PLAN DE FORMATION

Comment participer ?

1. Allez sur wooclap.com
2. Entrez le code d'événement dans le bandeau supérieur

Code d'événement

LZEYJQ

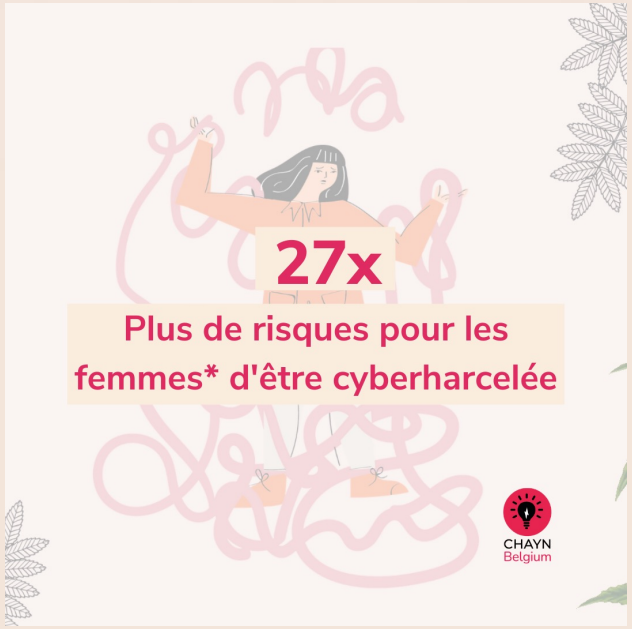
Copier le lien de participation

QUI SOMMES-NOUS ?

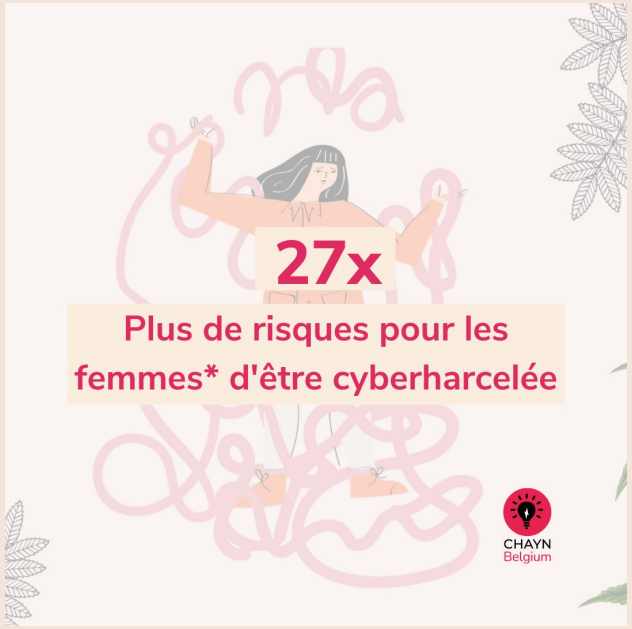
CHAYN BELGIUM

Nous sommes une collective féministe et antiraciste utilisant les technologies ouvertes pour lutter contre les violences et cyberviolences faites aux femmes*.

Par et pour les victimes



Certaines personnes se trouvant simultanément à l'intersection de plusieurs oppressions se retrouvent plus exposées à une forme de violence en ligne. En effet, au sexisme ou à la violence à l'égard des personnes LGBTQIA+, se superposent des violences basées sur l'appartenance ethnique, philosophique ou religieuse, au handicap ou encore la situation économique.



Certaines personnes se trouvant simultanément à l'intersection de plusieurs oppressions se retrouvent plus exposées à une forme de violence en ligne. En effet, au sexisme ou à la violence à l'égard des personnes LGBTQIA+, se superposent des violences basées sur l'appartenance ethnique, philosophique ou religieuse, au handicap ou encore la situation économique.

CHAYN BELGIUM

- Un partenaire sur la compréhension du phénomène et ses méthodologies d'étude
- Un partenaire dans l'outillage et dans le développement d'outils
- Un partenaire dans les protocoles à adopter sur base des expériences collectées
- Un partenaire des services publics et acteurs de terrain

AU SERVICE DES VICTIMES

CHAYN BELGIUM

Les entretiens des victimes

Des constantes

- Un sentiment d'insécurité
- La propagation dans l'espace hors-ligne
- La fuite du cyberespace
- La difficulté de réinsertion
- Le sentiment d'être démunies
- Le sentiment de ne pas être entendues par les institutions et autorités
- Ne pas savoir vers qui se tourner
- La culpabilité

Porter plainte est essentiel mais ne suffit pas et n'est pas une étape facile mais fera avancer la problématique en établissant une jurisprudence et permettant d'affiner les processus règlementaires – un guide ne suffira pas mais il est déjà une bonne base pour inspirer des solutions et comprendre les enjeux.

CHAYN BELGIUM

Quelles complexités ?

- Sa nature et le cyberespace: Rapidité de propagation et algorithmie
- Le harcèlement ne trouve pas de définition juridique.
- Diversité des formes
- Diversité des plateformes
- Diversité des contenus
- Diversité des cibles
- Désinhibition accentuant la violence
- Faire société ensemble
- Multiplicité des textes de référence et des motifs
- Comprendre la propagation
- Identification des auteurs
- Problématique des raids

- Complexité d'intervention
- Complexité d'appréhension
- Complexité de régulation
- Nécessité de compétences techniques
- Diversité des protocoles

CHAYN BELGIUM

Notre guide : objectifs et évolutions

Quels premiers gestes avant, pendant et après une situation de cyberharcèlement ?

- Mieux comprendre pour mieux agir et réagir
- Boites wiki : Enrichir des expériences vécues
- Décliner sous des formes plus accessibles
- Comment et où rassembler toutes les ressources et conseils, à portée de clic

Principe de l'open Knowledge : Documenter, étudier, mettre à contribution des ressources et outils.
Principe de l'open data : Compréhension par l'étude systématique de la donnée accessible. Exemple des avocats.

CHAYN BELGIUM

ATELIER 1

CYBERHARCELEMENT
MIEUX COMPRENDRE

Avant de commencer

Reconnaître le cyberharcèlement

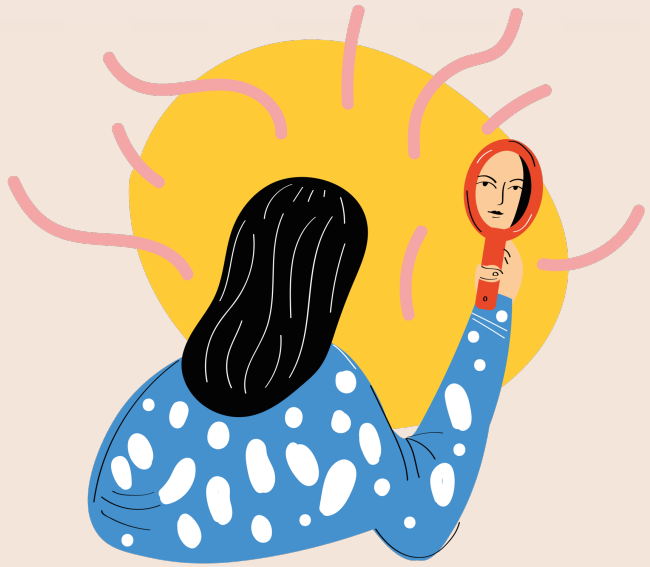
Le harcèlement ne trouve pas de définition claire dans le Code pénal. Néanmoins, le texte qui l'encadre (code du travail) stipule qu'il est composé de deux éléments :

- L'un matériel (les agissements doivent affecter la tranquillité d'une ou de plusieurs personnes)
- L'autre, moral (l'intention de nuire).

Il précise également les « Conditions à remplir pour qu'une situation soit acceptée juridiquement comme du harcèlement » :

- Le comportement doit être répétitif et abusif.
- Il doit y avoir atteinte à la tranquillité.
- Le harceleur doit être conscient du préjudice causé à sa victime.

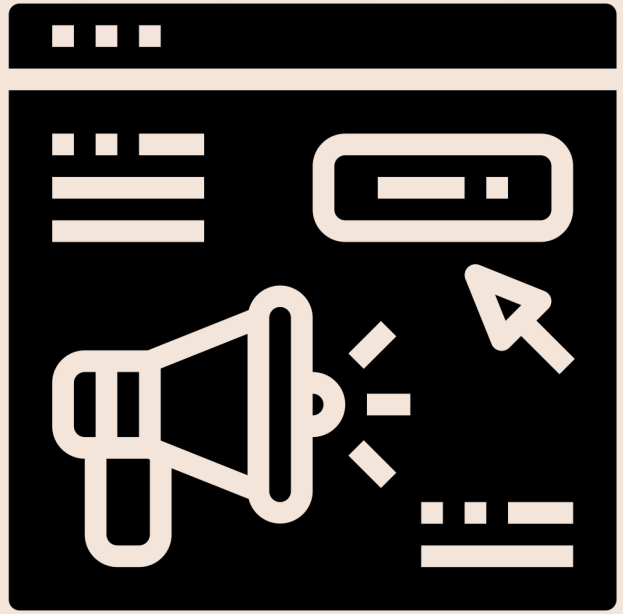
=> Important pour la plainte



Différences structurelles

En quoi le cyberharcèlement est-il spécifique ?

- Sa diffusion : rapide, instantanée et pouvant être médiatisée
- La double peine : l'espace cyber comme prolongement du harcèlement. Ajout d'un effet de traque, de contrôle. Le prolongement de violences de la vie
- L'identité : L'anonymat et renforcement du sentiment d'insécurité
- Sa gestion et son contrôle : la structure du web et la difficulté de contrôle
- La multiplicité des lieux : chaque lieu ayant sa propre règlementation et gestion



Diversité des espaces et du niveau de médiatisation

LES ESPACES NUMÉRIQUES DU CYBERHARCÈLEMENT

- **Emails**
- **Forums et salles de chat**
- **Conversations privées et en groupe:** sur des applications comme Whatsapp, Facebook, Messenger, Signal, Telegram, Viber, Twitter, Instagram, Youtube, etc.
- **Réseaux sociaux:** Publications, tags, commentaires et messages.
- **Plateformes de jeux:** en streaming ou en réseau, chat privés ou publics.
- **Commentaires:** sur les sites web des différents médias, sur YouTube, etc.
- **Plateformes collaboratives en milieu professionnel:** visioconférence, canaux de discussions de groupe, commentaire de documents, etc.
- **Sites de rencontre**

Diversité des supports

LES SUPPORTS ET MÉDIAS, VECTEURS DU CYBERHARCÈLEMENT

- **Supports écrits :** messages, commentaires.
- **Supports d'images :** photomontages, infographies, caricatures, dessins, photographies, gifs, etc.
- **Supports vidéo :** Reels, Stories, live chat et autres contenus vidéo.

- **Supports audios :** messages et commentaires vocaux, podcast, appels en ligne, etc.
- **Création de profils virtuels ou de pages, piratages de compte, vol d'identité, etc.**

A chaque forme son processus

LES FORMES QUE PEUVENT PRENDRE LES CYBER VIOLENCES/HARCÈLEMENTS : DE LA CYBERINTIMIDATION AU REVENGE PORN

- Cyberstalking :
Création d'un sentiment d'oppression chez une personne cible en la mettant dans une position de proie traquée. Technique qui vise à se saisir de l'ensemble de l'identité virtuelle d'une personne afin d'augmenter son sentiment d'insécurité et ainsi affecter sa vie personnelle.

- Affichage :
Création d'un sujet de discussion, d'une salle de chat, d'un groupe ou d'une page sur un réseau social à l'encontre d'une personne dans le but d'attirer l'attention sur elle et de la dénigrer auprès d'autres utilisateurs.

- Insultes et discours haineux :
Formulation ou reprise de discours haineux, de menaces, de provocations ou d'insultes dans le but de blesser ou d'attenter à la réputation de quelqu'un, ou d'un groupe. De là est né le terme de trolling en anglais.

- Diffamation et propagation de rumeurs :
Diffusion large et récurrente de faits, avérés ou non, impliquant une personne afin de promouvoir une image négative de celle-ci par dénigrement.

- Attaques coordonnées ou raids furtifs :
Lorsque plusieurs personnes/comptes coordonnés accablent collectivement une personne ciblée en se servant d'attaques personnelles, de menaces ou d'insultes. Cette technique est souvent utilisée lors de débats d'opinion sur internet. Ces raids peuvent également se dérouler par messages privés ou par visio-conférence, via les messageries par exemple.

- Exclusion :
Technique de discrimination volontaire et ciblée visant à évincer une personne d'un groupe, d'une conversation ou encore d'un jeux.

- Harcèlement sexuel par le biais de supports numériques:
Sollicitations à connotations sexuelles ou sexistes exercées de manière répétée sur une personne constituant une atteinte à la dignité d'une personne en raison de leur caractère dégradant. Phénomène incluant notamment le sexting et l'envoi de contenus sexuellement explicites non désirés.

- Revenge porn (Diffusion non consentie, sextorsion, chantage à la cam, compte fisha, …) :
Très proche du «harcèlement sexuel par le biais de supports numériques». Diffusions de photos ou de vidéos à caractère sexuel, mettant en scène la victime, sans son consentement et dans la volonté de lui nuire, le plus souvent dans un contexte de vengeance (jalousie, rupture,violence, etc.).

- Cyberviolences conjugales :
Lorsque le harcèlement s'inscrit dans les relations dysfonctionnelles et/ou abusives au sein d'un couple donné. Ces abus peuvent revêtir plusieurs formes: contrôle des activités du conjoint «en ligne» (lecture des sms, pression téléphonique constante, viol de l'intimité, etc.), d'injures et de campagnes de dénigrement sur les réseaux. Cela peut même mener à des menaces de mort dans certains cas. Les technologies numériques permettent également une surveillance accrue du conjoint (avec un contrôle des déplacements via des logiciels de traçage, par exemple). Il faut savoir que dans le cadre des violences conjugales, on observe depuis quelque temps un glissement vers l'espace numérique des violences sexuelles (comme c'est le cas du revenge porn mentionné plus haut) Une violence économique peut également découler de ce glissement (piratage des comptes bancaires, restriction des accès, etc.)

- Exposition et abus de la vie privée (Doxing) :
Utilisation et divulgation publique d'informations personnelles. Cette technique, communément appelée doxing, est utilisée par les harceleurs afin d'affaiblir la victime ou encore d'accentuer le processus d'intimidation.

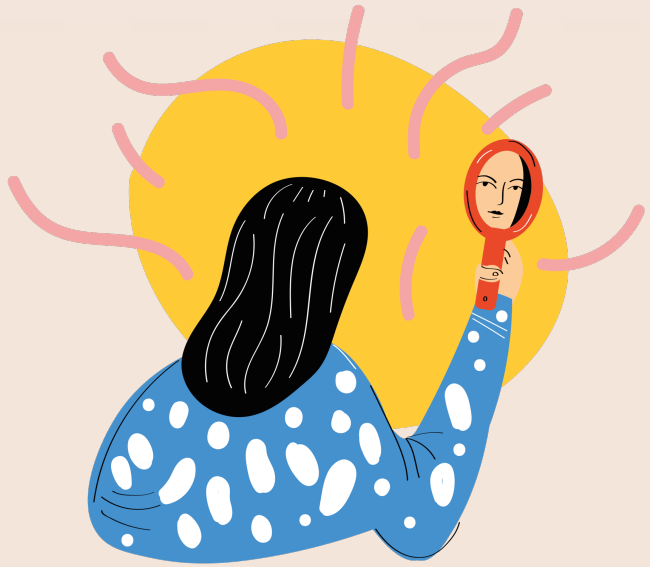
- Usurpation d'identité :
Création d'un compte, page ou profil sur un réseau social dans le but d'usurper l'identité digitale d'une personne.

- Phishing :
Fraude à l'identité reposant sur la confiance et le crédit accordé à un organisme public ou privé pour en imiter les usages. Cette arnaque sert très souvent des fins lucratives en permettant l'accès à des informations personnelles ou bancaires. Le harcèlement découle du caractère répétitif et récurrent de cette technique.

- Astroturfing :
Technique de harcèlement visant à coordonner des actions (création de faux comptes, achats de followers actifs, etc.) pour gonfler les volumes de propagation d'un message afin de faire croire à un engouement authentique. Cette méthode de pression est très souvent utilisée à des fins politiques ou polémiques. La pression exercée sur la personne ciblée est ainsi considérablement accrue par le soin apporté au réalisme et à la crédibilité du message véhiculé.

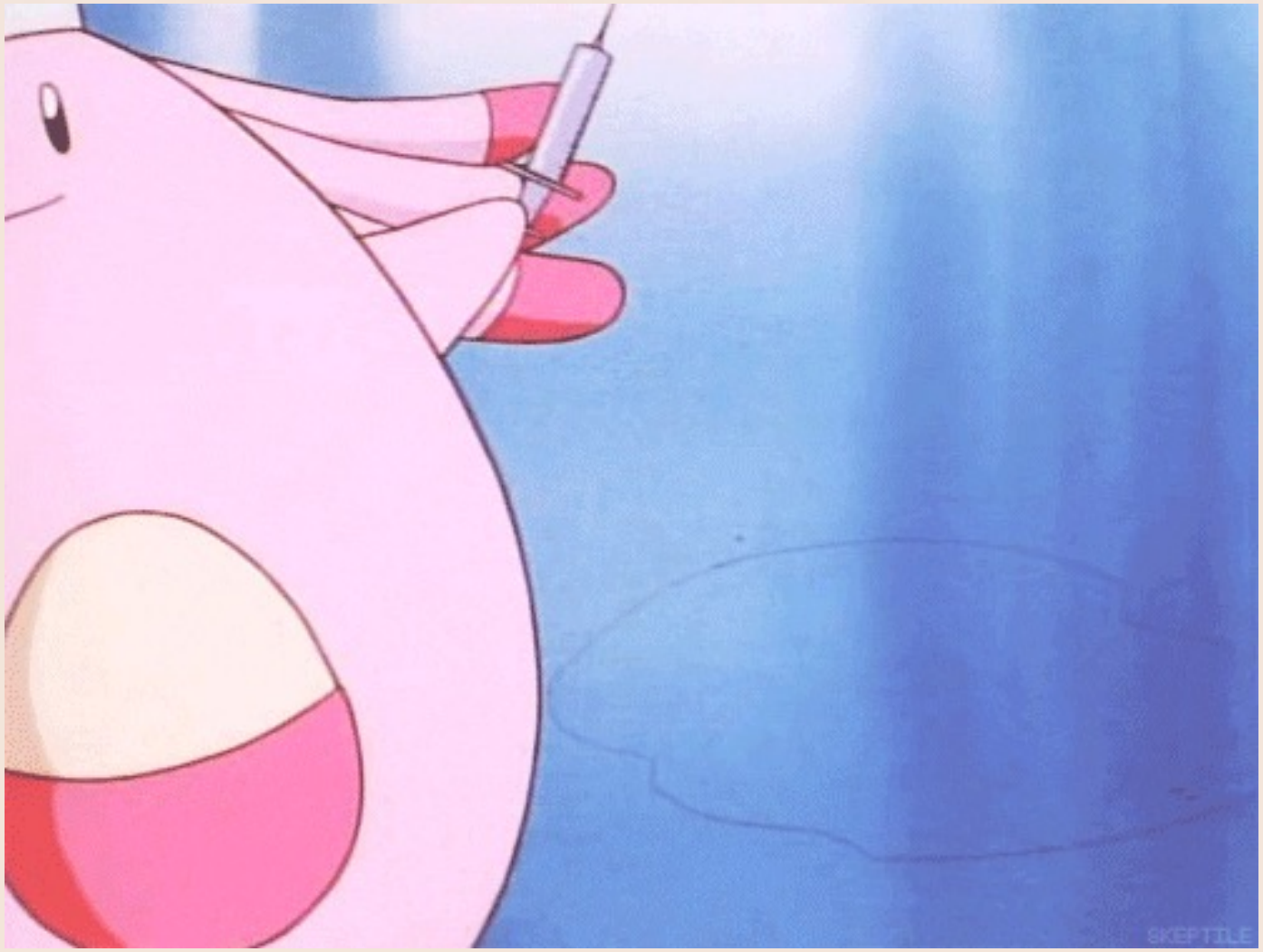
Les attaques

- Sexisme
- Chantage, message de haine, menaces et insultes, humiliation, envers des personnes LGBTQIA+
- Racisme
- Slut shaming
- Grossophobie
- Body Shaming
- Validisme



Mais que puis-je faire ?

Les premiers soins



Avant d’entrer dans les solutions

© Marilyn Nieves / Getty Images / CAPITAL

Conservez les messages et tout autre élément qui pourraient constituer une preuve devant les autorités avant de signaler, supprimer les contenus ou de bloquer les comptes. N’hésitez pas à demander à une personne de confiance de le faire pour vous.

Child Focus
116000

Contactez Child Focus :
En Belgique, Child focus est joignable gratuitement au 116 000 pour les questions de sécurité en ligne destinées aux enfants, adolescents, parents et professionnels de l’éducation.
ChildFocus :
Email : 116000@childfocus.org
116 000 (24h/24)
Clicksafe.be (sur la sécurité en ligne)
facebook.com/ChilDfocus

Les premiers gestes, un protocole possible ?

- Eviter de répondre
- Demander de l'aide
- Récolter et conserver les preuves
- Signaler aux plateformes
- Ensuite ...
- Ne restez pas seule

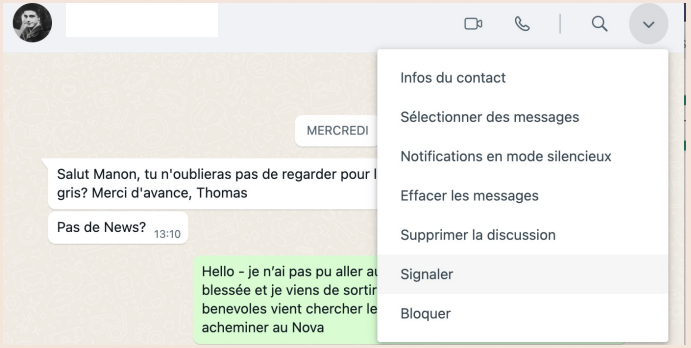
Récolter et conserver les preuves

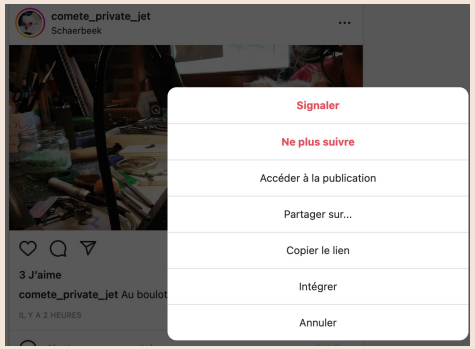
Screenshot sur Apple

Screenshot sur Windows

Comment signaler ?

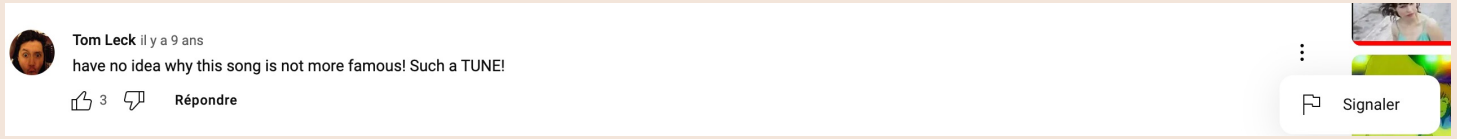
Signaler : Pour signaler des messages, ou autres contenus indésirables, aux plateformes qui les hébergent : https://onlineharassmentfieldmanual.pen.org/fr/le-signalement-aux-plateformes/





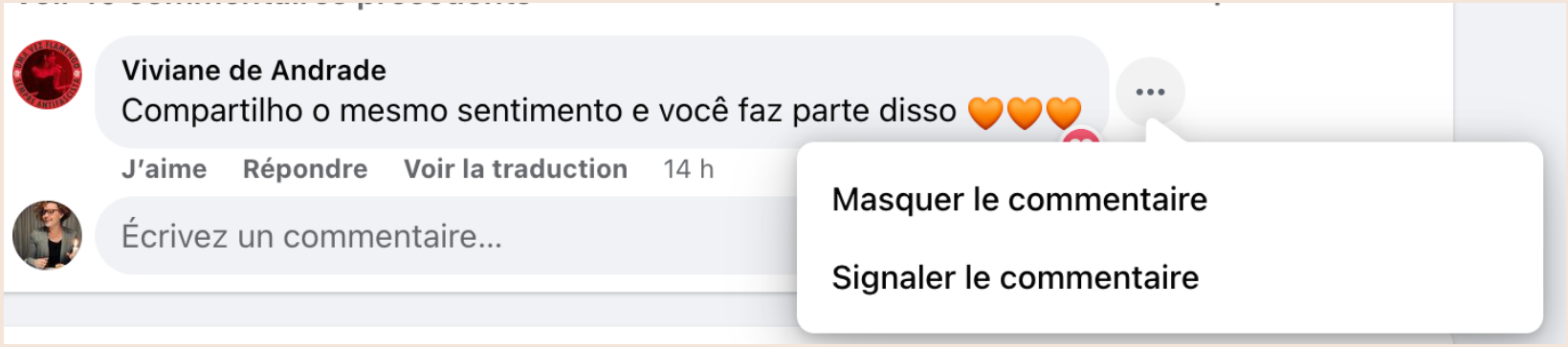
+ signaler la personne sur le profil https://help.instagram.com/contact/383679321740945

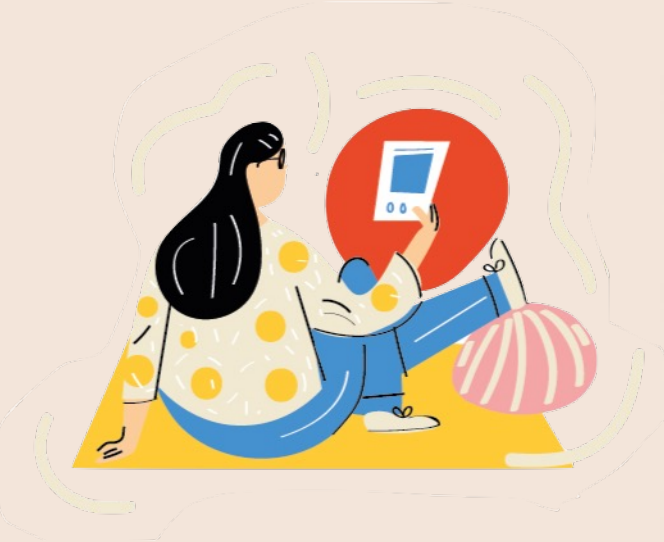
https://stopncii.org/



Comment masquer un commentaire sur Facebook ?

- **Masquer et/ou supprimer des commentaires** : Sur Facebook, une fonctionnalité vous permet de masquer certains commentaires au bas de vos publications. L'auteur n'en sera pas alerté et sera, lui, toujours disposé à les voir. Ces contenus seront cependant bien conservés mais inaccessibles aux autres utilisateurs.





Et les sites comme Tinder et Grindr ! ?

Comment signaler un profil ?

La sécurité de nos utilisateur.rice.s nous importe vraiment. Vous pouvez signaler un.e utilisateur.rice avec qui vous avez déjà eu un Match ou un.e utilisateur.rice avec qui vous n'avez pas encore matché.

Pour ce faire, rendez-vous sur le profil en question, faites défiler vers le bas et appuyez sur **Signaler.**

Nous vous encourageons fortement à signaler et bloquer tout utilisateur.rice ou comportement suspect.

Mon identité est usurpée

Ta sécurité est notre priorité. Si quelqu'un se fait passer pour toi sur Tinder, signale-le-nous en utilisant ce formulaire et en sélectionnant « Quelqu'un se fait passer pour moi » dans le menu déroulant. Fournis toutes les informations demandées, y compris d'éventuels détails sur le profil de la personne qui usurpe ton identité.

https://www.help.tinder.com/hc/fr/requests/new?ticket_form_id=360000234472

Une personne franchit la ligne ? Dis-le-nous pour nous aider à faire de Tinder la plateforme la plus sûre pour faire des rencontres. Tu peux signaler n'importe quel•le membre qui te met mal à l'aise, ne respecte pas nos règles, a commis un crime, est inscrit•e sur un registre de délinquants sexuels ou dont tu sais d'expérience qu'il•elle•iel a eu des comportements inappropriés par le passé. Le signalement sur Tinder est confidentiel et reste un moyen facile de nous informer des actions inappropriées d'une personne.

On est là pour toi et on prend les cas de harcèlement très au sérieux : ils n'ont pas leur place sur Tinder. Voici quelques motifs de bannissement d'utilisateur•rices :

- Insultes racistes ou autres paroles dégradantes
- Envoi de menaces ou de messages choquants sur l'application ou en dehors
- Harcèlement de Matchs sur l'application ou en dehors
- Envoi de contenus sexuellement explicites sur l'application ou en dehors sans consentement
- Envoi de spams ou de sollicitations commerciales, comme l'envoi de liens vers des sites de revente ou les tentatives de vente de produits ou de services

Protégez votre identité.

Ne publiez pas d'informations personnelles (numéro de téléphone, adresse, lieu de travail) sur votre profil public. Ne partagez ces informations avec d'autres utilisateurs que lorsque vous pensez pouvoir leur faire confiance. Tout ce que vous partagez avec un autre utilisateur pourrait devenir public grâce à leurs actions, alors merci d'en être conscient lorsque vous partagez des photos et des vidéos de vous. Soyez conscient des escroqueries d'hameçonnage et de romance, et ne fournissez aucune information financière aux autres utilisateurs. En outre, sachez que tous les codes de vérification SMS que Grindr vous envoie sont pour vous seul et ne doivent pas être partagés avec quiconque pour quelque raison que ce soit.

Si vous ne vous sentez pas à l'aise de poster une photo de votre visage sur Grindr, envisagez d'utiliser une image qui vous représente différemment (par exemple, une photo liée à vos passe-temps ou à votre personnalité). Si vous choisissez de poster une photo de votre visage, sachez qu'il est possible de faire une recherche avec la photo et de trouver les autres sites où vous l'avez postée.

De même, soyez prudent si vous choisissez de connecter vos comptes de médias sociaux (tels que Instagram, Facebook, Spotify ou Twitter) à votre profil Grindr.

Utilisez nos fonctionnalités de blocage et de signalement.

Si quelqu'un vous met mal à l'aise dans l'application, vous pouvez choisir de le bloquer en sélectionnant l'icône « 🚫 » sur le profil de l'utilisateur et en touchant « bloquer ».' L'utilisateur ne pourra plus vous voir, vous ne pourrez plus voir l'utilisateur, et vous ne pourrez pas vous contacter sauf si vous choisissez de le débloquer.

ISi vous pensez que quelqu'un enfreint nos Directives communautaires, signalez-le en sélectionnant l'icône « 🚫 » sur le profil de l'utilisateur et en touchant « signaler »' Notre équipe de modération examinera le profil de l'utilisateur ainsi que votre signalement et prendra les mesures appropriées.

Même si vous suivez tous nos conseils, aucun plan de réduction des risques n'est parfait. Si vous souhaitez signaler un incident qui s'est produit en dehors de Grindr, faites-le nous savoir sur help@grindr.com. Vous pouvez également vous adresser à un organisme de défense des droits de la personne ou LGBTQ+ pour obtenir de l'aide, et si vous vous sentez à l'aise, signalez-le auprès des autorités.

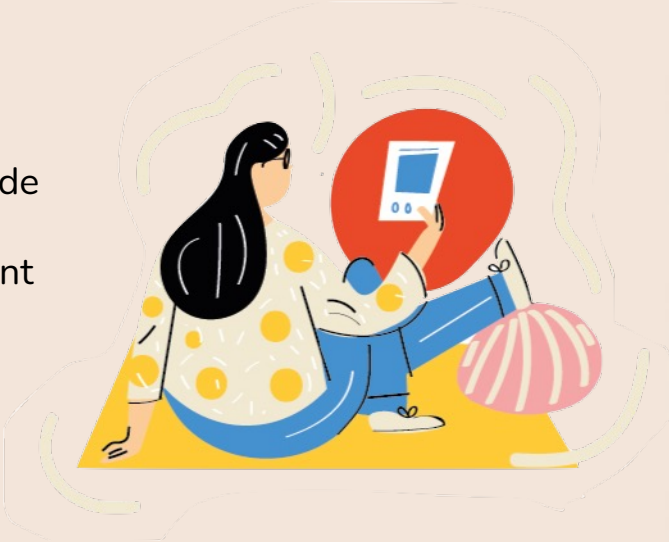
Sécurisez votre compte.

Il est judicieux de protéger votre compte en utilisant un mot de passe complètement unique et difficile à deviner sur Grindr, en plus d'utiliser notre fonction de code PIN. Nous offrons également des icônes d'application discrets.

Merci de comprendre que les gens peuvent enregistrer et/ou partager les informations privées que vous partagez dans le chat, telles que des messages ou des photos.

OSINT TOOLS

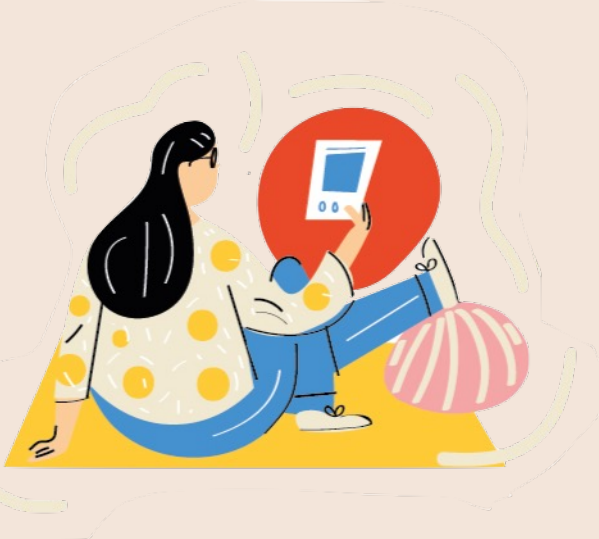
- **Démasquer/récupérer l'information** : Dans le cas d'attaques perpétrées par de très nombreux comptes, n'hésitez pas à questionner l'authenticité des comptes. En effet, lors de la création de faux comptes, il est fréquent qu'on laisse de nombreux indices qui peuvent permettre de remonter vers l'identité de la ou des personne, voire des organisations, dans certains cas, les ayant créés. Il existe de nombreuses techniques de repérage de faux comptes et d'identifications de leur(s) source(s). Elles font partie de la discipline : OSINT (Open Source INTelligence). Certaines associations s'y spécialisent ainsi que les services de police en ligne.



https://osintframework.com/
We Verify Plug in
Reverse Image
IP Adress
SNA
Moteurs de recherche

Les cas particuliers exigeant un protocole adapté

- Personnalité publique : journaliste, femme politique ou autre figure médiatique.
- Cas de raids coordonnés via des faux comptes (Astroturfing)
- Cas de diffusion d'informations privées (doxing : safeonweb)
- Cas de revenge porn
- Cas de cyberviolences conjugales
- Cas de phishing (Safe on web)



Les cas particuliers exigeant un protocole adapté

Revenge Porn

- Adulte :
En Belgique, l'IEFH, l'Institut pour l'égalité des femmes et des hommes peut vous aider en vous informant à propos de vos droits, de vos obligations et de vos possibilités d'actions, en vous apportant son soutien et parfois en entreprenant des démarches judiciaires avec vous.
L'Institut a élaboré un ☞ manuel qui explique, étape par étape, comment procéder pour signaler vous-même des images auprès des plateformes afin de les faire supprimer. Le manuel explique également comment déposer plainte à la police, ainsi que les conséquences d'une plainte.

Contacter l'IEFH :
0800/12 800
☞egalite.hommesfemmes@iefh.belgique.be
formulaire de contact
formulaire de signalement

- Mineur·e
Si la victime est mineure contactER Child Focus:
Le numéro d'urgence gratuit :
116 000 (24h/24)
☞ 116000@childfocus.org

+

Les cas particuliers exigeant un protocole adapté

Cyberviolences conjugales

On peut identifier 5 formes de cyberviolences conjugales:

- **Le cybercontrôle** : lecture des SMS, exigence que la partenaire soit joignable en permanence,...
- **Le cyberharcèlement**: appels incessants et envahissants, injures, menaces de mort.
- **La cybersurveillance**: contrôle continu des déplacements et agissements par exemple via un logiciel espion ou avec le GPS,...
- **Les cyberviolences sexuelles**: diffusion ou menace de diffusion d'images
- **Les cyberviolences économiques et administratives** : comptes bancaires piratés

Se protéger

https://onlineharassmentfieldmanual.pen.org/fr/seproteger-du-doxing/

https://chayn.gitbook.io/diy-online-safety/french

https://chayn.be/fr/ressources/comment-construire-un-dossier-judiciaire-de-violences-domestiques-sans-un-avocat

Guide : Comment monter un dossier judiciaire sans avocat.e

0800 30 030

LIGNE ÉCOUTE VIOLENCES CONJUGALES

Les preuves et traces numériques

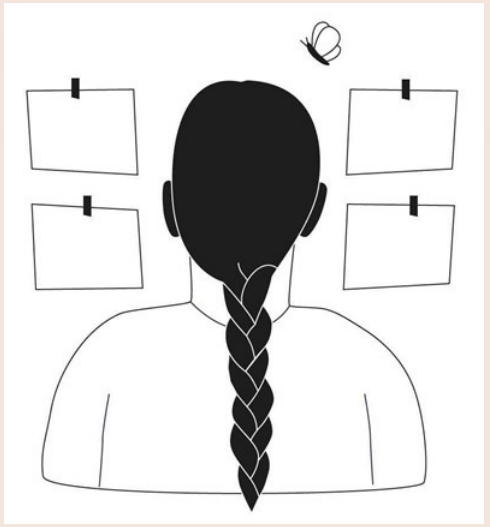
Lorsque vous vous sentez prêt·e, compilez l'ensemble des éléments susceptibles de prouver qu'il y a bien fraude ou intention de nuire. Conservez également tout indice pouvant mener à l'identité du/des auteur·s. Cet ensemble d'informations constitue ce que l'on appelle « les traces numériques ».

Dans un emplacement sécurisé, pensez à recenser et sauvegarder ce qui peut être considéré comme preuves numériques :

- Les dates et heures des messages ou échanges litigieux,
- La plateforme le réseau social, l'application ou le site internet utilisé,
- Le type de document ou de support employé (Message privé, commentaire, contenu visuel, etc.),
- Les éventuels liens URL (vous pouvez utiliser Archive.is pour conserver une adresse URL)
- Le nombre de messages,
- La nature de l'incident en ligne (menace de nature sexuelle, attaque à caractère raciste, etc.)
- Le nom ou pseudonyme utilisé par l'auteur ainsi que ses potentielles autres identités digitales (accompagnées des différentes photos le représentant, ou désignées comme telles.) Si vous êtes en mesure d'y avoir accès, notez également son adresse email, son numéro de téléphone, son adresse IP ou encore des indices permettant sa localisation. Tout élément relatif à son identité peut s'avérer déterminant pour confronter la personne à l'origine du harcèlement,
- Les captures d'écran ou vidéos enregistrées,
- Votre matériel informatique, vos identifiants et votre nom d'utilisateur
-Les autres agressions, verbales et/ou physiques, subies hors de l'espace numérique, liées aux faits relatés en ligne,
- Toute éventuelle preuve de préjudice : certificat médical, bilan psychologique, ordonnance psychiatrique, ou tout autre témoignage de votre entourage, professionnel ou privé,
- La fréquence des attaques, le type d'attaque, ou tout autre élément de contexte que vous jugerez pertinent de mentionner.

Les preuves et traces numériques

Recréer la timeline



9.15pm

WHAT: Arrived at the bar

WHERE: The Owl & Pussycat

WHO: With Emma & Jane

EVIDENCE: Uber receipt for arriving in the cab with friends

9.30pm

WHAT: Grabbed a drink at the bar and met perpetrator

WHERE: The Owl & Pussycat bar

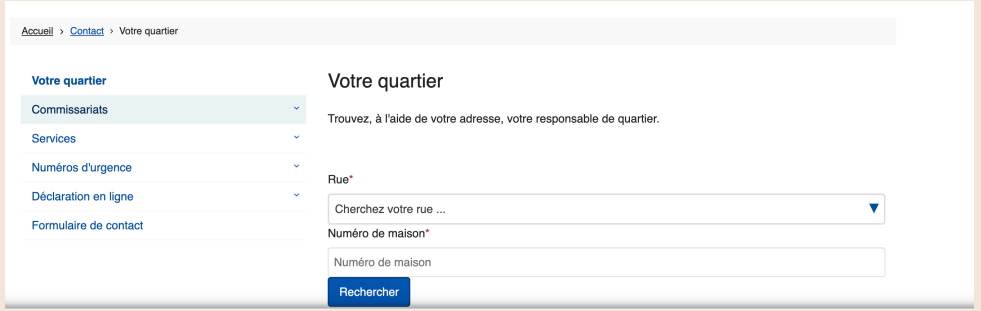
WHO: Brown-haired man, maybe late 20s.

EVIDENCE: Debit Card Payment

SENTIMENT DE CONTRÔLE

Porter plainte

Se préparer



Le Service d'Assistance Policière aux Victimes (SAPV) : vous accompagner moralement, vous conseiller dans vos démarches administratives ou encore vous informer de vos droits. Ces services n'interviennent qu'à court terme et ne proposent pas de suivi psychologique. Ils peuvent néanmoins vous orienter vers des services de prise en charge spécialisés pour vous assurer un suivi sur du plus long terme : http://www.victimes.cfwb.be/ou-trouver-aide/services-dassistance-policiere-aux-victimes-de-la-police-federale/#c7876. Les antennes locales ont également leur propre service d'aide aux victimes. N'hésitez pas à contacter votre commissariat à ce sujet

Cyberharcèlement sexiste

Se préparer

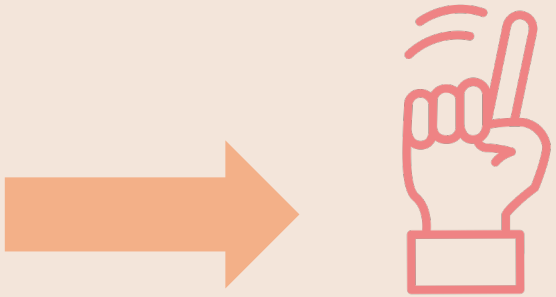
0800/12.800

INSTITUT POUR L'ÉGALITÉ DES FEMMES ET DES HOMMES

Le Service d'Assistance Policière aux Victimes (SAPV) : vous accompagner moralement, vous conseiller dans vos démarches administratives ou encore vous informer de vos droits. Ces services n'interviennent qu'à court terme et ne proposent pas de suivi psychologique. Ils peuvent néanmoins vous orienter vers des services de prise en charge spécialisés pour vous assurer un suivi sur du plus long terme : http://www.victimes.cfwb.be/ou-trouver-aide/services-dassistance-policiere-aux-victimes-de-la-police-federale/#c7876. Les antennes locales ont également leur propre service d'aide aux victimes. N'hésitez pas à contacter votre commissariat à ce sujet

Cyberharcèlement sexiste

Se préparer



0800/12.800

https://www.signalement.unia.be/fr/signale-le

Le Service d'Assistance Policière aux Victimes (SAPV) : vous accompagner moralement, vous conseiller dans vos démarches administratives ou encore vous informer de vos droits. Ces services n'interviennent qu'à court terme et ne proposent pas de suivi psychologique. Ils peuvent néanmoins vous orienter vers des services de prise en charge spécialisés pour vous assurer un suivi sur du plus long terme : http://www.victimes.cfwb.be/ou-trouver-aide/services-dassistance-policiere-aux-victimes-de-la-police-federale/#c7876. Les antennes locales ont également leur propre service d'aide aux victimes. N'hésitez pas à contacter votre commissariat à ce sujet

Comment procéder ?

Documents d'identité et preuves

Accueil

Attente

Entretien confidentiel

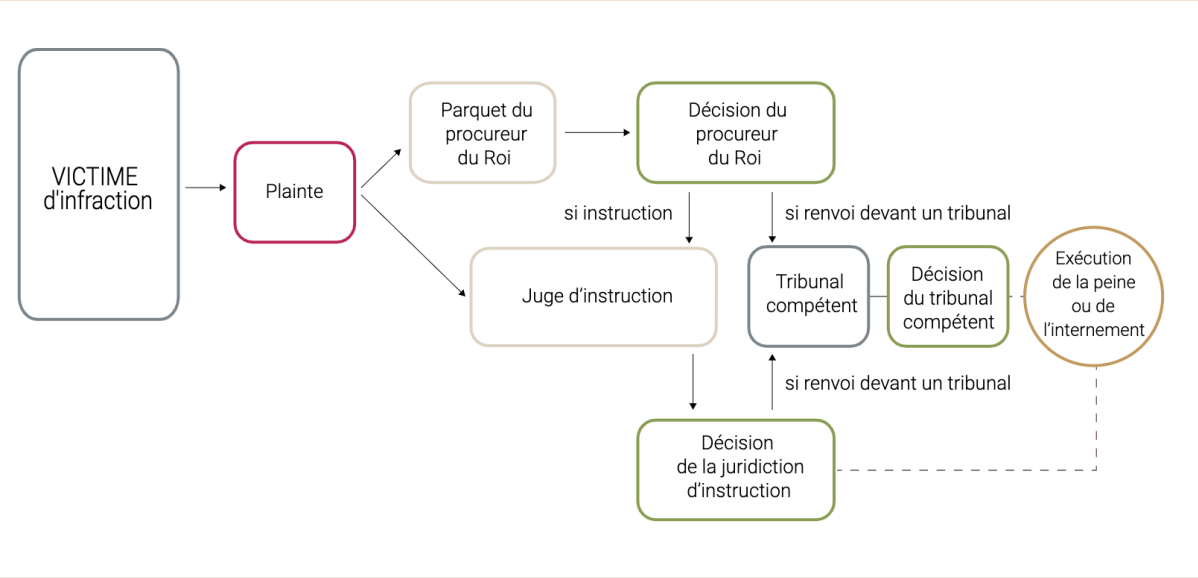
Sachez que vous pouvez aussi demander à remplir une « déclaration de personne lésée » Cette démarche vous permettra notamment de bénéficier d'un meilleur suivi de votre dossier. En voici les avantages 👉 http://www.victimes.cfwb.be/procedures-judiciaires/victime-vos-droits/#c7953
À la suite de l'entretien, il vous sera remis un document, votre attestation de dépôt de plainte, que vous devrez conserver. Ce document pourra vous être demandé par la suite lors de vos démarches administratives et juridiques. Vous y trouverez également les coordonnées des services d'aide.

Et après ?

Sauf exception, la police transmet toutes les plaintes (procès-verbaux) au procureur du Roi.

Lorsque votre plainte arrive au parquet, le procureur du Roi décide de l'orientation à lui donner. S'il l'estime nécessaire, une enquête – appelée « information judiciaire » – est ouverte.

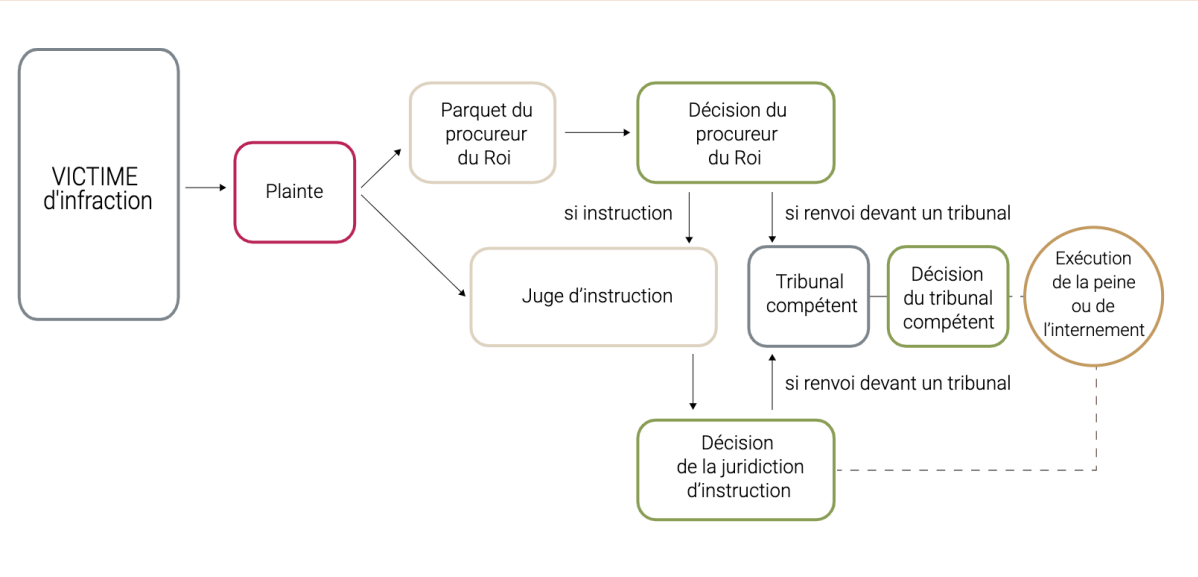
Le service de police chargé de l'enquête exécute les devoirs que le magistrat du parquet juge utiles pour l'enquête (par exemple : audition du suspect, audition de témoins, vérifications sur le lieu des faits...).
Pour prendre sa décision quant à l'orientation du dossier, le procureur du Roi tient compte des éléments du dossier, de la nature de l'infraction et du résultat de l'enquête.



N'hésitez pas à vous faire conseiller par les services d'accueil des victimes proposés au sein des tribunaux. Ces personnes vous accompagnent et vous informent tout au long de la procédure, du dépôt de plainte jusqu'aux délibérations finales et même dans le cadre de la mise en application de la peine.
👉 http://www.victimes.cfwb.be/ou-trouver-aide/services-accueil-victimes/

Et après ?

Le procureur du Roi peut demander au juge d'instruction de mener l'enquête notamment lorsque des mesures contraignantes sont nécessaires (comme par exemple une perquisition, des écoutes téléphoniques ou un mandat d'arrêt). Cette enquête est appelée "instruction judiciaire".
Si le suspect est placé en détention préventive, des audiences auront régulièrement lieu devant la chambre du conseil qui se prononcera sur le maintien ou non du suspect en détention. Cette chambre pourra également décider de libérer celui-ci (moyennant éventuellement le respect de conditions) ou de le placer sous surveillance électronique. Ces audiences se tiennent à huis-clos et la victime n'y est pas conviée.

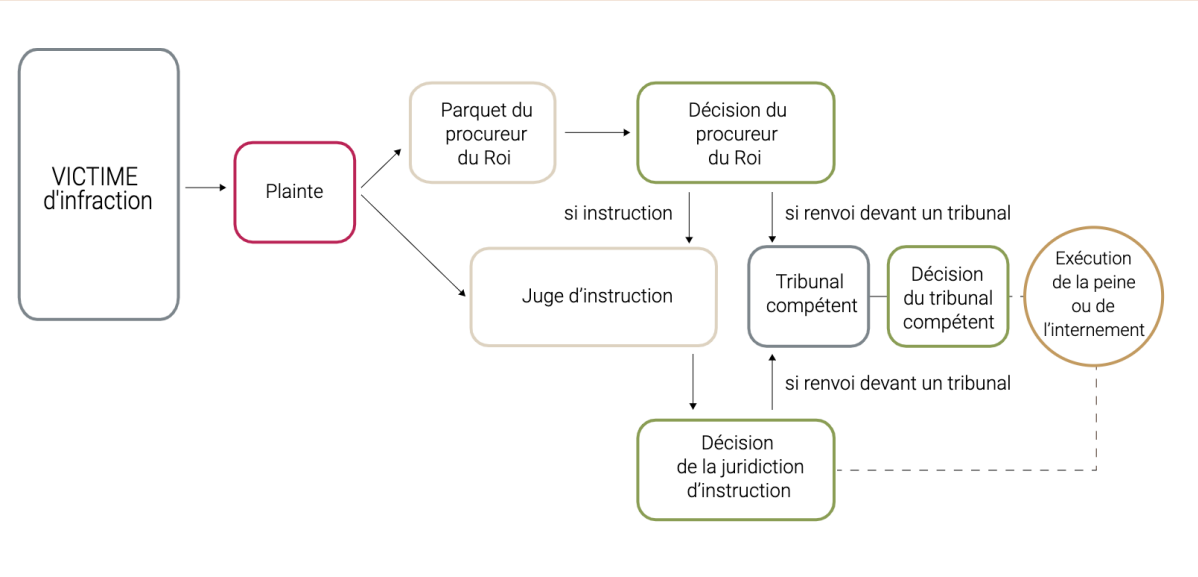


N'hésitez pas à vous faire conseiller par les services d'accueil des victimes proposés au sein des tribunaux. Ces personnes vous accompagnent et vous informent tout au long de la procédure, du dépôt de plainte jusqu'aux délibérations finales et même dans le cadre de la mise en application de la peine.
👉 http://www.victimes.cfwb.be/ou-trouver-aide/services-accueil-victimes/

Et après ?

•**Classement sans suite**
Le procureur du Roi peut classer le dossier sans suite car les poursuites ne sont pas possibles (par exemple parce que l'auteur n'a pas pu être identifié ou que les preuves sont insuffisantes) ou ne sont pas indiquées (par exemple parce que vous avez été entièrement indemnisé(e)). Cette décision est provisoire et peut être revue si, par exemple, de nouveaux éléments sont portés à la connaissance du procureur du Roi.

•**Médiation et mesures**
Sur décision du procureur du Roi, une médiation et mesures peut être mise en place par un assistant de justice. Dans un objectif de réparation du dommage, le procureur du Roi peut proposer à l'auteur et à la victime une médiation (échange direct ou indirect entre les parties) et/ou proposer des mesures uniquement destinées à l'auteur. Il peut s'agir d'un traitement ou toute autre thérapie, d'un travail d'intérêt général ou d'une formation socio-éducative (par exemple, gestion de la violence).



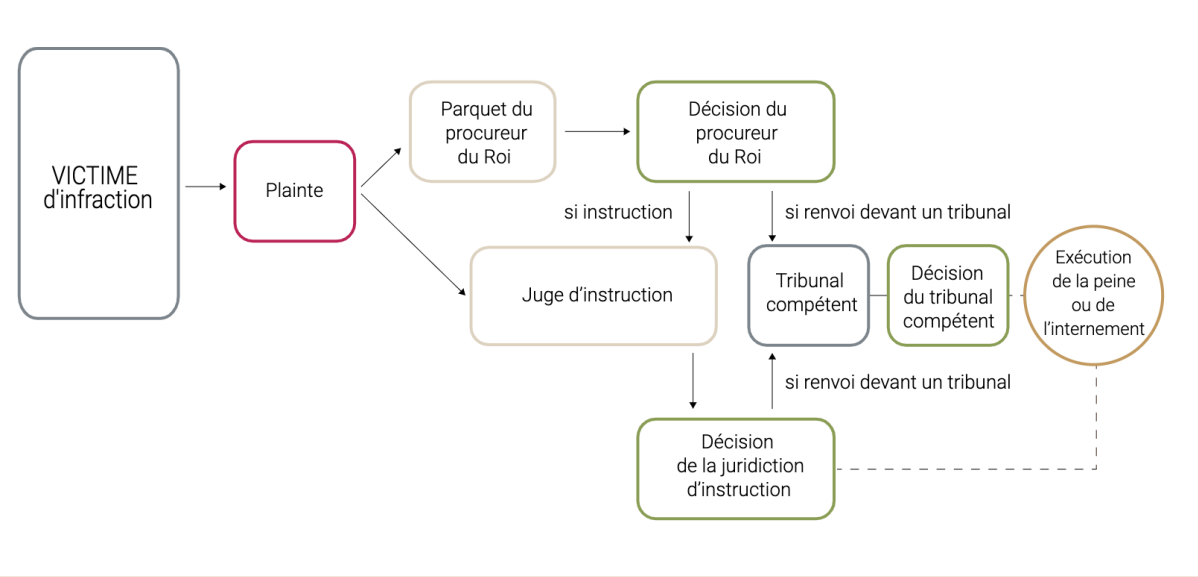
N'hésitez pas à vous faire conseiller par les services d'accueil des victimes proposés au sein des tribunaux. Ces personnes vous accompagnent et vous informent tout au long de la procédure, du dépôt de plainte jusqu'aux délibérations finales et même dans le cadre de la mise en application de la peine.
👉 http://www.victimes.cfwb.be/ou-trouver-aide/services-accueil-victimes/

Et après ?

•Transaction pénale
Le procureur du Roi peut proposer une transaction pénale à l'auteur de l'infraction : celui-ci devra payer une certaine somme d'argent dans un délai déterminé à condition qu'il ait reconnu sa culpabilité et indemnisé la victime pour les dommages causés.
Si l'auteur paye cette somme d'argent, le procureur du Roi ne pourra plus porter cette affaire devant le tribunal pénal (on parle alors d'extinction des poursuites).

•Ouverture d'une instruction
Le procureur du Roi peut demander l'ouverture d'une instruction afin que l'enquête soit menée par le juge d'instruction.

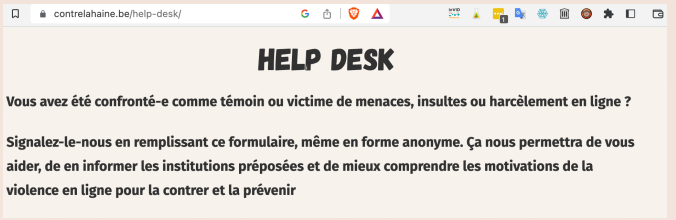
•Poursuites - Renvoi devant le tribunal compétent
Si le procureur du Roi estime, à l'issue de son enquête, que les charges sont suffisantes, des poursuites pénales peuvent être engagées contre l'auteur présumé par le renvoi de l'affaire devant le tribunal pénal compétent.



N'hésitez pas à vous faire conseiller par les services d'accueil des victimes proposés au sein des tribunaux. Ces personnes vous accompagnent et vous informent tout au long de la procédure, du dépôt de plainte jusqu'aux délibérations finales et même dans le cadre de la mise en application de la peine.
👉 http://www.victimes.cfwb.be/ou-trouver-aide/services-accueil-victimes/

Trouver de l'aide

VIS À VIS
CONTRE LA HAINE EN LIGNE



112

+ **Le Service d'Assistance Policière aux Victimes (SAPV)**

Politie Police

101

POLICE ON WEB
www.police-on-web.be

Écoute Violences Conjugales
0800 30 0 30
24/7 + GRATUIT + ANONYME

https://www.ecouteviolencesconjugales.be

SSM Services Santé Mentale

Bruxelles : https://www.ccc-ggc.brussels/fr/institutions/services-de-sante-mentale
Wallonie : http://www.cresam.be/adresses-2/

fédération des Centres de Planning Familial
fps

https://www.sosviol.be/

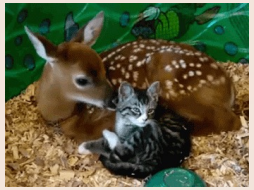
https://www.planningfamiliale.net/liste-des-centres/

Child Focus
116000

Contactez Child Focus :
En Belgique, Child focus est joignable gratuitement au 116 000 pour les questions de sécurité en ligne destinées aux enfants, adolescents, parents et professionnels de l'éducation.
ChildFocus :
Email : 116000@childfocus.org
116 000 (24h/24)
Clicksafe.be (sur la sécurité en ligne)
facebook.com/ChildFocus

https://findahelpline.com/be

PRENDRE SOIN DE SOI - BLOOM

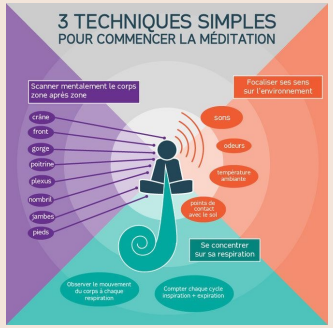


Faire des exercices de respiration et d'ancrage

3 6 5

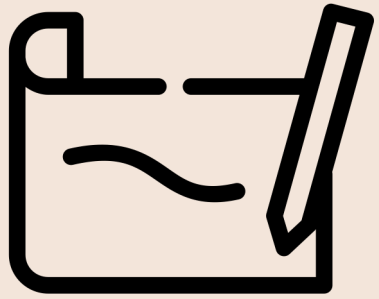
3 fois par jour — 6 respirations par minutes — 5 minutes

Méditation & pleine conscience

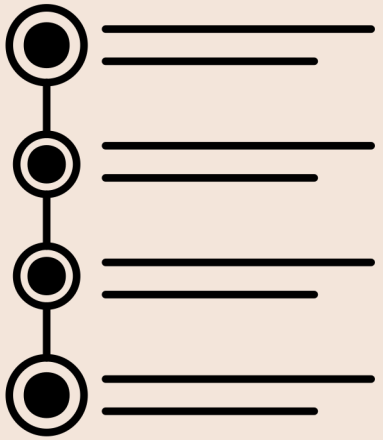


Calm

Ecrire & dessiner ses sentiments



Liste du bonheur



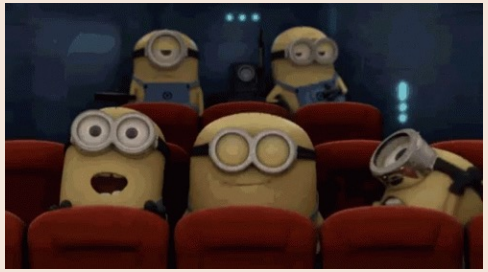
Amis

headspace

YouTube

Ne faites cette activité que si vous savez qu'elle ne vous conduira pas à ruminer des sentiments négatifs.

Lieux publics

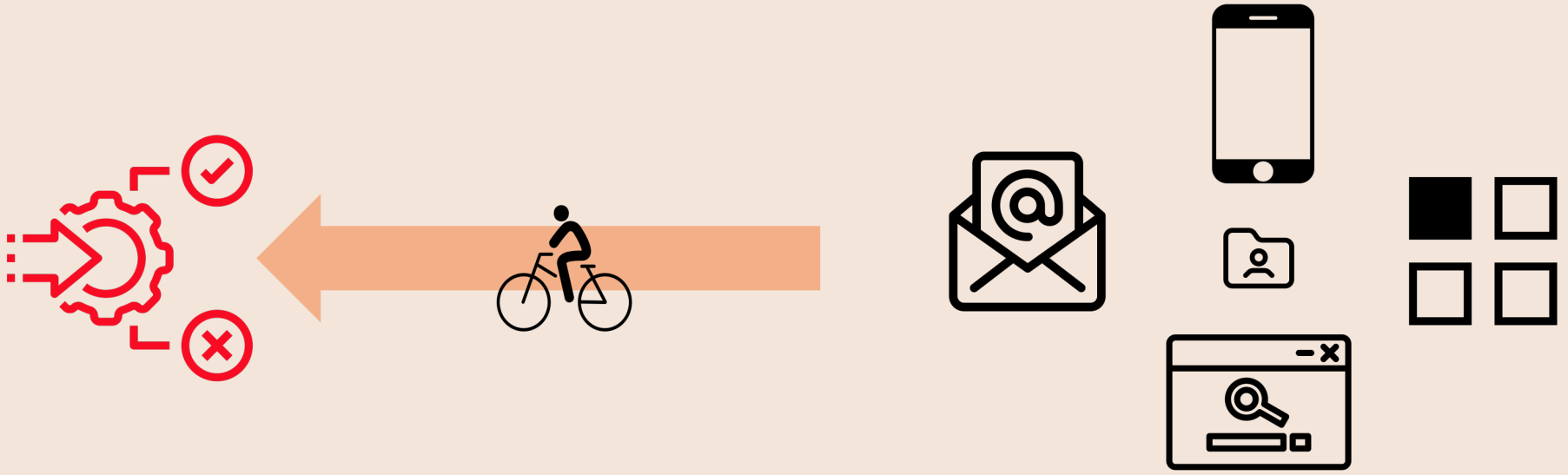


ATELIER 2

CYBERDEFENCE

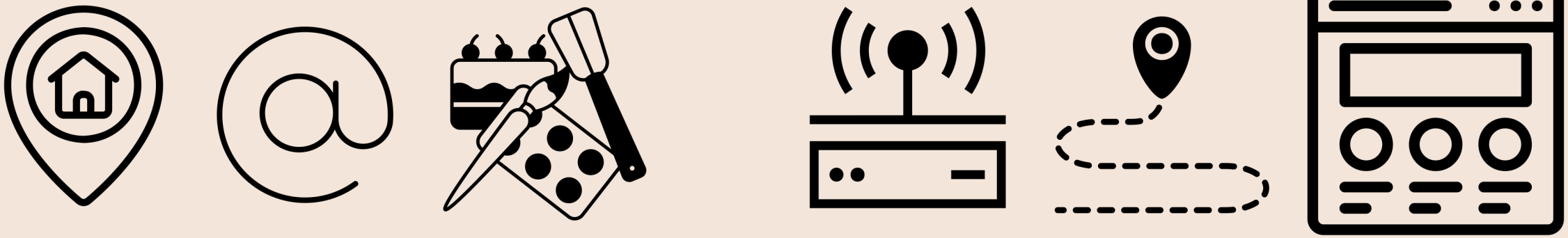
VOS INFORMATIONS PERSONNELLES – UN ENJEU ECONOMIQUE ET TECHNIQUE

Technologies avancées captant de la donnée sur base de vos habitudes, sur votre téléphone, via vos applications, via votre adresse email, via votre moteur de recherche



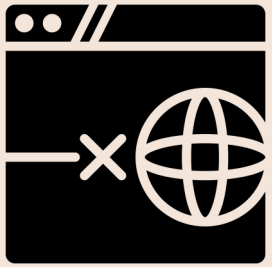
Dans les mains de ton agresseur, ces données peuvent menacer ta vie privée et ton identité en ligne, affecter ton contrôle sur tes profils, et remettre en jeu ta liberté d'accès à l'information.

VOS INFORMATIONS PERSONNELLES – UN ENJEU DE STALKING



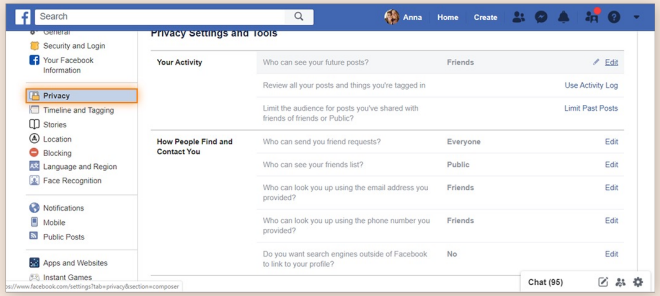
Si tu te rends compte que tu as révélé certaines informations dans le passé sans le vouloir, il n’est pas trop tard pour agir.

COMMENT SE PROTEGER ? QUELQUES CONSEILS



Déconnecte-toi des réseaux sociaux après chaque visite :
En règle générale, ni les trackers ni tes contacts ne pourront suivre tes activités une fois déconnectée)

Installe sur ton navigateur des extensions conçues pour interdire l'accès aux trackers et t'aider à garder ta vie privée, privée. Les trackers sont en général des cookies qui permettent à certains sites comme les réseaux sociaux de "pister" les pages que tu consultes en ligne, souvent à des fins commerciales.



Veiller aux paramètres de confidentialité de chaque réseau social

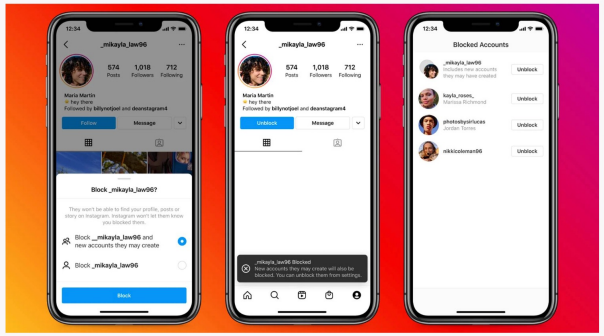
Utilise de préférence des messageries anonymes, et supprime tes historiques de messagerie. Utilise une adresse email « poubelle ». Préférez des navigateurs web sécurisés. Utilisez un vpn pour vos recherches sensibles.

PETITES ASTUCES

- Utilisez des adresses électroniques différentes pour vos différents comptes en ligne (il peut renvoyer vers votre véritable adresse).
- Mettez du ruban adhésif sur votre webcam
- Affichez vos profils Facebook, LinkedIn et Google Plus comme quelqu'un d'autre...Puis réglez les paramètres de confidentialité (capture d'écran)
- Activez le verrouillage du mot de passe sur votre téléphone, votre ordinateur portable et votre tablette.
- Ne vous connectez jamais sur le téléphone, l'ordinateur ou la tablette de quelqu'un d'autre
- Si vous effectuez des achats en ligne ou si vous exploitez une entreprise à domicile, pensez à vous procurer une boîte postale que vous pourrez utiliser à la place de votre adresse personnelle. (Vous minimiserez ainsi les risques d'usurpation d'identité, de harcèlement et autres dangers).
- Installez deux ou trois plugins et extensions anti-tracking sur votre navigateur (comme AdBlock Plus) : comment ajouter un plug in
- Utilisez un VPN pour les choses sensibles

Exemple de techniques et outils

Désormais, la filiale de Facebook va encore plus loin : les personnes victimes de cyberharcèlement vont ainsi avoir la possibilité de bloquer de manière préventive tous les comptes créés par une seule et même personne ayant déjà été bloquée pour comportement dérangeant. La plateforme n'a toutefois pas spécifié de quelle façon elle s'y prenait pour déterminer si un compte appartient à la même personne.



Désormais, les utilisateurs pourront bloquer tous les comptes créés par une personne ayant été bloquée pour cyberharcèlement. Image : Instagram

Le second outil consiste en une sorte de filtre permettant aux utilisateurs de directement enlever de leur liste de DM les messages contenant des mots, phrases ou émojis spécifiques. Ces derniers ont été choisis par Instagram en partenariat avec des organisations luttant contre le harcèlement et les discriminations. Les utilisateurs auront également la possibilité d'ajouter les mots qu'ils souhaitent filtrer.

Que serait Twitter sans ses bots agressifs et autres harceleurs ? L'outil filtrant Block Party, créé par l'ingénieure Tracy Chou, permet de se faire une idée.

Ouvrir son compte Twitter peut être une source d'angoisse. Pour certains, un déluge de messages haineux défile dans la rubrique « Mentions » (les tweets ayant mentionné votre compte). Tracy Chou, une ingénieure de la Silicon Valley, a voulu remédier à cela et faire du réseau social un endroit moins toxique. Elle a mis au point Block Party, une application qui permet de filtrer son compte Twitter.

Les trolls dans un fichier verrouillé

L'utilisateur sélectionne des paramètres : ne voir que les tweets de ses abonnés, des personnes avec lesquelles il ou elle a récemment échangé, ou bien de celles qui sont au moins suivies par 100 abonnés (de quoi éviter les bots). Les contenus filtrés n'apparaîtront plus dans la colonne « Mentions » de Twitter, et seront placés dans un fichier, que l'utilisateur peut consulter quand il se sent prêt - ou jamais. Il est aussi possible de demander à un ami de le consulter à sa place. Block Party est accessible à une quantité limitée de personnes depuis janvier 2021. Pour contourner la liste d'attente, il faut débourser 8 dollars. Un péage anti-troll, explique la start-up sur son site. Le service sera à terme utilisable contre un abonnement mensuel.

L'outil s'adresse à toute personne dont les tweets deviennent viraux (et attirent donc des messages d'inconnus), aux journalistes qui utilisent très régulièrement Twitter, mais aussi aux individus régulièrement harcelés qui souhaitent réunir les preuves de ce harcèlement sans avoir à le subir chaque jour.

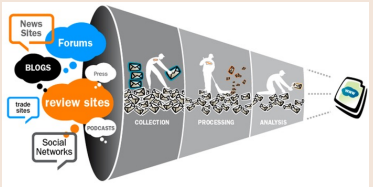
Tracy Chou, suivie par plus de 100 000 abonnés sur le réseau social, a elle aussi été victime de cyberharcèlement depuis ses années lycée. La situation s'est aggravée quand elle a commencé à travailler dans le secteur de la tech chez Qora, puis Pinterest. Elle a donc pensé son outil avec le point de vue d'une victime, explique-t-elle à *Fast Company*.

Une scientifique et inventrice de 15 ans a reçu le tout premier prix 'Enfant de l'année' décerné par le magazine américain Time. Malgré son jeune âge, Gitanjali Rao a signé des créations innovantes dans divers domaines, comme un dispositif capable d'identifier la présence de plomb dans l'eau potable -nommé Tethys– ou une application et extension pour Google Chrome qui utilise l'intelligence artificielle pour détecter le cyberharcèlement.

AT&T Cybersecurity › Blog

Cyberbullying and cybersecurity: how are they connected?

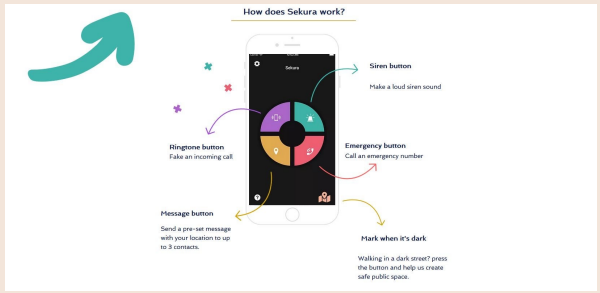
August 21, 2019 | Devin Morrissey



Autres outils

FLAG!
SIGNALEMENT

App’elles

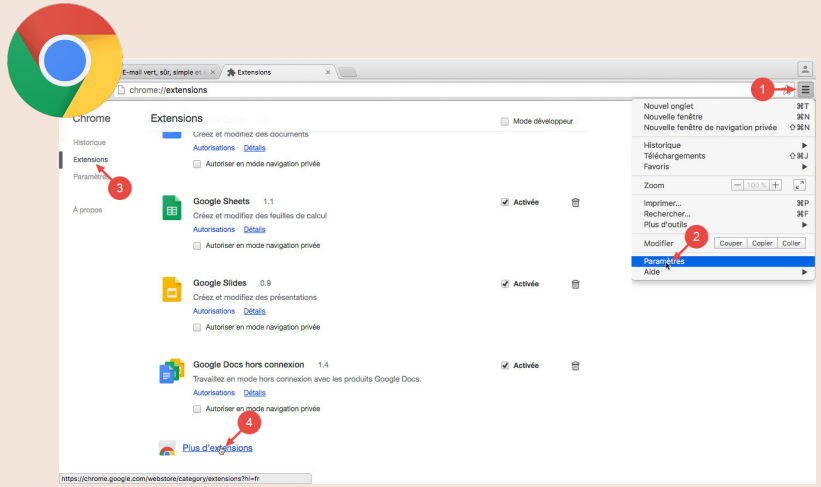


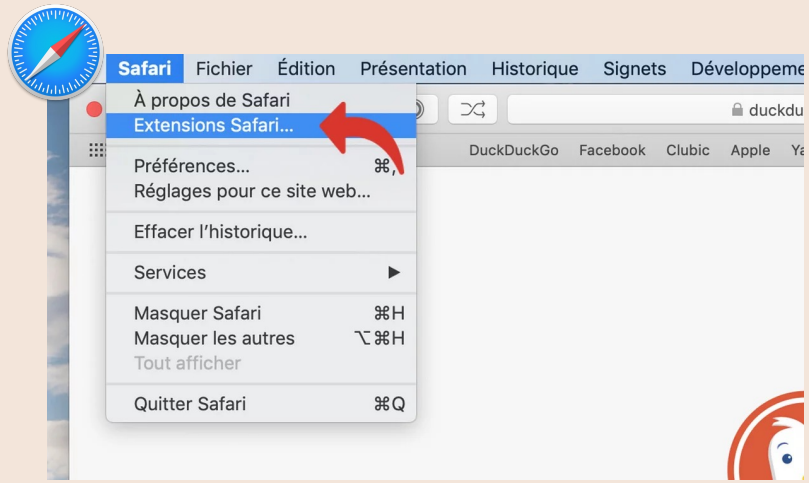
Sekura

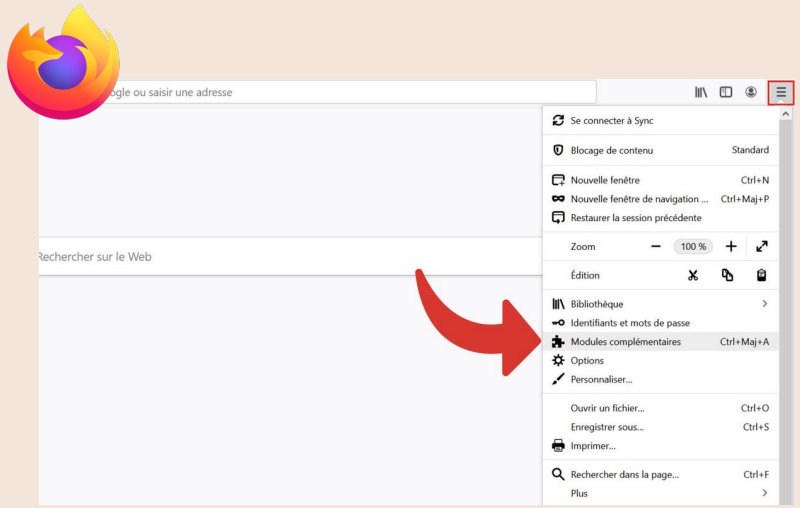
INSTALLER UNE EXTENSION – EXERCICE

ADD-ON **EXTENSIONS**

PLUG-IN



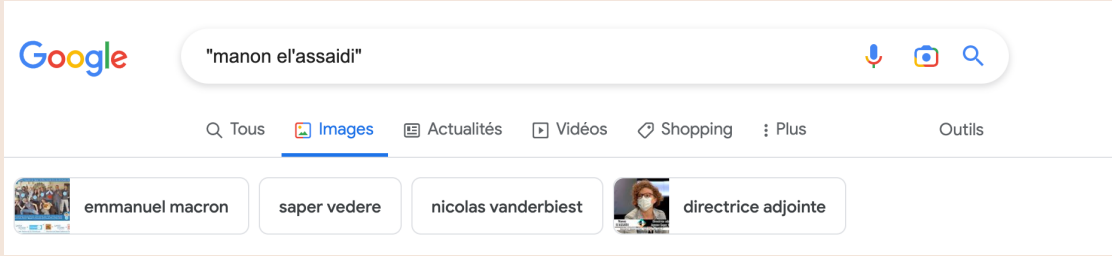


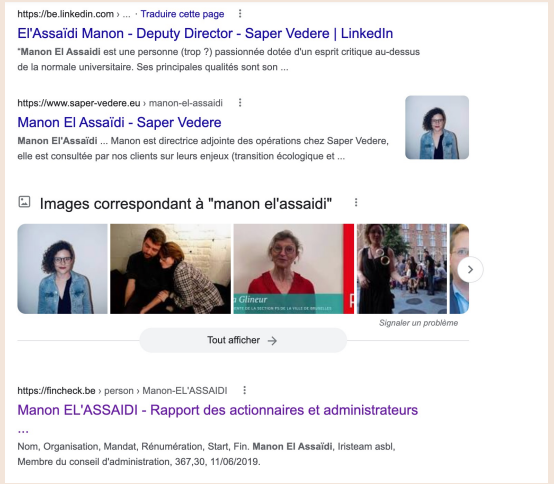


PETIT BILAN DE SECURITE

Feel Good

Exercice 1 : Google « votre nom et prénom» :





PETIT BILAN DE SECURITE

Exercice 1 : Google « votre numéro de téléphone » :

https://issuu.com › sukijenkins › docs › ncissuu.finalflat

Neufchâtel Biography by Suki Jenkins - Issuu

suki Jenkins +32 (0)478 438 988 Manon Elâ€™assaidi +32 (**0)478 476 240**. suki@musicbrussels.com manon.elassaidi@gmail.com ...

PETIT BILAN DE SECURITE

Exercice 1 : Google « votre adresse postale» :

https://www.pagesdor.be › entreprise › Bruxelles › EL+A...

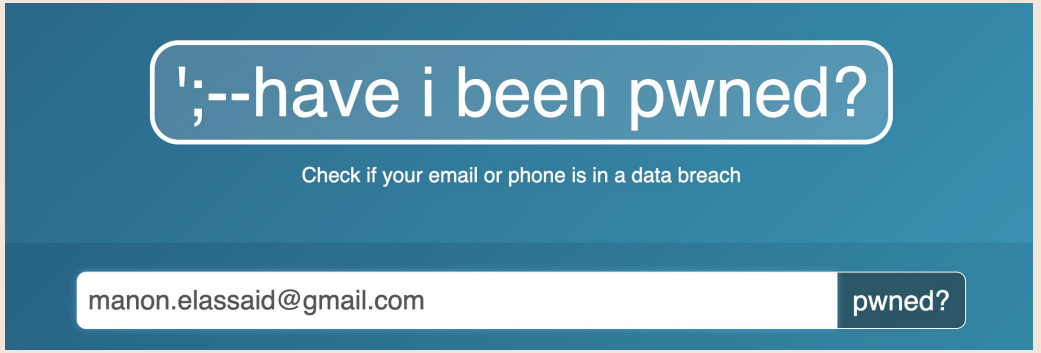
EL ASSAIDI MANON, Forest >> Communication - Pagesdor.be

1190 **Forest Rue Berthelot 21**. Voir la carte. Avis Laisser un avis. Catégories. Communication - Bureaux-conseil · **Forest**. Solutions digitales.

PETIT BILAN DE SECURITE

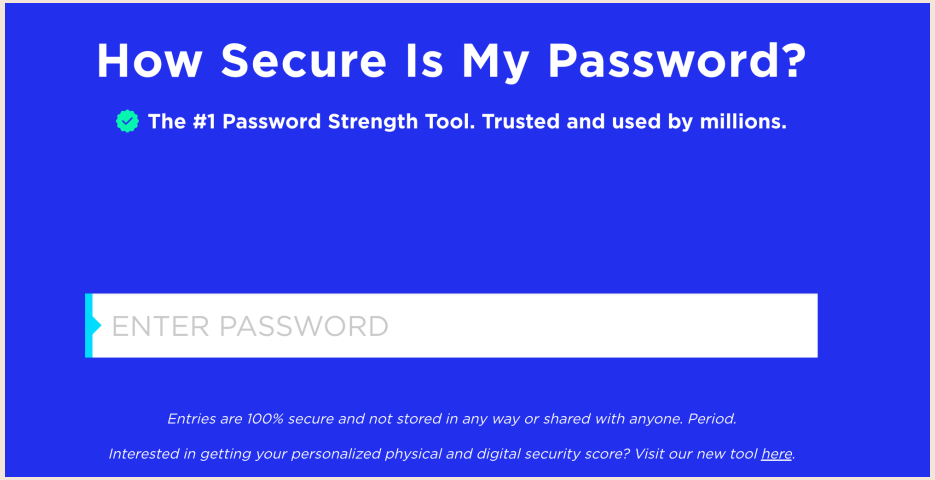
Exercice 2 : HAVE I BEEN PAWNED ?

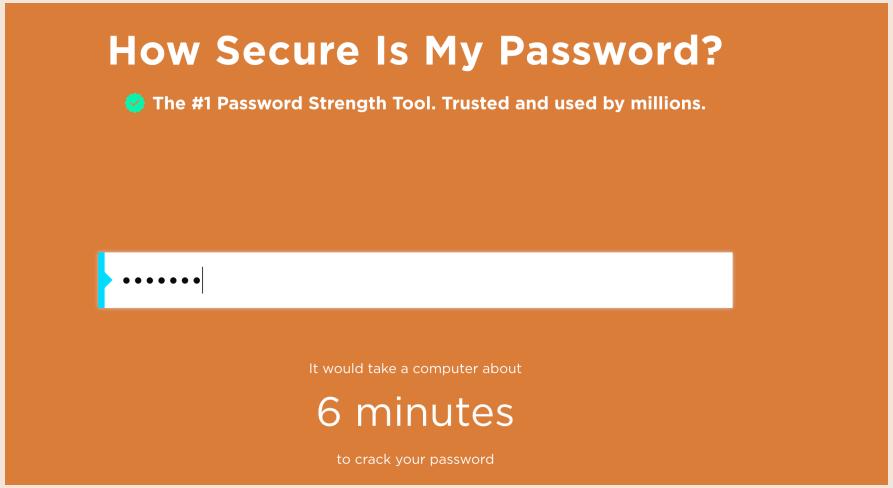
https://haveibeenpwned.com/



LA GESTION DES MOTS DE PASSE

Insérez votre/vos mots de passe et vérifiez sa/leur robustesse





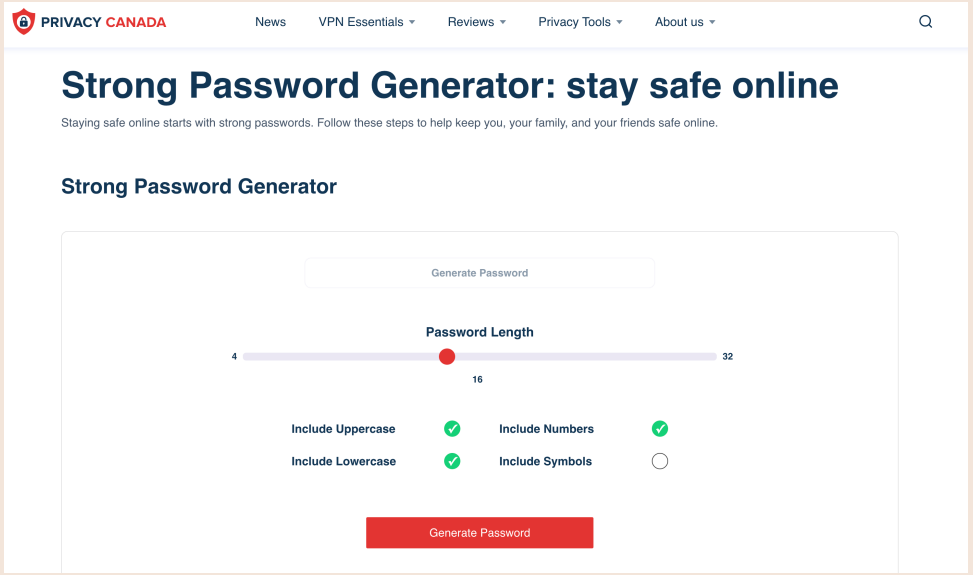
https://www.security.org/how-secure-is-my-password/

LA GESTION DES MOTS DE PASSE

QUELQUES CONSEILS

- ✓ Ne recycle et ne réutilise jamais un mot de passe
- ✓ N'utilise jamais un même mot de passe pour différents sites - crée un nouveau mot de passe pour chaque site
- ✓ Refuse que ton navigateur enregistre tes mots de passe
- ✓ Utilise des phrases secrètes, plus longues que les mots de passe
- ✓ Utilise une combinaison de minuscules, majuscules, chiffres et symboles.

Générateur de mots de passe



https://privacycanada.net/strong-password-generator/

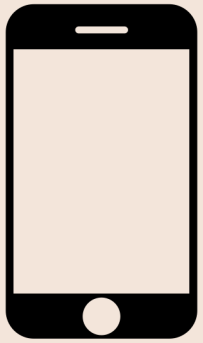
UTILISER UN GESTIONNAIRE DE MOTS DE PASSE

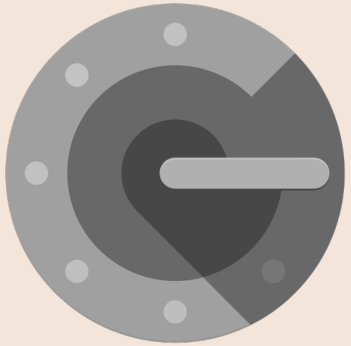
https://keepass.info/

https://www.lastpass.com/fr/how-lastpass-works

Il n'y a pas vraiment consensus sur la fréquence à laquelle un mot de passe doit être changé. Généralement, il est recommandé de changer de mot de passe tous les 3 à 9 mois. Notre recommandation est de changer de mot de passe aussi fréquemment que tu le penses nécessaire pour te sentir en sécurité.

L’authentification en deux facteurs



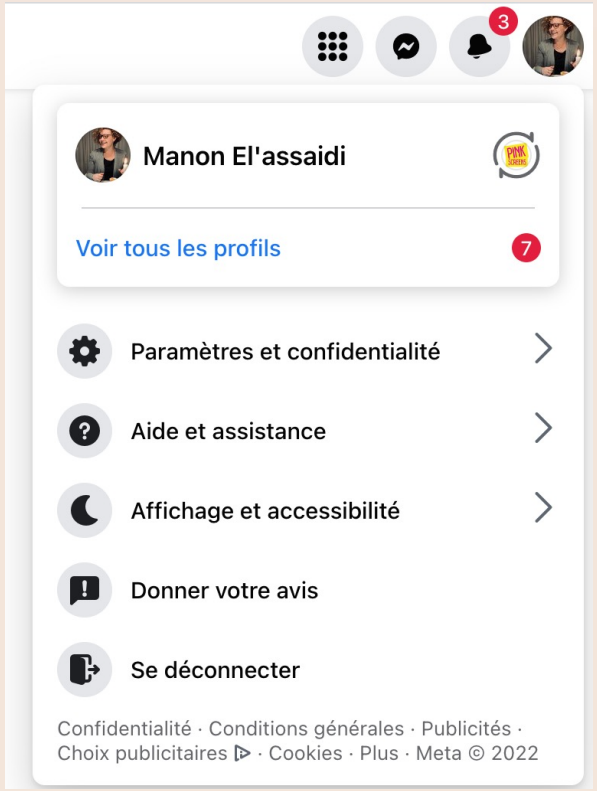


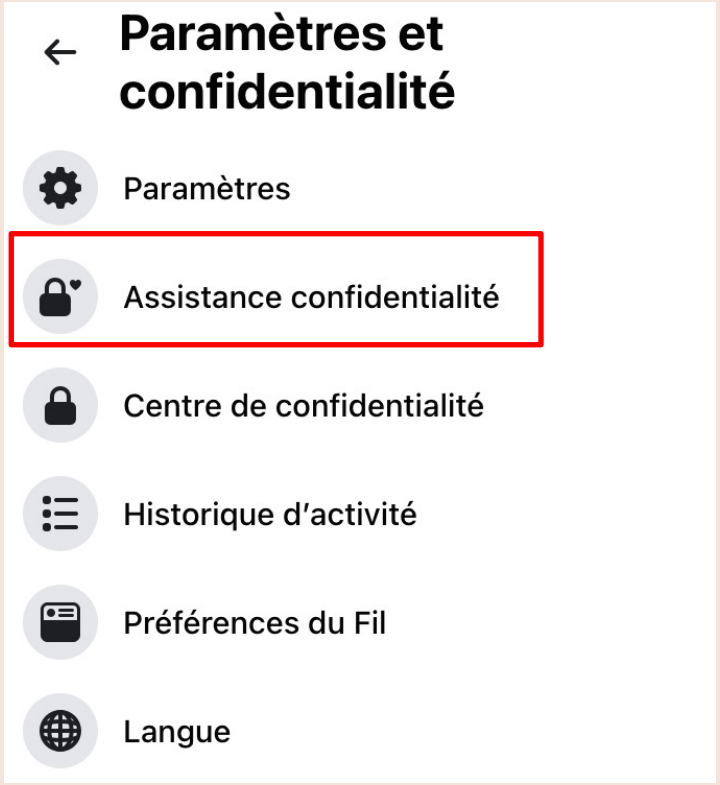
Google
authentificator

2FA
L’authentification à deux facteurs (2FA) rend la tâche plus difficile aux pirates informatiques. En plus de la première étape (ton mot de passe), 2FA requiert une seconde étape pour s’authentifier, une seconde série de données sous la forme d’un code que tu reçois par email, SMS, ou généré par une appli sur ton téléphone.

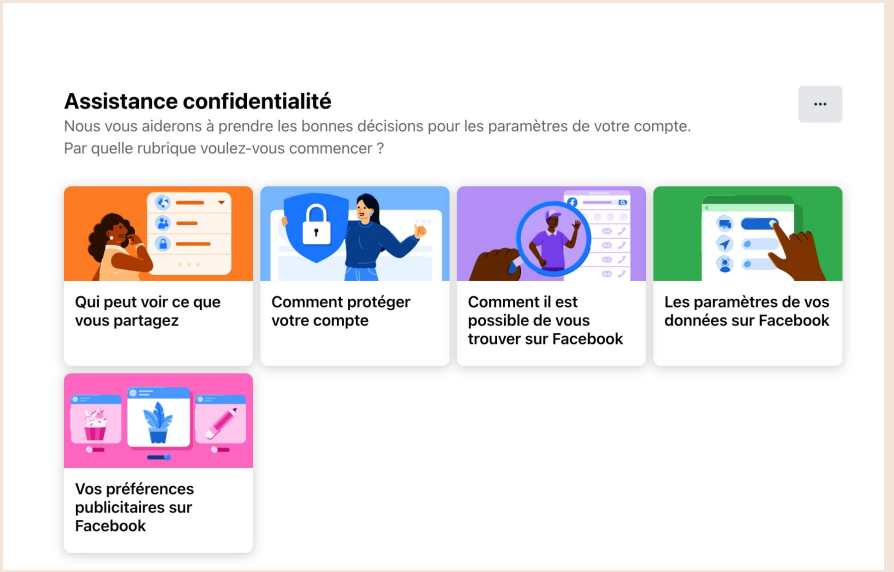
Il n’y a pas vraiment consensus sur la fréquence à laquelle un mot de passe doit être changé. Généralement, il est recommandé de changer de mot de passe tous les 3 à 9 mois. Notre recommandation est de changer de mot de passe aussi fréquemment que tu le penses nécessaire pour te sentir en sécurité.

COMMENT ME PROTEGER SUR FACEBOOK



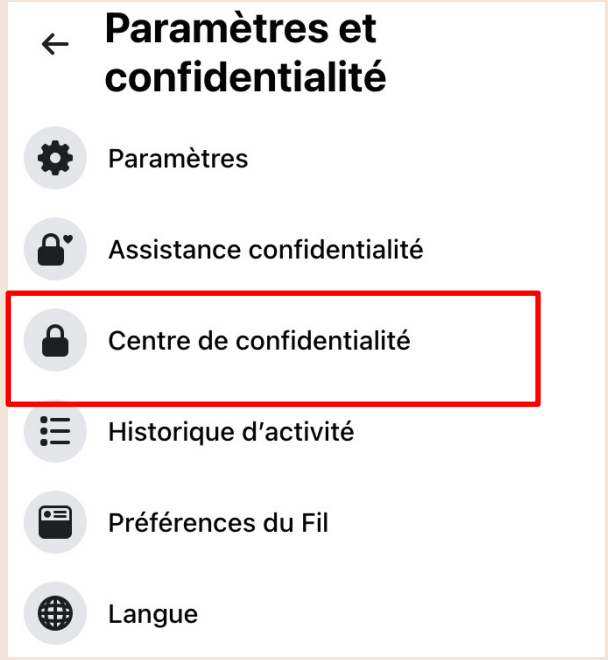


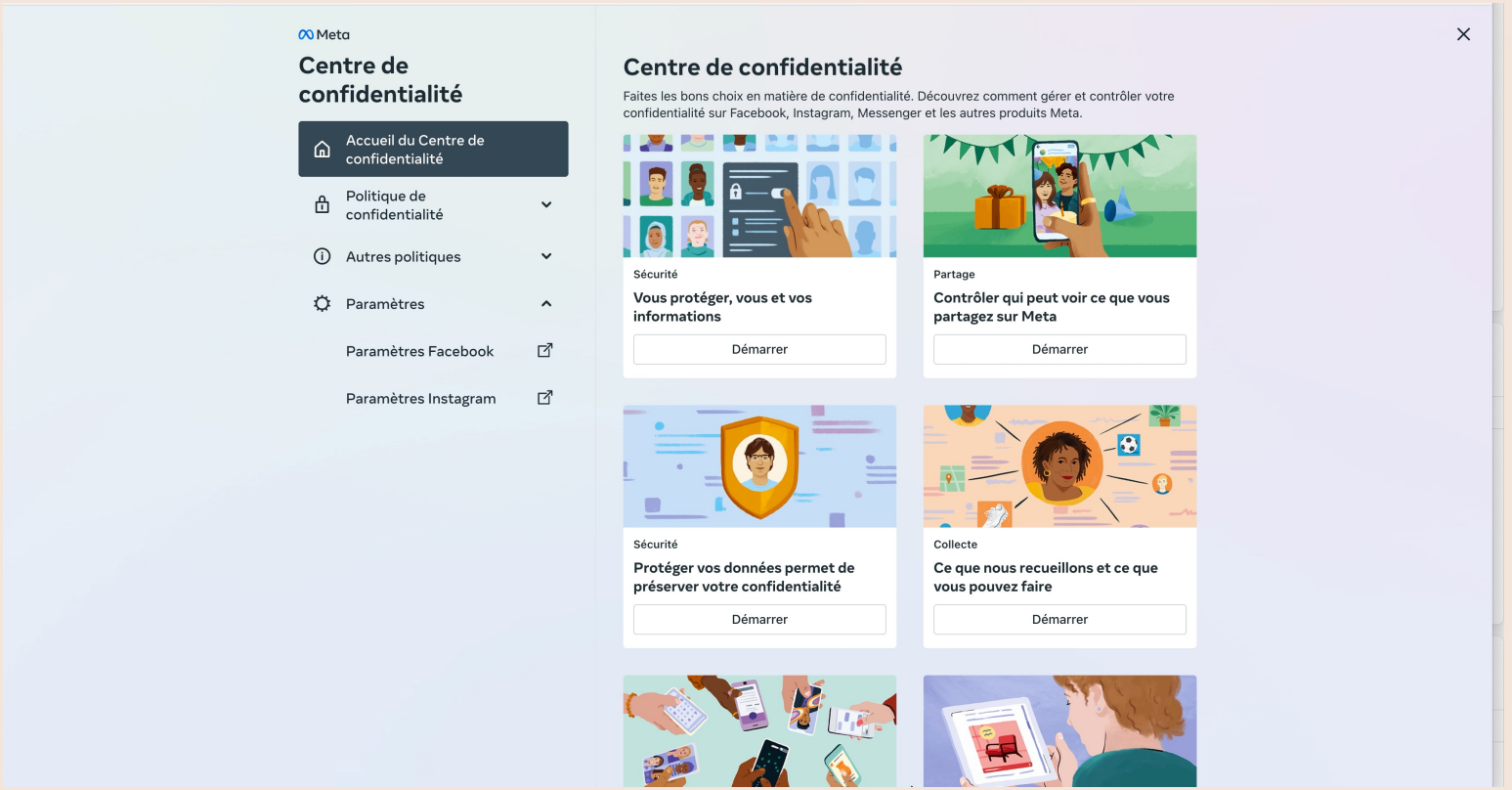
Qui peut voir mon contenu ?
Qui peut me contacter ?
Comment empêcher quelqu'un de me contacter ?



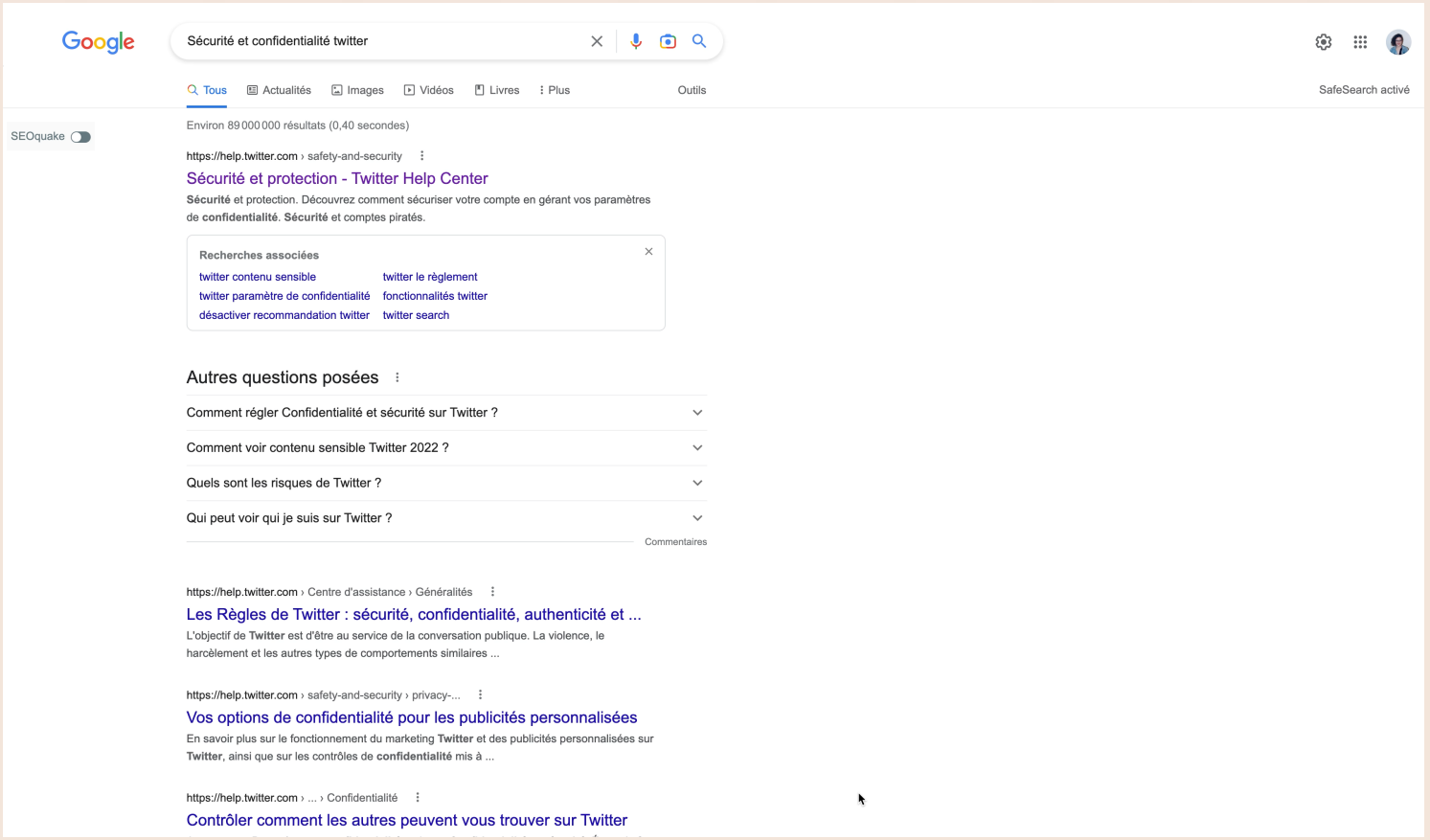
COMMENT ME PROTEGER SUR FACEBOOK

Qui peut voir mon contenu ?
Qui peut me contacter ?
Comment empêcher quelqu'un de me contacter ?



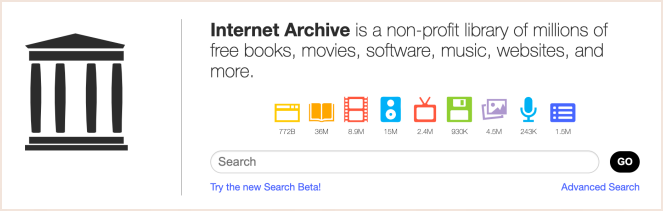


COMMENT ME PROTEGER SUR TWITTER



COMMENT PROTEGER MES APPAREILS : ANDROID

https://securityinabox.org/en/phones-and-computers/android/



Turn off connectivity you are not using

Remove suspicious recovery addresses

Check app permissions

COMMENT PROTEGER MES APPAREILS : ANDROID

https://securityinabox.org/en/phones-and-computers/android/

Turn off advertising and clear your search history

Make separate user accounts

Remove unknown devices from your account

Set your screen to lock with a password

COMMENT PROTEGER MES APPAREILS : ANDROID

https://securityinabox.org/en/phones-and-computers/android/

Turn off advertising and clear your search history

Make separate user accounts

Remove unknown devices from your account

Use apps from trusted sources

COMMENT PROTEGER MES APPAREILS : ANDROID

https://securityinabox.org/en/phones-and-computers/ios/

Turn off tracking

Set your device to erase after too many login attempts

Check your app permissions

Delete Siri and dictation history

COMMENT PROTEGER MES APPAREILS : ANDROID

https://securityinabox.org/en/phones-and-computers/ios/

Turn off access when locked

Turn off location

Remove suspicious accounts

Only use apps from the App Store

COMMENT PROTEGER MES APPAREILS : TOOLS

https://securityinabox.org/en/phones-and-computers/tools/

Malwarebytes

(Android, iOS, Mac, Windows)

An application that scans your phone or computer to detect if malicious software has been installed

Download | See their guide

Avira Antivirus

(Android, iOS, Mac, Windows)

An application that scans your phone or computer to detect if malicious software has been installed

Download | See their guide

Bitdefender

(Android, iOS, Mac, Windows)

An application that scans your phone or computer to detect if malicious software has been installed.

Download | See their guide

(Windows)

An application that can help protect your Windows computer by disabling certain risky features and services that are typically exposed

Download

Tools from Objective-See.com

(Mac)

Apps that configure, protect and scan your Mac computer to help detect and disable malicious software. We recommend LuLu, Do Not Disturb, OverSight, KnockKnock, BlockBlock, Task Explorer, Netiquette, Lockdown, and RansomWhere?.

Download | See their guide

DangerZone

(Linux, Mac, Windows)

Free and open-source app that convert documents and pictures which may infect your computer into safe form.

Download | See their guide

Qubes OS

A secure operating system that provides an alternative to Windows, Mac or Linux. Qubes OS lets you use different "compartments" (virtual machines known as *qubes*) to do different things on your computer, which helps protect against malicious software.

Download | See their guide

FIREFOX ADD-ONS TO HELP PROTECT AGAINST MALICIOUS SOFTWARE

NoScript

(Firefox, Chrome, Edge)

Stops malware on websites from infecting your device. (Until it is properly configured, NoScript makes some websites appear broken.)

Download | See their guide

uBlock Origin

(Firefox, Chrome, Edge, Opera)

A content blocker that can help protect you from spyware and malware when you browse the web

Download | See their guide

PROTECT AGAINST PHYSICAL THREATS

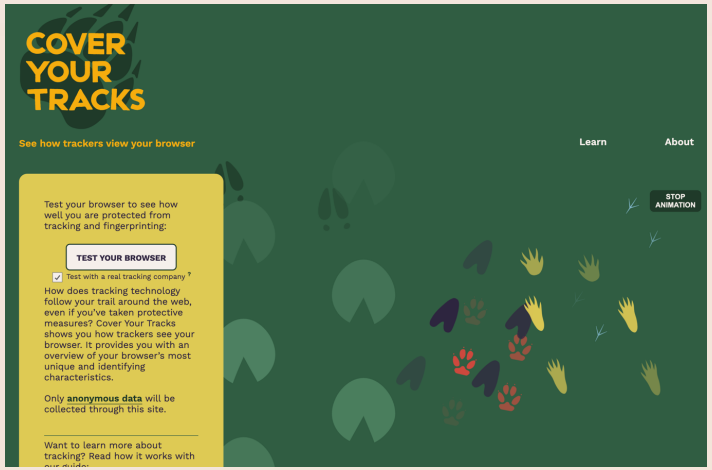
Haven

(Android)

A free and open-source app that turns your Android device into a surveillance camera

Download from Google Play

TESTER VOTRE NAVIGATEUR



Our tests indicate that you have **some protection** against Web tracking, but it has **some gaps**.

IS YOUR BROWSER:

Blocking tracking ads?	**Partial protection**
Blocking invisible trackers?	**Partial protection**
Protecting you from fingerprinting?	**your browser has a randomized fingerprint**

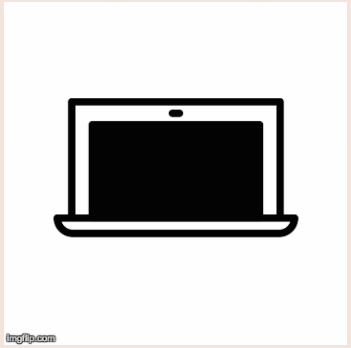
Still wondering how fingerprinting works?

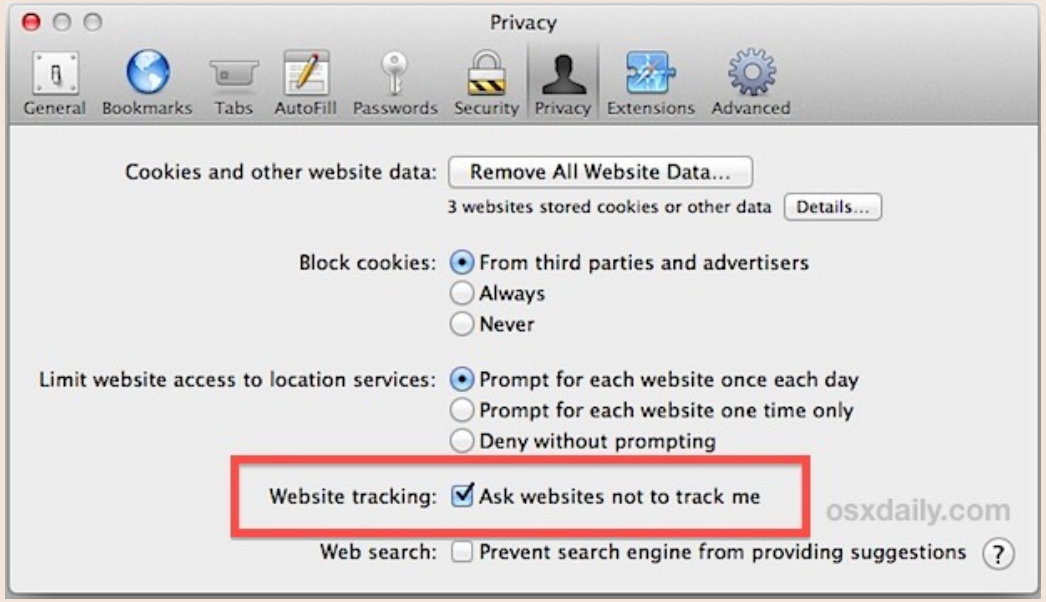
LEARN MORE

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

https://coveryourtracks.eff.org/

INTERDIRE LE SUIVI





Chrome > Paramètres > Afficher les Paramètres Avancés > Confidentialité > Envoyer une demande "Interdire le suivi" pendant la navigation

Firefox > Options > Vie privée > Gérer les paramètres Ne pas me pister

Safari > Menu > Préférences > Confidentialité > Suivi de site web > Demander aux sites web de ne pas me suivre

Autres navigateurs et moteurs de recherche

- Le navigateur Brave bloque automatiquement les publicités et les trackers
- Le logiciel de navigation Tor permet de consulter le web de manière anonyme
- DuckDuckGo est un moteur de navigation privée qui ne piste pas ses utilisateurs
- Le moteur de navigation privée StartPage n'enregistre jamais ton adresse IP, ni ne piste tes recherches

INTERDIRE LE SUIVI

Mode Navigation privée (Google Chrome)

•Le Mode Navigation privée sur le web empêche Google Chrome d'enregistrer l'historique des pages que tu visites ou de tes téléchargements

•Personnaliser et contrôler Google Chrome > Nouvelle fenêtre de navigation privée

•Ou appuie simultanément sur les touches : Ctrl + Maj + N

Nouvelle fenêtre privée (Firefox)

•Pour ouvrir une nouvelle fenêtre de navigation privée dans Firefox

•Ouvre le menu Firefox > Icône Fenêtre Privée

•Ou appuie simultanément sur les touches : Ctrl + Maj + P

Nouvelle fenêtre de navigation privée (Safari)

•New Private Window empêche Safari de conserver un historique des pages que tu visites

•Fichier > Nouvelle fenêtre privée

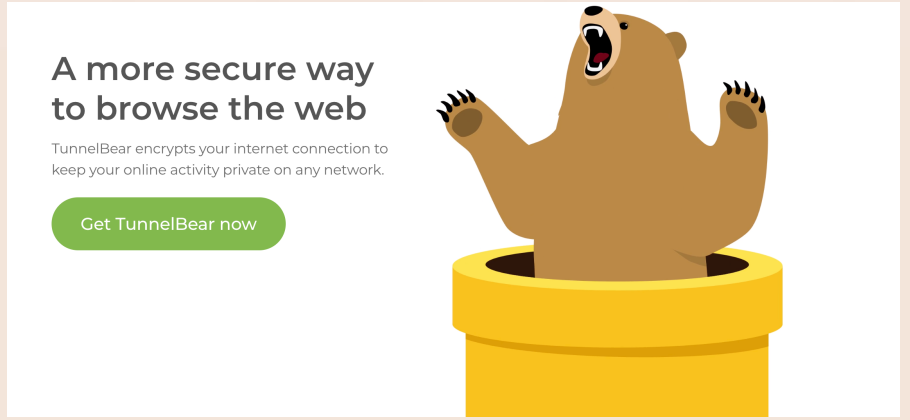
•Ou appuie simultanément sur les touches : Ctrl + Maj + N

INTERDIRE LE SUIVI

https://chrome.google.com/webstore/search/VPN?_category=extensions

Menu Firefox > Modules > Catalogue > Découvrir davantage de modules > tape “VPN” dans la barre de recherche

OkayFreedom VPN



https://www.torproject.org/fr/download/languages/

OpenVPN
OpenVPN is an application that is used to create a secure tunnel from your computer to the server you wish to connect to. It does this by means of SSL (Secure Sockets Layer)/TLS (Transport Layer Security), which are cryptographic protocols that encrypt communications over a network. (See Words for more information.) Alternatively, if you are using Windows, you can set up a VPN without OpenVPN.

INTERDIRE LE SUIVI

https://www.eff.org/https-everywhere

https://www.ublock.org/fr

Efface ton historique de navigation

•Chrome > Historique > Effacer les données de navigation

•Firefox > Ouvrir le menu > Historique > Effacer l'historique récent

•Nous recommandons les utilitaires de nettoyage suivants:

CCleaner

BleachBit

EN CAS D'ATTAQUE

Signalez un problème

Des questions ou des problèmes sur internet? Voici des organisations qui peuvent vous aider.

Dénoncer des délits en ligne

Vous pouvez **dénoncer un délit commis en ligne** en vous rendant dans votre commissariat local. Les policiers locaux collaborent avec les Computer Crime Units Régionales et Fédérale (RCCU et FCCU) spécialisées dans la lutte contre les crimes informatiques.

Porter plainte à la police

Pédopornographie

Si vous avez trouvé des images d'**abus sexuels d'enfants** sur internet, signaler-les à Child Focus sur www.stopchildporno.be

Protection des données privées

Si vous avez des questions sur la **protection de vos données** ou si vous souhaitez signaler une fuite de données contactez l'Autorité de protection des données.

Autorité de protection des données

Signaler des incidents en ligne

Si, en tant qu'entreprise ou organisation, vous êtes confronté à un incident sur internet ou sur votre réseau et que vous souhaitez le **signaler ou obtenir des conseils**: www.cert.be. CERT.be est la Cyber Emergency Response Team.

Signaler du phishing

Vous avez reçu **un message suspect** ? Envoyez-le à l'adresse suspect@safeonweb.be et supprimez-le ensuite. Si vous recevez un message suspect au travail, vous devez suivre les procédures en vigueur pour le phishing. Par exemple, l'envoyer vers le service ICT.

Qu'est-ce que suspect@safeonweb.be ?

Signaler une fraude ou une esqroquerie

Vous êtes victime d'une **tromperie, d'une arnaque, d'une fraude ou d'une escroquerie**, ou vos droits en tant que consommateur ou entreprise n'ont pas été respectés ? Point de contact

https://meldpunt.belgie.be/meldpunt/fr/bienvenue

Signaler une fraude en ligne à l'investissement et au crédit

Vous êtes victime d'une **fraude en ligne à l'investissement et au crédit** ?

Contactez la FSMA.

Votre compte a été piraté

Informez le site web auquel appartient votre compte.

https://safeonweb.be/fr/liens