Le Guide de la sécurité sur Internet pour les femmes

Avez-vous déjà été harcelée dans la rue ? Vous est-il arrivé de recevoir un message grossier sur une application de rencontres ? Un collègue vous a-t-il déjà fait une remarque déplacée sur votre apparence ?
Vous n'êtes pas la seule.
Avec le mouvement #MeToo qui a démarré à Holywood, suivi chez nous de #Balancetonporc, il suffit de se connecter sur Twitter ou Facebook pour avoir un aperçu de l'ampleur du phénomène et du nombre de femmes victimes de harcèlement sexuel. Que ce soit en personne ou en ligne, des femmes du monde entier en ont été victimes d'une manière ou d'une autre. Internet a ouvert des voies de communication, **et le harcèlement en ligne est plus répandu que jamais.**
Selon une étude du Pew Research Center, **la plupart des abus en ligne se produisent sur les réseaux sociaux**. Bien que les hommes soient également victimes de harcèlement en ligne, y compris des insultes, moqueries et menaces physiques, l'étude a révélé qu'en ligne, **les femmes sont deux fois plus susceptibles d'être victimes de harcèlement sexuel.**

En outre, **plus de la moitié des femmes de 18 à 29 ans déclarent avoir reçu des images sexuellement explicites sans leur consentement.**
Ce nombre ne cesse de croître, et bien que 70% des femmes considèrent le harcèlement en ligne comme un problème majeur, peu savent comment l'éviter.
Les femmes sont souvent des cibles simplement parce qu'elles sont des femmes. Les attaques sont souvent sexualisées ou misogynes, et la rhétorique a tendance à se centrer sur leur corps et la violence sexuelle. C'est une agression physique et émotionnelle, **et les femmes sont souvent intimidées et préfèrent garder le silence plutôt que de se mettre en danger.**
Cependant, il existe des moyens de nous protéger.
Ce guide a été conçu dans le but de permettre aux femmes de naviguer sur Internet sans crainte. Nous nous penchons sur des situations communes dans lesquelles les femmes sont victimes de harcèlement dans leur vie quotidienne : sur les réseaux sociaux, au travail, lors de rencontres… Et nous fournissons des conseils et astuces pour aider les femmes à prendre le contrôle.
Il nous tient à cœur de souligner que **certains des conseils donnés ici encouragent l'anonymat**, plutôt que de risquer d'être une cible. Bien que cela puisse sembler aller à l'encontre de l'idée d'encourager l'expression personnelle, nous pensons que chaque femme devrait avoir le pouvoir de faire ce choix pour elle-même.
Notre mission consiste à vous fournir les outils dont vous avez besoin pour cela.
Nous espérons que ce guide encouragera les femmes du monde entier à **se défendre, à se protéger et à faire face au harcèlement sexuel, à la fois sur et en dehors du Web.**

Harcèlement sur les réseaux sociaux

La majorité du harcèlement en ligne a lieu sur les réseaux sociaux, ce qui est logique étant donné le temps que la plupart d'entre nous consacrons à ces plateformes. Les réseaux sociaux étendus, souvent combinés à l'anonymat, génèrent une réalité dans laquelle tout ce que vous publiez, tweetez ou partagez vous expose à d'éventuels abus.
Ci-dessous, nous explorons les plates-formes de réseaux sociaux les plus populaires et vous expliquons comment vous protéger des sales types, des harceleurs et autres trolls.

Twitter

De par sa nature publique, **Twitter est l'une des plateformes de réseaux sociaux les plus connues en matière de harcèlement en ligne.** Et les célébrités et personnalités publiques ne sont pas les seules à être victimes d'abus. Il existe une infinité d'histoires de personnes ordinaires qui ont été attaquées, souvent uniquement pour avoir soulevé des sujets politiques ou féministes.

D'ailleurs, Amnesty International a publié un rapport reprochant à Twitter de ne pas gérer correctement le harcèlement des femmes. Dans l'étude, des dizaines de femmes évoquent les abus qu'elles ont subis sur Twitter, bon nombre d'entre elles mentionnant des réponses insatisfaisantes de la part du réseau social après avoir signalé les incidents.

Souvent, **le résultat est une réduction au silence, et les femmes choisissent simplement de ne pas s'engager de peur d'être harcelées.** De nombreuses femmes finissent par se censurer elles-mêmes ou abandonner complètement la plate-forme. Et pour certaines, en particulier les journalistes et militantes, cela peut être **préjudiciable à leur carrière.**

Les choses se sont envenimées en octobre 2017 lorsqu'**une série d'allégations d'agressions sexuelles très médiatisées a donné naissance au hashtag viral #MeToo.** Le hashtag, utilisé par les femmes du monde entier pour s'identifier comme victimes de harcèlement sexuel ou d'agression sexuelle, a pris le contrôle de Twitter en quelques heures et a clairement démontré la fréquence de ces incidents.

Côté francophone, la journaliste Sandra Muller a marqué les esprits avec son désormais célèbre tweet vengeur : « #balancetonporc !! toi aussi raconte en donnant le nom et les détails un harcèlement sexuel que tu as connu dans ton boulot. Je vous attends. » Les réactions ont été très contrastées : délation et vulgarité pour les uns, libération bienvenue de la parole pour les autres.

Les journalistes femmes ont été les premières à lui emboîter le pas et le milieu médiatique français en a été largement secoué. Après seulement un mois, on dénombrait 496 000 tweets porteurs du fameux hashtag.

Peu de temps après le début du mouvement MeToo, le compte Twitter de l'actrice Rose McGowen a été temporairement suspendu après qu'elle ait tweeté une série d'allégations à l'encontre du prédateur sexuel Harvey Weinstein et de plusieurs personnalités

notoires d'Hollywood, qui selon elle lui permettaient d'agir. La raison invoquée par Twitter ? Un de ses tweets comprenait un numéro de téléphone privé.
Mais au vu du nombre de tweets abusifs à l'encontre des femmes qui ne donnaient pas lieu à une suspension de compte, de nombreuses femmes en ont eu assez. La colère qui en a résulté a donné naissance au **hashtag #WomenBoycottTwitter, qui a appelé les femmes à boycotter la plate-forme lors d'une journée de solidarité.**
Twitter prétend avoir amélioré son système de gestion des signalements de harcèlement. Toutefois, c'est toujours un problème, et les femmes peuvent prendre certaines mesures pour réduire les risques d'être ciblées.

5 façons de vous protéger sur Twitter

1. **Utilisez plusieurs profils**

Les femmes dont la carrière dépend d'un profil public peuvent trouver utile d'utiliser plusieurs comptes.
Contrairement à d'autres plateformes de réseaux sociaux, selon les conditions d'utilisation de Twitter, il est parfaitement acceptable de le faire. D'ailleurs, les entreprises y ont souvent recours pour cibler différents publics.

Il est judicieux de créer un profil personnel et un profil public.

Votre profil personnel doit avoir les paramètres de confidentialité les plus forts. Étant donné que le paramètre par défaut de Twitter est public, vous devrez le modifier.
Généralement, lorsque vos tweets sont publics, tout le monde peut les voir. Même les personnes qui n'ont pas de compte Twitter peuvent potentiellement les trouver. Mais **lorsque vos tweets sont « protégés », seuls vos followers approuvés peuvent les voir, et personne ne pourra les retweeter.** Assurez-vous que les seules personnes auxquelles vous permettez de vous suivre sont des personnes que vous connaissez et en qui vous avez confiance.

Comment modifier vos paramètres de confidentialité sur Twitter :

Cliquez sur votre profil et allez dans Paramètres et confidentialité>Confidentialité et sécurité>Protéger vos Tweets.

Si ce changement est rétroactif, vos anciens tweets seront également protégés. Cela dit, il est important de souligner qu'étant donné Twitter n'a aucun contrôle sur les moteurs de recherche externes, **vos anciens tweets sont susceptibles d'être encore**

visibles sur Internet. Par conséquent, si vous souhaitez un véritable anonymat, vous devez créer un nouveau profil personnel et protéger vos tweets dès le départ.
Il est également important de mentionner que vos réponses aux autres tweets et mentions seront également protégées, et ne seront donc visibles que par vos « followers » approuvés. Cela rend évidemment **beaucoup plus difficile de participer aux discussions publiques qui ont fait la renommée de Twitter.** Par conséquent, à vous de décider s'il vaut la peine d'avoir un profil privé.
Pour créer un compte supplémentaire, allez sur l'app twitter sur votre smartphone ou votre tablette, en bas à droite touchez l'icône *Moi* (une tête), sur la page de votre profil touchez l'icône représentant deux têtes (comptes), optez pour *Plus d'options* dans le menu déroulant puis choisissez *Créer un nouveau compte*
Ce deuxième profil sera votre profil public. Si vous utilisez Twitter pour votre travail, **ce sera celui qui vous représente au niveau professionnel**, alors assurez-vous de ne pas tweeter des informations trop personnelles.
Une autre option consiste simplement à conserver ce profil anonyme. Cela implique de **ne pas utiliser votre vrai nom ou des photos de vous, et d'éviter de tweeter des informations susceptibles d'être utilisées pour identifier votre lieu de résidence ou de travail.**
À noter que vous ne pouvez pas garder les deux comptes ouverts sur le même navigateur en même temps. Si vous souhaitez les ouvrir tous les deux, utilisez des navigateurs différents ou utilisez l'application prise en charge par Twitter, TweetDeck.

2. Signalez et bloquez les agresseurs

Si vous recevez un tweet abusif, vous pouvez bloquer la personne qui vous l'a envoyé.
Comment bloquer quelqu'un sur Twitter :
Cliquez sur le lambda inversé dans le coin supérieur droit du tweet, et choisissez de bloquer l'utilisateur.
L'un des problèmes avec le blocage est qu'il est très facile pour les utilisateurs de créer de nouveaux comptes, qui n'ont pas encore été signalés.
Une façon d'y faire face est d'utiliser l'application Bock Together. Block Together bloque automatiquement tout compte qui tente de vous suivre et est actif depuis moins de 7 jours, a moins de 15

« followers » ou a été bloqué par vos « followers ». C'est très utile en cas d'attaque par une armée de trolls.
En plus de bloquer les utilisateurs, vous pouvez également signaler les incidents abusifs à Twitter.

Comment signaler un utilisateur sur Twitter :

Accédez au profil du compte en cliquant sur son nom, puis cliquez sur l'icône représentant 3 points verticaux juste à droite du bouton *Abonné*. Sélectionnez l'option *Signaler* et suivez les instructions.

Malheureusement, même si le harcèlement va à l'encontre du contrat d'utilisation de la plateforme, Twitter est tristement célèbre pour ne pas faire tout ce qui est en son pouvoir afin de lutter contre les comportements inappropriés.
D'ailleurs, selon une analyse de l'organisme à but non lucratif Women Action and the Media (WAM!), **67% des femmes qui ont signalé des abus ont déclaré avoir informé Twitter au moins une fois par le passé.**
Cependant, il vaut vraiment la peine de signaler des tweets et comptes abusifs, car cela ne coûte rien.
Actuellement, Twitter ne permet pas de vérifier le statut des signalements d'abus. Cela dit, depuis janvier 2018, Twitter vous informe de leur évaluation une fois que le rapport a été traité.
D'autre part, depuis juin 2018 Twitter affirme avoir pris un virage plus agressif dans sa politique de lutte anti spam pour réduire le nombre de faux comptes. Un pas vers une plus grande sécurité des utilisateurs et donc des utilisatrices.

3. Évitez le « geotagging »

Le « geotagging » consiste à **inclure le lieu d'envoi de votre message.** Pour vous protéger du « doxing » et du harcèlement, mieux vaut éviter d'utiliser cette fonction. Heureusement, le « geotagging » est optionnel, et votre localisation ne sera pas affichée par défaut.
Lorsque vous rédigez un tweet, vous voyez un bouton de localisation en bas, qui ressemble à une épingle. Si vous cliquez dessus, vous aurez la possibilité d'ajouter votre localisation à votre tweet.
Ne le faites pas.
En outre, sachez que vous pouvez révéler votre localisation même sans « geotagging », simplement en mentionnant où vous êtes. Nous comprenons qu'il soit sympa d'informer les gens que vous visitez une nouvelle galerie ou que vous

profitez de votre soirée en ville, mais il vaut parfois mieux attendre et partager votre expérience PLUS TARD, lorsque vous n'êtes plus sur place.

4. Évitez le « doxing »

La forme la plus extrême de harcèlement en ligne est le « doxing ». Le « doxing » (dérivé de « docs » comme « documents ») consiste à publier en ligne les informations personnelles de quelqu'un, telles que son adresse, numéro de téléphone, lieu de travail, coordonnées bancaires, et même des informations concernant les membres de sa famille, afin d'**encourager le harcèlement de la part des autres utilisateurs.** Le « doxing » est particulièrement utilisé dans le milieu des jeux vidéo, des hackers et à l'encontre des célébrités. C'est aussi un moyen revendiqué de se « faire justice » quand les autorités n'agissent pas.

Vous avez peut-être entendu ce terme pour la première fois à propos du #gamergate en 2014. Gamergate était un mouvement engendré par l'ex en colère de la développeuse de jeux vidéo Zoe Quinn, qui a rédigé un article de blog l'accusant d'avoir couché avec un journaliste en échange d'une critique positive.

Bien qu'une telle critique n'ait jamais vu le jour, **l'article a été considéré comme un cri de guerre par un groupe rebelle de joueurs masculins essentiellement blancs, qui ont vu non seulement leur passe-temps favori, mais également leur liberté de parole et leur masculinité, attaqués**.

Résultat ?

Non seulement Quinn, mais les femmes qui l'ont défendue, y compris la développeuse de jeux Brianna Wu et la journaliste Anita Sarkeesian, ont été attaquées sans relâche par des trolls Internet **qui les ont inondées de menace de meurtres et de viols quotidiennes**, principalement via Twitter.

Elles ont également été victimes de « doxing ».

L'impact sur le secteur des jeux vidéo a été glaçant, et **les femmes continuent d'y prendre des précautions supplémentaires de peur de devenir des cibles.**

Par exemple, Tessa*, une analyste en veille concurrentielle dont le travail l'oblige à interagir avec les joueurs, **connaît plusieurs femmes du secteur qui ont été harcelées**, et elle est souvent confrontée elle-même à un comportement de drague irrespectueux. Étant donné que de nombreuses interactions ont lieu sur Skype, elle ne peut pas cacher le fait qu'elle est une femme. Pourtant, **elle**

prend soin de dissimuler le fait qu'elle travaille directement pour une entreprise de jeux et ne révèle aucune information personnelle la concernant, comme son vrai nom ou sa localisation.
Bien sûr, les personnes du secteur des jeux vidéo ne sont pas les seules exposées au risque de « doxing ». **On peut se faire « doxer » pour ses opinions politiques, parce qu'on a été impliqué dans un fait divers, parce qu'on travaille dans une entreprise considérée par d'autres comme immorale, ou encore parce qu'on est confondu avec quelqu'un d'autre, « accidentellement ».**
Par exemple, à la suite de l'attentat du marathon de Boston, un étudiant de l'Université Brown a été victime de « doxing » après avoir été identifié à tort comme l'auteur du crime. En outre, après le rassemblement de suprémacistes blancs de Charlottesville, un ingénieur de l'Université de l'Arkansas a été victime de « doxing » après avoir été identifié par erreur comme participant.

4 façons d'éviter le « doxing »

1. **Cherchez-vous sur Google :** Une simple recherche vous montrera quel type d'informations vous concernant se trouve déjà en ligne. Si cela inclut des données susceptibles d'être utilisées pour vous identifier, essayez de voir si vous pouvez les supprimer. Les paramètres de confidentialité des profils sur les réseaux sociaux peuvent facilement être réinitialisés, et de nombreux sites Web, tels que les Pages Blanches, vous offrent la possibilité de vous désinscrire. Malheureusement, il ne sera peut-être pas possible d'effacer toutes vos informations sur Internet, mais la recherche vous permettra au moins de savoir ce que les autres peuvent trouver.
2. **Abonnez-vous à un service qui vous supprimera des sites de courtiers de données :** Si vous trouvez vos informations sur un site Web comme les Pages blanches, il est probable qu'elles apparaissent également dans d'autres annuaires en ligne, dont beaucoup ne seront pas faciles à trouver. Par conséquent, si vous avez des raisons de croire que vous pouvez être une cible de « doxing » potentielle, envisagez de payer pour un service tel que PrivacyDuck ou DeleteMe.

3. **Vérifiez que votre compte e-mail n'a pas été impliqué dans une fuite de données :** Vous pouvez utiliser l'outil https://haveibeenpwned.com/ pour voir si votre adresse e-mail et votre mot de passe ont été exposés lors l'une des nombreuses fuites de données de ces dernières années. Le cas échéant, réinitialisez votre mot de passe et envisagez d'ajouter une vérification en deux étapes à votre compte. Cela ajoutera une couche supplémentaire de sécurité en exigeant des informations complémentaires (en plus de votre mot de passe) pour vous connecter.
4. **Utilisez un VPN :** En utilisant un réseau privé virtuel, vous pouvez crypter l'intégralité de votre activité en ligne afin de vous protéger des pirates. Les VPN fonctionnent en tunnellisant vos données Internet via un serveur tiers, en évitant d'exposer votre adresse IP (et votre localisation réelle). Voici certains des VPN que nous recommandons.

5. Empêchez les hackers de pirater votre compte Twitter : De l'ancien président américain Obama à Britney Spears, au fil des ans, les comptes Twitter de nombreuses célébrités ont été piratés par des personnes souhaitant nuire à leur réputation et provoquer le chaos. Cela dit, les comptes des utilisateurs ordinaires sont également piratés à une fréquence alarmante.

4 façons d'éviter le piratage de votre compte Twitter

1. **Créez un mot de passe fort :** Cela peut sembler évident, mais vous seriez surpris (ou peut-être pas) de voir le nombre de personnes qui utilisent des mots de passe faibles, facilement déchiffrables. Pour créer un mot de passe fort, assurez-vous qu'il est long, qu'il comporte des majuscules et des minuscules et qu'il inclut des chiffres et symboles.
2. **Activez la vérification de connexion :** Ceci ajoute une couche supplémentaire de sécurité lorsque vous vous connectez. Au lieu de simplement saisir votre mot de passe, vous devrez également entrer un code que Twitter envoie sur votre dispositif mobile. Pour l'activer, cliquez sur l'icône de votre profil>Compte>Sécurité>Vérification de connexion. Sur le même onglet, vous pouvez également

choisir de demander des informations personnelles lors de la modification de votre mot de passe.

3. **Méfiez-vous de toute application tierce qui nécessite l'accès à votre compte :** Si vous avez des doutes quant à l'authenticité d'une application, ne l'installez pas. Pour voir quelles applications ont accès à votre compte Twitter, cliquez sur l'icône de votre profil et accédez à Applications. Pour supprimer une application, cliquez sur Révoquer l'accès.
4. **Prenez garde aux URL raccourcies :** Compte tenu de la limite de 280 caractères de Twitter, il est logique que de nombreuses personnes utilisent des URL raccourcies pour ajouter des liens. Le problème est qu'il est difficile de savoir où ces liens vous mènent, ou s'ils redirigent vers un site malveillant. Par conséquent, si vous souhaitez faire preuve de prudence, ne cliquez pas sur les liens affichés dans les tweets des autres utilisateurs.

Vous pouvez quasiment être certaine que quelqu'un a piraté votre compte quand vous constatez une activité inhabituelle. Par exemple si vous suivez quelqu'un de nouveau ou avez envoyé des tweets dont vous ne vous souvenez pas. Dans ce cas, la première chose à faire est de changer votre mot de passe. Vous devez également le signaler à Twitter. Vous pouvez le faire en vous rendant dans leur centre d'aide et en soumettant un ticket.

Vous devez également soumettre un ticket si quelqu'un a **créé un nouveau compte à votre nom.** Pour aider Twitter à savoir qu'il s'agit vraiment de vous, vous aurez la possibilité de télécharger une image d'une pièce d'identité officielle ou autre forme d'identification.

Facebook

Rachel n'a pas vraiment réfléchi avant d'afficher son intérêt pour le concert de l'un de ses groupes préférés sur Facebook. Mais elle a été ravie lorsque l'un des membres du groupe l'a ajoutée en amie et **a commencé à lui envoyer des messages privés.**

Au début, la conversation était désinvolte, jusqu'au moment où il a commencé à faire allusion à sa photo de profil, en lui disant qu'il l'aimait bien et que ce n'était pas grave si on voyait un de ses tétons.

Pardon, un de ses quoi ?

On ne voyait absolument pas son mamelon. Ou le voyait-on ? Rachel utilisait cette photo de profil depuis deux ans, et personne n'avait jamais rien dit. Elle a agrandi la photo et l'a soigneusement examinée. Il avait peut-être vu l'ombre de son haut ?

Elle lui a dit qu'il se trompait et a essayé d'expliquer l'ombre, lui accordant le bénéfice du doute. Mais il a insisté et lui **a bientôt demandé des photos nues.**

Rétrospectivement, Rachel sait qu'elle aurait dû stopper la conversation et le bloquer, mais à ce moment-là, elle a vraiment cru à un malentendu. C'était peut-être une photo *légèrement* provocante… **Elle aurait peut-être dû s'attendre à ce genre de réaction.**

Elle a essayé de ramener la conversation vers sa musique et le concert à venir, mais il était comme un chien avec un os, et ne

cessait de lui demander d'autres photos. Elle a fini par cesser de répondre, mais cela lui a laissé un goût amer pendant quelques jours, car **elle se demandait comment les autres la percevaient depuis tout ce temps.**

L'histoire de Rachel n'est pas si choquante. Elle n'est pas violente. Personne n'a été violé. Cela ressemble vraiment à une rencontre plutôt banale sur les réseaux sociaux. Mais en réalité, c'est sa banalité qui la rend si alarmante. **Tous les jours, des femmes sont sollicitées par des étrangers et finissent par se demander ce qu'elles ont fait pour les provoquer.** Elles doivent continuer à vivre leur vie en sachant qu'elles peuvent être objectivées par des inconnus.

La recherche révèle que **les conséquences émotionnelles qui en découlent sont particulièrement graves chez les femmes. Elles sont deux fois plus susceptibles que les hommes de décrire leur expérience la plus récente de harcèlement en ligne comme très, ou extrêmement bouleversante.**

Et la demande de photos sexy est seulement l'une des innombrables formes que le harcèlement sur Facebook peut prendre. Les femmes reçoivent régulièrement des **messages abusifs et des photos de pénis indésirables**, et les cas de « tag » sur des **photos dégradantes**, ou même de création de **faux profils** avec leurs noms et photos, sont loin d'être rares.

5 façons de vous protéger sur Facebook

1. **Contrôlez exactement qui voit quoi**

Au cours de ces dernières années, Facebook a déployé de nombreux efforts pour mettre à jour la plate-forme afin de vous permettre de personnaliser ces options, allant même jusqu'à vous permettre de **cacher vos informations à des personnes spécifiques.**

Comment contrôler ce que les gens voient sur votre profile Facebook :

Sur votre ordinateur, cliquez sur le curseur à l'envers dans le coin supérieur droit de la page, et sélectionnez les paramètres. Sur le panneau à gauche, cliquez sur Confidentialité. De là, vous pourrez gérer exactement qui peut voir vos publications, et comment les gens peuvent vous contacter.

Ensuite, allez dans Journal et identification. Cela vous permet de contrôler qui publie sur votre mur et qui voit les publications dans lesquelles vous êtes « taguée » (identifiée). Vous pouvez

également modifier vos paramètres afin de pouvoir **vérifier et approuver les « tags » avant leur publication.**
Un autre outil sympa que vous pouvez utiliser est celui qui vous **permet de voir exactement ce que les autres voient lorsqu'ils regardent votre profil.** Ainsi, vous pouvez être certaine que certaines personnes ne verront pas d'informations confidentielles si vous ne le souhaitez pas.

2. **Ne laissez pas les harceleurs potentiels savoir qui vous êtes**

Comme mentionné ci-dessus, le fait d'indiquer votre localisation dans les publications et photos peut être un moyen pour les harceleurs de savoir où vous êtes. Sur Facebook, lorsque vous rédigez une publication, vous avez la possibilité de sélectionner « Je suis là », pour ajouter une géolocalisation visible par tous vos amis. Il est judicieux de ne pas utiliser cette fonction.
Mais le « geotagging » n'est pas la seule façon pour les gens de savoir où vous êtes.
Avez-vous remarqué comment, après être allée dans un magasin particulier, vous avez soudainement commencé à voir des publicités sur Facebook ? Ou qu'après avoir rencontré quelqu'un lors d'une fête, Facebook le suggère comme ami le lendemain ?
Facebook est capable de faire tout ça car si vous avez votre téléphone sur vous (comme la plupart d'entre nous), avec l'application mobile, Facebook peut savoir **quelle est votre localisation à tout moment.**
Si vous le souhaitez, vous pouvez même voir exactement où Facebook vous a localisée. Cette information n'est pas publique, vous n'avez donc pas à vous soucier que l'un de vos amis Facebook l'utilise pour vous localiser.
Comment voir où Facebook vous a localisée :
Allez dans paramètres. Cliquez sur Localisation dans le panneau de gauche, puis sur Afficher l'historique des localisations. Une carte apparaîtra avec un **journal indiquant votre localisation depuis que vous avez activé les paramètres de localisation. Pour certains, cela remonte à des *années*.**

Comment effacer votre historique de localisation :
Cliquez sur les trois barres dans le coin supérieur droit de l'écran (ou en bas à droite si vous avez un iPhone). Sélectionnez Paramètres du compte>Localisation. Appuyez pour désactiver les

services de localisation et, en-dessous, faites glisser vers la gauche pour désactiver l'historique des localisations.
Pour supprimer l'intégralité de votre historique, cliquez sur Afficher votre historique des localisations et sélectionnez les trois petits points dans l'angle supérieur droit. Vous pourrez alors supprimer l'intégralité de votre historique. Vous devrez saisir à nouveau votre mot de passe pour le faire. (La réinitialisation de votre mot de passe est d'ailleurs un autre excellent moyen d'empêcher les autres d'accéder à votre localisation ou à votre compte Facebook en général.)

3. Bloquez les harceleurs et mettez les sales types dans une liste restreinte

Une autre option utile sur cette page est d'**ajouter certaines personnes à une liste restreinte** en allant sur leur profil et en cliquant sur l'onglet amis > Ajouter à une autre liste > Restreint. En les ajoutant à cette liste, ils apparaîtront comme vos amis mais pourront uniquement voir les informations que vous partagez publiquement. Ceci est particulièrement utile si vous souhaitez éviter une confrontation avec une personne susceptible de vous intimider ou de profiter de vous.
Bien qu'il soit facile de vous recommander de faire preuve de sincérité et de dire à quelqu'un que vous ne souhaitez pas qu'il voit vos publications personnelles, **nous savons toutes qu'une situation peut s'aggraver très rapidement lorsqu'un certain type d'homme se sent rejeté.**
Alors la prochaine fois que vous rencontrez un mec dans un bar qui *insiste* pour être votre ami sur Facebook **et** souhaite s'assurer que vous acceptez sa demande, il vous suffit de vous absenter aux toilettes et de l'ajouter à votre liste restreinte.

4. Signaler les comptes imposteurs

Même si cela va à l'encontre des conditions d'utilisation, Facebook estime qu'il y a actuellement **66 millions de faux comptes sur la plateforme.** L'une des raisons pour lesquelles les gens créent de faux comptes est l'usurpation de l'identité d'autres utilisateurs. En utilisant votre vrai nom et vos photos, **un imposteur est en mesure d'amadouer des personnes de votre réseau social réel, puis de publier du contenu dommageable et mensonger à votre sujet.**

Si vous vous apercevez qu'un faux compte utilise vos photos et vos informations personnelles, vous pouvez le signaler à Facebook et il sera probablement supprimé.

Comment signaler un faux profil sur Facebook :

Rendez-vous sur le faux profil, cliquez sur les trois points dans le coin supérieur droit de la page et sélectionnez Signaler>Signaler ce profil>Usurpation d'identité ou Faux compte.

Cela dit, un imposteur intelligent vous bloquera afin que vous ne puissiez pas accéder au faux compte. Le cas échéant, demandez à un ami de signaler le profil à votre place.

Facebook a également essayé d'être proactif dans l'identification des comptes imposteurs, et a récemment annoncé une initiative qui utilise **son logiciel de reconnaissance faciale pour signaler de nouvelles images de profil avec des utilisateurs existants.**

Toutefois, seuls les nouveaux comptes seront scannés. **Par conséquent, si un faux profil de vous a déjà été créé, à moins que vous, ou quelqu'un que vous connaissez ne le trouve et ne le signale, il n'y a aucun moyen de l'attraper.** De plus, les seules photos qui seront scannées pour identifier votre visage seront celles de votre réseau d'amis ou du réseau d'amis de vos amis, et non de tous les utilisateurs de la plateforme.

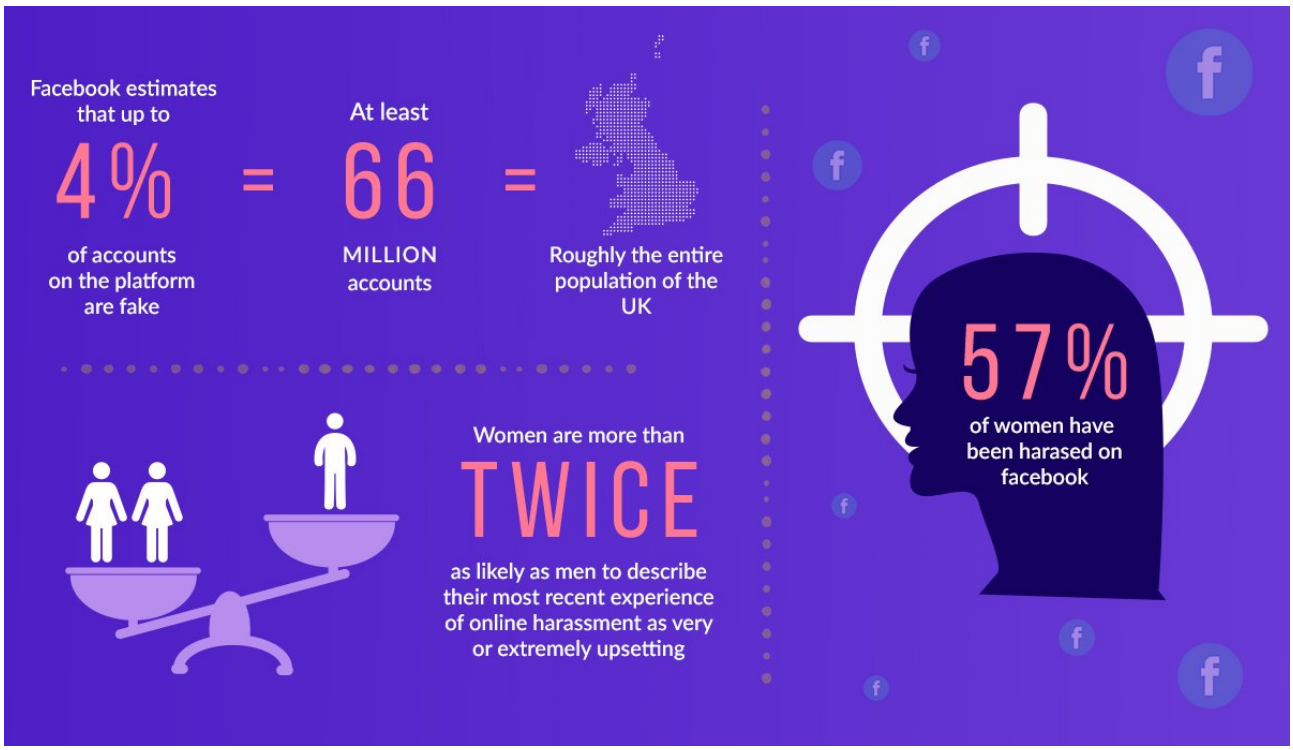
Cela remet en question l'efficacité de la tactique, surtout si l'on considère **la fréquence à laquelle les profils sont falsifiés, non pas pour réaliser des vendettas personnelles, mais pour escroquer des gens financièrement ou promouvoir des produits ou idéologies politiques.** Par exemple, des enquêtes récentes sur les élections présidentielles américaines de 2016 ont révélé comment Facebook avait été utilisé à grande échelle pour influencer l'opinion publique.

Dans ces cas-là, un moyen simple de vous protéger est de **rendre la plupart de vos photos privées.** Si le créateur du faux compte n'a pas accès à vos photos, vous serez une cible moins intéressante pour l'usurpation d'identité.

5. Protégez-vous de la vengeance pornographique

Au cours de ces dernières années, le « sexting » a totalement intégré le monde de la drague. En effet, selon une étude, 88% des adultes interrogés ont déclaré avoir envoyé des messages ou images sexuellement explicites au moins une fois. Ce n'est pas nécessairement une mauvaise chose; la même étude a révélé une **corrélation entre le « sexting » et la satisfaction sexuelle**, et a

constaté que les femmes trouvent souvent cela particulièrement stimulant.
Cela dit, l'envoi de photos révélatrices peut être risqué si elles tombent entre de mauvaises mains. Beaucoup trop de femmes on fait l'objet de campagnes d'humiliation, dans le cadre desquelles **d'anciens partenaires rancuniers ont fait de leur vie un enfer en envoyant des images intimes à leurs amis, aux membres de leur famille et même à leurs employeurs.**
Heureusement, Facebook a déjà un **algorithme qui identifie et supprime les images de nus.** Cependant, en novembre 2017, ils ont également annoncé une nouvelle approche quelque peu novatrice pour s'attaquer à l'inquiétante épidémie de « revenge porn », ou vengeance pornographique. Mais l'idée, qui sera d'abord testée en Australie, est susceptible de créer la polémique.
En gros, si vous soupçonnez qu'une image en particulier est susceptible d'être publiée sur Facebook sans votre consentement, **vous remplissez un formulaire pour expliquer votre inquiétude, puis vous envoyez l'image via l'application Facebook Messenger.** Après évaluation du signalement et de la photo, Facebook l'efface.
Étant donné que Facebook possède Instagram, cela empêchera également la diffusion de l'image sur ce réseau social.
Cette approche présente plusieurs problèmes. Tout d'abord, vous devez savoir que les images existent. (Parfois, des photos et des vidéos sont prises à l'insu de la victime ou sans son consentement.) Deuxièmement, vous devez avoir les images en votre possession, ce qui peut ne pas être le cas si elles ont été prises avec l'appareil photo de quelqu'un d'autre. Enfin, **vous devez faire confiance à Facebook, et accepter qu'une personne réelle voie des images que vous souhaitez explicitement cacher au public.**
Pour beaucoup, le fait de savoir qu'un technicien anonyme a accès à leurs photos intimes, même pour une courte période, ne fera qu'aggraver le traumatisme et l'anxiété qu'elles éprouvent déjà.



Instagram et SnapChat

Les photos n'ont pas été la seule chose à changer lorsqu'Instagram a vu le jour en 2010, et SnapChat en 2012. Le harcèlement en ligne a également évolué.

En rendant vos photos publiques, vous donnez à **n'importe qui la possibilité de les commenter**. Bien qu'il soit difficile de comprendre pourquoi une personne consacre son temps à gâcher la vie des autres, certains utilisateurs passent leur journée à chercher des occasions d'insulter autrui, à travers leurs photos. Le « body shaming » et les messages reçus via Instagram Direct en langage explicite et vulgaire empoisonnent des millions de comptes tous les jours.

En plus du « trolling », **de nombreuses femmes sont exposée à la vengeance pornographique, à des photos de pénis et autres photographies nues indésirables.**

Différentes techniques vous permettent de vous défendre et même de prévenir certaines de ces situations. Certes, les trolls et les imbéciles trouveront toujours une solution pour vous atteindre s'ils insistent, mais les mesures suivantes vous permettront de grandement leur compliquer la tâche.

3 façons de vous protéger sur Instagram et SnapChat

1. **Vérifiez les données qui permettent de vous identifier sur vos photos**

Certaines mesures simples vous aideront à rendre vos photos et comptes un peu plus sûrs.

Imaginons que vous êtes au restaurant et que vous voulez publier une photo de votre assiette sur Instagram. C'est sympa de taguer le restaurant pour lui faire la publicité. Mais **en taguant ce restaurant, vous indiquez que vous vous y trouvez à ce moment-là.**

N'importe quel harceleur sait maintenant exactement où vous êtes.

De même, en activant les paramètres de géolocalisation, vous courrez encore plus de risques. Si vous prenez une photo de votre latte au caramel de Starbucks, vous pouvez vous trouver dans l'un des 27 339 Starbucks du monde entier. Mais **si votre géolocalisation est activée, celui qui voit votre photo saura exactement où vous êtes.**

En juin 2017, Snapchat a lancé une nouvelle fonctionnalité appelée SnapMap, qui affiche les localisations de tous vos amis sur une carte. Bien que cela puisse sembler innocent, cela permet aux autres de constamment surveiller vos déplacements. **Désactivez la fonctionnalité SnapMap, et vous vous épargnerez de nombreuses situations potentiellement désagréables.**

2. **N'utilisez pas vos informations réelles**

Lorsque vous vous inscrivez à SnapChat, vous devez indiquer votre date de naissance, votre numéro de téléphone et votre adresse e-mail, ce qui est plutôt habituel avec les applications de réseaux sociaux. Mais **n'importe quelle personne avec un minimum de connaissances techniques peut ensuite trouver ces informations via votre compte SnapChat**. Cela rend extrêmement facile pour un utilisateur de SnapChat de poursuivre le harcèlement par email, sur WhatsApp, et via d'autres applications.

La meilleure façon de protéger vos informations est de les cacher. **Créez une nouvelle adresse e-mail pour vous inscrire.** En outre, utilisez un faux numéro de téléphone (vous savez, le numéro typique que vous donnez à un mec insistant au bar pour qu'il ne vous appelle pas), et créez une nouvelle date de naissance.

Une autre astuce simple pour compliquer la tâche des trolls est de **changer le statut de votre compte de public à privé.** Cela est valable pour Instagram et Snapchat. Le changement de votre compte en mode privé limite les personnes qui voient vos messages à vos amis, vos proches et à toute autre personne que vous autorisez.

Comment rendre votre compte privé sur SnapChat :

Allez dans Paramètres>Voir Ma Story>Mes amis/Personnalisé. Dans Paramètres, vous pouvez également décider qui peut vous contacter et qui peut voir votre localisation.

Comment rendre votre compte privé sur Instagram :

Allez dans Paramètres>Compte privé (faites glisser vers la droite pour activer).

Si vous devez utiliser ces applications pour promouvoir un produit, votre entreprise ou vous-même, créez un compte distinct. De cette façon, vos photos personnelles ne seront pas mélangées avec vos photos publiques.

Cela dit, même si vous faites tout cela, des commentaires grossiers sont susceptibles de se glisser entre les mailles du filet. Le cas échéant, il est utile de savoir comment…

3. Bloquer les sales types

Instagram et Snapchat offrent des options de blocage. En utilisant cette technique, vous pouvez bloquer un utilisateur, puis supprimer ses commentaires.

Allez dans Paramètres>Compte privé (faites glisser vers la droite pour activer).

Comment bloquer les gens sur Instagram :

Sélectionnez la personne que vous souhaitez bloquer, appuyez sur les trois points dans le coin supérieur droit, puis cliquez sur Bloquer l'utilisateur.

Comment bloquer les gens sur SnapChat :

Sélectionnez la personne que vous souhaitez bloquer, appuyez sur les trois lignes dans le coin supérieur gauche, puis cliquez sur Bloquer.

Le harcèlement au travail

Malheureusement, les abus sont également fréquents dans les environnements professionnels. Selon une étude IFOP, en France, une femme sur trois a été victime de harcèlement sexuel selon la définition légale. *« Le fait d'imposer à une personne, de façon répétée, des propos ou comportements à connotation sexuelle qui soit portent atteinte à sa dignité, en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante ».* Cette notion de répétition de la situation n'est pas valable dans le cas d'un attouchement sexuel ou si le harceleur fait pression pour obtenir un acte de nature sexuelle.

Ce harcèlement touche particulièrement les femmes homosexuelles et bisexuelles (58%), et les chefs d'entreprises (44% d'entre elles ont subi des situations de harcèlement). Notons que le harcèlement sexuel au travail est majoritairement subi par les cadres et les professions intellectuelles supérieures.

Si elles sont 60% à en avoir parlé, c'est en général à une personne de leur entourage, et très rarement à un supérieur hiérarchique ou à un représentant syndical. Et seulement 5% des cas sont portés à l'attention de la justice.

Nous ne pouvons que spéculer sur les raisons de cette situation, mais l'une d'entre elles est sans doute que le harcèlement sexuel n'est pas clairement défini.

Cependant, certains exemples de harcèlement sexuel comprennent :

1. Le partage d'images ou de vidéos sexuellement inappropriées.

2. L’envoi de lettres, de SMS ou d’emails avec un contenu suggestif.
3. Les blagues salaces ou les anecdotes sexuelles.

Mais même ces situations sont ambiguës ! Si quelqu’un envoie une photo de pénis, il s’agit clairement de harcèlement sexuel, mais un commentaire désinvolte pourrait être mal interprété.
Alors, comment savoir s’il s’agit de harcèlement sexuel ?
Lorsque vous n’êtes pas sûre, pensez à ce que vous ressentez. Cette remarque vous a-t-elle mise mal à l’aise ? La trouvez-vous écœurante ? Si oui, il est probable que la situation puisse être interprétée comme du harcèlement sexuel.

Le harcèlement sexuel au travail

Le harcèlement sexuel peut prendre différentes formes, et lorsqu’il se passe en ligne, il est souvent encore moins évident. Pourtant, le harcèlement au travail existe. Si vous vous trouvez dans une situation professionnelle où vous vous sentez mal à l’aise, vous devriez immédiatement commencer à prendre des notes. **Souvent, les cas plus importants se développent sur une série de petits incidents, qui ne seront pas considérés comme des preuves s’ils ne sont pas documentés correctement.**
Même si vous n’êtes pas sûre qu’une interaction soit considérée comme du harcèlement, mieux vaut la traiter en tant que tel au cas où la situation s’aggraverait et que vous décidiez d’agir.

Comment signaler le harcèlement au travail

1. **Documentez chaque interaction**

Toute remarque, tout e-mail inapproprié ou autre correspondance susceptible d’être qualifié(e) de harcèlement doit être enregistré(e) et stocké(e) à un endroit où vous seule avez accès (pas sur le Google Drive de l’entreprise, par exemple). Il se peut qu’une remarque ne soit pas intentionnelle, mais si cela se reproduit, vous pourrez monter un dossier.
Si une interaction implique des paroles ou un contact physique inapproprié, écrivez-vous dès que possible un e-mail (à partir de votre compte personnel) décrivant l’incident de la manière la plus détaillée possible. Indiquez l’heure, la date et le lieu de l’incident.

2. **Gardez des traces**

Prenez des captures d’écran, enregistrez les heures et les dates, sauvegardez vos e-mails et conservez un fichier de tout ce qui vous rend mal à l’aise.

3. Signalez-le

Une fois que vous avez des preuves, il est temps de porter plainte. Bien que cela soit parfois gênant, signaler le harcèlement au bureau est l'un des moyens les plus efficaces d'y mettre fin.

Envoyez vos preuves au service des ressources humaines, qui, nous l'espérons, a déjà une politique en place sur la façon de procéder. S'il votre entreprise n'a pas de service de ressources humaines, rédigez un e-mail détaillé et envoyez-le à la direction ou à votre supérieur hiérarchique (du moment que ce ne sont pas eux qui vous harcèlent).

Comment rédiger un e-mail pour signaler le harcèlement sexuel :

La rédaction de ce premier e-mail peut sembler intimidante. C'est pour cette raison que nous vous proposons un modèle.

Objet : Plainte officielle de harcèlement sexuel

Monsieur/Madame [RH] et [patron],

L'objet de cet e-mail est de vous informer que [nom du harceleur] me harcèle sexuellement depuis [x période].

Les incidents suivants se sont produits au cours de cette période :

- [Exemple 1 : Décrivez ce qui s'est passé et quand. Essayez d'inclure autant de faits que possible.]
- [Exemple 2 : Décrivez le deuxième incident qui vous a mise mal à l'aise. N'oubliez pas d'indiquer si vous avez discuté avec quelqu'un d'autre au travail à ce sujet.]
- [Exemple 3 : Joignez des documents ou des preuves à l'appui de votre cas.]

[Le cas échéant, indiquez les mesures que vous considérez que l'entreprise devrait prendre. Par exemple, vous pouvez écrire: « J'aimerais être transférée dans un autre département » ou « J'aimerais que l'on examine cette question et je voudrais des excuses formelles de la part de [nom du harceleur]. »]

Merci de vous pencher sur ce problème. Si vous avez besoin de plus amples informations, n'hésitez pas à me le faire savoir.

Cordialement,

[Votre nom]

Votre entreprise a probablement mis en place une politique d'évaluation et d'action en cas de harcèlement.

Si vous n'avez pas l'impression que votre plainte a été traitée correctement, rappelez-vous que **vous pouvez toujours faire**

appel à une aide juridique externe. Un professionnel avec une bonne connaissance de la législation pourra vous guider pour les prochaines étapes.
Il convient également de souligner que pour beaucoup, **le fait de signaler l'incident en interne n'est pas une option, car de nombreuses femmes travaillent à leur compte ou sont indépendantes.** Si c'est votre cas, vous devez vous-même prendre la situation en main.

Le harcèlement sexuel pour les travailleuses indépendantes

Si vous êtes travailleuse indépendante et que vous êtes victime d'un comportement inapproprié, étant donné que vous ne pouvez le signaler à personne, **vous devrez gérer la situation vous-même.**
C'est exactement ce qui est arrivé à Arielle*, une musicienne qui a reçu des messages sexuellement explicites de la part d'un autre professionnel de son secteur. Suite à une remarque sur la façon dont elle se déhanchait en jouant, Arielle a répondu « pauvre type », et le harceleur de surenchérir « Oh oui, parle-moi comme ça, j'aime ça ».
Arielle a décidé de ne pas l'humilier publiquement, mais elle lui a répondu que ses commentaires étaient suggestifs et agressifs. Le harceleur n'était pas d'accord et les choses se sont arrêtées là.
Le fait de confronter son harceleur a soulagé Arielle. D'autres peuvent trouver que le meilleur moyen de se protéger est d'ignorer les harceleurs. **Il n'y a pas de bonne ou de mauvaise façon d'aborder le harcèlement dans cette situation.** La décision vous appartient.

Le harcèlement sexuel sur LinkedIn

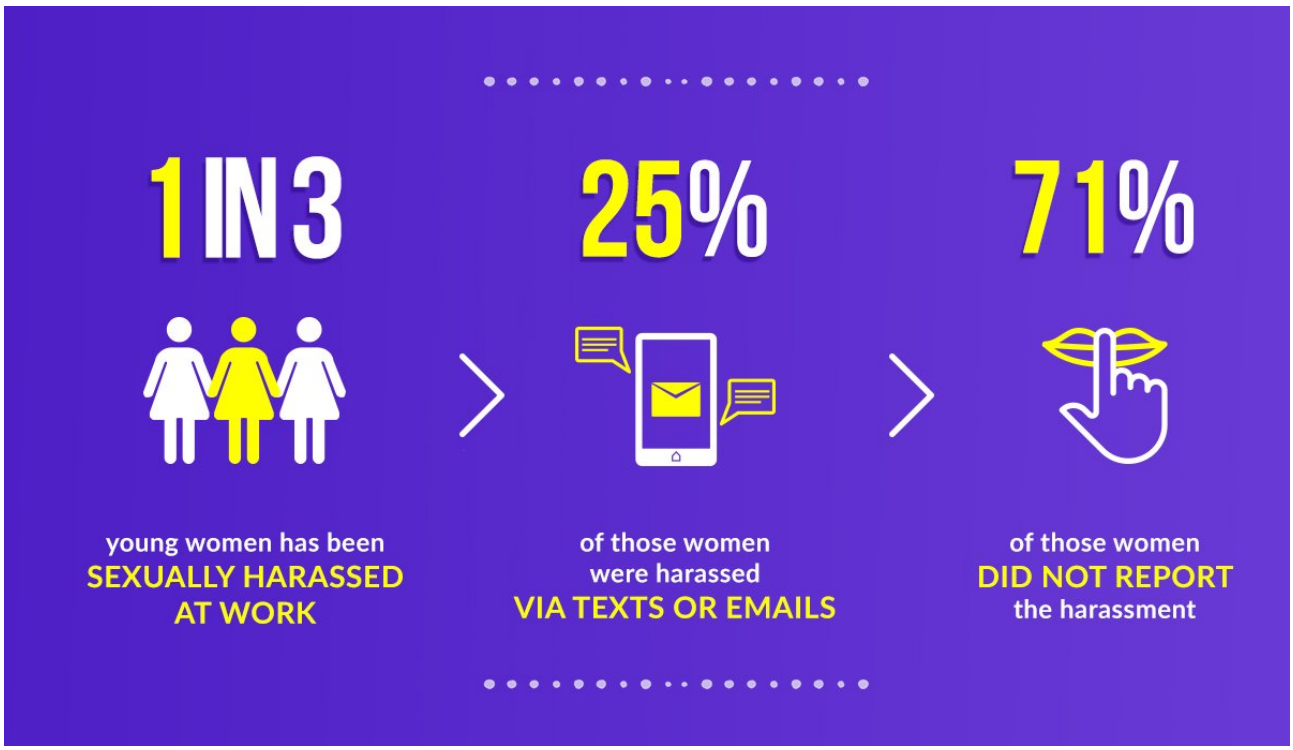
LinkedIn, une plate-forme en ligne pour faciliter le réseautage et les contacts professionnels, est malheureusement également devenue un lieu de harcèlement sexuel. **Bien que la politique de LinkedIn interdise toute forme de harcèlement, LinkedIn n'a aucun moyen de l'empêcher complètement** et, malheureusement, le harcèlement sexuel y est toujours présent actuellement.
Étant donné qu'il s'agit d'un site de réseautage, **certains utilisateurs le considèrent comme un site de rencontres.** Parmi les plaintes, des femmes ont signalé y avoir reçu des messages inappropriés et des remarques obscènes sur leur apparence en fonction de leurs photos de profil.

Autre piège potentiel : votre CV.
De nombreuses personnes mettent leur CV en ligne sans penser au fait que **leur adresse e-mail et numéro de téléphone sont visibles dans l'en-tête.** À moins que vous ne souhaitiez que l'ensemble de l'Internet ait accès à ces informations, supprimez-les de la version que vous publiez.
Les appels téléphoniques non désirés pour demander un rendez-vous peuvent ne pas être vus comme du harcèlement sexuel pour certains hommes, mais les femmes qui reçoivent des appels téléphoniques d'étrangers peuvent le percevoir différemment.
Mais c'est bien là le problème. Étant donné que la plupart des cas de harcèlement ne sont pas flagrants, il est plus difficile pour les femmes de les justifier et de les signaler. Bien que vous ne puissiez pas empêcher les sales types de vous envoyer des messages sur LinkedIn, il existe des moyens de vous protéger.

4 façons de vous protéger sur LinkedIn

1. Avant d'accepter un contact LinkedIn, vérifiez les degrés de connexion. Avez-vous des contacts en commun ? Travaillent-ils dans votre secteur ? Dans le cas contraire, ne l'acceptez pas.
2. Si vous recevez un message non sollicité, vous pouvez décider de bloquer l'expéditeur. Cliquez simplement sur les trois points en haut à droite, puis cliquez sur Signaler cette conversation.
3. Vous pouvez également empêcher cette personne de voir votre profil ou de vous contacter. Accédez au profil de la personne, cliquez sur Plus>Signaler/Bloquer et suivez les instructions.
4. Si vous chargez votre CV, vérifiez que votre numéro de téléphone, votre adresse personnelle et vos autres coordonnées ne sont pas affichées. Si quelqu'un veut vous contacter pour un motif professionnel, il peut le faire via LinkedIn.

Il n'y a aucune garantie que ces suggestions vous protégeront à 100%. Cependant, elles vous fournissent plus de contrôle sur les personnes qui peuvent vous contacter.



Les rencontres en ligne et le harcèlement sexuel

Elsa* discutait avec Marco* qu'elle avait rencontré sur Adopteunmec depuis environ un mois, mais ils ne s'étaient pas encore rencontrés en personne. Un soir, après plus d'une heure de SMS de plus en plus aguichants, Marco lui a suggéré de passer à quelque chose de plus visuel, plus concrètement du sexe sur Skype.

Le jour suivant, Elsa, horrifiée, a reçu un appel de l'une de ses amies l'informant qu'elle avait reçu un enregistrement de la session. Une heure plus tard, **Elsa recevait un message de Marco lui demandant de payer si elle ne voulait pas que l'enregistrement soit envoyé à encore plus de membres de son réseau social.**

Les rencontres en ligne sont le domaine où les femmes sont les plus vulnérables au cyberharcèlement sexuel.

La raison est que contrairement à la plupart des réseaux sociaux, **on va sur les sites de rencontres pour rencontrer, et potentiellement se rapprocher intimement d'inconnus.** Tandis que sur d'autres sites, les paramètres de confidentialité stricts peuvent servir de bouclier, sur les sites de rencontres, ces tactiques pour rester en sécurité risquent de se traduire par un autre samedi soir en solo.

Bien que les applications de rencontres soient censées être amusantes, elles sont également connues pour conduire à des rencontres plutôt désagréables.

Par exemple, Ludivine* a rencontré Raphael sur l'application Happn. Après avoir discuté sur l'application, la conversation est passée sur WhatsApp, mais lorsque Ludivine a vérifié sa photo de profil, elle a remarqué que Raphael **avait l'air différent et que son profil ne correspondait pas à celui de l'application de rencontres.** Souhaitant éviter la confrontation, elle a informé Raphael qu'elle avait des problèmes personnels à régler avant d'être prête à s'engager dans une relation. Au lieu d'accepter son explication, il a commencé à la bombarder de questions agressives pour savoir où elle était, et avec qui.

Ludivine a fini par le bloquer et le signaler à Happn. Sachant qu'il la chercherait sur les réseaux sociaux, elle l'a également bloqué sur Facebook, WhatsApp et Instagram. Et lorsqu'il a essayé de l'appeler, elle a également bloqué son numéro. Que Raphael ait finalement compris (ce qui est fort peu probable) ou simplement trouvé trop difficile de maintenir le contact, Ludivine est parvenue à mettre fin aux abus, mais toutes les femmes n'ont pas cette chance.

Ce qui est arrivé à Ludivine est connu sous le nom de **« catfishing », c'est à dire lorsque quelqu'un ment sur son identité, en utilisant souvent de fausses photos et des profils falsifiés.** Elle s'est facilement rendue compte que la personne sur le profil Happn était différente de la personne du profil WhatsApp, mais la plupart des « catfishers » sont suffisamment intelligents pour mieux dissimuler leurs traces.

De même, il est relativement facile de **devenir sans le savoir le complice d'un « catfisher ».** C'est ce qui est arrivé à Chloé*. Un jour, elle a reçu un appel d'une amie l'informant que **sa photo de profil Facebook était utilisée sur le profil de quelqu'un d'autre.** Chloé a signalé le faux profil et il a été effacé, mais qui sait combien de personnes ont vu son visage et ses informations avant la suppression ?

Malheureusement, il n'y a aucun moyen de rencontrer des gens en ligne en ayant la garantie que vous ne serez jamais une victime. Cependant, il existe des moyens de vous protéger.

3 façons de vous protéger sur les sites de rencontre

1. **Vérifiez l'identité de la personne**

Lorsque vous rencontrez quelqu'un en ligne pour la première fois, cherche-le sur Google, Facebook et d'autres applications de rencontres si vous y êtes inscrite. Rechercher des incohérences dans leurs images et descriptions de profil. Si vous en trouvez, signalez le profil à votre application.

2. **Faites connaissance sur l'application**

Discutez sur l'application avant de passer sur une plate-forme différente. Cela vous donnera une idée de la personne avant de révéler plus d'informations sur votre vie personnelle. Une fois que vous vous sentez suffisamment à l'aise pour discuter sur une autre plateforme, soyez consciente de ce qu'ils peuvent y voir. Par exemple, WhatsApp et Telegram autorisent les photos de profil, WhatsApp permet les mises à jour de statut, et Telegram vous permet d'écrire une brève bio vous concernant. Les deux applications ont également une fonctionnalité « dernière visite », qui indique à vos contacts la dernière fois que vous étiez sur l'application. Si vous ne voulez pas que quelqu'un voit ces informations, modifiez vos paramètres de confidentialité. Et si vous finissez par vous rencontrer en personne, **assurez-vous de le faire dans un lieu public et d'en informer un ami.**

3. **Gardez vos comptes et photos de réseaux sociaux privés**

Cela minimise les risques que quelqu'un dérobe vos photos et les utilise sur des sites de rencontres.

Le « sexting » en toute sécurité

La plupart des adultes connaissent bien le concept de « sexe protégé ». Mais ils n'ont peut-être pas pensé au « sexting protégé ».

Ceci est particulièrement important, car le « sexting » est en hausse. En effet, selon une étude, **près de la moitié des adultes interrogés déclarent « sexter ».**

Cependant, le fait que de nombreuses personnes le fassent ne signifie pas que ce n'est pas sans risques. Les histoires de vengeance pornographique et les piratages qui ont exposé les photos intimes des gens sont courantes. Et il n'est pas difficile d'imaginer que des photos nues tombant entre de mauvaises mains peuvent ruiner votre vie professionnelle et personnelle.

Le plus simple serait de vous conseiller d'arrêter le « sexting », mais ce n'est pas ce que nous allons faire. **Le « sexting » peut**

être un élément amusant et épanouissant de votre relation ou votre vie amoureuse, et nous ne sommes pas là pour vous empêcher de passer un bon moment.
Nous allons plutôt vous donner quelques conseils simples sur la façon de « sexter » en toute sécurité. Certains peuvent sembler relever du bon sens, mais **nous allons également vous expliquer certaines astuces techniques qui vous permettront de vous détendre lorsque votre smartphone chauffe.**

7 façons de vous protéger en « sextant »

1. **Ne montrez pas votre visage ou d'autres choses identifiables**

Si vos photos sont rendues publiques, votre première ligne de défense est un déni plausible. Cela signifie que vous devez vous assurer que vos photos ne comprennent pas votre visage, vos taches de naissance ou vos tatouages.

2. **Ne « sextez » pas sous l'emprise de l'alcool**

Vous vous sentez peut-être d'humeur coquine après quelques margaritas, mais cela ne signifie pas que c'est le meilleur moment pour déboutonner votre haut et sortir votre appareil photo.
Heureusement, il existe plusieurs applications disponibles pour éviter les regrets du lendemain matin. Par exemple, **Drunk Locker est une application très complète et utile pour les soirées de fête.** En plus de vous trouver un conducteur attitré, elle peut également **bloquer certains contacts** afin que vous ne puissiez pas les appeler, leur envoyer des SMS ou les contacter via les réseaux sociaux.

3. **Faites en sorte que vos photos s'autodétruisent**

L'application **Disckreet est spécialement conçue pour le « sexting »**, et requiert que l'expéditeur et le récepteur saisissent un code d'accès afin de voir une image envoyée. Le principal avantage de Disckreet est qu'elle vous **permet de supprimer vos images du téléphone de la personne à qui vous les avez envoyées.** Cela dit, rien n'empêche la personne qui reçoit vos photos de prendre une capture d'écran et de les enregistrer.
Pour contourner quelque peu le problème de capture d'écran, vous pouvez utiliser **SnapChat, qui supprime automatiquement les photos quelques secondes après leur ouverture.** Bien que SnapChat autorise les captures d'écran, il vous enverra une notification lorsqu'une capture d'écran est prise. Cela dit, ce n'est pas une solution parfaite, car une brève recherche sur Google

propose plusieurs façons de contourner la notification. Il est donc toujours possible pour quelqu'un d'enregistrer votre photo sans que vous le sachiez.
Confide, une application soigneusement cryptée qui supprime automatiquement les messages et photos, **ne permet pas aux destinataires de prendre des captures d'écran.** Mais, là encore, si quelqu'un souhaite vraiment enregistrer vos photos nues, il trouvera le moyen de le faire.

4. **Protéger vos téléphones et photos avec un mot de passe**

Pour vous assurer que personne ne tombe sur des photos compromettantes par accident en utilisant votre téléphone ou celui de votre partenaire, protégez vos téléphones avec des codes d'accès.
Vous pouvez également télécharger une application qui **conservera vos photos sexy dans un dossier séparé et protégé par mot de passe.** KeepSafe et Gallery Lock sont deux bonnes options. L'une des fonctionnalités sympas de Gallery Lock est que vous pouvez choisir de garder l'icône cachée, afin que personne ne sache que vous l'avez sur votre téléphone. En outre, si quelqu'un tente de se connecter à plusieurs reprises et échoue, l'application le prendra en photo.
Sachez toutefois que **toutes ces applications n'offrent pas de cryptage**, ce qui signifie que vos photos sont potentiellement exposées au piratage.

5. **Enregistrez vos photos de façon sûre**

Si vous prenez une photo où vos fesses sont vraiment sublimes, vous préfèrerez peut-être la sauvegarder plutôt que de l'autodétruire. Le cas échéant, mieux vaut la stocker sur un **ordinateur de bureau** plutôt que sur un dispositif mobile, plus susceptible d'être égaré ou volé.
Toutefois, gardez à l'esprit que vous pouvez être piratée même sur un ordinateur de bureau. Par conséquent, il est plus judicieux **d'enregistrer vos photos confidentielles dans un fichier crypté.** VeraCrypt est un programme open source gratuit qui vous permet de crypter des fichiers individuels sur votre Mac ou votre PC.
Toutefois, il convient de souligner qu'une fois que vos photos sont dans un dossier chiffré, **vous devez tout de même les effacer définitivement de votre ordinateur.** Il ne suffit pas de les jeter à la poubelle et de la vider.

Jusqu'à ce que ces données soient remplacées par de nouvelles données, elles existent encore et peuvent être trouvées par un pirate motivé. Heureusement, il existe un logiciel pour supprimer définitivement les fichiers. Pour Windows, l'une des options les plus populaires est Eraser, et sur Mac, vous pouvez utiliser Permanent Eraser.

6. Ne synchronisez pas vos photos

Si vous avez un dispositif Android, il est probable que vos photos soient automatiquement enregistrées dans Google Photos, et si vous avez un iPhone, sur l'iCloud.

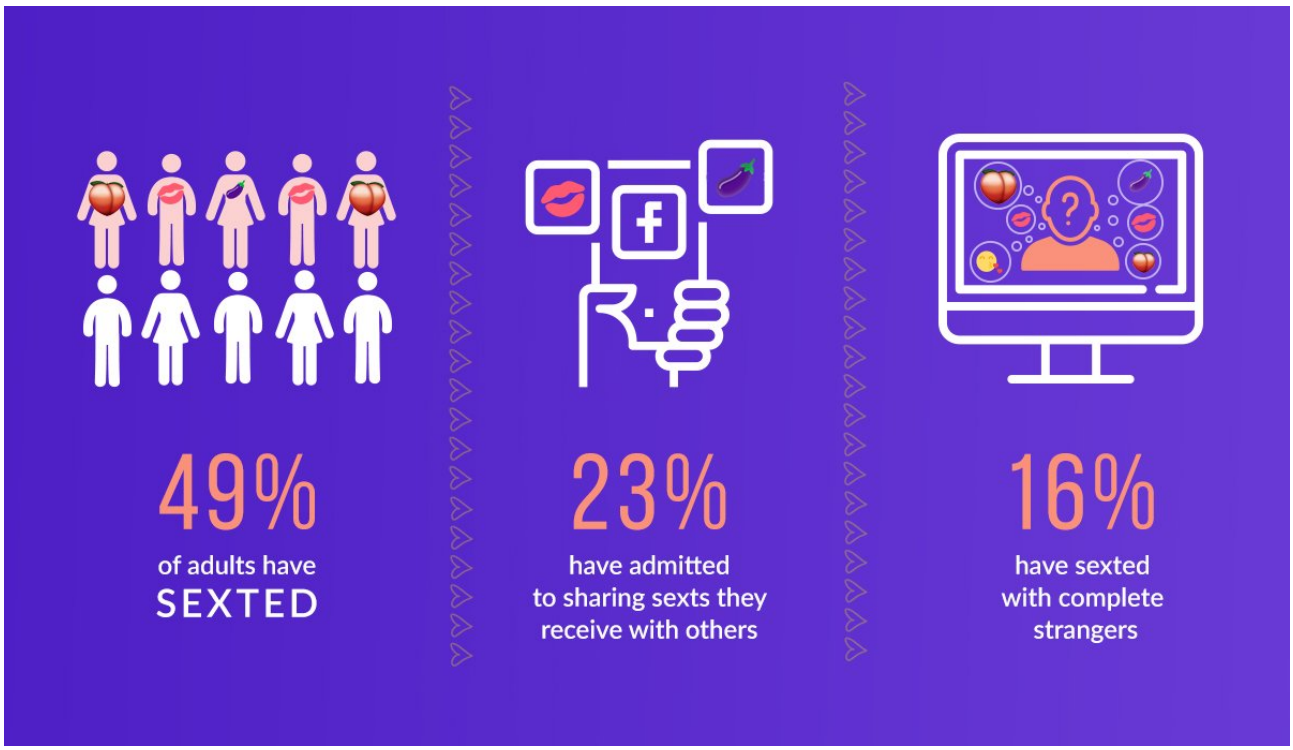
Vous vous souvenez peut-être du fameux piratage d'iCloud de 2014, lorsque des **photos privées de plusieurs célébrités (principalement des femmes), dont Jennifer Lawrence et Kirsten Dunst, ont été divulguées** à la suite d'une attaque de phishing. Puisque vous ne voulez pas que cela vous arrive, mieux vaut **garder vos photos confidentielles hors du cloud.**

Cela dit, nous ne vous recommandons pas de désactiver la synchronisation automatique, car cela peut entraîner la perte de vos informations en cas de perte ou de vol de votre téléphone. Au lieu de cela, vous devez vous connecter à Google Photos ou iCloud et les **supprimer une par une.** Sachez cependant que **si vous avez activé la synchronisation automatique, la photo sera peut-être également supprimée de votre téléphone lors de la prochaine synchronisation.** Par conséquent, si vous souhaitez enregistrer la photo, sauvegardez-la ailleurs, de préférence dans un dossier chiffré (voir ci-dessus).

7. N'envoyez pas de photos à des personnes en lesquelles vous n'avez pas confiance

Nous sommes conscientes que cela semble vraiment évident. Toutefois, 16% des personnes déclarent avoir envoyé des « sextos » à des étrangers, et il vaut donc la peine de le souligner.

Il est particulièrement important de ne pas envoyer de photos potentiellement compromettantes à une personne en laquelle vous n'avez pas entièrement confiance, car comme vous l'avez peut-être remarqué dans cette liste, **il n'existe pas de préservatif pour le « sexting » et il n'y a donc aucun moyen d'être totalement en sécurité.** Prenez donc vos précautions, et choisissez judicieusement vos partenaires de « sexting ».



Attaques IRL (« In Real Life », soit dans la vraie vie)

Bien sûr, les femmes ne sont pas uniquement agressées en ligne. Souvent, les attaques se poursuivent dans le monde réel, les auteurs utilisant la technologie pour les aider à traquer et à abuser leurs victimes. D'ailleurs, une enquête auprès des associations d'aide aux victimes a révélé que 79% d'entre elles aidaient des victimes qui avaient été surveillées via les réseaux sociaux.

Parfois, les auteurs sont des personnes que nous connaissons, par exemple un **partenaire dominant.** D'autres fois, les attaques sont des **crimes d'opportunité**, comme par exemple le fait de voler un téléphone portable, ou profiter de quelqu'un qui est simplement au mauvais endroit au mauvais moment.

Dans tous les cas, vous pouvez prendre des précautions pour rester en sécurité, y compris informer un ami de vos déplacements, crypter les données sur vos dispositifs mobiles ou encore conserver vos mots de passe en sécurité.

Comment utiliser une application de covoiturage en toute sécurité

En 2014, une habitante de New Delhi a été violée par son chauffeur Uber. Après qu'il ait été révélé que le conducteur avait un casier judiciaire chargé, comprenant en outre des agressions sexuelles,

certains ont demandé que l'application de covoiturage soit totalement interdite.
Après avoir connu une mauvaise passe, Uber a maintenant un nouveau PDG. Et **il semble que l'entreprise soit enfin prête à prendre la sécurité des passagers au sérieux** en lançant de nouvelles initiatives.
La principale, qui a déjà été implémentée, vous permet de partager votre trajet avec jusqu'à cinq contacts de confiance. Cela signifie que **vos amis peuvent suivre votre trajet et s'assurer que vous êtes arrivée à destination.** Si vous le souhaitez, vous pouvez également définir la fonction de contacts de confiance pour qu'elle soit uniquement activée pour les trajets nocturnes.
Les contacts de confiance sont similaires à la fonctionnalité Send ETA de Lyft, qui vous permet d'envoyer votre itinéraire et l'heure d'arrivée prévue à un ami. **Pour Uber et Lyft, ces messages comprennent la marque et le modèle de la voiture, le numéro de la plaque d'immatriculation et une photo du conducteur.**
Une fonction 911 est également déjà testée aux USA depuis mai 2018 et devrait être mise en place en France via un bouton d'urgence virtuel sur l'application. Les autres initiatives prévues par Uber comprennent une vérification des antécédents du conducteur et des analyses des bases de données concernant les infractions routières et la conduite en état d'ivresse.
En attendant, voici certaines étapes à suivre pour rester en sécurité.

5 façons de vous protéger en utilisant une application de covoiturage

1. **Assurez- vous qu'il s'agit bien du bon véhicule**

Avant de monter, vérifiez la plaque d'immatriculation, la marque et le modèle de la voiture, ainsi que le nom et la photo du conducteur pour vous assurer que tout correspond.

2. **N'indiquez pas à votre conducteur si votre lieu de prise en charge ou votre destination est votre domicile ou votre lieu de travail**

Le cas échéant, vous pouvez glisser un petit mensonge dans la conversation pour le mettre sur une fausse piste. Par exemple, s'il vous demande comment vous allez, vous pouvez lui dire « très bien, j'ai hâte de retrouver mes amis ». Une autre option est de lui indiquer un endroit à proximité comme destination plutôt que votre adresse exacte, quitte à devoir marcher un peu.

3. **Consultez les évaluations de votre chauffeur**

L'une des fonctionnalités intéressantes des applications de covoiturage est qu'elles permettent aux passagers d'évaluer leurs chauffeurs. Si le vôtre a de mauvaises évaluations, annulez le trajet et réservez-en autre. Pour éviter d'avoir à attendre trop longtemps, installez plusieurs applications sur votre téléphone afin de pouvoir utiliser celle qui vous permettra d'obtenir rapidement un chauffeur avec une bonne réputation.

4. **Contrôler l'itinéraire**

Si vous connaissez la région, vous remarquerez vite si le chauffeur ne va pas dans la bonne direction. Mais dans le cas contraire,

ouvrez l'application « carte » de votre téléphone et suivez votre itinéraire pour vous assurer que vous vous dirigez vers la destination que vous avez demandée. Si l'itinéraire vous semble étrange, faites-en part au chauffeur.

5. **Si quelque chose vous semble suspect, sortez**

Oui, vous serez peut-être en retard à votre rendez-vous, et vous perdrez peut-être quelques euros, mais si vous vous sentez en danger, demandez au conducteur de s'arrêter et sortez de la voiture. **Trop souvent, les femmes se retrouvent dans des situations dangereuses car elles ont honte de suivre leur instinct qui leur dit de fuir.** Oubliez cette idée.

Que faire si votre téléphone est perdu ou volé ?

Nous sommes nombreuses à avoir l'impression que toute notre vie se trouve sur nos téléphones. Nos téléphones contiennent nos contacts, nos photos et les applications que nous utilisons pour naviguer sur internet, suivre l'actualité, organiser notre travail et nos plannings personnels et rester en contact avec nos amis et proches ; c'est **beaucoup d'informations personnelles, et nous ne voulons pas qu'elles atterrissent entre les mains d'un étranger.** Heureusement, vous pouvez prendre quelques mesures simples pour vous protéger si votre téléphone est perdu ou volé.

4 façons de protéger le contenu de votre téléphone

1. **Protégez votre téléphone avec un mot de passe**

Afin d'empêcher quelqu'un d'accéder au contenu de votre téléphone une fois en sa possession, il est judicieux de définir un mot de passe.

La manière exacte de définir un mot de passe varie en fonction de votre dispositif, mais pour Android, vous devrez probablement aller dans Paramètres>Sécurité>Type de verrouillage d'écran. Vous pourrez ensuite choisir de déverrouiller votre téléphone en utilisant un motif, un code PIN ou un mot de passe.

Un mot de passe est l'option la plus sécurisée, mais c'est également la moins pratique car vous devrez le saisir à chaque fois que vous voulez jeter un œil à vos notifications Facebook. Vous avez peut-être également la possibilité de configurer votre téléphone pour qu'il se débloque uniquement avec votre empreinte digitale.

Le blocage intelligent (« smart lock ») est une autre fonctionnalité intéressante. Si vous l'utilisez, votre fonction de verrouillage ne s'activera pas tant que votre téléphone est sur vous, si vous vous trouvez à certains endroits (par exemple chez vous) ou à proximité d'autres dispositifs de confiance. Certains téléphones proposent même des options de reconnaissance vocale et faciale.

2. **Localisez votre téléphone**

L'un des gros avantages d'avoir un GPS sur votre téléphone est que s'il disparaît, vous pourrez savoir où il se trouve. **Toutefois, pour que cette fonctionnalité soit activée, vous devez la configurer à l'avance.**

Si vous avez un Android, plusieurs options sont à votre disposition. Certains dispositifs, comme les Samsung, ont cette fonctionnalité intégrée, bien que vous deviez créer un compte Samsung pour y avoir accès. En activant cette fonctionnalité, vous pourrez localiser votre téléphone en accédant à https://findmymobile.samsung.com/ depuis un autre appareil et en vous connectant. Une autre option consiste à télécharger **l'application Find My Device sur Google Play Store**. Cette application fonctionne de la même manière que Samsung et requiert uniquement un compte Google. De plus, si vous avez simplement égaré votre téléphone chez vous, elle peut le faire sonner, même si votre téléphone est en mode silencieux. Rendez-vous simplement sur https://myaccount.google.com/intro/find-your-phone, connectez-vous et vous pourrez voir la localisation

de votre téléphone sur une carte. Vous pourrez également réinitialiser le mot de passe de votre téléphone.
Toutefois, gardez à l'esprit que si vous avez un Android, **vous pourrez uniquement localiser votre dispositif si vos services de localisation sont activés et que vous êtes connectée à Internet.** Un voleur avisé saura désactiver ces fonctions afin que vous ne puissiez pas savoir où il se trouve (avec votre téléphone).
Si vous avez un iPhone, vous pouvez télécharger l'application Find My iPhone. Une fois installée, vous pourrez localiser votre téléphone sur une carte. Si vous n'avez pas l'application, vous pouvez aussi retrouver votre smartphone en vous rendant sur https://www.icloud.com/#find et en vous connectant à l'iCloud.
Vous pourrez aussi y configurer votre téléphone en Mode Perdu, ce qui le verrouillera. Le Mode Perdu vous permet également de définir un message sur l'écran verrouillé. Si vous avez simplement égaré votre téléphone, vous pouvez écrire quelque chose comme : « Téléphone perdu. Merci de contacter le 06 91 xx xx xx pour le restituer ». Si vous savez que votre téléphone a été volé, vous pouvez écrire quelque chose comme : « Vous êtes vraiment nul. »

3. Effacez vos données

Il s'agit de l'option la plus radicale. Si vous êtes sûre de ne pas récupérer votre téléphone, vous pouvez **utiliser les applications Find My Device/Find My iPhone pour effacer à distance toutes les données de votre téléphone.** Vous pouvez également effacer le contenu de votre iPhone depuis iCloud. Ainsi, même si le voleur parvient à contourner les protections de votre mot de passe, il ne sera pas en mesure d'accéder à vos informations personnelles.
Gardez à l'esprit qu'en faisant cela, vous **perdrez votre capacité à suivre votre téléphone à distance étant donné que vos comptes personnels seront supprimés.**
Cela dit, votre abonnement téléphonique sera peut-être encore activé, ce qui signifie que la personne qui détient votre téléphone est susceptible de passer des appels à partir de votre numéro et d'utiliser votre forfait de données. Pour résilier votre abonnement, **contactez votre fournisseur de services en lui indiquant que votre téléphone a été volé.**
Le fait de savoir que vous pourriez un jour avoir à supprimer les données de votre téléphone est une autre bonne raison de **sauvegarder le contenu de votre téléphone** (ce que vous devriez faire de toute façon). Si vous possédez un dispositifs Android, le

moyen le plus simple de sauvegarder vos données est d'utiliser le Google cloud. Si vous avez un iPhone, utilisez l'iCloud.
Mais que faire si vous n'avez pas installé les applications Find My Device/Find My iPhone à l'avance, si vous n'êtes pas sur iCloud, et que vous ne pouvez plus changer vos mots de passe, verrouiller votre téléphone ou effacer vos données à distance ? Le cas échéant, vous devriez…

4. **Modifier les mots de passe de toutes vos applications**

Faites une liste de toutes les applications de votre téléphone qui nécessitent des mots de passe, connectez-vous sur un autre appareil et commencez à modifier vos mots de passe. Cela comprendra probablement vos comptes e-mail, de réseaux sociaux, bancaires et app stores.

Utiliser Meetup.com en toute sécurité

L'une des choses formidables à propos d'Internet, c'est sa capacité à rassembler des inconnus qui ont quelque chose en commun, mais qui ne se seraient jamais rencontrés autrement.
C'est même la spécialité du site Web Meetup.com, qui permet aux utilisateurs de **créer et de participer à des événements et activités en fonction des thèmes qui les intéressent.** Les catégories populaires de meetups comprennent le cinéma, la santé et le bien-être, LGBTQ et les animaux de compagnie. C'est un moyen fantastique de se faire de nouveaux amis selon vos centres d'intérêts.
Sauf que… votre maman vous a toujours dit de ne pas parler aux étrangers, n'est-ce pas ? Avait-elle raison, ou était-elle juste paranoïaque ?
Un peu des deux. Vous devez sortir et profiter de la vie… à condition de prendre quelques précautions.

3 façons de vous protéger sur Meetup.com

1. **N'indiquez pas trop d'informations personnelles sur votre profil**

Soyez consciente que votre page de profil est entièrement accessible à toute personne ayant accès à Internet. Par conséquent, veillez à inclure uniquement des informations que vous considérez comme publiques.
Si vous êtes passionnée de gastronomie et que vous vous avez hâte de trouver des meetups culinaires dans votre ville, vous pouvez mentionner votre resto préféré sans aucun problème. Mais

n'indiquez pas qu'il se trouve juste devant votre immeuble au 33 rue des Peupliers, où vous résidez dans l'appartement 4D qui, d'ailleurs, n'a pas de verrou.
Ou si vous recherchez des rencontres familiales, vous pouvez indiquer que vos enfants ont six et dix ans, mais n'ajoutez pas qu'ils appellent Manon et Thomas, qu'ils vont à l'école Jacques Prévert, et qu'ils reviennent seuls à pied tous les jours à 16h30.

2. **Rencontrez les gens dans la vie réelle avant de communiquer en privé**

Meetup dispose d'un système de transfert d'e-mails, de sorte que vous pouvez recevoir des messages de membres envoyés à votre adresse e-mail sans qu'ils voient cette dernière.
Toutefois, si ne souhaitez pas que les personnes vous contactent avant de vous rencontrer en personne, vous pouvez **choisir de bloquer les messages des utilisateurs** et de recevoir uniquement les messages des organisateurs d'événements. Accédez simplement à votre compte et cliquez sur Paramètres>Confidentialité.
Vous **pouvez également choisir si vous souhaitez que vos groupes ou intérêts apparaissent sur votre profil.** Enfin, vous pouvez sélectionner qui peut vous contacter sur Meetup, que ce soit simplement les organisateurs, les membres de vos meetups ou n'importe quel visiteur du site.

3. **Informez un ami du lieu de rendez-vous**

Pour toutes les situations dans lesquelles vous allez rencontrer des étrangers, c'est une bonne habitude de dire à un ami où vous allez, et de décider d'une heure pour l'informer que vous êtes rentrée chez vous en toute sécurité. En outre, **si le meetup inclut des boissons, ne laissez jamais la vôtre sans surveillance.**

Prévenir les violences conjugales

En France, en 2016, 74 628 femmes ont porté plainte pour violences conjugales. Sachant que seules 14% des victimes de violence conjugale portent plainte, cela donne une idée de l'ampleur du phénomène. Pire, une femme meurt tous les 3 jours sous les coups de son compagnon. Bien que la technologie puisse fournir des outils aux victimes (par exemple pour réunir des preuves contre un agresseur), elle peut malheureusement aussi être utilisée par les auteurs. En effet, le contrôle fait partie intégrante de la violence conjugale, et **le mauvais usage de la technologie peut**

donner aux agresseurs un moyen d'exercer un contrôle sur leurs victimes.

Selon une étude récente, bien que de nombreux auteurs de violence utilisent une technologie spécialement conçue pour la surveillance, il est beaucoup plus courant d'utiliser d'autres types d'applications pour atteindre les mêmes objectifs. Certaines de celles utilisées comprennent **les applications qui permettent de retrouver son téléphone ou de savoir où sont les membres de sa famille.**

Le problème est que les organismes de lutte contre la violence conjugale ne peuvent pas se retourner contre les entreprises qui développent ces applications, et les app stores ne peuvent pas les bloquer car la plupart du temps, elles sont utilisées à des fins parfaitement légitimes.

Bon nombre de ces applications permettent aux agresseurs de **contrôler la localisation de leur victime, de lire ses messages** en les transférant vers un autre dispositif, et même de les **observer et de les écouter à distance** en activant la caméra et le micro du téléphone.

Comme mentionné ci-dessus, il existe également des **applications explicitement commercialisées pour la surveillance non consensuelle.** Bien qu'il soit rare de les trouver sur un app store officiel, elles sont facilement disponibles ailleurs sur Internet. Et même si la plupart des téléphones sont dotés d'un paramètre par défaut qui bloque les applications non disponibles dans les app stores, il est facile de trouver des guides en ligne pour contourner les blocages.

L'un des éléments les plus néfastes de ce type d'applications est qu'elles peuvent généralement être configurées pour que l'icône de l'application soit masquée, ce qui rend **presque impossible pour la victime de la détecter sur son téléphone.**

Vous pensez peut-être que la solution est de scanner le téléphone pour détecter les logiciels espions, mais malheureusement, même certains des plus grands noms du secteur, tels que Symantec, Kaspersky, et Avast, se sont révélés inefficaces dans la détection de ces applications.

Alors, que pouvez-vous faire pour vous protéger ?

3 façons d'empêcher un partenaire abusif de vous surveiller

1. **Gardez votre téléphone sur vous à tout moment**

Pratiquement toutes les applications examinées requièrent que l'agresseur ait physiquement accès au téléphone de la victime au moins une fois.

2. **Soyez prudente lors de l'utilisation d'un téléphone que vous n'avez pas acheté vous-même**

Les agresseurs qui exercent un puissant contrôle sur leurs victimes contrôlent souvent leur argent également, et ce sont eux qui leur achètent leur téléphone. Le cas échéant, ils peuvent non seulement préinstaller des applications, mais avec quelques connaissances technologiques, ils peuvent même « rooter » (ou « jailbreaker ») l'appareil, ce qui leur permet d'installer les applications les plus néfastes non disponibles sur les app stores. Certaines entreprises commercialisent même des téléphones déjà « rootés », ou avec un logiciel de surveillance préinstallé.

3. **Protégez votre téléphone avec un mot de passe, et n'en faites part à personne**

Comme mentionné ci-dessus, un mot de passe pour verrouiller votre téléphone est la première ligne de défense pour garantir la sécurité de son contenu. Si vous pensez que votre partenaire accède à votre appareil, modifiez immédiatement votre mot de passe. Choisissez un mot de passe long et complexe, et assurez-vous de ne pas utiliser d'éléments qu'il est susceptible de deviner, comme votre anniversaire ou le nom de votre animal de compagnie.

Cela dit, nous ne sommes pas naïves et ne pouvons ignorer la réalité que de **nombreuses victimes de violence conjugable sont forcées de révéler leurs mots de passe** ou de « permettre » l'installation de ces applications dangereuses sur leurs téléphones.

Que vous soyez ou non en mesure de protéger votre dispositif, **si vous êtes victime de violence conjugale, il existe des ressources qui peuvent vous aider à vous en sortir.** Voici certains des organismes consacrés à l'assistance aux victimes :

Le 39 19 : Un service spécialisé dans les violences faites aux femmes. Il ne traite pas les situations d'urgence.

Réseau France victimes : Réseau associatif professionnel engagé au service des victimes et du lien social. http://www.france-victimes.fr/.

CNIDFF : Centre d'information sur les Droits des Femmes et des Familles. http://www.infofemmes.com/v2/p/Contact/Liste-des-CIDFF/73

08 victimes : Écoute, informe et conseille les victimes d'infractions ainsi que leurs proches. **+33 (0)1 41 83 42 08**

Applications de secours

En général, c'est une bonne idée d'avoir une application d'urgence sur votre téléphone, juste au cas où. Ces dernières vous permettent de **prévenir vos amis ou proches lorsque vous vous sentez en danger** et/ou de contacter les **services d'urgence.**

Certains types de téléphones intègrent ces fonctionnalités, il vaut donc la peine de vérifier si c'est le cas du vôtre. Dans le cas contraire, voici une application disponible sur pour Android et iOS. ICE GéoAlert, qui signifie In Case of Emergency = En cas d'urgence, vous permet **d'envoyer un message d'alerte et votre position GPS aux contacts sélectionnés** lorsque vous voulez que vos amis ou proches sachent qu'il vous est arrivé quelque chose. Vous pouvez même signaler rapidement s'il s'agit d'un accident, d'un malaise, ou d'une agression. Votre trajet sera également retracé par l'application. Il existe aussi un mode « tracking » qui permet d'envoyer une alerte si vous n'êtes pas arrivée à bon port à l'heure prévue, après une randonnée ou une sortie en ville par exemple.

Vous pouvez également **afficher certaines informations sur votre écran de verrouillage** dans le cas où vous ne seriez pas en mesure de fournir des informations vous concernant aux services d'urgence. Par exemple, « En cas d'urgence, merci d'appeler [nom de votre partenaire] », suivi de son numéro de téléphone. Ou, si vous avez souffrez d'un problème médical spécifique, comme d'une allergie sévère ou d'épilepsie, vous pouvez y inclure ces informations pertinentes.

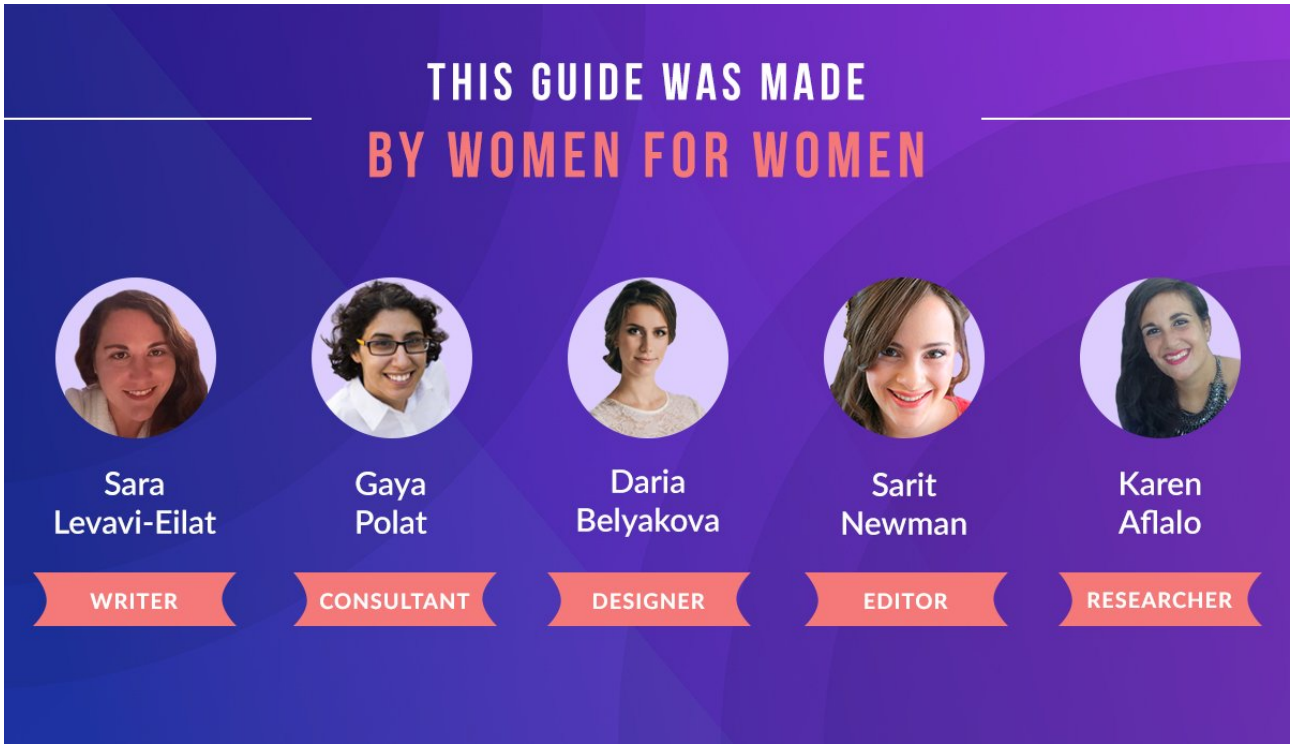
La façon de définir un message d'écran de verrouillage dépend du modèle de votre téléphone.

Conclusion

La technologie et l'Internet jouent un grand rôle dans nos vies, pour le meilleur et pour le pire. En tant que femmes, nous sommes des cibles potentielles pour de nombreuses raisons, mais cela ne signifie pas que nous devons rester passives ni que nous devons nous déconnecter.

Nous espérons que ce guide vous permettra de vous protéger et de vous défendre en ligne et dans la vraie vie, et que les outils fournis vous aideront à le faire.

Si vous avez trouvé ce guide utile de quelque façon que ce soit, n'hésitez pas à le partager avec d'autres afin que davantage de femmes puissent apprendre comment rester en sécurité, à la fois sur et en dehors du Web.



* Certains noms et informations d'identification ont été modifiés dans un souci de protection de la vie privée des individus.

Source : https://fr.vpnmentor.com/blog/le-guide-de-la-securite-internet-pour-les-femmes/