WhatsApp Sécurité 09/2026

WhatsApp offre un niveau de sécurité réel mais partiel, et la nuance est importante pour bien évaluer sa fiabilité.

Le point fort est solide : depuis 2016, WhatsApp utilise le protocole de chiffrement de Signal pour le chiffrement de bout en bout, activé par défaut sur toutes les conversations et en fait largement la promotion via sa pub.

Concrètement, cela signifie que le contenu des messages est chiffré sur l'appareil de l'expéditeur et ne peut être déchiffré que par le destinataire - les serveurs de Meta ne peuvent ni lire ni intercepter le contenu en clair. C'est un vrai rempart contre la surveillance de masse et l'espionnage passif du réseau, Mais :

Le problème est que ce chiffrement protège le contenu, pas tout le reste. Plusieurs failles structurelles restent exploitées ou documentées :

Les **métadonnées** (*) échappent au chiffrement. **WhatsApp sait qui parle à qui, quand, à quelle fréquence, quels appareils sont utilisés, et peut observer les statuts en ligne/hors ligne**.

Un document interne de WhatsApp révélé en 2024 montrait que ces métadonnées, croisées avec une surveillance du trafic internet à l'échelle d'un pays, peuvent **permettre à un État de reconstituer qui communique avec qui —** sans jamais casser le chiffrement lui-même.

Une faille découverte début janvier 2026 permettait d'identifier si un utilisateur était sur **iOS ou Android** à partir de son seul numéro de téléphone, en exploitant des différences dans la génération des clés de chiffrement

Le maillon faible reste l'appareil lui-même. Le chiffrement ne protège rien si le téléphone est compromis en amont.

À cela s'ajoutent des questions structurelles moins techniques : les sauvegardes cloud (Google Drive, iCloud) ne sont pas systématiquement chiffrées de bout en bout selon les configurations,

WhatsApp appartient à Meta et partage certaines métadonnées avec l'écosystème Meta (notamment à des fins publicitaires ou business), et l'application reste soumise aux réquisitions judiciaires dans les pays où elle opère.

En résumé, pour un usage grand public contre une interception passive des messages, WhatsApp est fiable et le chiffrement de bout en bout fonctionne.

Pour quelqu'un qui a un profil à risque spécifique (journaliste, militant, source protégée, personnalité visée par des acteurs étatiques), les angles morts, métadonnées, appareil compromis, sauvegardes sont significatifs, et des alternatives comme Signal (qui minimise davantage les métadonnées et n'appartient pas à un groupe publicitaire) sont souvent recommandées par les experts en sécurité pour ce type d'usage.

(*) **Métadonnées** : *Les métadonnées, ce sont toutes les informations autour d'un message, mais pas le message lui-même.*

Ex : Si le contenu chiffré est une lettre cachetée, les métadonnées sont tout ce qui est écrit sur l'enveloppe : qui l'envoie, à qui, quand, depuis où, même si personne ne peut ouvrir la lettre.

Concrètement, pour WhatsApp cela inclut par exemple :

Qui vous contactez et à quelle fréquence, *même si le contenu de la conversation reste illisible, WhatsApp sait que votre numéro a échangé des messages avec tel autre numéro entre 22h et minuit tous les soirs. Les horodatages précis d'envoi et de réception, ainsi que les accusés de lecture (les fameux doubles coches bleues).*

Votre statut en ligne/hors ligne*, y compris via des « pings silencieux » qui permettent de savoir quand vous êtes actif sur l'app sans que vous le sachiez.*

Les appareils que vous utilisez *(modèle, système d'exploitation, nombre d'appareils liés à votre compte).*

Votre localisation approximative, *déduite indirectement via l'adresse IP ou les délais de transmission réseau.*
Les membres et l'existence d'un groupe*, même si les messages échangés dedans restent chiffrés.*

Votre numéro de téléphone et vos contacts*, que WhatsApp utilise aussi à des fins publicitaires au sein de l'écosystème Meta (Facebook, Instagram).*

M. M.