



Manuel sur les violences numériques

Votre guide pour plus de sécurité numérique

Si la technologie facilite de nombreux aspects du quotidien, elle est aussi de plus en plus utilisée par les auteurs d'abus pour exercer un contrôle ou causer du tort. Certaines formes de violences technologiques sont évidentes, tandis que d'autres sont plus discrètes, dissimulées dans les paramètres des applications ou dans des connexions invisibles entre les appareils, les comptes en ligne ou les services. Ce guide vous aide à reprendre le contrôle. Il n'a pas vocation à couvrir toutes les situations, mais il se concentre sur des mesures simples qui peuvent réellement faire la différence.

Si vous ne comprenez pas certaines parties du guide, demandez de l'aide à une personne de confiance à l'aise avec les technologies ou à des spécialistes. Vous n'avez pas besoin de tout faire en une seule fois, et vous n'avez pas à faire cela sans aide. Si vous êtes dans une relation marquée par des violences physiques, adressez-vous d'abord à un centre d'aide aux victimes, car prendre des mesures techniques peut vous exposer à un plus grand danger.



Votre sécurité numérique

Les bases

Quelques mesures simples peuvent vous aider à protéger vos comptes en ligne et votre vie privée.

Protection des comptes

Passez en revue vos comptes les plus importants un par un, notamment messagerie électronique, réseaux sociaux, compte Google ou identifiant Apple, services bancaires en ligne, comptes d'achat en ligne, applications de santé et de sport, services de stockage dans le cloud, services de streaming (par ex. Netflix) et appareils connectés à la maison.

Lorsque c'est possible et sans risque, vous pouvez remplacer vos comptes existants par de nouveaux comptes, indépendants des précédents.

Nouvelle adresse e-mail et nouveaux comptes

Créez une nouvelle adresse e-mail à laquelle seulement vous avez accès. Des services comme ProtonMail, gratuits, permettent de créer un compte sans fournir d'informations personnelles ni de numéro de téléphone. Vous pouvez utiliser cette nouvelle adresse e-mail pour créer de manière sécurisée vos autres comptes, par exemple réseaux sociaux services bancaires en ligne.

Mots de passe robustes

Utilisez de nouveaux mots de passe difficiles à deviner, par exemple en combinant trois mots choisis au hasard, comme « TasseJardinJaune », ainsi que des caractères spéciaux et des chiffres.

Sur les appareils auxquels seulement vous avez accès, vous pouvez utiliser un gestionnaire de mots de passe gratuit, comme Bitwarden, pour générer et enregistrer un mot de passe unique pour chacun de vos comptes.



Protection de vos comptes existants

Au lieu de créer de nouveaux comptes, vous pouvez également vérifier les paramètres de vos comptes existants. Sachez que la modification de certains paramètres, comme l'adresse e-mail ou le numéro de téléphone de récupération, peut entraîner l'envoi d'une notification aux anciennes coordonnées. Si une autre personne y a accès, elle pourrait être informée de vos actions. N'effectuez les modifications suivantes que si vous estimez pouvoir le faire en toute sécurité.

- Remplacez vos mots de passe par de nouveaux mots de passe robustes.
- Définissez une nouvelle adresse e-mail sécurisée comme adresse e-mail du compte ou de récupération.
- Supprimez tout numéro de téléphone, y compris de récupération, que vous ne contrôlez pas entièrement.

Authentification à deux facteurs (2FA)

Pour renforcer la sécurité, activez l'authentification à deux facteurs. Même si une autre personne connaît votre mot de passe, elle ne pourra pas se connecter à un compte protégé par la 2FA sans avoir accès à votre téléphone. La première étape est d'installer une application comme Google Authenticator, Microsoft Authenticator ou Authy.

- Modifiez les questions de sécurité en utilisant des réponses que personne ne connaît; vous pouvez même utiliser de fausses réponses si cela vous semble plus sûr.
- Déconnectez toutes les sessions actives et tous les appareils, pas seulement celui que vous utilisez, afin d'empêcher l'accès à vos comptes depuis un autre appareil ou emplacement.
- Déconnectez tout compte connecté susceptible de permettre à une autre personne d'y accéder à votre insu.

Protection de la vie privée

Les mesures suivantes peuvent vous aider à empêcher que vos informations personnelles soient utilisées pour vous localiser, vous surveiller ou vous nuire.



Vérifiez les paramètres de confidentialité

De nombreuses applications peuvent révéler davantage d'informations sur vous que vous ne le pensez. Passez en revue vos comptes et modifiez les paramètres qui déterminent qui peut voir votre profil, vos photos et vos publications. Réglez les paramètres afin que votre statut « dernière connexion » ou votre localisation ne soient pas visibles. Vous pouvez généralement choisir des options telles que « Moi uniquement » ou « Privé ».

Partage prudent des informations

Évitez de publier des informations sur les réseaux sociaux ou dans votre statut WhatsApp. Envisagez de supprimer les anciennes publications ou photos qui révèlent votre localisation, vos habitudes ou vos relations. Demandez à vos proches de ne pas publier de photos de vous,

de ne pas vous identifier dans des publications et de ne pas mentionner votre localisation en ligne.

Désactivation des comptes

Si nécessaire, désactivez vos comptes, puis désinstallez les applications concernées afin de réduire les risques d'accès ou d'utilisation indésirables.

Recherchez vos informations en ligne

Recherchez votre nom et votre nom d'utilisateur sur des moteurs de recherche comme Google afin de voir quelles informations apparaissent. Vous pouvez effectuer une recherche sur Google à partir de vos photos pour vérifier si elles sont utilisées sans votre autorisation. Si vous trouvez un contenu qui ne devrait pas être en ligne, vous pouvez le signaler à la plateforme concernée et demander sa suppression.

Pour les parents

Les comptes et appareils de vos enfants, par exemple les tablettes, Xbox ou Nintendo Switch, peuvent être détournés pour les localiser, les surveiller ou leur nuire. Les protéger contribue à renforcer la sécurité en ligne de votre enfant comme la vôtre.

Appliquez les mesures générales de protection des comptes et de la vie privée

Les mêmes mesures de protection que celles utilisées pour vos propres comptes, comme des mots de passe robustes, des options de récupération sécurisées et des paramètres de confidentialité stricts, peuvent être appliquées aux comptes et appareils de votre enfant.

Vérifiez les listes de contacts et les conversations

Passez en revue avec votre enfant ses contacts dans les applications et les jeux. Supprimez les contacts non identifiés et désactivez les fonctionnalités permettant à des personnes inconnues de lui envoyer des messages.

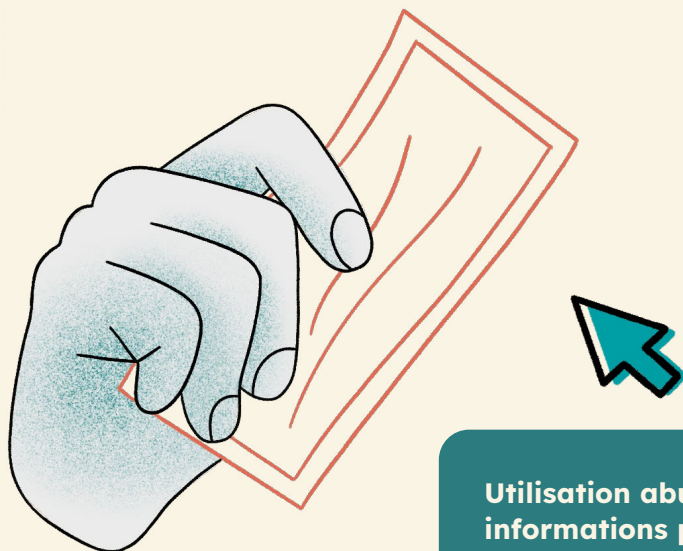
Désactivez le partage de localisation

De nombreuses applications et de nombreux jeux permettent le partage de localisation. Désactivez ces fonctionnalités afin d'empêcher qu'une autre personne puisse suivre les déplacements de votre enfant.

Recherchez les comptes supplémentaires sur les appareils

Sur les tablettes et les consoles de jeux, vérifiez s'il existe des comptes « famille », « invité » ou administrateur que vous n'avez pas créés. Supprimez tout compte susceptible de permettre à une autre personne d'accéder à l'appareil à votre insu.

Violence économique



Exemples de risques

Vous empêcher d'accéder à votre argent

Une personne vous empêche d'utiliser votre propre compte bancaire, vos cartes ou vos applications financières, ou détourne des sommes qui vous sont destinées, comme des prestations sociales ou une pension alimentaire, afin que vous ne puissiez pas y accéder.

Utilisation abusive de vos informations personnelles

Vos informations personnelles sont utilisées sans votre consentement, par exemple pour demander un crédit, percevoir des prestations ou souscrire des services en votre nom. Cela peut entraîner des problèmes juridiques ou financiers à long terme.

Surveillance de vos dépenses

Chacune de vos transactions est surveillée : la façon dont vous dépensez votre argent peut faire l'objet de questions, de jugement, voire de punition, quel que soit le montant.

Comment vous protéger

- Ouvrez un nouveau compte bancaire à votre seul nom afin d'empêcher l'accès à vos ressources financières par l'intermédiaire d'un compte joint, de liens familiaux ou de relations juridiques comme le mariage.
- Activez les alertes de transaction dans les paramètres de votre banque en ligne, généralement dans les rubriques « notifications » ou « alertes de sécurité », afin de surveiller en temps réel toute activité sur votre compte.
- Consultez régulièrement vos relevés de compte afin de repérer toute transaction inconnue ou suspecte.
- Surveillez vos informations de crédit et vos données financières afin de repérer tout prêt, toute carte de crédit ou tout autre engagement financier souscrit à votre nom à votre insu.
- Contactez le service d'assistance de votre banque si vous repérez quoi que ce soit de préoccupant.

Ressources complémentaires

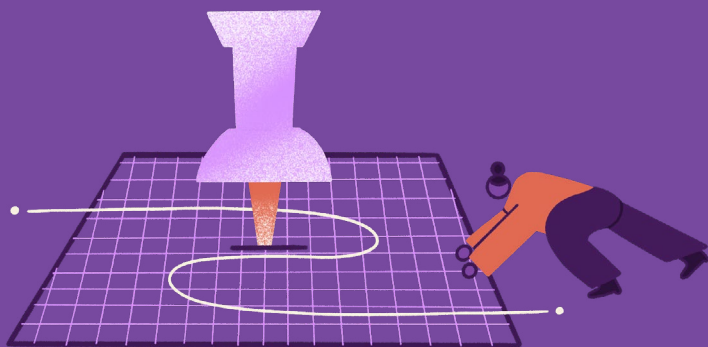
**Indicateurs
de violence
économique et
conseils**



**Informations
et conseils de
digital-violence.
info**



« Il ne s'agissait pas seulement d'argent; il s'agissait de contrôle, de me rendre totalement dépendant. »



Suivi de localisation

Exemples de risques

Logiciels espions

Des applications cachées peuvent être installées sur votre téléphone, votre tablette ou votre ordinateur. Elles peuvent permettre à une autre personne de suivre votre localisation, d'accéder à votre caméra ou à votre microphone, de voir ce qui s'affiche sur votre écran ou d'enregistrer ce que vous saisissez, y compris vos mots de passe.

Dispositifs de localisation cachés

De petits dispositifs de localisation, comme des AirTags ou des balises Bluetooth, peuvent être glissés dans des sacs ou des poches, ou dissimulés dans votre voiture.

Utilisation abusive des applications de localisation

Des applications légitimes comme « Localiser », Google Maps, Snapchat ou même des applications de sport peuvent être utilisées pour suivre vos déplacements, souvent par l'intermédiaire de comptes partagés ou connectés, ou de paramètres dont vous ignoriez l'activation.

Surveillance à domicile au moyen d'appareils connectés

Les appareils connectés de la maison, comme les sonnettes avec caméra, les enceintes connectées ou même votre routeur Wi-Fi, peuvent être utilisés pour surveiller vos heures de présence à domicile et savoir qui vous rend visite.

Comment vous protéger

- Désactivez les services de localisation pour toute application qui n'en a pas absolument besoin, depuis les paramètres de confidentialité ou les réglages de votre téléphone.
- Vérifiez dans des applications comme « Localiser », Google Maps, Snapchat ou les applications de suivi d'activité si l'historique de localisation ou le partage de position en temps réel sont activés, et désactivez ces fonctionnalités.
- Recherchez la présence éventuelle de logiciels espions. Sur Android, vous pouvez utiliser des applications comme Incognito Spyware Detector ; sur iOS, effectuez un contrôle de sécurité dans Réglages -> Confidentialité et sécurité afin de vérifier qui a accès à vos informations.
- Inspectez physiquement votre sac, votre manteau, votre voiture et vos objets personnels, comme les peluches ou les porte-clés, afin de repérer d'éventuels dispositifs de localisation cachés.

En cas de doute, demandez à un garagiste de confiance de vérifier si votre voiture contient un dispositif de suivi.

- Pour détecter des AirTags Apple, utilisez l'application « Localiser » sur iPhone ou téléchargez l'application gratuite Tracker Detect sur Android afin de rechercher les dispositifs de localisation à proximité qui ne sont pas enregistrés à votre nom.

Ressources complémentaires

Contrôle de sécurité (iOS)



Contrôle de sécurité (Android)



Réglages de localisation (iOS)



Réglages de localisation (Android)

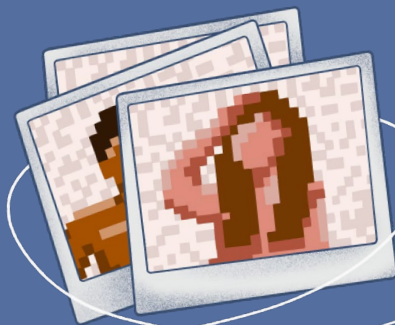


Application de détection des dispositifs de suivi



« Un AirTag a été caché dans le sac à dos de mon enfant et un autre dans ma voiture. C'est comme si nous ne pouvions aller nulle part sans être suivis. »

Images et vidéos intimes



« Il m'a forcée à envoyer des photos, puis il les a partagées sans mon consentement. Et maintenant, avec l'IA, il est même possible d'en créer de fausses. C'est comme si mon propre corps ne m'appartenait plus. »

Exemples de risques

Subir des pressions pour envoyer des images intimes

Une personne peut vous forcer, vous manipuler ou vous menacer afin que vous envoyiez des images ou des vidéos intimes.

Partage non consenti avec d'autres personnes

Des images intimes de vous sont diffusées, publiées en ligne ou montrées à d'autres personnes sans votre consentement.

Images fausses ou générées par l'IA

Une personne utilise des outils d'IA pour créer de faux contenus sexuels ou manipulés à partir de votre visage ou de votre corps, afin de vous humilier, de se faire passer pour vous ou de vous faire accuser à tort.

Chantage

Une personne menace de diffuser des images intimes de vous si vous ne faites pas ce qu'elle exige.

Comment vous protéger

- Signalez tout partage non consenti d'images intimes à l'aide d'outils comme StopNCII.org, ainsi que des fonctions de signalement proposées par les réseaux sociaux et les moteurs de recherche.
- Vous pouvez également créer un dossier de manière préventive sur StopNCII.org. Ce service vous permet de transmettre de manière sécurisée des empreintes numériques de vos images intimes afin que les plateformes puissent les bloquer avant même qu'elles ne soient diffusées en ligne.
- Conservez toute preuve de menaces ou d'abus fondés sur des images, au cas où vous auriez besoin de les signaler ultérieurement à la police ou à une plateforme. Pour les cas impliquant des personnes mineures, consultez clickandstop.ch pour obtenir des conseils.
- Si des images de vous générées par l'IA (« deepfakes ») apparaissent en ligne, signalez-les comme des violences basées sur l'image. En Suisse, de telles images peuvent porter atteinte à vos droits de la personnalité et, selon leur contenu et les circonstances, peuvent également relever du droit pénal.
- Évitez de créer ou de partager de nouvelles images ou vidéos intimes.

Ressources complémentaires

— Signalement d'images ou de vidéos (moins de 18 ans). —

**Signalement
d'images ou de
vidéos**



**Signalement
d'URL et
conseils**



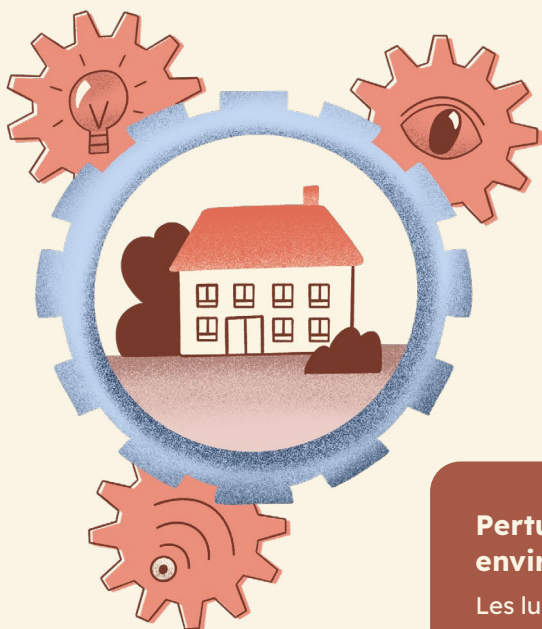
**Dépôt d'une
plainte pénale**



**Empêcher la
diffusion sur les
plateformes en
ligne**



Maison connectée



Exemples de risques

Ne pas pouvoir entrer ou sortir de chez soi

Une personne utilise des serrures connectées ou des systèmes d'alarme pour vous empêcher d'entrer chez vous ou de quitter votre domicile.

Perturbation de votre environnement domestique

Les lumières, téléviseurs, enceintes, systèmes de chauffage ou autres appareils peuvent être allumés, éteints ou manipulés à distance afin de vous désorienter, de vous effrayer ou de vous mettre mal à l'aise.

Faire l'objet d'une surveillance ou d'une écoute

Des enceintes connectées, des caméras ou des microphones cachés sont utilisés pour écouter secrètement vos conversations ou surveiller ce que vous faites chez vous.

Comment vous protéger

- Supprimez l'accès de l'auteur des violences en supprimant ses comptes utilisateur ou ses sessions actives dans les applications de maison connectée comme Amazon Alexa, Google Home, Apple HomeKit (app Maison), Ring, Nest, SmartThings ou Hue.
- Utilisez une application gratuite d'analyse du réseau, comme Fing, pour voir tous les appareils connectés à votre Wi-Fi. Cela peut aider à repérer des caméras, des microphones ou des dispositifs de suivi dissimulés.
- Recherchez les appareils Bluetooth à proximité dans les réglages Bluetooth de votre téléphone afin de repérer tout appareil suspect susceptible de vous suivre ou d'écouter ce qui se passe autour de vous.
- Modifiez le mot de passe de votre Wi-Fi afin d'empêcher les appareils configurés par l'auteur des violences de rester connectés. Vous pouvez généralement le faire en vous connectant à l'interface d'administration de votre routeur ou point d'accès Wi-Fi.
- Réinitialisez tous les appareils connectés, comme les caméras, thermostats, compteurs intelligents ou serrures numériques, à leurs paramètres d'usine, ou débranchez-les complètement si vous n'en avez pas réellement besoin.

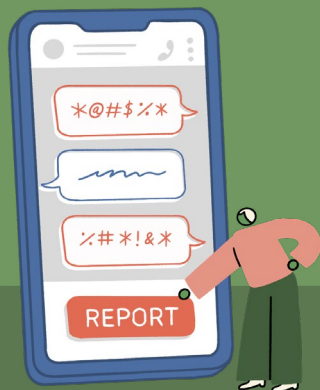
« Ma maison connectée était devenue un piège. Il m'empêchait d'y entrer, modifiait le chauffage, et je savais que les caméras me surveillaient et m'écoutaient en permanence. J'avais l'impression que ma propre maison m'espionnait. »

Ressources complémentaires

Informations et conseils de digital-violence.info



Applications de messagerie et réseaux sociaux



Exemples de risques

Contrôle par le biais de la messagerie

Vous pouvez subir des pressions pour donner constamment des nouvelles ou répondre immédiatement, ou vos messages peuvent être utilisés contre vous dans des conversations de groupe afin de provoquer des conflits ou de vous isoler des autres.

Surveillance de votre vie en ligne

Une personne peut surveiller votre statut « dernière connexion », suivre de manière obsessionnelle vos publications ainsi que vos listes de followers, voire surveiller vos contacts, par exemple leur localisation sur Instagram, afin de garder un œil sur vous.

Atteinte à votre réputation ou à votre carrière

Des contenus faux, éventuellement générés par l'IA, ou compromettants peuvent être publiés pour vous humilier publiquement. Une personne peut également intervenir dans vos e-mails, vos candidatures ou vos contacts professionnels afin de vous faire perdre des opportunités.

Suivi de localisation via les réseaux sociaux

Les publications, photos, identifications ou indications de présence sur des applications comme Snapchat ou TikTok peuvent être utilisées pour déterminer ou confirmer où vous vous trouvez, même si vous n'aviez pas l'intention de partager votre localisation.

« Il contrôlait mes messages, surveillait chacune de mes publications et a même interféré avec ma vie professionnelle. J'avais l'impression que toute ma vie numérique était devenue un moyen de me surveiller et de me piéger. »

Comment vous protéger

- Ajustez vos paramètres de confidentialité afin de limiter les personnes qui peuvent voir votre profil, vous contacter, consulter vos publications ou voir votre statut «dernière connexion». La plupart des plateformes vous permettent de définir ces éléments sur «Privé».
- Évitez de répondre aux messages abusifs.
- Conservez les messages ou faites des captures d'écran afin de garder des preuves. Sachez que certaines applications envoient une notification lorsqu'une capture d'écran est effectuée.
- Utilisez les outils de signalement intégrés à la plateforme pour signaler le harcèlement, les menaces ou l'usurpation d'identité. Le signalement peut souvent être effectué sans que l'autre personne en soit informée.
- Vous pouvez mettre en sourdine ou bloquer l'auteur des abus ainsi que tout compte qui lui est lié, y compris ceux de personnes qui vous suivent ou de faux profils, mais uniquement si vous estimez que cela ne risque pas d'aggraver la situation.

Ressources complémentaires

Stratégies pour faire face aux discours de haine



Signalement de discours de haine racistes

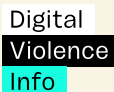
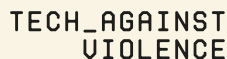


Ligne d'aide LGBTIQ



Service de conseil pour les jeunes





Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Département fédéral de l'intérieur DFI
Eidgenössisches Büro für die Gleichstellung von Frau und Mann EBG
Bureau fédéral de l'égalité entre femmes et hommes BFEH
Finanzhilfen
Aides financières

© Royal Holloway and Bedford New College 2026. Publié sous licence CC BY-NC-ND. Manuel sur les violences numériques – version française (Suisse) v1.0

Ce manuel a été élaboré par l'Information Security Group (ISG) de Royal Holloway, University of London (RHUL), en collaboration avec la Public Discourse Foundation et Tech against Violence. Sa réalisation a été rendue possible grâce au soutien financier de Soroptimist International Switzerland, du Bureau fédéral de l'égalité entre femmes et hommes, du canton de Genève et de la Fondation pour l'égalité de genre (FEG).

La version originale du manuel a été créée en 2025 par l'ISG de RHUL en collaboration avec le Surrey Domestic Abuse Partnership (SDAP), dans le cadre d'un projet financé par l'Economic and Social Research Council par l'intermédiaire du programme Social Science Impact Accelerator de Royal Holloway.

Les droits d'auteur relatifs à ce guide appartiennent à Royal Holloway and Bedford New College. Le manuel peut être utilisé conformément aux conditions de la licence Creative Commons CC BY-NC-ND. Si vous souhaitez modifier ce manuel ou l'utiliser à des fins commerciales, veuillez contacter TechAbuse-Research@rhul.ac.uk afin de discuter des conditions d'une licence.

Avertissement : les citations utilisées dans ce guide sont fictives, mais s'inspirent d'expériences réelles. Certains conseils présentés dans ce guide peuvent aller à l'encontre des bonnes pratiques générales en matière de cybersécurité ; leur pertinence dépend de la situation personnelle de chaque personne confrontée à des abus technologiques.

Cette version du manuel a été publiée en novembre 2026.

Numéros de téléphone importants pour une aide et un soutien immédiats

Police

 **117**

En cas de danger immédiat ou de situation menaçante

Urgences médicales

 **144**

En cas de blessure ou d'urgence médicale

Aide aux victimes

 **142**

Service gratuit, confidentiel, anonyme et disponible 24 h/24 et 7 j/7

Aide aux enfants et aux jeunes

 **147**

Service gratuit, confidentiel et disponible 24 h/24 et 7 j/7

Autres ressources en ligne

Informations sur la violence numérique

 www.digital-violence.info/fr

Aide aux victimes Suisse

 www.opferhilfe-schweiz.ch/fr

Campagne nationale contre la violence

 www.sans-violence.ch

Conseils et orientation sur la violence au sein du couple

 www.violencequefaire.ch

Stockage en ligne de preuves de violence domestique et de harcèlement

 www.with-you.ch/fr/safe-withyou

Reconnaître les relations toxiques et la violence domestique

 www.with-you.ch/fr

Stratégies pour faire face aux discours de haine

 www.stophatespeech.ch/fr