

PROTÉGER SA VIE PRIVÉE SUR SON MOBILE

GUIDE TECHNIQUE



INTRODUCTION

La libération récente de la parole des femmes a montré l'urgence d'agir pour faire reculer les violences subies quotidiennement par des millions de femmes en France. Le développement de l'utilisation des portables et des réseaux sociaux, fait naître de nouvelles formes de violences à l'égard des femmes : surveillance via leur mobile, trackage sur internet par les auteurs de violence ... Ce type de harcèlement a tendance à augmenter ainsi que la violence des attaques.

L'impact est dévastateur pour les femmes victimes. Il conduit à un isolement très rapide et très important : la victime se sent piégée 24h/24h, sans répit ni repos elle refuse d'en parler de peur de ne pas être entendue. Elle vit dans l'anxiété permanente et le sentiment de perdre le contrôle de sa vie.

L'objectif de ce guide est de mieux accompagner les victimes en leurs permettant de :

- repérer si elles sont surveillées
- se débarrasser des connexions indésirables
- sécuriser les réseaux sociaux
- trouver l'interlocuteur en Seine-Saint-Denis qui les soutient et les accompagne.

Ensemble, agissons !

Le directeur Départemental de la Cohésion sociale

Alexandre Martinet



SOMMAIRE

	INTRODUCTION	1
I.	MON PORTABLE EST-IL SURVEILLÉ ?	2
1.	Les signes	2
2.	L'application de contrôle	3
3.	Le logiciel espion	4
4.	Attention à la synchronisation	7
II.	SÉCURISER MES RÉSEAUX SOCIAUX	14
1.	Facebook	14
2.	Instagram	21
3.	Snapchat	25
4.	WhatsApp	27
III.	ME PROTÉGER	29
1.	Conservation des preuves	29
2.	Procédure juridique	30
3.	Contacts utiles	33

I. MON PORTABLE EST-IL SURVEILLÉ



1. Les signes :

La victime est questionnée sur des informations que son interlocuteur ne devrait pas connaître :

- Ses conversations écrites et téléphoniques.
- Un site qu'elle aurait consulté.
- Un évènement auquel elle aurait assisté.
- Les trajets qu'elle aurait effectués.
- Des photos ou vidéo dans son téléphone.
- Ou même sur ses actions au moment précis où son interlocuteur la contacte

Le portable fonctionne globalement beaucoup moins bien :

- La batterie se décharge vraiment vite sans raison particulière.
- L'utilisation est devenue plus lente voire pénible.
- Il bug et parfois se relance sans être soumis à une pression particulière.
- Certaines fonctionnalités telles que la position, les données internet ou le wifi s'activent sans raison.
- Le rétro-éclairage se modifie sans qu'on y touche.

C'est peut-être à cause d'un logiciel espion.

Une ou plusieurs applications sont soudainement présentes sur le mobile.

C'est peut-être à cause d'une application de contrôle.

2. L'application de contrôle :



Qu'est-ce que c'est ?

C'est une application de type **contrôle parental**. Elle est très souvent gratuite et on peut la trouver sur l'App Store ou GooglePlay. L'application permet de recevoir les messages d'un autre téléphone en temps réel, de surveiller le GPS, les applications installées et l'historique de navigation de ce téléphone. Pour fonctionner l'application doit être installée sur le portable qui reçoit les informations et sur celui qui est surveillé.

Il faut donc **autoriser l'installation** d'une telle application sur son portable pour qu'elle puisse transmettre des informations.

Cependant, il est tout à fait possible pour quelqu'un de l'installer sans le consentement de sa victime. Pour cela, il suffit de subtiliser son téléphone assez longtemps pour la télécharger et approuver toutes les autorisations de partage de données.

Comment s'en débarrasser ?



Cette méthode de surveillance est très simple à mettre en application, mais elle est aussi très facile à débusquer. Il suffit de faire le **tri dans les applications** du mobile : consulter l'écran d'accueil attentivement, fouiller tous les dossiers d'organisation des applications ainsi que la liste des applications dans les paramètres. **Si la victime ne reconnaît pas une application dans son portable, il faut la supprimer.**

3. Le logiciel espion :



Qu'est-ce que c'est ?

Le logiciel espion est bien plus difficile à détecter que l'application de contrôle, il est souvent payant et certains sites proposent des offres plus ou moins fournies selon les gammes de prix. Ces logiciels ne nécessitent pas forcément d'accéder physiquement au téléphone de la victime pour l'infecter. En fonction des différentes offres, il est possible d'avoir accès à la position GPS de la victime, son calendrier, ses SMS, sa galerie d'images jusqu'à avoir accès à l'intégralité de ses réseaux sociaux (applications de rencontres compris), son historique de navigation et même activer sa caméra, son micro et écouter ses appels en direct !



Un premier indice pour l'identifier

Un premier indice pour repérer ce type de logiciel est d'observer le fonctionnement du téléphone, **s'il fonctionne péniblement** (comme décrit dans les signes page 2), il est possible que le mobile soit effectivement surveillé.


Il faut commencer par aller dans les **paramètres** du téléphone de la victime : dans la **liste des applications** d'abord. Il faut alors inspecter minutieusement la liste pour voir s'il y a des **applications sur lesquelles la victime aurait le moindre doute**. Malheureusement, ce n'est généralement pas aussi facile car ces logiciels sont bien cachés et sont rarement présents dans le téléphone sous leurs vrais noms.

Note : Les logiciels les plus utilisés sont *Hoverwatch, mSpy, Snoopza, FoneMonitor et Spyzie*.



Un deuxième indice

Si c'est un **Iphone**, il aura probablement été "**jailbreaké**". Cela permet, au moyen d'une application facilement téléchargeable sur l'App Store, au logiciel espion de s'installer et **de changer la structure de l'Iphone** (attention ce n'est pas systématique, certains logiciels "premium" offre la surveillance sans "jailbreak").

Si une telle application est présente sur le téléphone, elle peut être trouvée dans **la liste des applications**. On peut également trouver sa trace dans l'historique de navigation ou de téléchargement dans l'Appstore. L'application de jailbreak la plus connue est **Cydia**. 

Un troisième indice

Dans **les paramètres**, il faut regarder dans les onglets **d'utilisation de la batterie** et **d'utilisation des données**. La victime pourra repérer si une activité lui semble anormale.

Généralement, ces logiciels espions envoient les informations recueillies sur le téléphone sur une plateforme consultable en ligne par la personne surveillant la victime. Ces informations sont envoyées sous forme **de rapport et de manière périodique**, ce qui génère des **pics d'activités** à des moments précis de la journée. On peut donc repérer ces pics sur les graphiques.



Pour repérer le logiciel espion :

Sous le graphique d'utilisation de la batterie ou d'utilisation des données mobiles, il est possible d'analyser la liste des applications et leur pourcentage d'utilisation. Si la victime ne reconnaît pas une application ou qu'une application a une activité anormalement élevée, il faut s'en inquiéter.



Comment se débarrasser d'un logiciel espion :



Après avoir identifié les applications, dossiers ou fichiers suspects, il faut les **supprimer**. En dernier recours, la victime peut remettre son téléphone à la **version d'usine** ou en changer. Attention, certains de ces logiciels ont des options pour notifier à leur client si le portable ou le numéro change et ainsi continuer à traquer la victime. Le mieux est donc de **changer de portable et de numéro en même temps**.



4. Attention à la synchronisation :



Qu'est-ce que c'est ?

A partir d'un **même compte** il est possible d'accéder aux informations qu'il contient via différents appareils. Un Android ou un Iphone sont reliés respectivement à un compte **Gmail** ou un compte **Apple**, ces comptes sont liés aux téléchargements d'applications, historiques de navigation, calendrier, contacts, mail, maps et même, parfois SMS. Il suffit donc d'avoir **l'identifiant et le mot de passe** de la victime et de **synchroniser ses comptes** via un autre portable, une tablette ou sur un ordinateur pour avoir accès à son quotidien.

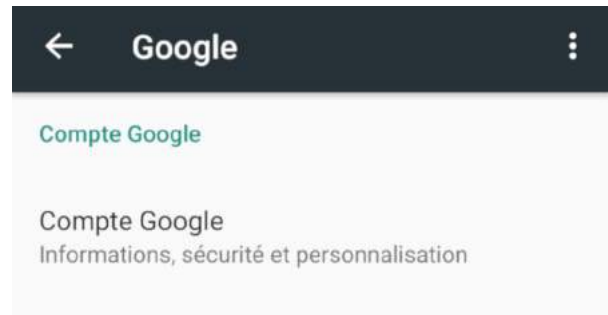


Les smartphones Android

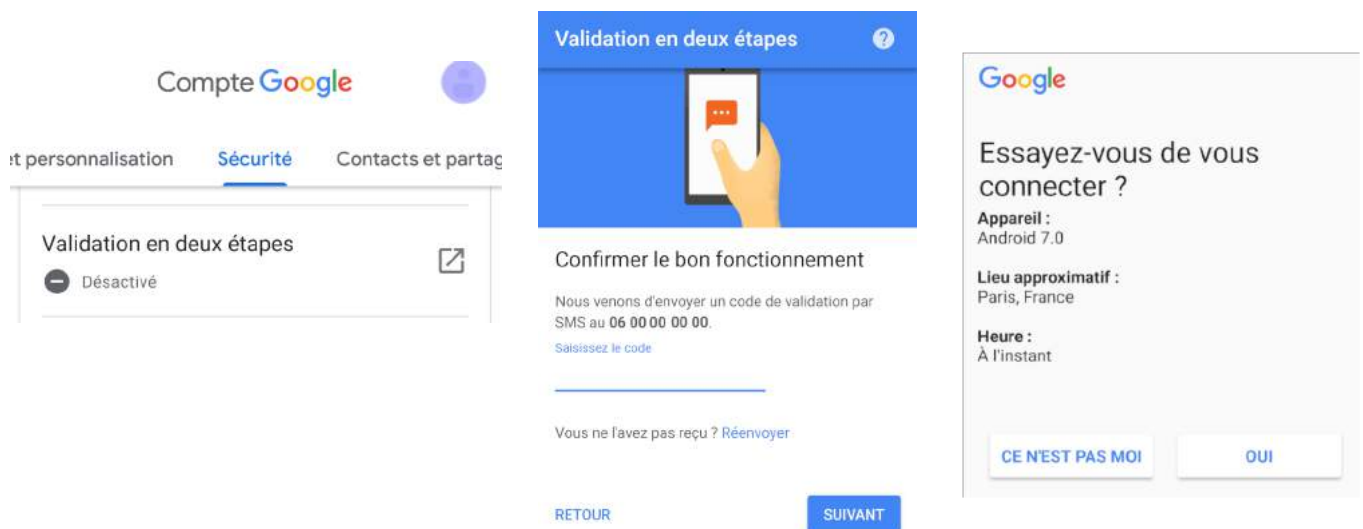
Pour utiliser un smartphone **Android**, il faut posséder un compte affilié, bien souvent via un **compte Gmail**. Avoir un compte Android via Gmail signifie que **toutes les activités** du portable sont reliées à **Google**, lequel enregistre un grand nombre d'informations dans le but d'apporter plus de fluidité dans l'usage du portable. Google regroupe un nombre important d'applications comme Maps, GooglePhotos, Drive, Docs, Youtube etc , mais pour faciliter l'usage du smartphone au quotidien et surtout **la synchronisation des données**, Google enregistre aussi les contacts, les évènements, les enregistrements audios, les notes, les achats, les trajets effectués, les applications téléchargées, les recherches et contenus visionnés sur tous les supports Google... Le risque étant qu'avec un accès au compte Google d'une personne, on **accède également à toutes ces informations**.

Comment éviter la synchronisation ?

Dans les paramètres du portable, il est possible d'accéder à un volet "Google Services", on peut directement se connecter à son compte Google depuis cette catégorie.



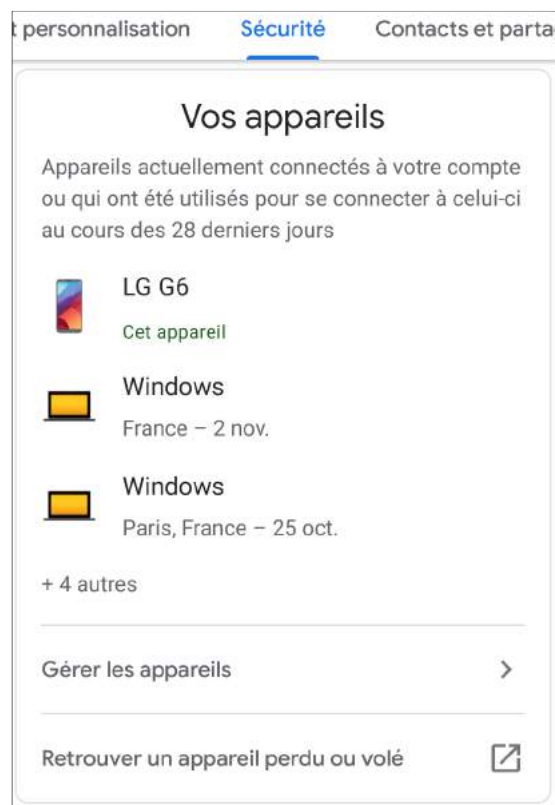
Une fois entré dans le compte Google, la catégorie "Sécurité" permet de gérer la sécurité du compte, notamment avec la validation en deux étapes, qui rend la connexion du compte plus sûre car il ne faut plus seulement entrer le mot de passe pour ouvrir le compte mais également confirmer la connexion avec le téléphone de l'utilisateur. Un test est lancé pour activer la procédure.



Grace à la validation en deux étapes le propriétaire du compte est immédiatement prévenu sur son portable si un appareil tente de se connecter et il est possible de décliner la connexion.

Comment repérer la synchronisation :

Dans la catégorie "sécurité", il est également possible d'avoir dans cette même catégorie une liste de tous les appareils qui se sont connectés au compte, ainsi que la date, l'heure, une adresse IP et un lieu approximatif. Si la victime ne reconnaît pas un appareil, il faut impérativement changer de mot de passe.



Un point de vigilance !

Les applications de stockage sont très souvent pré-installées comme **Google Photos** ou **Drive**. Elles **stockent en ligne** nos fichiers et photos sans que l'on s'en aperçoive. Elles gardent même les photos qui ont été **supprimées** sur la mémoire interne du téléphone.

La double validation s'applique à toutes les interfaces Google. L'utilisateur du compte peut donc être prévenu si quelqu'un tente de s'y connecter.



Les Iphones

Pour utiliser un Iphone, il faut posséder un **compte Apple**. Avoir un compte Apple signifie que toutes les **activités de l'Iphone sont reliées**. Un grand nombre d'informations sont enregistrées en conséquence, dans le but d'apporter plus de fluidité dans l'usage du portable et des **différents appareils Apple**. Des informations telles que les photos, les applications téléchargées sur l'AppStore, les fichiers présents sur le Cloud, les iMessages, les événements du calendrier et la localisation des différents appareils du compte sont ainsi partagées pour faciliter l'usage de l'Iphone au quotidien.

Il est donc possible pour une personne mal intentionnée d'accéder à toutes ces informations si elle possède **l'identifiant et le mot de passe du compte Apple**.

Comment éviter la synchronisation ?

Dans les **réglages** de l'Iphone, il est possible d'accéder au compte Apple en sélectionnant **l'identifiant du compte** sous "Réglages".

Réglages



Une fois entré dans le compte Apple, il faut appuyer sur **"Mot de passe et sécurité"**.

Il faut ensuite appuyer sur "Identification à deux facteurs" pour activer cette fonction.

L'identification à deux facteurs rend la connexion au compte plus sûre, car il ne faut plus seulement entrer le mot de passe pour ouvrir le compte, mais également confirmer la connexion avec un code communiqué par SMS ou appel.



Il faut ensuite renseigner son numéro de téléphone et choisir si l'utilisateur préfère recevoir son code par SMS ou appel. Il faut donc entrer un nouveau code à chaque connexion au compte Apple.



The screenshot displays the 'N° de téléphone' setup screen. It includes the following elements:

- Section title: N° de téléphone
- Instruction: Saisissez un numéro de téléphone pouvant être utilisé pour valider votre identité à l'aide d'un SMS ou d'un appel téléphonique.
- Country field: Pays, with a dropdown menu showing '+33 (France)' and a right arrow.
- Number field: Numéro, with the text 'obligatoire'.
- Verification method section: VALIDER PAR :
- Radio button for SMS, which is selected with a checkmark.
- Radio button for Appel téléphonique.

Comment repérer la synchronisation :

Dans la catégorie "Identifiant", il est possible d'avoir accès aux options de partage du Cloud, de l'AppStore et de la localisation. Pour empêcher le partage de ces informations via d'autres appareils du compte, il faut appuyer sur la fonctionnalité concernée et ensuite d'en désactiver le partage.



On peut également vérifier que le **partage familial** n'est pas déjà activé sur l'iPhone de l'utilisateur et n'envoie pas des informations à d'autres appareils par ce biais.



Partage familial

Jusqu'à six membres de votre famille peuvent partager musique, films, apps, espace de stockage et plus encore.

Vous disposerez également d'un album photos familial, d'un calendrier familial et pourrez avoir accès aux appareils de la famille avec Localiser mon iPhone.



Démarrer



Dans la catégorie "Identifiant", il est également possible d'avoir accès à la **liste des appareil connectés** au compte Apple. Pour voir les détails d'un appareil, il faut appuyer sur l'icône correspondante.

Si la victime ne reconnaît pas cet appareil, il est possible de **le localiser** si le partage de localisation est activé, on peut également voir **le numéro de série de l'appareil connecté** et le supprimer du compte.



II. SÉCURISER MES RÉSEAUX SOCIAUX



Il est très important de **sécuriser l'accès aux réseaux sociaux** qui sont utilisés quotidiennement pour converser, s'envoyer des photos et autres éléments. **Un piratage** de ses réseaux peut avoir des conséquences **dramatiques** autant dans la sphère privée que sociale de l'utilisateur.

1. Sécuriser l'accès à Facebook :



Pour accéder aux **paramètres de sécurité**, il faut commencer par se rendre dans les **paramètres de l'application**. Pour cela, il faut appuyer sur les trois barres à côté de la cloche de notification et ensuite appuyer sur "**Paramètres et vie privée**", puis "**Paramètre**".



Sécurité

Modifiez votre mot de passe et prenez d'autres mesures pour renforcer la sécurité de votre compte.



Sécurité et connexion

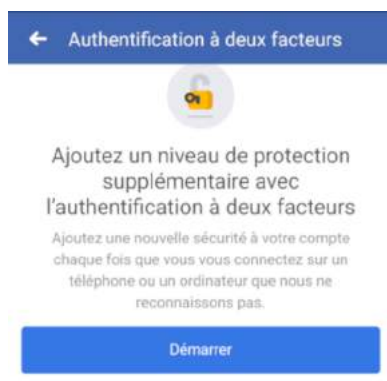
Modifiez votre mot de passe et prenez d'autres mesures pour renforcer la sécurité de votre compte.

Enfin, il faut appuyer sur l'onglet "**Sécurité et connexion**".



Comment éviter les connexions indésirables Facebook :

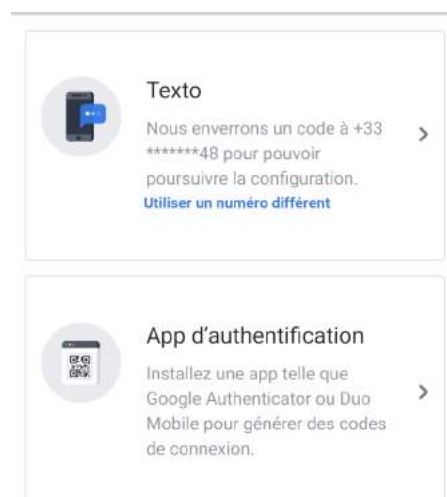
L'authentification à deux facteurs permet de rendre la connexion au compte plus sûre. Après avoir entré le mot de passe au moment de la connexion, il faut également fournir un **code** qui est communiqué par **SMS** ou par une application de générateur de codes.



-  Utiliser l'authentification à deux facteurs
- Utilisez votre téléphone comme moyen de sécurité supplémentaire afin d'empêcher d'autres personnes...
- Non

Pour activer l'authentification à deux facteurs, il faut se rendre dans la catégorie "**Renforcement de la sécurité**" et appuyer sur l'option concernée et ensuite démarrer la procédure.

Il faut ensuite choisir par quel biais obtenir le code. L'envoi d'un **SMS** est l'option la plus simple, car elle ne requiert pas d'installer une application.



Une fois cette option choisie, **un code va être envoyé par SMS** pour confirmer le bon fonctionnement de la procédure.



Saisir le code

Entrez le code à 6 chiffres que nous avons envoyé au +33 *****48 pour finaliser la configuration de l'authentification à deux facteurs.

Code de confirmation

Utilisez le code xxxxxx pour l'authentification à deux facteurs sur Facebook.

Dès que le code est reçu dans les SMS, il faut le rentrer dans la barre **"Code de confirmation"**.

Une fois le code entré, l'authentification à deux facteurs est activée. Si l'alerte de connexion est également activée sur le compte, il est également possible d'authentifier la connexion via **la notification**.



Authentification à deux facteurs activée

Nous vous demanderons dorénavant un code de connexion à chaque fois que vous vous connectez sur un téléphone ou un ordinateur que nous ne reconnaissons pas.

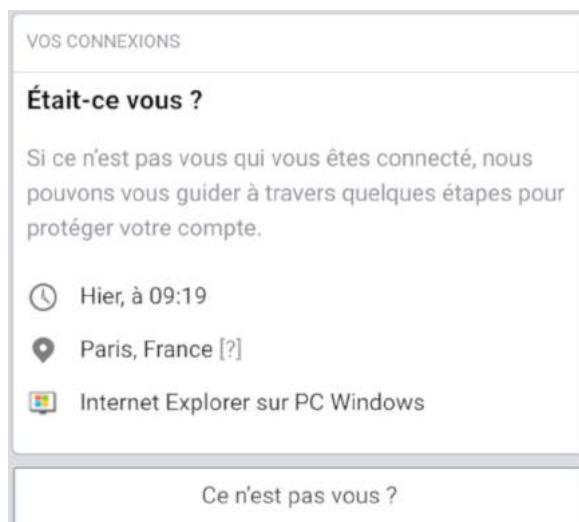
Comment repérer les connexions indésirables ?



La première catégorie permet d'identifier **quels appareils sont connectés sur la session**. Cette catégorie renseigne le type d'appareil connecté, la date, l'heure et une estimation du lieu.



Si la victime ne **reconnaît pas un appareil connecté**, il faut appuyer sur l'icône correspondant. Une fenêtre s'affiche par la suite et il faut cette fois appuyer sur **"Ce n'est pas vous ?"**.



Il faut ensuite appuyer sur "démarrer" pour accéder à un rapport des activités effectuées suite à la connexion de cet appareil.

Pour assurer la sécurité de votre compte, nous allons examiner vos dernières activités pour confirmer que vous êtes bien à l'origine de toutes les modifications.

Démarrer

The screenshot shows a mobile interface with a 'Activité' section. It includes a dropdown arrow, a 'Commentaires' item with 3 new comments, a 'Publications' item with no new posts, and 'Friends & Followers' with no new additions. Below this is a 'Connexions' section with a dropdown arrow, 'Vous êtes connectée sur' (4 new connections, 5 hours ago), and 'Connexions apps' (4 apps added, Oct 29).

Il est possible de savoir ce qui a été fait sur le compte pendant cette connexion.

En appuyant sur "vous êtes connectés sur", on peut sélectionner le ou les appareils non reconnus et les déconnecter. Il faudra également changer de mot de passe.

29 octobre



PC Windows

Internet Explorer · 09:19 AM le oct 29.



Se déconnecter

Comment être alerté des connexions indésirables ?



Les alertes de **connexion** sont des **notifications** que l'on reçoit sur son portable pour alerter d'une connexion sur le compte par un **appareil non reconnu**. Pour activer cette fonctionnalité, il suffit d'appuyer "Recevoir des alertes en cas de ..." dans la catégorie "Renforcement de la sécurité"


Renforcement de la sécurité

-  Recevoir des alertes en cas de connexions non reconnues Non
Nous vous avertirons si quelqu'un se connecte depuis un appareil ou un navigateur que vous n'avez pas l'ha...

Alertes de connexion

Si vous recevez une alerte provenant d'une source ou d'un navigateur inconnu, vous pourrez réinitialiser votre mot de passe et protéger votre compte

Ajouter une autre adresse e-mail ou un autre numéro de téléphone

 **Notifications** Oui >

 **Messenger** Oui >

 **E-mail** Oui >

Une fois sur les paramètres de notification, l'utilisateur décide par quel biais il souhaite être prévenu.

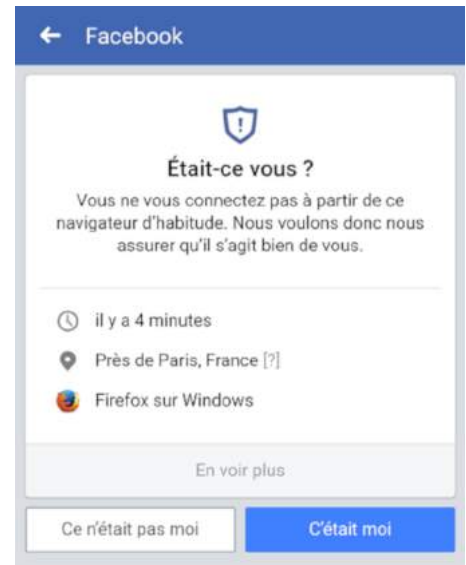
Il est possible d'être prévenu par une notification Facebook sur laquelle il faut appuyer pour **authentifier la connexion**.



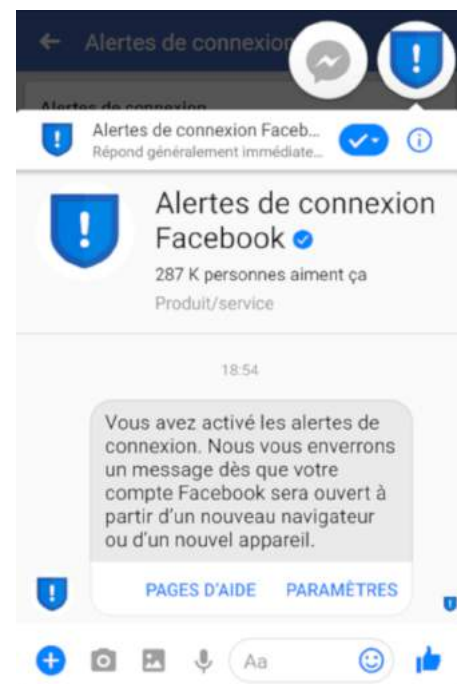
Nous avons détecté une connexion inhabituelle depuis un appareil ou un lieu non familier. Veuillez la vérifier.
il y a 8 minutes

Si la victime ne reconnaît pas l'appareil qui tente de se connecter, il faut appuyer sur **"Ce n'était pas moi"**. Ainsi, l'accès au compte sera interrompu.

Dans ce cas de figure, il faut impérativement changer le **mot de passe** du compte.



La notification peut également être envoyée via deux messages Messenger. Le premier message **alerte de connexion** et le deuxième apporte les **informations relatives à la connexion**, c'est-à-dire l'heure, la date, le lieu et le mode de connexion. Pour l'authentifier, il faut appuyer sur **"Afficher la connexion"**.



2. Sécuriser l'accès à Instagram :



Pour accéder aux options de sécurité, il faut ouvrir les **paramètres** de l'application. Pour cela, il faut d'abord se rendre sur son **profil** en appuyant sur l'icône du bonhomme dans le coin inférieur droit.



Une fois sur le profil, il faut appuyer sur les **trois barres** dans le coin supérieur droit pour dérouler le volet des options. Les paramètres se trouvent tout en bas du volet. En appuyant dessus, on peut accéder à la liste des paramètres.



Comment éviter les connexions indésirables sur Instagram:

L'authentification à deux facteurs permet de rendre la connexion au compte plus sûre. Après avoir entré le mot de passe au moment de la connexion, il faut également fournir un code qui est communiqué par SMS ou par une application de générateur de codes.

← Paramètres

Données du compte

Authentification à deux facteurs

Sous l'option "Données du compte", on trouve "Authentification à deux facteurs". La procédure se lance après avoir sélectionné cette option.

← Authentification à deux facteurs

Il faut ensuite appuyer sur "Démarrer" pour lancer la procédure. Il faut ensuite choisir si l'on souhaite recevoir le code par SMS ou une application de générateur de codes.

L'envoi d'un SMS est l'option la plus simple, car elle ne requiert pas d'installer une application.



Ajoutez encore un niveau de protection avec l'authentification à deux facteurs

Ajoutez un niveau de protection à votre compte pour toutes les fois où vous vous connectez sur un téléphone ou un ordinateur que nous ne reconnaissons pas.

Nous allons vous envoyer un texto avec un code de connexion. Vous pouvez également utiliser l'app de sécurité de votre choix comme Google Authenticator ou Duo Mobile.

[En savoir plus](#)

Démarrer

Une fois cette option choisie, un **code de sécurité** va être envoyé par **SMS** pour confirmer le bon fonctionnement de la procédure.

← Code de confirmation

Entrer le code

Entrez le code à 6 chiffres que nous avons envoyé à votre numéro se terminant par 2548 afin de finir la configuration de l'authentification à deux facteurs.

Suivant

Utilisez xxxxxx comme code de sécurité Instagram.

Dès que le code est reçu dans les SMS, il faut **le taper dans l'application**.

Une fois le code entré, l'authentification à deux facteurs est activée.



L'authentification à deux facteurs est activée

Nous vous demanderons dorénavant un code de connexion à chaque fois que vous vous connectez sur un téléphone ou un ordinateur que nous ne reconnaissons pas.

[En savoir plus](#)

Comment repérer les connexions indésirables ?



Cette fonction permet d'avoir la **liste des connexions au compte**. Pour y accéder, il faut se rendre dans la catégorie **"Données du compte"**.

← Paramètres

Données du compte

Authentification à deux facteurs

Activité

Connexions

[Voir tout](#)

Une fois entré dans la catégorie **"Données du compte"**, il faut appuyer sur **"Connexions"** dans la section **"Activité"**.

On accède donc à la liste des connexions au compte comprenant la date et l'heure de connexion.

Si l'utilisateur ne reconnaît pas une date de connexion, il faut impérativement **changer le mot de passe**.

← Données du compte

Connexions

8 novembre 2018 14:20
25 octobre 2018 10:38
31 juillet 2018 03:29
9 juillet 2018 12:24
11 mars 2018 15:00
18 février 2018 11:23
11 février 2018 15:48
1 novembre 2017 16:31
25 février 2017 00:50
16 janvier 2017 21:38

[Voir plus](#)

3. Sécuriser l'accès à Snapchat :



Comment éviter les connexions indésirables sur Snapchat :

L'authentification à deux facteurs, ici appelée "Authentification", permet de rendre la connexion au compte plus sûre.

Après avoir entré le mot de passe au moment de la connexion, il faut également fournir un code qui est communiqué par SMS ou par une application de générateur de codes.



Pour activer l'authentification, il faut se rendre dans **les réglages**. Pour cela, il faut appuyer sur son **avatar**, en haut à gauche.

Il faut ensuite appuyer sur la **molette** en haut à droite.



← Réglages

Authentification

Il faut alors sélectionner l'onglet "Authentification"

< Authentification

L'authentification permet de mieux sécuriser votre compte.

Lorsque que l'authentification est activée, vous aurez besoin d'un mot de passe et d'un code de vérification envoyé sur votre smartphone pour vous connecter sur un nouvel appareil.



CONTINUER

En appuyant sur "**Continuer**", on lance la procédure de notification.

Il faut ensuite choisir par quel biais obtenir le **code**. L'envoi d'un **SMS** est l'option la plus simple, car elle ne requiert pas d'installer une application.

< Authentification

Veillez choisir la façon dont vous souhaitez recevoir votre code de vérification.

SMS

Un code va être envoyé au +33XXXXXXXX

Application d'authentification

Générez un code sur votre appareil à l'aide d'une application comme Google Authenticator.

< Authentification

Nous avons envoyé un code au +33XXXXXXXX. Veuillez le saisir ci-dessous.

Ce n'est pas votre numéro ? [Modifiez-le](#).

Une fois cette option choisie, un **code de sécurité** va être envoyé par **SMS** pour confirmer le bon fonctionnement de la procédure.

Dès que le code est reçu dans les SMS, il faut le **taper dans l'application**, la procédure est alors finalisée.

Code Snapchat xxxxxx. Ne pas partager ou utiliser ailleurs!

4. Sécuriser l'accès à WhatsApp :



Comment éviter les connexions indésirables sur WhatsApp :



L'authentification à deux facteurs permet de rendre la connexion au compte plus sûre. En effet, après avoir reçu le SMS pour confirmer le numéro de téléphone, il faut également entrer un mot de passe sous forme de code.

Paramètres

Pour activer la vérification en deux étapes, il faut se rendre dans les paramètres.

Il faut ensuite sélectionner l'onglet "Compte".



Compte

Vérification en deux étapes

Puis choisir l'option "Vérification en deux étapes".

Il faut ensuite activer la procédure de vérification en deux étapes en appuyant sur "Activer" et ensuite décider d'un code PIN.



Pour plus de sécurité, activez la vérification en deux étapes. Cela nécessitera un PIN lorsque vous enregistrerez votre numéro de téléphone avec WhatsApp à nouveau.

ACTIVER

Entrez un code PIN à 6 chiffres. Ce code PIN vous sera demandé lorsque vous enregistrerez votre numéro de téléphone avec WhatsApp :

* * * * *



SUIVANT

Il faut ensuite une adresse e-mail pour finaliser l'activation.

Ajoutez une adresse e-mail à votre compte. Elle sera utilisée pour réinitialiser votre PIN si vous l'oubliez et protégera votre compte.

Passer

E-mail



La vérification en deux étapes est activée.



TERMINÉ

III. ME PROTÉGER



1. Conservation des preuves



Pour pouvoir entamer une **procédure judiciaire**, il est très important de pouvoir apporter des **preuves** d'une surveillance. Pour cela, il faut conserver les preuves d'une intrusion sur le téléphone. Dès qu'un signe suspect apparaît sur le téléphone, ou qu'une connexion suspecte a été effectuée sur un compte, qu'un appareil n'est pas connu de la victime, il est primordial de **faire une capture d'écran** avant d'effectuer la moindre modification.

Il est aussi plus sûr de ne pas stocker ces captures d'écrans seulement sur le portable, mais également sur un **ordinateur** ou une **clé USB**.

Il est crucial pour la bonne évolution de la plainte d'apporter un maximum de détails. Les captures d'écrans sont généralement acceptées par le juge si **d'autres éléments**, tel que des **témoignages** ou des **faits de violences**, prouvent leur **crédibilité**.

2. Procédure juridique :



Identifiants et mots de passe :

Il est important de rappeler que **forcer** son conjoint à communiquer ses identifiants et mots de passe pour pouvoir accéder à ses comptes peut être qualifié de **harcèlement moral**. Il faut pour cela que cette action s'inscrive dans un schéma de **comportements systématiques** dont la conséquence est la dégradation du niveau de vie du conjoint.

Le harcèlement moral (art. 222-33-2-1) est puni de 3 à 5 ans d'emprisonnement et 45 000 à 75 000 € d'amende.



L'application de contrôle :

L'application de contrôle est un moyen de **surveillance**. Ce genre d'application est le plus souvent utilisé par des parents pour surveiller les activités et déplacements de leurs enfants, mineurs, dans un souci de protection.

Cependant, si l'application a été installée à **des fins de surveillance** sur le téléphone de la victime sans qu'elle ne s'en aperçoive ou sans qu'elle ne puisse s'y opposer, cela relève d'une **infraction**.

Fouiller dans le téléphone de son conjoint afin d'y chercher des informations, dans ses mails ou dans ses messages, de manière déloyale ou frauduleuse, est une **atteinte à la vie privée et une violation du secret de correspondance**.

Le délit de violation du secret de correspondance (art. 226-15) est puni d'1 an de prison et 45 000 € d'amende.



Logiciel espion :

Contrairement à l'application de contrôle dont l'usage est détourné à des fins de surveillance, l'utilisation d'un logiciel espion est illégale.

Selon l'article 226-3 du Code pénal, la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques permettant la réalisation du délit d'atteinte à l'intimité est passible de 300 000 euros d'amende et de 5 ans d'emprisonnement.

En droit, les ordinateurs, les téléphones, les tablettes et les sites web sont considérés comme des systèmes de traitement automatisé des données et s'y introduire est un **délit**.

Selon l'article 323-1, le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

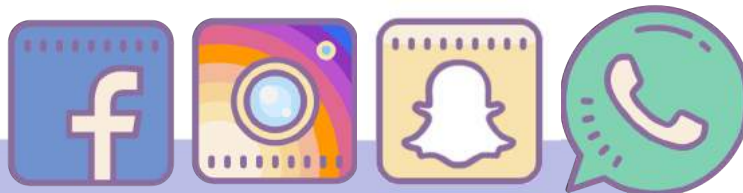
De plus l'utilisation d'un tel logiciel pour lire les e-mails ou messages de la victime est également considérée comme une **violation du secret de correspondance** (art. 226-15) puni d'1 an de prison et 45 000 € d'amende.



La synchronisation :

Le détournement de l'usage de la synchronisation dans le but d'espionner son conjoint peut aussi être considéré comme un **délit d'atteinte aux systèmes de traitement automatisé de données** (art. 323-1) puni de deux ans d'emprisonnement et de 60 000 € d'amende, ainsi qu'une **violation du secret de correspondance** (art. 226-15) puni d'1 an de prison et 45 000 € d'amende.

Cependant, il faut réussir à **prouver** que la victime n'était pas au courant de la synchronisation de ses comptes par son conjoint.



Les réseaux sociaux :

Les réseaux sociaux sont également considérés comme des systèmes de traitement automatisé des données. S'introduire de manière frauduleuse sur les réseaux sociaux de son conjoint est donc un délit d'atteinte aux systèmes de traitement automatisé de données (art. 323-1) puni de deux ans d'emprisonnement et de 60 000 € d'amende, ainsi qu'une violation du secret de correspondance (art. 226-15) puni d'1 an de prison et 45 000 € d'amende.

Si l'agresseur utilise également son accès aux comptes de sa victime pour envoyer des messages ou poster des publications, cela est aussi considéré comme un délit d'atteinte aux systèmes de traitement automatisé de données (art. 323-3) mais également comme un délit d'usurpation d'identité.

Selon l'article 323-1, le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Le délit d'usurpation d'identité (art. 226-4-1) est le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.



3. Contacts utiles en Seine-Saint-Denis

Ecoute, accompagnement social et psychologique des femmes victimes de violences

SOS FEMMES 93 01 48 48 62 27

- Accueil, écoute spécialisée, soutien psychologique, entretien conseil.
- Permanence téléphonique de 14h à 17h.
- Accueil collectif de 10h à 13h.
- Accueil individuel tous les jours sur rendez-vous.
- 3 allée du Moulin, Bondy

**Mouvement Français pour le
Planning Familial (MFPF93)**
01 55 84 04 04

- Information, entretien, consultation médicale : contraception, IVG, violences et agressions sexuelles.
- 3 rue Edourd Vaillant, Saint-Denis

39-19 Appel gratuit

- Lundi au vendredi:
9h-22h
- Les jours fériés :
10h-20h.

Maison des Femmes Thérèse Clerc
01 48 46 58 59

- Permanence tous les jeudis à 14h, sans rendez-vous.
- 24/28 rue de l'Eglise, Montreuil
- contact@maisondesfemmes.fr

**Maison des Femmes, Hopital
Delafontaine** 01 42 35 61 28

- Permanence d'accueil.
- 1 chemin du Moulin Basset, Saint-Denis

Information et accompagnement juridique des femmes victimes de violences

SOS VICTIMES 93

- Accueil, écoute, information sur les droits et les procédures, soutien psychologique.
- Sur rendez-vous de 9h à 12h et de 13h à 17h30, appeler au 01 41 60 19 60
- Sans rendez-vous de 13h à 17h30 au Tribunal de Grande Instance de Bobigny

Ordre des Avocats 01 41 60 80 80

- Permanence téléphonique vendredi de 10h à 18h pour les femmes victimes de violences, 01 48 96 20 95
- Maison de l'avocat et du Droit : 11-13 rue de l'indépendance, Bobigny
- 01 48 96 20 96, Palais de Justice

CENTRE D'INFORMATION SUR LES DROITS DES FEMMES ET DES FAMILLES (CIDFF) 01 48 36 99 02

- Accueil, écoute, information sur les droits, aide à l'insertion sociale et professionnelle, aide aux femmes victimes.
- Du lundi au vendredi sur rendez-vous
- 1 rue Pierre Curie, 93 120 La Courneuve.

Procureur de la République 01 48 95 13 93

- Tribunal de Grande Instance : 173 avenue Paul Vaillant Couturier, Bobigny

Commissariats de Police

Contactez le référent violences faites aux femmes du commissariat

Aubervilliers

16 Rue Léopold Rechossière
01 48 11 17 00

Aulnay-sous-Bois

26 Rue Louis Barrault
01 48 19 30 00

Bagnolet, Les Lilas, Pré-saint-Gervais et Romainville

55 Boulevard Eugene
Decros, Les Lilas
01 41 83 67 00

Blanc-Mesnil

Place Gabriel Péri
01 48 14 29 30

Bobigny

45 Rue de Carency
01 41 60 26 70

Bondy

26 Avenue Henri
Barbusse
01 48 50 30 00

Le Bourget et Drancy

6 rue de la République,
Drancy
01 41 60 81 40

Clichy-sous-Bois, Coubron et Montfermeil

1 Carrefour des Libertés,
Clichy-sous-Bois
01 82 46 60 00

La Courneuve

16 Place du pommier de
bois
01 43 11 77 30

Dugny, Pierrefitte-sur-Seine et Stains

47 avenue Marcel-Cachin,
Stains
01 49 71 33 50

Epinay-sur-Seine

40 Rue de Quetigny
01 49 40 17 00

Gagny

13 Rue Parmentier
01 43 01 33 50

Noisy-le-Grand et Gournay-sur-Marne

1 bis Rue Emile Cossonneau
01 55 85 80 00

Montreuil

18 Boulevard Paul Vaillant
Couturier
01 49 88 89 00

Pantin

14 Rue Eugène Marie
Louise Cornet
01 41 83 45 00

Saint-Denis et Villetaneuse

15 Rue Jean Mermoz, Saint-Denis
01 49 71 80 00

Villepinte et Tremblay-en-France

1 Rue Jean Fourgeaud,
Villepinte
01 49 63 46 10

Ile-Saint-Denis et La Plaine-Saint-Denis

39 Rue du Landy,
Saint-Denis
01 48 09 61 90

Neuilly-Plaisance et Neuilly-sur-Marne

34 boulevard du
Maréchal-Foch,
Neuilly-Plaisance
01 56 49 10 10

Pavillon-Sous-Bois, Le Raincy et Villemomble

9 boulevard de l'Ouest,
Le Raincy
01 43 01 35 00

Saint-Ouen

15 Rue Dieumegard
01 41 66 27 00

Noisy-le-Sec

2 Rue de Neuilly
01 48 10 12 50

Rosny-sous-Bois

20 Rue Lech Walesa
01 48 12 28 30

Sevran

Place Gaston-Bussière
01 41 52 16 40

Livry-Gargan et Vaujours

2 Avenue du Consul
Général Nording,
Livry-Gargan
01 41 70 18 30

RÉDACTION

Anne-Gabrielle Lavalette - Service civique auprès de la Délégation Départementale aux Droits des Femmes et à l'Egalité de Seine-Saint-Denis

Sous la direction de Claire Vercken - Déléguée Départementale aux Droits des Femmes et à l'Egalité de Seine-Saint-Denis

Contact : ddcs-ddfe@seine-saint-denis.gouv.fr

RETROUVEZ LE GUIDE EN VERSION NUMÉRIQUE SUR LE SITE DE LA DÉLÉGATION AUX DROITS DES FEMMES DE LA SEINE-SAINT-DENIS :

<https://dddfe93.wordpress.com/guide-protéger-sa-vie-privée-sur-son-mobile/>

