

GUIDE PRATIQUE POUR SE PROTÉGER À L'ÈRE NUMÉRIQUE



Guide pour comprendre et signaler la violence fondée
sur le genre facilitée par la technologie



Coalition pour
le Leadership des
Femmes de l'Î.-P.-É.



TABLE DES MATIÈRES

Remerciements..... 2

Introduction 3

Violence facilitée par la technologie à l'Île-du-Prince-Édouard et au Canada..... 4

Définitions..... 8

Comment prévenir la VFT et y réagir..... 9

Quel est le rôle des témoins en ligne? 11

Pourquoi est-il important de préserver les preuves de VFT? 14

Le registre de rapports de violence facilitée par la technologie 15

Soutien et ressources supplémentaires 21

Glossaire..... 22

Références 22

REMERCIEMENTS

Reconnaissance territoriale

Nous reconnaissons que la PEI Coalition for Women's leadership est située sur un territoire ancestral et non cédé des Mi'kmaq. Nous respectons tous les Mi'kmaq et autres peuples autochtones vivant sur la terre d'Epekwitk, au sein des Mi'kma'ki. Nous sommes tous visés par les traités.

Contexte

La violence fondée sur le genre facilitée par la technologie, ainsi que l'absence de réglementation efficace régissant les nombreuses plateformes de médias sociaux, constituent des menaces pour la démocratie et le bien-être collectif. Ces enjeux continueront d'avoir un impact direct sur l'accès aux postes de leadership dans le pays. La Coalition espère que le présent *Guide pratique pour se protéger à l'ère numérique* permettra d'informer sur la violence facilitée par la technologie et d'apporter un soutien à celles et ceux qui en sont victimes.

Lors de la création du guide, la Coalition a reçu des conseils inestimables de la part du personnel des organismes sans but lucratif de l'Î.-P.-É. suivants :

Jane Affleck, Native Council of PEI

Sarah Dennis, Information juridique communautaire

Lucky Fusca et Adam MacIntyre, PEI Transgender Network

Khousmita Gopaul, ResourceAbilities

Tout au long du développement du projet, la Coalition a bénéficié de l'expertise des personnes et groupes suivants dont les travaux universitaires et l'expérience dans le domaine du droit canadien et de la violence facilitée par la technologie ont largement contribué à la création de ce guide pratique.

Suzie Dunn, Assistant Professor, Université de Dalhousie

Rhiannon Wong, Sécurité technologique Canada

Constable Robert Yaschuk, gendarme, division L de la Gendarmerie royale du Canada (GRC)

Courtney Clarke, Our Time to Lead

Hannah Jones, Information juridique communautaire

Women's Network

PEI PEERS Alliance

Services de prévention de la violence familiale

Pride PEI

Centraide - Maritimes

BIPOC USHR

L'équipe de la Coalition souhaite également remercier **Mag Lillo**, de Ruby Square Graphic Design, pour son superbe travail sur ce guide pratique. Nous tenons à remercier à nouveau toutes les contributrices et tous les contributeurs!

Ce *Guide pratique pour se protéger à l'ère numérique* est rendu possible grâce au Secrétariat interministériel des femmes de l'Île-du-Prince-Édouard, avec le soutien financier du ministère des Femmes et de l'Égalité des genres du gouvernement du Canada, en appui au Plan d'action national pour mettre fin à la violence fondée sur le genre.



Women and Gender
Equality Canada

Femmes et Égalité
des genres Canada

INTRODUCTION

Connaissez-vous le terme « cyberintimidation »? Et avez-vous entendu parler des termes « harcèlement », « cyberviolence » ou « cyberharcèlement »? À quoi ces mots vous font-ils penser? Est-ce que quelqu'un que vous connaissez a déjà reçu des textos ou des appels de nature violente? Est-ce que quelqu'un a partagé leurs informations privées sans leur permission? Ces quelques termes ne représentent que la pointe de l'iceberg. Pour en apprendre davantage à leur sujet, il faut discuter de la violence facilitée par la technologie (VFT).



On utilise la VFT comme un outil pour réduire au silence, harceler, intimider et limiter la pleine participation d'une personne ou d'un groupe dans la société, souvent sous la menace de leur sécurité ou leur bien-être. Aujourd'hui, il est pratiquement inévitable d'avoir à interagir avec la technologie tant elle occupe une place centrale dans notre société. On entend souvent l'idée de simplement « se déconnecter » ou « ignorer la haine », mais cela n'est pas toujours possible.

On parle de violence facilitée par la technologie (VFT) lorsque les technologies telles que les ordinateurs, les téléphones intelligents, les appareils GPS, les appareils photo et l'intelligence artificielle (IA) sont utilisées à mauvais escient pour blesser ou contrôler autrui (Sécurité technologique Canada, 2024).

Ce guide pratique pour se protéger à l'ère numérique se consacre à la violence fondée sur le genre facilitée par la technologie (VFGFT), en particulier celle qui survient dans les espaces en ligne. Il traite également de l'utilisation abusive de la technologie pour perpétrer des actes de violence. Il présente les différentes formes de violence liée à la technologie, ainsi que des conseils de sécurité. Ce guide propose également un registre permettant de documenter et de signaler les incidents. La présente ressource s'appuie sur des données montrant que les femmes et les personnes de diverses identités de genre au Canada sont statistiquement plus susceptibles de subir de la VFGFT. Notre objectif est d'aider toutes les femmes et les personnes de diverses identités de genre en position de leadership à mieux comprendre ces enjeux, tout en encourageant la discussion et la mobilisation collective pour lutter contre la VFGFT et la VFT.

Ce qui suit représente quelques exemples concrets de VFT ou VFGFT qui se produisent au Canada et ailleurs dans le monde à l'heure actuelle :

- Publier des menaces de violence physique sur Facebook
- Envoyer un virement électronique de 1 \$ à un compte bancaire après une ordonnance de non-communication
- Traquer quelqu'un par l'entremise de Snapchat
- Partager l'adresse de quelqu'un sur les réseaux sociaux avec une intention malveillante
- Utiliser les comptes en ligne de quelqu'un sans permission
- Créer et distribuer des images générées par l'IA dans le but de nuire à la réputation d'une personne
- Distribuer une image intime de quelqu'un sans son consentement
- Faire des appels répétés à un téléphone ou un cellulaire pendant la nuit
- Envoyer des images par message texte sans consentement
- Utiliser le téléphone de quelqu'un, une caméra cachée ou une application pour la surveiller
- Utiliser la technologie pour savoir ce qu'une personne fait sans obtenir sa permission

Pour saisir les causes profondes et les origines de la violence fondée sur le genre au Canada aujourd'hui, il faut examiner les effets du colonialisme passé et présent. Les monarchies et institutions colonisatrices ont occupé les territoires autochtones, imposant des structures, des politiques, des récits patriarcaux et des systèmes de domination qui continuent à exercer une influence sur la société. Nous ne devons pas oublier que ces récits nuisent à l'ensemble de la population, ayant provoqué une perte forcée de l'identité culturelle, une fragmentation des liens communautaires et des traumatismes intergénérationnels toujours présents. Il est également essentiel de souligner que les femmes, filles et personnes bispirituelles autochtones sont davantage touchées par la violence fondée sur le genre à l'échelle nationale, illustrée par la crise persistante des disparitions et des meurtres des femmes, filles et personnes bispirituelles autochtones, ainsi que l'incarcération disproportionnée des femmes autochtones (*Réclamer notre pouvoir et notre place : le rapport final de l'Enquête nationale sur les femmes et les filles autochtones disparues et assassinées*, 2019). L'enjeu est indissociable du colonialisme persistant et du génocide culturel dont sont victimes les peuples autochtones; il se rattache directement à la violence fondée sur le genre d'aujourd'hui.

LA VIOLENCE FACILITÉE PAR LA TECHNOLOGIE À L'Î.-P.-É. ET AU CANADA

La violence facilitée par la technologie touche toutes les personnes vivant dans des milieux où l'on utilise la technologie. Cependant, certains individus et groupes de personnes sont plus touchés que d'autres, notamment les femmes, les personnes autochtones, noires et de couleur, les personnes vivant avec un handicap et les membres de la communauté 2ELGBTQIA+ (*Déplatformer la misogynie : Rapport sur la responsabilité des plateformes pour la violence sexiste facilitée par la technologie*, 2021).

Si vous lisez ceci et que vous avez vécu une forme de violence technologique, sachez que vous n'êtes pas seule.

Pour mieux comprendre ces déclarations, jetons un coup d'œil aux données actuelles.

N'oubliez pas !

La technologie et Internet ne sont pas en cause ;

ce sont les politiques de sécurité inadéquates et les préjugés humains intégrés qui ont favorisé l'émergence de nouvelles formes de violence. Il est donc essentiel que les plateformes de médias sociaux assument davantage leurs responsabilités envers leurs utilisatrices et utilisateurs et qu'elles soient tenues redevables de leurs actions.

La PEI Coalition for Women's Leadership continuera de revendiquer des changements juridiques et systémiques afin de protéger les individus contre la cyberviolence.



En 2025, la Fondation canadienne des femmes a publié un rapport de recherche intitulé « Lutter contre la violence numérique fondée sur le genre ». Voici certaines de leurs principales constatations :

- Au Canada, 61 % des femmes et des personnes de diverses identités de genre ont subi de la cyberviolence fondée sur le genre, contre 53 % de la population générale.
- Les membres de la communauté 2ELGBTQIA+, les femmes noires et les femmes autochtones sont parmi les personnes les plus fréquemment visées.
- 0 % des femmes autochtones subissent des comportements indésirables en ligne.
- Les jeunes (18 à 25 ans) et les groupes mal desservis sont deux fois plus susceptibles d'avoir des comportements autodestructeurs ou suicidaires ou de passer à l'acte en raison de la cyberviolence.
- 84 % des femmes et 87 % des personnes 2ELGBTQIA+ prennent des mesures supplémentaires pour se protéger de la haine et des abus en ligne, contre 77 % des hommes.

Statistique Canada a trouvé que les jeunes femmes (18 à 29 ans) sont deux fois plus susceptibles de subir de la VFT que les jeunes hommes du même âge.

(Statistique Canada, 2023)

Un sondage mené par deux organismes canadiens, Open Digital Literacy and Access Network (ODLAN) et Wisdom2Action, a révélé que 80 % des personnes bispirituelles, transgenres et non binaires dans le milieu professionnel ont subi de la haine transphobe en ligne, ciblant elles-mêmes ou leur organisme 2ELGBTQIA+.

(Navigating Digital Harms, 2025)

Les formes les plus répandues de haine en ligne envers les personnes bispirituelles, transgenres et non binaires énumérées dans le rapport incluent, sans s'y limiter :

- Des accusations de comportement sexuel prédateur envers les enfants
- Des insultes transphobes et homophobes
- Des menaces de violence physique

Quelles sont les répercussions sur les personnes et les collectivités?

La violence facilitée par la technologie (VFT) peut avoir un impact immédiat et durable sur le bien-être mental, émotionnel et physique d'une personne. Sur le coup, les survivantes et survivants peuvent ressentir une peur intense, de l'anxiété et le sentiment de perdre le contrôle. Les répercussions de la VFT et de la VFGFT incluent :

- ◉ L'autocensure
- ◉ Le retrait des espaces en ligne
- ◉ Les préoccupations en matière de sécurité
- ◉ Les effets néfastes à long terme sur leurs perspectives de carrière, leurs relations et leur santé
- ◉ Les comportements destructeurs envers soi-même ou autrui

L'étude de 2025 de la Fondation canadienne des femmes indique que 55 % des auteurs de préjudices sont identifiés comme étant des hommes, et dans 23 % des cas, la personne survivante ne connaissait pas son genre.

Les plateformes numériques où se produit cette violence ont tendance à attiser la cyberviolence plutôt qu'à la prévenir. Les entreprises de médias sociaux sont principalement guidées par les indicateurs d'engagement et les revenus publicitaires. Ainsi, leurs algorithmes mettent en vedette les publications qui suscitent des réactions vives, comme celles marquées par la misogynie, le racisme ou la haine. Ce mécanisme alimente une boucle où le contenu nuisible gagne en visibilité et en traction, enfermant les utilisatrices et utilisateurs dans la visualisation de contenu marqué par la toxicité.

Quel est le rôle de la technologie et du harcèlement dans le leadership féminin et quelle influence exercent-ils sur une démocratie saine?

La cyberviolence, les préjudices numériques et la violence technologique influencent la participation électorale et la stabilité des mandats dans le contexte politique.



Le jour de l'élection, j'ai publié une photo de moi-même sur X/Twitter sur le compte de ma campagne pour souligner l'importance d'aller voter. Sous la publication, j'ai reçu plus de 35 réponses de différents comptes qui remettaient en question ma stabilité mentale, et qui tenaient des discours haineux liés à mon genre. Certains comptes venaient de l'Île-du-Prince-Édouard, mais apparemment la plupart venaient d'ailleurs.



(Candidate aux élections provinciales de l'Île-du-Prince-Édouard de 2023)



Did you know that tech-facilitated violence has been used to target women and gender-diverse leaders on PEI?

Vous pouvez en apprendre davantage à ce sujet dans le rapport de la Coalition :

Violence fondée sur le genre facilitée par la technologie : Rapport sur la prévalence de la VFGFT lors des élections provinciales de l'Île-du-Prince-Édouard de 2023.



Les personnes élues au Canada jouent un rôle déterminant dans les décisions qui ont des répercussions sur notre vie quotidienne. Une représentation diversifiée dans ces rôles favorise une inclusion accrue des différents groupes communautaires. La promotion de l'égalité de représentation est importante pour une démocratie saine. Des études démontrent une corrélation étroite entre le statut des femmes dans un pays et la qualité de sa démocratie, comme l'atteste l'indice du Georgetown Institute for Women, Peace, and Security (GIWPS). L'évaluation de 96 pays démocratiques a prouvé que le statut des femmes est étroitement lié à des concepts démocratiques clés tels que l'intégrité électorale, la liberté d'association et de réunion, ainsi que l'existence de contre-pouvoirs exécutifs (Exploring the links between women's status and democracy, Université de Georgetown, 2023). La VFGFT et la VFT constituent des obstacles à la diversité, contribuant à l'exclusion de certaines voix et à l'intimidation. Il est donc fondamental de comprendre la terminologie associée à ces formes de harcèlement et de savoir quoi faire lorsque la violence est dirigée contre soi-même ou une personne de son entourage.

73%

Selon les données, 73 % des Canadiennes craindraient d'être victimes de harcèlement en ligne en se présentant à des élections, alors que ce taux s'élève à 63 % chez les Canadiens.
(Voix égales, 2023)

63%



J'ai été victime de menaces. Un homme a réussi à trouver mon courriel personnel, je ne sais pas trop comment. Son courriel renfermait des menaces de violence physique à peine voilées, avec beaucoup de jurons. J'ai identifié sa circonscription, puis nous avons évité sa maison et son secteur au cours de la campagne. On m'a dit de peut-être appeler la GRC, mais rien de plus. Personne ne semblait savoir quoi faire.



DEFINITIONS

Comprendre le langage associé à la violence facilitée par la technologie

Les termes suivants définissent la violence fondée sur le genre facilitée par la technologie, ainsi que ses formes courantes. Les effets individuels liés à la cyberviolence sont souvent sous-estimés à cause de la fausse perception que la violence perpétrée en ligne ou par le biais de la technologie ne cause pas de véritables préjudices. Cela est complètement faux. Il est essentiel de nommer ces actes dès qu'ils surviennent, car cela nous permet de les comprendre et d'intervenir. Gardez à l'esprit que la technologie, tout comme la terminologie utilisée pour décrire ces actes de violence facilitée par la technologie, évolue constamment. (*Violence basée sur le genre facilitée par la technologie : rendre tous les espaces sûrs*, 2021)

Abus fondé sur l'image (AFI) : Utilisation d'images pour contraindre, menacer, harceler, chosifier ou maltraiter une victime. Cela inclut de prendre, de créer, de menacer le partage, ou de partager des images intimes ou sexuelles sans consentement. Ces images peuvent être de nature sexuelle ou non. Une image non sexuelle est toute photo que la victime définit comme étant privée; par exemple, si une personne partage sur les réseaux sociaux la photo d'une femme musulmane qui ne porte pas le hijab, alors qu'elle en porte toujours en public. (Voir « distribution non consentie d'images intimes », « creepshots », « exploitation sexuelle », « sextorsion » et autres termes dans le glossaire)

Auteur ou auteure : Personne qui utilise la technologie dans le but de nuire à une personne ou un groupe, quelles que soient ses motivations. Ce terme doit être interprété de manière inclusive, reconnaissant que chaque personne possède la capacité de causer du tort, mais également d'apprendre de ses erreurs.

Cyberintimidation : Utilisation de la messagerie numérique comme les messages de groupe, les textos, les courriels ou les messages directs pour harceler, intimider ou nuire à autrui; ce terme s'utilise généralement en relation avec les enfants et les jeunes.

Cyberharcèlement : Utilisation de la technologie pour traquer et surveiller les comportements d'une personne en temps réel ou par l'historique. Cela peut inclure l'installation d'Apple AirTags sur la voiture de quelqu'un ou la surveillance de ses déplacements par l'entremise du partage de localisation sur Snapchat ou des cartes Instagram.

Diffamation en ligne : Diffusion publique de fausses informations qui portent atteinte à la réputation d'une personne et visent à humilier, menacer, intimider ou punir. La diffamation est particulièrement courante chez des personnalités publiques comme les fonctionnaires, les activistes et les journalistes. En fait, toute personne occupant un poste de leadership visible est davantage susceptible d'être ciblée.



Cyberviolence

Un terme qui devient de plus en plus courant. Bien qu'il se rapproche de la définition de la VFT, il ne s'agit pas de la même chose.

Le préfixe du mot est « cyber », qui signifie « impliquant, utilisant ou se rapportant à l'informatique, en particulier à Internet ».

Cette définition exclut donc l'utilisation de technologies qui ne se rapportent pas aux ordinateurs ou à l'Internet, telles que les appareils photo, les lignes fixes, etc.

(Dictionnaire Cambridge, 2024).



Le saviez-vous ?
L'organisme
Information juridique
communautaire
a publié un guide
qui explique
comment procéder
si quelqu'un partage
vos images intimes.

Pour obtenir cette
ressource :



Divulgaration malveillante (Doxing) : Utilisation d'une plateforme en ligne pour divulguer publiquement des informations personnelles d'une personne telles que son adresse, son courriel personnel, ses numéros de téléphone, son lieu de travail, les coordonnées de sa familiale ou des photos des membres de sa famille, dans le but de la localiser et de lui causer des préjudices. (Voir « morinommer » dans le glossaire.)

Harcèlement en ligne : Utilisation de plateformes en ligne pour contacter, menacer ou effrayer une autre personne de manière répétée par des images, commentaires ou messages offensants, dégradants ou insultants. (Voir : « harcèlement multiplateforme », « discours haineux numérique » et « cybermenace » dans le glossaire)

Piratage : Utilisation de la technologie pour obtenir un accès illégal ou sans permission à des systèmes ou des ressources dans le but d'attaquer, de nuire ou d'incriminer une personne. Cela inclut le vol de données, l'acquisition d'informations personnelles, la modification d'informations, la violation de la vie privée ou l'installation de virus sur les appareils.

Usurpation d'identité : Processus consistant à voler l'identité d'une personne afin de la menacer, de l'intimider ou de porter atteinte à sa réputation. Par exemple, cela pourrait être l'utilisation des photos d'une personne pour créer un faux profil et se faire passer pour un ami de confiance afin d'obtenir des informations privées. (Selon la plupart des plateformes sociales courantes, l'usurpation d'identité ne s'applique pas aux comptes parodiques évidents.)

Violence fondée sur le genre facilitée par la technologie (VFGFT) : Tout acte commis, aidé, aggravé ou amplifié par l'utilisation des technologies de l'information et de la communication ou des médias numériques qui entraîne ou est susceptible d'entraîner des préjudices physiques, sexuels, psychologiques, sociaux, politiques ou économiques, ou d'autres atteintes aux droits et libertés. Cette forme de violence vise une personne en raison de son genre, ciblant de manière disproportionnée les femmes, les filles et les personnes bispirituelles, trans et non binaires (ONU Femmes).

Violence numérique qui devient de la violence physique : Lorsque les menaces en ligne antérieures ou en cours, ainsi que les discours haineux numériques, dégénèrent en harcèlement ou agressions physiques dans la vie réelle ou en personne.

COMMENT PRÉVENIR LA VFT ET Y RÉAGIR EN TANT QU'INDIVIDU

Avant de discuter des mesures d'action communautaire, parlons des coûts individuels liés à la prévention et à la lutte contre la violence facilitée par la technologie, ainsi que des obstacles financiers possibles.

Coûts du bien-être

Il est important de reconnaître le fardeau émotionnel lié à la mise en place de mesures de protection individuelle contre la violence facilitée par la technologie. Être ciblé peut entraîner des répercussions sur votre bien-être physique et mental, vos revenus, votre sentiment de sécurité, votre confiance, et davantage. N'oubliez pas que de vous tourner vers vos amis, votre famille et votre communauté pour solliciter de l'appui est un signe de force. Vous n'avez pas à affronter cette situation seule.

Coûts financiers

Les coûts financiers pour se protéger peuvent être élevés. Certaines personnes peuvent se permettre des mesures de sécurité supplémentaires, comme un service de réseau privé virtuel (RPV), des logiciels de protection antivirus et des gestionnaires de mots de passe, tandis que d'autres ne peuvent se permettre ces dépenses.

Voici les cinq principaux conseils de prévention de base, servant d'exemples de mesures individuelles que vous pouvez prendre pour améliorer votre sécurité.

LES 5 MEILLEURS CONSEILS SUR LA SÉCURITÉ TECHNOLOGIQUE

1. Utilisez des mots de passe et des noms d'utilisateur forts (évitiez d'utiliser le nom de vos animaux de compagnie!)

HABITUDES À HAUT RISQUE POUR LES MOTS DE PASSE

- Utiliser des mots de passe courants ou évidents comme « QWERTY123 » ou « Password »
- Utiliser votre anniversaire, l'anniversaire d'un proche, ou des dates d'anniversaire importantes
- Utiliser un seul mot de passe pour tous les comptes
- Utiliser des réponses aux questions de vérification d'identité que d'autres pourraient connaître ou deviner (par exemple, le nom de jeune fille de votre mère, votre couleur préférée, le modèle de votre première voiture)

Mon mot de passe est-il assez sécuritaire?

Mettez-le à l'essai avec Sécurité technologique Canada :





Si une personne passait 10 minutes à examiner votre profil Facebook ou Instagram, pourrait-elle deviner votre mot de passe ?



HABITUDES SÉCURITAIRES POUR LES MOTS DE PASSE

(Sécurité technologique Canada, 2024).

- Utiliser des phrases passe : une séquence de mots différents non liés
- Changer les lettres en symboles ou chiffres (utiliser @ au lieu de « a », utiliser 3 au lieu de « E »), par exemple : H@ppyw@t3rbottl3
- Tester son mot de passe pour voir s'il est sécurisé : www.security.org/how-secure-is-my-password/
- Utiliser un gestionnaire de mots de passe sécurisé
- Modifier ses mots de passe tous les 6 mois
- Ne pas autoriser son compte Google ou Facebook à partager l'accès à ses mots de passe pour d'autres sites web ou comptes

2. Déconnectez-vous de vos comptes et applications

Décochez l'option « Rester connecté » et ne laissez pas les navigateurs web sauvegarder les mots de passe pour établir une connexion automatique. Cela empêche d'autres personnes d'utiliser votre appareil pour se faire passer pour vous par l'entremise de vos comptes. Notez vos données de connexion sur papier ou utilisez un gestionnaire de mots de passe.

3. Désactivez le partage de localisation

Les téléphones intelligents peuvent suivre votre localisation, et certaines applications vendront vos données à des entreprises tierces. Il est possible de partager sa localisation sans même s'en rendre compte. Empêchez les applications d'utiliser votre localisation en désactivant cette fonction dans les paramètres de confidentialité de votre téléphone. Les comptes de médias sociaux ont aussi des paramètres de confidentialité pour limiter qui peut voir votre localisation.

Le saviez-vous ? Instagram a récemment mis en place un partage de localisation sur sa plateforme. Assurez-vous de vérifier les paramètres de confidentialité régulièrement, particulièrement après la mise à jour d'une application sur votre appareil.

4. Utilisez la navigation privée

Il est possible de naviguer sur Internet en privé en utilisant Mozilla Firefox, Microsoft Edge, Safari et DuckDuckGo. La navigation privée empêche les autres de voir les sites que vous avez visités. Cette fonction apporte une sécurité accrue lorsque vous utilisez l'ordinateur d'un ami ou un appareil public, ou si vous soupçonnez que quelqu'un surveille votre appareil sans votre permission. Veuillez noter que ce geste ne garantit pas la vie privée; par exemple, Google Chrome est visé par une poursuite à l'heure actuelle parce qu'il a été reconnu que son mode incognito portait atteinte à la vie privée.

5. Utilisez la vérification en deux étapes

Pour configurer une vérification en deux étapes, vous aurez besoin d'une deuxième adresse courriel ou d'un numéro de cellulaire sécurisé. Si quelqu'un tente de se connecter à votre compte à partir d'un autre appareil ou d'un autre endroit, la plateforme de courriel, la banque ou un autre service enverra un code à votre deuxième courriel ou à votre téléphone. Vous aurez besoin de ce code ainsi que de votre mot de passe pour vous connecter. Si vous n'avez pas accès à ce courriel ou à ce téléphone secondaire, la connexion ne pourra être établie.

COMMENT PRÉVENIR LA VFT ET Y RÉPONDRE EN TANT QUE COLLECTIVITÉ

Pour mettre fin à la violence facilitée par la technologie (VFT) et à la violence fondée sur le genre facilitée par la technologie (VFGFT), il faut un soutien collectif. Il est essentiel d'agir ensemble au sein de la collectivité afin de promouvoir des espaces numériques sécurisés et responsables. Voici des mesures concrètes que vous et votre communauté pouvez entreprendre ensemble pour apporter un changement significatif :

Mobilisez-vous auprès des différents paliers de gouvernement

Encouragez un changement de politique : Unissez vos forces aux organisations qui plaident en faveur du renforcement de la réglementation en matière de sécurité numérique. Communiquez avec votre député(e) fédéral(e) ou votre député(e) provincial(e) par courriel, téléphone, réseaux sociaux ou lors d'événements, afin de leur faire part de votre désir de rendre l'utilisation des technologies numériques plus sécuritaire.

Exigez la création d'une Commission de sécurité numérique : Encouragez le gouvernement fédéral à établir une Commission de sécurité numérique pour superviser la sécurité en ligne et les droits numériques. Vous pouvez commencer en envoyant un courriel ou en communiquant avec votre député(e) fédéral(e) pour discuter de l'importance la sécurité en ligne pour vous et votre collectivité.

Parlez au nouveau ministre canadien de l'Intelligence artificielle et de l'Innovation numérique, le ministre de la Justice et procureur général du Canada, ainsi que d'autres ministres concerné(e)s du Cabinet : Invitez ces ministres ou votre député(e) à déposer un projet de loi tenant les grandes entreprises technologiques responsables de leurs actes qui incluent de permettre les comportements préjudiciables sur leurs plateformes ou de ne pas en tenir compte.

Tirez des leçons des mouvements mondiaux

Des pays comme l'Australie, le Chili, le Brésil, l'Union européenne et plusieurs autres ouvrent déjà la voie avec de nouvelles réglementations qui traitent de la VFT. Explorez leurs diverses approches et pensez de façon critique. Avec quoi êtes-vous en accord ou en désaccord? Qu'est-ce qui pourrait fonctionner dans votre collectivité? Le partage des meilleures pratiques mondiales contribue à renforcer le mouvement pour la sécurité numérique à l'échelle locale.

Aidez à responsabiliser les grandes entreprises technologiques

Exigez la transparence et la responsabilisation : Participez à des campagnes ou des initiatives qui visent à encourager les entreprises technologiques qui sont lentes à agir à prendre des mesures concrètes et à assumer pleinement la responsabilité des préjudices causés sur leurs plateformes..

Soutenez des règlements qui comportent des conséquences : Préconisez l'adoption de lois comportant des mécanismes explicites de reddition de comptes pour les plateformes numériques qui permettent la violence incontrôlée.

Bâtir des communautés en ligne sécuritaires

Adoptez des codes de conduite : Encouragez votre lieu de travail, votre école ou vos espaces de bénévolat à adopter des codes de conduite en ligne et des règles claires qui priorisent la sécurité numérique.

Proposez d'autres formes de responsabilisation : La violence facilitée par la technologie ne devrait pas systématiquement être traitée par la justice pénale. Impliquez-vous et soutenez des modèles de responsabilisation communautaires qui placent les survivantes et survivants au cœur du processus et qui favorisent la réparation..

Soutenez l'éducation et l'apprentissage au sujet de la misogynie en ligne : À l'heure actuelle, on retrouve des groupes de propagande haineuse sur plusieurs plateformes en ligne. Ces groupes s'organisent dans le but de propager et de diriger la haine envers les femmes, les personnes transgenres et les personnes de genre non conforme. L'apprentissage des termes comme « androsphère », « célibat involontaire (incel) » et la « pilule rouge », ainsi que de compétences de pensée critique pour repérer ce contenu, est essentiel pour mettre fin au soutien à ces mouvements. Cette éducation est particulièrement importante pour les jeunes hommes et garçons, car ces groupes ciblent activement les jeunes hommes et ils recrutent auprès de ce groupe démographique.

Parlons-en

La VFGFT ne reçoit pas l'attention qu'elle mérite. Lancez des conversations avec vos amis, votre famille et votre collectivité. La sensibilisation est l'un des outils les plus puissants à notre portée. Plus les gens saisissent la problématique, plus ils peuvent y apporter une réponse concrète.

N'OUBLIEZ PAS

L'action communautaire accroît l'efficacité des initiatives. Que vous adressiez vos préoccupations à un(e) représentant(e) politique, mettiez en place une nouvelle politique en milieu de travail ou lancez simplement un dialogue, chaque démarche contribue à la création d'un environnement numérique plus sécuritaire pour tous.

QUEL EST LE RÔLE DES TÉMOINS EN LIGNE?

La violence facilitée par la technologie varie en intensité. Si vous ou quelqu'un que vous connaissez êtes dans une situation qui présente une menace pour la vie, contactez les autorités compétentes ou les services locaux avec lesquels vous vous sentez en sécurité. Le rôle des témoins dans de telles circonstances est d'assurer leur propre sécurité, tout en évaluant soigneusement les risques d'intervenir et les conséquences possibles sur autrui. La section suivante détaille des étapes précises permettant aux témoins de contribuer de manière efficace et responsable.

Une excellente façon de contrer les discours haineux en ligne est de se soutenir mutuellement dans des espaces virtuels. De la section des commentaires sur Facebook aux chaînes de courriels de travail, il existe de nombreuses façons d'afficher son soutien et d'agir comme un modèle positif pour ceux qui vivent la VFGFT ou la VFT.

L'acronyme suivant vous aidera à vous souvenir des actions à entreprendre en tant que témoin actif. Le modèle AIDED a été créé par l'Université de La Trobe à Melbourne, en Australie. Il a été modifié pour ce guide pratique comme suit :

A - AIDER à trouver du soutien

I - Agir de façon INDIRECTE

D - Agir de façon DIRECTE

E - ÉTABLIR les preuves de l'incident

D - DÉTOURNER la violence

Il n'est pas nécessaire d'utiliser toutes les actions énumérées ci-dessus pour chaque situation. Voici quelques exemples du modèle AIDED en action pour savoir à quel moment utiliser les différentes méthodes :

EXEMPLE UN

Votre collègue reçoit un courriel d'un compte inconnu vers son compte de courriel du bureau. Ce message renferme des menaces de violence, y compris des insultes de nature sexiste. Votre collègue ne comprend pas comment cette personne a trouvé son adresse courriel, et elle ne sait pas quoi faire.

Agir de façon indirecte : Discutez de l'événement avec votre collègue. Offrez-lui du soutien, et restez à l'écoute si elle désire parler de la situation.

Êtes-vous à la recherche de **méthodes détaillées pour rester en sécurité**? Consultez cette ressource de **Take Back the Tech** :



Désirez-vous encourager le gouvernement fédéral à former une **Commission de sécurité numérique**? Suivez ce lien pour en savoir davantage :



Aider à trouver du soutien : Trouvez les soutiens offerts par votre organisation, que ce soit par l'entremise des ressources humaines ou d'une politique de VFT à suivre.

Détourner la violence de la cible : Comment votre lieu de travail pourrait-il empêcher que cette situation se reproduise ? Par exemple, on pourrait établir une adresse courriel générale qui reçoit toutes les demandes et qui exige une réponse à un test CAPTCHA avant d'accepter les courriels. Une autre solution serait de s'assurer que l'équipe du bureau sache où se trouve leur adresse de courriel professionnel sur Internet. Vous pouvez aussi encourager l'équipe à bloquer cet expéditeur inconnu de leur compte.

EXEMPLE DEUX

Votre amie vous confie que son ex-partenaire, qui partage une amitié avec vous, distribue des images intimes d'elle sans sa permission depuis la fin de leur relation. Elle se sent très mal à l'aise et contrariée que ces photos soient partagées avec d'autres.

Agir de façon directe : Demeurez attentifs à la dynamique relationnelle de chacune des personnes impliquées et parlez à votre amie des actions qu'elle souhaite entreprendre. Ces actions pourraient inclure de parler aux personnes qui ont reçu les images et leur demander de veiller à ce qu'elles les suppriment de leurs appareils.

Établir les preuves de l'incident : Par exemple, si quelqu'un lui a envoyé des captures d'écran des images divulguées par l'ex-partenaire, dites à votre amie d'imprimer des copies de l'échange et de les sauvegarder sur un appareil protégé, surtout si elle souhaite tenter une action en justice.

Remarque : Il y a lieu d'intenter une action en justice à l'Île-du-Prince-Édouard dans l'exemple deux puisque le partage d'images intimes sans consentement est régi par la loi intitulée Intimate Images Protection Act (Loi sur la protection des images intimes), 2021.

EXEMPLE TROIS

Un membre de votre famille proche partage son opinion sur un sujet controversé sur un site public des réseaux sociaux. Lorsque la publication attire l'attention, un groupe d'utilisateurs et utilisatrices en désaccord commence à harceler cette personne en ligne avec des commentaires haineux, des messages violents et des menaces de violence sexuelle. Votre proche a peur et communique avec vous pour obtenir de l'aide.

Établir les preuves de l'incident : Aidez votre proche à documenter tous les messages privés et commentaires publics, y compris les noms des utilisateurs et utilisatrices ayant participé au harcèlement, en prenant des captures d'écran.

Aider à trouver du soutien : Si votre proche dit vouloir signaler cet incident à la police, utilisez le registre de violence facilitée par la technologie dans le présent guide pour recueillir des preuves organisées afin de constituer un dossier. Vous pouvez aussi soutenir votre proche en signalant les utilisateurs et utilisatrices concernés à la plateforme de médias sociaux et en aidant à bloquer leurs comptes.

N'oubliez pas : Bien que les règlements varient selon les plateformes, il demeure important de signaler les harcèlements en ligne soupçonnés ou confirmés, et de bloquer les auteur(e)s. Avant de supprimer des messages harcelants ou de bloquer les utilisateurs concernés, n'oubliez pas de documenter l'incident avec des captures d'écran.

En collaborant avec le gouvernement et les entreprises de médias sociaux, nous pouvons normaliser une culture de bienveillance envers autrui, établir de meilleures limites en ligne et améliorer la sécurité sur Internet pour tous.

POURQUOI EST-IL IMPORTANT DE PRÉSERVER LES PREUVES DE VFT?

Voici quatre raisons de tenir un registre de rapports de VFT :

1. Pour établir les schémas de comportement

Vous pouvez être la cible d'un incident de VFT à une ou plusieurs reprises. Il est important d'établir les dates de tous les incidents et de les organiser en ordre chronologique. Cette méthode pourrait établir un schéma qui mène à des réponses, surtout dans le cas où le harcèlement provient d'une source anonyme.

2. Pour documenter des preuves fiables à l'appui d'une enquête

Les preuves recueillies à la suite de l'incident serviront à évaluer dans quelle mesure le système judiciaire peut intervenir. Si vous décidez de signaler l'incident à la police ou d'engager une procédure judiciaire, on vous demandera de fournir des déclarations détaillant cet événement. Tenir un registre peut ainsi vous permettre d'assurer la cohérence de vos preuves.

3. Pour vous donner l'occasion de maîtriser une situation émotionnelle

Le choix d'être la cible de VFT ne vous revient pas, mais il est possible de prendre des mesures concrètes par rapport à ces expériences, comme les consigner par écrit. Cela permet de garder la main sur la situation et, éventuellement, de déterminer s'il convient de présenter ce registre aux autorités.

4. Pour confirmer et garder le souvenir

Avec le temps, les souvenirs d'expériences abusives peuvent s'estomper. Tenir un registre permet d'obtenir un témoignage fiable sur l'impact négatif de ces incidents. Cela peut également vous apporter la certitude que les faits ont eu lieu, dissipant ainsi tous les doutes ou sentiments de déni concernant leur réalité et leurs conséquences nuisibles.



PLAN DE SÉCURITÉ!

Pour vous protéger contre une personne abusive qui pourrait trouver le registre, songez à un endroit où vous pouvez le cacher en toute sécurité.

Conseils pour la confidentialité en utilisant les navigateurs Internet :



À quel moment serait-il utile d'apporter votre registre de rapports de VFT à la police ?

Selon les circonstances, il peut être important d'ouvrir un dossier par rapport à l'incident. Il est également important de noter qu'un signalement ne signifie pas toujours une action. La police déterminera si votre dossier correspond à la définition de harcèlement ou d'un autre crime du Code criminel.

Lorsque vous signalez un incident, la police peut vous demander quelles mesures vous souhaitez qu'ils prennent contre l'auteur(e). Songez à votre réponse avant de signaler l'incident.

Important : Le Code criminel du Canada n'a pas de code particulier qui couvre tous les actes de la VFT. La VFT relève donc des 14 codes ci-dessous :

- | | |
|--|---|
| 1. Les infractions contre la personne et la réputation | 8. Le vol d'identité |
| 2. Le harcèlement criminel | 9. La publication non consensuelle d'images intimes |
| 3. Les méfaits à l'égard de données | 10. L'intimidation |
| 4. L'utilisation non autorisée d'ordinateur | 11. L'incitation à la haine |
| 5. L'extorsion | 12. Le fait de conseiller le suicide |
| 6. Proférer des menaces | 13. La diffamation |
| 7. Les faux renseignements, les communications indécentes ou harcelantes | 14. L'incitation publique à la haine |

LE REGISTRE DE RAPPORTS DE VIOLENCE FACILITÉE PAR LA TECHNOLOGIE

Utilisez le formulaire ci-dessous pour tenir un registre de tout incident de VFT perpétré contre vous. Documentez chaque incident séparément et incluez toutes les preuves à l'appui en utilisant des captures d'écran, photos, vidéos ou enregistrements audio sauvegardés. Nous vous recommandons de garder votre propre copie des registres si vous les soumettez au service de police. Envisagez aussi de partager ce registre avec une personne de confiance qui pourra fournir une cachette sécuritaire pour la documentation, en cas d'activation du plan de sécurité.

Le programme RISE de l'Information juridique communautaire de l'Î.-P.-É. offre des informations juridiques en langage clair aux victimes de violence sexuelle, de violence entre partenaires intimes, ou de harcèlement sexuel en milieu de travail, incluant jusqu'à 4 heures de conseils juridiques gratuits de la part d'un(e) avocat(e) spécialisé(e) en traumatismes.

***Remarque :** Si vous vivez actuellement une situation abusive ou que vous soupçonnez que quelqu'un surveille vos appareils, songez à utiliser l'appareil d'une personne de confiance ou un appareil public dans une bibliothèque ou une école locale pour accéder à ce registre. Si vous n'avez accès qu'à votre appareil personnel, consultez les conseils de confidentialité de navigateur Internet à www.techsafety.ca pour apprendre comment renforcer les paramètres de sécurité de vos données et de votre historique de navigation.

Cette ressource a été adaptée à partir du Journal des abus facilités par la technologie créée par Sécurité technologique Canada, un projet d'Hébergement femmes Canada.

Registre de rapports de violence facilitée par la technologie

Vos coordonnées

Nom :

Date :

Mode de communication préféré :

Courriel :

Numéro de téléphone :

Informations sur l'auteur(e) ou l'agresseur(-se)

Nom(s) légal(-aux) et nom(s) d'utilisateur(s) si connus :

Lien avec cette personne (le cas échéant) :

Coordonnées de l'auteur(e) ou de l'agresseur(-se) (si connues)

Adresse du domicile :

Numéro de téléphone :

Adresse courriel :

Noms de comptes ou de profils en ligne :

Autres informations pertinentes (noms d'utilisateur/comptes avec lesquels la personne interagit, type de contenu qu'elle partage) :

Description de l'incident

Date de l'incident :

Heure :

Décrire l'incident :

Noter les noms/noms d'utilisateur des témoins :

Appareils

Énumérer les appareils, comptes ou autres technologies ayant servi dans cet incident.
Cocher toutes les cases nécessaires pour décrire l'événement.

- | | |
|---|---|
| ☐ Téléphone intelligent | ☐ Appareil photo |
| ☐ Tablette | ☐ Traque de la localisation |
| ☐ Ordinateur/ordinateur portable | ☐ Intelligence artificielle |
| ☐ Appareil des enfants | ☐ Console de jeu |
| ☐ Plateforme de médias sociaux | ☐ Appareil intelligent (ex. Alexa, montre, téléviseur) |
| ☐ Téléphone | ☐ Autres |
| ☐ Dispositif d'enregistrement | |
| ☐ Inconnu, mais suspect _____ | |

Identifier le type/modèle/marque de l'appareil (par exemple, iPhone 12) :

Comptes

- | | |
|--|---------------------------------------|
| ☐ Adresses courriel | ☐ Banque |
| ☐ Compte de médias sociaux | ☐ Gouvernement |
| ☐ Application de rencontres | ☐ Autres |
| ☐ Application | ☐ Sans objet |

Type de compte (ex. Gmail, Facebook, application bancaire) :

Conséquences personnelles de l'incident

Décrire tout changement de comportement ou de routine que vous avez apporté à la suite de cet incident et décrire toute détresse émotionnelle causée par cet incident.

Describe any emotional distress caused by this incident: **NEED FRENCH**

Nom(s) ou nom(s) d'utilisateur de la famille, des ami(e)s ou des autres personnes impliquées :

Inclure tous les documents (captures d'écran, enregistrements) énumérés ici :

Chercher du soutien

À qui l'incident a-t-il été signalé ?

- | | |
|---|--|
| ☐ Service de police | ☐ Entreprise technologique |
| ☐ Services de soutien | ☐ Professionnel(le) en TI dans une entreprise technologique |
| ☐ Thérapeute | ☐ Famille ou ami(e) de confiance |
| ☐ Prestataire de services médicaux | ☐ Employeur |
| ☐ Service téléphonique/Internet | ☐ Autres |

Décrivez la réponse donnée par les services cochés ci-dessus :

Signalement à la police

Si vous avez signalé cet incident à la police et leur avez fourni les informations ci-dessus pour la collecte de preuves dans votre dossier, conservez cette partie du registre pour vos propres documents.

Date :

Titre de l'agent(e) :

Poste de police :

Numéro d'insigne de l'agent(e) :

Nom de l'agent(e) :

Numéro de téléphone de l'agent(e) :

Recueillez tous les reçus liés au présent incident et notez la valeur en dollars des coûts associés à ce cas (par exemple, le remplacement d'un appareil, les frais d'annulation ou d'inscription à un nouveau forfait téléphonique, les séances de thérapie, etc.) ci-dessous :

SOUTIEN ET RESSOURCES SUPPLÉMENTAIRES

Numéros de téléphone non urgents

- GRC – 902-566-7112
- Service de police de Charlottetown – 902-629-4172
- Service de police de Summerside – 902-432-1201
- Service de police de Kensington – 902-836-4499

Arbre d'aide de l'Î.-P.-É.

Cet organigramme vise à informer les Insulaires des nombreuses ressources d'aide offertes à l'Île-du-Prince-Édouard.

<https://pei.cmha.ca/find-help/the-pei-helping-tree/>

211 Î.-P.-É.

Le 211 est un service téléphonique conçu pour aider à trouver de l'information sur les programmes et services sociaux offerts dans la province. Le 211 offre aux Insulaires et aux fournisseuses et fournisseurs de services un accès rapide et facile, 24 heures sur 24, 365 jours par an, en composant le 2-1-1. Le service offre également une base de données en ligne de tous les programmes. www.pe.211.ca.

Information juridique communautaire de l'Î.-P.-É.

CLI est un organisme de bienfaisance enregistré au service de l'Île-du-Prince-Édouard. Il offre des informations juridiques aux résidentes et résidents, et les aide à naviguer dans le système judiciaire provincial. Le programme RISE offre un soutien et des ressources particulières aux personnes touchées par la violence sexuelle, y compris le signalement et la recherche d'aide. Les personnes de toute identité ou expression de genre de 16 ans ou plus peuvent accéder à leurs services confidentiels.

<https://legalinfopei.ca/>

Services de prévention de la violence familiale à l'Î.-P.-É.

Cet organisme communautaire repose sur les principes de justice, d'égalité et de paix. Il s'engage à éliminer toute forme de violence – physique, sexuelle ou émotionnelle – au sein des familles, notamment par la défense des droits, la mise en place de programmes de prévention et l'offre de services de qualité destinés à soutenir et à renforcer les personnes victimes de violence familiale. <https://fvps.ca/>

Commission des droits de la personne de l'Î.-P.-É. : SHIFT

Ce projet vise à la lutte et la prévention du harcèlement sexuel dans les milieux de travail de l'Île grâce à la sensibilisation et à l'éducation. Il offre une formation gratuite adaptée aux employeurs, aux membres du personnel, aux élèves du secondaire et au grand public.

<https://www.makeityourbusinesspei.ca/>



Service d'aide aux victimes, gouvernement de l'Île-du-Prince-Édouard

Le service d'aide aux victimes aide les victimes d'actes criminels tout au long de leur expérience dans le système de justice pénale. Cette aide est accessible aux victimes d'actes criminels de l'ensemble de l'Î.-P.-É. Si vous habitez à l'extérieur de l'Île, mais que vous avez été victime d'un acte criminel à l'Île, vous êtes également admissible à ce service. Ce service confidentiel est offert gratuitement.

<https://www.princeedwardisland.ca/en/information/justice-and-public-safety/victim-services>



Ministère de la Justice et de la Sécurité publique de l'Î.-P.-É., Programme de justice réparatrice

Le programme de justice réparatrice offre aux auteurs d'infractions et aux victimes l'occasion de participer à une communication sécuritaire et efficace (directe ou indirecte) pour discuter des répercussions de l'acte criminel sur la victime.

<https://www.princeedwardisland.ca/en/information/justice-and-public-safety/restorative-justice>



Programme de justice autochtone de la Mi'kmaq Confederacy of PEI

La Mi'kmaq Confederacy offre un soutien juridique important aux peuples autochtones vivant à Epekwitk (Î.-P.-É.). Elle se centre sur l'aide aux auteurs d'infractions, aux victimes et aux communautés impliquées dans des conflits juridiques à comprendre les causes profondes de leurs actes. Elle travaille en collaboration avec la communauté autochtone, veillant à ce que son programme respecte les valeurs et les traditions culturelles.

<https://mcpei.ca/contact/>



Cybervigilance

Il s'agit d'une campagne de sensibilisation publique et d'une ressource en ligne visant à soutenir les parents, les prestataires de soins et les éducatrices et éducateurs à aider les jeunes à utiliser Internet de façon sécuritaire et responsable. La campagne offre des conseils sur des sujets comme les jeux vidéo, les médias sociaux, la cyberintimidation, l'équilibre sain par rapport au temps d'écran et le bien-être numérique dans le contexte particulier de l'Île-du-Prince-Édouard. La campagne a été lancée par le Secrétariat interministériel aux affaires féminines, par l'entremise du gouvernement de l'Î.-P.-É.

<https://www.cybersafecarepei.ca/>



RESSOURCES CANADIENNES ET INTERNATIONALES



Réseau ouvert de littératie numérique et d'accès

ODLAN fournit aux organisations canadiennes qui desservent les communautés 2ELGBTQIA+ les outils, les ressources et les connaissances nécessaires pour créer des espaces en ligne inclusifs et les faire croître. <https://odlan.ca/>



Sécurité technologique Canada

Ce site fournit aux femmes, aux enfants et aux personnes de diverses identités de genre les connaissances et ressources nécessaires pour gérer leurs expériences de violence fondée sur le genre facilitée par la technologie. Les informations pour les survivantes, pour celles qui appuient les survivantes et les guides pour sécuriser les appareils technologiques se trouvent ici : <https://securitetech.ca/>



Fondation canadienne des femmes : Reprends ton espace numérique

Cette fondation offre un cours d'apprentissage en ligne gratuit pour renforcer ses compétences et ses connaissances, et offre des ressources pour pouvoir interagir en toute sécurité dans les espaces en ligne et pour contribuer à mettre fin à la cyberviolence fondée sur genre.

<https://canadianwomen.org/fr/mettons-fin-a-la-cyberviolence-fondee-sur-le-genre/>



Centre canadien pour l'autonomisation des femmes

Le CCAF est un organisme à but non lucratif qui œuvre à démanteler les obstacles systémiques auxquels font face les survivantes de violence économique, d'endettement forcé et d'exploitation financière. En nous appuyant sur des recherches centrées sur l'équité et en tenant compte des traumatismes, nous favorisons la prévention et l'intervention par le biais de changements systémiques et de l'engagement communautaire <https://ccfwe.org/>



Crash Override

Ce groupe de défense offre du soutien et des ressources aux personnes victimes de violence en ligne. Ils forment un réseau d'experts(es) et de survivants(es) qui travaillent directement avec les victimes, les entreprises technologiques, les législateurs, les médias, les experts(es) en sécurité et les forces de l'ordre pour éduquer et fournir une assistance directe afin d'éliminer les causes de la violence en ligne. <http://www.crashoverridenetwork.com/index.html>

GLOSSAIRE

Ces termes sont liés à la violence facilitée par la technologie et en sont les fondements. Veuillez noter qu'il ne s'agit pas de définitions juridiques et que ces termes peuvent avoir une définition différente dans le contexte de la loi canadienne.

Abus basé sur l'image : Il s'agit d'un terme générique utilisé pour décrire les formes de VFGFT liées aux images numériques (Dunn, 2020).

- i. **Divulgaration non consensuelle d'images intimes :** Cela se produit lorsque les images sexuelles ou intimes d'une personne sont partagées avec d'autres personnes, ou un public plus large que prévu, sans leur consentement.
- ii. **Documentation ou diffusion d'agressions ou de violences sexuelles :** L'enregistrement ou la diffusion en direct de vidéos renfermant de la violence sexuelle. Ces vidéos sont parfois publiées sur les réseaux sociaux, envoyées par texto entre pairs, et vendues ou échangées à des personnes ou des sites web.
- iii. **Médias modifiés ou hypertrucage (*deepfakes*) :** Images, vidéos et audios numériques créés ou modifiés par l'IA ou un logiciel de retouche photo pour donner l'impression qu'une personne dit ou fait quelque chose qu'elle n'a jamais dit ou fait. L'hypertrucage peut être difficile à distinguer des vidéos et images réelles. Il est souvent utilisé pour créer du faux contenu sexuel, comme permuter le visage d'une personne sur des vidéos pornographiques sans son consentement. L'hypertrucage sert également à créer de faux enregistrements audios qui peuvent servir dans les appels téléphoniques frauduleux.
- iv. **Sexploitation :** Ce terme consiste à tirer profit de sites web dédiés au partage d'images intimes distribuées sans consentement ou à la poursuite de contenus de violence sexuelle. Par exemple, une offre d'emploi à un poste de mannequin qui trompe les gens en leur faisant envoyer des images sexuelles d'eux-mêmes.
- v. **Sextorsion :** Un type d'extorsion qui se produit lorsqu'une personne possède ou prétend posséder une image sexuelle d'une autre personne et qu'elle l'utilise pour contraindre la cible à faire quelque chose qu'elle ne veut pas faire, ou pour exiger de l'argent, en menaçant la diffusion de ses images.
- vi. **Voyeurisme numérique (*creepshots*) :** À mesure que les gens passent du temps en ligne, ils commencent à se forger une réputation. Cette réputation est façonnée par leur comportement en ligne, incluant les sites web et applications qu'ils utilisent publiquement, ainsi que le contenu qu'ils choisissent de publier ou de partager.

Compte robot : Il s'agit d'un compte en ligne ou d'un profil de réseau social géré par un logiciel plutôt qu'un humain. Les robots peuvent automatiser des actions comme la publication, la messagerie ou l'interaction avec les utilisateurs. Certains jouent des rôles utiles, mais d'autres servent uniquement à l'envoi de pourriels, à la désinformation ou à la manipulation.

Consentement : Il s'agit d'un processus continu d'octroi et d'obtention de permission. Cela signifie qu'il y a un « oui » actif entre tous ceux qui sont capables de consentir authentiquement et légalement à ce qui se passe.

Contrôle coercitif : Un comportement ou une suite de comportements impliquant des agressions, des menaces, de l'humiliation, de l'intimidation ou d'autres formes de violence visant à nuire ou à punir une personne ou lui instiller la peur.

Cyberharcèlement de groupe : Type de harcèlement en ligne où plusieurs personnes ciblent collectivement une personne avec des insultes, des menaces ou des messages hostiles. Les attaques sont souvent coordonnées ou s'enchaînent, visant à submerger et à intimider la personne.

Cybermenace : Une déclaration d'intention d'infliger une douleur, une blessure ou un dommage à une personne, à sa famille ou à ses biens par l'utilisation de la technologie numérique.

Désinformation populaire planifiée : A Une tactique trompeuse qui cache les véritables partisans d'un message ou d'une campagne planifiée, qu'elle soit politique, commerciale, religieuse ou promotionnelle. L'objectif est de donner l'impression que le message est une contribution locale authentique et indépendante, plutôt que d'un effort secret ou commandité.

Discours haineux numérique : Toute communication textuelle (commentaires, publications, messages directs, emojis) ou médiatique (images, vidéos, animations, enregistrements vocaux, etc.) qui attaque et incite à la violence contre une personne ou un groupe en fonction de son identité. Cela inclut de cibler le genre, la race, l'origine ethnique, le handicap, la sexualité ou tout autre marqueur d'identité d'une personne.

Discrimination : Un comportement découlant d'attitudes préconçues adoptées par les individus ou les institutions, entraînant des disparités de traitement à l'égard des personnes perçues comme différentes.

Embrigadage de votes (*vote brigading*) : Ce terme décrit une action coordonnée visant à manipuler les résultats d'un sondage en ligne, ou d'un vote (comme voter sur les vidéos ou commentaires de façon positive ou négative), afin de modifier le résultat souhaité ou de mettre en valeur le contenu à davantage de personnes par la manipulation de nombreux algorithmes en ligne.

Harcèlement multiplateforme : Harcèlement coordonné et organisé contre une cible, par une ou plusieurs personnes, à travers différentes plateformes en ligne et de façon simultanée.

Morinommer (deadnaming) : Un type de harcèlement direct qui consiste à révéler l'ancien nom de quelqu'un contre sa volonté dans le but de causer du tort. On l'utilise souvent pour exposer les membres de la communauté 2ELGBTQIA+ qui se servent d'un nom différent de celui qu'ils utilisaient auparavant ou qui leur avait été donné à la naissance.

Personne bispirituelle, aux deux esprits ou 2E : Ce terme générique désigne les nombreux mots utilisés dans différentes langues autochtones pour affirmer l'interdépendance de multiples aspects de l'identité, notamment le genre, la sexualité, la communauté, la culture et la spiritualité. Certains Autochtones s'identifient comme personnes bispirituelles plutôt que, ou en plus de, s'identifier comme lesbiennes, gais, bisexuels, transgenres ou queer. L'étiquette identitaire de personne aux deux esprits est exclusive aux peuples autochtones. Une personne qui n'est pas d'origine autochtone ne devrait pas s'identifier avec ces termes.

Préjugé : Ce terme englobe des attitudes positives ou négatives envers une personne ou un groupe, formées sans fondements justes ou sans connaissances suffisantes, qui ne changeront probablement pas malgré de nouvelles preuves ou des arguments contraires. Souvent, les préjugés ne sont pas reconnus comme des hypothèses fausses ou des stéréotypes erronés, et, par la répétition, peuvent devenir acceptés comme des notions de bon sens.

Réputation en ligne : À mesure que les gens passent du temps en ligne, ils commencent à se forger une réputation. Cette réputation est façonnée par leur comportement en ligne, incluant les sites web et applications qu'ils utilisent publiquement, ainsi que le contenu qu'ils choisissent de publier ou de partager.

Trace numérique : Cela fait référence à l'ensemble de données que vous laissez derrière vous lorsque vous utilisez Internet (par exemple, l'historique ou le cache de navigation). Cela inclut les données générées par les sites web que vous visitez, les courriels que vous envoyez, les formulaires que vous remplissez ou les fichiers que vous téléchargez.

Transphobie : Une forme de discrimination où les personnes ont des attitudes, croyances, sentiments ou comportements négatifs envers les personnes bispirituelles, trans, non binaires, non conformes au genre et intersexes en raison de leur transidentité ou parce qu'elles sont perçues comme étant trans. La base sous-jacente de la transphobie est un rejet de la diversité de la sexualité humaine au-delà de deux genres fixes (c'est-à-dire la croyance en une binarité hétéronormative sexe/genre). Les personnes bispirituelles, transgenres et non binaires (2ETN+) font face à des formes distinctes de préjugés, entraînant des expériences de violence fondée sur le genre propres à ce groupe.

Violence fondée sur le genre : Se rapporte à des actes nuisibles dirigés contre une personne en raison de son genre ou de son identité de genre perçue. Elle est enracinée dans l'inégalité des genres, l'abus de pouvoir et des normes ancrées dans le patriarcat, le colonialisme et d'autres systèmes d'oppression.



RÉFÉRENCES

CAMBRIDGE DICTIONARY. « CYBER », signification anglaise, [https://dictionary.cambridge.org/dictionary/english/cyber] (Consulté le 21 août 2024).

DUNN, S. Technology-Facilitated Gender-Based Violence : An Overview, Faculté de droit Schulich de l'Université Dalhousie, 2020.

EQUAL VOICE. Modernizing Legislatures – What we heard Report, [https://www.equalvoice.ca/modernizing_legislatures/] (Juin 2023).

HOWARD, J. Online Hate and Cyberviolence, Fondation canadienne des femmes. [https://canadian-women.org/the-facts/online-hate-and-cyber-violence/] (consulté le 2 avril 2024).

KHOO, C., et LEAF. Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence, Executive Summary, [https://www.leaf.ca/publication/deplat-forming-misogyny/] (2021).

LA TROBE UNIVERSITY. Bystander Action: Technology-facilitated abuse, [https://www.latrobe.edu.au/mylatrobe/bystander-action-technology-facilitated-abuse/] (Consulté le 18 août 2021).

LEARNING NETWORK. Glossary, [https://gbvlearningnetwork.ca/our-work/glossary/index.html] (sans date).

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS. Reclaiming Power and Place: The Final Report of the National Inquiry Into Missing and Murdered Indigenous Women and Girls (Vol. 1a). [https://www.mmiwg-ffada.ca/wp-content/uploads/2019/06/Final_Report_Vol_1a-1.pdf] (2019)

RANEY, T., et COLLIER, C. N. Gender-Based Violence in Canadian Politics in the #MeToo Era, University of Toronto Press, 2024.

STATISTIQUE CANADA. Study: Online harms faced by youth and young adults: The prevalence and nature of cybervictimization, [https://www150.statcan.gc.ca/n1/daily-quotidien/230221/dq230221c-eng.html] (21 février 2023).

TECH SAFETY CANADA. Passwords: Simple Ways to Increase Your Security, [https://techsafety.ca/resources/toolkits/passwords-simple-ways-to-increase-your-security] (2024).

TECH SAFETY CANADA. 10 Easy Steps to Maximize Tech Use Privacy, [https://techsafety.ca/resources/toolkits/10-easy-steps-to-maximize-tech-use-privacy] (2024)

TECH SAFETY CANADA. Stalking and Technology-Facilitated Abuse Log, [https://techsafety.ca/resources/toolkits/stalking-and-technology-facilitated-abuse-log] (2024).

THE SAMARA CENTRE FOR DEMOCRACY, Online Abuse in Local Elections: The SAMbot Municipal Report, Toronto, [<https://www.samaracentre.ca/articles/sam-botmunicipal-elections-report/>] (2023).

UNITED NATIONS POPULATION FUND. Technology-facilitated Gender-based Violence: Making All Spaces Safe, [<https://www.unfpa.org/publications/technology-facilitated-gender-based-violence-making-all-spaces-safe/>] (Consulté le 1er décembre 2021).

UN WOMEN. FAQ : Tech-facilitated violence against women and girls. [<https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women>] (sans date).

VIPOND, E., SAIED, R., et DIETZEL, C. Navigating Digital Harms : An Investigation of Transphobic Online Hate Against 2SLGBTQIA+ Organizations, Open Digital Literacy and Access Network (ODLAN) and Wisdom2Action, p. 25, 2025.



Un guide conçu à l'Île-du-Prince-Édouard / Epekwitk pour comprendre et signaler la cyberviolence.

Ce guide pratique pour se protéger à l'ère numérique donne aux femmes et aux personnes de diverses identités de genre en position de leadership des stratégies pratiques, des ressources et du soutien pour s'orienter dans le monde de la cyberviolence et pour combattre les menaces numériques.

Si vous vivez de la cyberviolence, ou toute forme de violence facilitée par la technologie, vous n'êtes pas seule. Ensemble, nous pouvons travailler à rehausser la sécurité de l'utilisation d'Internet et des technologies pour toutes et tous.

Vous pouvez télécharger un PDF du présent guide sur notre site web :



**Coalition pour
le Leadership des
Femmes de l'Î.-P.-É.**