Maltraitance facilitée par la technologie.

Un guide TELUS Averti® pour les adultes de tous âges.



La présente ressource se veut un complément, et non un substitut à un soutien professionnel offert par des conseillers juridiques en matière de droits des victimes de violence conjugale.
Si vous êtes en danger immédiat, faites le 9-1-1.

TELUS MD Averti

© TELUS 2026. 26-0872

Table des matières

Qu'est-ce que la maltraitance facilitée par la technologie? 1

Pourquoi la technologie facilite-t-elle la maltraitance? 1

Personnes touchées 1

Le cercle de contrôle et de pouvoir 2

Signes avant-coureurs de maltraitance facilitée par la technologie 3

S'agit-il vraiment d'un cas de maltraitance? 4

Types de maltraitance facilitée par la technologie 5

Surveillance et logiciels traqueurs 5

GPS et suivi de la position 5

Maltraitance liée à une image (images intimes non consensuelles) 6

Domotique et Internet des objets (IdO) 6

Cyberharcèlement et cybertraque 7

Maltraitance financière en ligne 7

Planifier sa sécurité 8

Effacer vos traces numériques 8

Liste de vérification de sécurité rapide 9

Obtenir de l'aide 10

Lignes d'aide et de soutien 10

Organismes et ressources 10

Ce guide a été créé en collaboration avec The Today Family Violence Help Centre, dont l'expertise, les conseils et les données ont contribué à façonner cette ressource.

Qu’est-ce que la maltraitance facilitée par la technologie?

Il y a maltraitance facilitée par la technologie lorsque quelqu’un utilise une technologie numérique comme outil pour surveiller, contrôler, harceler, intimider ou blesser une autre personne.

La technologie en soi n’est pas le problème. Les malfaiteurs utilisent les appareils, les applications, les téléphones intelligents, les dispositifs de domotique, les médias sociaux, les GPS et autres pour exercer leur pouvoir et leur contrôle au-delà des lieux physiques.

La maltraitance facilitée par la technologie n’est pas une forme distincte de maltraitance, c’est une tactique utilisée dans un modèle plus large de contrôle coercitif. Elle accompagne souvent la maltraitance physique, émotionnelle, financière et sexuelle.

Pourquoi la technologie facilite-t-elle la maltraitance?

- La technologie est intégrée à tous les aspects de la vie quotidienne, à la maison, au travail et dans les relations sociales.
- De nombreux outils de surveillance sont présentés comme des applications de sécurité familiale, ce qui permet de déguiser facilement la maltraitance
- Les malfaiteurs peuvent surveiller leurs victimes à distance, en temps réel, en tout temps.
- Les preuves numériques de maltraitance peuvent être difficiles à documenter et faciles à supprimer.
- Les victimes ne reconnaissent pas toujours les tactiques fondées sur la technologie comme de la maltraitance.
- Le fait de quitter un malfaiteur ne met pas automatiquement fin à la maltraitance facilitée par la technologie. La situation peut même s’aggraver après la fin de la relation.

Personnes touchées

Il peut y avoir de la maltraitance facilitée par la technologie dans n’importe quelle relation, peu importe le sexe, l’âge, l’orientation sexuelle ou les antécédents. Cela dit, elle est davantage fréquente dans les situations suivantes :

- Relations intimes avec un partenaire (actuel ou ancien)
- Relations familiales (parents, frères et sœurs, enfants adultes)
- Situations où une personne contrôle des comptes ou des appareils partagés
- Relations où un déséquilibre du pouvoir important existe

Selon une recherche du gouvernement du Canada, la maltraitance facilitée par la technologie touche de manière disproportionnée les femmes, les personnes 2ELGBTQ+, les immigrants, les personnes handicapées et les Autochtones, bien que tout le monde puisse en être victime.

Les jeunes sont aussi particulièrement à risque. Dans le monde numérique où ils grandissent, le partage de l'emplacement et des renseignements personnels ainsi que le partage des mots de passe et de l'accès aux médias sociaux entre pairs est la norme. Il peut donc être plus difficile de reconnaître les risques associés à ces comportements.

Le cercle de contrôle et de pouvoir

Tout comme le modèle Duluth, un cadre fondamental pour la sensibilisation et l'intervention en matière de violence familiale, décrit les tactiques de maltraitance physique et émotionnelle. La maltraitance facilitée par la technologie s'inscrit dans le même cadre de pouvoir et de contrôle :

Surveillance : suivi de la position, lecture des messages, surveillance des appels

Isolement : blocage des contacts, contrôle de l'accès aux appareils

Intimidation : menace de partager des images ou des renseignements privés

Contrôle économique : contrôle des transactions bancaires en ligne, des comptes partagés ou des comptes professionnels

Coercition : obtention forcée de mots de passe et du partage de l'emplacement

Minimiser et nier : « Je ne fais que veiller à ta sécurité » et « Tu es paranoïaque. »



Les prochaines sections explorent comment ces tactiques se manifestent au moyen de technologies numériques précises.

Signes avant-coureurs de maltraitance facilitée par la technologie

Vous pourriez être victime de maltraitance facilitée par la technologie si votre partenaire ou un membre de votre famille commet un des actes suivants :

Suivre votre position : La personne sait constamment où vous vous trouvez sans que vous le lui disiez, et elle exige que vous partagiez votre position en tout temps.

Exiger des mots de passe : La personne insiste pour avoir tous vos mots de passe, NIP et accès à des comptes, et elle se fâche si vous les changez.

Surveiller vos messages : La personne lit vos textos, courriels et messages sur les médias sociaux, et elle demande de voir votre téléphone en tout temps.

Menacer : La personne menace de partager des images intimes de vous sans votre consentement.

Contrôler les dispositifs de domotique : La personne utilise des serrures, caméras, thermostats ou haut-parleurs intelligents pour surveiller ou contrôler votre environnement.

Contrôler les comptes en ligne : La personne gère vos courriels, vos médias sociaux ou vos comptes bancaires; elle vous empêche d'accéder à vos propres comptes; elle accède aux comptes de votre travail pour entacher votre réputation auprès de vos collègues ou nuire à votre travail dans le but de vous faire licencier (une forme de contrôle économique). Elle peut aussi utiliser l'accès pour mener des activités illégales, faire du chantage ou vous rendre coupable d'un crime.

Accéder aux renseignements personnels : La personne accède à des dossiers médicaux en ligne, à des dossiers de l'Agence du revenu du Canada ou à d'autres documents sensibles aux fins de surveillance ou d'intimidation.

Procéder à des enregistrements sans votre consentement : La personne enregistre vos conversations, prend des photos ou des vidéos de vous sans votre autorisation, ou installe un logiciel espion.

Vous isoler en ligne : La personne bloque vos contacts, contrôle les personnes que vous pouvez suivre ou à qui vous pouvez parler, ou publie des choses qui portent atteinte à votre réputation.

Contrôler les finances : La personne contrôle les transactions bancaires en ligne, les virements électroniques ou elle vous empêche d'accéder à vos fonds par des moyens numériques.

Créer de la peur et de l'anxiété : Vous vous sentez anxieux d'utiliser votre téléphone ou vos appareils, et vous vous censurez par peur de faire l'objet d'une surveillance.

Continuer après la cessation d'emploi : La personne continue le harcèlement, la surveillance ou les menaces par des moyens technologiques même après la fin de la relation.

Créer de faux profils : La personne crée de faux comptes pour vous surveiller, se faire passer pour vous ou communiquer avec vos proches.

S’agit-il vraiment d’un cas de maltraitance?

Les malfaiteurs décrivent souvent la surveillance technologique comme nécessaire pour assurer la sécurité ou la santé. Posez-vous les questions suivantes :

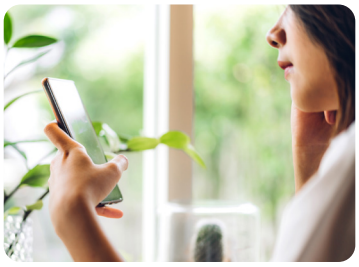
- L’utilisation de mes appareils est-elle une source de peur ou d’anxiété?
- Dois-je cacher à qui je parle ou ce que je fais en ligne?
- Ai-je consenti à cette surveillance, ou l’a-t-on exigée?
- Mon partenaire utilise-t-il les renseignements de mes appareils pour me punir ou me contrôler?
- Mon partenaire serait-il en colère si je changeais de mot de passe ou si je désactivais la fonction de partage de l’emplacement?

N’OUBLIEZ PAS que les relations saines sont fondées sur la confiance et le respect mutuel, et non sur la surveillance. Vous avez droit au respect de votre vie privée, même dans une relation.



Types de maltraitance facilitée par la technologie

1. Surveillance et logiciels traqueurs



De quoi s'agit-il? Un logiciel installé secrètement sur votre appareil pour surveiller les appels, les textos, l'emplacement, les photos et l'activité dans les applications à votre insu.

Signes que votre appareil pourrait avoir été compromis :

- La pile s'épuise anormalement vite
- Le téléphone reste chaud même lorsqu'il n'est pas utilisé
- L'utilisation de données est plus élevée que prévu
- Votre partenaire sait des choses que vous ne lui avez jamais dites
- L'appareil est lent ou se comporte de manière étrange

MISE EN GARDE : Ne supprimez PAS le logiciel traqueur sans avoir d'abord parlé à un conseiller juridique en matière de droits des victimes de violence conjugale. Si vous le supprimez, vous alerterez le malfaiteur et vous augmenterez vos risques de violence. Un conseiller juridique peut vous aider à planifier des stratégies de retrait sécuritaires sans détection.

2. GPS et suivi de la position

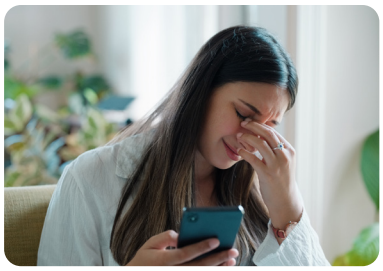


De quoi s'agit-il? L'utilisation d'applications, d'appareils ou de dispositifs GPS cachés pour surveiller votre emplacement physique.

Méthodes courantes :

- Partage d'emplacement intégré au téléphone (partage par Localiser mon iPhone et Google Maps)
- Fonctions de localisation avec partage familial
- Dispositifs GPS dissimulés dans des véhicules, des sacs ou des effets personnels
- Applications pour voiture intelligentes qui recueillent des données sur la conduite
- AirTags ou vignettes de suivi dissimulées sans consentement
- Appareils et applications pour enfants avec fonctions de partage de l'emplacement
- Colliers et dispositifs de suivi des animaux de compagnie avec fonctions de localisation

3. Maltraitance liée à une image (images intimes non consensuelles)



De quoi s'agit-il : Cela consiste à prendre ou à partager des images intimes ou à menacer de les partager sans consentement, aussi parfois appelé « pornodivulgation ».

Exemples :

- Partager ou menacer de partager des images intimes avec la famille, les employeurs ou publiquement
- Enregistrer une activité sexuelle sans consentement
- Utiliser des images comme chantage pour contrôler un comportement
- Créer des images hypertruquées créées à l'aide de l'IA

C'est un crime au Canada. Le partage non consensuel d'images intimes est illégal en vertu du Code criminel du Canada. Vous pouvez signaler le cas à la police.

4. Domotique et Internet des objets (IdO)



De quoi s'agit-il? L'utilisation de dispositifs connectés à la maison pour surveiller, contrôler ou intimider.

Exemples :

- Serrures intelligentes : verrouiller et déverrouiller les portes à distance pour contrôler les déplacements
- Caméras intelligentes : surveiller l'intérieur de la maison
- Haut-parleurs intelligents : écouter les conversations
- Thermostats : contrôler la température comme punition
- Interphones de surveillance de bébé : espionner les victimes
- Sonnettes intelligentes : surveiller la présence de visiteurs

CONSEIL: Avant de partir, vérifiez tous vos dispositifs de domotique. Modifiez vos mots de passe et supprimez les accès partagés de tous vos comptes avant de partir et même après.

5. Cyberharcèlement et cybertraque



De quoi s'agit-il? L'utilisation de plateformes numériques pour harceler, intimider ou contrôler.

Exemples :

- Envoyer à répétition des messages menaçants ou agressifs
- Créer de faux profils pour vous surveiller ou usurper votre identité
- Créer de faux échanges de textos ou de courriels et des hypertrucages générés par l'IA pour vous inculper ou manipuler des actions en justice
- Publier en ligne des renseignements inexacts ou préjudiciables à votre sujet
- Communiquer en ligne avec vos amis, votre famille ou votre employeur
- Vous inonder d'appels, de textos ou de courriels
- Pirater vos comptes

C'est un crime au Canada. En savoir plus sur les lois sur le harcèlement criminel.

6. Maltraitance financière en ligne



De quoi s'agit-il? L'utilisation de la technologie pour contrôler ou restreindre l'accès à l'argent.

Exemples :

- Contrôler l'accès aux services bancaires en ligne
- Surveiller les achats et les transactions
- Vous empêcher de créer vos propres comptes
- Contracter des dettes en votre nom en utilisant votre identité numérique
- Contrôler de la cryptomonnaie ou des actifs numériques
- Accéder aux documents juridiques et financiers confidentiels ou les contrôler (déclarations de revenus, hypothèques, prêts, assurances, testaments, placements)

Planifier sa sécurité

Votre sécurité est primordiale. Avant d'apporter des changements à des dispositifs ou à des comptes, veuillez communiquer avec un conseiller juridique en matière de droits des victimes de violence conjugale. Certaines actions, comme supprimer un logiciel espion ou modifier un mot de passe, peuvent alerter un malfaiteur et augmenter le danger.

Important : La planification de la sécurité devrait toujours être effectuée avec le soutien d'un conseiller formé qui comprend la maltraitance facilitée par la technologie. Les étapes ci-dessous sont fournies à titre d'exemple seulement. Bien que ces mesures puissent améliorer votre sécurité, elles ne peuvent pas éliminer les risques. La planification de la sécurité est une stratégie de réduction des risques, et il n'y a pas un plan qui convient à tout le monde.

Effacer vos traces numériques

Si vous devez chercher de l'aide sur un appareil partagé ou surveillé :

- Naviguez en mode privé ou incognito (Ctrl+Maj+N ou Commande+Maj+N)
- Effacez l'historique de votre navigateur après chaque session
- Utilisez un réseau privé virtuel (RPV) si possible
- Utilisez un ordinateur d'une bibliothèque ou l'appareil d'un ami
- Effectuez des recherches avec le moteur de recherche DuckDuckGo; il n'enregistre pas l'historique des recherches
- Appelez une ligne d'aide depuis un téléphone public ou celui d'un ami si vous en ressentez le besoin

Remarque : Le mode de navigation privée n'empêche pas votre fournisseur d'accès Internet ou un logiciel de surveillance installé sur votre appareil de consulter vos activités.

Étape 1 : Utiliser un appareil fiable

Si possible, utilisez un appareil auquel le malfaiteur n'a pas accès – le téléphone d'un ami, l'ordinateur d'une bibliothèque ou un nouveau téléphone prépayé – pour faire des recherches et établir des communications confidentielles. Demandez à un organisme de lutte contre la violence familiale de vous fournir un téléphone fiable. Certains organismes offrent des téléphones prépayés.

Étape 2 : Vérifier la présence d'applications de suivi

Demandez à un conseiller ou à une personne de confiance qui s'y connaît en technologie de vous aider à vérifier la présence d'un logiciel traqueur sur votre appareil. Ne le supprimez pas sans aide, car cela pourrait alerter le malfaiteur. Pour en savoir plus, consultez Ressource HabiloMédias pour protéger vos appareils.

Étape 3 : Protéger vos comptes

Si vous pouvez le faire en toute sécurité, changez les mots de passe sur un appareil fiable, activez l'authentification à deux facteurs pour les numéros ou les adresses de courriel auxquels votre malfaiteur n'a pas accès, et examinez les options de récupération de compte.

Étape 4 : Examiner le partage de l'emplacement

Vérifiez les paramètres du partage de l'emplacement de toutes les applications. Cherchez des AirTags ou des dispositifs GPS dans votre véhicule, vos bagages ou vos effets personnels.

Étape 5 : Documenter la maltraitance

Faites des saisies d'écran des messages menaçants, conservez les enregistrements d'appels et notez les dates et heures des incidents. Conservez les preuves sur un appareil fiable ou auprès d'une personne de confiance.

Étape 6 : Ajuster la protection de la vie privée sur les réseaux sociaux

Passez en revue les paramètres de confidentialité sur toutes les plateformes de médias sociaux. Pensez à rendre vos comptes privés, à retirer les balises de localisation des publications et à bloquer le malfaiteur sur toutes les plateformes.

Étape 7 : Dispositifs de domotique

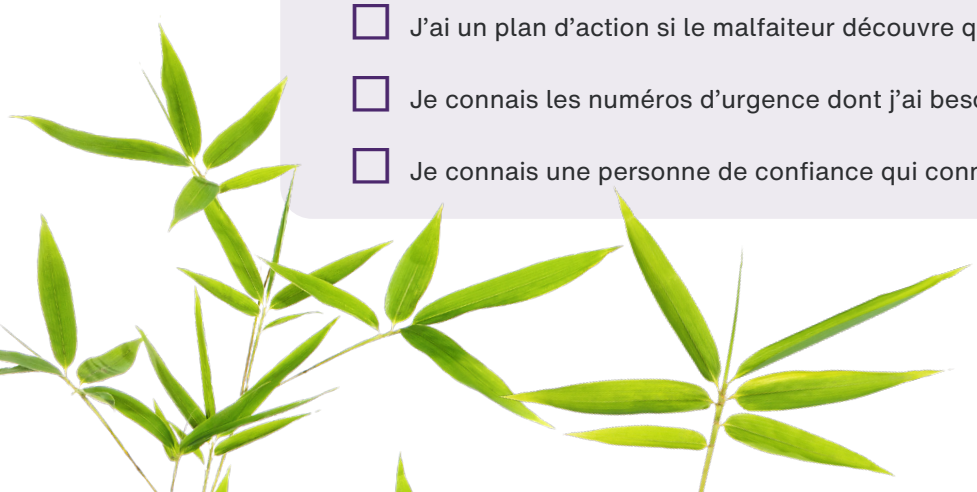
Si vous êtes en mesure de le faire après le départ : changez tous les mots de passe des dispositifs de domotique, supprimez les accès du malfaiteur à toutes les applications et envisagez de réinitialiser les dispositifs aux paramètres d'usine.

Étape 8 : Créer une nouvelle adresse de courriel

Configurez un nouveau compte de courriel sur un appareil fiable pour communiquer avec les refuges, les avocats et les services d'aide. N'y accédez pas à partir d'un appareil que le malfaiteur peut surveiller.

Liste de vérification de sécurité rapide

- ☐ J'ai accès à un appareil fiable pour les communications confidentielles
- ☐ J'ai parlé à un conseilleur juridique en matière de droits des victimes de violence familiale à propos de ma sécurité technologique
- ☐ Je sais comment effacer l'historique de mon navigateur au besoin
- ☐ J'ai documenté les preuves de maltraitance facilitée par la technologie
- ☐ J'ai un plan d'action si le malfaiteur découvre que j'ai besoin d'aide
- ☐ Je connais les numéros d'urgence dont j'ai besoin (police, refuge, ligne d'aide)
- ☐ Je connais une personne de confiance qui connaît ma situation



La technologie numérique est-elle nouvelle pour vous?

Notre série de vidéos Techno 101 de TELUS Averti couvre tout ce que vous devez savoir, de la connexion à Internet à la protection de vos appareils et de vos comptes, en passant par les mots de passe, les paramètres de confidentialité et la sécurité dans les médias sociaux.

Pour en savoir plus, visitez telus.com/**Techno101Averti**

Obtenir de l'aide

Entourez-vous de proches. Voici des organismes de confiance et des ressources qui peuvent vous aidez.

Lignes d'aide et de soutien

- Ontario : Ligne de soutien pour femmes violentées : 1-866-863-0511 (24/7, plus de 200 langues)
- Alberta : Ligne d'information contre la violence familiale : 1-780-310-1818 ou 310-1818 par texto
- Colombie-Britannique : VictimLinkBC : 1-800-563-0808 (en tout temps)
- Partout au pays : Composez le 211. Offert dans la plupart des provinces, ce service vous met en contact avec des services communautaires, sociaux et gouvernementaux, y compris du soutien pour les hommes victimes de maltraitance.

Organismes et ressources

- L'association canadienne contre la violence sexuelle
- Fondation canadienne des femmes
- Centre canadien pour l'autonomisation des femmes
- Pour les survivantes – Sécurité technologique Canada
- Stalking and Technology-Facilitated Abuse Log - TechSafety
- Reprends ton espace numérique
- Security in a box
- Technology Safety – New Beginnings
- Resources-Survivors — Safety Net Project
- Ressources du programme à l'intention des survivantes de HabiloMédias