Sécurité numérique et gestion des risques

Séance n° 2 : Il faut prendre soin des communications

2025

Funded by the European Union

Sécurité numérique ? Je n'y connais rien !

Réfléchissons à la manière de nous protéger dans les médias numériques

Sécurité numérique et analyse des risques

Introduction à la sécurité numérique pour les organisations non gouvernementales (ONG) et les défenseurs des droits humains (DDH)

Comprendre l'environnement numérique, les acteurs présents et les menaces auxquelles nous sommes confrontés.

1

2

Il faut prendre soin des communications

Décider des outils à utiliser et comment les configurer pour améliorer la sécurité et la confidentialité.

3

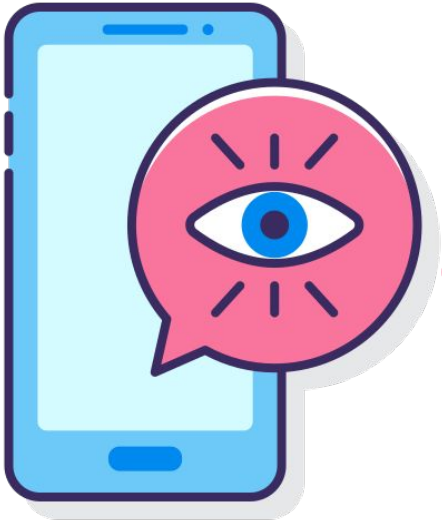
Meilleures pratiques numériques

Élaborer un plan d'amélioration incluant les meilleures pratiques et les engagements d'utilisation.

Séance n° 2 : Il faut faire attention aux communications

Objectifs

- Trouver le juste équilibre entre le besoin de communiquer et la sécurité de votre ONG.
- Nous allons analyser les outils afin de déterminer la meilleure option pour nos communications internes et externes.
- Configurer les paramètres de confidentialité et de sécurité des outils que nous utilisons.



Les téléphones portables et Internet ont rendu la communication plus facile que jamais, mais ils facilitent également la surveillance.

1. Le cycle de vie de l'information

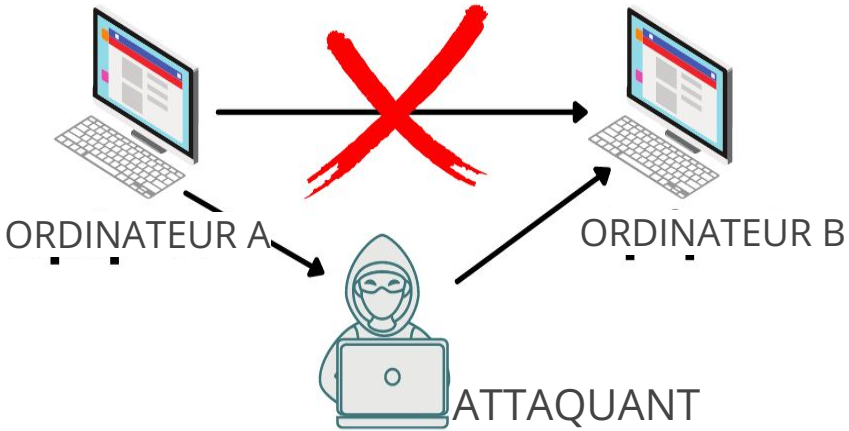
Le cycle de vie des informations

Les messages numériques sont créés, transmis, stockés et supprimés.

Pour protéger la communication, il faut la protéger tout au long de son cycle de vie.

- Lorsqu'elles sont **créées**, il faut **protéger** les appareils et les applications avec lesquels nous générons les messages.
- Lorsqu'elles sont **transmises**, il faut **protéger** les informations pendant leur transfert entre les appareils, entre l'expéditeur et le destinataire.
- Lorsqu'elles sont **stockées**, il faut **protéger** les informations dans les endroits où elles sont enregistrées, dans nos appareils, mais aussi sur les serveurs des fournisseurs qui nous offrent le service que nous utilisons pour communiquer.
- Enfin, nous devons également nous assurer que si nous **supprimons** un message, celui-ci ne puisse pas être **récupéré**.

“Attaque de la personne du milieu”



Chaque appel, SMS, e-mail, chat textuel, audio ou vidéo et message sur les réseaux sociaux peut être vulnérable à une attaque si un pirate parvient à intercepter la communication.

Si la communication est compromise, il est possible **de lire, bloquer**, **supprimer** ou **modifier** les messages. Il est également possible **d'usurper** l'identité de la personne qui envoie ou qui reçoit le message.

Activité 1

Quelques cas de surveillance des ONG

Que s'est-il passé dans cette actualité ?

Escudodigital

CIBERSEGURIDAD

L'auteur des attaques du jumeau maléfique utilisant le Wi-Fi de plusieurs aéroports a été arrêté

Vous vous connectez au Wi-Fi de l'aéroport ? Vous pourriez être victime d'une arnaque.

por **Luis Miranda**
1 de julio de 2024

Activité 1

Quelques cas de surveillance des ONG

Quel type d'attaque reconnaissons-nous ?

RAPPEL

Attaques fréquentes

Comment agissent nos adversaires

- Hameçonnage
- Exploitation des vulnérabilités
- Doxxing
- Logiciels espions
- Chantage
- Harcèlement en ligne
- Menaces en ligne
- Violence sexiste facilitée par la technologie

Activité 1

Quelques cas de surveillance des ONG

Reconnaissons-nous une vulnérabilité qui a favorisé cette attaque ?

RAPPEL

Vulnérabilités

Quelques éléments qui nous exposent à des risques

- ➔ Utilisation de mots de passe faibles
- ➔ Ne pas verrouiller les équipements
- ➔ Ne pas utiliser la 2FA
- ➔ Ouvrir des pièces jointes inconnues
- ➔ Ne pas avoir de copie de sauvegarde
- ➔ Ne pas mettre à jour les programmes
- ➔ Utiliser des réseaux publics
- ➔ Utilisation d'applications de communication non sécurisées

Activité 1

Quelques cas de surveillance des ONG

Pouvez-vous penser à une bonne pratique qui aurait pu atténuer l'attaque ?

RAPPEL

Bonnes pratiques

Éléments qui font pencher la balance

- Utiliser des mots de passe uniques et forts
- Protéger les appareils avec des mots de passe de démarrage
- Utiliser l'authentification à deux facteurs (2FA) sur tous les comptes
- Se méfier des pièces jointes inconnues
- Effectuer des sauvegardes régulières
- Configurer votre confidentialité
- Maintenir les mises à jour à jour
- Crypter tout ce que vous pouvez crypter
- N'utilisez que des réseaux fiables
- Utilisez des applications de communication sécurisées

2. Protéger les communications

Protéger les communications

Chiffrement, chiffrement, CHIFFREMENT !!!!

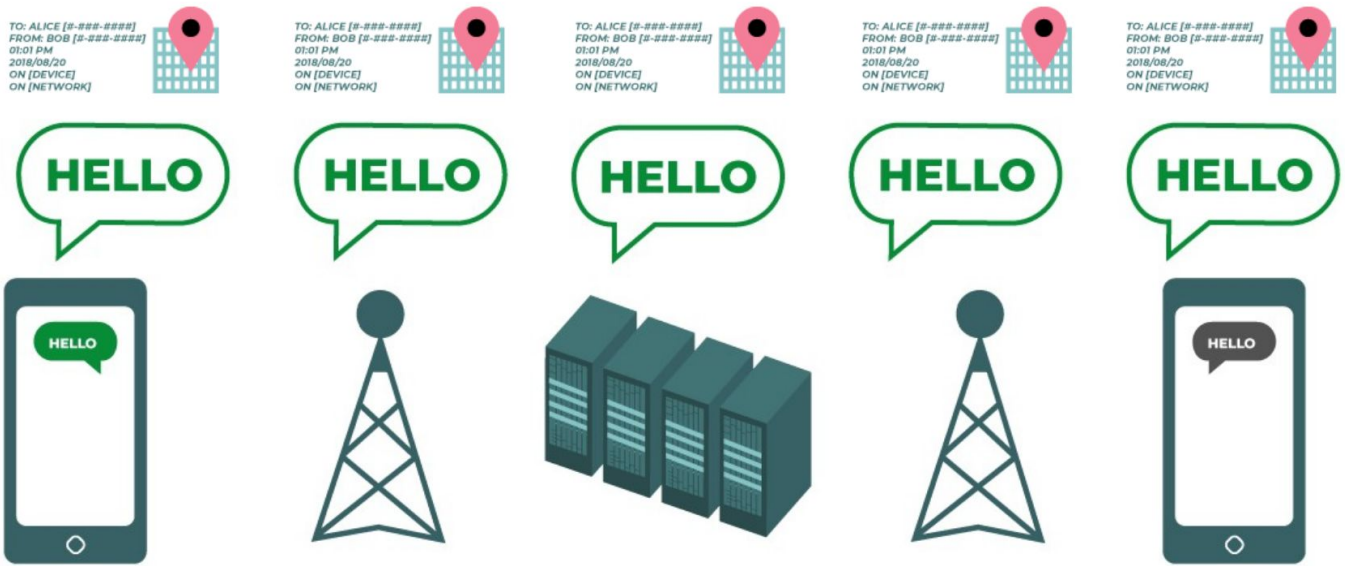
Le meilleur moyen dont nous disposons pour protéger les informations lorsqu'elles sont en transit ou stockées sur un appareil quelconque est le chiffrement.

Le chiffrement est un processus qui rend les informations **illisibles**, sauf pour la personne qui sait comment inverser le processus. En technologie numérique, il implique une **méthode** (qui définit le processus spécifique à suivre) et une **clé** ou un **secret** (connu de la personne qui envoie ou reçoit la communication, ou qui la stocke) qui permet de la **chiffrer**.

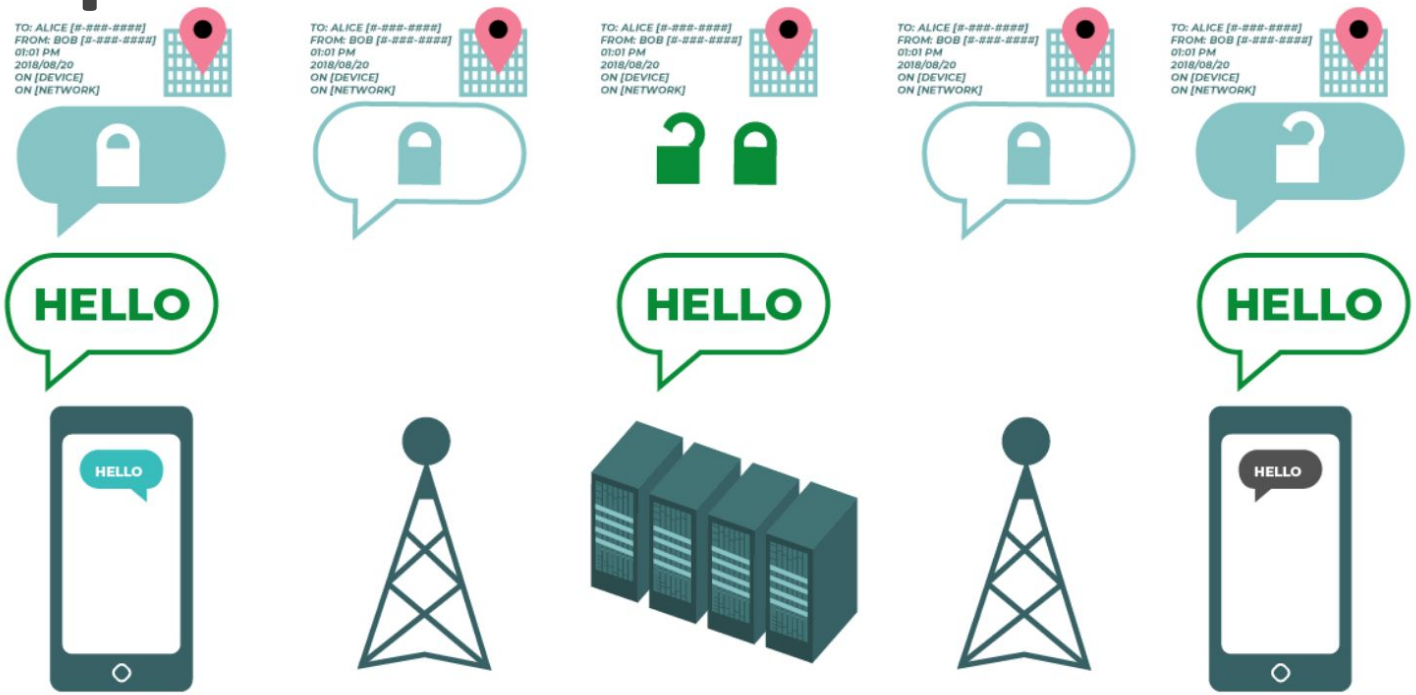
Pour communiquer en toute sécurité, nous devons choisir des applications qui intègrent un **chiffrement** de bout en bout.

Pour protéger les informations que nous allons stocker, nous devons utiliser des appareils **chiffrés** ou **chiffrer** les informations.

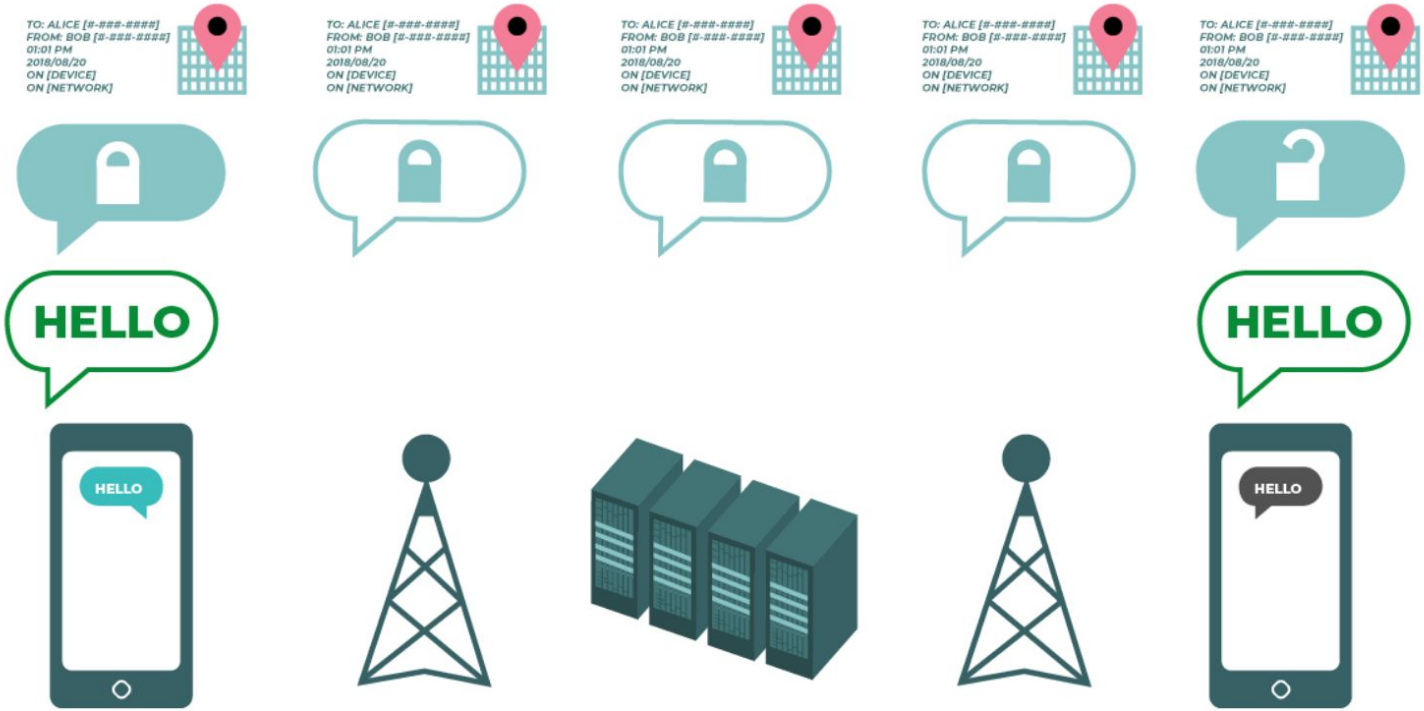
Sans chiffrement



Chiffrement au niveau de la couche transport



Chiffrement de bout en bout



Activité 2

Identifiez les types de communication

Sans chiffrement

Couche transport

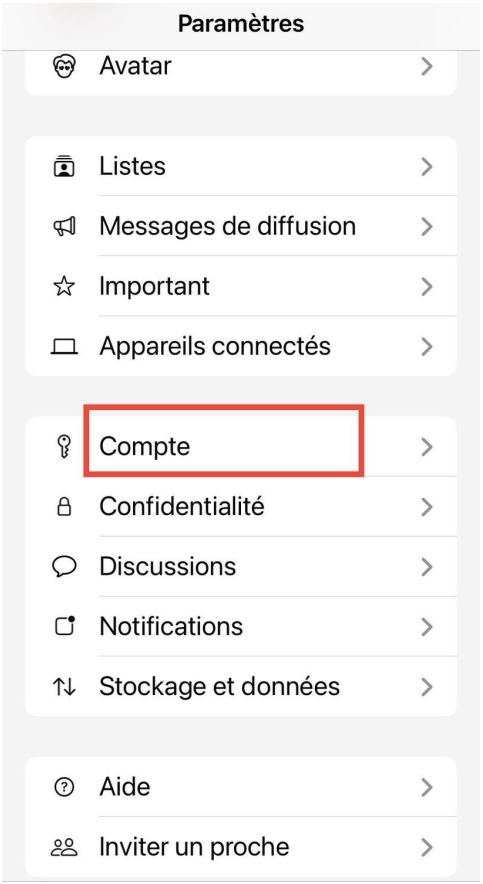
De bout en bout

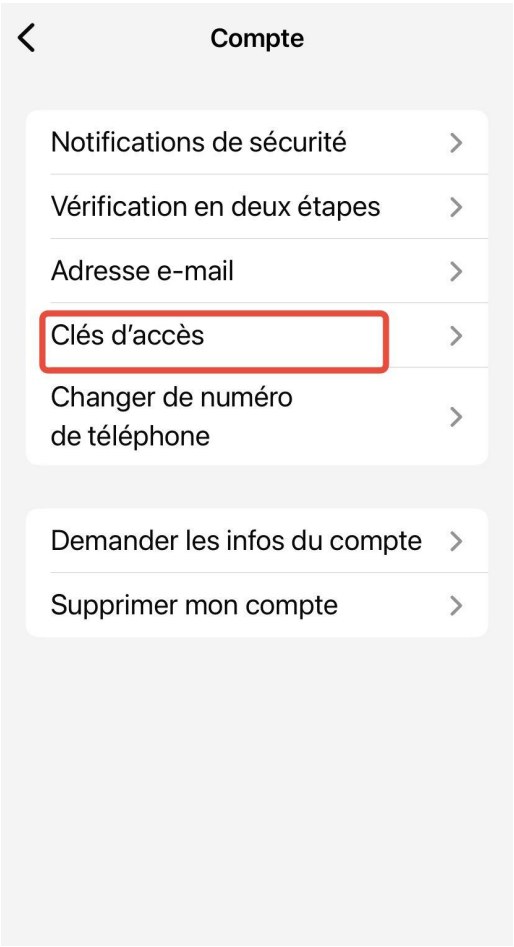
3. Améliorer nos communications

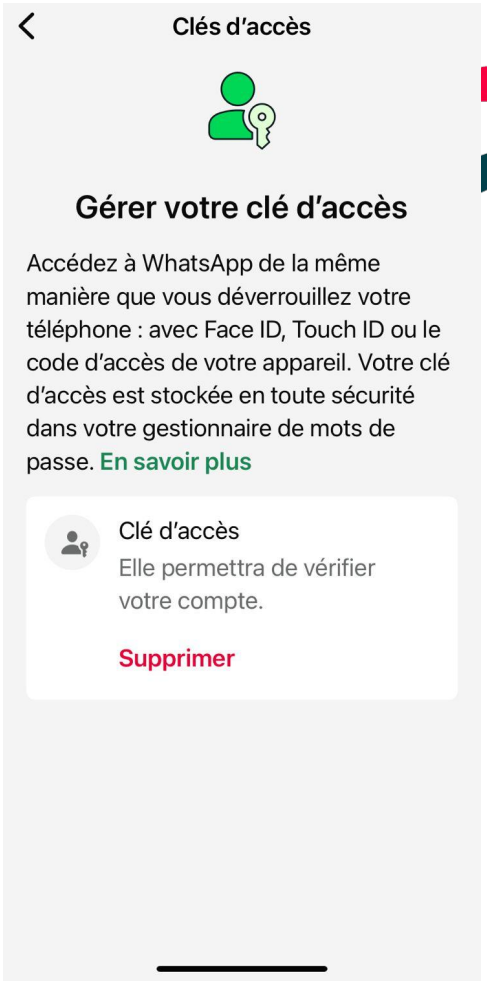
La clé réside dans la configuration

WhatsApp

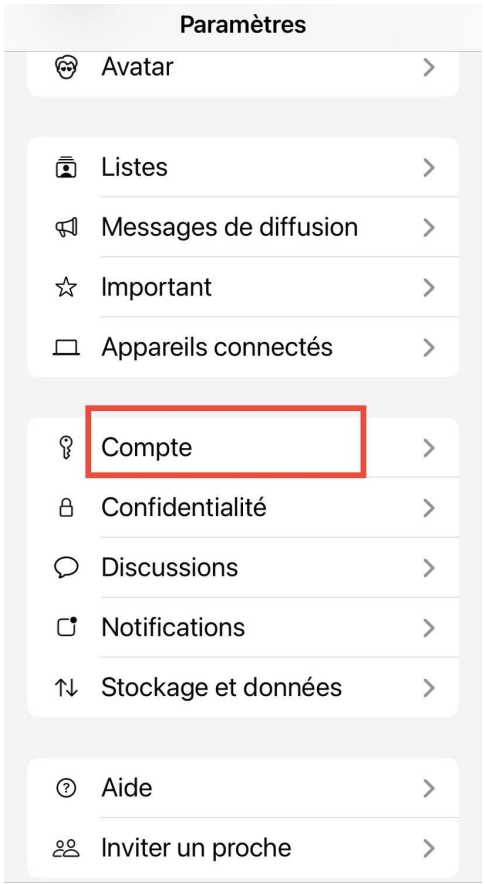
- Compte
  - Mots de passe
  - Adresse e-mail
  - Vérification en deux étapes
  - Ajouter un compte
- Confidentialité
  - Groupes
  - Blocage d'application
  - Avancé
- Chats
  - Sauvegarde
  - Historique des chats

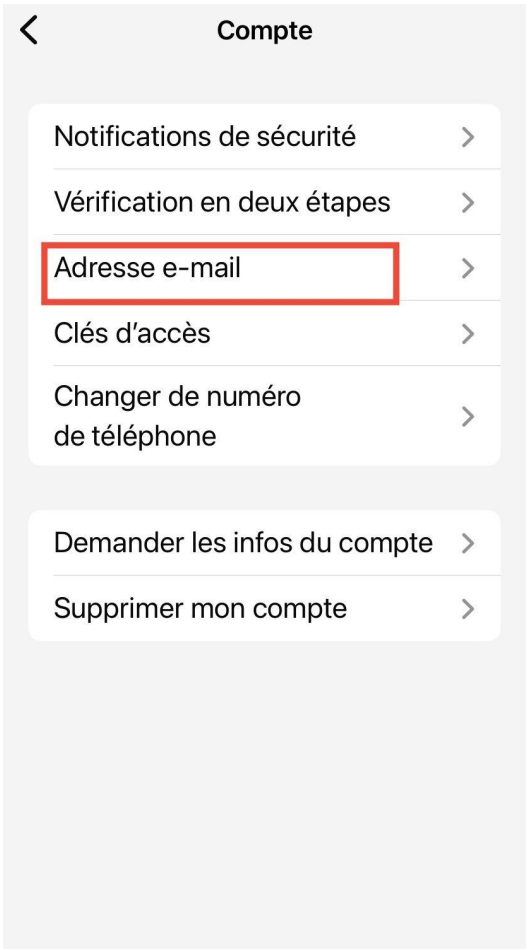

Paramètres
Avatar
Listes
Messages de diffusion
Important
Appareils connectés
Compte
Confidentialité
Discussions
Notifications
Stockage et données
Aide
Inviter un proche


Compte
Notifications de sécurité
Vérification en deux étapes
Adresse e-mail
Clés d'accès
Changer de numéro de téléphone
Demander les infos du compte
Supprimer mon compte

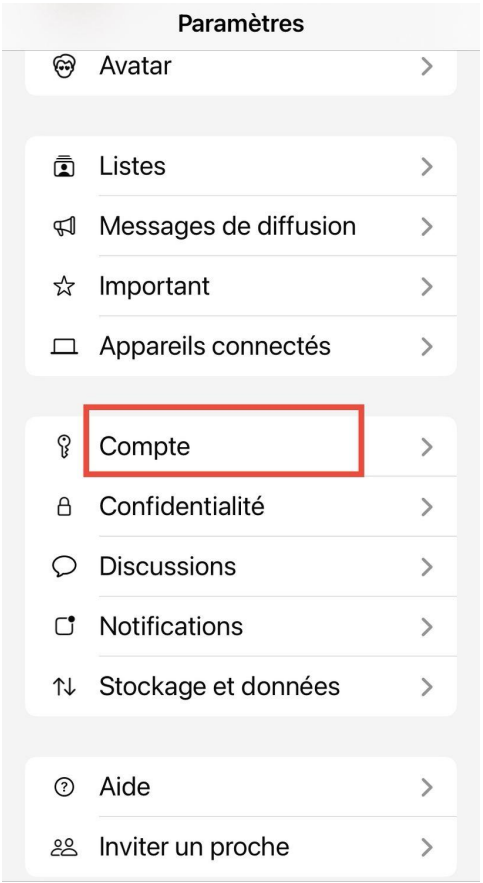

Clés d'accès
Gérer votre clé d'accès
Accédez à WhatsApp de la même manière que vous déverrouillez votre téléphone : avec Face ID, Touch ID ou le code d'accès de votre appareil. Votre clé d'accès est stockée en toute sécurité dans votre gestionnaire de mots de passe. En savoir plus
Clé d'accès
Elle permettra de vérifier votre compte.
Supprimer

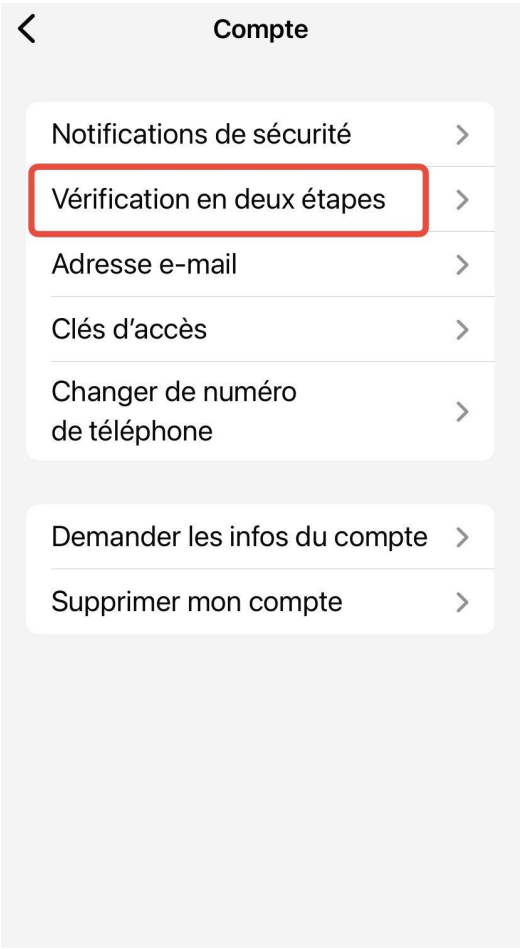
Clés d'accès

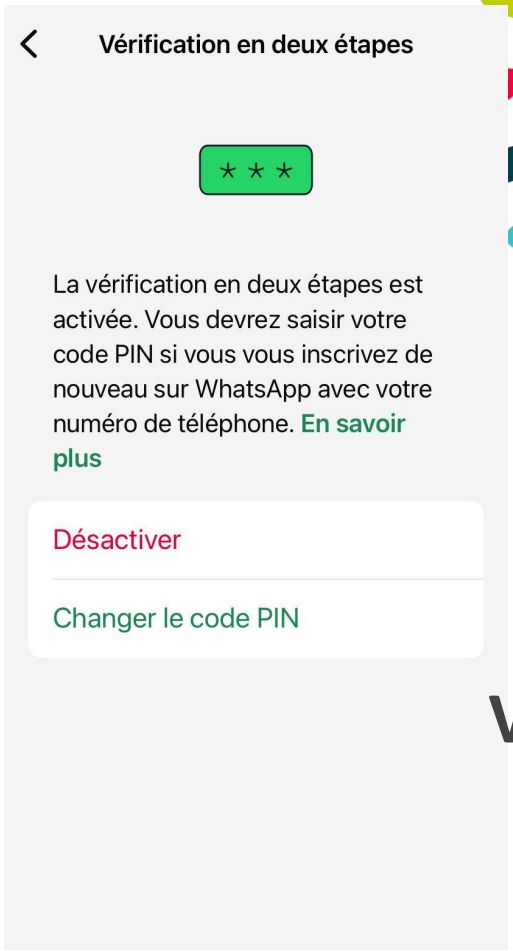




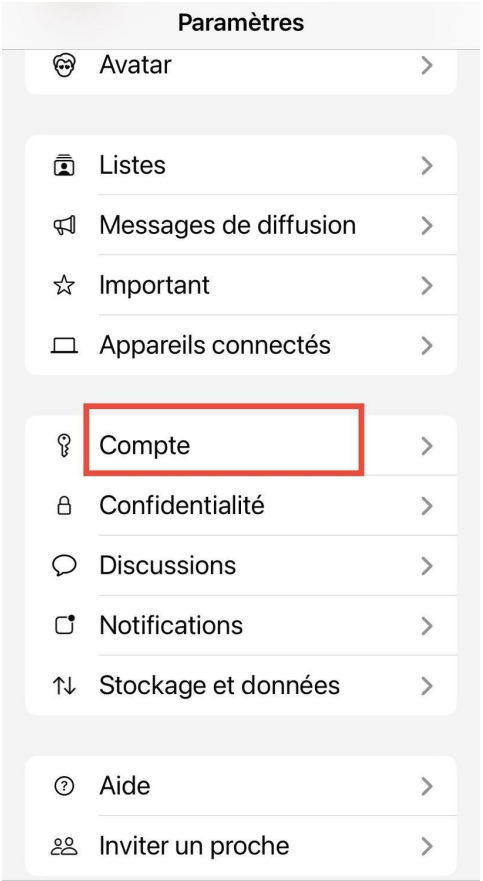
Adresse e-mail

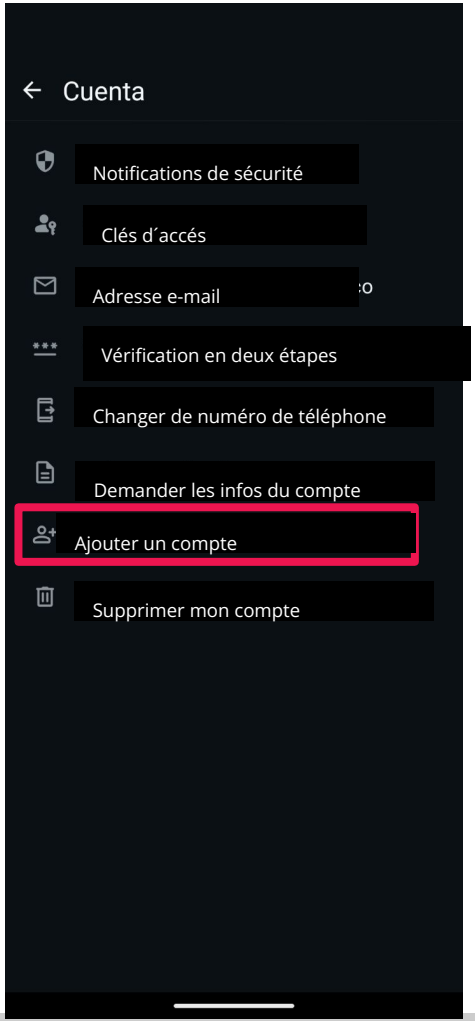






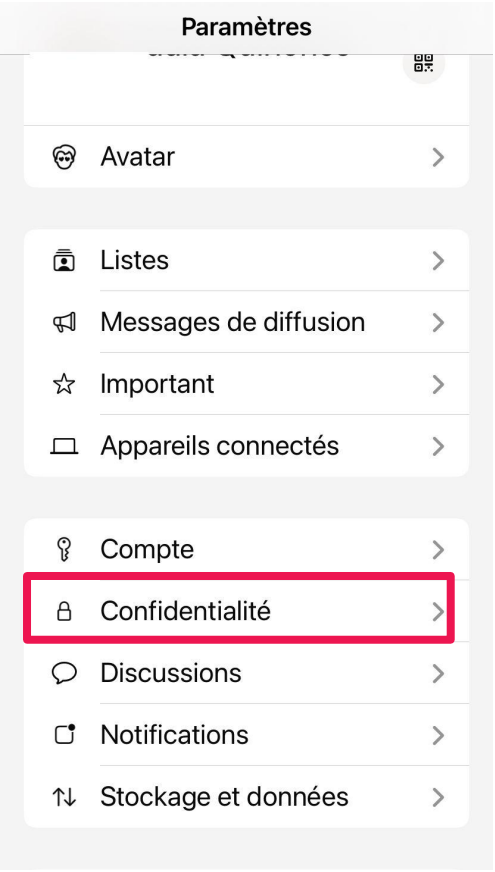
Vérification en deux étapes

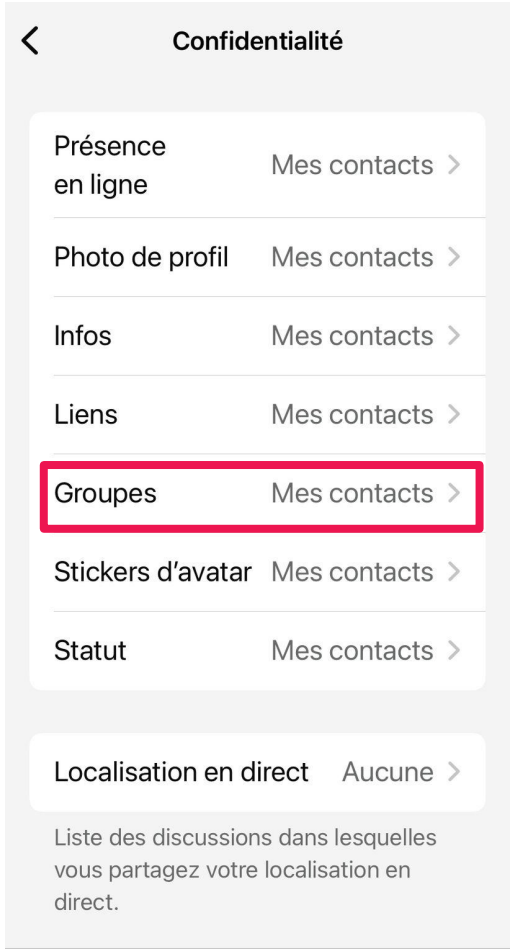


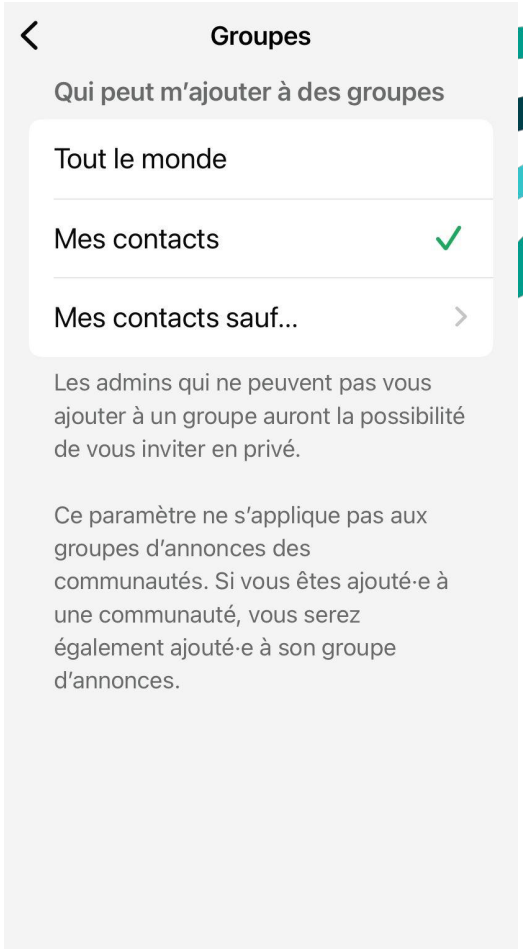


Ajouter un compte

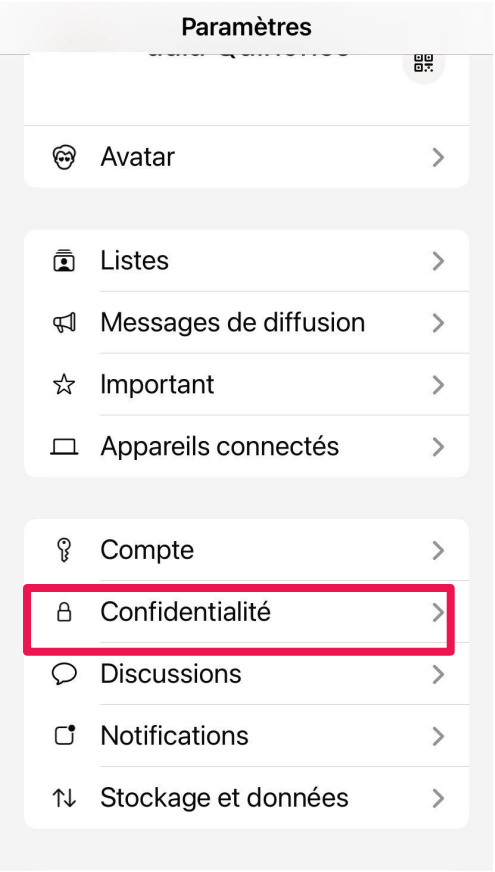
*seulement android

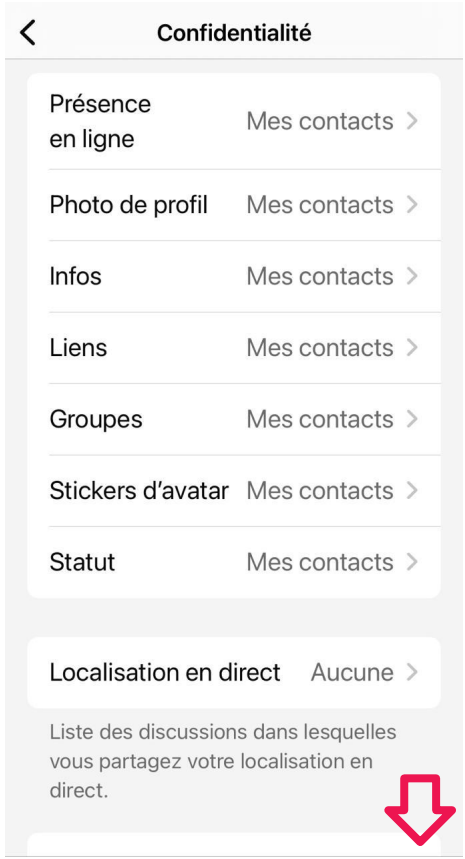

Paramètres
Avatar
Listes
Messages de diffusion
Important
Appareils connectés
Compte
Confidentialité
Discussions
Notifications
Stockage et données

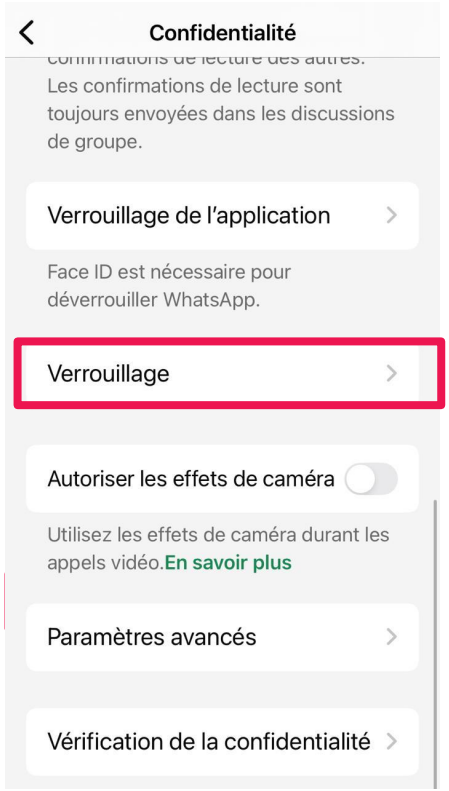

Confidentialité
Présence en ligne
Mes contacts
Photo de profil
Mes contacts
Infos
Mes contacts
Liens
Mes contacts
Groupes
Mes contacts
Stickers d'avatar
Mes contacts
Statut
Mes contacts
Localisation en direct
Aucune
Liste des discussions dans lesquelles vous partagez votre localisation en direct.

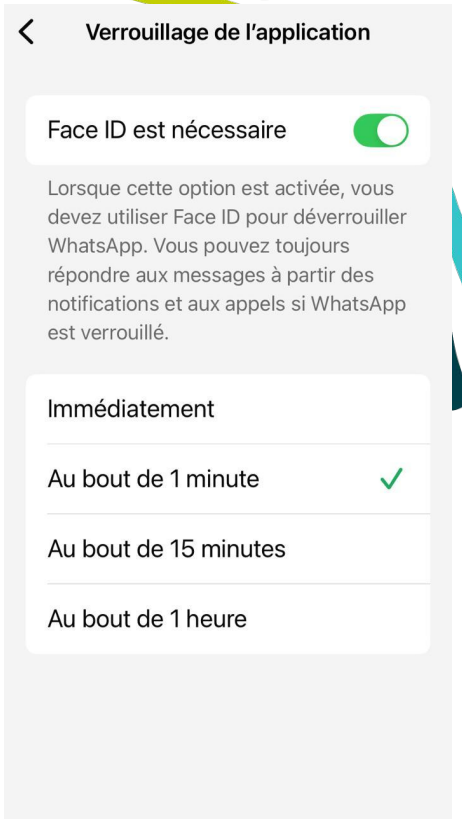

Groupes
Qui peut m'ajouter à des groupes
Tout le monde
Mes contacts
Mes contacts sauf...
Les admins qui ne peuvent pas vous ajouter à un groupe auront la possibilité de vous inviter en privé.
Ce paramètre ne s'applique pas aux groupes d'annonces des communautés. Si vous êtes ajouté·e à une communauté, vous serez également ajouté·e à son groupe d'annonces.

Groupes

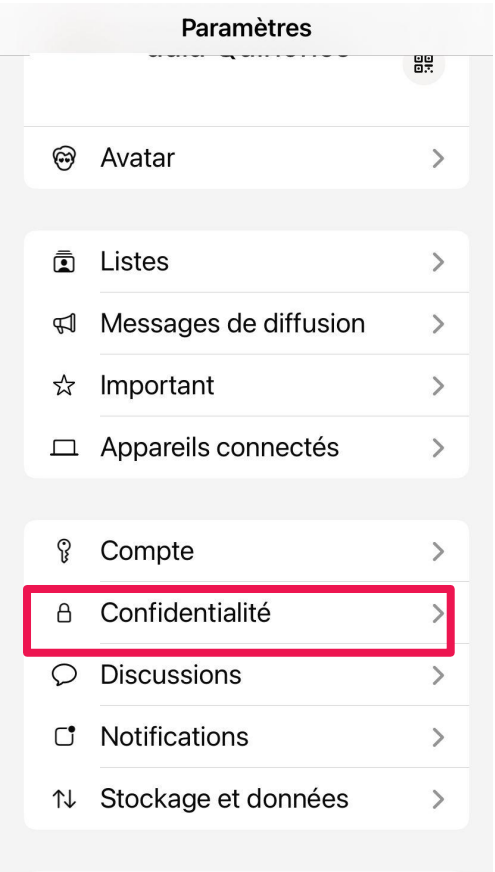


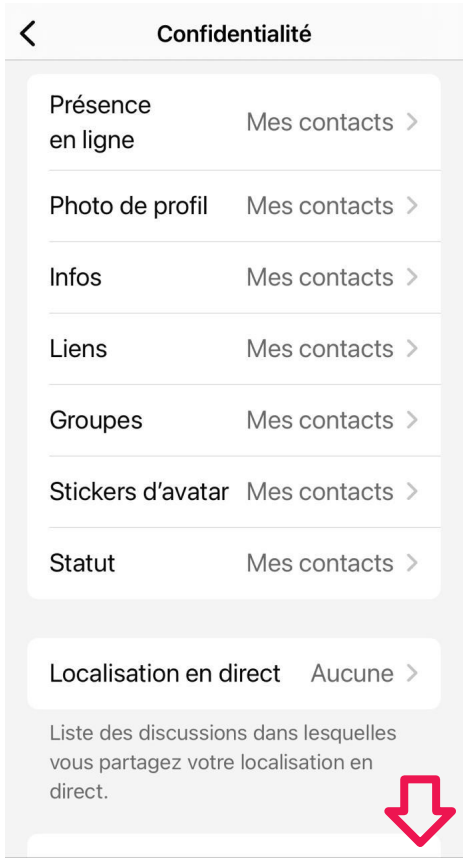


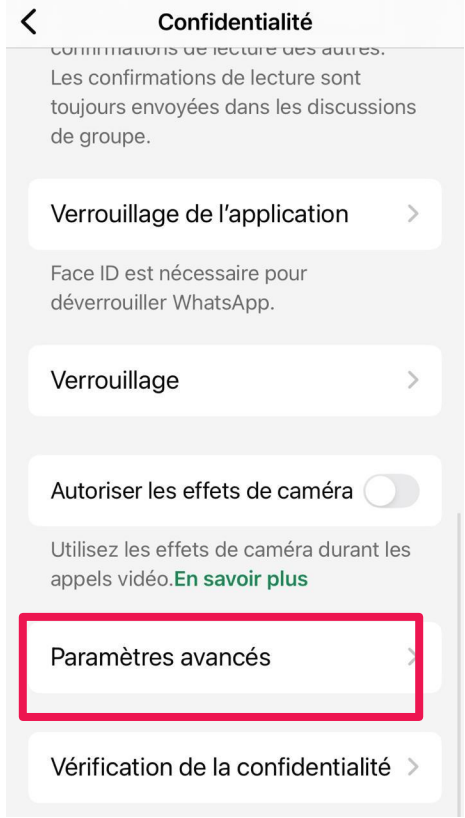


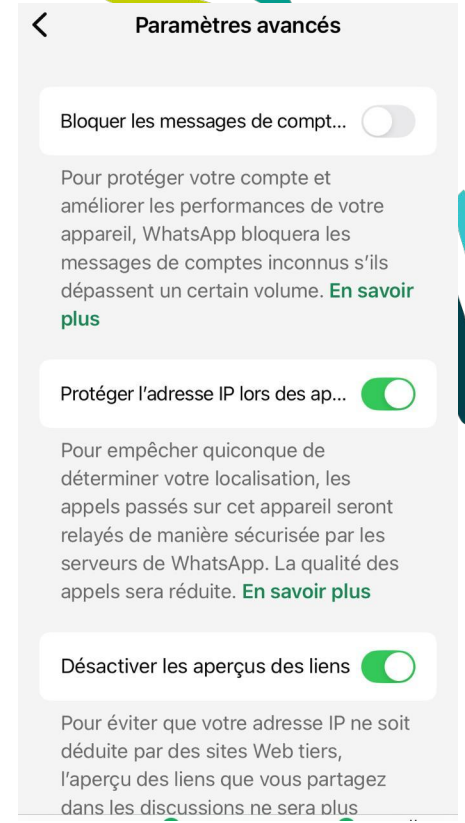


Verrouillage

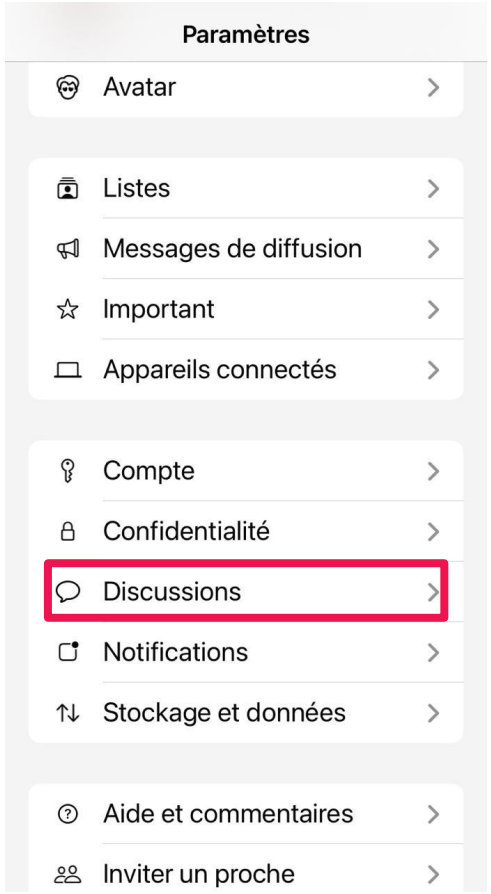

Paramètres
Avatar
Listes
Messages de diffusion
Important
Appareils connectés
Compte
Confidentialité
Discussions
Notifications
Stockage et données

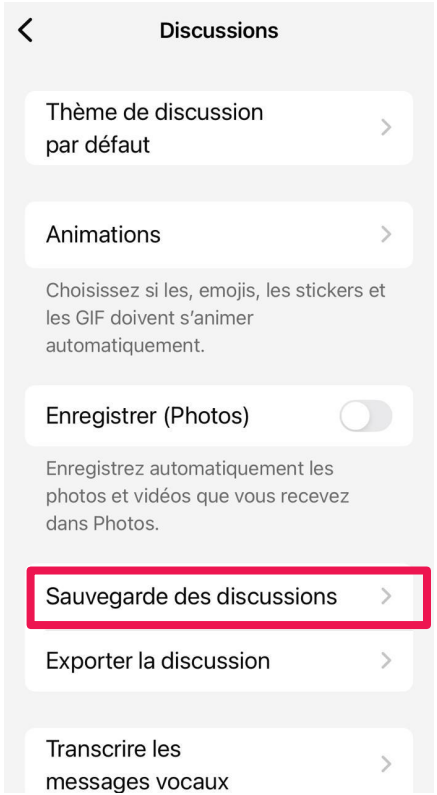

Confidentialité
Présence en ligne
Mes contacts
Photo de profil
Mes contacts
Infos
Mes contacts
Liens
Mes contacts
Groupes
Mes contacts
Stickers d'avatar
Mes contacts
Statut
Mes contacts
Localisation en direct
Aucune
Liste des discussions dans lesquelles vous partagez votre localisation en direct.

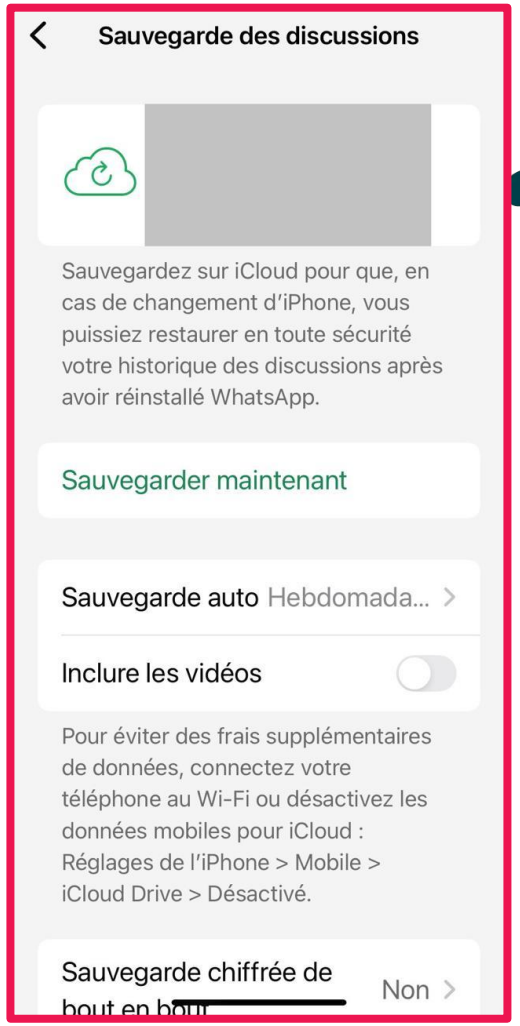

Confidentialité
Les confirmations de lecture sont toujours envoyées dans les discussions de groupe.
Verrouillage de l'application
Face ID est nécessaire pour déverrouiller WhatsApp.
Verrouillage
Autoriser les effets de caméra
Utilisez les effets de caméra durant les appels vidéo.En savoir plus
Paramètres avancés
Vérification de la confidentialité


Paramètres avancés
Bloquer les messages de compt...
Pour protéger votre compte et améliorer les performances de votre appareil, WhatsApp bloquera les messages de comptes inconnus s'ils dépassent un certain volume. En savoir plus
Protéger l'adresse IP lors des ap...
Pour empêcher quiconque de déterminer votre localisation, les appels passés sur cet appareil seront relayés de manière sécurisée par les serveurs de WhatsApp. La qualité des appels sera réduite. En savoir plus
Désactiver les aperçus des liens
Pour éviter que votre adresse IP ne soit déduite par des sites Web tiers, l'aperçu des liens que vous partagez dans les discussions ne sera plus

Avancée


Paramètres
Avatar
Listes
Messages de diffusion
Important
Appareils connectés
Compte
Confidentialité
Discussions
Notifications
Stockage et données
Aide et commentaires
Inviter un proche


Discussions
Thème de discussion par défaut
Animations
Choisissez si les, emojis, les stickers et les GIF doivent s'animer automatiquement.
Enregistrer (Photos)
Enregistrez automatiquement les photos et vidéos que vous recevez dans Photos.
Sauvegarde des discussions
Exporter la discussion
Transcrire les messages vocaux


Sauvegarde des discussions
Sauvegardez sur iCloud pour que, en cas de changement d'iPhone, vous puissiez restaurer en toute sécurité votre historique des discussions après avoir réinstallé WhatsApp.
Sauvegarder maintenant
Sauvegarde auto Hebdomada...
Inclure les vidéos
Pour éviter des frais supplémentaires de données, connectez votre téléphone au Wi-Fi ou désactivez les données mobiles pour iCloud : Réglages de l'iPhone > Mobile > iCloud Drive > Désactivé.
Sauvegarde chiffrée de bout en bout
Non

Sauvegarde

Glossaire

VPN ou réseau privé virtuel, est une technologie qui crée une connexion sécurisée et chiffrée via Internet, permettant aux utilisateurs de naviguer en toute confidentialité et d'accéder à des contenus soumis à des restrictions géographiques. En substance, un VPN agit comme un tunnel sécurisé qui crypte vos données et masque votre adresse IP, protégeant ainsi votre confidentialité et votre sécurité en ligne.

Merci !

www.innovusconsulting.co

Animateurs de la séance : Catalina Valenzuela, Paula Quiñones et Camilo Forero

Créatrice du module : Carolina Botero