Techno habile

# Scénario

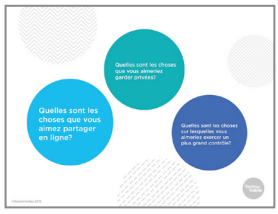

Avec un financement du Canada

Habilo Médias

YWCA CANADA
A TURNING POINT FOR WOMEN
UN POINT TOURNANT POUR LES FEMMES


**1.** Bienvenue à cet atelier sur la protection de la vie privée lors de la navigation en ligne.

Il y aura une période de questions à la fin, mais je vous invite tout de même à lever la main pour poser toute question qui surgirait en cours de route.



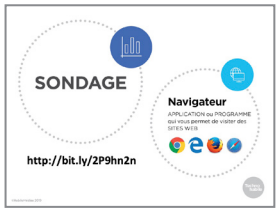

**2.** Avant de commencer, j'aimerais que vous preniez une minute pour penser à ce que vous aimeriez retirer de cet atelier.

Vous n'avez pas à répondre à voix haute. L'important est simplement d'y réfléchir.

Quelles sont les choses que vous aimez partager sur Internet?

Quelles sont les choses que vous aimeriez garder privées?

Quelles sont les choses sur lesquelles vous aimeriez exercer un plus grand contrôle?




**3.** Avant de commencer, nous allons faire un sondage rapide pour voir ce que vous savez déjà.

Vous pouvez répondre à la première question en levant votre main. – Combien d'entre vous avez apporté un appareil que vous savez utiliser?

Combien d'entre vous avez apporté un appareil que vous n'avez encore jamais utilisé?

Si vous avez un appareil que vous savez déjà utiliser, allumez-le et, à l'aide du navigateur, rendez-vous sur le site Web qui apparaît à l'écran. Une fois que vous y êtes, vous pouvez remplir le sondage. Ça ne devrait prendre que quelques minutes.

Si vous n'avez encore jamais utilisé votre appareil, commencez par trouver l'un des logos de navigateur sur votre écran. Une fois que c'est fait, ouvrez le navigateur et entrez l'adresse du site Web pour accéder au sondage.

Je vais circuler dans la salle pour m'assurer que tout le monde est capable d'accéder au sondage. Si vous avez fini avant les autres, vous pouvez aider votre voisin.


**4.** Nous avons abordé de nombreuses notions fondamentales dans le cadre de l'atelier *Explorer la vie privée en ligne* et nous approfondirons maintenant le sujet afin de protéger vos comptes et vos appareils.

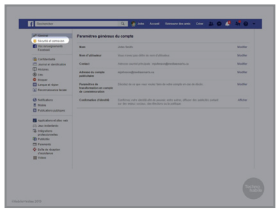
Si vous n'avez pas participé à cet atelier, ne vous en faites pas! Je vais vous aider à comprendre sur ce que vous avez manqué et que vous ne connaissez pas encore.


**5.** Nous avons discuté de l'importance de créer un mot de passe efficace lors de l'atelier *Explorer la sécurité en ligne*.

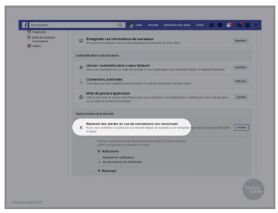
Un autre outil que vous pouvez utiliser pour protéger encore davantage vos comptes est l'authentification à *deux facteurs*.

Si vous avez activé l'authentification à deux facteurs, en plus d'entrer votre mot de passe, vous recevrez également sur votre téléphone un message texte contenant un code à usage unique. Vous devrez entrer ce code ainsi que votre mot de passe pour ouvrir une session.

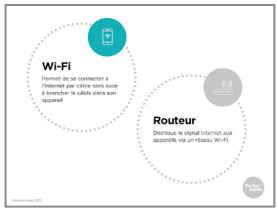
Ainsi, une personne qui obtiendrait votre mot de passe ne pourrait pas accéder à vos comptes. L'inconvénient, c'est que vos comptes seront verrouillés si vous perdez votre téléphone et qu'il s'agit de votre principal moyen d'accéder à Internet.



**6.** Vous pouvez également demander à certains réseaux sociaux de vous envoyer une alerte si un nouvel appareil se connecte à votre compte. Sur Facebook, accédez à vos paramètres et cliquez sur Sécurité et connexion à gauche.



**7.** Cliquez ensuite sur « Recevoir des alertes en cas de connexions non reconnues ».




**8.** Nous sommes nombreux à utiliser le réseau Wi-Fi public des endroits comme les bibliothèques ou les cafés. Toutefois, il est important de savoir que celui-ci est moins sécuritaire que votre réseau résidentiel.

Les réseaux qui ne nécessitent pas l'entrée d'un mot de passe sont particulièrement risqués puisque tout le monde peut

s'y connecter. Cela signifie qu'une personne qui dispose des bons programmes peut voir ce que vous envoyez au routeur, y compris votre identifiant et votre mot de passe, ainsi que les renseignements relatifs à votre carte de crédit.

Certes, il est plus sécuritaire d'entrer un mot de passe pour vous connecter au réseau, mais n'oubliez pas que vous le partagez tout de même avec toute autre personne qui s'y connecte.

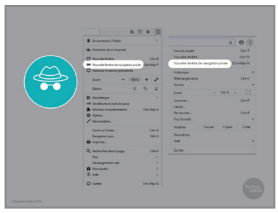

**9.** Il y a trois choses que vous pouvez faire pour rendre l'utilisation du réseau Wi- Fi public plus sécuritaire.

D'abord, assurez-vous d'utiliser un réseau de confiance. Comme il est possible de donner n'importe quel nom à un réseau, certaines personnes choisissent de nommer le leur « Bibliothèque publique » ou « Wi-Fi Starbucks » pour épier les autres ou installer des programmes malveillants sur leur ordinateur. Revérifiez toujours pour vous assurer de vous connecter au bon réseau.

Ensuite, n'utilisez jamais les réseaux publics pour magasiner ou vérifier vos comptes bancaires en ligne. Même sur un réseau sécurisé, il est possible qu'une personne puisse voir les données que vous envoyez.

Finalement, dans la mesure du possible, naviguez sur des sites sécurisés. Il s'agit de ceux pour lesquels un cadenas fermé s'affiche dans la barre d'adresse et dont l'adresse commence par « https » plutôt que « http ». Vous devriez également installer l'extension HTTPS Everywhere, qui indique aux sites Web de vous connecter uniquement à la version sécurisée du site.

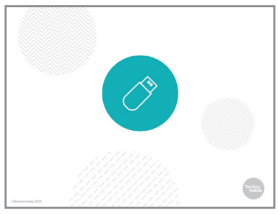
Si vous utilisez un iPhone ou un iPad, vous pouvez activer la mise à jour automatique du HTTPS en vous rendant dans les paramètres avancés de Safari.



**10.** Si vous devez envoyer des renseignements importants au moyen d'un ordinateur public, essayer d'utiliser celui qui est connecté à un câble réseau, comme un ordinateur de bureau, plutôt qu'un ordinateur connecté au réseau Wi-Fi. Assurez-vous de naviguer en mode incognito (ou navigation privée) afin que l'ordinateur n'enregistre pas les données saisies ni les sites visités.

Dans la plupart des navigateurs, il est possible d'activer ce mode en cliquant sur le bouton situé dans le coin supérieur

droit pour sélectionner ensuite « Nouvelle fenêtre privée » ou « Nouvelle fenêtre incognito ».



**11.** Tout comme vous ne devriez pas vous connecter à des réseaux qui ne sont pas dignes de confiance, n'utilisez jamais une clé USB ou une carte mémoire à moins de l'avoir achetée vous-même ou de faire confiance à la personne qui vous l'a donnée. Ces composantes peuvent facilement propager des programmes malveillants d'un ordinateur à un autre. Certaines personnes laissent même délibérément traîner des clés USB infectées à des endroits où d'autres pourront les trouver.


**12.** Vous devriez également vous assurer d'exécuter un antiprogramme malveillant.

Les appareils sous Windows sont livrés avec Windows Defender, un programme intégré gratuit. Assurez-vous qu'il est activé et qu'aucun autre antiprogramme malveillant ne s'exécute. Autrement, ils pourraient se faire obstacle.

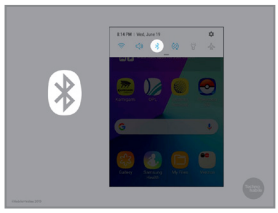
Pour les appareils Mac et les appareils mobiles, installez un outil fiable comme Malwarebytes ou AVG. Même s'il s'agit de logiciels gratuits, on tentera de vous vendre des services supplémentaires.


**13.** Les sociétés qui développent des programmes y découvrent souvent des problèmes de sécurité qu'elles règlent par la suite. C'est pourquoi il est important d'activer la mise à jour automatique, particulièrement en ce qui concerne les navigateurs –par lesquels vous envoyez la majorité de vos renseignements personnels – et les systèmes d'exploitation comme Windows ou iOS.

Cela signifie également qu'il est risqué d'utiliser les versions piratées des systèmes d'exploitation comme Windows ou des programmes comme Microsoft Office puisque vous ne bénéficierez pas de ces mises à jour.

Si vous avez besoin de programmes comme Word ou Excel mais n'avez pas les moyens de vous les procurer, utilisez une alternative légale et gratuite comme Libre Office. Il n'est pas identique à Microsoft Office, mais il permet de lire et d'enregistrer des fichiers dans les mêmes formats. Ainsi, vous pouvez lire un fichier Word dans Libre Office et enregistrer vos fichiers dans un format qu'un utilisateur de Word pourra lire.

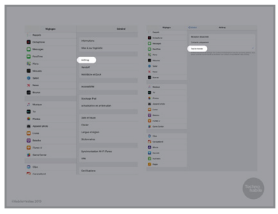

**14.** De nombreux sites Web vous offrent la possibilité d'ouvrir une session avec votre compte Facebook ou Google plutôt que de créer un nouveau compte avec eux. Cette option semble rapide et pratique, mais sachant qu'elle permet également au site Web d'avoir accès à tout ce qui se trouve dans votre compte – vos amis, les messages que vous avez aimé et ainsi de suite. Le jeu en vaut-il vraiment la chandelle?



**15.** Enfin, il y a quelques fonctionnalités de vos appareils que vous devriez désactiver lorsque vous ne les utilisez pas.

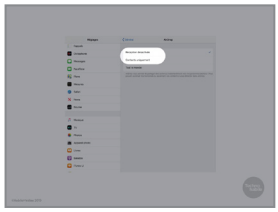
Le Bluetooth permet à différents appareils de se connecter sans fil. Il est utile pour la connexion à des haut-parleurs ou à des écouteurs, mais il rend également possible pour d'autres personnes de se connecter à vos appareils lorsqu'il est activé.

Certains appareils vous permettent d'activer ou de désactiver le Bluetooth simplement en touchant l'icône correspondante. Pour certains, vous devez vous rendre dans les Paramètres pour le faire.

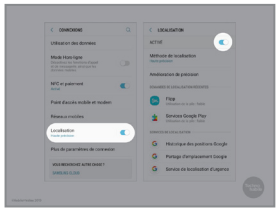


**16.** Les appareils Apple sont également dotés d'une fonctionnalité appelée AirDrop qui permet aux utilisateurs de partager des fichiers entre eux. Si elle est activée, certaines personnes pourraient s'en servir pour envoyer des photos ou autres éléments indésirables sur votre appareil.

Pour éviter cela, rendez-vous dans Réglages et touchez l'icône Airdrop. Vous y verrez ainsi les réglages qui y sont associés.



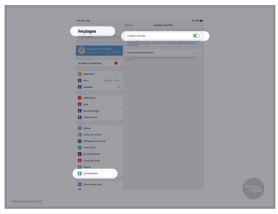
**17.** Si vous souhaitez contrôler qui peut envoyer du contenu sur votre appareil au moyen de AirDrop, choisissez Contacts uniquement, afin que seules les personnes préapprouvées y soient autorisées, ou Réception désactivée, tout simplement.



**18.** Le GPS est une autre fonction que vous pouvez désactiver lorsque vous ne l'utilisez pas. Elle peut être utile lorsque vous voulez connaître votre emplacement, mais elle peut également envoyer cette information aux sites Web que vous visitez ou aux applications que vous utilisez.

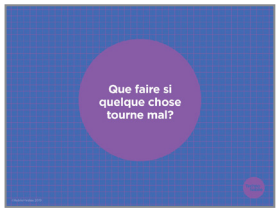
Pour désactiver la localisation sur un appareil Android, rendez-vous dans Paramètres, déroulez jusqu'à Position, touchez

l'icône correspondante, puis touchez le bouton pour désactiver la fonction.



**19.** Pour désactiver la localisation sur un iPhone ou un iPad, accédez à Réglages, puis Confidentialité.

Glissez ensuite le bouton Service de localisation pour désactiver la fonction.




**20.** Toutefois, malgré toutes les précautions prises pour protéger nos comptes et nos appareils, il est toujours possible que les choses tournent mal.

La bonne nouvelle est qu'il est assez facile de corriger ses erreurs la plupart du temps.


**21.** Voici quelques signes pouvant indiquer un problème avec votre appareil ou vos comptes :

Les gens reçoivent des messages que vous n'avez pas envoyés;

Vous ne recevez pas et ce, de façon répétée, les messages que d'autres personnes affirment vous avoir envoyés;

Vous ne parvenez pas à vous connecter à un ou plusieurs de vos comptes;

Votre appareil est inhabituellement lent.

De plus, si vous recevez une notification de connexion ou de demande de changement de mot de passe que vous ne vous souvenez pas avoir faite, il est fort probable que quelqu'un ait tenté d'accéder à vos comptes.


**22.** Si vous croyez qu'une personne pourrait avoir accédé, ou tenté d'accéder, à votre appareil ou à l'un de vos comptes, voici ce que vous devez faire :

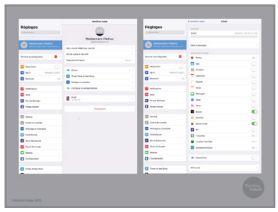
D'abord, n'envoyez aucun renseignement personnel ou sensible avant que le problème soit réglé.

Ensuite, déconnectez-vous de tous vos comptes, et ce, sur chaque appareil que vous utilisez.

Puis, changez tous vos mots de passe. Pour votre compte de messagerie électronique, n'oubliez pas d'utiliser un mot de passe complètement différent de tous les autres.

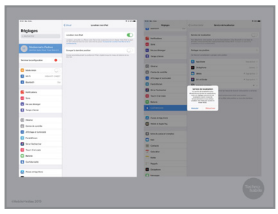
Finalement, exécutez votre antiprogramme malveillant.

Même si votre appareil ou vos comptes sont verrouillés, il est possible d'obtenir l'aide de l'entreprise. Dans la mesure où vous pouvez prouver votre identité, vous devriez pouvoir reprendre le contrôle.

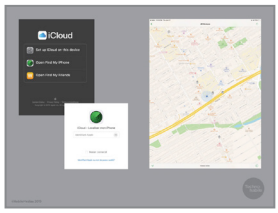


**23.** Il existe également des moyens pour trouver votre appareil en cas de perte ou de vol.

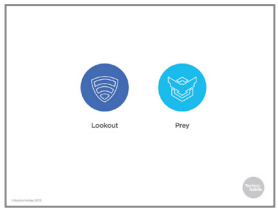
Pour un iPhone ou un iPad, vous devez activer la fonction « Localiser mon iPhone » ou « Localiser mon iPad ». Pour ce faire, accédez à Réglages, puis touchez le nom de l'appareil dans le coin supérieur gauche.



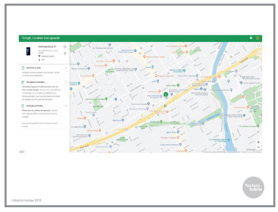
**24.** Touchez ensuite le commutateur Localiser mon iPad ou Localiser mon iPhone, puis touchez OK dans la boîte de dialogue qui s'affiche.




**25.** Pour le trouver, ouvrez iCloud.com sur n'importe quel navigateur, cliquez sur Localiser mon iPhone, puis entrez votre identifiant Apple et votre mot de passe. Une carte indiquant l'emplacement de votre appareil s'affichera ensuite.




**26.** Vous pouvez également télécharger des applications comme Lookout et Prey qui vous permettent de suivre, de verrouiller et de supprimer les données de vos appareils en cas de perte. Comme de nombreuses applications, les versions de base sont gratuites, mais certaines fonctionnalités sont payantes.



**27.** Malheureusement, il est possible de trouver les appareils Android uniquement lorsque les services de localisation sont activés. Vous devrez donc faire un choix entre préserver votre vie privée et être en mesure de trouver votre téléphone.

Si les services de localisation et la fonction Localiser mon appareil sont activés dans les Paramètres, vous pouvez le trouver en accédant à la page Android.com/find et en vous

connectant à votre compte. En plus de voir l'emplacement de votre téléphone sur la carte, vous pouvez le verrouiller ou en effacer le contenu à distance.


**28.** Quiz : http://bit.ly/2RC5uDC


**29.** Essayez de faire l'*une* des choses dont nous avons parlé au cours des dernières minutes :

configurer l'authentification à deux facteurs;

configurer vos réseaux sociaux afin de recevoir une alerte si quelqu'un d'autre tente de se connecter;

désactiver le Bluetooth, la localisation ou AirDrop; localiser votre appareil à distance.


**30.** Bien sûr, la vie privée et la sécurité ne se limitent pas aux appareils et aux comptes. De nos jours, une grande partie de notre vie personnelle se retrouve en ligne et il est également important de la protéger.


**31.** Bien des gens ont recours à des applications de rencontre en ligne. Voici quelques conseils de sécurité en la matière.

Créez d'abord une nouvelle adresse de courrier électronique auprès d'un service gratuit comme Gmail ou Outlook, adresse que vous utiliserez pour vous inscrire. Garder cette adresse distincte de votre adresse de courrier électronique principale peut vous aider à protéger votre vie privée.

Consultez ensuite la politique de protection des renseignements personnels ainsi que les conditions générales d'utilisation. Vous n'avez pas toujours à lire le document en entier, mais vous devriez vous assurer de pouvoir supprimer entièrement vos photos et toutes vos publications après la fermeture de votre compte.

Lorsque vous établissez un lien avec quelqu'un, ne communiquez pas vos renseignements personnels, en

particulier ceux qui pourraient être utilisés pour vous trouver dans la « vraie vie », comme votre adresse ou votre numéro de téléphone, tant que vous n'êtes pas à l'aise de partager ces informations.

Les fraudes amoureuses, qui consistent en une personne vous demandant de lui envoyer de l'argent pour quitter son pays ou se sortir du pétrin, sont courantes sur les sites ou les applications de rencontre.

Si vous décidez de passer du virtuel au réel, demandez à ce que la première rencontre ait lieu dans un endroit public et confiez vos plans à un(une) ami(e) ou à un membre de votre famille. Demandez également à cette personne de communiquer avec vous pendant le rendez-vous afin de vous fournir une excuse pour quitter si nécessaire.


**32.** Le sextage, ou l'envoi à quelqu'un d'autre de photos nues ou sexy de vous, peut s'inscrire dans une relation saine, mais comporte également des risques.

N'envoyez jamais de sexto à moins que le destinataire vous ait clairement signifié son intérêt.

Si vous envoyez un sexto, n'oubliez pas qu'il est impossible d'empêcher une personne d'en faire des copies en ligne, et ce, même avec une application comme Snapchat.

Ne montrez jamais votre visage, de tatouages distinctifs, ou tout élément susceptible de vous identifier.

Si vous recevez un sexto non sollicité, bloquez immédiatement l'expéditeur (nous avons vu comment faire dans le cadre de l'atelier *Explorer la vie privée en ligne*). Si vous possédez un appareil Apple, désactivez AirDrop.

Si vous recevez un sexto *sollicité*, ne le partagez pas et ne le montrez pas sans le consentement de la personne concernée.

Ne forcez jamais une personne à vous envoyer un sexto.


**33.** Notre vie en ligne est également affectée par la fin d'une relation.

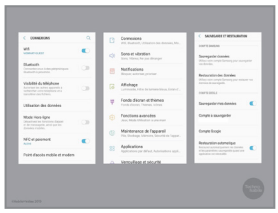
Même si la rupture a été amicale, il est toujours avisé de changer vos mots de passe. Et même si vous ne vous souvenez pas avoir communiqué vos mots de passe, faites comme si c'était le cas. Pensez également à changer les questions de sécurité auxquelles vous répondez lorsque vous oubliez vos

mots de passe puisqu'elles concernent habituellement des choses que votre partenaire aurait pu apprendre au cours de votre relation, comme le nom de votre premier animal de compagnie. Ne prenez donc pas de risques et choisissez de nouvelles questions.

Une autre précaution à prendre consiste à sauvegarder vos photos, vos fichiers et tout ce qui est important pour vous. Pour ce faire, vous pouvez utiliser un service infonuagique comme Google Drive, une clé USB, ou les deux.

Si au contraire la rupture est difficile et que vous avez besoin de soutien pour mettre fin à une relation, servez-vous de ce que vous avez appris dans le cadre de cet atelier (comme l'utilisation de sites sécurisés HTTPS) pour garder vos recherches privées. (L'atelier *Explorer la vie privée en ligne* vous sera utile à cet effet.)

Vérifiez bien qu'aucun logiciel traqueur en mesure d'indiquer à quelqu'un d'autre où vous êtes et ce que vous faites n'a été installé sur votre appareil. Désinstallez toutes les applications que vous ne reconnaissez pas et accédez aux autorisations des applications du menu Paramètres afin de connaître les applications qui peuvent accéder à vos données de localisation. Vérifiez également vos paramètres de localisation afin de vous assurer que votre emplacement ne peut pas être déterminé.



**34.** Si vous avez pris toutes les mesures présentées précédemment et que vous croyez que votre ancien(ne) partenaire vous suit toujours, il pourrait être nécessaire d'effacer entièrement le contenu de votre téléphone.

Sur un téléphone Android, accédez à Paramètres, à Sauvegarder et réinitialiser, puis à Restaurer les données d'usine. Cela effacera tout ce que vous aviez enregistré sur votre téléphone ainsi que toutes les applications que vous y aviez téléchargées.


**35.** Sur un iPhone ou un iPad, touchez Réglages, Général, puis Réinitialiser. Touchez ensuite Effacer contenu et réglages puis entrez votre mot de passe ou votre identifiant Apple.


**36.** Quiz : http://bit.ly/2LEFQdw


**37.** Toutefois, malgré nos efforts, notre vie privée peut également mal tourner en ligne.

Voici quelques mesures que vous pouvez prendre pour vous aider à garder les choses sous contrôle.


**38.** Si une personne a partagé un sexto provenant de vous sans votre accord, voici ce que vous pouvez faire.

Sauvegardez d'abord la preuve. S'il a été publié sur un espace public, faites une capture d'écran. Si quelqu'un affirme l'avoir vu, enregistrez son témoignage.

Vous pouvez demander à la personne concernée de cesser de le partager ou de le retirer. Même si elle refuse ou ne répond pas, gardez un dossier des textos ou des courriels envoyés afin de démontrer ultérieurement que le partage s'est effectué sans votre consentement.

S'il a été partagé sur un réseau social ou un site Web, demandez à ce qu'il soit retiré. Pensez à dire que la publication enfreint les conditions générales d'utilisation. Presque tous les sites ont des règlements qui interdisent la publication de sextos sans l'accord de l'expéditeur. S'il s'agit d'une photo que vous avez prise, vous en détenez les droits d'auteur et vous pouvez demander à ce que la photo soit retirée en invoquant ce motif.

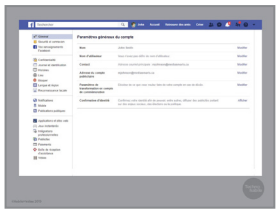
Au Canada, il est illégal de partager des « images intimes » d'une personne sans son accord, peu importe son âge, et un juge peut ordonner le retrait de la photo en plus de déposer des accusations criminelles contre la personne l'ayant partagée. Mieux vaut toutefois être préparé pour cette étape avant d'aller voir la police, en consultant la feuille À l'aide! Quelqu'un a publié un sexto sans mon consentement ou le Guide éclair sur la violence sexuelle liée à des images intimes du YWCA pour obtenir d'autres conseils.

Si vous souhaitez procéder sans passer par la police, vous pouvez vous rendre au palais de justice pour rencontrer un juge

de paix ou demander à un avocat de s'en occuper pour vous. Certaines villes ont également des bureaux d'aide juridique qui peuvent vous aider dans de telles situations, et ce gratuitement ou à tarif réduit.


**39.** Si une personne vous harcèle en ligne, la loi peut aussi vous aider.

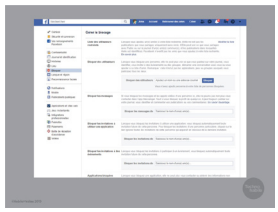
Le harcèlement consiste à communiquer avec une personne de façon à lui faire craindre pour sa sécurité physique ou psychologique, ou celle d'une de ses connaissances.



**40.** En matière de harcèlement, l'une des premières étapes consiste à bloquer l'expéditeur.

Sur Facebook, une personne bloquée ne pourra pas vous envoyer une demande d'amitié, ne verra pas votre profil, ne pourra pas vous identifier sur une publication et ne pourra pas vous envoyer de messages sur ce réseau.

Pour bloquer une personne, accédez à vos Paramètres, puis sélectionnez Blocage dans le menu de gauche.



**41.** Tapez ensuite le nom de la personne que vous souhaitez bloquer dans « Bloquer des utilisateurs ». Une fois que vous avez sélectionné la bonne personne, cliquez sur Bloquer.

La plupart des réseaux sociaux et des applications de messagerie offrent également une forme de blocage quelconque.


**42.** Avant de bloquer une personne, assurez-vous toutefois d'enregistrer la preuve de ce qu'elle fait.

Si vous ne voulez pas voir les messages ou les textos dans votre boîte de réception, créez un dossier spécial.

En plus de garder des copies lorsque c'est possible, vous devriez également faire une capture d'écran de tout ce que la personne qui vous harcèle vous envoie. Le site take-a-screenshot.org (disponible seulement en anglais) explique en détail comment faire une capture d'écran selon l'appareil ou le système d'exploitation.

En plus de bloquer une personne, vous pouvez également signaler ses agissements à l'application ou au site Web où le

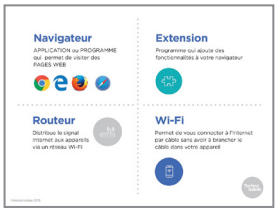
harcèlement se produit. Vous pouvez également faire part de la situation à votre fournisseur de services téléphoniques ou Internet, qui empêchera son numéro de téléphone ou son adresse IP de vous contacter.

Si vous avez bloqué une personne qui vous harcèle, soyez prudent avant d'accepter de nouvelles demandes d'amitié. Il est facile pour les gens de créer de nouveaux comptes.

Tout comme pour les sextos, vous pouvez signaler le harcèlement à la plateforme sur laquelle il se produit, ainsi qu'à la police ou à un juge de paix.

Un avocat peut également vous aider à obtenir un engagement de ne pas troubler l'ordre public qui empêchera la personne concernée de vous contacter de quelque façon que ce soit. Comme les engagements de ne pas troubler l'ordre public fonctionnent différemment d'une province à l'autre, il est préférable d'obtenir un avis juridique au préalable.

Le refuge pour femmes battues de votre région est également une bonne source d'information pour savoir quoi faire en cas de harcèlement.

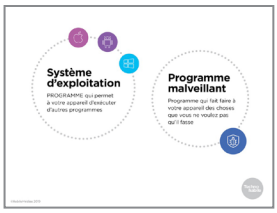



**43.** Avant de se laisser, revenons un peu sur les nouveaux termes appris au cours de l'atelier.

Un *navigateur* est l'application ou le programme qui permet à votre appareil de visiter des pages Web. Chrome, Firefox et Safari sont des exemples de navigateurs.

Une *extension* est un petit programme qui ajoute des fonctionnalités à votre navigateur.

Le *Wi-Fi* envoie un signal Internet à votre ordinateur sans qu'aucun fil ou câble ne soit requis en utilisant un *routeur* sans fil connecté à l'Internet par câble.



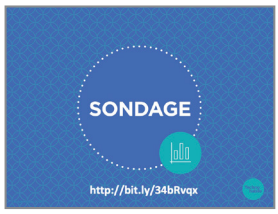

**44.** Un système d'exploitation est un programme informatique qui permet à votre appareil d'exécuter d'autres programmes. Il y a trois grands systèmes d'exploitation pour les ordinateurs : Windows, Mac et Chrome. En ce qui concerne les téléphones et les tablettes, il existe seulement deux grands systèmes d'exploitation : iOS et Android.

Un *programme* malveillant ressemble à un virus et apporte des modifications indésirables à votre ordinateur.


**45.** Cet atelier tire à sa fin. Si vous avez encore des questions au sujet des notions abordées aujourd'hui, c'est le moment de les poser.

Si vous préférez me les poser en privé, n'hésitez pas à venir me voir après l'atelier. Je resterai sur place un petit moment.


**46.** Assurez-vous d'apporter la fiche d'exercice pour cet atelier. Utilisez le lien vidéo qui s'y trouve pour revoir ce que nous avons couvert aujourd'hui.




**47.** Nous avons couvert beaucoup de matière au cours de l'atelier. J'aimerais maintenant vous entendre. Qu'avez-vous appris? Des questions sont-elles restées sans réponse? Avez-vous des suggestions pour améliorer l'atelier?