COFEM



Fiche pratique 1 :

Sécurité numérique

Points clés

La violence numérique n'est pas un problème individuel. Elle est souvent utilisée pour réduire les femmes au silence, les intimider et les exclure de la vie publique.

Une sécurité numérique efficace commence par la compréhension des risques. Demandez-vous ce que vous cherchez à protéger, contre qui et quelles seraient les conséquences si certaines informations étaient divulguée

Les mots de passe robustes, l'authentification à deux facteurs, les communications sécurisées et les paramètres de confidentialité adaptés restent parmi les protections les plus efficaces de se protéger contre les préjudices numériques.

La sécurité numérique est une responsabilité collective. Des pratiques organisationnelles partagées, des procédures d'intervention claires et des réseaux de soutien contribuent à protéger l'ensemble des équipes et des mouvements.

Sécurité numérique et bien-être sont indissociables. Répondre aux violences en ligne nécessite un accompagnement technique, juridique, psychosocial et émotionnel.

L'objectif n'est pas de se retirer des espaces numériques, mais d'y participer en toute sécurité, avec confiance et selon nos propres règles.

La dimension politique de la présence en ligne

Ce qui est extraordinaire avec le numérique, c'est la rapidité avec laquelle les personnes, les idées et les informations peuvent circuler. Les espaces numériques nous permettent d'être en mouvement. Ils nous permettent de nous déplacer d'une communauté à l'autre, d'une langue à l'autre, d'un pays à l'autre et d'une conversation à l'autre. Ils permettent aussi aux idées, aux données et aux récits de voyager. Nous nous trouvons, tissons des liens, remettons en question les discours dominants et nous mobilisons collectivement au-delà des frontières.

Cependant, les mouvements ne se résument jamais uniquement aux avancées qu'ils permettent. Les mêmes espaces numériques qui permettent de se connecter, d'accroître sa visibilité et de mener une action collective peuvent aussi nous exposer à de nouvelles formes de surveillance, de harcèlement et de violence. Partout dans le monde, les mouvements féministes affirment depuis longtemps que les violences faites aux femmes ne sont pas une affaire privée, mais une violation systémique des droits humains. Cette position est consacrée dans plusieurs instruments normatifs internationaux, notamment la Déclaration sur l'élimination aux femmes, le Protocole de Maputo et la Recommandation générale n° 35 de la CEDAW. Le mouvement #MeToo s'inscrit dans cet héritage. Lancé en 2006 par la militante Tarana Burke, comme une initiative portée par les survivantes, il a acquis une visibilité mondiale lorsque le hashtag est devenu viral sur les réseaux sociaux en 2017. En quelques semaines, des millions de personnes dans environ 85 pays ont partagé leur histoire en ligne, démontrant comment les espaces numériques peuvent transformer des expériences individuelles en action collective et en levier de changement social.[1]

En Argentine, le mouvement #NiUnaMenos a émergé en 2015 à la suite du féminicide de Chiara Páez, une adolescente de 14 ans, un drame qui a suscité une vive indignation publique face aux féminicides. Un tweet de la journaliste Marcela Ojeda, appelant les femmes à élever la voix contre les féminicides, est rapidement devenu viral et a été largement relayé par les réseaux militants, les milieux culturels et les médias. Sous le slogan #NiUnaMenos (« Pas une de moins »), le message s'est propagée à grande vitesse sur Twitter et Facebook, contribuant à mobiliser des centaines de milliers de personnes lors de ce qui est devenu l'une des plus grandes manifestations féministes de l'histoire de l'Amérique latine. À l'instar de #MeToo, ce mouvement a démontré que les espaces numériques peuvent transformer des expériences individuelles de violence en action collective et en pression politique en faveur du changement.

Ces exemples révèlent une réalité essentielle : les espaces numériques ne sont jamais neutres. Les mêmes technologies qui rendent possibles la mobilisation féministe et l'action collective sont façonnées par des rapports de pouvoir, des enjeux politiques et des intérêts parfois contradictoires. Dans un monde toujours plus connecté, évoluer dans les espaces numériques nous expose également à de nouvelles formes de violence. Les mêmes technologies qui permettent la diffusion des idées féministes peuvent aussi favoriser le harcèlement, la surveillance, la désinformation et les abus. La visibilité qui nous aide à construire des mouvements peut aussi faire de nous des cibles. Les réseaux qui tissent des liens peuvent également devenir des vecteurs de violence.

Pour les féministes qui luttent contre les violences faites aux femmes et aux filles, la circulation de l'information, des témoignages et des ressources est l'une de nos plus grandes forces. Elle nous permet de documenter les injustices, de soutenir les survivantes, d'apprendre les unes des autres et de nous organiser collectivement, au-delà des frontières. Mais cette transmission numérique des connaissances nous oblige aussi à réfléchir attentivement aux questions de sécurité, de confidentialité et de gestion des risques. Comment, dès lors, utiliser de manière intentionnelle le pouvoir qu'offrent les espaces numériques ? Comment tirer parti des possibilités qu'ils créent tout en réduisant les risques qu'ils comportent ? Comment rester visibles sans devenir vulnérables? Comment nous protéger, protéger nos organisations et les personnes avec lesquelles nous travaillons, tout en continuant à participer pleinement à la vie publique ?

Cette fiche pratique propose des pistes de réponse concrètes à ces questions. Elle nous guide, de la compréhension des violences numériques comme un enjeu politique à l'évaluation des risques, à la mise en œuvre de mesures de protection concrètes, au renforcement de la sécurité collective et aux réponses à apporter lorsque des préjudices surviennent.

[1] Sweeney J 2020

[2] https://8am.media/eng/ni-una-menos/

[3] Amnesty International (mai 2021). Azerbaïdjan : mettre fin à la campagne vicieuse de diffamation fondée sur le genre et de représailles contre les femmes militantes Azerbaijan (Stop the Vicious Campaign of Gendered Smears and Reprisals against Women Activists). Londres : Amnesty International. Disponible sur : https://www.amnesty.org

Regard sur L'affaire Narmin Shahmarzadeh[4]

Le 8 mars 2021, Narmin Shahmarzadeh, militante azerbaïdjanaise pour les droits des femmes, participait à l'organisation d'une marche à Bakou à l'occasion de la Journée internationale des femmes. Le lendemain matin, à son réveil, elle a découvert que son compte Facebook avait été piraté.

Les auteurs de cette cyberattaque ont utilisé son compte pour publier de fausses conversations et du contenu pornographique. Ils ont obtenu l'accès à ses documents d'identité, se sont servis de sa pièce d'identité officielle pour l'empêcher de récupérer son compte et ont volé sa carte bancaire afin de financer des publicités faisant la promotion de ce contenu abusif. Sur Telegram, les auteurs ont créé une chaîne où étaient diffusées de fausses images pornographiques attribuées à Narmin. En peu de temps, cette chaîne a attiré plus de 1 600 abonnés et cumulé des milliers de vues.

C'était certes une attaque numérique, mais son objectif était politique. Narmin a été ciblée parce qu'elle était visible. Elle s'était organisée, avait pris la parole et avait contesté le pouvoir en place. Les auteurs Les auteurs ont retourné contre elle les outils mêmes qui avaient permis son militantisme en armes contre elle. Son expérience illustre une réalité de plus en plus fréquente pour les femmes défenseures des droits humains et les militantes féministes. La violence numérique vise souvent non seulement à intimider les individus, mais aussi à nuire à leur réputation, à saper leur crédibilité, à perturber leurs efforts de mobilisation et à instaurer un climat de peur. Si leurs conséquences prennent naissance en ligne, elles s'arrêtent rarement là.

Le prix de la visibilité

L'expérience de Narmin n'est pas un cas isolé. Elle illustre un phénomène plus large où la violence numérique est utilisée pour punir la visibilité des femmes, entraver l'activisme et restreindre leur participation à la vie publique. Les violences en ligne dépassent de plus en plus les espaces numériques ; elles se répand dans le monde réel, compromettant la sécurité, le bien-être, les moyens de subsistance des femmes ainsi que leur à s'engager dans la vie publique et politique.

L'impact des préjudices numériques visant les femmes engagées dans la vie publique est à la fois généralisées et croissante. Une étude menée en 2025 par ONU Femmes auprès de plus de 640 réparties dans 119 pays révèle que 70 % des défenseures des droits humains, militantes, journalistes et professionnelles de la communication publique avaient subi des violences en ligne dans le cadre de leur travail, et que les conséquences ne se limitaient pas au monde virtuel. En effet, 41 % d'entre elles ont déclaré avoir subi des violences hors ligne, notamment des agressions physiques, du harcèlement obsessionnel (stalking) et des actes du harcèlement verbal, qu'elles reliaient directement à des violences ayant commencé en ligne. Chez les défenseures des droits humains et les militantes, cette proportion atteignait 44 %. La progression des violences en ligne vers le monde réel s'accélère également ; chez les femmes journalistes et professionnelles des médias, la proportion de celles qui établissent un lien entre les violences en ligne et les violences hors ligne a plus que doublé entre 2020 et 2025, passant de 20 % à 42 %. Près d'un quart des personnes interrogées ont également déclaré avoir été victimes de violences en ligne facilitées par l'intelligence artificielle. Cette proportion s'élève à 28 % des défenseuses des droits humains et des militantes, qui rapportent que des technologies d'intelligence artificielle ont été utilisées dans les violences dont elles ont été victimes. Le rapport est sans équivoque quant aux objectifs de ces violences : il s'agit d'un instrument stratégique, déployé pour réprimer la liberté d'expression des femmes, entraver leur participation démocratique et restreindre leurs droits à l'égalité des genres, avec des effets qui sont, comme le disent les auteurs, tout sauf virtuels.[5]

Mais la reconnaissance de ces risques ne doit toutefois pas nous conduire à nous retirer des espaces numériques ni à accepter la violence comme prix à payer pour y participer à la vie en ligne. Les femmes, les filles et les personnes de la diversités de genre ont le droit d'être visibles, de s'exprimer librement, de construire des communautés, de s'organiser, de créer et d'éprouver de la joie dans les espaces numériques, sans craindre les violences. L'objectif n'est pas de nous faire plus discrètes ou de réduire notre présence dans les espaces numériques, mais de transformer ces espaces afin que chacune puisse y participer en toute sécurité, sur un pied d'égalité et dans le respect de sa dignité. Se protéger en ligne, ce n'est donc pas seulement réduire les risques ; c'est aussi défendre Internet comme un espace d'expression, de solidarité, de créativité et de possibilités féministes.

Mais la reconnaissance de ces risques ne doit toutefois pas nous conduire à nous retirer des espaces numériques ni à accepter la violence comme prix à payer pour y participer à la vie en ligne. Les femmes, les filles et les personnes de la diversités de genre ont le droit d'être visibles, de s'exprimer librement, de construire des communautés, de s'organiser, de créer et d'éprouver de la joie dans les espaces numériques, sans craindre les violences. L'objectif n'est pas de nous faire plus discrètes ou de réduire notre présence dans les espaces numériques, mais de transformer ces espaces afin que chacune puisse y participer en toute sécurité, sur un pied d'égalité et dans le respect de sa dignité. Se protéger en ligne, ce n'est donc pas seulement réduire les risques ; c'est aussi défendre Internet comme un espace d'expression, de solidarité, de créativité et de possibilités féministes.

[4] Ibid

[5] Posetti et al., ONU Femmes, décembre 2025

Évaluer son niveau de risque

Bien qu'il incombe en premier lieu aux gouvernements, aux entreprises technologiques et aux plateformes numériques de créer des environnements numériques plus sûrs, les mécanismes actuels de protection et de responsabilisation demeurent inégaux. Dans ce contexte, les organisations et les militantes féministes peuvent choisir de prendre des mesures concrètes pour contribuer à minimiser les risques. Ces mesures ne peuvent éliminer complètement les préjudices, et ne doivent jamais avoir pour effet de déplacer la responsabilité des auteurs vers les victimes. Elles peuvent néanmoins contribuer à renforcer notre capacité à naviguer dans l'espace numérique selon nos propres conditions.

Toutes les menaces ne s'appliquent pas de la même manière à chaque militante, organisation ou mouvement. Une chercheuse féministe qui recueille des témoignages de survivantes court des risques différents de ceux d'une militante sur les réseaux sociaux. De même, une défenseure des droits humains qui documente les violences commises par l'État fait face à des défis différents de ceux d'une intervenante animant un groupe de soutien local. Plutôt que de se demander : "*Quelle est la manière la plus sûre d'agir ?*", il serait plus pertinent de se poser la question suivante : "*Qu'est-ce que je cherche à protéger, et contre qui ?*"

Les éléments à protéger varient d'une organisation à l'autre. Pour certaines organisations, il peut s'agir de protéger les informations des survivantes, les dossiers ou les bases de données de contacts. Pour d'autres, la priorité sera de protéger l'identité du personnel, de sécuriser les communications ou de protéger les comptes sur les réseaux sociaux. Les militantes, quant à elles, peuvent à titre individuel s'inquiéter du doxxing, du harcèlement obsessionnel (stalking), du cyberharcèlement ou de la divulgation d'informations personnelles pouvant mettre en danger leur sécurité ou celle de leurs proches. Il n'existe pas d'approche unique qui convienne à toutes les situations. Les évaluations des risques sont plus efficaces lorsqu'elles tiennent compte du contexte, des priorités et du niveau de visibilité publique de chaque personne, permettant ainsi de prendre des décisions éclairées quant aux mesures de protection appropriées. L'expérience de Narmin Shahmarzadeh illustre la rapidité avec laquelle une cyberattaque peut dégénérer lorsque des informations personnelles, des pièces d'identité et des comptes sur les réseaux sociaux sont compromis. Identifier les informations, les relations et les comptes qui nécessitent la plus grande protection constitue donc un bon point de départ pour réduire sa vulnérabilité et limiter les risques.

Une première évaluation des risques peut s'appuyer sur quatre questions essentielles :[6]

- Quelles informations ou quels actifs est-ce que je cherche à protéger ?
- Qui pourrait vouloir y avoir accès ?
- Quels moyens pourraient être utilisés pour y parvenir ?
- Quelles seraient les conséquences si ces informations étaient divulguées ?

La plupart des organisations ne disposent ni du temps, ni des ressources financières, ni de l'expertise technique nécessaires pour se préparer à toutes les menaces possibles. L'objectif est plutôt de prendre des décisions éclairées quant aux risques les plus importants dans son contexte et de hiérarchiser ses efforts en conséquence. Une fois les principaux risques identifiés, il devient beaucoup plus facile de déterminer quelles mesures concrètes auront le plus d'impact.

[6] Ces questions s'inspirent des approches reconnues de modélisation des menaces en cybersécurité, adaptées aux pratiques féministes de sécurité numérique. Voir, notamment Slupska et al. Participatory Threat Modelling, 2021.



Sécuriser vos comptes et appareils

Le point d'entrée le plus fréquent des atteintes graves à la sécurité numérique est le piratage de compte , c'est-à-dire lorsqu'une personne obtient l'accès à un compte de messagerie, à un compte sur les réseaux sociaux ou à un autre service au moyen d'un mot de passe volé, deviné ou réutilisé. Une fois un compte de messagerie compromis, tous les comptes qui y sont liés deviennent à leur tour vulnérables. Pour les militantes féministes, les chercheuses et les défenseurs des droits humains, les conséquences peuvent aller bien au-delà d'un simple désagrément personnel, exposant leurs sources, les survivantes, leurs collègues et des communications sensibles.L'expérience de Narmin Shahmarzadeh montre à quel point la compromission d'un compte peut rapidement prendre de l'ampleur. Les auteurs de l'attaque ont accédé à son compte sur les réseaux sociaux, ont usurpé son identité pour diffuser de faux contenus et l'ont empêché d'accéder à son propre profil. Ce qui avait commencé comme une intrusion numérique s'est rapidement transformé en une attaque contre sa réputation et son intégrité psychologique.

La bonne nouvelle, c'est que certaines des mesures de protection les plus efficaces sont aussi les plus simples :

Utilisez des mots de passe robustes et uniques pour chacun de vos comptes et conservez-les dans un gestionnaire de mots de passe reconnu, comme Bitwarden ou 1Password. Ces gestionnaires génèrent et mémorisent des mots de passe complexes à votre place, éliminant ainsi la pratique courante et risquée consistant à réutiliser le même mot de passe sur plusieurs plateformes.

Associez cette mesure à l'authentification à deux facteurs (2FA) sur tous les comptes qui le permettent. Dans la mesure du possible, privilégiez une application d'authentification plutôt que la vérification par SMS, qui demeure vulnérable aux attaques par échange de carte SIM (SIM swapping). Portez une attention particulière à votre compte de messagerie. Il constitue la clé d'accès à l'ensemble de votre vie numérique et devrait donc être considéré comme votre priorité en matière de sécurité.

La sécurité de vos appareils est également essentielle. Maintenez vos systèmes d'exploitation, navigateurs et applications à jour, car les mises à jour corrigent régulièrement les vulnérabilités exploitées par des personnes malveillantes. Activez le chiffrement complet du disque sur vos ordinateurs portables et utilisez un logiciel antivirus fiable lorsque cela est nécessaire. Soyez vigilant·e face aux liens, aux pièces jointes et aux demandes de connexion inattendus. L'hameçonnage (phishing) reste l'un des moyens les plus efficaces pour voler des identifiants de connexion ou installer des logiciels malveillants.

Les recommandations qui précèdent constituent une première étape importante. Toutefois, la sécurité numérique n'est pas une démarche ponctuelle ni une simple liste de vérification. C'est une pratique continue qui évolue au rythme des technologies et des menaces. Plusieurs organisations féministes ont élaboré des guides accessibles et adaptés aux réalités des femmes, des filles et des personnes issues de la diversité genre. Parmi ces ressources figurent les Resources en Sécurité Numérique pour les jeunes femmes de FRIDA, Gitbook, le Guide de sécurités en Ligne de ONU Femmes, et le Guide des Jeunes pour Mettre Fin aux violences Basées sur le Genre en Ligne. Ces ressources offrent des conseils pratiques plus approfondis pour renforcer le bien-être numérique, répondre aux violences en ligne et adopter des pratiques numériques plus sûres.



Gérer son empreinte numérique et protéger sa vie privée

Chaque photo, géolocalisation, mise à jour de profil et publication sur les réseaux sociaux contribue à votre empreinte numérique. Pour les militantes féministes et les défenseures des droits des femmes, ces informations, en apparence anodines, peuvent révéler bien plus que prévu. Gérer son empreinte numérique ne signifie pas devenir invisible, mais à agir de manière réfléchie et intentionnelle. Commencez par examiner les informations que vous rendez publiques. Renforcez les paramètres de confidentialité sur les plateformes de réseaux sociaux, en portant une attention particulière aux personnes autorisées à vous identifier, à vous rechercher ou à consulter votre contenu. Vérifiez régulièrement ces paramètres, car les plateformes modifient fréquemment leurs paramètres de confidentialité par défaut sans préavis.

Soyez particulièrement vigilantes quant aux informations de localisation que vous partagez. Les publications indiquant votre position en temps réel, les photographies géolocalisées ainsi que les contenus révélant les lieux où vous ou les membres de votre famille vivez, travaillez ou passez beaucoup de temps peuvent permettre à d'autres de suivre vos déplacements. Les photos prises avec un smartphone contiennent souvent des métadonnées de géolocalisation par défaut ; il est donc conseillé de les supprimer avant de partager publiquement des images sensibles.

Pour vos communications sensibles, utilisez des outils conçus dans le respect de la vie privée :

- Pour vos communications sensibles, utilisez des outils conçus dans le respect de la vie privée.
- Signal reste l'une des applications les plus fiables pour les messages et les appels chiffrés.
- Pour la messagerie électronique, les fournisseurs axés sur la confidentialité, tels que Proton Mail, offrent une protection renforcée par rapport aux services classiques.
- Lorsque vous travaillez dans des lieux publics, évitez d'accéder à des informations sensibles via des réseaux Wi-Fi non sécurisés et, si cela s'avère inévitable, Si cela est inévitable, envisagez d'utiliser un réseau privé virtuel (VPN) de confiance.

Aucune de ces mesures n'est particulièrement compliquée. Appliquées de façon constante, elles peuvent toutefois réduire considérablement l'exposition au risque.

Protection collective et organisationnelle

La sécurité numérique est souvent présentée comme une responsabilité individuelle. Pourtant, au sein des organisations et mouvements féministes, la compromission d'un seul compte peut exposer les communications, les contacts et le travail de toute une équipe. Un seul mot de passe faible sur une plateforme partagée peut créer des vulnérabilités pour tous les collaborateurs. La sécurité numérique doit donc être envisagée comme une pratique de soin collectif, plutôt que comme une simple question de compétence individuelle. Cela commence par l'adoption de pratiques partagées. Convenez des outils qui seront utilisés pour les communications sensibles, établissez des exigences minimales en matière de mots de passe et d'authentification à deux facteurs (2FA), et veillez à ce que les comptes de l'organisation ne dépendent pas d'un seul appareil ou du compte personnel d'une seule personne.

Lorsqu'un membre du personnel quitte une organisation, leur accès aux comptes partagés doit être retiré rapidement et systématiquement. Il est tout aussi important de mettre en place des structures de soutien avant même qu'elles ne soient nécessaires. Identifiez au sein de vos réseaux, des personnes de confiance capables d'offrir un soutien technique, des conseils juridiques ou un accompagnement psychosocial si vous, ou une personne de votre entourage, êtes visées. Élaborez des procédures internes simples pour réagir aux incidents tels que le piratage, le doxxing ou la compromission de compte. Savoir à l'avance qui fait quoi en situation de crise peut considérablement réduire la confusion et limiter les préjudices. Les organisations féministes investissent déjà dans la sécurité physique et le bien-être de leurs équipes et de leurs communautés. La sécurité numérique mérite la même attention.

Réagir aux incidents et préserver son bien-être

Les attaques numériques et le harcèlement en ligne sont souvent les plus préjudiciables lorsque les personnes qui en sont victimes n'ont prévu aucun plan pour y faire face. Établir un cadre de réponse de base avant qu'un incident ne survienne peut faire toute la différence.

Documenter

Lorsqu'un cas de harcèlement ou de piratage de compte survient, documentez d'abord les faits. Prenez des captures d'écran, sauvegardez les URL, notez les noms d'utilisateur et conservez les preuves avant que le contenu ne soit supprimé. Cette documentation peut être essentielle pour les signalements aux plateformes, engager des démarches juridiques ou déposer une plainte auprès de la police.



Signaler

Sachez vers qui vous tourner pour obtenir de l'aide. Les mécanismes de signalement des plateformes ne sont pas parfaits, mais ils restent une première étape importante, notamment en cas de menaces de violence, d'usurpation d'identité, de harcèlement obsessionnel (stalking) ou ou de diffusion non consentie d'images. De nombreux pays disposent d'organisations qui offrent un soutien juridique, psychosocial ou technique aux militantes confrontées à des violences numériques. Familiarisez-vous avec ces ressources avant qu'une crise ne survienne et conservez leurs coordonnées dans un endroit facilement accessible.

Prendre soin de soi

Les répercussions émotionnelles des violences numériques sont considérables. Les violences à caractères sexuels, les contenus falsifiés, les campagnes de harcèlement coordonnées et les menaces persistantes sont conçus pour épuiser, isoler et intimider. Leurs effets sont réels, cumulatifs et souvent invisibles pour les autres. C'est pourquoi la planification de la sécurité numérique doit toujours inclure une approche bienveillante. Parlez-en à vos collègues de confiance. Faites des pauses sur les réseaux sociaux lorsque vous en ressentez le besoin. N'hésitez pas à utiliser les fonctions de mise en sourdine, de blocage et de restriction de comptes. Si les répercussions deviennent trop importantes, n'hésitez pas à solliciter un soutien professionnel. La sécurité numérique et bien-être numérique ne sont pas deux préoccupations distinctes. Ils constituent les deux volets d'un même engagement : garantir que les militantes, les organisations et les mouvements féministes puissent poursuivre leur action en toute sécurité, de manière durable et selon leurs propres conditions.

Visibilité, sécurité et pouvoir

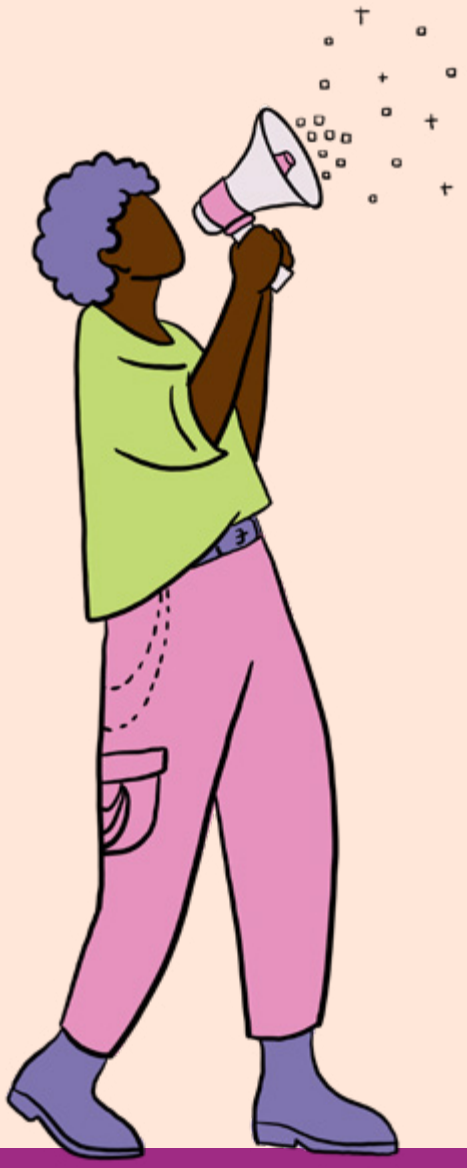
La sécurité numérique, c'est la possibilité de participer pleinement à la vie publique selon nos propres conditions. Les mouvements féministes ont toujours dû s'adapter à l'évolution du contexte politique en trouvant de nouvelles façons de s'organiser, de communiquer et de se mobiliser. Aujourd'hui, les espaces numériques font partie intégrante de ce paysage. Ils nous permettent de partager des connaissances, de soutenir les survivantes, de lutter contre l'injustice et de tisser des liens au-delà des frontières d'une manière qui aurait été inimaginable il y a encore une génération. Toutefois, ils créent également de nouveaux risques qui exigent de la vigilance, de la préparation et des pratiques de soin.

L'objectif est de faire des choix éclairés face aux risques, de renforcer la protection collective et d'acquérir la confiance nécessaire pour continuer à participer aux espaces numériques de manière sûre et stratégique. Ainsi, la sécurité numérique est à la fois un enjeu technique et un enjeu de mouvement. Lorsque les militantes, les organisations et les communautés féministes peuvent communiquer en toute sécurité, se protéger mutuellement et répondre efficacement aux violences, elles sont mieux à même de poursuivre leur travail de promotion des droits, de soutien aux survivantes et de transformation sociale. Nos mouvements reposent sur les liens que nous tissons. La sécurité numérique contribue à garantir que ces liens demeurent une source de force plutôt qu'une source de vulnérabilité.

Ressources

The following organisations and resources offer free, practical digital safety support :

Ressource	What it offers
Ligne d'assistance en sécurité numérique (Access Now Digital Security Helpline)	Soutien gratuit et confidentiel en matière de sécurité numérique destiné aux militant·es, journalistes et défenseur·es des droits humains dans le monde entier — y compris en Afrique du Sud.
Coalition contre la violence en ligne (Coalition Against Online Violence (CAOV))	Ressources et accompagnement consacrés au harcèlement en ligne Basé sur le genre, avec une attention particulière aux femmes journalistes.
Guide pratique sur le harcèlement en ligne (PEN America Online Harassment Field Manual)	Guide pratique complet pour prévenir et répondre au harcèlement en ligne — accessible gratuitement en ligne.
Initiative pour les droits civils dans le cyberespace (Cyber Civil Rights Initiative)	Soutien aux survivantes de la diffusion non consentie d'images intimes,, incluant des informations juridiques et des outils de signalement.
Fondation pour les frontières électroniques (Electronic Frontier Foundation (EFF) — Surveillance Self-Defence)	Guides pratiques et gratuits sur la sécurité numérique destinés aux militant·e·s et aux journalistes, adaptés à différents niveaux de menace.
Défenseures de première ligne (Front Line Defenders)	Soutien en matière de protection et de sécurité numérique destiné aux défenseur·e·s des droits humains dans le monde entier.
Échange féministe sur les technologies (Feminist Tech Exchange)	Ressources, formations et outils de sécurité numérique conçus spécifiquement pour les organisations féministes.



Remerciements

Ce texte a été rédigé par Lauren Messina puis révisé par Jennifer Chinoye Amadi, Leah Goldmann, Joy Watson ainsi que par les membres de l'équipe EVAW d'ONU Femmes. La conception graphique est de Mara Ayuningtyas et Léa Drougard et les illustrations de Sarah Imran. Cette publication a été produite par COFEM dans le cadre du programme ACT« Agir pour mettre fin à la violence à l'égard des femmes et des filles » d'ONU Femmes, financé par l'Union européenne. Son contenu relève de la seule responsabilité de la COFEM et ne reflète pas nécessairement les positions de l'Union européenne ni d'ONU Femmes.

Citation suggérée

Coalition des Féministes pour le Changement Social (COFEM). Introduction, Bytes de résistance : Lutter contre la violence sexiste facilitée par la technologie (2026).

Références

Amnesty International (2021) *Azerbaijan: Stop the vicious campaign of gendered smears and reprisals against women activists*. London: Amnesty International. Available at: https://www.amnesty.org

Andreasen, M.B. (2020) 'Feminist/activist responses to online abuse', in The International Encyclopaedia of Gender, Media, and Communication. Hoboken: Wiley.

Andreasen, M.B. (2024) 'Evidentiary activism in the digital age: on the rise of feminist struggles against gender-based online violence', in Edited volume title. London: Routledge.

Bansal, V., Eruyar, S., Wang, S. & Wessells, M. (2024) 'A scoping review of technology-facilitated gender-based violence in low- and middle-income countries across Asia', Trauma, Violence, & Abuse, online.

Bennett, L. and Livingston, S. (2020) 'The #MeToo movement, digital media and the public sphere', in Digital Media and the Public Sphere. London: Routledge.

Koch, L., Russo Riva, M.P. & Steinert, J.I. (2025) 'Technology-facilitated gender-based violence against politically active women: A systematic review of psychological and political consequences and women's coping behaviours', Trauma, Violence, & Abuse, online.

Loney-Howes, R. and Mendes, K. (2023) 'It's a global #MeToo: A cross-national comparison of social media responses to sexual violence', Feminist Media Studies, 24(7), pp. 1032–1050.

Posetti J, Hellmueller L, Williams K, Renaud P, Aboulez N and Shabbir N 2025 *Tipping Point: The Chilling Escalation of Online Violence Against Women in the Public Sphere*, UN Women, New York.

UN Women (2025) AI and anonymity: Digital violence against women in the age of online backlash. New York: UN Women.

VAWG Helpdesk (2017) Cyber VAWG: Violence against women and girls and information and communications technology. VAWG Helpdesk Research Report No. 211. London: UK Aid.

Slupska J, Dawson S, Ma L and Neff G (2021) Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity. Proceedings of the ACM on Human-Computer Interaction.

Sweeney J 2020 The *#Me Too Movement in Comparative Perspective, Journal of Gender, Social Policy and the Law*, Volume 29, Issue 1, 2020

Organized Crime and Corruption Reporting Project (OCCRP) (2023) 'How revenge porn is used to silence dissidents in Azerbaijan', OCCRP, 3 April. Available at: https://www.occrp.org/en/feature/how-revenge-porn-is-used-to-silence-dissidents-in-azerbaijan