Comment Faire Confiance sans être Expert ? Messageries Chiffréestechnologiesintelligence-artificielle

ChatGPT préconise Signal et Matrix.

Matrix : https://wiki.chatons.org/doku.php/services/messagerie_instantanee/matrix https://club1.fr/docs/fr/services/matrix.html Mais il semble que : https://www.mobilicites.com/matrix-la-chute-spectaculaire-de-la-messagerie-cryptee-preferee-des-criminels.html En fait c'est “l'infiltration” qui insécure les messageries.

Réponse ChatGPT

https://chatgpt.com/share/6751c0dd-bd4c-8001-8d0a-fdc33c94593c Comment être sûr d'une messagerie chiffrée qui n'a pas de “poorte dérobée” ? ChatGPT a dit : ChatGPT Pour être sûr qu'une messagerie chiffrée n'a pas de “porte dérobée” (backdoor), il est essentiel de suivre ces étapes et critères :

1. Utiliser des solutions open source

Code ouvert : Préférez les messageries dont le code source est public et accessible, comme Signal ou Matrix. Cela permet à des experts indépendants d’auditer le code pour détecter d’éventuelles failles ou backdoors. Communauté active : Une communauté open source active garantit une mise à jour régulière et une surveillance continue.

2. Privilégier le chiffrement de bout en bout (E2EE)

Assurez-vous que la messagerie utilise un chiffrement de bout en bout par défaut. Cela garantit que seuls l’expéditeur et le destinataire peuvent lire les messages. Protocole vérifié : Le protocole de chiffrement utilisé (par exemple, Signal Protocol, Olm pour Matrix) doit être reconnu comme sécurisé par la communauté cryptographique.

3. Audit indépendant et régulier

Vérifiez si la messagerie a été auditée récemment par des experts en sécurité indépendants. Les rapports d'audit devraient être publiés et accessibles au public. Transparence de l'éditeur : Une entreprise ou un projet sérieux publie des informations sur les audits et leur conformité aux standards de sécurité.

4. Fédération et décentralisation

Les plateformes décentralisées, comme Matrix, offrent plus de contrôle aux utilisateurs et sont plus difficiles à compromettre globalement. Une architecture fédérée signifie qu’il n’y a pas un point unique de contrôle, réduisant le risque d’implanter une porte dérobée.

5. Vérification des clés

La messagerie devrait permettre une vérification manuelle des clés publiques (comme un échange de clés via QR code). Cela garantit que le chiffrement n’est pas compromis par une attaque de type Man-In-The-Middle. Fonctionnalités associées : Fonction de gestion des clés, notification en cas de changement de clé d’un contact, etc.

6. Modèle économique aligné sur la sécurité

Les messageries financées par des donations (comme Signal) ou par des modèles payants transparents sont plus fiables. Évitez celles financées par la publicité ou basées dans des pays avec des lois intrusives (ex. : surveillance étatique ou obligations de backdoors).

7. Examinez le cadre légal

Vérifiez où se situe juridiquement le service. Par exemple : Signal : basé aux États-Unis, mais son code est open source. Threema : basé en Suisse, pays réputé pour ses lois strictes sur la vie privée. Lois sur la surveillance : Certaines juridictions obligent les entreprises à insérer des backdoors.

8. Méfiez-vous des options suspectes

Les messageries avec des options “facultatives” pour activer le chiffrement (ex. : Telegram, où le chiffrement n'est pas activé par défaut pour toutes les conversations). Solutions non vérifiables ou fermées (comme WhatsApp, qui utilise Signal Protocol, mais reste une entreprise sous la coupe de Meta).

9. Tests indépendants et réputation

Consultez les analyses et classements de chercheurs indépendants (ex. : EFF - Electronic Frontier Foundation) pour voir quelles messageries sont jugées sécurisées.

En conclusion

, une messagerie comme Signal (avec son modèle open source, son financement transparent, et ses audits réguliers) ou des solutions décentralisées comme Matrix/Element sont parmi les meilleures options pour éviter les backdoors. Cependant, la sécurité dépend aussi de votre usage : utilisez des mots de passe forts, ne sauvegardez pas les messages sur des serveurs non sécurisés, et gardez vos appareils à jour.

Face aux cyberattaques, le FBI conseille ...

28/04/2025

Face aux cyberattaques, le FBI conseille d'utiliser des messageries chiffrées

Les cyberattaques sur les réseaux cellulaires d'AT&T et de Verizon poussent les autorités américaines, le FBI en tête, à recommander aux citoyens d'utiliser des messageries chiffrées de bout en bout pour s'assurer que leurs communications ne tombent pas entre de mauvaises mains. Un conseil pour le moins étonnant, alors que le FBI ne cesse de réclamer un affaiblissement du chiffrement de bout en bout pour faciliter ses enquêtes.

« Salt Typhoon » : derrière ce nom imagé se cache une redoutable attaque menée par des pirates chinois sur les infrastructures de télécommunications américaines, AT&T et Verizon en tête. C'est une des plus importantes campagnes de piratage jamais essuyées par les États-Unis. Une attaque d'une ampleur historique aux États-Unis Les hackers tentent de récupérer trois types d'informations, selon le FBI : les métadonnées des appels (numéros appelés, durée et localisation), les appels téléphoniques pour certaines cibles que le Bureau n'a pas voulu révéler (les pirates se concentrent sur la capitale fédérale Washington), et les systèmes de surveillance CALEA. Ces derniers sont utilisés pour permettre aux agences de renseignement et aux forces de l'ordre de surveiller les communications avec autorisation judiciaire. Lire : des pirates chinois rôderaient toujours dans les réseaux américains Le FBI a demandé aux employés du gouvernement de communiquer avec des applications chiffrées de bout en bout (E2EE), comme WhatsApp, Facebook Messenger ou encore l'app Messages d'Apple entre utilisateurs d'iPhone. Une recommandation désormais élargie à l'ensemble des citoyens américains. « Notre recommandation, ce que nous avons dit en interne, n'a rien de nouveau : le chiffrement est votre allié, que ce soit pour les messages texte ou, si vous en avez la possibilité, pour les communications vocales chiffrées. Même si l'adversaire parvient à intercepter les données, si elles sont chiffrées, cela les rendra inexploitables », a déclaré un représentant du FBI à NBC News. Autre recommandation : utiliser un smartphone qui reçoit des mises à jour de sécurité régulièrement, qui utilise un chiffrement bien géré ainsi qu'un système d'authentification multi-facteurs pour résister aux tentatives d'hameçonnage. Des conseils de bon sens que tout le monde devrait suivre, pas uniquement les Américains ! Le FBI tente ici de ménager la chèvre et le chou. Si le chiffrement E2EE est efficace pour se protéger des attaques de l'étranger, le FBI milite aussi (et depuis longtemps !) pour des portes dérobées afin d'accélérer ses enquêtes. Une communication E2EE s'assure que seuls les correspondants y aient accès, et personne d'autre, pas même la plateforme, le constructeur du smartphone, l'opérateur ou la police, ne peut y accéder. Y intégrer une porte dérobée, même pour les forces de l'ordre, c'est affaiblir le chiffrement : qui dit que des pirates ne pourraient pas s'y engouffrer ? Cette problématique du chiffrement à casser revient régulièrement sur le tapis, aux États-Unis, en Europe ainsi qu'en France. Pour ne manquer aucune actualité de 01net, suivez-nous sur Google Actualités et WhatsApp. Source : NBC News https://www.01net.com/actualites/face-cyberattaques-fbi-conseille-utiliser-messageries-chiffreesles-cyberattaques-sur-les-reseaux-cellulaires-datt-et-de-verizon-poussent-les-autorites-americaines-fbi-en-tete-a-recom.html

---

Comments

Menu ▼ |Daily|jmc947|Carte|

Connexion List & Search