

SÉCURISER VOTRE PROFIL FACEBOOK EN 10 ÉTAPES

POUR DÉBUTANT ET
PROFESSIONNEL

AUTEUR DYPCKER

www.cyberdyp.com

SOMMAIRE

Introduction	04
ETAPE 1 – Avoir un bon mot de passe pour son compte	05
ETAPE 2 – Activer l’authentification à double facteur	06
ETAPE 3 – Activer les alertes de connexion	07
ETAPE 4 – Désactiver l’enregistrement de vos informations de connexion	08
ETAPE 5 – Déconnecter les appareils que l’on ne reconnaît pas	09
ETAPE 6 – Qui peut voir ce que vous partagez ?	09
ETAPE 7 – Comment partagez votre compte ?	10
ETAPE 8 – Comment est-il possible de vous trouver sur facebook ?	11
ETAPE 9 – Les parametre de vos données facebook	12
ETAPE 10 – Vos préférence de publicité facebook	13
	14
Conclusion	15

AUTEUR

Salut, je m'appelle Darile , un professionnelle du numérique avec plus de 4 ans d'expérience dans le secteur numérique. Je suis passionnée par l'idée de donner aux personnes non familiariser les moyens de prendre le contrôle de leurs propres connaissances numériques et d'atteindre leurs objectifs. Grâce à mon travail dans le domaine et d'éducateur, j'ai pu constater par moi-même le pouvoir et l'impact qu'elle peut avoir sur la vie des gens.

Je suis ravie de partager mes connaissances et mes idées dans cet ebook et d'aider les personnes à acquérir les compétences sur la sécurité des outils sociaux.

INTRODUCTION

Retrouvez les meilleurs trucs et conseils pour éviter que votre compte Facebook ne soit piraté. Nous vous partageons les meilleures précautions à prendre pour protéger votre compte, vos informations, vos amis et tout ce que vous avez publié sur le réseau social.

Facebook est une cible de prédilections pour les pirates informatiques. D'une part, le réseau regorge d'informations personnelles permettant d'effectuer des fraudes. Mais surtout, avec son important bassin d'utilisateurs, c'est un immense océan de proies potentielles.

Il suffit que notre compte soit piraté pour compromettre également ceux de nos amis, voir même notre entreprise si l'on a une page.

C'est pourquoi il est important de prendre toutes les précautions possibles pour sécuriser son compte Facebook, afin d'éviter que celui-ci ne tombe entre de mauvaises mains.

Nous vous partageons ici une liste des actions à envisager pour renforcer la sécurité de votre compte.

ETAPE I

AVOIR UN BON MOT DE PASSE POUR SON COMPTE

Le mot de passe de notre compte Facebook est évidemment la base de la base.
C'est la clé de la porte d'entrée vers notre compte.

Il faut donc s'assurer que notre clé est solide!

D'abord, il ne faut jamais utilisé le même mots de passe pour nos différents comptes

Si oui, c'est un simple jeu de dominos pour des pirates. Il suffit qu'un de nos comptes tombe entre de mauvaises mains et tous nos comptes avec le même mot de passe ont de graves chances d'être compromis aussi.

Ensuite, il faut choisir un mot de passe fort. Le plus long, le mieux s'est. Y ajouter des **majuscules, des chiffres, des caractères spéciaux**, bref le rendre le plus complexe possible.

Certes, j'en conviens, ce n'est pas évident de retenir un tel mot de passe. C'est pourquoi les gestionnaires de mots de passe ont été inventés!

Des solutions comme [Dashlane](#), [NordPass](#) et autres enregistrent et cryptent nos mots de passe. Nous n'avons donc pas à retenir tous les mots de passe complexes que l'on a pour chacun de nos comptes.

ETAPE 2

ACTIVER L'AUTHENTIFICATION À DOUBLE FACTEUR

Si le mot de passe est la clé principale pour notre compte Facebook, l'authentification à double facteur est le verrou en acier que l'on ajoute à notre porte.

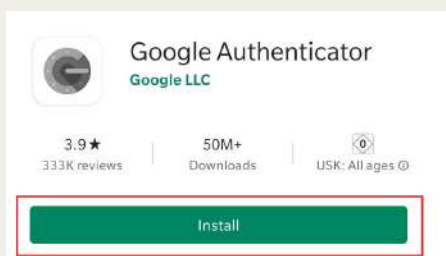
En plus d'entrer notre mot de passe pour se connecter à notre compte, Facebook va chercher à obtenir une deuxième validation. C'est l'authentification à double facteur!

On reçoit, par texto SMS ou bien via une application de 2FA, un code de 6 chiffres que l'on va devoir inscrire pour se connecter.

Je le concède, c'est un peu plus fatigant pour se connecter chaque fois, mais ça ajoute tellement une grosse couche de sécurité.

Les chances ne sont pas nulles à 100% que notre code ne sera pas intercepté via SMS. Si notre carte SIM ou notre téléphone est compromis par exemple, il se peut que notre code soit intercepté.

Mais une application de 2FA quant à elle génère des codes toutes les 30 secondes! C'est pas mal plus difficile à craquer.



ETAPE 3

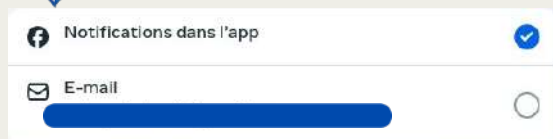
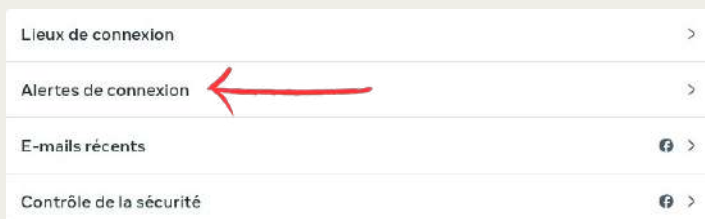
ACTIVER LES ALERTES DE CONNEXION

Si l'idée de la double authentification vous semble laborieux ou que vous voulez quand même vous ajouter une précaution supplémentaire, il est possible d'activer les alertes de connexion sur son compte Facebook.

Moindrement qu'une connexion est faite sur notre compte, Facebook va nous avertir. On peut déterminer si l'on veut être averti via une notification Facebook, Messenger ou bien par courriel.

CHEMIN D'ACCÈS:

Parametre  Mots de passe et Sécurité



ETAPE 4

DÉSACTIVER L'ENREGISTREMENT DE VOS INFORMATIONS DE CONNEXION

Avoir un bon mot de passe pour son compte Facebook et avoir activé la double authentification c'est bien beau, mais tout ceci ne vaut plus rien si l'on a activé l'enregistrement de nos informations de connexion.

De quoi je parle?

Je parle de la proposition que Facebook nous fait lorsqu'on se connecte et qu'il nous demande si l'on veut enregistrer nos informations pour le navigateur ou appareil que l'on utilise.

Ceci fait donc en sorte qu'on appuie sur sa photo de profil, sur la page de connexion, et hop on est connecté!

C'est super pratique si l'on veut se connecter le plus rapidement possible, mais très dangereux si notre appareil tombe entre de mauvaises mains!



ETAPE 5

DÉCONNECTER LES APPAREILS QUE L'ON NE RECONNAIT PAS

Dans la même veine, il est judicieux d'aller faire un tour dans les appareils qui ont accès à notre compte Facebook. Il y en a peut-être là-dedans qu'on n'utilise plus ou qui ne sont carrément pas à nous!

En effet, il n'est pas impossible que l'on se soit connecté via l'appareil d'un ami, à la bibliothèque ou à notre hôtel en voyage.

À l'inverse, un intrus est peut-être parvenu à se connecter à notre compte!

CHEMIN D'ACCÈS:

Paramètre

Informations & autorisations

Informations personnelles



Accéder à vos informations

- Informations consignées**
Les informations que Facebook conserve sur votre activité, notamment l'historique de votre localisation et de vos recherches.
- Informations de connexion et de sécurité**
Informations techniques et activité consignées liées à votre compte.
- Applications et sites web en dehors de Facebook**
Les applications que vous possédez et l'activité que nous recevons des applications et sites web en dehors de Facebook.
- Préférences**
Actions prises pour personnaliser votre expérience sur Facebook.
- Informations sur les publicités**
Vos interactions avec les publicités et les annonces de Facebook.

ETAPE 6

QUI PEUT VOIR CE QUE VOUS PARTAGEZ ?

C'est quelque chose que bien des gens ne font pas encore, limiter l'audience de leurs publications.

Par défaut, Facebook veut que l'on fasse découvrir notre chien, nos vacances, nos états d'esprit et toutes nos publications à la terre entière en les rendant publiques.

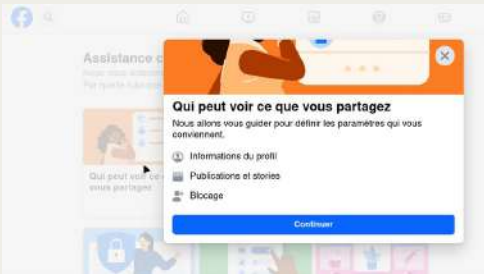
Seulement, est-ce vraiment nécessaire? Le moins d'information que l'on partage sur les réseaux sociaux, le mieux s'est. Mais c'est encore mieux si on limite le nombre de personnes qui ont accès à nos publications.

Comment faire pour que personne ne voit mes photos sur Facebook?

Prenons un exemple de base, mais si l'on publie des photos de nous sur Facebook et que celles-ci sont paramétrées pour être visibles au grand public, qu'est-ce qui empêche un pirate d'aller les enregistrer et tenter de faire un vol d'identité?

Même chose pour toutes les informations que l'on partage! Celles-ci pourraient se retourner contre nous, notamment dans des cas d'hameçonnage.

Bref, il est toujours mieux limité nos publications à nos amis. Dans la chronique ci-bas, j'expliquais où aller pour modifier la confidentialité de nos publications passées. Pour celles futures, l'option est au même endroit.



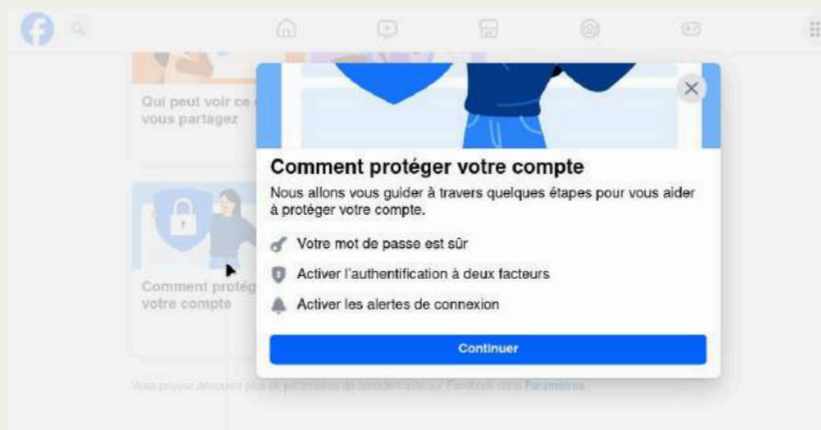
ETAPE 7

COMMENT PROTÉGER VOTRE COMPTE

Toujours dans l'assistance confidentialité, cliquez cette fois-ci dans la rubrique « Comment protéger votre compte ». Cet espace va tout d'abord vous permettre de changer votre mot de passe. Modifier votre mot de passe est la première chose à faire si vous votre profil Facebook a été piraté.

Vous pourrez également activer l'authentification en deux facteurs. C'est une option de sécurité très importante visant à vous envoyer un SMS ou une notification sur votre mobile dans le cas où quelqu'un se connecte à votre compte depuis un endroit inhabituel. Grâce à cela, si vous ne validez pas la connexion, l'utilisateur sera bloqué et vous pourrez ainsi aller changer votre mot de passe en toute sécurité.

Enfin, vous pourrez choisir à partir de quels endroits vous souhaitez être notifié si une connexion n'est pas reconnue à savoir, sur votre application Facebook, sur Messenger et enfin sur votre boîte mail.



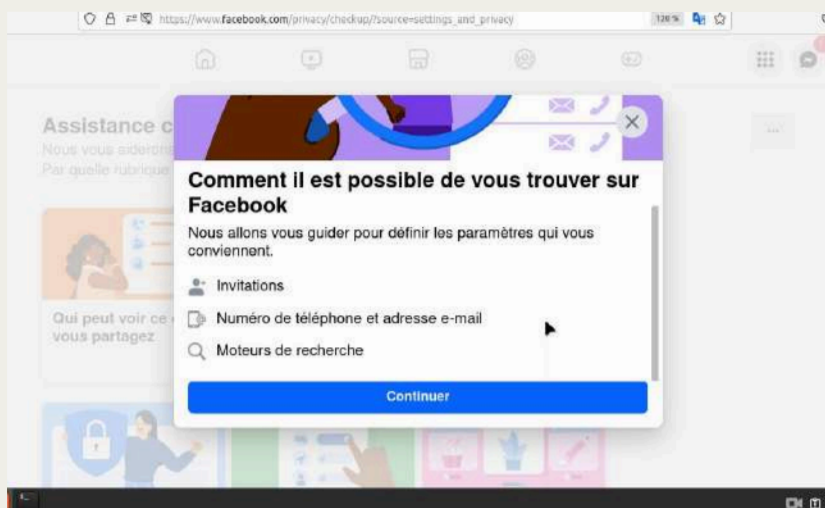
ETAPE 8

COMMENT IL EST POSSIBLE DE VOUS TROUVER SUR FACEBOOK ?

Cette troisième série de réglages va vous permettre de définir qui peut vous inviter en tant qu'ami, de déterminer qui peut voir votre numéro de téléphone et votre boîte mail et, paramètre très très important, de définir si Facebook doit permettre ou non aux moteurs de recherches (Google) d'indexer votre profil.

Ce dernier réglage n'est pas à négliger et d'après moi, cette case doit être décochée pour la majorité d'entre vous (exception pour les personnes maîtrisant de manière certaine les paramètres de Facebook et ayant conscience de ce qu'elles publient dessus et à qui...).

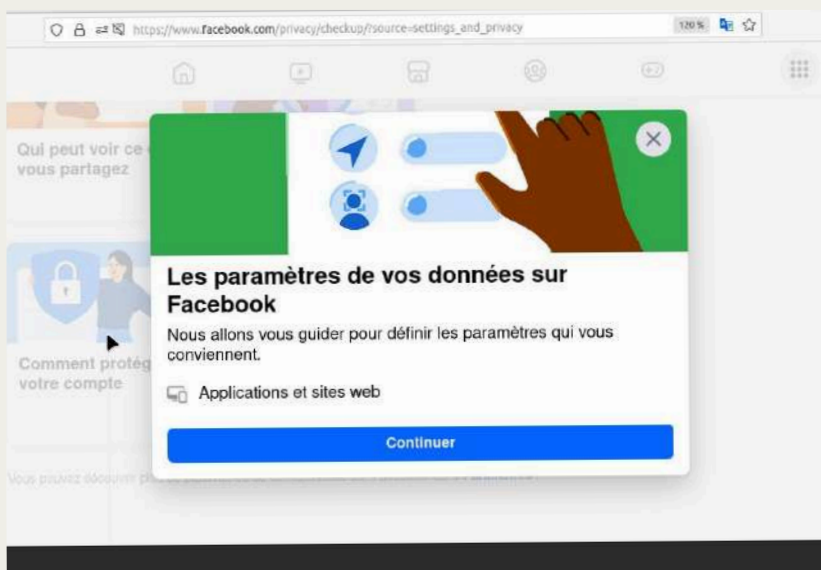
C'est typiquement à cause de ce réglage que certaines photos compromettantes se retrouvent sur la rubrique Google Images. Je vous invite donc vivement à désactiver ce paramètre pour ne pas prendre de risque.



ETAPE 9

LES PARAMETRES DE VOS DONNEES FACEBOOK

Cette rubrique vous permettra de gérer les applications et site internet liés à votre profil Facebook en les supprimant par exemple si vous ne souhaitez plus que ces outils ne puissent plus accéder à vos données.



ETAPE 10

VOS PREFERENCES PUBLICITAIRES SUR FACEBOOK

Cette rubrique est très importante puisqu'elle vous permettra de définir ce que vous souhaitez que Facebook puisse utiliser dans vos informations de profil pour vous diffuser de la publicité payante. Par exemple, si vous avez communiqué votre situation amoureuse sachez que Facebook peut vous afficher une publicité car vous êtes dans une situation amoureuse qui correspond à la publicité affichée. Pour aller plus loin, si par exemple vous venez de mettre votre situation amoureuse à célibataire parce que vous venez de vous séparer (je ne vous le souhaite pas 😊) il y a de fortes chances pour que des pubs de sites de rencontres apparaissent sur votre profil.

En gérant ces paramètres vous ne pourrez plus être ciblé par ce type d'affichage puisque Facebook n'aura plus le droit de communiquer ces données à une entreprise.

