Scénario

Avec le financement de

Agence de la santé publique du Canada | Public Health Agency of Canada

1. Bienvenue à la séance consacrée à la sécurité des relations en ligne. Cet atelier est conçu pour aider les personnes ayant subi de la violence à se sentir plus en sécurité et plus confiantes dans la gestion de leurs relations et de leurs renseignements personnels en ligne.

Nous aurons du temps pour les questions à la fin, mais j'aimerais aussi vous inviter à lever la main en tout temps si vous avez une question en cours de route. *[Les participants à distance sont invités à poser leurs questions dans la boîte de clavardage.]*

2. Du matériel de référence est fourni dans le cadre de cet atelier, notamment une feuille d'exercice et une vidéo pour vous aider à vous souvenir du contenu essentiel. Vous pouvez consulter ce matériel à tout moment, y compris après l'atelier, et pouvez revenir à l'atelier lui-même sur le site Web de HabiloMédias, https://habilomedias.ca/favoriser-la-resilience- grace-technohabile.

3. Certains sujets peuvent être bouleversants alors avant de commencer, parlons de la façon dont nous allons composer avec ces situations.

Nous vous indiquerons le contenu de chaque partie de l'atelier afin que vous puissiez vous retirer quelques minutes si vous préférez ne pas aborder un sujet particulier. Si vous devez vous retirer, levez le pouce avant de partir pour que je sache que vous allez bien. Si vous avez besoin d'aide, *[nom de la personne disponible pour du soutien supplémentaire]* est à votre disposition pour vous aider.

Pour les participants à distance uniquement : Pouvez-vous me dire si vous êtes dans un endroit sûr pour discuter? Si ce n'est pas le cas, y a-t-il un autre endroit plus sûr où vous pourriez vous rendre?

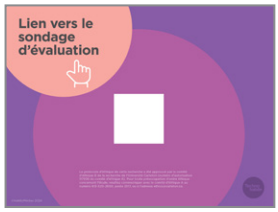
Assurez-vous d'avoir à proximité quelque chose qui vous réconforte. Des pauses sont prévues au cours de l'atelier, mais vous devez vous sentir libre de vous retirer à tout moment.

4. Nous ferons d'abord un bref sondage pour nous aider à comprendre ce que vous savez et ne savez pas sur la protection de la vie privée et la gestion des relations en ligne. Ensuite, nous aborderons les sujets énumérés à l'écran et ferons quelques exercices pour mettre en pratique ces compétences. Enfin, nous terminerons par un bref sondage qui nous aidera à comprendre si cet atelier a bonifié vos connaissances et vos compétences en matière de protection de la vie privée en ligne et de gestion des relations en ligne.

Au terme de cet atelier, vous saurez comment :

- protéger votre vie privée et vos appareils numériques;
- restreindre le public qui voit votre localisation;
- gérer les renseignements que vous partagez en ligne;
- protéger votre vie personnelle en ligne;
- trouver et supprimer des logiciels espions sur votre téléphone.

Avant de commencer, arrêtons-nous un instant pour voir si quelqu'un a des questions.



5. Vous aurez deux occasions de faire part de vos commentaires à l'équipe de HabiloMédias qui a élaboré cet atelier : maintenant avant de commencer l'atelier et à la toute fin. Ces sondages aideront l'équipe de HabiloMédias à déterminer si l'atelier permet aux survivantes de développer leurs connaissances et leurs compétences numériques et leur confiance en elles.

Avant de commencer l'atelier, nous vous demandons de prendre cinq minutes pour répondre à ce sondage anonyme d'évaluation du programme. L'équipe de HabiloMédias qui a élaboré cet atelier utilisera les réponses au sondage pour guider les futures mises à jour du programme et évaluer la valeur et l'impact de cet atelier. Vos réponses resteront confidentielles et anonymes. L'objectif est d'évaluer le programme, et non les participantes. Il est tout à fait acceptable de ne pas connaître les réponses à certaines questions et il n'est pas nécessaire de posséder les compétences en question. Votre participation est entièrement volontaire. Si vous souhaitez participer au sondage, il vous suffit de scanner le code QR à l'aide de l'appareil photo de votre téléphone ou de taper le lien fourni dans votre navigateur pour y accéder. Nous allons maintenant faire une pause afin de permettre à celles qui le souhaitent de remplir le sondage. Prenez tout le temps dont vous avez besoin.

6. Il existe de nombreux types d'abus, ce qui rend difficile l'élaboration d'une seule définition générale des abus. Dans le contexte des relations, les abus sont un ensemble de comportements utilisés pour obtenir ou maintenir le pouvoir et le contrôle sur un partenaire. La violence physique (ou les menaces de violence physique) est un exemple parmi d'autres de ce type de comportement.

La violence émotionnelle et verbale (comportements non physiques visant à contrôler, isoler et effrayer), la violence financière (un partenaire violent étend son pouvoir et son contrôle à la situation financière du partenaire), la violence sexuelle (forcer ou contraindre une personne à faire quelque chose qu'elle ne veut pas faire sur le plan sexuel ou faire pression sur elle), ainsi que la violence et les abus facilités par la technologie (VAFT) en sont d'autres exemples. Les VAFT peuvent être définis de manière générale comme une forme d'abus ou de comportement contrôlant comportant l'utilisation de la technologie pour contraindre, traquer, surveiller ou harceler une autre personne.

Un traumatisme (individuel) est un événement ou une circonstance entraînant un préjudice physique, émotionnel ou mettant la vie en danger. Le traumatisme a des impacts négatifs durables sur la santé et le bien-être physiques, mentaux, émotionnels, sociaux et spirituels d'une personne.

La retraumatisation est la réactivation des symptômes du traumatisme par des pensées, des souvenirs ou des sentiments liés à l'expérience passée du traumatisme, ce qui peut se produire à la suite d'un événement déclencheur lorsque les circonstances vous rappellent un traumatisme antérieur, ou que vous parlez d'un traumatisme.

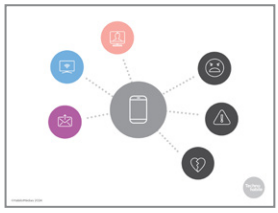
7. Voici quelques signes possibles de la retraumatisation.

- Pensées négatives associées à la peur ou à d'autres émotions ressenties lors du traumatisme
- Souvenirs (*flashbacks*)
- Dissociation
- Problèmes de concentration
- Sentiment de nervosité, d'anxiété ou de tension ou être facilement surpris
- Fatigue

- Détresse ou réactions physiques fortes (p. ex. respiration ou rythme cardiaque rapide, transpiration)
- Sentiment d'isolement, de distance ou de repli sur soi
- Sentiment intense de culpabilité, de colère, de peur, de tristesse, de honte ou de désespoir
- Sentiment d'incapacité à contrôler ses émotions (p. ex. incapacité de se calmer, sentiment de sécurité amoindri)

Pour les participants en personne : Nous vous indiquerons le contenu de chaque partie de cet atelier afin que vous puissiez vous retirer quelques minutes si vous préférez ne pas aborder un sujet particulier. N'oubliez pas de lever le pouce avant de partir pour que nous sachions que vous allez bien ou si vous avez besoin d'aide.

Pour les participants à distance : Nous vous encourageons à fermer votre micro et votre caméra si vous vous sentez bouleversé et avez besoin de prendre une pause. N'oubliez pas d'utiliser l'émoji de pouce levé (dans l'onglet des réactions) avant de quitter pour que nous sachions que vous allez bien ou si vous avez besoin d'aide.



8. De nos jours, une grande partie de nos vies, dont nos relations, se passe en ligne. Cela a beaucoup de bons côtés : cela peut nous aider à rester en contact avec des amis et des membres de la famille et nous aider à rencontrer de nouvelles personnes qui partagent nos centres d'intérêt.

Mais il y a aussi des risques. La technologie peut être utilisée pour abuser de nous, nous harceler et nous espionner. Nous devons donc savoir comment nous protéger et protéger nos appareils.

9. L'une des étapes les plus importantes pour rester en sécurité dans nos relations en ligne est quelque chose que nous devrions tous faire : assurer la sécurité de nos comptes et de nos appareils.

10. La meilleure façon de sécuriser vos comptes et vos appareils est d'avoir un bon mot de passe.

N'utilisez aucun des mots de passe affichés sur la diapositive. Déverrouiller un appareil par empreinte digitale ou reconnaissance faciale n'est pas non plus un moyen sécurisé, sauf si vous combinez cette méthode avec un mot de passe puisque quelqu'un qui a accès à votre téléphone pourrait le pointer vers votre visage ou vous le faire toucher du bout du doigt.

11. Mais même lorsque vous n'utilisez pas un mot de passe commun oui qui est facile à deviner, celui-ci peut tout de même être considéré comme « faible ». En effet, il y a trois règles à retenir pour créer un mot de passe dit « fort»:

D'abord, il n'est pas composé que d'une seule chose. Un bon mot de passe combine des mots, des lettres et des symboles.

Ensuite, il ne doit pas être composé d'un seul mot.

Enfin, il ne doit pas être utilisé sur plus d'un site.

12. Une autre option qui s'offre à vous est d'utiliser un *gestionnaire de mots de passe*. Il s'agit d'un programme qui gère vos mots de passe pour différents comptes. Il crée un mot de passe différent, presque impossible à trouver, pour chacun de vos comptes, puis s'occupe de remplir les identifiants de connexion pour vous.

Les gestionnaires de mots de passe peuvent être utiles, mais ils servent uniquement à vous éviter d'avoir à vous rappeler plusieurs mots de passe pour différents sites Web. Vous devez tout de même vous assurer d'avoir un mot de passe fort auprès du gestionnaire de mots de passe, car quiconque réussit à se connecter à ce compte a accès à tous vos autres comptes.

Bitwarden est l'un des gestionnaires de mots de passe populaires à offrir une version de base gratuite.

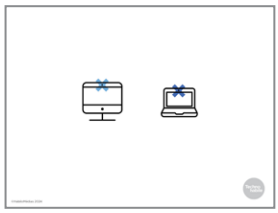
13. Les appareils Apple, comme les iPhone et les Mac, disposent également de leur propre gestionnaire de mots de passe intégré, que vous pouvez utiliser si vous disposez d'un compte iCloud. Pour l'utiliser, allez d'abord dans les réglages du système, puis cliquez sur votre nom et ensuite sur « iCloud ». (Sur les appareils plus anciens, vous devrez peut-être cliquer sur « Identifiant Apple », puis sur « iCloud ».)

14. Activez ensuite la fonction « Mots de passe et trousseau iCloud ».

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

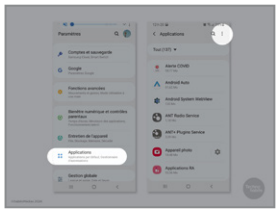
Si vous avez activé l'authentification à deux facteurs, en plus d'entrer votre mot de passe, vous recevrez également sur votre téléphone un message texte contenant un code à usage unique. Vous devrez entrer ce code ainsi que votre mot de passe pour ouvrir une session.

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.

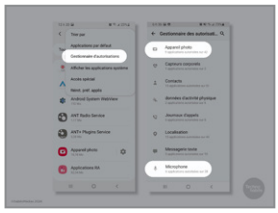


16. Une autre façon de protéger votre appareil consiste à couvrir les caméras sur les ordinateurs portables et les autres appareils lorsque vous ne les utilisez pas, de sorte que l'on ne vous verra pas lorsque vous ne le souhaitez pas. Vous pouvez le faire avec un post-it (ou quelque chose du genre), qui est facile à enlever quand vous voulez utiliser la caméra.

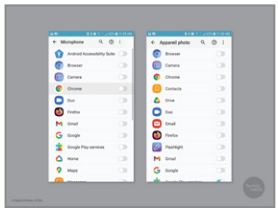
17. Éteindre le microphone de vos appareils est un peu plus compliqué, mais c'est aussi une bonne habitude à prendre. Nous verrons comment le faire sur un appareil mobile.



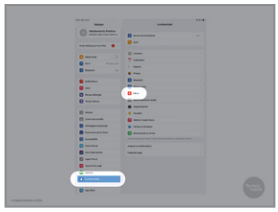
18. Sur les appareils Android, appuyez sur « paramètres » (l'icône représentant un engrenage), puis sur « applications ». Appuyez sur les trois points en haut à droite de l'écran.



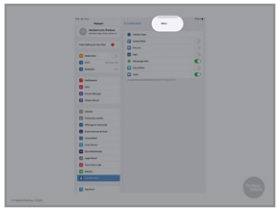
19. Dans la fenêtre qui apparaît, appuyez sur « autorisations d'application ». Vous pouvez maintenant appuyer sur « microphone » ou « appareil photo ».



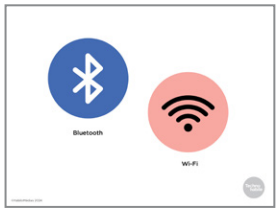
20. Vous pouvez maintenant voir toutes les applications ayant accès au microphone ou à l'appareil photo. Faites-les glisser vers la gauche pour les désactiver - vous pourrez toujours les réactiver plus tard.



21. Sur iPhone ou iPad, accédez aux paramètres et appuyez sur « confidentialité ».

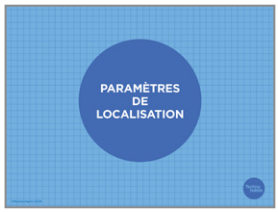


22. Ensuite, appuyez sur « microphone » et glissez tous les éléments vers la gauche. Vous pouvez faire de même pour l'appareil photo.



23. Les fonctionnalités Bluetooth et Wi-Fi rendent votre appareil visible aux autres appareils. Elles sont activées par défaut. Lorsque vous ne les utilisez pas, désactivez-les en accédant aux réglages ou en appuyant sur les icônes Bluetooth et Wi-Fi.

Vous pouvez également accéder à vos réglages Bluetooth (Réglages > Bluetooth) et rechercher tous les appareils jumelés à votre téléphone. Si vous voyez des appareils que vous ne reconnaissez pas, désactivez le jumelage.

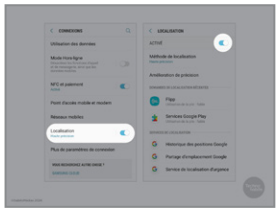


24. Les téléphones sont également configurés par défaut pour partager votre *localisation*, c'est- à-dire l'endroit où vous vous trouvez. Ils le font principalement par le biais du système mondial de localisation (GPS).

Le risque pour la sécurité et la vie privée est bien réel. Il est donc important de savoir comment désactiver les paramètres de localisation.

Le GPS envoie un signal qui indique où se trouve votre appareil. Vous devez le 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.

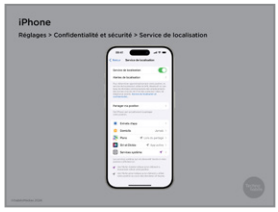
25. Pour désactiver la géolocalisation sur les appareils Android, vous devez désactiver le GPS, comme nous l'avons vu il y a quelques minutes pour les réglages du micro et de la caméra.



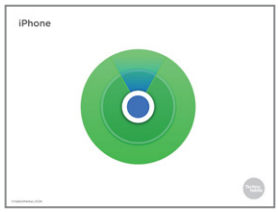
26. Pour désactiver la localisation, rendez-vous dans Paramètres, déroulez jusqu'à Position, touchez l'icône correspondante, puis touchez le bouton pour désactiver la fonction.

27. Vous pouvez également empêcher certaines personnes de voir votre position. Pour ce faire, ouvrez Google Maps, tapez sur votre photo de profil, puis sur « Partage de position ».

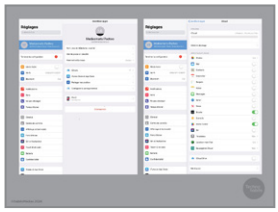
Appuyez sur la photo de profil de la personne qui ne devrait pas voir votre position, puis sur « Arrêter ».



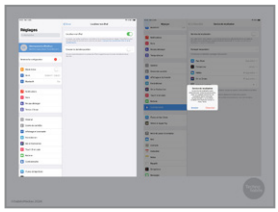
28. Sur un appareil iPhone, ouvrez les réglages. Tapez sur « Confidentialité et sécurité », puis sur « Service de localisation », ou cherchez les mots « Service de localisation », et désactivez le partage de position.



29. Le partage de la localisation et les applications vous aidant à trouver votre téléphone fonctionnent toujours si votre téléphone est éteint. Vous devez donc désactiver ces applications spécifiques dans les réglages.

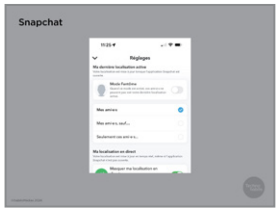


30. Sur les appareils iPhone et iPad, vous devez désactiver la fonction « Localiser » (mon iPhone ou iPad). Pour ce faire, ouvrez les réglages, puis tapez le nom de l'appareil dans le coin supérieur gauche.

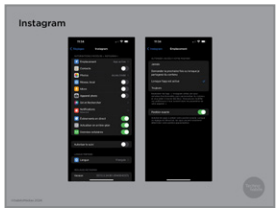


31. Tapez ensuite sur le bouton à bascule « Localiser mon iPhone » ou « Localiser mon iPad » et sur « Ok » dans la boîte qui apparaît.

32. Certaines applications de médias sociaux partagent également votre position. Voyons comment vous pouvez désactiver cette fonction.



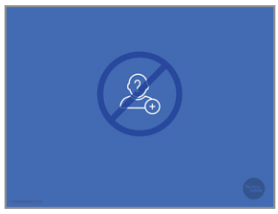
33. Snapchat affiche votre position sur une carte. Pour désactiver cette fonction, ouvrez Snapchat et appuyez sur l'icône de votre profil. Tapez ensuite sur les trois points verticaux en haut à droite et descendez jusqu'à la section « Qui peut… ». Si vous appuyez sur « Voir ma position », une fenêtre contextuelle indiquant « Mode fantôme » s'affiche. Activez la fonction en faisant basculer le bouton.



34. Sur Facebook ou Instagram, vous pouvez désactiver la localisation en appuyant sur Paramètres > Confidentialité > Services de localisation, puis en appuyant sur le bouton situé à côté. La plupart des autres réseaux sociaux placent la localisation à des endroits similaires, dans les réglages sous « Confidentialité » ou « Sécurité ».

35. Avant de poursuivre, arrêtons-nous un instant pour voir si quelqu'un souhaite faire une pause ou a besoin de soutien.

36. Voyons maintenant de manière plus générale comment vous pouvez gérer votre vie privée sur les réseaux sociaux.



37. Du point de vue de la protection de la vie privée, il existe deux types de réseaux sociaux : les réseaux *fermés* comme Facebook, où deux personnes doivent se mettre d'accord pour être connectées, et les réseaux *ouverts* comme Twitter, où vous pouvez suivre quelqu'un sans qu'il vous suive nécessairement en retour.

Vous devez faire attention à qui vous acceptez comme ami sur un réseau social fermé, parce qu'ils verront tout ce que vous publiez et pourront partager vos publications avec leurs amis, qui ne sont pas forcément les vôtres.

N'acceptez pas les demandes d'amis de personnes que vous ne connaissez pas ou auxquelles vous ne faites pas confiance.

38. Presque tous les réseaux sociaux ont également des *paramètres de confidentialité* qui vous donnent un peu plus de contrôle sur qui voit ce que vous publiez.

Vous pouvez modifier les paramètres de confidentialité *par défaut*, de sorte que toutes vos publications sont vues par plus ou moins de personnes que d'habitude.

Sur un grand nombre de réseaux sociaux, vous pouvez également choisir différents paramètres de confidentialité pour chaque publication, de sorte que vous pouvez rendre certaines totalement publiques ou décider que seuls certains de vos amis pourront la voir.

Nous allons maintenant voir comment modifier ces paramètres dans Facebook.

39. Pour modifier vos paramètres sur Facebook, cliquez sur « paramètres », puis sur « confidentialité » dans le menu de gauche. Trouvez « qui peut voir vos futures publications » et cliquez sur « modifier ».

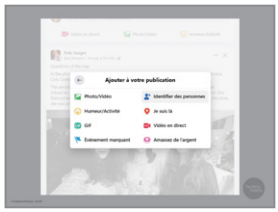
40. Vous pouvez choisir l'option « Public », ce qui signifie que les personnes qui ne sont pas vos amis verront vos publications. Cette option n'est pas une bonne idée puisqu'elle vous donne le niveau le moins élevé possible de protection de la vie privée.

Vous pouvez aussi choisir l'option « Ami(e)s sauf… » pour exclure certains amis, l'option « Ami(e)s spécifiques » pour que seuls certains de vos amis voient vos publications, ou encore l'option « Moi uniquement » pour que vous soyez le seul à les voir.

L'option « Moi uniquement » peut être un bon choix si vous publiez souvent des contenus que vous souhaiteriez ne pas avoir publiés. Définissez par défaut l'option « Moi uniquement », puis, quelques heures plus tard, revenez sur la publication et décidez si vous voulez finalement que vos amis la voient.

41. Vous pouvez également contrôler qui voit chacune de vos publications en choisissant « Personnaliser » dans le menu déroulant.

42. Si vous voulez, vous pouvez laisser tous vos amis voir la plupart de ce que vous publiez, mais partager certaines publications avec seulement quelques-uns d'entre eux - ou même une seule personne.

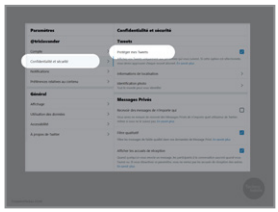


43. Beaucoup de réseaux sociaux vous laissent « identifier » quelqu'un dans une publication ou sur une photo. Cela signifie que si quelqu'un vous cherche sur ce réseau, il verra tout ce qui a été publié avec votre nom.

Si vous cliquez sur « journal et identification » dans le menu de gauche, vous pouvez décider qui peut voir les publications où vous êtes identifiés. Cela signifie que vous pouvez empêcher les amis de vos amis de les voir.

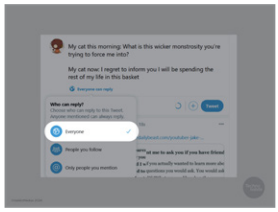
Vous devriez également configurer les paramètres de sorte que vous soyez prévenu chaque fois qu'on vous identifie dans une publication ou sur une photo. Ainsi, vous pouvez demander à quelqu'un qui publie une photo de vous de la retirer immédiatement si vous ne l'aimez pas.

44. Vous pouvez également personnaliser les *paramètres de confidentialité* de vos réseaux sociaux.



45. Il est plus difficile de contrôler qui voit ce que vous publiez sur un réseau ouvert, mais la plupart d'entre eux offrent un outil, comme « Protéger mes posts » sur X, qui oblige les gens à obtenir votre permission pour voir vos tweets.

Pour le faire sur X, cliquez sur « profil», allez dans « confidentialité et securité», puis cliquez sur « confidentialité et sécurité » et cochez la case qui dit « protéger mes Posts. »



46. Vous pouvez également contrôler qui peut répondre à vos tweets. Avant de publier, cliquez ou appuyez sur « tout le monde peut répondre », puis choisissez qui peut vous répondre.

47. Vous pouvez également modifier les paramètres de certains réseaux sociaux pour qu'ils vous avertissent lorsqu'un nouvel appareil se connecte à votre compte.

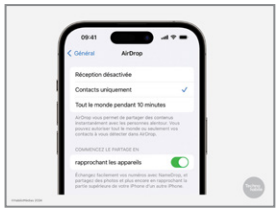
48. Sur Facebook, accédez à vos paramètres et cliquez sur Sécurité et connexion à gauche.

49. Cliquez ensuite sur « Recevoir des alertes en cas de connexions non reconnues ». Vous pourrez ainsi savoir si quelqu'un se connecte à votre compte à partir d'un nouvel appareil en recevant un courriel à l'adresse que vous avez utilisée lors de votre inscription.

Si vous recevez cette alerte et que ce n'est pas vous qui vous êtes connecté, changez immédiatement votre mot de passe.

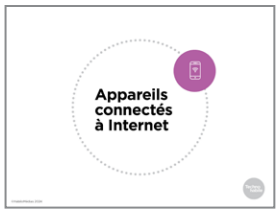
50. Les appareils Apple sont également dotés d'une fonctionnalité appelée AirDrop qui permet aux utilisateurs de partager des fichiers entre eux. Si elle est activée, certaines personnes pourraient s'en servir pour envoyer des photos ou autres éléments indésirables sur votre appareil.

Pour éviter cela, rendez-vous dans Réglages et touchez l'icône Airdrop.



51. Vous y verrez ainsi les réglages qui y sont associés. 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. (La désactivation est probablement votre meilleur choix puisqu'elle vous offre davantage de protection.)

Vous pouvez également la configurer pour recevoir des messages de n'importe qui pendant 10 minutes. La fonction passera ensuite en mode « Contacts uniquement ».



52. Les appareils connectés à Internet, y compris les haut-parleurs intelligents comme Amazon Echo et Google Home, constituent un autre risque pour la vie privée. Vous ne pouvez pas désactiver le microphone, car ils doivent pouvoir entendre la commande qui les « réveillera ».

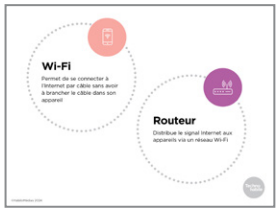
Si vous avez de tels appareils connectés, sachez qu'ils peuvent être utilisés pour vous espionner. Vous pouvez les déconnecter du Wi-Fi ou les désactiver si vous avez besoin d'avoir une conversation privée ou, encore, discutez en dehors de votre maison.

Les « jouets intelligents » connectés à Internet et les appareils portables comme les montres intelligentes ou les porte-clés GPS peuvent également constituer un risque pour la vie privée. Même les localisateurs pour animaux peuvent permettre aux gens de savoir où vous êtes.

53. Voici quelques conseils pour gérer votre vie privée lorsque vous utilisez des appareils intelligents.

Créez un compte d'invité sur votre réseau Wi-Fi. En ne connectant pas votre appareil à votre compte Wi-Fi principal, vous limitez ainsi les données qui sont recueillies.

54. Votre fournisseur de service Internet, comme Rogers, Bell, TELUS, Vidéotron ou TekSavvy, vous a peut-être fourni une application qui vous permet de modifier les paramètres de votre routeur Internet.



55. Votre routeur envoie les signaux WiFi à vos appareils. Si vous avez Internet à domicile, la compagnie qui vous fournit le service fournit probablement votre routeur.

56. Cette application devrait comporter une option permettant de créer un réseau pour les invités. S'il n'y en a pas, communiquez avec votre fournisseur de service Internet pour demander de l'aide.

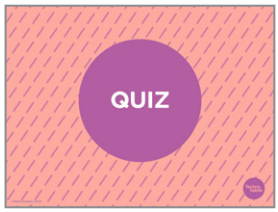
57. Il est également utile *d'apprendre à connaître l'application*. La plupart des appareils intelligents n'ayant pas d'écran, ils sont presque tous dotés d'une application que vous installez sur votre téléphone ou tablette. L'application permet de modifier les différents paramètres de l'appareil. Une grande partie des mesures de protection de la vie privée que vous pouvez prendre suppose la modification des paramètres de l'application. Il est donc judicieux de se familiariser avec l'application et son utilisation. Examinons maintenant de plus près certains de ces paramètres.

58. *Modifiez le mot d'activation.* Les haut-parleurs intelligents ont également un « mot d'activation » qui les invite à commencer à vous écouter, comme « Ok Google » ou « Alexa ». Pour vous assurer que l'appareil ne se « réveille » pas par accident, modifiez le mot d'activation. (Les haut-parleurs intelligents ne permettent pas tous de modifier le mot d'activation. Certains appareils ne proposent qu'une gamme limitée d'options de mots d'activation. Choisissez donc celui qui vous convient le mieux.)

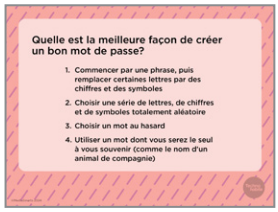
Désactivez tous les micros et les caméras lorsque vous n'en avez pas besoin. Bon nombre d'appareils intelligents dotés de micros ou de caméras disposent d'interrupteurs physiques ou d'options dans l'application pour les désactiver.

Couvrez également les caméras lorsque vous ne les utilisez pas. La plupart des appareils intelligents dotés de caméras ont une lumière qui s'allume lorsque la caméra est active, mais pour plus de sécurité, vous devriez placer une note autocollante ou quelque chose de similaire sur tout appareil intelligent dont la caméra n'a pas besoin d'être allumée en permanence.

Si vous envisagez acheter un appareil comme une sonnette intelligente pour des raisons de sécurité, gardez à l'esprit que différents appareils recueillent plus ou moins d'informations que d'autres. Recherchez un appareil qui stocke les vidéos localement seulement (sur un disque dur ou une carte mémoire) au lieu de les télécharger sur la plateforme.

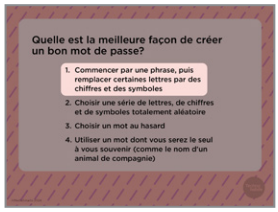


59. Faisons un petit quiz pour vérifier que vous avez bien assimilé tout ce que nous avons vu jusqu'à présent.



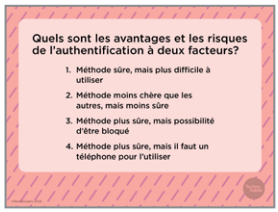
60. Parmi les réponses énumérées, quelle est la meilleure façon de créer un bon mot de passe?

- Devriez-vous commencer par une phrase, puis remplacer certaines lettres par des chiffres et des symboles?
- Utiliser une chaîne de lettres, de chiffres et de symboles totalement aléatoire?
- Choisir un mot de passe au hasard?
- Ou utiliser un mot dont vous êtes le seul à vous souvenir, comme le nom de votre animal de compagnie?



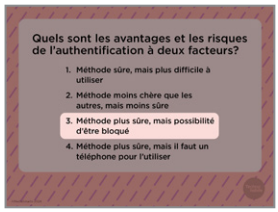
61. Un mot choisi au hasard est trop facile à deviner, et une série totalement aléatoire de lettres, de chiffres et de symboles est trop difficile à mémoriser. Et toute personne qui vous connaît pourrait connaître le nom de votre animal de compagnie.

Commencez plutôt par une phrase, comme « J'aime les bananes » et remplacez certaines lettres par des chiffres et des symboles (comme des points d'exclamation).



62. Quels sont les avantages et les risques de l'authentification à deux facteurs?

- Cette méthode est-elle sûre, mais plus difficile à utiliser?
- Cette méthode est-elle moins chère que les autres, tout en étant moins sûre?
- Cette méthode est-elle plus sûre, tout en bloquant possiblement votre accès à la plateforme?
- Cette méthode est-elle plus sûre, mais il vous faut un téléphone pour l'utiliser?



63. L'authentification à deux facteurs est plus sûre, mais elle pourrait bloquer votre accès à la plateforme.

Vous n'avez pas besoin d'un téléphone pour l'authentification à deux facteurs, mais simplement d'un autre appareil ayant accès à Internet. Vous pouvez également vous procurer un dispositif comme YubiKey qui permet une authentification physique à deux facteurs : branchez l'appareil sur votre téléphone ou ordinateur, ou tapez-le sur un dispositif qui l'accepte, ce qui équivaut à entrer un code de confirmation.

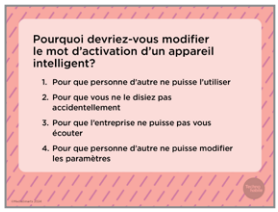
La plupart des applications d'authentification à deux facteurs, comme Google Authenticator ou Microsoft Authenticator, sont gratuites. Elles peuvent parfois être difficiles à configurer, mais ne sont généralement pas très compliquées à utiliser.

Toutefois, il existe un risque : si vous perdez l'accès au deuxième facteur (votre téléphone, l'application ou votre dispositif YubiKey), vous risquez d'être complètement bloqué. Par exemple, si vous perdez votre téléphone, vous ne pourrez pas obtenir un code par texto, et si vous ne pouvez pas accéder à votre compte de messagerie, vous ne pourrez pas l'obtenir par courriel.

64. Comment s'appelle l'outil qui permet de cacher votre position sur Snapchat?

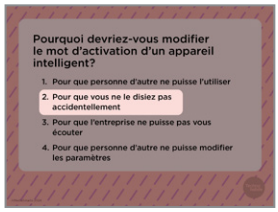
- Mode Snap
- Mode privé
- Mode caché
- Mode fantôme

65. Mode fantôme! Si vous avez Snapchat sur votre téléphone, optez pour le mode fantôme afin que les gens ne puissent pas voir qui vous êtes.



66. Pourquoi devriez-vous modifier le mot d'activation d'un appareil intelligent?

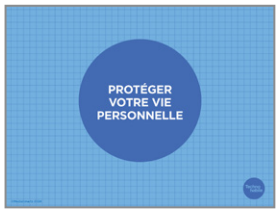
- Pour que personne d'autre ne puisse l'utiliser
- Pour que vous ne le disiez pas accidentellement
- Pour que l'entreprise ne puisse pas vous écouter
- Pour que personne d'autre ne puisse modifier les paramètres



67. Vous devriez modifier le mot d'activation pour que vous ne le disiez pas accidentellement.

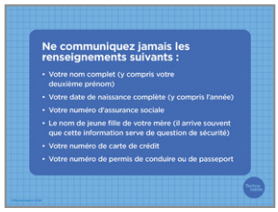
Malheureusement, la modification du mot d'activation n'empêche pas l'entreprise de savoir ce que vous dites à vos appareils intelligents. Cette mesure pourrait empêcher d'autres personnes de l'utiliser, jusqu'à ce qu'elles vous entendent dire le mot d'activation.

68. Avant de poursuivre, arrêtons-nous un instant pour voir si quelqu'un souhaite faire une pause ou a besoin de soutien.



69. Parlons maintenant de la manière dont vous pouvez protéger votre vie privée.

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.



70. Commençons par protéger vos informations personnelles. Certaines informations ne doivent jamais être partagées en ligne. Ces informations pourraient permettre à quelqu'un d'accéder à votre compte bancaire ou d'obtenir une nouvelle carte de crédit à votre nom.

Votre nom complet (y compris votre deuxième prénom)

Votre date de naissance complète (y compris l'année)

Votre numéro d'assurance sociale

Le nom de jeune fille de votre mère (il arrive souvent que cette information serve de question de sécurité)

Votre numéro de carte de crédit

Votre numéro de permis de conduire ou de passeport

71. Parlons maintenat d'astuces pour les rencontres en ligne.

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.

72. 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.

73. Il est également utile de vérifier quels outils de sécurité ont été intégrés au site ou à l'application de rencontre. Exemple : Comment signaler un cas de harcèlement ou l'envoi de photos indésirables? Comment bloquer une personne si nécessaire?

Il est important de vous fier à votre instinct lorsque vous entamez une relation en ligne. Si quelqu'un vous met de la pression ou se montre agressif en demandant à vous rencontrer en personne, vous demande des photos ou se met en colère si vous ne répondez pas à ses messages, bloquez-le immédiatement. Nous verrons comment procéder un peu plus loin dans l'atelier.

74. 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.

75. 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.

76. 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.

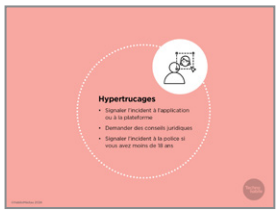
Vous pouvez demander à la personne concernée de cesser de le partager ou de le retirer. Même si elle refuse ou ne répond pas, gardez un dossier des textos ou des courriels envoyés afin de démontrer ultérieurement que le partage s'est effectué sans votre consentement.

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.



77. Les hypertrucages, c'est-à-dire des photos ou des vidéos qui vous montrent en train de faire quelque chose que vous n'avez jamais fait, constituent un autre risque. Les hypertrucages qui mettent en scène des femmes dans des contenus pornographiques sont de plus en plus fréquents, et ce sont souvent des femmes et des jeunes filles ordinaires qui en sont victimes, et pas seulement des célébrités.

Malheureusement, on ignore si la loi sur le partage d'images intimes non consensuelles s'applique aux hypertrucages. Si vous avez plus de 18 ans et que vous apparaissez dans un hypertrucage, la meilleure solution consiste à le signaler à l'application ou au site Web qui l'a publié. (La plupart des sites pornographiques commerciaux disposent de politiques contre les hypertrucages non consensuels.) Si cette mesure ne fonctionne pas, vous pouvez envisager d'intenter une poursuite au civil : consultez un avocat ou une clinique d'aide juridique pour connaître les options qui s'offrent à vous. (Si vous avez moins de 18 ans, la photo ou la vidéo reste légalement de la pornographie juvénile, même si elle est générée par l'intelligence artificielle.)

78. Avant de poursuivre, arrêtons-nous un instant pour voir si quelqu'un souhaite faire une pause ou a besoin de soutien.

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

80. 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.

81. Pour télécharger des fichiers vers un compte Google, rendez-vous sur drive.google.com et cliquez sur le bouton « Nouveau » en haut à gauche. Vous pouvez télécharger des fichiers individuels ou un dossier entier, ce qui vous fera gagner du temps si vous placez d'abord tout ce que vous voulez télécharger dans un seul dossier.

Une clé USB est une clé physique que vous branchez dans votre ordinateur. Elle se présente comme un dossier dans lequel vous pouvez copier des fichiers. Comme elle se branche sur le port USB de l'ordinateur, vous ne pouvez pas utiliser une clé USB sur la plupart des téléphones.

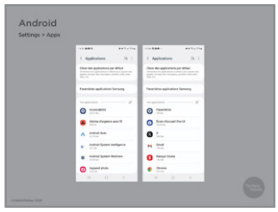
82. Si les choses ne sont pas amicales et que vous cherchez du soutien pour sortir d'une relation, utilisez les outils que nous avons abordés dans cet atelier pour préserver la confidentialité de vos recherches. (Vous trouverez plus d'informations à ce sujet dans l'atelier *Explorer la vie privée en ligne*.)

Vérifiez de nouveau que votre appareil ne contient pas de logiciels espions ou traqueurs qui indiquent à quelqu'un d'autre où vous vous trouvez ou ce que vous faites.

Certains logiciels espions portent des noms évidents comme « Mobile Tracker » ou « Spy Tracker », mais en général, vous devez vous méfier de toute application sur votre appareil que vous ne reconnaissez pas.

Voyons maintenant comment procéder.

83. Sur un iPhone, balayez l'écran d'accueil vers la droite jusqu'à ce que vous voyiez la bibliothèque d'applications. Tapez dans le champ de recherche au haut de l'écran, puis parcourez la liste des applications et supprimez celles que vous ne reconnaissez pas.



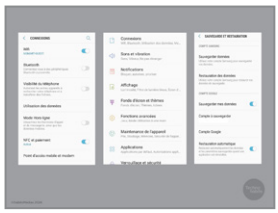
84. Sur un appareil Android, allez dans les réglages, puis dans « Applications » et « Voir toutes les applications », ou recherchez le mot « Applications.

Utilisez un moteur de recherche pour trouver les noms des applications que vous ne reconnaissez pas. Si la recherche indique qu'il s'agit d'un logiciel espion, ou ne montre pas qu'il s'agit d'une application légitime, désinstallez-la.

85. Il existe également des applications comme Certo et Incognito qui analysent vos appareils à la recherche de logiciels espions.

86. Si vous avez un iPhone, vous pouvez également activer le mode de confinement, qui vous protège de la plupart des logiciels espions. Il limite aussi l'utilisation d'applications comme FaceTime et Safari.

Pour activer le mode de confinement, allez dans « Réglages », puis dans « Confidentialité et sécurité » et faites basculer le bouton « Mode de confinement ».



87. Aucune de ces méthodes n'est efficace à 100 %.

Si vous avez pris cette mesure et que vous pensez toujours que votre ex-partenaire vous suit à la trace, le seul moyen d'être absolument sûr de vous débarrasser des logiciels espions est de procéder à une « réinitialisation d'usine » de votre téléphone et d'en effacer complètement tout le contenu.

Sur un téléphone Android, allez dans les réglages, puis dans « Sauvegarde et réinitialisation » et « Réinitialisation d'usine des données ». Cette opération effacera tout ce que vous avez sauvegardé sur le téléphone et toutes les applications qui y ont été téléchargées.

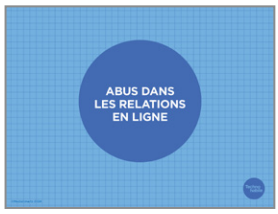
Avant de procéder à cette opération, notez sur une feuille tous vos contacts importants (p. ex. numéros de téléphone et adresses électroniques d'amis proches ou de membres de votre famille) et toute autre information essentielle contenue dans votre téléphone, et conservez cette feuille dans un endroit sûr. Une réinitialisation efface tout ce qui se trouve sur votre téléphone, y compris vos applications et contacts.

Si vous utilisez votre adresse électronique pour l'authentification à deux facteurs, vous devrez réinstaller votre application de messagerie et vous connecter de nouveau.

88. Sur un iPhone ou un iPad, tapez sur « Réglages », puis sur « Général » et « Réinitialiser ». Tapez ensuite sur « Effacer contenu et réglages » et entrez votre code d'accès ou identifiant Apple.

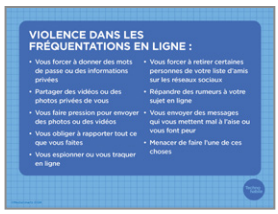
Quel que soit le type d'appareil que vous utilisez, vous ne devez pas le restaurer à partir d'une sauvegarde ou d'un service infonuagique après l'avoir réinitialisé. Vous risqueriez de réinstaller le logiciel espion qui s'y trouvait.

89. Avant de poursuivre, arrêtons-nous un instant pour voir si quelqu'un souhaite faire une pause ou a besoin de soutien.



90. Comme tout de nos jours, la violence relationnelle s'est également installée en ligne.

Voyons maintenant ce qu'est la violence relationnelle en ligne et la manière de la reconnaître.



91. Ce qu'il faut savoir de la violence relationnelle en ligne, c'est qu'il est parfois difficile de reconnaître qu'il *s'agit bien* d'un abus. Certains comportements abusifs sont dépeints comme romantiques par les médias (films, émissions de télévision…), et les agresseurs ont tendance à dire qu'ils font ces choses par amour - ou que vous avez besoin d'accepter ces comportements pour montrer que vous *les* aimez.

Voici certaines choses que votre partenaire ne devrait jamais faire ou vous demander de faire :

Vous forcer à lui donner vos mots de passe, ou toute autre information privée Partager des photos ou des vidéos privées de vous

Vous faire pression pour envoyer des photos ou des vidéos que vous ne voulez pas prendre ou partager

Attendre de vous que vous lui disiez toujours où vous êtes et ce que vous faites Vous espionner ou vous traquer en ligne

Vous forcer à retirer certaines personnes de votre liste d'amis sur les réseaux sociaux Répandre des rumeurs à votre sujet en ligne

Envoyer des messages qui vous mettent mal à l'aise ou vous font peur

Ou menacer de faire l'une de ces choses.

Pour de plus amples renseignements, consultez la trousse à outils *Sécurité et confidentialité technologiques* de Sécurité technologique Canada.

92. Il est important d'obtenir des preuves du harcèlement en ligne au cas où vous décideriez de demander une aide juridique.

Les captures d'écran demeurent la façon la plus sûre de le faire. Découvrez comment faire des captures d'écran sur différents appareils et navigateurs sur le site take-a-screenshot.org.
Si vous pensez que l'appareil que vous utilisez n'est pas en sécurité, transférez les captures d'écran sur une clé USB ou un disque dur externe.

Qu'il s'agisse de harcèlement, de logiciels espions, d'hypertrucages ou de sextos, il est important de garder une trace de tout ce qui s'est passé, que vous pourrez remettre à la police ou à un avocat si vous décidez d'intenter une action en justice. Pour ce faire, vous pouvez utiliser le tableau des preuves qui accompagne cet atelier.

Si cette tâche vous perturbe ou vous contrarie trop, demandez à une personne de confiance de vous aider à le faire.

93. Cependant, vous n'avez pas à continuer de subir du harcèlement en ligne. Une fois que vous avez enregistré les preuves de ce qui s'est produit jusqu'à présent, vous pouvez bloquer l'expéditeur. Bloquer quelqu'un ne supprime pas vos anciennes conversations privées.

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.

94. 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.

95. Si vous avez quitté une relation et avez besoin de vous cacher de votre ancien partenaire, vous pouvez prendre certaines mesures pour l'empêcher de vous trouver en ligne. Vous n'aurez probablement pas à le faire éternellement, mais il peut s'agir d'une mesure temporaire importante pour assurer votre sécurité.

Même sur des réseaux ouverts comme X (anciennement Twitter), il existe des moyens de passer votre compte en privé. Passer en revue vos listes d'amis ou d'abonnés afin de vous assurer que vous connaissez chaque personne et que ce sont des personnes de confiance.

Vous pouvez également créer de nouveaux comptes que vous utiliserez jusqu'à ce que vous vous sentiez en sécurité. Si vous le faites, utilisez un nouveau nom sous lequel on ne pourra pas vous reconnaître et utilisez une photo de profil générique comme un coucher de soleil. Mettez une autre ville en lieu de résidence sur votre profil.

Ne publiez pas d'informations sur votre travail, l'école que vous fréquentez, votre famille ou toute autre chose qui pourrait vous rendre plus facile à trouver, et n'indiquez pas votre emplacement lorsque vous publiez des messages ou des photos. (Désactiver le GPS de votre appareil est un bon moyen d'éviter que votre position ne soit automatiquement indiquée,

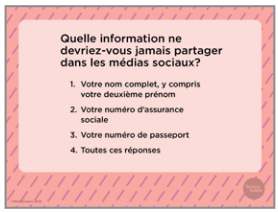
mais il est également important de vérifier avant et après chaque publication que votre position n'a pas été ajoutée par défaut.)

Si vous souhaitez publier un article sur un lieu où vous êtes allé ou un événement auquel vous avez assisté, attendez de ne plus y être pour le faire.

96. Si vous ne souhaitez pas couper complètement le contact avec votre ex-partenaire, par exemple si vous avez la garde partagée des enfants, si vous êtes encore en train de réfléchir au partage des biens ou si vous voulez être au courant de son humeur et de son état mental, envisagez de créer des comptes de messagerie ou de réseau social distincts, uniquement pour rester en contact avec lui. Vous pouvez utiliser Google Voice ou un service téléphonique virtuel similaire pour les appels vocaux.

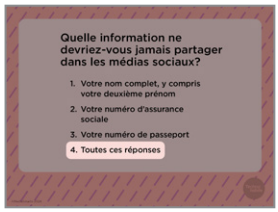
97. Après avoir quitté une relation abusive, vous pouvez également modifier les paramètres de vos réseaux sociaux afin d'éviter de voir des « souvenirs » ou d'anciennes publications qui pourraient être bouleversantes. Par exemple, pour Facebook, vous pouvez visiter la page Facebook.com/memories pour modifier vos paramètres de notification ou masquer certaines personnes ou dates.

98. Faisons un petit quiz pour vérifier que vous avez bien assimilé tout ce que nous avons vu jusqu'à présent.

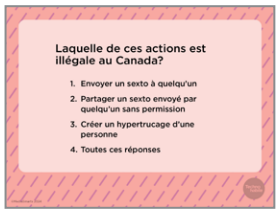


99. Quelle information ne devriez-vous jamais partager dans les médias sociaux?

- Votre nom complet, y compris votre deuxième prénom
- Votre numéro d'assurance sociale
- Votre numéro de passeport
- Toutes ces réponses

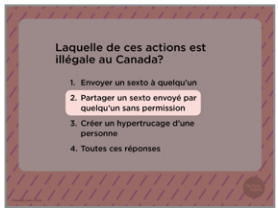


100. Le partage de l'une ou l'autre de ces informations en ligne peut permettre à des personnes d'accéder à vos comptes ou de se faire passer pour vous.



101. Laquelle de ces actions est illégale au Canada?

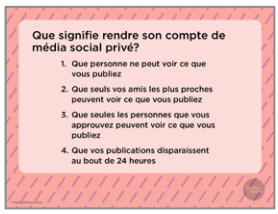
- Envoyer un sexto à quelqu'un
- Partager un sexto envoyé par quelqu'un sans permission
- Créer un hypertrucage d'une personne
- Toutes ces réponses



102. Le partage d'un sexto (ce que la loi appelle une « image intime ») envoyé par quelqu'un sans permission est illégal au Canada, quel que soit l'âge de la personne figurant dans le sexto. En plus des sanctions pénales, un juge peut également ordonner que le sexto soit retiré de n'importe quel endroit sur Internet.

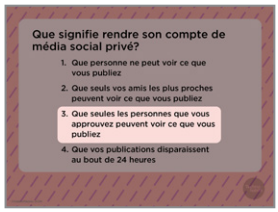
Ce n'est pas un crime d'envoyer un sexto à quelqu'un, à condition qu'il veuille le voir. (Si ce n'est pas le cas, l'envoi pourrait être considéré comme du harcèlement.) Même les expéditeurs de moins de 18 ans ont très peu de chances d'être inculpés pour avoir envoyé un sexto.

À l'heure actuelle, on ignore si la loi sur le partage d'images intimes s'applique également aux hypertrucages.

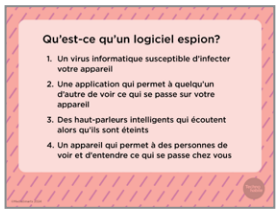


103. Que signifie rendre son compte de média social privé?

- Que personne ne peut voir ce que vous publiez
- Que seuls vos amis les plus proches peuvent voir ce que vous publiez
- Que seules les personnes que vous approuvez peuvent voir ce que vous publiez
- Que vos publications disparaissent au bout de 24 heures

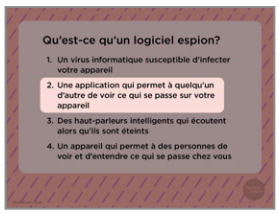


104. Seules les personnes que vous approuvez peuvent voir ce que vous publiez. Même si vous utilisez un réseau social public par défaut comme TikTok, vous pouvez contrôler qui vous suit et qui voit votre contenu en activant la fonction « privé » de votre compte.



105. Qu'est-ce qu'un logiciel espion?

- Un virus informatique susceptible d'infecter votre appareil
- Une application qui permet à quelqu'un d'autre de voir ce qui se passe sur votre appareil
- Des haut-parleurs intelligents qui écoutent alors qu'ils sont éteints
- Un appareil qui permet à des personnes de voir et d'entendre ce qui se passe chez vous



106. Les logiciels espions sont des applications installées sur votre appareil qui permettent à quelqu'un d'autre de vous espionner. N'oubliez pas : si vous ne reconnaissez pas une application, désinstallez-la.

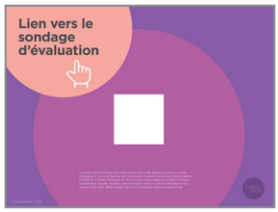
107. Les appareils exploitant Windows sont équipés d'un programme gratuit intégré appelé Windows Defender. Assurez-vous qu'il est activé et qu'aucun autre programme anti-maliciel n'est en cours d'exécution. Si vous en avez plusieurs, ils pourraient se gêner mutuellement.

Pour les appareils Mac et mobiles, installez un outil fiable comme Malwarebytes ou AVG. Ces logiciels sont gratuits, mais ils essayeront tout de même de vous faire payer davantage pour obtenir des services supplémentaires.

108. 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.

109. 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.



110. Avant de faire un compte rendu, nous vous demandons de prendre cinq minutes pour répondre à ce sondage anonyme d'évaluation du programme. Ce sondage est semblable à celui présenté au début de l'atelier. Ces sondages aideront l'équipe de HabiloMédias à déterminer si l'atelier réussit à favoriser les compétences numériques et la confiance des victimes, et guider les futures mises à jour du programme. Vos réponses resteront confidentielles et anonymes. L'objectif est d'évaluer le programme, et non les participantes. Il n'y a pas de bonnes ou de mauvaises réponses; il n'est pas nécessaire de posséder les compétences en question.
Encore une fois, votre participation est entièrement volontaire. Si vous souhaitez participer au sondage, il vous suffit de scanner le code QR à l'aide de l'appareil photo de votre téléphone ou de taper le lien fourni dans votre navigateur pour y accéder. Nous allons de nouveau faire une pause afin de permettre à chacune de remplir le sondage. Prenez tout le temps dont vous avez besoin.

111. Nous en sommes maintenant à la fin de l'atelier. Nous aimerions faire le point avec vous avant que vous quittiez.

Y a-t-il des préoccupations ou des besoins immédiats que nous pourrions vous aider à résoudre? Si nous ne pouvons pas vous aider, nous vous indiquerons des ressources disponibles qui pourraient vous aider.

Avez-vous d'autres questions concernant l'atelier? Si nous connaissons la réponse, nous vous la communiquerons. Dans le cas contraire, nous vous indiquerons des ressources disponibles qui pourraient vous aider ou nous vous mettrons en contact avec quelqu'un qui pourrait vous renseigner.

Terminons par une question : quelle compétence avez-vous acquise au cours de cet atelier et qui vous sera utile dans votre propre vie?