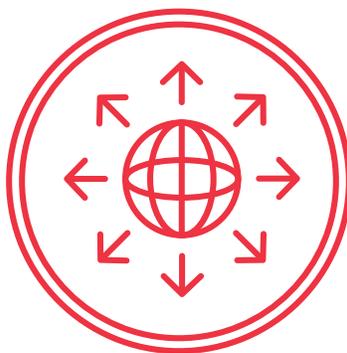


# Naviguer sur le Web



## 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

- > Connaître les risques de la navigation sur le Web.
- > Connaître les éléments à surveiller dans le navigateur.
- > Savoir configurer les paramètres d'un navigateur.



## Contexte et détail pour le formateur

### 1 Risques de la navigation sur le Web

#### 1.1 En bref

La publicité, le ciblage, les téléchargements furtifs, les attaques de l'homme du milieu, le typosquattage et l'hameçonnage sont tous des procédés qui comportent des dangers dont nous devons nous méfier en ligne.

#### 1.2 En détail

Internet regorge de menaces, lesquelles peuvent prendre plusieurs formes. Le simple fait d'en connaître les plus communes peut aider à éviter des dangers et, plus important encore, à en atténuer les conséquences.

- Publicité
  - Les sites de publication de moyenne et grande importance (comme Facebook et Google), que nous appellerons plateformes ci-après, sont capables de rassembler et d'analyser une quantité impressionnante de données très rapidement, ce qui leur permet de personnaliser la publicité en fonction de chaque utilisateur.
  - Les annonceurs peuvent acheter de la publicité sous forme d'enchères où le prix est déterminé en fonction des similitudes entre la page Web et la publicité, de votre emplacement, de votre historique de navigation et des renseignements que vous avez fournis à la plateforme ou à ses partenaires, par exemple dans des formulaires d'inscription ou dans ce que vous avez publié sur les réseaux sociaux.
  - Ces nouvelles façons d'afficher de la publicité incitent davantage les agences à recueillir des renseignements personnels sur les consommateurs et à s'en servir efficacement. Cet aspect a soulevé des questionnements chez les organismes de réglementation et les consommateurs concernant les effets négatifs que pourraient avoir ces pratiques.
    - Parmi les conséquences potentielles, notons la violation de la vie privée, l'utilisation frauduleuse de renseignements personnels, le ciblage comportemental et la modification des prix.
  - Depuis que la publicité en ligne a gagné en popularité, les criminels ont commencé à s'y intéresser.
    - La publicité malveillante consiste à diffuser un programme malveillant en utilisant les publicités.
      - Elle peut avoir de graves conséquences. En effet, l'attaquant peut se servir de sites Web populaires pour que son programme malveillant puisse atteindre un très grand nombre de personnes.
      - De plus, les internautes peuvent être vulnérables au risque s'ils ne savent pas qu'ils peuvent se buter à du contenu malveillant sur des sites dignes de confiance.



- Ciblage
  - Les services de tiers en ligne apportent une grande valeur au Web. Ils permettent de doter les sites Web de bandeaux publicitaires et de compteur de visiteurs, d'intégrer la publicité aux réseaux sociaux, et bien plus encore.
  - Ils suscitent toutefois des questionnements quant à la protection de la vie privée.
  - Les fournisseurs de services tiers donnent la possibilité aux annonceurs de surveiller vos habitudes de navigation à partir de nombreux sites, puis d'adapter la publicité en conséquence.
    - Les publicités personnalisées sont considérées comme l'avenir de la publicité en ligne; elles représentent d'ailleurs déjà une grande partie de ce marché mondial.
      - Les publicités semblent donc plus pertinentes aux yeux des utilisateurs, et les propriétaires de sites Web, eux, en retirent de plus gros revenus.
      - Ce type de publicité suscite des questionnements quant à l'utilisation de tierces parties pour faire le suivi et la collecte de données personnelles.
      - Il est possible que les internautes ne sachent pas de quelle façon ils sont surveillés d'un site à l'autre et ne connaissent pas les répercussions sur leur vie privée ni les modalités de l'entente de service avec le fournisseur tiers.
- Téléchargements furtifs
  - Votre ordinateur peut se faire infecter par un téléchargement furtif sur une page Web quelconque.
    - Dans un tel cas, la page comporte une programmation malveillante qui profite de n'importe quelle vulnérabilité de votre ordinateur, par exemple dans le navigateur ou le système d'exploitation, pour effectuer des opérations malveillantes ou encore installer d'autres programmes malveillants.
      - Vous pourriez même ne pas vous en rendre compte.
      - Ces pages Web peuvent être créées par des criminels ou être des pages authentiques qui ont été attaquées.
      - Toutefois, 99 % des pages Web sont sûres.
- Typosquattage
  - Le typosquattage consiste à enregistrer un nom de domaine graphiquement apparenté à une marque connue afin de tirer avantage des fautes de frappe faites par les internautes.
  - La simplicité et le faible coût de l'enregistrement d'un nom de domaine encouragent les spéculateurs à enregistrer des noms de domaine en lot pour pouvoir utiliser les publicités afin de rediriger les internautes vers des pages de tiers, pour créer des sites d'hameçonnage ou pour diffuser des programmes malveillants.
  - Très peu de propriétaires de sites Web se protègent en s'appropriant ce type de nom de domaine avant que des typosquatteurs ne le fassent.
  - Les typosquatteurs ciblent tous les sites, pas seulement les plus populaires.



- Voici un exemple de typosquattage à partir du nom de domaine hypothétique **exemple.com** :

<i>Adresse URL typosquattée</i>	<i>Type d'erreur</i>	
xemple.com, exemlpe.com, xample.com	Faute de frappe	MISE EN GARDE : Ne visitez aucun de ces sites. Certains contiennent des programmes malveillants.
example.org, example.biz, example.info, example.ca	Domaine différent (suffixe)	
example.cm	Domaine semblable (suffixe)	

- Attaque de l'homme du milieu

- Dans une attaque de l'homme du milieu, l'attaquant lit ou altère des communications en ligne en les interceptant entre l'expéditeur et le destinataire prévu. Voici des attaques de ce type et leurs conséquences possibles :
  - Reniflage
    - Le reniflage, ou l'écoute clandestine, consiste à intercepter des communications en circulation et à y recueillir des renseignements.
    - La plupart du temps, on utilise le reniflage pour subtiliser des données dans des textes en clair, soit des données non chiffrées.
  - Programme malveillant
    - Les programmes malveillants peuvent s'immiscer de diverses façons, par exemple en redirigeant l'internaute vers une autre page ou en exploitant directement une vulnérabilité.
  - Modification du code binaire
    - L'attaquant réécrit une partie du code d'un fichier exécutable pour y introduire un programme malveillant ou perpétrer d'autres actes malveillants.
  - Insertion ou vol de témoins
    - En volant des témoins d'un utilisateur, l'attaquant pourrait être en mesure de copier la session de ce dernier et ainsi de naviguer sous son identité.
  - Empoisonnement du cache
    - Le cache est l'endroit où sont stockées de façon temporaire des données visant à réduire les temps de réponse d'un appareil.
    - L'empoisonnement du cache se produit lorsqu'un attaquant y implante des données erronées; cela peut mener le navigateur à se connecter à une mauvaise adresse IP d'un site.



- Faux certificats électroniques
  - Les certificats électroniques servent à valider l'identité d'une page Web. Si un attaquant crée un faux certificat qui semble digne de confiance pour l'ordinateur, l'attaquant peut se faire passer pour n'importe quel site et ainsi avoir accès aux connexions chiffrées.
- Détournement de session
  - Certains protocoles fonctionnent au moyen de sessions, une sorte de conversation officielle où les participants et la durée sont définis. L'attaquant peut détourner la session pour se faire passer pour un de ces « participants ».
- Mise à niveau inférieur
  - Ce type d'attaque consiste à empêcher l'utilisateur de se servir de ses plus récents (et plus sûrs) protocoles ou capacités.
- Hameçonnage
  - Vos renseignements personnels peuvent être d'une grande valeur pour les criminels.
    - C'est tout particulièrement le cas pour les noms d'utilisateur, les mots de passe et les données de comptes bancaires et de cartes de crédit.
      - Les criminels consacrent beaucoup d'efforts à leurrer les gens pour leur soutirer des renseignements de valeur.
      - Cette pratique se nomme **hameçonnage**.
  - La plupart du temps, les courriels hameçons semblent provenir d'organisations à qui vous avez fourni des données confidentielles.
    - Ces courriels contiennent habituellement un hyperlien menant vers une page où l'on vous demande d'ouvrir une session ou d'entrer des données confidentielles sous prétexte d'une vérification ou d'une mise à jour.
      - Méfiez-vous des liens menant vers des pages où vous devez entrer des renseignements ou vous connecter à un compte.
      - Évitez de cliquer sur les liens dans les courriels venant prétendument des banques (ou encore de Microsoft, Apple, PayPal, etc.).
    - Si vous recevez un courriel de ce type et voulez vérifier s'il y a vraiment un problème avec votre compte, connectez-vous au site de l'organisation en question comme vous le feriez habituellement ou appelez-la directement.
    - Ne cliquez pas sur le lien dans le courriel et ne copiez pas l'adresse URL dans la barre de votre navigateur.



## 1.3 En pratique

Soyez à l'affût des différentes menaces possibles pour pouvoir cerner les dangers auxquels vos renseignements ou votre ordinateur pourraient être exposés.

## 2 Éléments à surveiller

### 2.1 En bref

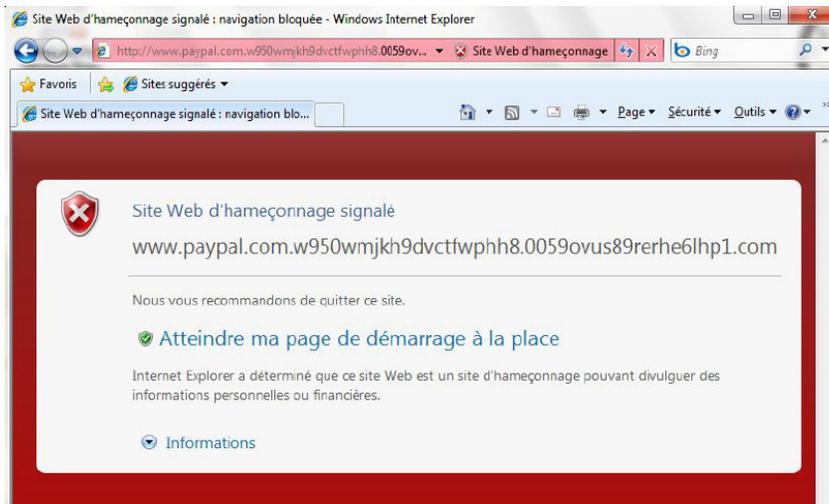
Les navigateurs sont dotés d'outils qui vous aident à naviguer sur le Web de façon sécuritaire. Servez-vous-en, mais faites preuve de jugement; votre expérience n'en sera que plus sûre.

### 2.2 En détail

- Lorsque vous naviguez sur le Web, pensez aux points suivants:
  - Ne faites confiance qu'aux icônes et aux repères propres au navigateur, PAS à ceux qui font partie de la page.
    - La présence d'une icône de cadenas et de la mention https dans la barre de l'URL signifie que les communications du site Web sont chiffrées. Il serait très difficile pour quiconque d'intercepter les données envoyées depuis votre ordinateur jusqu'au site en question. Cependant, cela ne garantit pas l'authenticité du site; de faux sites pourraient aussi avoir cette icône. En pareil cas, les données sont en sécurité lorsqu'elles circulent jusqu'au site Web, mais aboutissent dans un site malveillant.
    - Un certificat de validation étendue (EV, pour extended validation) est représenté par une boîte ou du texte en vert et signifie que le site Web a fait l'objet de plus amples vérifications pour en assurer l'authenticité. Il n'y a rien de garanti, mais c'est un bon signe.
    - Ensemble, le cadenas et la boîte verte du certificat EV vous donnent une certaine assurance que le site que vous visitez est authentique et que vos données peuvent circuler en toute sécurité vers celui-ci.
  - Tout le contenu d'une page Web peut être faux.
    - Les attaquants sont capables de faire des copies exactes d'authentiques sites Web pour donner une allure professionnelle aux faux. Ils donnent aussi l'impression que l'on peut faire confiance à leurs faux sites en y ajoutant des SCEAUX inventés de toutes pièces.
      - Ne vous fiez pas uniquement au contenu d'une page Web pour déterminer si elle est authentique ou pas. Servez-vous plutôt des repères du navigateur.
  - Tapez vous-même les adresses URL des sites Web que vous connaissez plutôt que de vous fier à des hyperliens.
  - Recherchez les repères dans le navigateur avant d'entrer quelconque renseignement personnel ou financier comme votre numéro de carte de crédit ou un mot de passe.

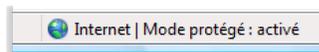


- Si le navigateur vous prévient de ne pas visiter une page, prenez l'avertissement au sérieux. Vérifiez l'URL de nouveau et assurez-vous que c'est bien la bonne.
- Il est impératif de connaître les fonctions de sécurité du navigateur.
  - Internet Explorer
    - Le filtre d'hameçonnage peut vous aider à vous protéger de l'hameçonnage, de la fraude en ligne et des faux sites Web.



> Image 1 : Barre d'adresse d'Internet Explorer avec un avertissement d'hameçonnage

- Le mode protégé peut aider à protéger votre ordinateur des sites qui tenteraient d'installer des programmes malveillants ou d'enregistrer des fichiers sur votre ordinateur à votre insu.



> Image 2 : Indicateur d'état du mode protégé

- Indicateur d'état du mode protégé
  - Plus le niveau de sécurité est élevé, plus vous êtes susceptible d'être à l'abri des pirates informatiques et des attaques.
  - La barre d'état affiche l'identité des sites sécurisés pour éclairer vos décisions lorsque vous faites des transactions sur le Web. De plus, comme Internet Explorer prend désormais en charge les certificats EV, les propriétaires des sites Web y sont encore mieux identifiés.



> Image 3 : Barre d'état (côté droit de la barre d'adresse)

- Barre d'état d'Internet Explorer (côté droit de la barre d'adresse)

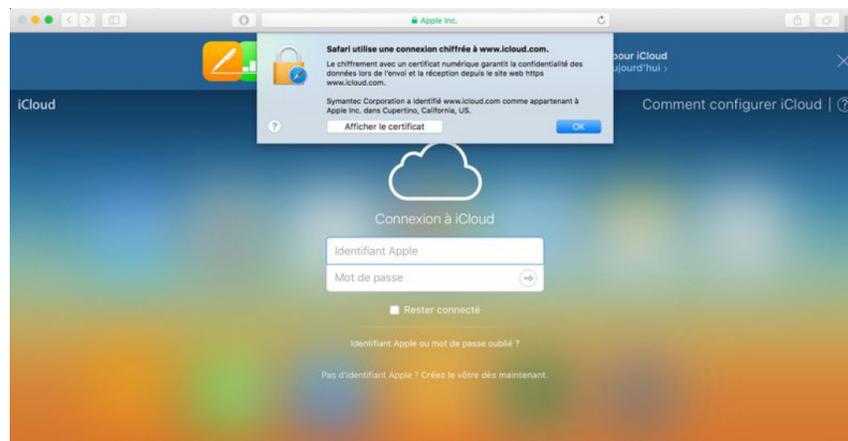


- Lorsque vous visitez un site Web sécurisé, la couleur de la barre d'état vous indique si le certificat de sécurité est valide ou non ainsi que le niveau de la validation effectuée par l'organisme de certification.
- Voici la signification des couleurs de la barre d'état.

<b>Couleur</b>	<b>Signification</b>
Rouge	Le certificat est expiré, non valide ou comporte une erreur.
Jaune	L'authenticité du certificat ou l'organisme de certification qui l'a délivré ne peut être vérifiée. Cela peut révéler un problème avec le site Web de l'organisme.
Blanc	Le certificat est valide; la communication entre votre navigateur et le site Web est donc chiffrée. L'organisme de certification n'a rien à signaler à propos des pratiques du site.
Vert	Le certificat profite d'une validation étendue. Cela signifie que la communication entre votre navigateur et le site Web est chiffrée, et que l'organisme de certification a pu confirmer que le site appartient à une entreprise légalement reconnue selon les modalités de la barre d'état et celles précisées dans le certificat, ou est exploité par celle-ci. L'organisme de certification n'a rien à signaler à propos des pratiques du site <sup>1</sup> , <sup>2</sup> .

– Safari

- Lorsque vous vous connectez à un site Web chiffré dans Safari, vous verrez, dans la barre d'outils, une icône de cadenas verte à côté du nom de l'entreprise à laquelle vous vous êtes connecté (p. ex., Apple Inc.).
  - Si vous cliquez sur l'icône, une boîte de dialogue avec le message « Safari utilise une connexion chiffrée à www.icloud.com » s'affichera. Ce message indique que la connexion est sécurisée.



> Image 4: Connexion à un site sécurisé dans Safari

1 Sur Internet : <<http://windows.microsoft.com/fr-ca/windows/know-online-transaction-secure#1TC=windows-7>>.

2 Sur Internet : <<http://windows.microsoft.com/fr-ca/windows-vista/internet-explorer-at-a-glance>>.



- Par contre, si le site n'est pas sécurisé, le message suivant s'affichera : « Safari ne parvient pas à vérifier l'identité du site Web ». Dans ce cas, ne tentez pas de vous connecter ou de poursuivre votre navigation sur le site en question<sup>3</sup>.



> Image 5: Site non sécurisé dans Safari

## – Chrome

- Un des indicateurs de sécurité le plus important dans Google Chrome est situé dans la barre d'adresse. On appelle cette barre omnibox, car elle peut aussi servir de champ de recherche.



> Image 6: L'omnibox de Chrome

- La première chose à noter est le nom de domaine du site. Celui-ci indique le site Web actuellement affiché dans l'onglet. Il est d'une couleur légèrement plus foncée que le reste. Par exemple, sur l'image ci-dessus, le nom de domaine est **www.google.com**.
  - Vérifiez si le nom de domaine indiqué est bien celui que vous voulez. Si ce n'est pas le cas, vous avez peut-être affaire à un faux site Web.
- La deuxième chose à noter est l'icône du cadenas situé à gauche de l'adresse URL; dans le cas ci-dessus, le cadenas est en vert.
  - Cet endroit est prévu pour afficher l'état de la connexion et du certificat de la page. L'icône affichée peut être l'une des suivantes:

<sup>3</sup> Sur Internet : <<https://support.apple.com/fr-ca/HT203126>>.



- Cadenas sur fond vert 
    - Le site présente un certificat de sécurité valide, et son identité a été authentifiée par un tiers de confiance. Une connexion sécurisée a été établie avec le site auquel vous accédez dans Google Chrome.
  - Point d'exclamation sur fond orange 
    - Le site n'a présenté aucun certificat au navigateur. Cela est normal pour les sites HTTP standard, car les certificats ne sont généralement fournis que si le site utilise le chiffrement.
  - Page 
    - Votre connexion au site n'est pas chiffrée. Ceci est normal pour les sites HTTP standard.
  - Cadenas avec triangle d'avertissement jaune 
    - Google Chrome a accès au certificat du site, mais ce dernier utilise une configuration de sécurité faible. Il est donc possible que votre connexion ne soit pas sécurisée.
    - Il s'agit d'erreurs courantes dans la configuration de sites Web.
    - Si vous voyez cette icône, rien ne garantit que votre connexion est sécurisée. Faites preuve de prudence et n'entrez aucun renseignement personnel sur cette page.
  - Cadenas sur fond rouge 
    - Des problèmes relatifs au certificat du site et des scripts mixtes ont été détectés.
    - On parle de scripts mixtes lorsqu'une page contient un mélange de contenu chiffré et non chiffré. Il peut être difficile de savoir si la page est sûre ou non. Faites donc preuve de prudence<sup>4</sup>.
- o Certificat de validation étendue (EV) (voir l'adresse Web et la boîte verte qui englobe l'icône du cadenas sur l'image ci-dessous).



> Image 7: Certificat de validation étendue de PayPal

- Le certificat EV permet au navigateur de déterminer le nom de l'organisation exploitant le site Web.
- L'indicateur de certificat EV vous permet de savoir quelle organisation gère la page affichée. Par exemple, pour le site Web <https://www.benefitaccess.com/>, on aperçoit Citigroup Inc. [US]<sup>5</sup>.

<sup>4</sup> Sur Internet : <<https://support.google.com/chrome/answer/95617?hl=fr>>.

<sup>5</sup> Sur Internet : <<https://chrome.googleblog.com/2010/10/understanding-omnibox-for-better.html>>.



## 2.3 En pratique

Regardez bien la barre d'adresse pour y détecter les indices de sécurité.

Vérifiez que vous êtes bien connecté au bon site.

## 3 Configuration du navigateur

### 3.1 En bref

Les sites Web malveillants sont conçus avec les mêmes outils que les sites authentiques. Il est donc impossible de simplement contourner les outils non sécuritaires. Apprenez quels sont ces outils et comment allouer les bonnes autorisations dans votre navigateur.

### 3.2 En détail

- Les mêmes outils de programmation sont utilisés pour tous les sites Web.
  - Il n'y a pas d'outils malveillants, seulement des programmeurs malveillants.
  - Il est impossible de désactiver des outils sans qu'il y ait de conséquences.
  - La désactivation d'outils peut nuire au fonctionnement des sites de diverses façons.
    - Témoins
      - Les pages Web enregistrent parfois des données dans votre navigateur; ce sont des témoins.
        - Les témoins permettent aux pages de retenir votre identité et vos préférences, le plus souvent pour rendre la page plus conviviale.
      - Ils servent à recueillir des renseignements très précis sur votre utilisation des pages Web.
      - Il est possible de supprimer les témoins, et de les bloquer à différents degrés.
        - Le blocage des témoins pourrait nuire au fonctionnement de certains sites conçus de sorte que les témoins doivent être autorisés.
      - À l'aide de technologies de pointe, les entreprises peuvent suivre votre utilisation d'Internet sans recourir aux **témoins**.
        - Il n'existe pas de moyen simple et fiable de contourner ces technologies. Par conséquent, même si vous bloquez les témoins, votre confidentialité n'est pas garantie.
      - Soyez à l'affût et sachez que les témoins ne sont pas le seul moyen de vous surveiller.
    - Comment bloquer les témoins.
      - Google Chrome



- Cliquez sur. 
- Sélectionnez **Paramètres**.
- Dans le bas de la page, cliquez sur **Afficher les paramètres avancés...**
- Dans la section **Confidentialité**, cliquez sur **Paramètres de contenu...**
- Cochez **Interdire à tous les sites de stocker des données**.
- Cliquez sur **OK**<sup>6</sup>.
- Vous pouvez aussi supprimer les témoins<sup>7</sup>.
- Internet Explorer
  - Ouvrez Internet Explorer en cliquant sur . Dans le champ de recherche, tapez « Internet Explorer », puis cliquez sur **Internet Explorer** dans la liste.
  - Cliquez sur , sélectionnez **Sécurité**, puis cliquez sur **Supprimer l'historique de navigation...**
  - Cochez la case **Cookies**, puis cliquez sur **Supprimer**<sup>8</sup>.
- Safari
  - Ouvrez **Safari**. Cliquez sur **Préférences**, puis sur **Confidentialité**. Ensuite, effectuez l'une des opérations suivantes:
    - Pour définir les témoins et les données de sites Web autorisés : sélectionnez une option relative aux Cookies et données de site Web :
      - **Toujours bloquer** : Safari ne stocke aucun témoin.
      - **Autoriser à partir du site Web actif uniquement** : Safari autorise les témoins et les données de sites Web provenant uniquement du site actuellement ouvert. Les sites Web intègrent souvent du contenu provenant d'autres sources. Safari ne permet pas à ces tiers de stocker des témoins et d'autres données ou de les consulter.
      - **Autoriser à partir des sites Web que j'ai visités** : Safari accepte les témoins et les données de sites Web provenant uniquement des sites visités. Safari utilise les témoins existants pour déterminer si un site a été visité. Le fait de sélectionner cette option empêche les sites Web qui ont intégré du contenu à ceux visités de stocker des témoins et d'autres données sur le Mac.

<sup>6</sup> Sur Internet : <<https://support.google.com/accounts/answer/61416?hl=fr>>.

<sup>7</sup> Sur Internet : <<https://support.google.com/chrome/answer/95647?hl=fr>>.

<sup>8</sup> Sur Internet : <



- IOS (iPhone, iPad)
  - o Appuyez sur **Réglages**, puis sur **Safari**. Appuyez ensuite sur **Bloquer les cookies**, puis choisissez l'une des options proposées:
    - Toujours bloquer
    - N'autoriser que les sites Web actuellement ouverts
    - N'autoriser que les sites Web visités
    - Toujours autoriser<sup>9</sup>
- Android
  - o Ouvrez Google Chrome. 
  - o Appuyez sur. 
  - o Appuyez sur **Paramètres**, puis sur **Paramètres du site**.
  - o Désactivez l'option **Cookies** pour éviter que les sites enregistrent des témoins sur l'appareil mobile.
- o JavaScript
  - JavaScript offre des outils supplémentaires aux développeurs de pages Web et, par le fait même, aux développeurs de programmes malveillants.
  - En désactivant JavaScript, vous rendrez votre navigateur plus sûr, mais pourriez aussi nuire au bon fonctionnement de certaines pages Web.
    - o La désactivation de JavaScript est une mesure extrême; il est préférable de ne le faire que temporairement, le temps d'effectuer des opérations où le risque est très élevé.
- Google Chrome
  - o Cliquez sur. 
  - o Dans le bas de la page, cliquez sur Afficher les **paramètres avancés...**
  - o Dans la section **Confidentialité**, cliquez sur **Paramètres de contenu...**
  - o Dans la section **JavaScript**, cochez **Interdire à tous les sites d'exécuter JavaScript**.
  - o Cliquez sur **OK**.
- Internet Explorer
  - o Dans le menu du navigateur, cliquez sur **Outils** ou sur l'icône des outils (qui ressemble à un engrenage), puis sélectionnez **Options Internet**.

<sup>9</sup> Sur Internet : <<https://support.apple.com/fr-ca/HT201265>>.



- La fenêtre **Options Internet** s'ouvre, puis sélectionnez l'onglet **Sécurité**.
- Sous l'onglet **Sécurité**, sélectionnez la zone **Internet**, puis cliquez sur **Personnaliser le niveau...**
- Dans la boîte de dialogue **Paramètres de sécurité – Zone Internet**, cochez **Désactiver** dans la section des scripts.
- La fenêtre **Avertissement** s'ouvre, puis s'affiche un message demandant si les paramètres de la zone doivent bien être modifiés. Vous devez alors confirmer.
- Cliquez sur **OK** dans le bas de la fenêtre des options Internet pour fermer la boîte de dialogue<sup>10</sup>.
- Apple Safari
  - Dans le menu de Safari, cliquez sur **Préférences**. Dans la sous-fenêtre **Sécurité**, activez JavaScript.
- Java
  - Il faut distinguer Java de JavaScript. Java est un outil qui permet aux programmeurs d'écrire des logiciels sur une plateforme.
    - Il est fort pratique pour les programmeurs: ces derniers n'ont pas à écrire une version de leur programme pour chaque type d'ordinateur.
    - Il aussi très pratique pour les développeurs de programmes malveillants.
  - Java n'est pas nécessaire pour la majorité des opérations sur un ordinateur; il vaut donc mieux de le désactiver.
  - Il se peut que vous n'avez pas Java sur votre ordinateur. Si vous l'avez, vous pouvez le désactiver en deux étapes.
    - Étape 1 (Trouver le panneau de configuration de Java)
      - Windows
        - Lancez le menu **Démarrer**.
        - Cliquez sur **Programmes**.
        - Trouvez **Java** dans la liste des programmes.
        - Cliquez sur **Configurer Java** pour ouvrir le **Panneau de configuration Java**.
      - Windows (versions antérieures)
        - Utilisez l'option de recherche pour trouver le panneau de configuration.

<sup>10</sup> Pour en savoir plus, consultez le site : <<https://support.microsoft.com/fr-ca/kb/3135465>>.



- Sur le clavier, appuyez sur la touche logo de Windows + W pour ouvrir le champ de recherche.  
OU
- Placez le pointeur de la souris dans le coin inférieur droit de l'écran, puis cliquez sur l'icône de recherche.
- Dans le champ de recherche, inscrivez « Panneau de configuration Java ».
- Cliquez sur l'icône Java pour ouvrir le panneau de configuration.
- Mac OS
  - Cliquez sur l'icône d'Apple dans le coin supérieur gauche de l'écran.
  - Allez à **Préférences Système**.
  - Cliquez sur l'icône Java pour ouvrir le panneau de configuration Java<sup>11</sup>.
- Étape 2 (Désactiver Java – identique pour Windows et Mac OS)
  - Dans le panneau de configuration de Java, cliquez sur l'onglet **Sécurité**.
  - Décochez la case **Activer le contenu Java dans le navigateur**. Cette opération désactive le module d'extension Java dans le navigateur.
  - Cliquez sur **Appliquer**. Lorsque la boîte de dialogue du contrôle de compte d'utilisateur s'affiche, accordez les droits d'accès permettant d'apporter des modifications.
  - Cliquez sur **OK** dans la fenêtre de confirmation du module d'extension Java.
  - Redémarrez le navigateur pour appliquer les modifications.
- Mode privé
  - De nombreux navigateurs offrent un mode de navigation privée conçu pour offrir une certaine confidentialité aux utilisateurs qui partagent des ordinateurs.
    - Le navigateur n'enregistre pas l'historique de navigation.
    - Il ne s'agit pas d'une confidentialité totale; vous ne serez pas anonyme en naviguant avec ce mode.
    - La confidentialité est limitée à l'ordinateur, elle ne s'étend pas à tout le Web.

<sup>11</sup> Pour en savoir plus sur les options de Safari, consultez le site Web : <<https://support.apple.com/fr-ca/HT202447>>.



- On active habituellement le mode privé en ouvrant une nouvelle fenêtre privée à partir du menu.

Chaque navigateur a sa propre appellation et sa propre façon d'ouvrir une fenêtre privée. Toutefois, les raccourcis clavier sont plutôt semblables d'un navigateur à l'autre. Dans Windows, appuyez sur la touche Ctrl; pour un Mac, appuyez sur « ⌘ ».

<b><i>Navigateur</i></b>	<b><i>Nom du mode de navigation privée</i></b>	<b><i>Raccourci clavier</i></b>
Safari	Nouvelle fenêtre privée	Ctrl (⌘) + Shift + N
Chrome	Nouvelle fenêtre de navigation privée	Ctrl (⌘) + Shift + N
Firefox	Nouvelle fenêtre de navigation privée	Ctrl (⌘) + Shift + P
Internet Explorer	Navigation InPrivate	Ctrl (⌘) + Shift + P

- o Bloqueurs de publicité
  - On peut installer des bloqueurs de publicité dans les navigateurs pour bloquer le contenu publicitaire des pages Web.
    - o Ils peuvent améliorer la sécurité, car certaines publicités sont utilisées pour diffuser des programmes malveillants.
    - o Les bloqueurs de publicité sont des applications de tiers. Nous ne faisons aucune recommandation, mais nous vous suggérons de les acheter de fournisseurs reconnus.
    - o Vous trouverez des exemples et de plus amples renseignements aux adresses suivantes :
      - <https://getadblock.com>
      - <https://adblockplus.org><sup>12</sup>

- o Flash
  - Créé à la fin des années 1990, l'outil de développement de contenu interactif Flash a déjà été très populaire grâce à ses nombreux outils puissants.
  - Désormais, de nouveaux outils plus performants sont offerts.
  - Flash est de moins en moins utilisé vu qu'il a grandement servi à l'installation de programmes malveillants.

<sup>12</sup> Nous ne faisons pas la promotion de ces produits. Nous ne les avons pas mis à l'essai.



- Chrome
  - Tapez « chrome://plugins/ » dans l'omnibox de Google Chrome, puis appuyez sur **Entrée**. Cliquez sur **Désactiver** sous le module d'extension Adobe Flash Player.
- Internet Explorer
  - Cliquez sur l'icône en forme d'engrenage, puis sélectionnez **Gérer les modules complémentaires**. Sous **Afficher**, cliquez sur **Tous les modules complémentaires**. Sélectionnez « Shockwave Flash Object » dans la section **Microsoft Windows Third Party Application Component**, puis cliquez sur **Désactiver**.
- Microsoft Edge
  - Cliquez sur le menu, puis sélectionnez **Paramètres**. Faites défiler jusqu'au bas, puis cliquez sur **Voir les paramètres avancés**. Faites passer le bouton sous **Utiliser Adobe Flash Player** à **Désactivé**.
- Safari
  - Cliquez sur **Safari**, puis sur **Préférences...** Cliquez sur l'icône Sécurité. Cliquez ensuite sur **Réglages des sites Web**. Dans la fenêtre suivante, sélectionnez **Adobe Flash** à gauche, puis choisissez **Bloquer** dans le menu situé dans le coin inférieur droit (tout juste au-dessus du bouton **Terminé**). Cliquez sur **Terminé**, puis sortez du menu<sup>13</sup>.

## 3.3 En pratique

Désactivez Java et faites les bons choix à propos des témoins, de JavaScript, des bloqueurs de publicité et de Flash.

Servez-vous du mode de navigation privée pour naviguer discrètement.

## 4 Mise en pratique

### 4.1 En bref

Mettez en pratique ce que vous avez appris. Souvenez-vous de porter attention aux adresses des pages Web, aux indicateurs de sécurité et aux messages d'avertissement lorsque vous utilisez un navigateur.

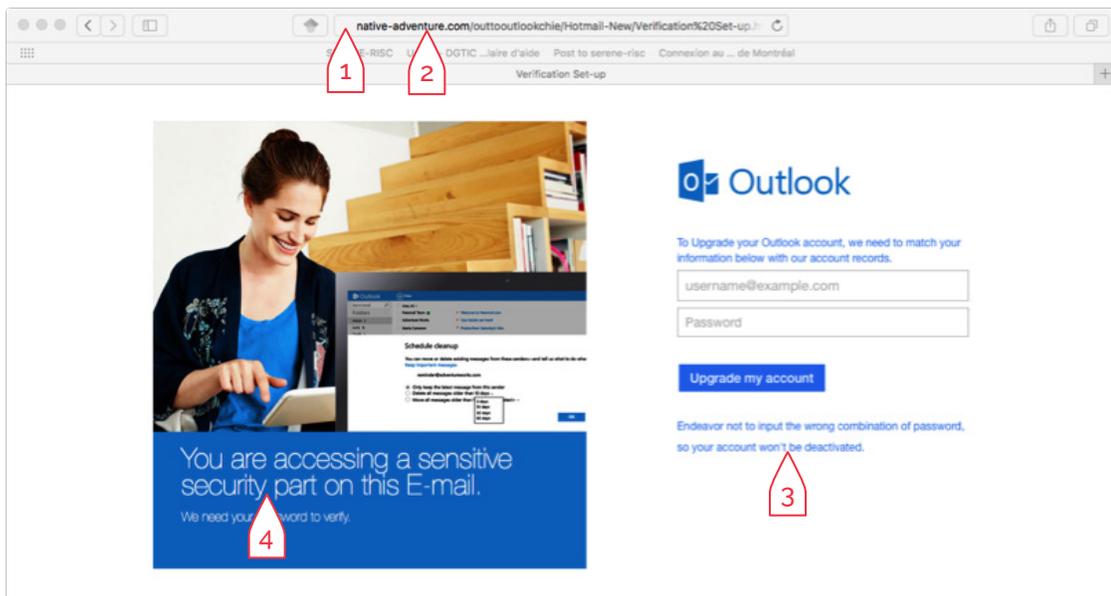
### 4.2 En détail

- Fiez-vous à l'exemple suivant pour naviguer sur une page et repérer les dangers potentiels :
  - Taper l'URL.
    - Tapez « outlook.com » en prenant soin de respecter l'orthographe, puis appuyez sur **Entrée**.

<sup>13</sup> Sur Internet : <<http://gizmodo.com/disable-flash-1688209571>>.



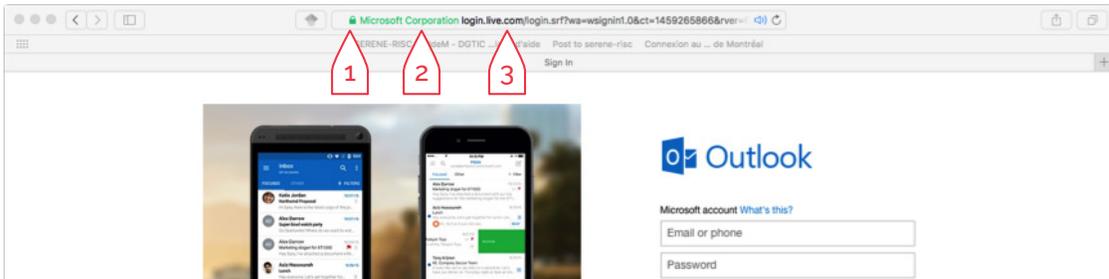
- **ATTENTION à « uotlook.com ».** Cette adresse mène à une page potentiellement dangereuse.
  - Vérifiez si l'URL contient une adresse IP (chiffres seulement) et si elle est bien celle que vous voulez.
  - Vérifiez le nom de domaine et soyez à l'affût des possibles coquilles, comme o pour O ou vv pour w.
- Examiner la page.



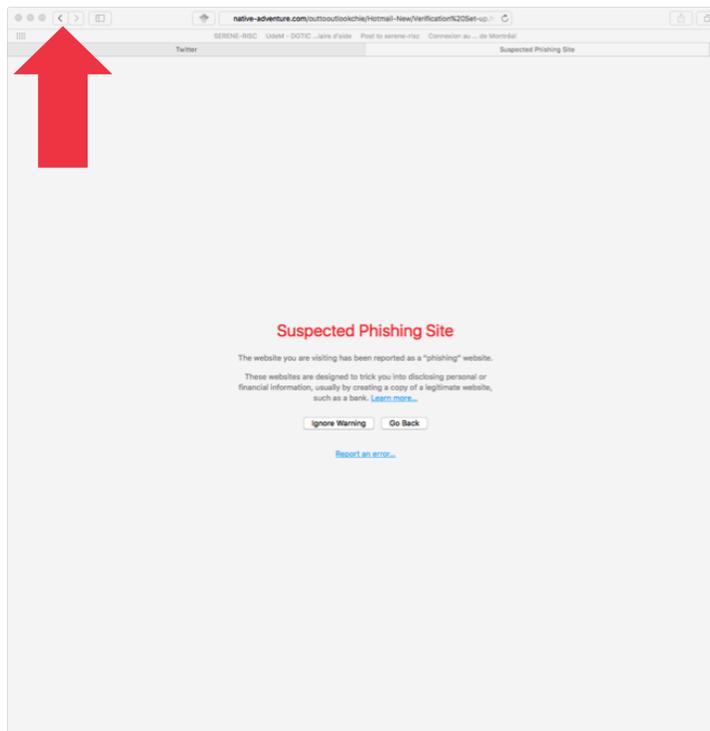
- o Plusieurs indices sur la page ci-dessus indiquent qu'elle est dangereuse. Deux d'entre eux sont très évidents (1 et 2). Les deux autres le sont un peu moins (3 et 4), mais viennent appuyer les premiers.
  1. Il n'y a pas d'icône de cadenas ni de vert dans la barre d'adresse. Cela indique que la page n'utilise pas de connexion sécurisée et ne présente aucun certificat de sécurité. La page outlook.com devrait avoir les deux.
  2. Le nom de domaine n'appartient pas à Microsoft. En effet, « native-adventure.com » n'est pas ce qu'on devrait voir. Cela nous indique que la page est probablement fausse et qu'elle sert à de l'hameçonnage.
  3. Propos menaçants. Il n'est pas normal pour les entreprises authentiques de menacer les clients de désactiver leur compte.
  4. Grammaire de piètre qualité. Il est très peu probable qu'une grande entreprise comme Microsoft publie du contenu mal rédigé.



- o La page suivante comporte des indices confirmant son authenticité.



1. L'icône de cadenas verte confirme la présence d'une connexion sécurisée.
2. Il y a un certificat de sécurité provenant de l'organisation qui est censée posséder ce site.
3. Le nom de domaine est particulier; toutefois, la boîte verte indiquant le propriétaire de la page vient l'appuyer (live.com est une marque utilisée par Microsoft pour rassembler plusieurs services comme Hotmail, Outlook et MSN).



- o À noter aussi l'absence d'erreur de grammaire et de propos menaçant.
- o Une page comme celle-ci est un clair avertissement que la page à laquelle vous tentez d'accéder est dangereuse. Elle s'affiche lorsque le navigateur détecte que la page a un problème. Cliquez sur le bouton de retour pour éviter le site.



- Si vous croyez avoir fait une erreur, modifiez vos mots de passe sans attendre.
  - Dans le cas d'un compte bancaire, vérifiez vos relevés et communiquez avec votre institution financière en cas de problème.
- Si vous croyez que vous ou un proche êtes victime de fraude, communiquez avec le Centre antifraude du Canada, par téléphone au 1 888 495-8501, ou en ligne à l'adresse <http://www.antifraudcentre.ca>.

## 4.3 En pratique

Portez attention à l'adresse URL, aux indicateurs de sécurité et aux messages d'avertissement.



## Glossaire

<b>Navigateur</b>	Logiciel, ou application mobile, utilisé pour consulter des pages Web sur Internet.
<b>Adresse IP</b>	Numéro qui identifie de façon unique un appareil (ordinateur, imprimante, etc.) connecté au réseau Internet (p. ex., 206.167.212.121).
<b>Attaque de l'homme du milieu</b>	Interception malveillante des communications entre l'expéditeur et le destinataire.
<b>Cache</b>	Endroit où sont stockées de façon temporaire des données visant à réduire les temps de réponse d'un appareil.
<b>Certificat</b>	Outil de validation de l'identité d'une page Web.
<b>Certificat de validation étendue</b>	Certificat démontrant que le site Web a subi un processus de validation approfondi pour confirmer son authenticité et indiquant le propriétaire de la page.
<b>Chiffrement</b>	Processus de conversion de l'information en format illisible par les entités non sécurisées, mais lisible par le destinataire désigné.
<b>Hameçonnage</b>	Courriels, appels ou toute autre communication visant à duper les gens pour leur soutirer des renseignements personnels et mots de passe.
<b>Nom de domaine</b>	Nom servant à trouver un ordinateur sur Internet (p. ex., serene-risc.ca).
<b>Programme malveillant</b>	Logiciel créé dans un mauvais dessein.
<b>Publicité malveillante</b>	Programmes malveillants cachés dans les publicités.
<b>Réseau social</b>	Service en ligne permettant d'échanger de l'information de façon publique ou semi-privée.
<b>Système d'exploitation</b>	Logiciel de base d'un ordinateur, comme Windows ou OS X, chargé de commander l'exécution des programmes.
<b>Téléchargement furtif</b>	Attaque consistant à implanter un programme malveillant dans un ordinateur par la simple visite d'une page Web.
<b>Témoin</b>	Donnée enregistrée dans un navigateur et utilisée par un site Web.