Sécurité technologique Canada

Sécurité et confidentialité en ligne

Une note sur la langue

Dans cette trousse, nous utiliserons parfois le mot femme et les pronoms féminins par souci de simplicité et pour reconnaître l'impact significatif de la violence facilitée par la technologie sur les femmes et les filles. Nous reconnaissons que la VFGFT a également un impact sur les personnes trans, non binaires et bispirituelles. Nous espérons que toutes les personnes touchées par la VFGFT trouveront ces documents utiles.

Misogynie et violence en ligne

Que sont la misogynie et la violence en ligne?

On parle de cybermisogynie lorsqu'Internet et des technologies connexes servent à cibler les femmes, leur causer du tort et exprimer de la haine à leur égard.

La misogynie en ligne peut commencer par:

- Partage d'attitudes, de blagues et de mèmes sexistes
- Traiter les femmes comme des objets
- Stéréotyper les femmes
- Envoi de pornographie non sollicitée ou de «sextos»
- Harcèlement
- Hameçonnage (utilisation d'une fausse identité pour inciter quelqu'un à nouer une relation)

Et conduire à des abus plus graves:

- Doxxing (publier vos informations personnelles en ligne contre votre gré ou encourager les autres à vous cibler)

- Piratage ou usurpation d'identité
- Abus d'images (par exemple, publication de photos intimes)
- Harcèlement, surveillance électronique, contrôle
- Traite et exploitation des personnes
- Menaces ou incitation au viol et au meurtre
- Crimes contre vous ou votre famille

Quelles sont les conséquences de la misogynie et de la violence en ligne?

La cybermisogynie peut avoir une série d'effets psychologiques et émotionnels et influencer la façon dont une femme voit le monde. Cela peut conduire à des sentiments de:

- Peur, pour soi-même ou pour ses proches
- Anxiété, stress et panique
- Insomnie
- Faible estime de soi ou confiance en soi
- Isolement et solitude
- Impuissance et perte
- Colère, cynisme, suspicion, méfiance
- Dépression, suicide.

L'expérience de la misogynie en ligne peut amener une femme à renoncer, partiellement ou complètement, aux espaces en ligne ou à se censurer. Cela a un impact sur la protection de ses droits humains fondamentaux, notamment le droit à la liberté d'opinion et d'expression et le droit à la vie privée.

Au fil du temps, une femme qui renonce aux espaces en ligne pour se sentir en sécurité ou pour se protéger, elle et ses enfants, peut perdre certaines connaissances techniques, et voir diminuer ses possibilités d'emploi, ses contacts sociaux, son accès aux services et d'autres avantages offerts par la technologie.

Quelle est la fréquence de la misogynie et des abus en ligne?

Les Nations unies signalent que 73% des femmes utilisant Internet ont été exposées à des abus en ligne et qu'elles sont 27 fois plus susceptibles d'être victimes de cyberharcèlement que les hommes. La cyberviolence que vivent les jeunes femmes (18-24 ans) comprend souvent des formes plus pernicieuses de harcèlement et de violence.

Quelles sont les causes de la misogynie et de la violence en ligne?

La misogynie et la violence en ligne commencent par des attitudes et des croyances néfastes à l'égard des femmes. Sur Internet, il est plus facile d'abuser d'une personne de manière anonyme et sans les répercussions de la vie réelle.

Certains misogynes s'associent pour cibler les femmes dont l'opinion diverge de la leur, généralement dans le but de les faire taire, les contrôler et susciter la peur. Les femmes sont souvent prises pour cible simplement parce qu'elles sont des femmes.

La cybermisogynie n'est pas la faute de la femme violentée. Nous avons le droit d'accéder aux technologies sans crainte ni violence.

Comment savoir si je suis la cible de cybermisogynie?

Il est parfois difficile de savoir ce que quelqu'un veut vraiment dire en ligne, ou quelle est son intention. Par exemple, lorsqu'un homme que vous appréciez vraiment publie un commentaire sur le fait que vous êtes sexy en utilisant une photo qu'il a prise à votre insu ou sans votre consentement et où vos seins sont visibles, cela peut prêter à confusion. Est-ce un compliment ou une forme de misogynie et de violence en ligne, ou les deux?

Pour savoir ce que vous pensez d'un scénario, vous pouvez vous poser quelques questions:

- Bien qu'il puisse partager son appréciation de votre corps, ses actions communiquent-elles le respect, les limites, le consentement, la confiance et l'attention?
- Quelles autres images ont été prises ou partagées? Comment voulez-vous être représentée en ligne?
- Quels autres comportements ou habitudes pourraient vous donner des indices sur les valeurs, l'empathie et le caractère de cette personne?

Conseils aux femmes qui sont la cible de misogynie et de violence en ligne

Il existe des mesures à prendre pour protéger les femmes contre la misogynie et la violence en ligne. Nous pouvons agir de multiples façons, individuellement ou en groupe, pour lutter contre les attitudes et les croyances néfastes qui conduisent à la violence faite aux femmes.

1. **Sécurisez vos technologies (comptes, appareils, jeux et médias sociaux**) grâce aux Conseils de sécurité et de confidentialité que vous trouverez dans notre Trousse à outils sur la sécurité et la confidentialité technologiques
2. **Ignorez, bloquez ou signalez les trolls et les auteurs de violence si vous pouvez le faire en toute sécurité.** Cela peut vous aider à retrouver votre voix. La plupart des médias sociaux disposent de paramètres permettant d'ignorer, de bloquer ou de signaler les abus. Consultez nos ressources pour plus d'informations.
3. **Connectez-vous avec d'autres personnes qui vont vous soutenir et vous guider.** Vous pouvez trouver des ressources locales sur www.hebergementfemmes.ca.

Préparez-vous à prendre soin de vous. Faites une pause et préparez-vous avant de lire des commentaires en ligne ou de vérifier les messages d'une personne violente. Envisagez de vous déconnecter pendant un certain temps pour prendre soin de vous et retrouver votre équilibre, mais ne vous laissez pas réduire au silence. Partager ce que vous vivez avec quelqu'un qui vous soutient peut vous aider

*La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Si vous êtes la cible de misogynie en ligne, voyez le Projet Shift ou Hack*Blossom's DIY Guide to Feminist Cybersecurity (en anglais seulement) pour d'autres ressources utiles. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de*

sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Tech Safety Project de WESNET, d'après leur ressource *Online Misogyny and Abuse*.

Conseils sur la confidentialité des navigateurs Internet: Paramètres du navigateur

L'utilisation d'Internet débute avec un navigateur. C'est la première étape pour améliorer votre confidentialité sur Internet et contrôler vos informations personnelles. Google Chrome, Mozilla Firefox et Safari offrent tous des paramètres de confidentialité intégrés au navigateur. Ces options comprennent la navigation privée, le contrôle des journaux d'activité, la suppression des cookies, etc.

Pour les survivantes de violence et de harcèlement, l'utilisation de ces options de confidentialité peut améliorer leur sécurité et leur confidentialité, en particulier si elles craignent qu'un auteur de violence puisse accéder physiquement à leur appareil. Ces options peuvent également les aider à mieux contrôler la manière dont leurs informations personnelles sont collectées et stockées. Toutefois, les options de confidentialité du navigateur ne protègent pas contre l'espionnage ou la surveillance à distance si l'auteur utilise un stalkerware. En savoir plus à propos des stalkerware sur les appareils mobiles et les ordinateurs.

Ce document présente diverses options permettant d'améliorer la confidentialité de vos données dans Google Chrome, Mozilla Firefox et Safari. Ce document a été mis à jour en octobre 2022. Il est préférable de rechercher directement le «mode d'emploi» sur ces sites pour obtenir des informations récentes.

Nous examinons ici les options suivantes:

- La ***navigation privée*** permet de surfer sur Internet sans que le navigateur collecte l'historique. Cette fonction est utile si vous craignez que quelqu'un vous surveille et ait accès à l'historique de votre navigateur. Cependant, la navigation privée **n'empêchera pas quelqu'un de savoir ce que vous faites en ligne** s'il regarde physiquement par-dessus votre épaule ou s'il surveille votre appareil avec un stalkerware.

- ***«Interdire le suivi»*** est un paramètre qui permet de refuser le suivi par des tiers, comme les annonceurs, sur un site web que vous visitez. Cette fonction ne concerne que le suivi à des fins de publicité comportementale; elle n'empêche pas le site web que vous visitez de recueillir des informations sur vous.

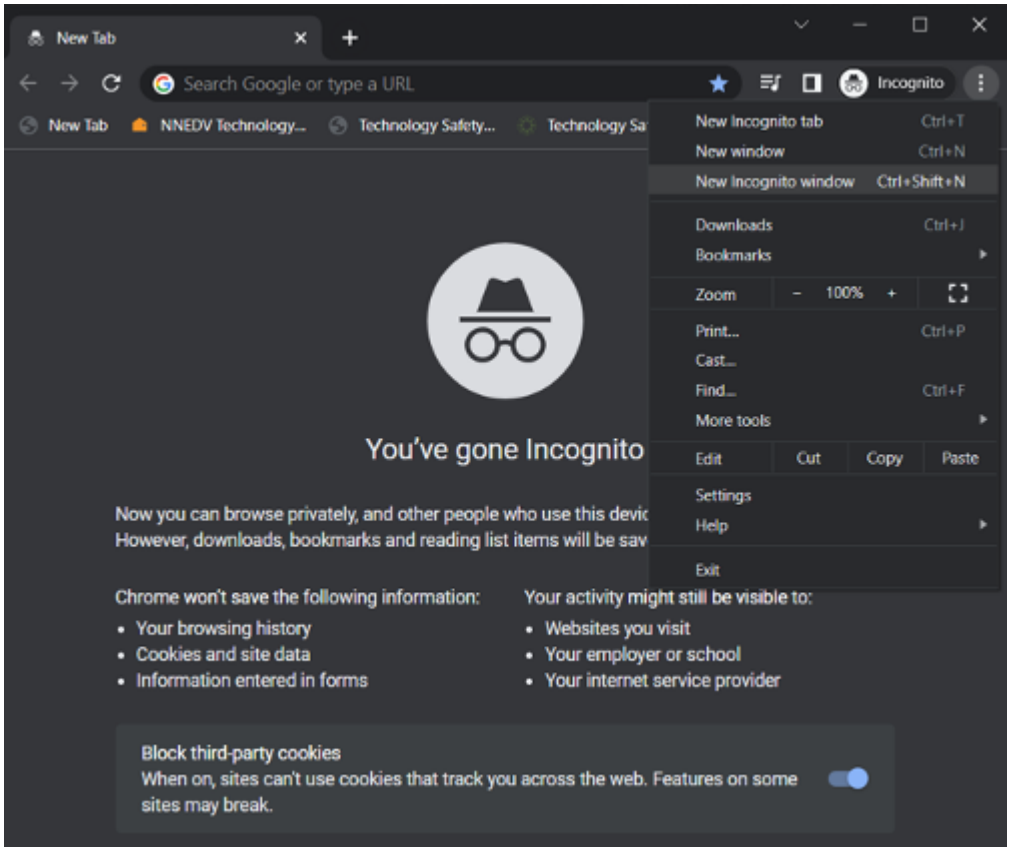
Tous les navigateurs examinés ici permettent de supprimer l'historique de navigation. N'oubliez pas que si quelqu'un surveille votre ordinateur, la suppression de l'historique de votre navigateur peut sembler suspecte.

Toutefois, la suppression périodique de votre historique de navigation peut renforcer la confidentialité.

Google Chrome

Navigation privée: Mode Incognito

1. Dans une nouvelle fenêtre, cliquez sur l'icône du menu ⋮ de Chrome.
2. Choisissez **Nouvelle fenêtre Incognito.**
3. Une nouvelle fenêtre s'ouvrira avec un message expliquant le mode incognito. Vous resterez en mode incognito jusqu'à ce que vous fermiez cette fenêtre du navigateur.



Interdire le suivi:

1. Sur votre ordinateur, ouvrez Chrome.
2. En haut à droite, cliquez sur Plus de ⋮ › **Paramètres**
3. Cliquez sur **Confidentialité et sécurité** › **Cookies et autres données du site**.
4. Activez ou désactivez l'**envoi d'une requête «Interdire le suivi» avec votre trafic de navigation**.

Historique:

1. Sur votre ordinateur, ouvrez Chrome.
2. En haut à droite, cliquez sur Plus ⋮ › **d'historique**.
3. À gauche, cliquez sur **Effacer les données de navigation**.
4. Dans le menu déroulant, sélectionnez la période que vous souhaitez supprimer.
5. Cochez les cases correspondant aux informations que vous souhaitez que Chrome supprime, notamment l'**historique de navigation**.
6. Cliquez sur **Effacer les données**.

Options de confidentialité supplémentaires:

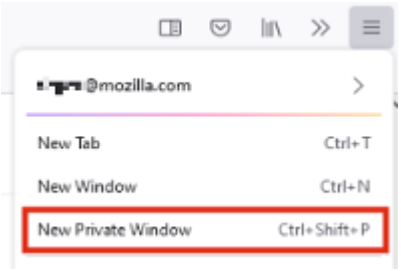
1. Sur votre ordinateur, ouvrez Chrome.
2. En haut à droite, cliquez sur Plus de ⋮ › **Paramètres**.
3. Cliquez sur **Confidentialité et sécurité**.
4. Choisissez les paramètres à désactiver.
   a. Pour contrôler la façon dont Chrome gère le contenu et les autorisations d'un site, cliquez sur **Paramètres du site**.
   b. Pour supprimer les informations de votre activité de navigation, comme l'historique, les cookies ou les mots de passe enregistrés, cliquez sur **Effacer les données de navigation**.
   c. Pour contrôler la façon dont Chrome gère les cookies et le suivi, cliquez sur **Cookies et autres données du site**.
   d. Pour gérer la navigation sécurisée et la protection, cliquez sur **Sécurité**.

Google propose également une vérification de la confidentialité qui vous permet de vérifier les paramètres de confidentialité des produits Google que vous utilisez, tels que YouTube. Visitez https://myaccount.google.com/privacycheckup/ pour plus d'informations.

Mozilla Firefox

Navigation privée

1. Cliquez sur le bouton de menu ☰ et cliquez ensuite sur **Nouvelle fenêtre privée**



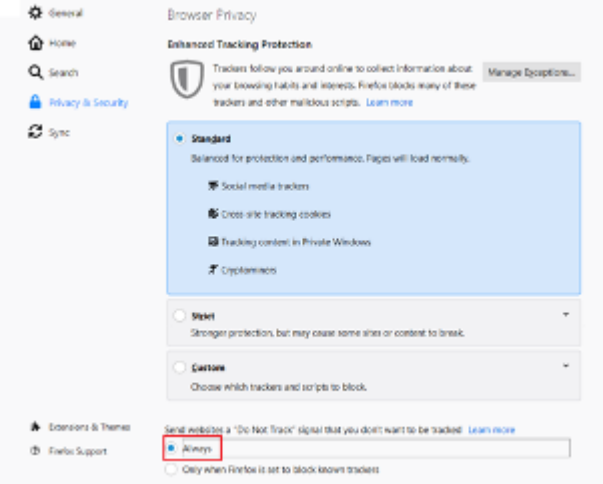
2. Une nouvelle fenêtre apparaitra, expliquant l'option de navigation privée de Firefox. Vous resterez dans ce mode jusqu'à ce que vous fermiez la fenêtre du navigateur.

Il existe également une option permettant de toujours naviguer en privé. Voir ici pour plus d'informations.

Ne pas me pister:

La fonction **«**Ne pas me pister» est désactivée par défaut, sauf dans les Fenêtres privées où elle est activée en permanence. Pour toujours utiliser la fonction «Ne pas me pister»:

1. Cliquez sur le bouton menu ☰ et sélectionnez **Paramètres**.
2. Sélectionnez l'onglet **Confidentialité et sécurité**
   a. Vous accédez ainsi à la Protection renforcée contre le pistage dans les paramètres de confidentialité de votre navigateur.



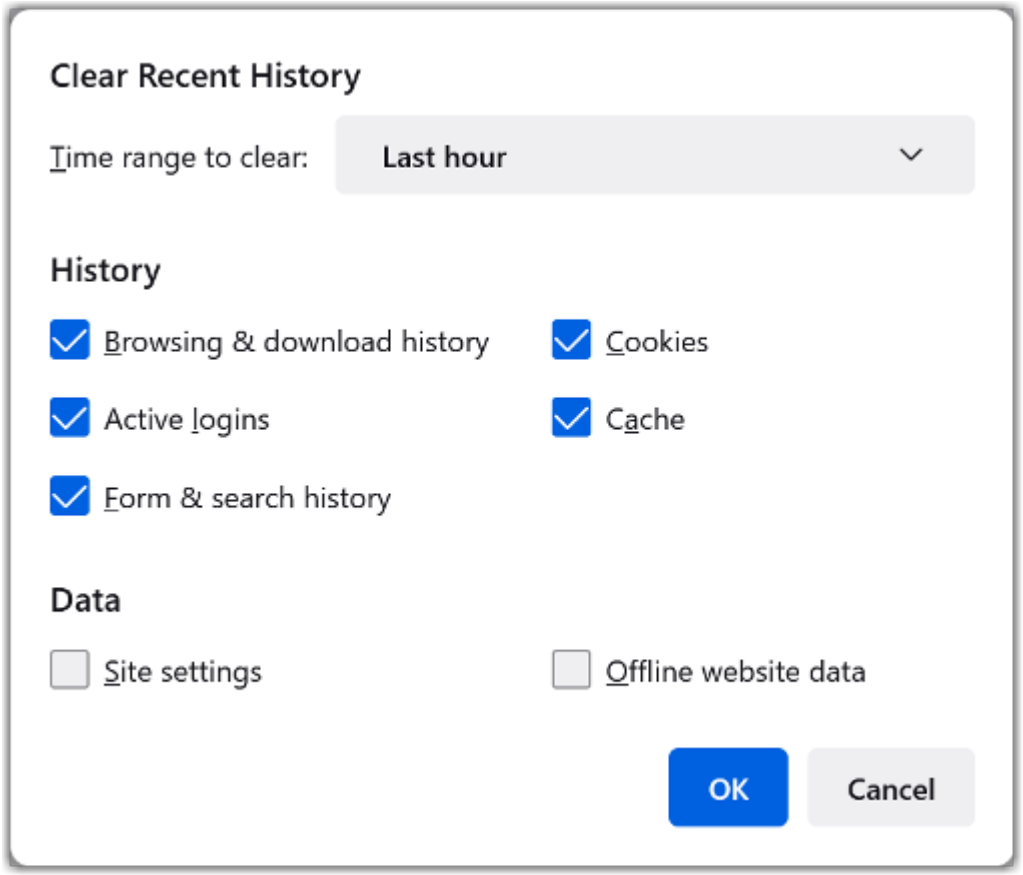
3. Sous **Envoyer aux sites Web un signal «Ne pas me pister» indiquant que vous ne voulez pas être suivie**, choisissez **Toujours**.
4. Fermez la page **À propos de: préférences**. Toutes les modifications que vous avez apportées seront automatiquement enregistrées.

Pour en savoir plus sur la manière dont Firefox vous protège des traqueurs dans Fenêtres privées, voir SmartBlock pour une protection renforcée contre le pistage.

History:

1. Cliquez sur le bouton menu ☰ pour ouvrir le panneau de menu.
2. Cliquez sur **Historique** et sélectionnez **Effacer l'historique récent**.
3. Sélectionnez une période à effacer dans l'historique:
   a. Cliquez sur le menu déroulant à côté de **Intervalle à effacer** pour choisir la partie de votre historique que Firefox effacera (la dernière heure, les deux dernières heures, les quatre dernières heures, la journée en cours ou

tout le contenu).



b. Cochez les cases pour sélectionner les informations que vous souhaitez effacer de votre historique. Vos choix sont décrits dans Quels éléments sont inclus dans mon historique?

4. Cliquez sur le bouton **OK**. La fenêtre se ferme et les éléments que vous avez sélectionnés sont effacés de votre historique.

Safari

Navigation privée

Navigation privée spontanée

1. Dans l'appli Safari sur votre Mac, choisissez **Fichier > Nouvelle fenêtre privée**, ou passez à une fenêtre privée déjà ouverte.
   a. Une fenêtre privée a une couleur sombre Champ de recherche intelligente avec du texte blanc.

2. Naviguez comme vous le feriez normalement.

Lorsque vous utilisez une fenêtre privée:

- La navigation entamée dans un onglet est isolée de celle entamée dans un autre onglet, de sorte que les sites web que vous visitez ne peuvent pas enregistrer un suivi de votre navigation.
- Les pages Web que vous visitez et vos informations en saisie automatique ne sont pas enregistrées.

- Les pages que vous avez ouvertes ne demeureront pas dans l'appli iCloud, elles n'apparaitront donc pas lorsque vous afficherez tous les onglets précédemment ouverts sur d'autres appareils.
- Vos recherches récentes ne figureront pas dans la liste des résultats lorsque vous utilisez un moteur de recherche.
- Les éléments que vous téléchargez ne sont pas inclus dans la liste des téléchargements. (Les éléments restent sur votre ordinateur)
- Si vous utilisez un téléphone de transfert, les fenêtres privées ne sont pas reliées à votre iPhone, iPad, iPod touch ou autres ordinateurs Mac.
- Les modifications apportées à vos cookies et données du site web ne sont pas sauvegardées.

Les sites web ne peuvent pas modifier les informations stockées sur votre appareil. Les services normalement disponibles sur ces sites peuvent donc fonctionner différemment jusqu'à ce que vous utilisiez une fenêtre non privée.

Note: Aucun des éléments ci-dessus ne s'applique aux fenêtres Safari non privées que vous pouvez avoir ouvertes.

Toujours naviguer en privé

1. Dans l'appli Safari sur votre Mac, choisissez **Safari > Préférences**, puis cliquez sur **Général**.
2. Cliquez sur le menu contextuel **Safari s'ouvre avec**, puis choisissez **Nouvelle fenêtre privée**.
3. Si vous ne voyez pas cette option, choisissez **le menu Apple** > **Préférences système**, cliquez sur **Général** et vérifiez que l'option **Fermer les fenêtres en quittant une appli** est sélectionnée.

Ne pas me pister:

1. Dans l'appli Safari sur votre Mac, choisissez **Safari > Préférences**, puis cliquez sur **Intimité**.
2. Sélectionnez **Empêcher le suivi intersite**.

À moins que vous ne visitiez et n'interagissiez avec le site web du fournisseur de contenu tiers, leurs cookies et données du site web sont supprimés.

Les sites de médias sociaux offrent souvent des boutons Partager, J'aime ou Commenter sur d'autres sites web. Ces boutons peuvent être utilisés pour suivre votre navigation sur Internet, même si vous ne les utilisez pas. Safari bloque ce suivi. Si vous voulez quand même utiliser les boutons, on vous demandera la permission d'autoriser le site à voir vos activités sur les autres sites.

Historique:

1. Dans Safari sur votre Mac, choisissez **Historique > Effacer l'historique**, puis cliquez sur le menu contextuel.
2. Choisissez jusqu'à quand vous souhaitez effacer votre historique de navigation.

Confidentialité supplémentaire:

Consultez les préférences de confidentialité d'Apple ici.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource Internet Browsing Tips.

Conseils de sécurité et de confidentialité en ligne

Vous avez peut-être déjà entendu la phrase: rien de ce qui se passe en ligne n'est vraiment privé ou anonyme. Même si cela est vrai à bien des égards, il existe également de bons moyens de protéger sa vie privée et de se sentir plus en sécurité sur le Web. Cette fiche-conseils s'adresse à toutes les personnes qui cherchent des moyens de rester connectées, tout en se sentant en sécurité et en préservant la confidentialité de leurs informations.

Ouverture de comptes

- Créez des adresses courriel et des noms d'utilisateur qui ne contiennent pas d'informations permettant de vous identifier, comme votre nom complet ou votre date ou année de naissance.
- Utilisez des noms d'utilisateur et des photos de profil différents pour chaque site, et ayez plusieurs comptes courriel pour différents usages, comme le travail, l'école et les groupes sociaux. Vous pouvez également envisager d'utiliser une image plutôt qu'une photo de vous pour votre profil.
- Réfléchissez avant de partager des informations personnelles au-delà de ce qui est requis pour créer un compte ou un profil. Parfois, les sites n'indiquent pas de manière évidente que les informations demandées sont facultatives, alors faites attention aux petits caractères!
- Cliquez sur «non» lorsque des sites ou des applis vous proposent de consulter votre liste de contacts pour vous aider à vous connecter avec les personnes qui ont déjà un profil sur le site.
- Vous pouvez refuser que votre profil puisse être consulté sur le site lui-même et qu'il apparaisse dans les résultats de recherche généraux comme Google.

Mots de passe

- Les meilleurs mots de passe comportent au moins 12 à 15 caractères et contiennent des lettres, des chiffres et des symboles.
- Créez un nouveau mot de passe pour les comptes qui contiennent des informations sensibles ou identifiantes.
- Déconnectez-vous lorsque vous avez terminé et refusez que l'appareil, le navigateur, le site ou l'appli se souviennent de votre mot de passe.
- En savoir plus sur la sécurité des mots de passe.

Paramètres et politiques de confidentialité

- Lisez les guides de paramètres de confidentialité que proposent désormais de nombreux sites de médias sociaux et faites des ajustements en fonction de vos besoins. Voici des liens vers les guides de confidentialité de quelques-uns des principaux sites:
  - Sécurité@Facebook
  - Conseils de sécurité sur WhatsApp
  - Centre de sécurité Instagram
  - Sécurité et confidentialité sur Twitter: Un guide pour les survivantes de harcèlement et d'abus
  - Centre de sécurité Google
  - Centre de sécurité TikTok
  - Comment rester en sécurité sur Snapchat
- Lisez les politiques de confidentialité des applis et des sites pour savoir qui a accès à vos informations et comment elles peuvent être obtenues. De nombreux sites et applis partagent des informations s'ils reçoivent une assignation à comparaître ou une ordonnance du tribunal, un élément à prendre en considération pour les femmes qui ont ou peuvent avoir des interactions de nature juridique avec la personne qui les a violentées ou harcelées.
- Plus d'informations sur les considérations relatives à la protection de la vie privée lors de la publication de contenu en ligne.
- Les médias sociaux sont par nature conviviaux. Certaines informations sont toujours publiques, tandis que d'autres peuvent être restreintes (aux proches par exemple) ou demeurer privées. Vérifiez régulièrement qui figure dans vos listes d'amis ou de followers, et sachez que vos publications peuvent être vues au-delà de votre réseau.

Médias sociaux

Proches et famille

- Discutez avec vos proches et votre famille de ce qu'ils peuvent ou non publier en ligne à votre sujet.
- N'oubliez pas que vos employeurs, groupes religieux, équipes sportives, groupes bénévoles peuvent partager vos informations personnelles en ligne. Si vous avez des inquiétudes quant au type d'informations personnelles que ces groupes partagent en ligne, vous pouvez les contacter pour leur demander de retirer vos informations.

Naviguer en toute sécurité sur le Web

- Utilisez un antivirus, tenez-le à jour et analysez régulièrement vos appareils.
- Supprimez périodiquement l'historique, les cookies, les fichiers Internet temporaires, les formulaires et les mots de passe enregistrés dans votre navigateur Web.
- Pour des Conseils de confidentialité pour les navigateurs Internet.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource *Online Privacy and Safety Tips*.

10 étapes faciles pour maximiser la confidentialité dans l'utilisation des technologies

Le monde d'aujourd'hui fonctionne avec une abondance de technologies, nous permettant de partager presque tout ce que l'on fait. La famille, les proches, les collègues de travail et les anciens camarades de classe s'y retrouvent et se connectent plus facilement que jamais. Notre vie en ligne est devenue tout aussi importante que notre vie hors ligne. Mais ce que vous partagez ne reste pas toujours dans vos cercles malgré votre intention de limiter l'accès à vos informations.

Alors, que pouvez-vous faire? Voici quelques moyens rapides d'utiliser la technologie de manière plus sécuritaire. Ces mesures faciles peuvent faire une grande différence dans la protection de votre vie privée, en dépit de leur simplicité.

1. Se déconnecter des applis et des comptes

Déconnectez-vous de vos comptes et applis lorsque vous ne les utilisez pas. Décochez la fonction «Rester connecté» et n'autorisez pas le navigateur à se souvenir de votre mot de passe pour vous connecter automatiquement. Si vous restez connectée, l'on pourra toujours accéder physiquement à votre ordinateur, votre tablette ou votre téléphone et publier des messages à partir de vos comptes et ces publications sembleront provenir de vous. La déconnexion de vos comptes est encore plus importante si vous utilisez un appareil qui ne vous appartient pas.

2. Employez des mots de passe forts

Utilisez des mots de passe pour empêcher les étrangers, les partenaires, les parents et les enfants d'accéder à vos comptes. N'utilisez pas le même mot de passe pour plusieurs comptes, un mot de passe que votre entourage peut facilement deviner, ou un mot de passe simple (un seul mot) facile à craquer. Créez un système de mots de passe uniques que vous êtes seule à connaître. En savoir plus sur la sécurité des mots de passe.

3. Réglages de confidentialité

Vérifiez les paramètres de confidentialité de tous vos comptes, en particulier vos médias sociaux. La plupart des sites permettent de limiter ce que les autres voient, qu'il s'agisse de mises à jour de statut ou d'informations sur votre profil. N'oubliez pas que les réseaux sociaux comme TikTok, Snapchat, Facebook ou Twitter ne sont pas les seuls à disposer de paramètres de confidentialité. La plupart des comptes, tels qu'Amazon et Google, vous permettent de limiter le nombre de personnes qui peuvent voir vos informations.

4. Réduire le partage de la localisation

Les appareils mobiles sont dotés d'une fonction de localisation GPS. Vous pouvez donc partager votre position sans même vous en rendre compte. Vous pouvez contrôler les applis qui ont accès à votre localisation avec les paramètres de votre téléphone. La plupart des téléphones disposent de différents réglages de confidentialité de localisation. Certains

réseaux sociaux disposent de paramètres de confidentialité pouvant protéger votre localisation directement sur leur site.

5. Ne pas inclure les coordonnées des lieux dans vos photos

Saviez-vous que lorsque vous prenez une photo sur votre téléphone, vous pouvez également partager votre position par inadvertance? Cela signifie que le *selfie* que vous venez de mettre en ligne pourrait contenir vos coordonnées (via le GPS). Vous pouvez y remédier avec les paramètres de confidentialité de votre appli caméra. N'oubliez pas que, même si vous avez désactivé l'option de localisation de l'appli de l'appareil photo, l'appli de partage de photos que vous utilisez peut révéler votre position – désactivez donc également l'option de localisation de cette appli.

6. Réfléchissez avant de connecter différents comptes de médias sociaux

Vous pouvez connecter votre Instagram à votre Facebook ou votre compte Pinterest à d'autres réseaux sociaux. Il peut être plus facile de les mettre à jour en un seul clic, mais cela signifie que beaucoup plus de personnes auront accès à une multitude d'informations vous concernant. Cela complique également le contrôle de votre vie privée. Réfléchissez donc bien aux divers comptes de médias sociaux que vous connectez ensemble.

7. Usez de prudence lorsque vous utilisez des réseaux sans fil gratuits

L'Internet gratuit c'est fantastique, mais vous payez le prix en vous exposant aux risques. L'utilisation de réseaux sans fil ouverts de votre café local ou de votre centre communautaire peut permettre à des pirates d'accéder à vos informations privées. Si vous avez l'intention de consulter des comptes bancaires, d'effectuer des achats pour lesquels vous devez inclure vos informations de carte de crédit, ou toute autre activité privée, attendez d'accéder à un réseau sécurisé. Et si votre réseau sans fil personnel n'est pas doté d'un mot de passe, créez-en un.

8. Utilisez HTTPS partout

Tous les sites web ne sont pas créés égaux. Certains sont plus susceptibles de transmettre des virus. Cependant, certains sites disposent d'une version sécurisée – vous pouvez le savoir en regardant le lien dans la barre d'adresse URL. S'il commence par HTTPS, il s'agit d'une page sécurisée. Si elle commence par HTTP, il s'agit d'une page normale.

Un moyen simple de vous assurer que vous utilisez la page sécurisée chaque fois que vous le pouvez consiste à télécharger le module complémentaire HTTPS-everywhere du navigateur. Chaque fois que vous accédez à un site, il tentera d'ouvrir la version sécurisée (HTTPS) plutôt que le site normal. Si le site n'a pas de page sécurisée, la page normale sera ouverte par défaut.

9. Utilisez la fonction «Incognito» ou «Navigation privée»

Vous pouvez choisir de naviguer sur Internet de manière confidentielle dans Google Chrome, Mozilla Firefox, Microsoft Edge et Safari. La navigation en mode privé signifie que personne ne peut ouvrir votre navigateur web après que vous l'ayez utilisé et parcourir l'historique pour voir les sites visités. La navigation en mode privé est plus sécuritaire si vous

utilisez l'ordinateur ou la tablette d'un·e ami·e ou si vous êtes sur un ordinateur public. Sachez que vous devez fermer le navigateur pour effacer votre historique. Si vous le laissez ouvert, la personne suivante sera en mesure de consulter votre historique de navigation.

10. Utilisez plusieurs adresses courriel

Les adresses courriel sont gratuites, alors vous pouvez en avoir autant que vous voulez! Une adresse courriel avec un mot de passe très fort est préférable pour vos opérations bancaires et vos achats. Une autre adresse courriel peut servir pour les pourriels et les comptes que vous devez créer pour utiliser un service web particulier.

Vous pouvez même envisager d'utiliser plusieurs adresses courriel pour vos comptes de médias sociaux. Il est plus sécuritaire d'utiliser des adresses courriel différentes pour des comptes différents, car si quelqu'un devine l'un de vos mots de passe, il n'a accès qu'à un seul compte. Vous pouvez même aller plus loin et télécharger un service qui «masque» l'adresse d'un compte afin que votre principale adresse courriel ne soit jamais utilisée.

Faites confiance à votre instinct

Si vous vivez une situation de violence ou si vous êtes récemment séparée, il n'est peut-être pas très prudent de mettre à jour vos mots de passe ou de prendre des mesures supplémentaires pour protéger votre vie privée. Vous connaissez votre situation mieux que quiconque. Faites confiance à votre instinct. Si cela risque d'aggraver la violence, attendez pour appliquer des mesures et demandez de l'aide et des idées de planification de sécurité à un service spécialisé en matière de violence conjugale et familiale ou d'agressions sexuelles. Vous pouvez en trouver un près de chez vous sur www.hebergementfemmes.ca.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource *10 Easy Steps to Maximize Online Privacy*.

Être avisée sur le Web

Les informations sur notre vie, y compris nos informations personnelles, se retrouvent de plus en plus souvent sur le Web. Nous sommes nombreuses à nous inquiéter de la sécurité et de la confidentialité de ce niveau de partage. Par conséquent, les femmes subissant la violence conjugale, la violence à caractère sexuel et le harcèlement sont confrontées à des risques et à des préoccupations encore plus complexes en matière de sécurité.

Comment mes informations se retrouvent-elles sur le Web?

Pour comprendre comment vos informations sont collectées, partagées et archivées, vous devez d'abord comprendre comment elles sont publiées sur Internet. Les informations peuvent s'y retrouver de deux façons: soit vous les publiez,

soit quelqu'un d'autre les publie.

Informations que vous publiez

Voici quelques exemples d'informations personnelles que vous pourriez partager en ligne:

- Publier des mises à jour sur les réseaux sociaux
- Partager votre position en vous inscrivant par le biais d'applis sociales avec localisation telles que Snap Map
- Laisser des commentaires sur des blogs ou écrire des critiques sur des sites d'achat
- Créer des listes de souhaits ou aimer certains contenus sur des sites comme Amazon, Etsy ou Pinterest
- Partager des photos ou des vidéos en ligne
- Interagir avec d'autres par le biais de mondes virtuels ou de jeux en ligne
- Partager par inadvertance des informations personnelles, comme des données de localisation lors du téléchargement de photos

Même si les informations que vous publiez ne semblent pas vous identifier, elles peuvent révéler beaucoup de choses sur vous. Publier une photo de la mascotte de votre école locale ou de votre restaurant préféré peut indiquer votre position par inadvertance. Si la localisation est activée sur l'appli de votre appareil photo, le téléchargement des photos prises avec cet appareil peut indiquer exactement où la photo a été prise.

Assurez-vous de savoir qui peut voir vos informations lorsque vous vous inscrivez à un site web ou créez un nouveau profil. Selon le site, ces informations peuvent être accessibles. En général, les paramètres par défaut permettent à toute personne qui visite ce site (membres de la famille, employeurs potentiels et harceleurs) de voir vos informations personnelles. N'oubliez pas que, même si vous êtes autorisée à «verrouiller» votre compte par le biais des paramètres de confidentialité, certaines informations relatives au compte ou au profil peuvent demeurer publiques (par exemple, votre nom d'utilisateur).

Conseils de sécurité

- Si vous vous inscrivez sur des sites où vous créez un compte et un profil, vérifiez si vous pouvez modifier vos paramètres de confidentialité pour minimiser le contenu auquel les autres auront accès. Ces sites sont destinés à attirer le plus grand nombre de personnes possible et, par défaut, vos informations peuvent être accessibles à tous.
-
- Découvrez ce que l'entreprise fait des informations que vous partagez avec elle en lisant sa politique de confidentialité. La plupart des entreprises partageront vos informations avec des partenaires commerciaux ou les vendront à des annonceurs et des entreprises de marketing. Vos informations personnelles sont précieuses pour de nombreuses raisons, notamment pour créer des publicités ciblées. Cela pourrait poser un risque pour la sécurité si les informations privées et confidentielles d'une femme, comme son lieu de résidence, sont obtenues par la mauvaise personne.

Informations que les autres publient à votre sujet

N'importe qui peut publier des informations sur vous, y compris vos proches, votre famille (notamment vos enfants et vos partenaires et ex-partenaires), vos employeurs, les groupes religieux et communautaires, l'école, le gouvernement, les courtiers en informations, etc. Il peut également s'agir d'informations provenant de différentes sources:

- Dossiers de justice
- Répertoires du personnel des employeurs
- Répertoires web
- Bulletins d'information pour groupe religieux, travail ou école
- Sites de réseaux sociaux

Vos informations peuvent aussi être publiées sur Internet par des voies moins évidentes. Elles peuvent notamment être vendues à des annonceurs et des spécialistes en marketing. Les courtiers en information compilent des données provenant d'organismes publics, d'annuaires téléphoniques, de sondages auprès des consommateurs, de cartes de garantie, de commerçants (magasins locaux et chaînes de magasins), de concours, de médias sociaux, de sites web, etc. Vos informations sont regroupées puis vendues à des tierces parties qui souhaitent obtenir des informations sur vous, comme les médias, services de police, employeurs, propriétaires, banques, sociétés de cartes de crédit, fabricants d'automobiles, ainsi que le gouvernement fédéral et les détectives privés.

Conseils de sécurité

- Demandez aux organisations dont vous faites partie si elles ont tendance à partager sur les médias sociaux ou sur l'Internet et quelles informations personnelles pourraient être incluses. Si vous êtes préoccupée par votre sécurité et votre confidentialité, demandez-leur de ne rien publier qui vous concerne.
- Soyez consciente que les écoles ou les employeurs peuvent publier des choses sur vous et vos enfants.
- Demandez à vos proches et aux membres de votre famille de ne pas vous mentionner, vous taguer ou publier des photos ou des vidéos de vous en ligne.

Comment savoir ce qui se trouve sur le Web?

- **Utilisez un moteur de recherche comme Google ou Bing pour faire une recherche sur vous-même**. Les moteurs de recherche comme Google font un index du web et créent des catalogues de cartes virtuelles qui réfèrent à du contenu. Les moteurs de recherche existent depuis que le web a été développé et ils deviennent plus rapides et plus intelligents chaque jour. La plupart des moteurs de recherche «archivent» ou «mettent en cache» les sites web périodiquement, en sauvegardant des copies de chaque page afin que le contenu puisse toujours être consulté même si le site est hors ligne, a été modifié ou est indisponible pour tout autre motif. Cela signifie que toute information publiée sur le Web peut être consultée indéfiniment (ou aussi longtemps qu'Internet existe). Même si un site web est modifié pour supprimer des informations inexactes ou dangereuses, l'ancien contenu peut toujours être indexé par un moteur de recherche.

- **Parcourez les annuaires en ligne pour vous informer**. Les annuaires téléphoniques en ligne comme canada411.ca comprennent des fonctions de recherche inversée qui permettent de rechercher un numéro de téléphone pour trouver le nom associé à ce numéro, l'adresse et une carte détaillant les lieux. Même si votre numéro de téléphone n'est pas inscrit sur la liste de votre compagnie de téléphone, il est possible de trouver votre adresse et votre numéro de téléphone grâce à des renseignements obtenus auprès de sociétés de marketing et d'autres bases de données.

- **Parcourez les sites Web où vous pensez que vos informations peuvent être présentes**. Visitez les sites Web des groupes et des lieux auxquels vous êtes liée: travail, groupe religieux, équipes sportives, groupes communautaires et bénévoles, etc.

Puis-je retirer des informations inexactes, fausses ou désagréables d'Internet?

Les moteurs de recherche comme Google et Yahoo ne sont généralement pas responsables de la diffusion de vos informations personnelles sur Internet. Par une simple recherche, ils trouvent tous les sites qui peuvent répertorier vos informations. Pour supprimer complètement vos informations, vous devez vous rendre sur chaque site et demander qu'elles soient supprimées.

Selon l'exactitude et la sensibilité de l'information, il peut être préférable de ne pas y toucher. De nombreuses survivantes de violence préfèrent laisser des informations inexactes en ligne pour masquer les informations exactes que l'on peut y trouver. Si les informations publiées sont abusives ou potentiellement dangereuses, vous pouvez contacter le site et lui demander de les supprimer. La plupart des réseaux sociaux disposent d'options qui vous permettent de signaler les contenus abusifs. Les sites web supprimeront le contenu en fonction de leurs conditions d'utilisation et des directives communautaires.

Certains sites peuvent vous demander des informations supplémentaires pour prouver que vous êtes bien la personne sur laquelle portent les informations. Partagez seulement ce que vous êtes à l'aise de partager. Par exemple, si vous demandez à un site de supprimer votre numéro de téléphone, mais que vous devez fournir votre adresse physique, votre numéro de permis de conduire ou une photo pour procéder à la suppression, cela peut ne pas vous convenir.

Gardez également à l'esprit que le fait de supprimer ce qu'un auteur de violence a publié peut l'alerter de votre démarche, et que certains peuvent réagir par une escalade du harcèlement et de la violence. Pensez aux éventuelles représailles lorsque vous planifiez votre sécurité. Si les informations publiées à votre sujet sur le web sont extrêmement dangereuses, inexactes ou autrement préjudiciables, adressez-vous à une intervenante en matière de violence conjugale ou sexuelle (vous pouvez en trouver une près de chez vous sur www.hebergementfemmes.ca) pour obtenir de l'aide, et contactez un·e avocat·e pour connaître vos options juridiques.

Comment puis-je stopper la publication d'informations à mon sujet?

Le meilleur moyen d'empêcher la mise en ligne de nouvelles informations est d'aller à la source. Bien que cela soit plus facile à dire qu'à faire, voici quelques conseils pour vous aider à éviter ce partage:

- Lorsqu'une caissière vous demande votre numéro de téléphone ou votre code postal, vous n'êtes pas obligée de le lui donner. Dans les situations où vous devez fournir un numéro de téléphone, envisagez de donner votre numéro au travail plutôt que votre numéro personnel. Vous pouvez également utiliser un numéro virtuel sans aucun lien avec vos informations personnelles comme Google Voice.
- Si vous vous inscrivez à un programme de rabais d'épicerie ou de pharmacie, remplissez un minimum d'informations. Certains magasins ont une «carte de magasin» que vous pouvez demander à utiliser.
- Utilisez un pseudonyme lorsque vous écrivez des lettres à un éditeur ou que vous publiez en ligne.
- Faites des dons anonymes.
- Dans la mesure du possible, évitez de payer avec des cartes de débit ou de crédit.
- Si vous êtes membre d'organisations qui ont un site web, demandez à ce que votre nom ne figure pas dans les publications et à ce que vous ne soyez pas «taguée» dans les photos.

- Lorsque vous cherchez un emploi, ne publiez pas votre CV sur les sites liés à l'emploi. Recherchez plutôt les emplois disponibles sur le web et envoyez directement votre CV aux employeurs qui vous intéressent.
- Demandez à vos proches de ne pas vous inclure dans leurs blogs, de ne rien publier vous concernant sur les réseaux sociaux et de ne pas publier de photos ou de vidéos où vous pouvez être identifiée.
- Vérifiez tous vos paramètres de sécurité et de confidentialité sur les sites que vous utilisez, tant sur votre ordinateur que sur votre téléphone, pour vous assurer que vous ne partagez pas d'informations sensibles.

En plus d'empêcher la publication d'informations, vous pouvez surveiller ce qui est mis en ligne. Créez une alerte Google qui vous enverra un courriel chaque fois que votre nom est publié. Lorsque vous vous inscrivez à des alertes, communiquez le moins d'informations personnelles possible.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource *Being Web Wise*.

Considérations sur la confidentialité lors de la publication de contenu en ligne

Le Web regorge d'occasions de partager des informations sur nous-mêmes, qu'il s'agisse d'un article de blog, de la mise à jour de nos médias sociaux ou de la publication d'une vidéo sur YouTube. Si nous publions ces informations pour partager notre vie avec nos proches et notre famille, elles peuvent également être consultées par des millions d'autres personnes.

Si certaines personnes sont à l'aise avec le fait que leurs publications puissent être largement consultées, pour d'autres, ce n'est pas le cas. Voici quelques questions à se poser avant de publier du contenu en ligne.

Qui verra ces informations?

Parfois, nous ne réalisons pas à quel point nos informations sont partagées, surtout lorsque nous pensons publier de simples mises à jour sur nous-mêmes, surtout pour nos proches. Avec Internet et les moteurs de recherche, tel que Google Search, tout ce qui est en ligne est indexé et peut être consulté. Même les sites dont vous pensez que seuls les membres ou les followers peuvent voir le contenu peuvent s'avérer publics.

Réfléchissez bien à ce que vous partagez en ligne, et demandez-vous si vous êtes à l'aise avec le fait que ce contenu soit accessible à un public plus large. Certains réseaux sociaux disposent de paramètres de confidentialité qui vous permettent de choisir ou de bloquer les personnes qui peuvent voir le contenu que vous partagez.

Que partagez-vous?

Le type d'informations que vous partagez peut révéler beaucoup ou très peu sur vous. Parfois, nous partageons des informations personnelles sans même nous en rendre compte. Des points de repère sur une photo, ou même un blog

sur l'excellent restaurant où vous avez dîné la veille, peuvent indiquer où vous vous trouvez. Prenez votre décision en considérant le fait que ces informations seront vues par d'autres personnes.

Usez de prudence lorsque vous partagez des informations sur vos proches et votre famille, car vous pourriez commettre des indiscrétions par inadvertance. Si vous partagez des informations sur vos proches, avez-vous leur permission?

Quelle est la politique de confidentialité du site?

Savez-vous ce que font les propriétaires du site des informations que vous leur donnez? Même si les informations que vous partagez ne sont pas publiées, elles peuvent être partagées avec des annonceurs ou des tiers. De nombreux sites ont des politiques de confidentialité qui précisent ce qu'ils font des informations que vous leur communiquez.

Les informations que vous partagez sont-elles illégales ou contraires aux politiques de contenu du site?

De nombreux sites n'autorisent pas de contenu violent ou discriminatoire et, si vous en publiez, ils peuvent le supprimer ou fermer votre compte. Si vous partagez des informations sur d'autres personnes, veillez à ne pas partager de matériel protégé par des droits d'auteur, de fausses informations ou du contenu néfaste, car cela pourrait vous exposer à des poursuites civiles ou pénales.

Quel contrôle exercez-vous sur les informations que vous partagez?

Certaines personnes pensent que leurs publications leur appartiennent et qu'elles peuvent les contrôler. Mais vous n'avez pas vraiment de contrôle une fois le contenu publié. D'autres peuvent le partager, en parler, et même le modifier. Si vous l'avez initialement publié sur votre site personnel, votre blog ou votre page de médias sociaux, vous pouvez retirer la publication originale. Toutefois, il vous sera difficile de la faire retirer sur un autre site, ou si quelqu'un a publié une capture d'écran de votre contenu.

Que puis-je faire pour me protéger?

- Faites attention à ce que vous partagez en ligne.
- Faites attention à ce que vous publiez sur autrui.
- Lorsque vous créez des comptes en ligne, lisez attentivement les directives. C'est souvent à ce moment-là que vous pouvez refuser que le site collecte et partage vos informations.
- Naviguez sur le web en toute sécurité en installant un antivirus et un antispyware sur votre ordinateur.
- Pour en savoir plus, consultez nos conseils de sécurité et de confidentialité en ligne.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource *Considerations for Posting Online Content*.

Conseils pour l'utilisation des sites de partage et d'hébergement de vidéos

Le nombre de personnes qui regardent des vidéos sur YouTube, TikTok, Facebook et autres plateformes n'a jamais été aussi élevé. Si ces plateformes peuvent ouvrir des portes vers de nouvelles informations et ressources, les survivantes de violence doivent être conscientes des risques liés à la diffusion de vidéos dans ces espaces.

Voici quelques éléments à prendre en compte lorsque vous visionnez ou partagez des vidéos.

1. Supprimer l'historique de navigation

Les navigateurs web des ordinateurs et des appareils mobiles enregistrent souvent des informations sur les sites que vous avez visités et les vidéos que vous avez regardées. Si vous pensez que vos appareils sont surveillés, envisagez de supprimer votre historique de navigation, car il peut révéler les sites visités et le contenu visionné. Supprimez périodiquement l'historique, les cookies, les fichiers temporaires, les formulaires enregistrés et les mots de passe de votre navigateur si vous pouvez le faire en toute sécurité.

2. Utilisez la navigation privée, en toute sécurité

Si vous souhaitez que l'on ne sache pas quelles vidéos vous avez regardées, vous pouvez utiliser les fonctions incognito/privé. Une fois fermées, les fenêtres privées empêchent l'enregistrement de l'historique et des cookies. Cela signifie également que tous les comptes auxquels vous êtes connectée dans la fenêtre normale du navigateur n'apparaitront pas dans la fenêtre privée.

Les options de navigation privée peuvent limiter les données suivies et stockées. Sachez que les sites que vous visitez peuvent demeurer visibles si vous ne fermez pas la fenêtre une fois la visite terminée. Consultez nos conseils sur la confidentialité de la navigation sur Internet pour en savoir plus. Consultez nos conseils de sécurité et de confidentialité en ligne pour plus d'informations.

Vous pouvez également utiliser des navigateurs et des moteurs de recherche conçus dans le respect de la confidentialité. Parmi les navigateurs qui ne suivent pas vos activités et empêchent les tiers de le faire, citons Firefox, Epic, Tor et Brave. Les moteurs de recherche respectueux de la vie privée comprennent Startpage, DuckDuck et Swisscows. Vous devrez peut-être installer un de ces navigateurs sur votre appareil.

3. Se déconnecter des comptes

Certaines plateformes de diffusion vidéo (par exemple YouTube) vous offrent la possibilité de créer un compte. Ces sites stockent souvent des données sur les vidéos que vous avez consultées et sur vos recherches à partir du moment où vous créez un compte. Cet historique sert entre autres à vous faire des suggestions sur mesure. Si vous souhaitez conserver ces informations privées, ou qu'une autre personne utilisant votre compte ne reçoive pas vos suggestions, ce qui révèlerait vos habitudes, visionnez les vidéos sans vous connecter à votre compte. De même, ces comptes (YouTube, TikTok, etc.) peuvent être liés à d'autres comptes sur votre téléphone, comme votre compte Google ou iTunes. Ces comptes peuvent partager ou sauvegarder des informations sensibles provenant des plateformes vidéo.

4. Attention aux commentaires

Souvent, les services de partage de vidéos tels que TikTok, YouTube ou Vimeo permettent de publier des commentaires sous les vidéos. Si vous publiez un commentaire, les spectateurs peuvent voir ou accéder à votre identifiant et à votre profil. Si cela vous préoccupe, choisissez avec prudence les vidéos que vous commentez. Si les commentaires sont souvent source d'inspiration, ils servent parfois à troller, attaquer et harceler. Soyez prudente lorsque vous publiez des commentaires et renseignez-vous sur les politiques et les mécanismes de signalement du site.

5. Envisagez d'utiliser un appareil plus sécuritaire

Si vous pensez que l'on surveille votre ordinateur ou tout appareil mobile, essayez d'utiliser un autre appareil auquel l'auteur de violence n'a pas pu accéder physiquement ou à distance dans le passé et auquel il n'a pas accès (comme un ordinateur à la bibliothèque ou le téléphone d'un·e ami·e). Idéalement, cela permet de visionner une vidéo sans être surveillée par l'auteur.

6. Vérifiez les paramètres de confidentialité et de compte

Chaque plateforme dispose de paramètres de compte et de confidentialité qui offrent la possibilité de verrouiller les comptes du public, de limiter les types de vidéos diffusées et de renforcer la sécurité du mot de passe ou du compte. Certaines plateformes offrent de nombreuses options pour sécuriser et garantir l'engagement des paramètres de confidentialité, tandis que d'autres offrent des possibilités plus limitées. Vérifiez vos paramètres de confidentialité sous les informations de votre compte pour déterminer ceux qui vous conviennent le mieux. Lorsque vous utilisez YouTube, Vimeo ou tout autre site de partage de vidéos, assurez-vous que vos paramètres reflètent le niveau de sécurité désiré, et revenez-y fréquemment. Si vous ne savez pas comment les trouver, utilisez un moteur de recherche pour modifier les paramètres de compte, de confidentialité ou de sécurité sur la plateforme de votre choix.

7. Faites confiance à votre instinct.

Les auteurs de violence sont souvent très déterminés à maintenir leur contrôle sur les femmes et la technologie est l'un des nombreux outils qu'ils utilisent pour y parvenir. Si quelqu'un semble en savoir trop sur vous, il se peut que des informations aient été obtenues par le biais de diverses sources, comme la surveillance de vos appareils, l'accès à vos comptes en ligne, la géolocalisation, ou en récoltant des renseignements vous concernant sur Internet.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource *Tips for Using Video Sharing and Hosting Sites*.

Conseils pour un courriel sécurisé

Une adresse courriel est plus qu'un autre moyen de vous joindre. De nos jours, une adresse courriel est essentielle pour la plupart de vos transactions, qu'il s'agisse d'activer un appareil mobile, de faire des achats ou de créer un compte en ligne. Votre courriel peut contenir des communications sensibles et il est souvent relié à des comptes importants, comme votre banque. Il est primordial que votre courriel soit sécurisé – que vous seule y avez accès.

Cette fiche-conseils offre des suggestions sur la manière de rendre votre courriel aussi sécuritaire que possible.

Quel fournisseur choisir?

Si vous craignez que quelqu'un ne pirate votre courriel (messages interceptés/trafiqués), un service crypté de bout en bout peut offrir la solution que vous cherchez. Par exemple, ProtonMail est entièrement chiffré et vous pouvez le régler de manière à ce que le courriel ne soit plus disponible après un certain temps. Parmi les autres services gratuits de courriel crypté figurent Tutanota et Mailfence.

Mais n'oubliez pas que l'utilisation de ces services peut être légèrement plus compliquée qu'un courriel traditionnel. Par exemple, pour certains courriels sécurisés, la personne à qui vous envoyez le message doit utiliser le même service de messagerie que vous, ou un lien peut être nécessaire pour lire le courriel. N'oubliez pas qu'un service crypté n'empêchera pas que votre courriel soit intercepté si quelqu'un connait votre adresse et votre mot de passe ou si votre appareil est surveillé.

Il est possible de sécuriser son compte avec de grandes entreprises comme Gmail ou Yahoo. En somme, la sécurité de votre courriel comprend le mot de passe, la sécurité de l'appareil utilisé et de bonnes habitudes en matière de sécurité et de confidentialité.

Configuration d'une adresse courriel

La confidentialité et la sécurité commencent dès la création du compte.

Utilisation d'informations non identifiantes

Les survivantes de violence et de harcèlement peuvent ne pas souhaiter qu'une adresse courriel les identifie facilement. Lorsque vous configurez une adresse, vous ne devez pas utiliser d'informations pouvant vous identifier (comme votre nom). Vous pouvez utiliser n'importe quoi pour votre adresse, par exemple: *brightredstar3@gmail.com*.

Lorsque vous créez un courriel, le fournisseur de services vous demandera des informations comme votre nom et votre date de naissance. Vous pouvez utiliser un pseudonyme et une fausse date de naissance. Mais n'oubliez pas que ce pseudonyme et cette date de naissance seront votre moyen de vérifier votre compte, assurez-vous d'y avoir accès. Certains services de messagerie vous demandent également votre genre, votre numéro d'appareil mobile et une adresse courriel secondaire. D'autres vous permettent de contourner ces questions sans rien vous demander; cela peut varier en fonction du service de messagerie. Par exemple, Gmail exige un nom, un identifiant, un mot de passe, une date de naissance et un genre. Cependant, vous n'êtes pas obligée de fournir votre numéro de téléphone et une adresse courriel. Yahoo Mail exige un nom, un courriel, une date de naissance et un numéro d'appareil mobile, tandis que le genre est facultatif. Outlook ne requiert que votre nom, une adresse courriel et un mot de passe.

Assurez-vous d'être seule à connaitre votre mot de passe

Pour la plupart des gens, la sécurité d'un compte courriel se résume à la question de savoir si quelqu'un d'autre connait l'adresse et le mot de passe. N'utilisez pas un mot de passe pouvant être facilement deviné ou qui sert pour plusieurs comptes. Créez un mot de passe dont vous pouvez vous souvenir sans avoir à l'écrire. Il s'agit soit d'une longue phrase, soit d'un mot contenant des lettres, des chiffres et des caractères.

Utilisez la vérification en deux étapes

Si vous disposez d'une deuxième adresse courriel ou d'un numéro de téléphone sécurisé (c'est-à-dire que personne d'autre n'y a accès), vous pouvez configurer la vérification en deux étapes. Si quelqu'un essaie de se connecter à ce compte à partir d'un autre appareil ou d'un autre lieu, le service de messagerie enverra un code au deuxième courriel ou au numéro de téléphone. Le code, ainsi que le mot de passe, permettront de se connecter au compte. Si vous (ou la personne qui tente de se connecter à votre compte) n'avez pas accès à cette adresse courriel ou à ce numéro de téléphone secondaires pour obtenir le code, il est impossible de se connecter au compte.

Un deuxième courriel ou numéro de téléphone auquel personne d'autre n'a accès sont essentiels pour que cette méthode soit efficace. Si quelqu'un d'autre y a accès, il lui sera possible de se connecter à votre compte avec la vérification en deux étapes et d'être avertie lorsque vous essayez de vous connecter à partir d'un nouveau lieu ou d'un nouvel appareil. Selon votre situation, vous ne souhaiterez peut-être pas activer la vérification en deux étapes avant d'avoir obtenu l'adresse courriel et le numéro de téléphone secondaires.

Si vous ne fournissez pas d'adresse courriel ou de numéro de téléphone secondaires, le service de messagerie peut vous demander périodiquement d'en fournir un lorsque vous vous connectez à votre compte. Dans la plupart des cas, vous pouvez ignorer ces demandes et cliquer sur Continuer ou OK sans fournir les informations demandées. L'utilisation d'une adresse courriel et d'un numéro de téléphone secondaires peut être une mesure de sécurité très utile, mais elle doit vous convenir. Si vous n'avez pas d'adresse courriel ou de numéro de téléphone secondaires, ou s'ils ont été compromis, cette méthode ne rendra pas votre compte plus sécuritaire.

Assurez-vous que votre courriel et votre téléphone secondaires sont sécurisés avant de les utiliser.

Passez les notifications de sécurité en revue

Certains services de messagerie vous informeront de tout événement lié à la sécurité de votre compte, comme le changement de votre mot de passe, la connexion à partir d'un nouvel endroit ou d'un autre appareil, ou la modification de tout autre paramètre de sécurité.

Les notifications de sécurité peuvent être envoyées à votre adresse secondaire. Comme dans le cas de la vérification en deux étapes, si quelqu'un d'autre a accès à cette adresse secondaire, il sera informé de toute modification de sécurité apportée à votre compte. Vous pouvez choisir de limiter les notifications que vous recevez ou changer l'adresse courriel secondaire pour une adresse plus sécuritaire. (Vous pouvez généralement trouver les notifications de sécurité sous l'onglet Paramètres de sécurité de votre compte de messagerie)

Adoptez de bonnes habitudes

En plus de disposer d'un mot de passe fort et d'activer les fonctions de sécurité (par exemple, la vérification en deux étapes) fournies par le service de messagerie, il est important d'adopter des habitudes sécuritaires afin de s'assurer que personne d'autre ne peut se connecter à votre compte ou lire vos courriels.

Utilisez des appareils sécurisés.

Essayez de ne pas vous connecter à votre compte sur des appareils (par exemple, appareil mobile, tablette, ordinateur) auxquels l'auteur de violence a accès ou qu'il surveille. Selon la façon dont l'appareil est surveillé, l'auteur peut être en mesure de voir une adresse courriel ou un mot de passe.

Toujours se déconnecter

Chaque fois que vous vous connectez à votre compte courriel, sur votre propre appareil ou sur celui de quelqu'un d'autre, n'oubliez pas de vous déconnecter. Ne vous contentez pas de fermer le navigateur web ou l'appli ou d'éteindre l'appareil, car cela ne vous déconnectera pas. Sans déconnexion en bonne et due forme, toute personne qui utilise l'appareil après vous pourra consulter votre courriel. Même sur vos propres appareils, la déconnexion est utile au cas où quelqu'un s'empare de votre téléphone ou de votre ordinateur ou en cas de perte.

Si vous consultez vos courriels sur votre appareil mobile par une appli ou sur votre ordinateur par un logiciel, il peut être difficile de vous déconnecter. Dans ce cas, vous avez quelques options. La mise en place d'un code ou d'un mot de passe sur l'appareil permet de restreindre l'accès. Dans certains cas, vous pouvez même supprimer le compte courriel de votre appli ou logiciel de messagerie. Certaines personnes le font lorsqu'elles voyagent ou lorsqu'elles craignent qu'une personne mal intentionnée puisse avoir accès à leur appareil. Vous pouvez toujours consulter vos courriels via un navigateur web ou configurer l'appli ou le logiciel de messagerie pour accéder à votre compte après vous être assurée que votre téléphone ou votre ordinateur est sécurisé.

Ne laissez pas votre navigateur ou votre appareil mobile se souvenir de votre courriel ou de vos mots de passe

Certains services de messagerie (Gmail, en particulier) proposent une option qui permet au navigateur Web de se souvenir de votre compte, sauf si vous lui demandez de ne pas le faire. La prochaine fois que vous (ou n'importe qui d'autre) ouvrez la page de connexion, votre adresse courriel est répertoriée et il suffit de saisir le mot de passe. Ne permettez pas au navigateur Web de se souvenir de votre compte courriel, en particulier sur les appareils qui ne vous

appartiennent pas. Cette demande d'autorisation se présente souvent sous la forme «Faites-vous confiance à ce navigateur?» Choisissez «non».

Certains navigateurs et appareils mobiles vous demanderont si vous souhaitez qu'ils stockent vos mots de passe ou se souviennent de vous. Dans ce cas, ils se souviendront à la fois de votre courriel et de votre mot de passe. Si vous craignez qu'une autre personne ait accès à vos appareils, refusez que vos mots de passe soient enregistrés. Cela peut être pratique pour certains comptes moins sensibles, comme votre connexion Netflix, mais votre compte courriel doit être le plus sécurisé possible.

- **Ne cliquez sur aucun lien provenant de personnes inconnues ou suspectes**

Pour renforcer la sécurité, ne cliquez pas sur des liens provenant de personnes inconnues ou suspectes et ne fournissez pas d'informations personnelles par courriel ou par un lien électronique.

- **N'envoyez pas d'informations personnelles par courriel**

Si quelqu'un (même s'il s'agit de votre banque ou de votre société de services publics) vous demande des informations personnelles (mots de passe, informations sur votre carte de crédit, informations bancaires, etc.) par courriel, ne fournissez pas ces informations. Trouvez plutôt le numéro de téléphone de l'entreprise et donnez-leur ces informations par téléphone.

Soyez prudente lorsque vous donnez votre adresse courriel

Les gens ont besoin de votre adresse courriel pour vous contacter. Toutefois, vous n'avez peut-être pas envie de donner votre adresse chaque fois qu'on vous la demande, notamment dans les magasins ou lors de la création de comptes sans importance. Vous trouverez ci-dessous quelques moyens d'éviter de donner votre adresse principale.

- Vous pouvez créer une adresse électronique pour les pourriels ou pour les cas où vous devez fournir une adresse, mais ne souhaitez pas vraiment recevoir de messages. Ce compte est spécifiquement destiné aux pourriels et ne doit pas recevoir des informations importantes, telles que vos relevés bancaires, ou être connecté à des comptes importants, tels que votre service de téléphonie mobile.

- Certains services de messagerie vous permettent de créer des comptes temporaires. Ces adresses éphémères durent de 10 minutes à 24 heures. Les courriels sont envoyés sur le site du service de messagerie où vous pouvez les consulter. Cette fonction est utile lorsque vous devez fournir une adresse pour «confirmer» une inscription, mais que vous ne souhaitez pas fournir votre courriel principal. N'oubliez pas que certains services de messagerie temporaire ne respectent pas la confidentialité. Toute personne connaissant la fausse adresse peut voir tous les messages envoyés à cette adresse (exemples de services de messagerie temporaire publics: Mailinator ou Maildrop). Parmi les autres services de courriel temporaire, citons Guerrilla Mail ou 10-Minute Mail.

- Abine Blur offre une solution à plus long terme pour protéger votre adresse courriel. Abine Blur est une extension de navigateur web pour ordinateur et appareil mobile qui agit comme un service de redirection. Il «brouille» vos informations afin que les destinataires obtiennent une adresse courriel anonyme. Abine Blur redirige toute réponse à votre principale adresse courriel. De votre côté, vous envoyez des courriels dans les deux sens comme d'habitude, mais les destinataires n'obtiennent qu'une adresse anonyme.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource *Tips for a Secure Email Account*.

Mots de passe: Des moyens simples pour renforcer votre sécurité

La violence conjugale peut rendre la sécurité des mots de passe plus compliquée

Un partenaire ou ex-partenaire violent en sait souvent beaucoup sur vous, ce qui peut mettre en danger vos informations personnelles stockées dans des comptes et des appareils. L'auteur peut vous contraindre à partager vos mots de passe ou peut même être en mesure de les deviner.

Il est important de créer un plan de sécurité avant de changer vos mots de passe si l'auteur est susceptible de devenir plus violent s'il ne peut pas accéder à vos informations. Vous pouvez contacter votre organisation locale antiviolence pour élaborer un plan de sécurité.

Qu'est-ce qui rend un mot de passe moins sécuritaire?

La connaissance intime que l'auteur a de vous signifie que les mots de passe courants ne sont PAS sécuritaires pour une personne subissant la violence. Il ne faut pas:

- Utiliser des mots de passe comme ABC123 ou password
- Utiliser votre nom, celui de vos enfants ou d'un animal de compagnie, ou encore une date d'anniversaire
- Utiliser le même mot de passe pour tous les comptes
- Répondre à des questions de sauvegarde par des réponses que l'auteur peut connaitre ou deviner (par exemple, le nom de jeune fille de votre mère ou votre couleur préférée).

Les bonnes habitudes en matière de mot de passe

Utilisez des mots de passe différents pour des comptes différents

Ainsi, si quelqu'un découvre l'un de vos mots de passe, il n'aura pas accès à tous vos comptes.

Évitez d'utiliser des porte-clés

Résistez à l'utilisation de porte-clés via votre navigateur (par exemple Safari ou Google Chrome) pour stocker vos mots de passe. Il s'agit de petits messages que vous pouvez voir en haut de votre navigateur et qui vous demandent si vous souhaitez que le navigateur enregistre votre mot de passe. Pensez à utiliser un gestionnaire de mots de passe (voir ci-dessous).

Soyez stratégique avec vos questions et réponses secrètes

Ces questions secrètes ne le sont pas vraiment. Quelqu'un qui vous connait (ou qui sait comment chercher sur Google) peut deviner où vous avez étudié au secondaire ou votre couleur préférée. Aucune règle ne vous oblige à être honnête lorsque vous répondez à ces questions secrètes. Inventez une réponse dont vous vous souviendrez, mais que personne d'autre ne pourra deviner, ou utilisez l'option permettant de créer votre propre question secrète si disponible.

Empêchez quelqu'un de craquer votre mot de passe en le testant

Il n'y a pas que les personnes qui vous connaissent qui peuvent deviner votre mot de passe. Les programmes informatiques peuvent facilement et rapidement craquer les mots de passe. Les mots qui sortent d'un dictionnaire sont plus faciles à décoder pour ces programmes. Créez un mélange de mots et de symboles ou de phrases, et allongez-le pour qu'il soit plus difficile à déchiffrer.

Vous pouvez:

- Vérifier si votre adresse courriel a fait l'objet d'une violation à l'adresse suivante: Have i been pwned?
- Tester votre mot de passe sur le site How secure is my password? pour voir à quel point il serait facile pour un logiciel de piratage de le deviner. Vous serez surprise de ce que vous allez apprendre! Par exemple, un programme ne prendrait que 5 secondes pour craquer «blahblah», mais «blahblahblahblah» prendrait 35 MILLIERS d'années! (N'allez pas utiliser celui-là – trouvez-en un par vous-même!)

Enfin, assurez-vous que toutes les adresses courriel et tous les numéros de téléphone de récupération sont à jour et vous appartiennent avant d'activer la vérification en deux étapes ou l'authentification multifactorielle comme mesure de sécurité supplémentaire.

Privilégiez la simplicité

Si vous rendez votre mot de passe trop complexe ou difficile, vous allez peut-être l'oublier et verrouiller votre compte. Votre mot de passe doit être un mélange de lettres, de mots et de chiffres que vous pouvez facilement mémoriser. Si

vous devez prendre un mot de passe en note, faites attention à l'endroit où vous le conservez.

Par exemple, le coller sous votre clavier ou sur votre écran n'est pas du tout sécuritaire. Vous ne voulez pas non plus le conserver dans un endroit où quelqu'un pourrait facilement le trouver. Vous pouvez aussi noter un indice pour vous en souvenir au lieu de noter le mot de passe lui-même.

Gardez les comptes séparés

Parfois, des comptes avec Facebook ou Google vous offrent la possibilité de vous connecter à d'autres services instantanément. Cela peut être pratique, mais si quelqu'un obtient le mot de passe de votre Facebook, par exemple, cela lui donne accès à de nombreux autres comptes.

Ne partagez jamais vos mots de passe.

Avant de partager un mot de passe, choisissez une personne en qui vous avez confiance, maintenant et à l'avenir. La plupart de nos comptes contiennent une quantité importante d'informations personnelles, et vous ne souhaitez peut-être pas les partager avec d'autres.

Changez souvent vos mots de passe

Si vous pensez que quelqu'un connait vos mots de passe, les changer l'empêchera d'accéder à vos comptes. Il est également bon de prendre l'habitude de changer ses mots de passe de temps en temps.

Décochez la fonction «Se souvenir de moi» ou «Rester connecté»

Si ces fonctionnalités facilitent grandement l'accès, elles permettent également d'accéder facilement à vos comptes. Veillez tout particulièrement à décocher ces fonctionnalités si vous vous connectez à un compte sur l'appareil d'une autre personne ou sur un ordinateur public.

N'oubliez jamais de vous déconnecter

Votre compte peut rester ouvert pendant des jours si vous ne vous déconnectez pas, permettant ainsi à d'autres d'y accéder. Certains comptes, comme Facebook et Gmail, vous permettent de voir les autres endroits où vous vous êtes connectée et de désactiver ces connexions.

Supprimer le compte ou l'appli

Si vous utilisez une appli sur un appareil intelligent qui ne vous permet pas de vous déconnecter, vous pouvez envisager de supprimer l'appli ou le compte. Il s'agit d'une étape supplémentaire, mais vous pouvez évaluer la sensibilité des informations contenues dans ce compte et le risque que quelqu'un d'autre y accède.

Suggestions pour rendre les mots de passe plus faciles à retenir

Les personnes exposées à la violence ont souvent bien d'autres choses en tête que de se souvenir d'un grand nombre de mots de passe. Cela peut être notamment lié à des choses comme un traumatisme, un manque de sommeil, le stress ou la dépression. Ce n'est pas votre faute si vous oubliez des mots de passe. Essayez ces suggestions pour rendre les mots de passe plus faciles à retenir:

Choisissez quatre choses

Créez un mot de passe avec quatre choses différentes qui ne sont pas liées. Essayez de les classer par ordre alphabétique pour vous aider à vous souvenir de leur ordre (par exemple, Noix de cocoEléphantMicroscopeNetball).

Écrivez une phrase

Écrivez une phrase avec des fautes d'orthographe ou utilisez une autre langue que le français pour certains des mots (par exemple, MifavouriteactorisNicoleKiiidman).

Envisagez d'utiliser un gestionnaire de mots de passe ou un coffre-fort

Ces outils peuvent non seulement stocker vos mots de passe dans un espace sécurisé, mais aussi générer des mots de passe forts et uniques afin que vous n'ayez pas à consacrer d'énergie à le faire vous-même. Nous vous recommandons de faire des recherches sur des sites techniques réputés pour choisir un gestionnaire de mots de passe qui vous convient. Beaucoup proposent des abonnements gratuits de base. Il suffit d'un mot de passe solide pour «verrouiller» le coffre-fort et tous les autres mots de passe qu'il contient.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource *Tips for a Secure Email Account*.

Utilisation abusive et distribution non consensuelle d'images intimes

Qu'est-ce que la distribution non consensuelle d'images?

Au Canada, la distribution non consensuelle d'images est le partage d'une image intime, sans consentement, alors que l'image est censée rester privée. Une image intime montre une personne nue, exposant ses seins, ses organes génitaux ou sa région anale, ou engagée dans une activité sexuelle. Il peut s'agir de tout enregistrement visuel, y compris une photographie ou un enregistrement vidéo.

Dans le contexte de la violence conjugale, les auteurs de violence partagent souvent ou menacent de partager des photos ou des vidéos intimes pour manipuler les femmes, les punir ou les contrôler. Nombre de ces vidéos ou photos sont publiées et partagées en ligne sur des sites de médias sociaux populaires, de pornographie ou de «pornographie de vengeance».

Lorsque publiées en ligne, certaines images intimes contiennent des informations permettant d'identifier la personne, telles que son nom, son adresse, son numéro de téléphone et son lieu de travail ou d'études, ce qui peut exacerber le risque de violence, de traque et de harcèlement par d'autres personnes. Des femmes ont déclaré avoir été contactées par des inconnus leur demandant des faveurs sexuelles obscènes ou d'autres photos après la publication de leurs photos, vidéos ou informations personnelles.

Les auteurs peuvent également envoyer, ou menacer d'envoyer des images directement aux proches, à la famille et à d'autres membres de la communauté qui connaissent la survivante, par courriel ou par SMS.

Un auteur peut entrer en possession de photos ou de vidéos intimes de différentes manières.

- Il a pris la photo ou la vidéo à l'origine
- La photo ou la vidéo lui a été envoyée par la personne qui l'a captée (*selfie*)
- Il a volé l'image (en accédant à votre téléphone, ordinateur ou compte infonuagique)
- Il a photoshopé une image pour qu'elle ressemble à la personne.

Impact sur les femmes

Les effets de cette violence peuvent être dévastateurs et avoir un impact sur tous les aspects de la vie et de l'avenir d'une femme. Nombre d'entre elles sont revictimisées à l'école, sur leur lieu de travail ou dans leur communauté, et certaines ont tenté de se suicider ou sont passées à l'acte. Malheureusement, les victimes sont très souvent blâmées, les gens suggérant que ces images n'auraient pas dû être partagées en premier lieu. Même lorsque les images ont été obtenues sans consentement ni permission (par exemple, en enregistrant secrètement quelqu'un ou en filmant une agression sexuelle), c'est souvent la femme qui est remise en question. L'accent ne devrait jamais être sur ce qu'elle a fait, mais plutôt sur la distribution par l'auteur d'images intimes sans consentement.

Terminologie

La distribution non consensuelle d'images est souvent appelée «pornographie de vengeance» ou «cyberharcèlement». Parmi les autres termes utilisés, citons la sexploitation ou la sextorsion (chantage et menaces de révéler des images explicites), et l'e-vengeance, qui fait référence à la diffusion électronique.

Le terme actuellement préféré est «distribution non consensuelle d'images». Cette terminologie ne met pas l'accent sur ce qu'a fait la femme (ce qui peut constituer un blâme de la victime) ou sur les motivations de la personne qui a partagé l'image (qui n'est souvent pas la vengeance), mais se concentre plutôt sur l'absence de consentement.

En outre, il n'est pas nécessaire que les images montrent de la nudité ou des organes génitaux (critère souvent utilisé pour déterminer si une image est considérée comme pornographique) ou soient de nature sexuelle. Le terme «image intime» englobe également les photos ou vidéos qui peuvent être relativement intimes, en fonction du contexte culturel ou social, sans avoir à montrer de nudité ou de sexe (par exemple, le partage de la photo d'une femme sans son hijab pour lui causer honte et embarras ou pour l'extorquer).

Que peuvent faire les femmes?

Documenter votre expérience

Pour beaucoup de femmes, le premier réflexe est de faire retirer immédiatement les images du Web. Demandez-vous toutefois si vous voulez d'abord documenter ou capturer des preuves afin d'avoir une trace de ce qui a été publié et par qui. Ces informations seront importantes si vous optez pour le signalement, que ce soit à la police, à un·e avocat·e ou à d'autres services.

Voici quelques conseils pour documenter les preuves:

- Saisissez l'URL de l'image
- Si l'URL ne semble pas indiquer le site de publication, notez cette information
- S'il est possible de voir qui a publié l'image, faites une capture d'écran où le nom et toute autre information de profil de l'auteur sont visibles
- Tâchez d'y inclure la date et l'heure de publication de l'image si possible et notez toujours la date de collecte des preuves
- Collectez également toute autre trace de harcèlement, comme des courriels ou des SMS
- Si l'auteur de violence a commenté ou fait allusion à l'image intime, notez-le dans votre journal de documentation.

Signalement au site Web

De nombreux sites de médias sociaux disposent d'un processus permettant de supprimer les images intimes non consensuelles. Ces entreprises ont des politiques qui interdisent les images intimes non consensuelles sur leurs sites et, une fois signalées, elles sont supprimées. C'est pourquoi il importe de capturer d'abord les preuves avant de les signaler, car une fois supprimées, vous en perdrez toute trace.

Certains sites ne disposent pas d'un processus de signalement pour retirer les images intimes non consensuelles. Si c'est le cas, lisez leurs directives communautaires ou relatives au contenu pour voir s'ils suppriment certains contenus. Certains sites ont des directives relatives au contenu en matière de harcèlement, de violence, de haine ou de nuisance. Bien qu'ils ne disposent pas d'un processus de notification de retrait, ils peuvent autoriser les demandes de retrait de contenu si vous leur envoyez un courriel ou les contactez. Certains sites suppriment le contenu en cas d'infraction aux droits d'auteur. Cela peut être utile si c'est vous qui avez pris la photo ou la vidéo.

Méfiez-vous des sites qui vous demandent beaucoup d'informations personnelles ou un paiement pour supprimer l'image. Si la plupart s'efforcent de vous aider, certains sites douteux peuvent tenter d'exploiter ce qui vous est arrivé en demandant des informations d'identification personnelle afin de pouvoir les publier à côté de l'image intime, ou vous faire chanter pour obtenir de l'argent afin de retirer le contenu.

Supprimez votre image des moteurs de recherche

Certaines femmes sont très inquiètes que ces images apparaissent si quelqu'un les recherche. Vous pouvez soumettre une demande à Google ou à Bing et leur demander de faire disparaitre les URL liées à votre image des résultats de recherche. Ainsi, lorsque quelqu'un cherche votre nom, il sera beaucoup plus difficile à trouver.

Si l'image a été partagée sans consentement, voir le Guide de l'initiative pour les droits civils sur Internet pour faire retirer le contenu indésirable.

Signaler la violence

Il est possible de faire un rapport à la police. Selon le Code criminel canadien, la distribution non consensuelle d'images constitue une infraction.

Cherchez le soutien d'un programme antiviolence

Si la violence basée sur la distribution d'images intimes fait partie d'un schéma plus large de violence conjugale ou sexuelle, demandez l'aide d'un programme antiviolence dans votre communauté. Vous pouvez obtenir de l'aide concernant l'utilisation abusive d'images et d'autres formes de violence.

Conseils de sécurité technologique

Voici quelques conseils utiles:

- Si vos photos et vos vidéos sont automatiquement téléchargées sur un service infonuagique, vérifiez que ces comptes sont sécurisés et que personne d'autre que vous ne connait le mot de passe. Il est toujours bon de s'assurer que tous vos comptes sont sécurisés et que vous êtes seule à connaitre les mots de passe.
-
- Vérifiez les paramètres de confidentialité de vos médias sociaux, afin de savoir qui voit ce que vous partagez. Vous pouvez passer en revue vos amis et vos followers, et retirer l'accès à vos informations au besoin.

- Mettez des codes d'accès sur vos appareils, en particulier ceux qui contiennent des photos et des vidéos de vous.

- Envisagez de créer une alerte Google à votre nom afin d'être avertie dès qu'il est publié en ligne. Une personne dont le nom n'est pas très courant aura plus de facilité à utiliser ces alertes. Gardez en tête que vous recevrez une alerte chaque fois que votre image intime sera réaffichée. Certaines femmes trouvent cela utile, tandis que d'autres trouvent le processus particulièrement éprouvant.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource *Image Based Abuse*.

Réinitialisation de votre réseau Wi-Fi

Lorsque vous ne vivez plus avec l'auteur de violence, il est important de prendre des mesures pour vous assurer que votre technologie et vos comptes sont sécurisés afin d'empêcher l'accès à vos informations sensibles. La réinitialisation de votre réseau Wi-Fi fait partie de ces mesures. En effet, n'importe qui sur votre réseau pourrait facilement épier ce que

vous faites, voir vos mots de passe et d'autres informations privées à l'aide de simples outils numériques. Ce document explique comment réinitialiser votre réseau Wi-Fi afin de garantir la sécurité de votre connexion Internet et des appareils qui l'utilisent.

Étape 1: Trouvez votre routeur

La première étape consiste à savoir où se trouve le routeur Wi-Fi dans votre maison. Avec tant d'appareils électroniques branchés, il peut s'avérer difficile de reconnaitre votre routeur. En cas de doute, essayez de débrancher l'appareil. Avez-vous perdu votre accès Internet? Si tel est le cas, c'est le routeur! Rebranchez-le et passez à l'étape suivante.

Étape 2: Trouvez votre manuel

Certaines des étapes suivantes impliquent de consulter le manuel du routeur. Les étapes à suivre peuvent varier selon le modèle. Essayez de trouver le numéro de modèle de votre routeur. Il doit être indiqué quelque part au dos ou sur le côté de l'appareil. Saisissez ensuite la marque (par exemple, Linksys) et le numéro de modèle dans une recherche Google et ajoutez le mot «manuel». Le manuel devrait figurer parmi les premiers résultats Google. Si vous ne trouvez pas la marque du routeur, contactez votre fournisseur Internet (par exemple Rogers, Shaw, Telus, Northwest Tel) pour obtenir cette information. L'on pourra même vous aider à le réinitialiser.

Étape 3: Effacer les paramètres existants

Maintenant que vous avez trouvé votre routeur Wi-Fi et son manuel, il est temps d'effacer tous les paramètres existants, car il n'y a aucun moyen de savoir exactement ce qu'a fait la personne qui a configuré votre routeur à l'origine. Pour ce faire, repérez le bouton de réinitialisation à l'arrière du routeur. Souvent, ces boutons ne sont que de petits trous que vous ne pouvez enfoncer qu'avec un stylo, un trombone déplié ou une boucle d'oreille. Si vous ne le trouvez pas, essayez de rechercher les mots «bouton de réinitialisation» ou «défaut-usine» dans le manuel.

Maintenez le bouton de réinitialisation enfoncé (là encore, vous devrez peut-être utiliser un trombone ou un autre objet semblable pour le pousser). Vous devriez voir tous les voyants du routeur clignoter pour vous indiquer qu'il est sur le point d'être réinitialisé. Maintenez ce bouton enfoncé. Lorsque la réinitialisation est terminée, les voyants cessent de clignoter.

Étape 4: Reconfigurer le routeur

Après la réinitialisation, vous devez maintenant de reconfigurer le routeur avec un nouveau mot de passe.

La première étape consiste à se connecter à l'Internet du routeur. Recherchez la nouvelle connexion dans la liste des connexions Wi-Fi disponibles sur votre ordinateur. Si vous aviez un nom de réseau personnalisé, ce nom aura été effacé. Le nom de votre réseau sera désormais un nom générique, pouvant comprendre la marque de votre routeur. Si vous voyez beaucoup de réseaux dans la liste des réseaux auxquels vous pouvez vous connecter, assurez-vous d'être à proximité du routeur et essayez de vous connecter au Wi-Fi qui a le signal le plus fort. Habituellement, lors de votre première connexion, vous n'avez pas à entrer de mot de passe. Par contre s'il en faut un, recherchez un mot de passe par défaut imprimé sur votre routeur Wi-Fi ou dans le manuel d'instruction. Sur certains routeurs, le nom de réseau et le mot de passe par défaut sont imprimés sur l'appareil.

Étape 5: Accéder aux paramètres de votre routeur

Une fois votre appareil connecté à votre routeur, il est temps d'accéder aux paramètres. Vous pouvez les trouver dans votre navigateur en entrant une adresse destinée spécialement aux paramètres du routeur Wi-Fi. Ouvrez votre navigateur et essayez de saisir chacune de ces adresses jusqu'à ce que vous en trouviez une qui vous permette d'accéder à la page des paramètres de votre routeur:

- 192.168.0.1
- 192.168.1.1
- 10.0.0.1

Si aucune de ces adresses ne vous conduit aux paramètres, cet article peut vous montrer comment trouver l'adresse de votre routeur en fonction du type d'appareil que vous utilisez.

Si l'une de ces adresses vous offre des directives pour télécharger une appli permettant de modifier les paramètres du routeur, suivez ces directives pour télécharger l'appli sur un appareil mobile et y modifier les paramètres du routeur.

Si vous ne parvenez pas à accéder aux paramètres de votre routeur, essayez d'appeler votre fournisseur de services Wi-Fi. Leur équipe d'assistance technique sera probablement en mesure de vous aider.

Étape 6: Connectez-vous aux paramètres du routeur

Une fois que vous êtes sur la page des paramètres, vous devriez voir un écran vous demandant le nom d'utilisateur et le mot de passe de l'administrateur. Il s'agit d'un mot de passe différent de celui que vous avez utilisé précédemment pour vous connecter au Wi-Fi. Chaque fabricant définit un nom d'utilisateur et un mot de passe par défaut. Parfois, ces mots de passe par défaut sont inscrits sur le routeur lui-même ou dans le manuel. Vous pouvez également rechercher le mot de passe par défaut de votre modèle de routeur en visitant cette page web.

Étape 7: Configurer un nouveau mot de passe

Après vous être connectée aux paramètres de votre routeur Wi-Fi, il est temps de définir un nouveau mot de passe réseau. Les paramètres de chaque routeur sont différents. Regardez dans le manuel ou essayez simplement de cliquer sur les différentes sections et cherchez quelque chose comme «Network Name» ou «Network Password». Créez un mot de passe fort et efficace pour votre réseau. Notez votre nouveau mot de passe et conservez-le dans un endroit sécuritaire. Un bon mot de passe est constitué d'au moins douze caractères de lettres et de chiffres aléatoires. Vous n'aurez pas à mémoriser ce mot de passe, il est donc préférable qu'il soit long et compliqué. En effectuant une recherche Google sur le thème «générateur de mot de passe aléatoire», vous trouverez de nombreux outils pour vous aider à créer un nouveau mot de passe.

Vous pouvez aussi modifier le nom du réseau au besoin. À vous de décider si vous voulez utiliser le nom générique du réseau ou non. Si vous le changez, mieux vaut choisir un nom qui ne vous identifie pas, surtout si vous vivez dans une maison, un appartement ou un immeuble avec plusieurs réseaux Wi-Fi à portée.

Une fois que vous aurez changé le mot de passe ou le nom de votre réseau, vous perdrez votre connexion au routeur. Vous devez maintenant consulter les paramètres Wi-Fi de votre appareil et vous reconnecter à votre réseau, en entrant cette fois votre nouveau mot de passe.

Étape 8: Désactiver WPS

Avant de terminer, il y a deux autres paramètres de votre routeur que vous devriez envisager de modifier.

Tout d'abord, retournez à la page des paramètres et voyez si vous pouvez trouver un paramètre appelé WPS. Si vous le trouvez, désactivez cette fonction. Le WPS est une méthode de connexion à votre routeur qui présente une grave faille de sécurité que de nombreux fabricants n'ont pas corrigée. Vous n'aurez jamais besoin d'activer cette fonction, il est donc plus prudent de la désactiver.

Étape 9: Configurer un nom d'utilisateur et un mot de passe différents (facultatif)

Enfin, vous pouvez configurer un nom d'utilisateur et un mot de passe différents pour accéder aux paramètres du routeur Wi-Fi. Ceci est différent du nom et du mot de passe du réseau. Il s'agit du nom d'utilisateur et du mot de passe utilisés pour se connecter à la page des paramètres de votre routeur Wi-Fi. Consultez le manuel ou cliquez sur les différents paramètres jusqu'à ce que vous trouviez un paramètre ressemblant à «admin username» et «admin password». Le nom d'utilisateur n'est pas très important, mais assurez-vous que le mot de passe soit assez fort, aléatoire et différent de celui de votre réseau.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Un grand merci à Steven Jenkins de EmpowerDB pour son expertise sur le contenu de ce document.

Conseils de sécurité pour les ordinateurs

De nos jours, rares sont les foyers qui ne possèdent pas d'ordinateur. Les enfants s'en servent pour faire leurs devoirs et vous l'utilisez régulièrement pour vos courriels ou pour payer des factures. Au bureau, on l'allume chaque matin et on l'éteint chaque soir.

Les ordinateurs sont une technologie vulnérable que les auteurs de violence, connus ou non, peuvent exploiter pour obtenir des informations sur une femme. Si un ordinateur n'est pas aussi familier qu'un téléphone, il contient néanmoins beaucoup d'informations personnelles: courriel, historique de navigation sur le web, formulaires et documents ou informations importantes dignes de sauvegarde.

La seule façon de couper complètement l'accès à votre ordinateur est de le déconnecter du Web ou d'un autre réseau (comme un réseau domestique, non connecté à Internet) et de créer un code d'accès que vous êtes seule à connaitre. Si vous craignez que quelqu'un ne s'introduise dans votre ordinateur et que le déconnecter d'Internet ne pose pas problème, cette solution peut vous convenir. Pour la plupart des gens, cependant, la déconnexion d'Internet peut compliquer la vie de tous les jours. Que vous soyez en train de configurer un nouvel appareil ou de revoir les paramètres, voici quelques conseils de sécurité et de confidentialité.

Prévention et protection

Voici quelques moyens de minimiser les risques.

Employez une protection pare-feu

Sur la plupart des ordinateurs, tablettes et appareils mobiles, des pare-feu sont déjà installés. Les pare-feu surveillent ce qui entre et sort de l'appareil. Lorsqu'ils détectent des données suspectes, ils les empêchent de parvenir à votre ordinateur. Essentiellement, un pare-feu protège votre ordinateur du piratage par le biais de connexions compromises.

Sur la plupart des systèmes d'exploitation Windows, les protections du pare-feu sont activées par défaut. Les pare-feu des systèmes d'exploitation Mac et Linux sont désactivés par défaut et leur activation peut faire une grande différence. Pour savoir si le pare-feu est activé, vérifiez les paramètres dans le Panneau de configuration (pour le système d'exploitation Windows) ou dans Préférences système / Sécurité et confidentialité (pour les Mac).

Exécutez un antivirus générique ou spécialisé dans les logiciels espions

Pour protéger votre appareil contre les virus et les logiciels espions, vous devez installer et exécuter un antivirus. Les antivirus analysent votre ordinateur et les fichiers que vous téléchargez. S'ils détectent des virus, ils en bloquent l'installation. Certains logiciels peuvent mettre le virus en quarantaine pour l'empêcher d'infecter votre ordinateur, tandis que d'autres sont capables de le supprimer.

Les antivirus s'appuient sur les caractéristiques particulières des virus pour les détecter; toutefois, les cybercriminels les modifient constamment pour pouvoir infecter des appareils. Pour cette raison, assurez-vous d'avoir la dernière version de votre antivirus. La plupart des antivirus se mettent à jour automatiquement. Si tel n'est pas le cas, configurez votre antivirus pour qu'il le fasse.

Il existe aussi des antivirus spécialisés dans les logiciels espions (antispyware). Si vous craignez que l'auteur puisse utiliser un logiciel espion, l'exécution d'un antispyware peut être de mise.

Les antivirus et les antispyware n'empêchent pas forcément toute installation de logiciels malveillants. Cependant, ils renforcent la protection de votre ordinateur. Il en existe de nombreux qui sont gratuits pour les particuliers. Consultez les moteurs de recherche sur le «meilleur antivirus ou antispyware gratuit» pour vous assurer que ces programmes répondent à vos besoins spécifiques.

Désactiver l'accès à distance

Si vous craignez que quelqu'un accède à votre ordinateur à distance, avec ou sans votre permission, vous pouvez désactiver l'autorisation d'accès à distance. Vous pourrez toujours la réactiver au besoin.

La manière de désactiver l'accès à distance sur votre ordinateur dépend du système d'exploitation. Sur un ordinateur Windows, vous voulez activer le paramètre: «Ne pas autoriser les connexions à distance à cet ordinateur» (se trouve généralement dans le Panneau de configuration). Si vous avez un Mac, allez dans Préférences Système / Partage, et décochez «Connexion à distance» et «Gestion à distance». Le meilleur moyen de trouver des directives spécifiques à votre ordinateur est de rechercher sur Google «comment désactiver l'accès à distance à [votre système d'exploitation (par exemple, Windows 11)]».

Désactiver le partage de fichiers

Si votre ordinateur est relié à un réseau (même s'il n'est pas connecté à Internet), d'autres appareils reliés au même réseau peuvent accéder aux fichiers de votre ordinateur. Cela peut être problématique si vous êtes connectée à un réseau Wi-Fi public et que vos paramètres sont configurés pour le partage. Si vous n'avez pas besoin que quelqu'un d'autre ait accès à vos fichiers, désactivez le partage de fichiers.

La manière de désactiver le partage de fichiers dépend du système d'exploitation que vous utilisez. Le meilleur moyen est de rechercher sur Google «comment désactiver le partage de fichiers sur [votre système d'exploitation (par exemple Windows 11)]». Pour la plupart des versions de Windows, le paramètre se trouve dans le Panneau de configuration et vous devez sélectionner «désactiver le partage de fichiers et d'imprimantes». Pour un Mac, allez dans Préférences Système / Partage, et décochez «partage de fichiers» et «partage d'imprimante».

Utiliser un compte non-administrateur pour l'usage quotidien

Certains logiciels malveillants et «*hacks*» nécessitent un accès administratif à votre ordinateur. Par conséquent, si vous êtes connectée en tant qu'administrateur et que vous cliquez accidentellement sur un lien contenant un logiciel malveillant, celui-ci sera téléchargé et installé. Toutefois, si vous êtes connectée en tant que non-administrateur et que la configuration n'autorise pas un non-administrateur à installer de logiciels, celui-ci ne s'installera pas, même si vous cliquez accidentellement sur un lien contenant un logiciel malveillant.

Il est donc utile de créer un compte non-administrateur pour votre utilisation quotidienne. Vous pouvez toujours vous connecter sur le compte administrateur lorsque vous devez installer un logiciel ou apporter des modifications à votre ordinateur. Windows et Mac vous permettent tous deux de créer plusieurs utilisateurs.

Pratiques visant à renforcer la sécurité informatique

Outre les paramètres que vous pouvez activer ou désactiver et l'exécution de logiciels pour améliorer la protection, il existe d'autres bonnes pratiques qui peuvent renforcer la sécurité et la confidentialité.

Utiliser un mot de passe sur votre ordinateur

Pour empêcher quiconque d'accéder à votre contenu, commencez par verrouiller votre ordinateur avec un mot de passe. Alors que la plupart des gens craignent le piratage, le moyen le plus simple d'accéder à votre ordinateur est simplement de l'avoir à portée de main, soit à partir de chez vous ou parce qu'on vous l'a dérobé. N'oubliez pas qu'il est plus facile pour un ex-partenaire de deviner votre mot de passe et d'accéder à votre appareil.

Ne cliquez pas sur des liens provenant de personnes inconnues ou suspectes

Une autre bonne pratique consiste à ne pas cliquer sur les liens ou les pièces jointes d'origine suspecte. Ces liens ou pièces jointes peuvent parfois contenir des logiciels malveillants qui s'installent automatiquement, dès que vous cliquez. Si vous devez recevoir des fichiers ou ouvrir des liens d'une personne en qui vous n'avez pas confiance, envisagez de le faire à partir d'un service infonuagique ou trouvez une autre manière de communiquer.

Se déconnecter des comptes et quitter les programmes

Lorsque vous avez fini d'utiliser un compte, un programme ou l'ordinateur lui-même, quittez et déconnectez-vous. Si vous laissez votre ordinateur connecté, il sera plus facile pour quelqu'un d'autre d'accéder à vos comptes. Il est toujours préférable de se déconnecter lorsque vous avez terminé.

Éteindre les points d'accès lorsqu'ils ne sont pas utilisés

Désactivez l'accès Wi-Fi, Bluetooth, Airdrop ou tout autre accès de connectivité que vous n'utilisez pas. Si le point d'accès est éteint, il sera plus difficile pour quelqu'un de se connecter à distance. Vous pouvez toujours l'allumer quand vous voulez vous connecter.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Ce document fait partie du projet Sécurité technologique Canada d'Hébergement femmes Canada. Nous vous encourageons à visiter le site www.securitetech.ca pour trouver des informations et des ressources supplémentaires sur la violence facilitée par la technologie, la planification de la sécurité technologique et la préservation des preuves numériques. Ce document, ou toute partie de celui-ci peut être reproduit ou utilisé à condition de citer la source. Si vous souhaitez adapter le contenu, veuillez contacter Hébergement femmes Canada à l'adresse info@endvaw.ca.

Ce projet est rendu possible grâce au financement du ministère Femmes et Égalité des genres Canada (FEGC).