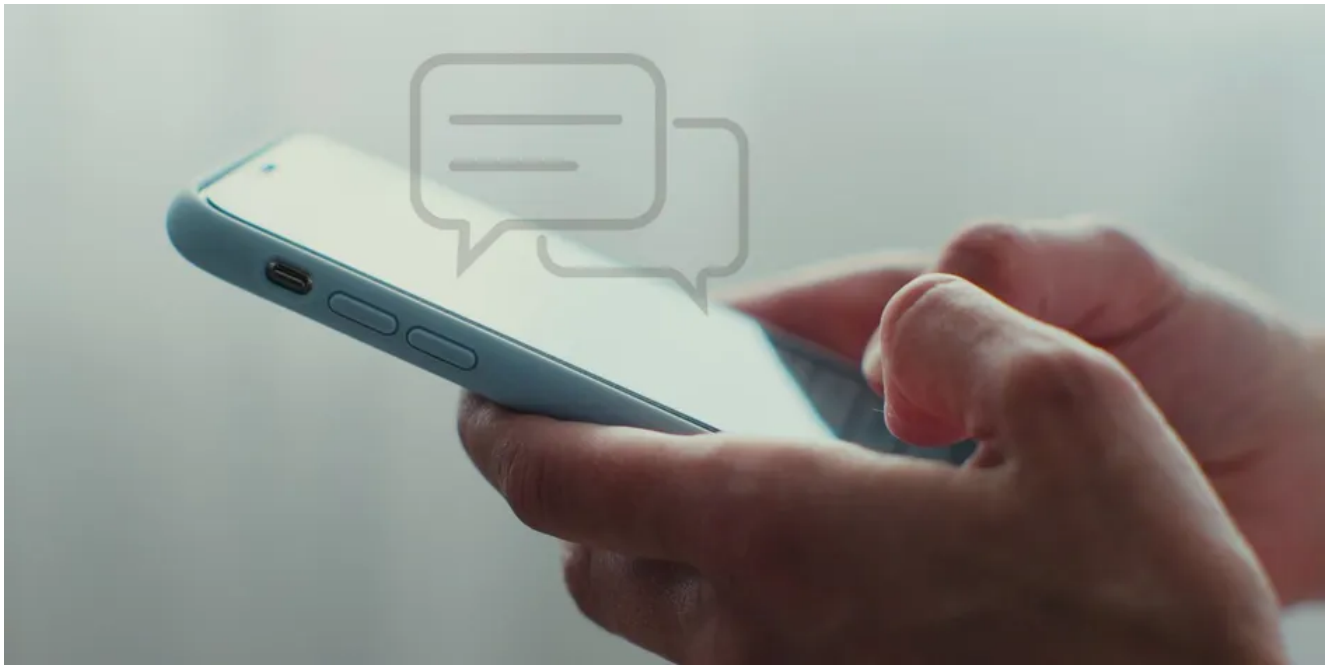
Vous utilisez toujours des SMS, voici pourquoi vous devriez arrêter

Beaucoup d'utilisateurs utilisent encore par défaut les SMS sur leurs cellulaires.
Mais c'est une mauvaise nouvelle pour votre sécurité et votre vie privée.
Voici pourquoi et ce que vous pouvez faire.

Damir Mujezinovic :



Le service de messagerie courte (SMS) est un élément de base de la communication mobile depuis les années 1990, lorsqu'il a été déployé commercialement sur les réseaux cellulaires du monde entier.

Avec l'avènement des smartphones, les services de messagerie basés sur le protocole Internet sont devenus plus populaires, mais les SMS sont encore largement utilisés, et ce n'est pas nécessairement une bonne chose.

Pourquoi les SMS ne sont pas sûrs: 5 raisons

SMS est pratique et facile à utiliser.
Il est présent sur à peu près tous les téléphones portables, et vous n'avez même pas besoin d'Internet pour l'utiliser.
Cela démontre de manière convaincante pourquoi les SMS restent populaires. Cependant, si vous voulez rester en sécurité et préserver votre vie privée, vous ne devriez pas l'utiliser.
Voici cinq raisons.

1. Absence de chiffrement de bout en bout

Les SMS ne sont pas chiffrés de bout en bout.
En fait, les messages SMS sont généralement envoyés en texte brut.
Cela signifie qu'il n'y a aucune protection en place et que presque n'importe qui avec un savoir-faire suffisant peut intercepter un SMS.
Si votre opérateur mobile utilise un certain type de cryptage, il utilise probablement un algorithme faible et obsolète, et il n'est appliqué que pendant le transit.

2. Le SGS repose sur une technologie désuète

La technologie SMS repose sur un ensemble de protocoles de signalisation appelé Signaling System No. 7 (SS7), qui a été développé dans les années 1970.
Il est obsolète et très peu sécurisé, ce qui le rend vulnérable à divers types de cyberattaques.
En 2017, comme Ars Technica l'a rapporté à l'époque, un groupe de pirates informatiques a exploité une faille de sécurité dans SS7 pour contourner l'authentification à deux facteurs afin de vider les comptes bancaires des gens.
Des attaques similaires ont été enregistrées à de nombreuses reprises au fil des ans.

3. Le gouvernement peut lire vos SMS

Capture d'écran, pour visionner la vidéo, cliquer le lien YouTube suivant:

Exposing Government Mobile Phone Surveillance Program via SS7 Attack - YouTube

Pourquoi les failles de sécurité de SS7 n'ont-elles pas été corrigées ?
Une explication possible est que les régulateurs ne sont pas particulièrement intéressés à le faire, parce que

les gouvernements du monde entier écoutent leurs citoyens.
Que ce soit la vraie raison ou non, il est incontestable que votre gouvernement pourrait lire vos SMS s'il le voulait.
Aux États-Unis, les forces de l'ordre n'ont même pas besoin d'un mandat pour accéder aux messages datant de plus de 180 jours.
Le représentant du Congrès, Ted Lieu, a présenté un projet de loi qui mettrait fin à cela en 2022, mais en vain.

4. Votre opérateur stocke vos messages

Les messages SMS sont stockés par les opérateurs pendant une certaine période de temps (la durée dépend de l'opérateur). Les métadonnées, qui concernent les informations sur les données elles-mêmes, sont stockées encore plus longtemps.
Si vous ne craignez pas que les forces de l'ordre lisent vos messages, sachez peut-être que votre opérateur mobile peut également y accéder.
S'il est bien sûr vrai que les lois, les règlements et les politiques internes empêchent les fournisseurs de téléphonie mobile d'espionner les utilisateurs, des accès non autorisés et des violations se produisent toujours.

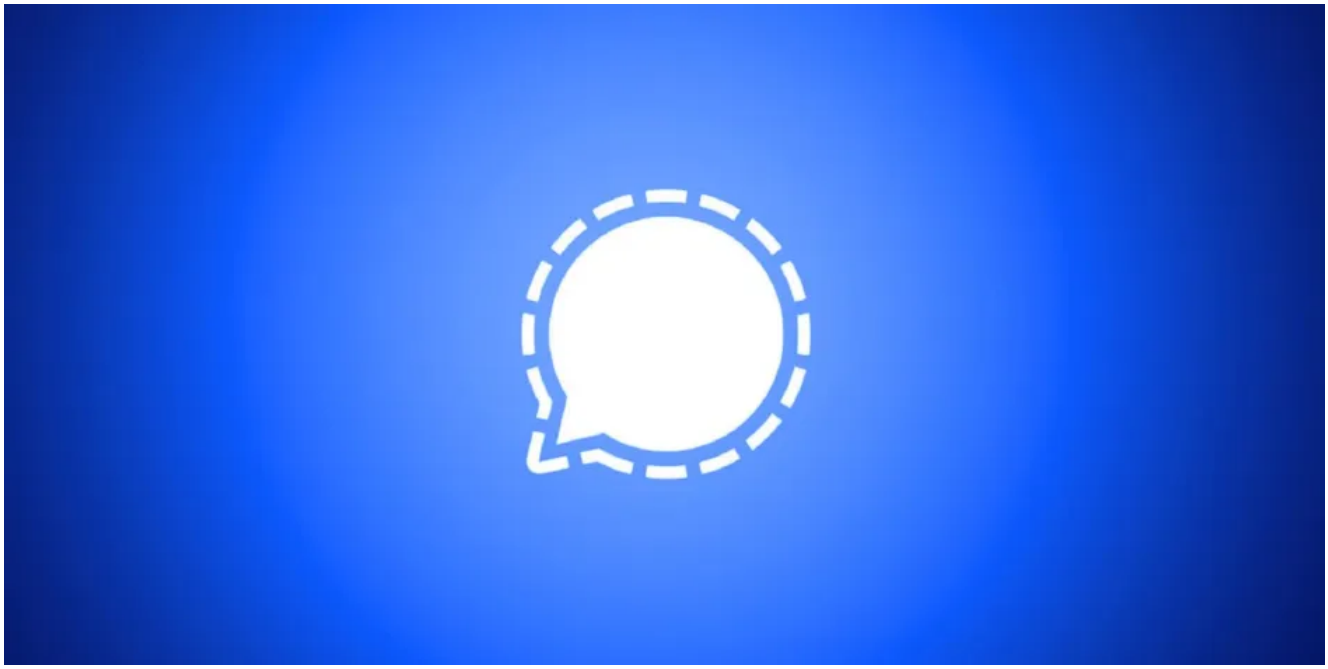
5. Vous ne pouvez pas annuler l'envoi d'un message SMS

Il n'est pas possible d'annuler l'envoi d'un SMS.
Une fois que le destinataire l'a reçu, il restera sur son téléphone indéfiniment, à moins qu'il ne le supprime manuellement. Envoyer un SMS regrettable et embarrassant est une chose, mais que se passe-t-il si le téléphone du destinataire est piraté ou compromis d'une manière ou d'une autre?
Et que se passe-t-il si vous avez révélé dans un SMS des informations personnelles que vous n'auriez pas dû révéler?
C'est probablement un scénario que vous préférez ne pas envisager.

Quelle est la meilleure alternative aux SMS ?

Voici l'avantage: il existe de nombreuses alternatives aux SMS, et elles sont beaucoup plus sûres.
Voici trois applications de messagerie cryptées que vous devriez envisager d'utiliser, au lieu de mettre vos données entre les mains d'une technologie SMS obsolète.

1. Signal



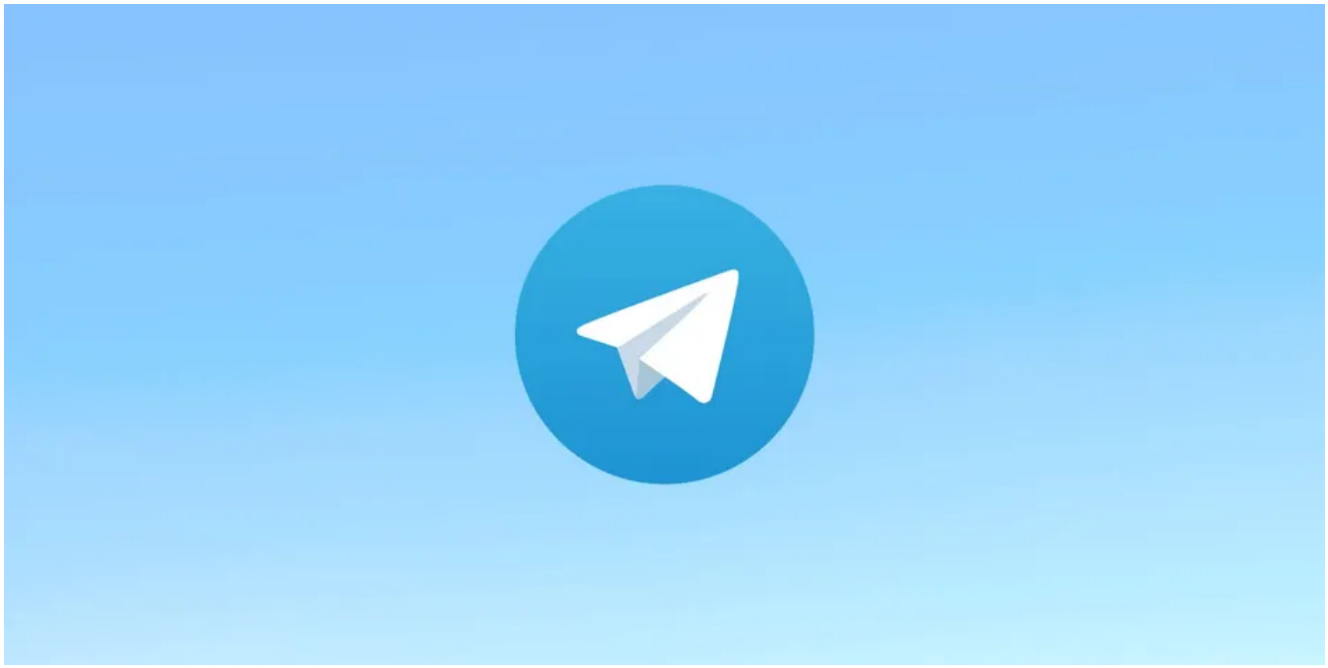
Signal est sans doute la meilleure application de messagerie sécurisée disponible aujourd'hui.
Pour commencer, il utilise un cryptage de bout en bout, ce qui signifie que seuls vous et le ou les destinataires en retrait pouvez lire les messages que vous échangez.
Le contenu d'un message ne peut pas être intercepté, récupéré ou consulté par quelqu'un d'autre, et cela inclut Signal.

L'application, qui a été développée par la Fondation à but non lucratif Signal et Signal Messenger LLC, ne collecte aucune donnée.
Il ne sait rien de vous et n'exige aucun accès à votre appareil photo, à vos contacts ou à quoi que ce soit du genre.

De plus, il est 100% gratuit.
Tout ce que vous avez à faire en tant qu'utilisateur est de le télécharger et de mettre votre numéro de téléphone.

Télécharger: Signal pour iOS | Android | Windows | MacOS

2. Telegram (Télégramme)



Telegram est probablement la meilleure option si vous recherchez une bonne alternative aux SMS.
Les messages envoyés via Telegram ne sont pas chiffrés de bout en bout par défaut, mais l'utilisateur peut activer le chiffrement en activant les conversations secrètes.
Les messages des chats secrets ne peuvent être transférés ou consultés par personne. Cela inclut les photos, les vidéos et les documents, qui peuvent également être configurés pour s'autodétruire après un certain temps.

Bien que Signal ne soit, à bien des égards, pas différent des applications de messagerie ordinaires, Telegram est plutôt unique.
C'est aussi un réseau social que vous pouvez utiliser pour participer à des discussions avec d'autres personnes, échanger des informations, rejoindre des groupes, etc.
La société derrière Telegram ajoute souvent de nouvelles fonctionnalités sociales à l'application, ce qui l'a rendue plus populaire ces dernières années.

Télécharger: Telegram pour iOS | Android | Windows | MacOS

3. WhatsApp

WhatsApp est une autre bonne alternative.
Oui, il appartient à Meta, la même société qui possède Facebook et Instagram, et personne ne se fait d'illusions sur le fait que c'est une bonne chose.
Mais il a un avantage majeur par rapport aux autres applications de messagerie: WhatsApp a quelques milliards d'utilisateurs actifs, il est donc plus que probable que la plupart de vos contacts l'ont installé sur leur téléphone.

Malgré l'association Meta problématique, rien n'indique que WhatsApp est dangereux. Tous les messages envoyés via le chat sont cryptés de bout en bout, ce qui signifie que personne ne peut y accéder ou les lire.
Dans tous les cas, WhatsApp est beaucoup plus sécurisé que les SMS, et le fait qu'il soit extrêmement populaire ne peut être ignoré.
Il est également gratuit et disponible sur toutes les principales plateformes.

Télécharger: WhatsApp pour iOS | Android | Windows | MacOS

Abandonner les SMS pour une application de messagerie sécurisée

Les SMS ne devraient pas être une option pour quiconque se soucie de sa cybersécurité personnelle et souhaite préserver sa vie privée.
Le problème est qu'il offre un niveau de commodité que les alternatives ne peuvent tout simplement pas égaler, du moins pas pour l'instant.
Mais ce n'est pas une raison suffisante pour l'utiliser, dans la plupart des circonstances.

Les applications de messagerie cryptées sécurisées de bout en bout sont supérieures aux SMS à presque tous les autres égards.
Et dans les situations où vous n'avez pas d'autre option, utilisez les SMS à bon escient. Ne partagez pas d'informations auxquelles vous ne voudriez pas qu'un tiers accède et n'oubliez pas de prendre d'autres mesures de sécurité.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231003
"C'est ensemble qu'on avance"