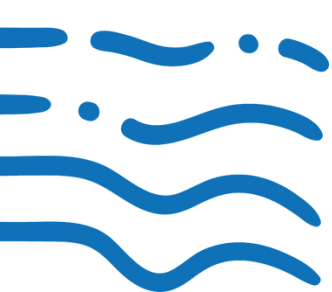


Guide pour se protéger des cyber- violences





Qu'est-ce qu'il y a dans ce guide ?

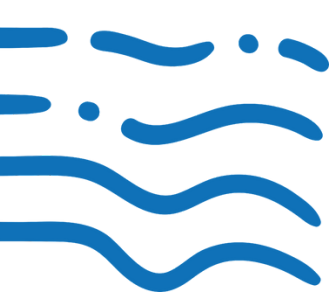
I. Contexte	3
1. Pourquoi ce guide ?	4
2. Qui sommes-nous ?	5
II. De quoi parle-t-on ?	7
1. Violences et cyber-violences	8
2. Harcèlement et cyber-harcèlement	9
3. Expression de cyber-violences	11
4. Signes de mal-être	13
III. Que peut-on faire ?	14
1. Se sentir en sécurité en ligne	15
2. Les bons réflexes avec Mémo de vie	19
IV. Et maintenant ?	21
1. Résumé et premiers pas	22
2. Ressources boussole	23
3. Services d'aide	24



I. Contexte

Pourquoi ce guide ?.....	4
Qui sommes-nous ?.....	5
Comment utiliser ce guide ?.....	6





Pourquoi ce guide ?

Internet, les écrans, les réseaux sociaux font partie de notre quotidien. Ce sont des outils qui nous accompagnent à travers les différentes sphères de la vie (sociales, familiales, administratives, médicales, scolaires, académiques, professionnelles..) et dont il est important de parler afin de pouvoir choisir comment les utiliser, avec conscience et sécurité.

Pourquoi parler de “cyber” violence ?

Les cyber-violences sont les violences qui se déroulent dans les espaces numériques et/ou via des outils digitaux. Certaines de ces violences sont transposées directement du monde physique dans le monde digital (ex : insulte par texto) tandis que d'autres émergent spécifiquement de ce que la technologie numérique permet notamment via les IA génératives (ex : deep fake, deep nudes).

Ces violences ont des spécificités propres à garder en tête pour pouvoir à la fois les prévenir et y réagir. L'interposition d'un écran, l'impression d'éloignement et l'absence de communication kinésique limitent le niveau d'empathie des auteurs, qui ne sont pas nécessairement confrontés aux effets de leurs actes sur la personne ciblée. Les capacités d'adaptation de la victime sont également réduites. N'étant parfois pas certaine de l'identité de son ou ses agresseur(s), elle peut se trouver en situation de déséquilibre de pouvoir et ressentir un sentiment d'impuissance accru couplé à une impression de non-recours et d'impunité.

Les cyber-violences peuvent avoir de graves impacts sur le court et le long termes, des incidences aussi bien sur la santé physique et mentale des individus que sur l'équilibre sociétal, la vie en ligne étant aujourd'hui indissociable de la vie physique.

Dans des contextes d'intimité, de relation amoureuse ou de couple, la violence peut également s'exercer par des moyens numériques ; ce sont autant d'opportunités de contrôle, de manipulation et autres abus. Il est alors spécialement important de comprendre les possibilités de fonctionnement de ces outils pour trouver des façons de vivre en ligne le plus en sécurité possible.

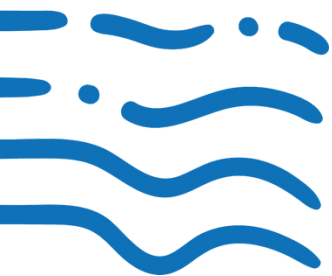
C'est pour accompagner, informer et transmettre de bonnes pratiques autour des situations de cyber-violences que Mémo de Vie et Respect Zone s'associent dans la création de ce guide.



Pour qui est ce guide ?

Pour toutes personnes victimes, proches ou témoins de cyber-violence, que ce soit dans la sphère privée ou bien dans un contexte professionnel ou scolaire.

Pour MIEUX comprendre le sujet des cyber-violences et reprendre du pouvoir avec ces outils afin de MIEUX se protéger et (ré)agir.



Qui sommes-nous ?

France Victimes

La fédération France Victimes, fondée en 1986, regroupe 130 associations d'aide aux victimes agréées par le ministère de la Justice. Ces associations, composées de professionnels (juristes, psychologues, travailleurs sociaux), offrent accueil, écoute, aide psychologique, information juridique et accompagnement social aux victimes d'atteintes personnelles ou matérielles.

France Victimes administre le 116 006, la plateforme téléphonique nationale d'aide aux victimes.

Elle propose également des formations spécialisées pour son réseau et ses partenaires. Avec plus de 1 350 lieux d'accueil, les services sont gratuits et confidentiels, garantissant l'autonomie et la liberté des victimes.

La plateforme Mémo de Vie offre un espace digital sécurisé pour les victimes de violences répétées, accessible via téléphones, tablettes et ordinateurs.

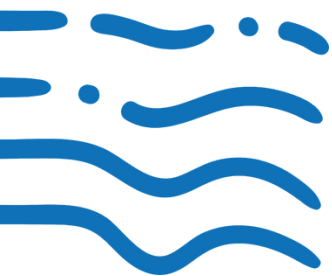
Respect Zone

Association 1901 créée en 2014, Respect Zone œuvre pour la protection des personnes dans l'espace numérique. Elle soutient l'exercice d'une liberté d'expression responsable et la participation engagée de tous à créer un environnement de respect en ligne. Elle mobilise et sensibilise les internautes aux cyber-violences, au cyber-harcèlement et à la haine en ligne.

Héritière des grands combats pour l'acceptation des différences, l'association entend asseoir la notion de dignité numérique tout en développant des outils de prévention positifs comme le label et la charte Respect Zone.

Elle utilise le droit et l'éducation pour agir positivement sur ces enjeux sociétaux en intervenant auprès de différents publics pour les sensibiliser et les former.

Grâce à sa Clinique Juridique, son Cercle des Juristes et ses réseaux partenaires, l'association participe à des chantiers législatifs et offre une aide juridique aux victimes. L'application Respect Zone, accessible gratuitement, est un de ses derniers outils développés pour accompagner les personnes en situation de cyber-violence, qu'elles soient cibles, témoins ou autrices.



Comment utiliser ce guide ?

Le but de ce guide est de vous aider à mieux **comprendre le sujet des cyber-violences** pour pouvoir les reconnaître, savoir y réagir si elles ont lieu et mettre en place des mesures de protection dès maintenant. Que vous soyez directement concerné ou que vous cherchiez à aider un proche, vous pouvez y trouver des outils pour prévenir ces abus et y (ré)agir.

Pour pouvoir être accessible à tous et s'assurer que l'on comprenne les mêmes choses, nous avons inclus des explications sur des notions clés liées au large sujet des violences. C'est une question complexe, les définitions ne sont pas figées et les informations ne sont pas exhaustives mais nous proposons ces repères comme un cadre utile pour comprendre les cyber-violences.

Voici ce que vous trouverez dans ce guide :

- 1 - Les points d'attention concernant l'usage des outils numériques, notamment en situation de violence
- 2 - Des idées d'actions pour prévenir et (ré) agir aux cyber-violences
- 3 - Des services d'aide spécialisés pour demander du soutien ou une prise en charge
- 4 - D'autres ressources pour approfondir votre compréhension du sujet des violences en ligne

Soyez libre de prendre ce qui vous aide et de l'adapter selon ce qui a du sens pour vous.

Notre souhait est en tout cas de proposer des actions concrètes à mettre en place dès la lecture de ce guide.



Nous n'avons pas besoin d'être des experts du numérique, ni d'être nous-mêmes des pratiquants, pour pouvoir comprendre le sujet et mettre en place (ou aider à mettre en place) de bons réflexes de sécurité. Comme pour toute chose, le plus important est de se poser des questions et chercher une réponse adaptée !



II. De quoi parle-t-on ?

Violences et cyber-violences.....	8
Harcèlement et cyber-harcèlement.....	9
Expressions de cyber-violence.....	11
Signes de mal-être.....	13





Violences et cyber-violences

Violences

Nous entendons par violence le fait de “faire mal” et cela peut prendre différentes formes :

- **verbale** (insulte, moquerie, dénigrement)
- **non verbale** (grimace, imitation, geste obscène)
- **psychologique** (propagation de rumeur, processus d'isolement, pression, contrainte, chantage)
- **et/ou physique** (coup, restriction, attouchement, viol, menace).



Les **micro-violences** sont des “petites” violences ordinaires, dans le sens où elles sont imperceptibles, invisibles, silencieuses, diffuses. Elles peuvent être petites, nombreuses, multifformes et sont souvent banalisées, normalisées.

Ex : nier ou invisibiliser notre contribution à une tâche, remettre en question notre force ou capacité à faire quelque chose, ne pas être consulté pour un choix qui nous concerne...

Dans un contexte d'intimité, de relation amoureuse ou de couple :

Il peut être spécialement difficile de se rendre compte des violences que l'on vit.

Le **contrôle coercitif** est une forme continue de violence relationnelle caractérisée par des micro-violences quotidiennes. Cela passe par l'utilisation de techniques de manipulation, domination et contrôle, incluant l'isolement social, la surveillance, les menaces, les humiliations et le contrôle des finances. L'agresseur peut avoir recours à la force et/ou la privation pour que la victime lui obéisse, la rendre dépendante et lui ôter son sentiment de liberté dans la relation.

Pour en savoir plus, rendez-vous page 11

Cyber-violences

Ce sont **l'ensemble** des violences

Menace, injure, insulte, exclusion, prise ou partage d'image ou d'information privée sans le consentement, photo-montage, intimidation, incitation à la violence, usurpation d'identité, etc... tout acte portant atteinte à la dignité d'une personne ou d'un groupe de personnes

qui se déroulent dans un **espace digital et/ou avec des outils numériques**.

Différents formats (texte, image, photographie, vidéo, audio..) et différents moyens (téléphone, messagerie instantanée, forum, chat, jeu en ligne, courrier électronique, réseau social, application, site de partage de photographies..) peuvent être employés.



Harcèlement et cyber-harcèlement

Le harcèlement est de la **répétition de violences**, par une ou plusieurs personnes ; intensive, graduelle ou régulière ; pouvant survenir dans toutes sphères de la vie.

Quand il est commis “par l'utilisation d'un service de communication [...] en ligne ou par le biais d'un support numérique ou électronique” (art.222-33-2-2 code pénal), on parle de cyber-harcèlement.

Le harcèlement peut combiner les différentes formes de violence déjà citées. Parmi les éléments spécifiques à une dynamique de harcèlement, l'on retrouve la répétition mais aussi le déséquilibre de pouvoir entre la victime et l'agresseur.



Quand on traite un mal-être, le point de vue qui importe est celui de la victime ; peu importe si l'auteur n'a pas eu conscience de son impact ou n'a agi qu'une seule fois TANT que cela nuit à la victime. Cela peut être le cas dans le "harcèlement de meute" ou raid numérique.

Envoyer des insultes par message et commenter les publications de son ex-partenaire, lui suscitant angoisse et auto-censure



Le cyber-harcèlement (art.222-33-2-2 code pénal) est puni de peines pouvant aller jusqu'à **2 ans d'emprisonnement et 30 000 € d'amende**.

Si vous avez - de 15 ans, la peine peut être de **3 ans et 45 000 €** (art.222-33-2-2 code pénal).

Si le harcèlement moral et le cyber-harcèlement viennent d'un actuel ou ex partenaire, la peine peut aller jusqu'à **5 ans d'emprisonnement et 75 000 €** (art. 222-33-2-1 code pénal).

Si le harcèlement est à caractère sexuel, la peine peut aller jusqu'à **3 ans et 45 000 €** (art. 222-33 code pénal).



Le cyber-sexisme



Le sexisme peut s'exprimer par des paroles et attitudes préjudiciables, discriminatoires et/ou violentes envers des personnes en raison de leur sexe et leur genre. En ligne, on parle de "cyber-sexisme".

Ex : commentaire de dénigrement physique, envoi de photo de partie génitale (dick pic), menace de diffusion d'image intime, groupe de partage de photo-montage pornographique, comportement visant à exclure les femmes d'un espace en ligne..

SLUT SHAMING "honte à la salope"

Forme de dénigrement, qui consiste à dévaloriser la personne dont la tenue vestimentaire, le maquillage, l'attitude, voire les activités sexuelles, ne correspondent pas aux normes en vigueur dans un groupe de personnes.

VICTIM BLAMING "blâmer la victime"

Tenir partiellement ou entièrement responsable une victime de ce qu'elle a subi.



Le "slut shaming", le "victim blaming" peuvent être des formes de cyber-violences participant à du cyber-harcèlement.

Reprocher à une femme qui porte un décolleté de ne pas avoir un comportement professionnel

Dire que c'est normal de se faire insulter si on poste une photo de soi en maillot de bain



Expressions de cyber-violence

Il existe différentes formes de cyber-violences, en voici des exemples.

LES CYBER-VIOLENCES QUI TOUCHENT À LA VIE PRIVÉE

Porter atteinte à la vie privée signifie mener des actions qui nient le droit d'une personne à préserver ses **informations personnelles et ses activités privées**.



C'est une **infraction** (art. 266-1 code pénal) qui peut être punie de **2 ans d'emprisonnement et 60 000 € d'amende** si elle est commise par un ex ou actuel partenaire car il s'agit d'une circonstance aggravante.

Des exemples en ligne :

DOXING

Transmettre des informations sur une personne qui permettent de l'identifier ou de la localiser, dans le but de lui nuire, elle ou ses membres de famille.

infraction punissable de 3 ans d'emprisonnement et de 45 000 € d'amende (art. 223-1-1)

OUTING

"extérioriser"

Révéler des informations confidentielles sur une personne sans son consentement.

infraction punissable de 1 an d'emprisonnement et de 45 000 € d'amende (art. 226-1)

USURPATION D'IDENTITÉ

Toute action qui consiste à utiliser les informations personnelles d'une personne pour se faire passer pour elle.

infraction punissable de 1 an d'emprisonnement et de 15 000 € d'amende (art. 226-4-1)

Publier le numéro de téléphone ou l'adresse d'une personne

Faire un post dévoilant l'orientation ou les pratiques sexuelles d'une personne

Créer un compte au nom et à l'image d'une personne pour se faire passer pour elle

Dans un contexte d'intimité, de relation amoureuse ou de couple :

- vérifier la communication de son/sa partenaire (texto, appel, message, e-mail...)
- utiliser les appareils et comptes sans l'accord de son/sa partenaire
- monitorer les déplacements de son/sa partenaire (géolocalisation)
- empêcher que son/sa partenaire communique (contrôler ce qui est dit et à qui, confisquer les appareils, changer les mots de passe)
- se faire passer pour sa partenaire en vue de lui nuire socialement, professionnellement etc.

Ces cyber-violences peuvent être des faits constitutifs de harcèlement moral qui est punissable de **3 à 5 ans d'emprisonnement et de 45 000 à 75 000 € d'amende** dans le cadre du couple (art. 222-33-2-1).

LES CYBER-VIOLENCES QUI TOUCHENT À L'IMAGE

Porter atteinte à l'image d'une personne signifie mener des actions qui nient son droit à contrôler l'utilisation de son image. Cela inclut la publication ou l'utilisation de photos ou vidéos sans le consentement de la personne dont c'est le corps.



C'est une **infraction** (art. 266-1 code pénal) qui peut être punie de **2 ans d'emprisonnement et 60 000 € d'amende** si elle est commise par un ex ou actuel partenaire car il s'agit d'une circonstance aggravante.

DIFFUSION D'UN PHOTOMONTAGE

Diffuser, publiquement (ex : site internet) ou en privé (ex : groupe de messagerie), un montage (son, image..) sans le consentement de la personne qui y figure et sans indiquer qu'il s'agit d'un montage.

Envoyer ou publier une photo d'un animal mort avec le visage d'une personne collé dessus

infraction punissable de 2 ans d'emprisonnement et de 45 000 € d'amende (art. 226-8) si à caractère sexuel : 2 ans et 60 000 € d'amende, et 3 ans et 75 000 € s'il s'agit d'un deepfake (art. 226-8)

DIFFUSION DE CONTENU INTIME NON CONSENTIE

Diffuser, publiquement (ex : sur les réseaux) ou en privé (ex : par messagerie), un contenu intime sans le consentement de la personne qui y figure, y compris à son insu, c'est-à-dire que le contenu est enregistré (ex : photo prise en cachette) ou partagé sans que la personne en ait connaissance.

Partager un nude de son/sa partenaire sans son accord OU d'une personne à son insu

infraction punissable de 2 ans d'emprisonnement et de 60 000 € d'amende (art. 226-2-1)



Un contenu intime peut être une photo, une vidéo, un texte, un audio. Un "nude" (=nu) désigne une photo nue ou dénudée, suggestive ou sexuellement explicite.

Dans un contexte d'intimité, de relation amoureuse ou de couple :

- imposer de prendre ou de recevoir des contenus intimes
- conserver ou diffuser des contenus intimes sans consentement
- diffuser ou menacer de diffuser des contenus intimes

Ces cyber-violences peuvent être des faits constitutifs du délit renforcé d'atteinte à la vie privée (atteinte à l'image) qui est punissable de **2 ans d'emprisonnement et de 60 000 € d'amende** cf ci-dessus. Et même d'agressions sexuelles (art. 222-28) si la personne est forcée à filmer des actes sexuels.



Signes de mal-être

Les cyber-violences peuvent avoir des conséquences sur les individus qui sont similaires aux violences ayant lieu dans le monde physique. Voici des exemples de signaux manifestés par une personne qui peuvent indiquer une situation de mal-être :

- Nervosité, angoisse, agressivité, irritabilité
- Perte d'estime de soi, perte de confiance en soi
- Changements radicaux dans son apparence, ses habitudes, ses humeurs, ses envies
- Baisse de résultats, de performance, de motivation
- Phobie scolaire/du travail, absentéisme, arrêt maladie
- Isolement
- Angoisse lors de consultation des réseaux sociaux/réception de messages, fréquentation augmentée des réseaux ou retrait total
- Maux de ventre/tête, perte de sommeil, trouble alimentaire, addictions
- Atteinte à son corps, envie de mourir, pensées morbides, tentative de suicide

Exemples de changements d'attitude qui peuvent alarmer dans un contexte d'intimité, de relation amoureuse ou de couple :

- changer sa photo de profile ou supprimer des photos parce que son/sa partenaire nous critique
- ne plus poster ce que l'on veut par crainte de ce que son/sa partenaire en dira
- être toujours connectée à son téléphone pour pouvoir répondre tout le temps et tout de suite à son/sa partenaire
- quitter les groupes de messagerie parce que son/sa partenaire n'en fait pas partie



Astuce Mémo de vie* : utiliser le journal pour raconter son vécu

Raconter et enregistrer les situations que l'on vit (positives comme négatives) le plus régulièrement possible permet de structurer les événements dans le temps et construire un récit cohérent. Le journal est consultable quand vous le souhaitez.

Renseigner ses émotions, ses humeurs permet de prendre du recul et peut être un signal d'alerte quant à la situation que vous traversez.

« Ça m'aide à prendre du recul pour analyser, puis une fois que l'événement est enregistré, on a dit les choses qui nous pesaient, on sait que c'est sauvegardé, donc c'est libérateur. Ça fait prendre conscience et c'est aussi un travail que je continue avec ma psychologue. » - une utilisatrice de Mémo de vie

***Qu'est-ce que c'est Mémo de vie ?**



La plateforme Mémo de Vie est destinée à toute personne victime de violences (sans distinction de genre, ni de sexe) ou en questionnement sur des situations de violence vécues, ainsi qu'aux proches et aux professionnels.

C'est une plateforme digitale, gratuite et sécurisée où l'on peut faire le suivi de ce que l'on vit, conserver des informations et documents, préparer des démarches, se renseigner et être accompagné par des professionnels.





III. Que peut-on faire ?

Se sentir en sécurité en ligne.....	15
Les bons réflexes avec Mémo de vie.....	19





Se sentir en sécurité en ligne

Une première question à se poser est : est-ce que je me sens en sécurité en ligne ?

Pour vous aider à y répondre, voici 3 questions :

1. Est-ce que je peux accéder librement aux outils numériques ?
2. Est-ce que j'ai le contrôle sur mes appareils, comptes et applications ?
3. Est-ce que je peux exister en ligne sans limite ou crainte ?

Si vous avez des doutes ou si vous répondez non à l'un ou plusieurs de ces 3 points, il peut être utile d'explorer pourquoi. La suite de ce guide propose des choses à faire pour se sentir plus en sécurité dans ses activités et plus à l'aise avec ses propres outils.



1

Accès libre

Avoir une adresse e-mail, des mots de passe et des comptes dont on est le seul à avoir accès.

Comme première étape de sécurisation, il vous faut une [adresse e-mail à laquelle seul vous avez accès](#), (elle vous est notamment nécessaire pour créer votre compte [Mémo de Vie](#) !) ainsi que des mots de passe dont vous seul avez connaissance.



*Si ce n'est pas le cas, vous pouvez en créer une depuis un **appareil jamais utilisé** (celui d'un proche, d'une bibliothèque ou d'un cyber-café) + sélectionner un moyen de récupération (autre adresse e-mail, numéro de téléphone ou question de sécurité) qui ne soit pas accessible à d'autres personnes que vous + choisir un mot de passe fort (voir ci-après) + se déconnecter dès que vous quittez l'appareil.*



Votre confidentialité et sécurité sur Mémo de Vie

Vos données sont sauvegardées par un hébergeur certifié et sécurisé en Europe. Vous pouvez optimiser ces mesures avec les conseils « Confidentialité & Sécurité » et ceux de l'article « Comment optimiser mes mesures de confidentialité et de sécurité sur [Mémo de Vie](#) ».

Votre historique est quasiment inexistant.

De plus, vous pouvez quitter [Mémo de Vie](#) à tout moment en cliquant sur

le bouton **Vite, je quitte** toujours en bas à droite de la page, bouton qui vous redirigera vers un autre site.

Bien choisir ses mots de passe



Choisissez des mots de passe complexes, différents et non-signifiants !
Ne les communiquez pas ! Même à votre partenaire ou autre proche. On sait que ce n'est pas évident et voici les 4 choses importantes à suivre :

1

Ils doivent être **forts** : + de 12 caractères (dont des majuscules, chiffres, minuscules et caractères spéciaux... Pas de suite de chiffres !)

2

Un **mot de passe différent pour chaque compte**, site et application. Ou au moins pas le même partout ! Vous pouvez utiliser un générateur de mots de passe et coffre-fort pour vous aider.

3

Ne jamais les écrire sur des post-it ou sur des documents accessibles sur vos appareils.

4

Ils **ne doivent pas avoir un rapport avec votre identité ou vos proches** (pas de nom, surnom, adresse, date d'anniversaire !)



Précision : quitter une app ou fermer une page est différent que se déconnecter ! La session peut encore être accessible sur ces appareils ou même en communication avec d'autres appareils connectés ou applications ouvertes. Pour empêcher que d'autres aient accès à votre compte ou session après vous, déconnectez-vous.

2

Contrôle de ses comptes et appareils

Vérifier quels appareils et quelles applications sont connectées à vos outils.

Vérifier qui a accès à vos comptes

Si vous utilisez des plateformes comme google ou microsoft, des smartphones et des objets connectés, vous pouvez aller vérifier dans la partie "compte" quels appareils et applications sont reliées et même actuellement connectées.

1

Si vous remarquez des connexions ou appareils connus ou inconnus : prendre une capture d'écran avec l'identification de l'appareil, date et heure.

2

Éjecter l'appareil pour révoquer l'accès (si c'est possible dans votre situation sans vous mettre en danger).

3

Désactiver la liaison avec d'autres applications si vous n'êtes pas sûres qu'elles sont sécurisées (ex : youtube).

4

Changer le mot de passe de votre compte.

5

Mettre en place une double authentification. Toute tentative de connexion nécessitera un code reçu par sms ou e-mail.

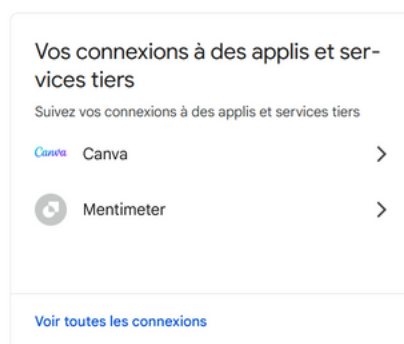
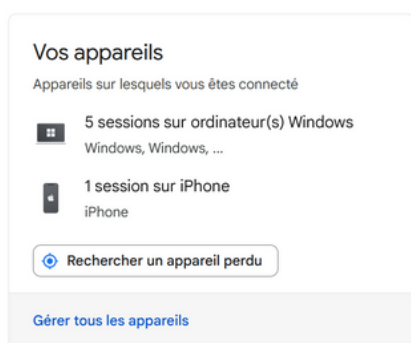
6

Mettre en place des fonctions qui vous alertent si un nouvel appareil tente de se connecter à votre compte.



Réfléchir à une variété de comptes que vous utilisez :

e-mail, liaison entre appareils (télévision, téléphone, tablette, ordinateur), comptes communs (banques, cartes de fidélité supermarché/magasins, service de livraison (nourriture, objet), taxi/service de transport, plateforme d'achat en ligne, etc).



Est-ce qu'il y a des logiciels ou des objets qui me surveillent ?

La surveillance électronique peut avoir lieu via des caméras, microphones, "mouchards" (ou appareils de mise sur écoute), réseaux sociaux ou e-mails. Cela peut aussi inclure l'abus de logiciels ou applications de surveillance installés sur un ordinateur, une tablette ou un smartphone pour suivre les activités de l'utilisateur. Des traceurs de localisation peuvent également être utilisés. Vous pouvez déjà faire un tour dans votre maison, bureau, voiture pour vérifier qu'il n'y a pas de trackers (ex : air tag).



Attention aux micros et aux caméras des ordinateurs, tablettes et smartphones qui peuvent être activés à distance par d'autres appareils connectés !

Pour des activités délicates : utiliser un appareil sécurisé, la navigation privée et effacer l'historique.

D'autres points d'attention :

- Téléchargement

Ne téléchargez des documents que lorsque vous êtes sur un appareil sécurisé et dans un espace temps où vous vous sentez en sécurité. Les charger dans Mémo de Vie. Supprimer les documents téléchargés dans les dossiers Téléchargements et Captures d'écrans. Vider la corbeille. Les supprimer aussi dans le Cloud !

- Applications connectées

Ex : sur android, les photos prises sur le téléphone peuvent être directement reliées au google drive.

Ex : sur iphone, la prise de photo peut préciser la localisation.

Témoignages d'utilisateurs de Mémo de vie

« Ça me rassure d'avoir mes papiers importants et ceux de mes enfants sécurisés et accessibles en ligne ! Ça me permet d'être autonome. »
- une utilisatrice de Mémo de vie

3

Régulation de ses comptes et appareils

Vérifier les paramétrages (tous écrans, réseaux sociaux, e-mail, applications) pour savoir ce que vous partagez et à qui.

Les réseaux sociaux fonctionnent tous avec des paramètres “par défaut” concernant le partage d’information sur votre vie privée, de votre profil (photo, âge..), vos activités (like, partage, commentaire) et vos publications, etc... Vous pouvez bien évidemment les modifier pour protéger votre compte en régulant les interactions, les contenus et les informations que vous partagez.

Quelques exemples :



- *Whatsapp* : déterminer si les personnes qui ne sont pas dans vos contacts peuvent ou non vous ajouter à des groupes de discussion, choisir si les photos que l’on vous envoie sont directement enregistrées dans la galerie de votre téléphone
- *Instagram* : stopper temporairement toutes les interactions sur votre compte grâce à l’outil “limites”
- *Snapchat* : décider du caractère éphémère ou non des messages et des photos échangées (attention tout de même aux captures d’écran), autoriser ou refuser l’accès à votre géolocalisation

Il existe plusieurs options pour restreindre les interactions avec un utilisateur spécifique :

1. Bloquer totalement la personne (elle ne peut plus vous contacter. Attention : elle peut sans rendre compte)
2. “Muter” (=mettre en sourdine) la personne (vous continuez de recevoir ce qu’elle vous envoie mais sans notification mais avec enregistrement des conversations, si vous souhaitez regarder parfois ce qu’elle vous envoie ou garder des preuves)
3. Pas de blocage mais filtrage de mots (la personne peut vous contacter mais vous pouvez, par exemple, décider de cacher les insultes)

En plus de ces paramètres, un parcours de signalement est proposé sur l’ensemble des réseaux sociaux.



Les bons réflexes avec Mémo de vie

Comment réagir face à une cyber-violence ?

Face à une cyber-violence, il est important de réagir et rapidement si possible. Nous vous proposons de suivre ces 3 étapes simples.

1

Garder les preuves

capture(s) d'écran avec date, heure et pseudonyme, stockée(s) dans le coffre fort Mémo de vie, sur clé usb ou disque dur.

Rassembler ses documents dans le coffre fort Mémo de vie



Ce coffre fort numérique sécurisé et confidentiel est à votre disposition, pour stocker des documents officiels mais aussi des photos, vidéos, captures d'écran qui pourront constituer des preuves.

« Je regrette de ne pas avoir connu Mémo de Vie avant ! J'ai perdu beaucoup d'indices dont j'aurais bien eu besoin avant ! Maintenant je garde tout, on ne sait jamais ! » - une utilisatrice de Mémo de vie



Renseigner ses émotions, ses humeurs permet de prendre du recul et peut être un signal d'alerte quant à la situation que vous traversez. N'oubliez pas le journal !



Si l'on s'aperçoit que l'on éprouve des émotions négatives durant plusieurs jours d'affilée alors peut être que l'on traverse une situation difficile.

Humeur du jour
Afin de suivre mon évolution, j'indique l'émotion qui me correspond le plus aujourd'hui :

Joyeux.e	Neutre	En colère
Stressé.e	Triste	Déprimé.e
Positif.e	Perdu.e	Négatif.e

VALIDER

de 00000



"Contacter un professionnel a été la première étape dans mon chemin vers la liberté." - utilisatrice de Mémo de vie



2

Signaler, bloquer le contenu / compte

via la plateforme en question, signaleur de confiance, pharos (voir Services d'aide p.24)

Signaler un contenu, c'est **avertir** la plateforme ou les personnes compétentes qu'une **publication doit être supprimée** car elle enfreint les règles de la plateforme ou qu'elle porte atteinte à une personne ou à soi.

Un **signaleur de confiance** est une entité compétente, directement en lien avec les réseaux sociaux, et **capable d'agir rapidement** pour supprimer une publication.



Si un contenu intime circule sans votre consentement, signalez-le à l'association Point de contact !

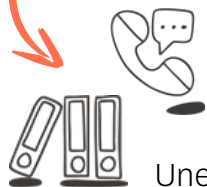
En cas de cyber-harcèlement, l'association Respect Zone et le 3018 sont là pour vous aider.



3

En parler !

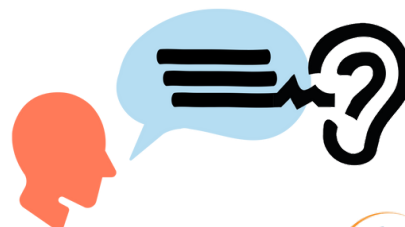
à une personne de confiance ou à un professionnel. Il est également possible de porter plainte.



Trouver de l'aide et des réponses

Une liste de **ressources** (documents utiles, outils, articles...) est accessible depuis **Mémo de vie** pour vous renseigner, répondre à vos questions et vous aider dans vos démarches. L'application mobile Respect Zone - gratuite - peut aussi vous accompagner en cas de cyber-violence.

Vous trouverez **une liste de contacts, de numéros d'assistance ainsi qu'un tchat anonyme pour vous aider** quelque soit votre situation. Ainsi, vous pourrez entrer en contact avec des professionnels qui sont là pour vous accompagner à tout moment.

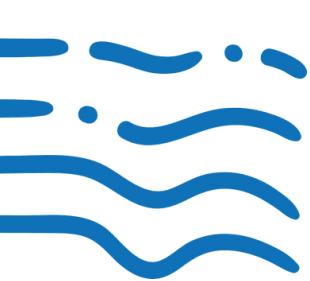




IV. Et maintenant ?

Résumé et premiers pas.....	22
Ressources boussole.....	23
Services d'aide.....	24





Résumé et premiers pas

pour un plan de sécurisation en ligne

Des questions pour commencer dès maintenant :



Est-ce que j'ai une **adresse e-mail** dont je suis la seule personne à avoir accès ?

Si non, en créer une !



Est-ce que je suis la seule à connaître mes **mots de passe**, surtout pour mes comptes les plus importants ?

Si non, changer mes mots de passe et en choisir des "forts" !



Est-ce que je sais quels **appareils** sont connectés à mes téléphone/ tablette/ ordinateur ?

Si non, aller vérifier dans les paramètres de téléphone/ tablette/ ordinateur !



Est-ce que je suis sûre de ne pas exposer d'**informations privées** en ligne, sans le savoir ?

Si non, aller vérifier les paramètres par défaut de mes appareils et comptes les plus importants, dont :

- accès public/privé ou restreint
- géolocalisation
- affichage de prénom, nom, numéro de téléphone, adresse
- bluetooth, air drop/nearby share

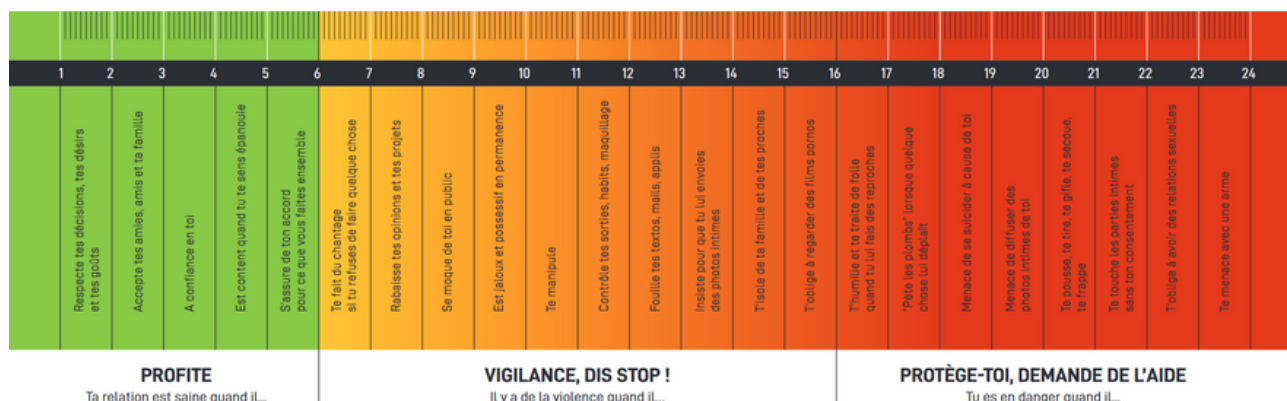
Pas besoin d'être des experts de la technologie pour mettre en place de bons réflexes de sécurité.





Ressources boussole

Violentomètre / harcèlomètre



Suis-je victime de cyber-violences conjugales ?

Pour en savoir plus
[cliquer ici](#)

DANS UNE RELATION RESPECTUEUSE ET ÉGALITAIRE MON OU MA PARTENAIRE :

- ☐ Respecte ma vie privée et ne cherche pas à consulter mon téléphone
- ☐ Me fait confiance et ne me demande pas de me justifier sur mes communications
- ☐ Me demande mon autorisation avant de prendre une photo de moi ou de la montrer à d'autres personnes
- ☐ Demande mon accord avant de m'envoyer un contenu à caractère sexuel
- ☐ Commente mes publications sur les réseaux sociaux d'une manière qui ne me met pas mal à l'aise
- ☐ Ne conserve pas mes *nudes* (images intimes) après la séparation

MON OU MA PARTENAIRE N'A PAS LE DROIT DE :

- ☒ Exiger que je sois tout le temps joignable
- ☒ Consulter mes communications (sms, mails, réseaux sociaux, comptes administratifs, etc.) sans mon consentement
- ☒ Me harceler pour savoir ce que je fais, où je suis et avec qui
- ☒ M'insulter par messages, m'envoyer des menaces
- ☒ M'interdire de communiquer avec certaines personnes
- ☒ Répondre à ma place à des messages ou des appels sans mon accord
- ☒ Exiger que j'envoie des photos pour prouver où je suis
- ☒ Exiger que je partage ma géolocalisation lors de mes déplacements
- ☒ Contrôler mes publications sur les réseaux sociaux
- ☒ Exiger d'avoir les mots de passe de mon téléphone/ma tablette/mon ordinateur ou de mes comptes (mails, réseaux sociaux, administratifs, etc.)
- ☒ Me confisquer mon téléphone/ma tablette/mon ordinateur
- ☒ Insister pour que je prenne des photos intimes, me faire du chantage si je refuse
- ☒ Me forcer à filmer nos relations sexuelles
- ☒ Me menacer de diffuser ou diffuser des images/informations intimes
- ☒ Me forcer à regarder du contenu pornographique
- ☒ Obtenir des informations pour savoir où je suis et avec qui, en surveillant ou en communiquant avec mes enfants/mes proches
- ☒ Utiliser des informations en ligne pour me surveiller après la séparation





Services d'aide



Tous ces services sont gratuits, anonymes et/ou confidentiels. Certains sont accessibles 7j/7 et 24h/24*



**Retrouver tous les contacts
de Mémo de vie**

Cyber-harcèlement, cyber-violences



Écrire à Respect Zone

app, site, réseaux sociaux

(Cyber)harcèlement, cyber-violences,
haine en ligne



Appeler ou écrire au 3018

9h-23h

Cyber-harcèlement, harcèlement scolaire,
exposition à des contenus violents - mineurs

Signalement de contenu interdit



**Pharos (police),
internet-signalement.gouv.fr**

Plateforme de signalement de contenu
interdit en ligne



pointdecontact.net (association)

Signalement de contenu illicite, contenu
à caractère intime

Autres sujets spécialisés



Appeler le 119

Service national d'accueil
téléphonique de l'enfance en danger



Écrire au 114

Service d'aide aux personnes en situation
de handicap



Appeler le 116 006

9h-19h

Aide aux personnes victimes,
renseignement juridique



Appeler le 3919

*Accessible en 12 langues ainsi qu'aux personnes
sourdes et malentendantes*

Violences faites aux femmes



Appeler le 3977

9h-19h (sauf de 13h à 14h le WE)

Maltraitance des personnes âgées et des
adultes en situation de handicap



Contacter SOS Homophobie

horaires variables selon le jour

Aide aux personnes victimes de LGBTphobie



Appeler le 3928

du Lundi au Vendredi, 9h30-19h

Service gouvernemental contre les
discriminations



*sauf indication contraire

