comparaison de la performance, consulter le site : <http://www.av-comparatives.org/wp-content/uploads/2015/11/avc_per_201510_en.pdf>. Notez que « plus rapide » ne veut pas dire « plus efficace ».

- Il peut être difficile de s'y retrouver avec tout le jargon marketing et les graphiques tape-à-l'œil. On peut tout de même classer les fonctions comme suit :

Ce que c'est	***Autres appellations***	***Ce que ça fait***
Outil de sécurité réseau	Pare-feu, système de détection d'intrusion, système de protection contre l'intrusion	Repère et interrompt le mauvais trafic sur le réseau (transmission de données par un programme malveillant)
Système de détection active	Protecteur de messagerie instantanée, filtre antipourriel, système de détection antihameçonnage, bloqueur de publicité, filtre de confidentialité	Détecte et bloque les codes de programme malveillants dans les applications utilisées
Filtre de contenu	Contrôle parental	Limite l'utilisation de l'ordinateur aux sites Web sécuritaires
Antivirus	Anti-programmes malveillants (virus, etc.), Windows Defender et sécurité Apple	Examine les fichiers lorsqu'ils sont utilisés et balaie régulièrement tous les fichiers pour déterminer s'ils exécutent des actions indésirables ou non autorisées sur l'ordinateur
Système de suppression sécurisée	Destructeur de données	Supprime les fichiers de façon à ce qu'ils ne puissent pas être récupérés
Réseau et anonymat	Réseau privé virtuel (RPV ou VPN)	Fournit une connexion plus sécurisée sans divulguer votre emplacement

- Choisissez un service de sécurité comprenant au moins un antivirus et un système de détection active.
  - Les ordinateurs fonctionnant sous Windows 8 ou une version plus récente et les ordinateurs Apple offrent un certain degré de protection intégrée.
    - Ces applications ne sont pas dédiées à la sécurité, alors elles n'offrent pas nécessairement le même degré de sécurité ni les mêmes possibilités de personnalisation des alertes et des notifications qu'une application spécialisée.
- Soyez conscient qu'il y a des arnaqueurs. Microsoft ne vous appellera jamais. Les fournisseurs de logiciels de sécurité authentiques non plus.

> ***L'arnaque du technicien Microsoft ou Windows.***
>
> Les arnaqueurs peuvent appeler des gens en se faisant passer pour le représentant d'une entreprise bien connue, comme Microsoft ou Apple, et prétendre que l'ordinateur transmet des virus ou a été piraté et qu'il doit être nettoyé. L'arnaqueur obtient ainsi un accès à l'ordinateur à distance et peut exécuter des programmes ou modifier des paramètres. Il explique ensuite à la personne qu'elle doit payer des frais pour le service et lui demande un numéro de carte de crédit. Dans certains cas, l'arnaqueur fait un virement à partir de l'ordinateur de la victime au moyen d'un service bancaire comme Western Union ou MoneyGram. La victime se retrouve alors à payer pour un service dont elle n'avait pas besoin puisque son ordinateur n'était pas infecté[9].
>
> Si vous recevez ce genre d'appel, ne fournissez aucun renseignement à votre interlocuteur. Raccrochez. Vous pouvez ensuite signaler l'incident au Centre antifraude du Canada en composant le 1 888 495-8501 ou en vous rendant sur le site : http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-fra.htm

2.3 En pratique

Installez un logiciel de sécurité pour protéger votre ordinateur.

Tenez votre abonnement à jour.

3 Couverture de la caméra Web

3.1 En bref

Couvrez votre caméra Web pour éviter d'être espionné.

3.2 En détail

- Il se peut qu'un attaquant accède à votre ordinateur à distance à votre insu[10].
  - Certains programmes malveillants, appelés « cheval de Troie »[11], sont conçus pour donner secrètement accès à votre ordinateur à d'autres personnes. Un criminel peut vous amener à installer le programme malveillant en le dissimulant dans un autre fichier ou programme ou en vous invitant à cliquer sur un lien ou à visiter un site Web frauduleux. Il peut ensuite voir tout ce que vous faites sur votre ordinateur, accéder à vos fichiers et activer la caméra et le micro.
    - Couvrir la caméra garantit que personne ne pourra vous voir à la maison et assure un minimum de vie privée.
- Il est facile de couvrir la caméra.
  - Vous n'avez qu'à coller un morceau de papier sur la lentille et à la retirer seulement lorsque vous utilisez vraiment la caméra.

---

9 Bureau de la concurrence du Canada. Le petit livre noir de la fraude (en ligne), p. 24. Sur Internet : <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/Little-Black-Book-Scams-f.pdf/$FILE/Little-Black-Book-Scams-f.pdf>.

10 Sur Internet : <http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/Thompson2005_CACM48_8_Spyware.pdf>.

11 Sur Internet : <http://www.trusteer.com/en/glossary/remote-access-trojan-rat>.

- Vous pouvez aussi utiliser les petits autocollants que l'on retrouve sur les bananes et les autres fruits et légumes. Ils n'endommagent pas les lentilles et sont faciles à retirer.

- Il est possible d'acheter des couvercles plus jolis, mais le résultat sera le même qu'avec un morceau de papier ou un autocollant.

3.3 En pratique

Couvrez votre caméra Web.

Glossaire

Arnaque (scam)	Procédé malhonnête ou trompeur créé à des fins criminelles.
Arnaqueur (scammer)	Une personne procédant à des escroqueries (scams).
Caméra Web	Caméra vidéo compatible avec Internet.
Cortana	Assistant personnel de Windows à commandes vocales.
Pare-feu	Barrière de sécurité entre des réseaux ou entre un ordinateur et un réseau.
Programme malveillant	Logiciel créé dans un mauvais dessein.
Verrouillage de l'écran	Barrière prévenant l'accès aux fonctions d'un appareil tactile par le blocage de l'écran.