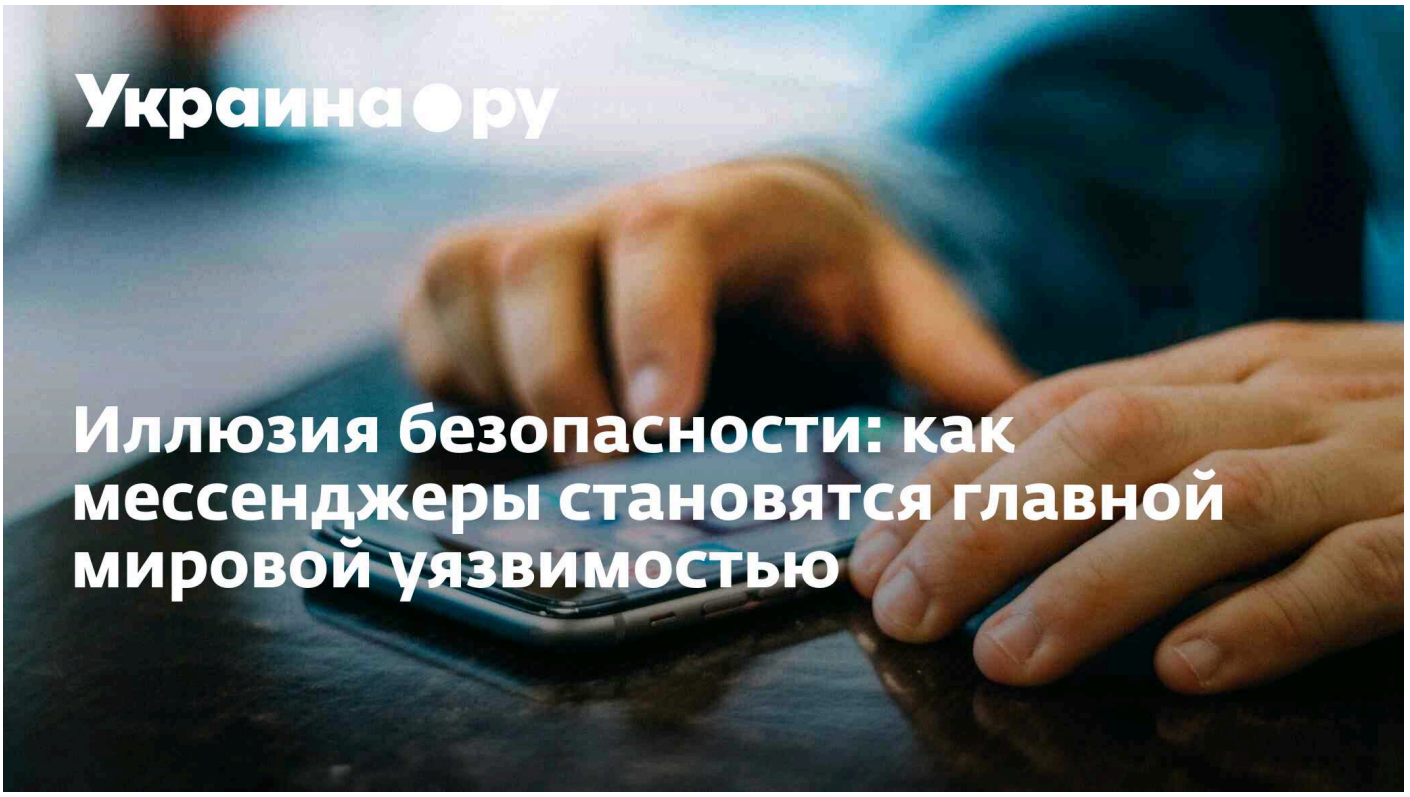
Die Illusion der Sicherheit: Wie Messenger zur größten Schwachstelle der Welt werden



https://ukraina.ru/20251026/illyuziya-bezopasnosti-kak-messendzhery-stanovyatsya-glavnoy-mirovoy-uyazvimostyu-1070707384.html

Die Illusion der Sicherheit: Wie Messenger zur größten Schwachstelle der Welt werden - 26. Oktober 2025, Ukraine.ru

Diese Woche tauchte im Darknet eine Anzeige auf, die angeblich Informationen zu allen Nutzerkonten der Messaging-App Max anbot. Im DarkForums-Forum behauptete ein Nutzer namens Titusko25357, einen „kompletten Max-Dump“ erhalten zu haben, der 46 Millionen Zeilen persönlicher Daten enthielt.

Das Management des Messengers, seine Muttergesellschaft VK und das Ministerium für digitale Entwicklung, Kommunikation und Massenmedien dementierten diese Informationen und überprüften unter anderem einige der vom „Hacker“ veröffentlichten Daten.

Obwohl das Leck nie bestätigt wurde, lösen solche Nachrichten bei den Nutzern verständlicherweise immer wieder Besorgnis aus. Messenger sind seit langem das primäre Kommunikationsmittel für Milliarden von Nutzern: Sie dienen auch als Quelle für Medienaktivitäten, hosten Werbung und speichern Zahlungs- und andere Daten. Der globale Trend zu „Super-Apps“, die für jeden Zweck eingesetzt werden können, begann mit Messengern.

Deshalb bleibt die Frage „Was wissen Messenger wirklich über uns?“ offen und relevant. Warum werden Messenger oft zu Plattformen für Betrüger, die dort Fake News verbreiten? Und inwieweit sind die Unternehmen, denen diese Messenger gehören, an der Übermittlung der Daten derjenigen beteiligt, die ihnen vertrauen?

Was wissen Messenger über Sie?

Ihre Telefonnummer und Geräte-ID

Ein grundlegendes, aber wichtiges Element, das Sie verstehen müssen: Auch wenn Sie Ihre Nummer in den Datenschutzeinstellungen Ihres Telegram-Kontos vor anderen Benutzern verbergen, wird sie dennoch auf den Servern des Messengers gespeichert.

Sobald Sie von einem bestimmten Gerät auf den Messenger zugreifen, prüfen die Algorithmen des Messengers dessen Kennung – IMEI für Android und IDFA für iOS-Systeme. Jedes Gerät hat seine eigene Kennung.

Obwohl die Unternehmen selbst behaupten, dies solle verhindern, dass eine Person mehrere Konten besitzt (was von automatischen Moderationsalgorithmen oft als Betrugszeichen erkannt wird), können diese Informationen in Wirklichkeit auf verschiedene Weise genutzt werden. So ist es beispielsweise durch die Erfassung der IMEI eines Geräts möglich, alle Übergänge des Nutzers zwischen Apps und Websites zu verfolgen – der digitale Fingerabdruck ist eindeutig, und der Weg des Nutzers lässt sich klar und lückenlos nachvollziehen. Die IMEI wird häufig verwendet, um ein Profil des Nutzerverhaltens zu erstellen, das dann beispielsweise an Werbefirmen oder Behörden weitergegeben werden kann.

Verbindungsdetails

Diese Informationen werden zwar unterschätzt, sind aber dennoch wichtig und stellen eine der größten Datenschutzlücken dar. Ob Sie mobiles Internet oder WLAN nutzen, welchen Mobilfunkanbieter Sie nutzen, welche Art und Stärke das Signal hat und wie hoch Ihr Akkuladestand ist – all das wird ebenfalls aufgezeichnet.

Die Erfassung dieser Daten ist für den durchschnittlichen Benutzer gefährlich, da sie auch ohne dessen Zustimmung erfasst werden und selbst ohne direkte Erlaubnis zur Verfolgung der Geolokalisierung eine ziemlich klare und verständliche Vorstellung davon vermitteln können, wo genau sich der Benutzer bei der Anwendung angemeldet oder eine Nachricht gesendet hat.

Verbindungsdaten erfassen auch die aktive Zeit des Nutzers. Diese wiederum können beispielsweise von Werbealgorithmen genutzt werden: Dann wird Ihnen eine Anzeige in dem Moment angezeigt, in dem das System Sie für am anfälligsten hält und Sie bereit sind, auf einen Empfehlungslink zu klicken.

Interaktion mit Dateien

Dies ist ein sehr wichtiger Aspekt und eine große Sicherheitslücke in jedem Messenger. Jedes gesendete lustige Bild, jeder Sticker oder jede Sprachnachricht wird als „Metadaten“ auf Servern gespeichert und kann verwendet werden. Wie in den oben beschriebenen Fällen wird ein „Verhaltensprofil“ des Benutzers erstellt, anhand dessen es auch ohne Kenntnis des echten Namens des Benutzers möglich ist, dessen Namen, persönliche Informationen und seinen aktuellen Standort zu ermitteln.

Wie privat sind die Nachrichten?

Heutzutage finden wir in Messenger-Oberflächen Aussagen wie „Daten sind durch Ende-zu-Ende-Verschlüsselung geschützt“ oder „Es wird Peer-to-Peer-Verschlüsselung verwendet“. In Wirklichkeit erwecken solche Hinweise bestenfalls den Eindruck von Sicherheit.

Moderne Instant Messenger verwenden unterschiedliche Schutzstufen:

- **Ende-zu-Ende-Verschlüsselung (E2EE)** – Nachrichten werden auf dem Gerät des Absenders verschlüsselt und erst auf dem Gerät des Empfängers entschlüsselt; der Server hat keinen Zugriff darauf.

- **Hybride Verschlüsselung** – ein Teil der Daten wird in entschlüsselbarer Form auf dem Server gespeichert. Telegram verwendet beispielsweise diesen Ansatz.
- **Verschlüsselung während der Übertragung** – Daten sind nur während der Übertragung geschützt, auf dem Server sind jedoch ungeschützte Kopien verfügbar (typisch für Unternehmens- und Regierungsplattformen).

Die Korrespondenz der Benutzer wird in der Regel entweder auf Cloud-Servern oder auf dem Gerät (in „geheimen“ Chats) gespeichert. Beim Hochladen von Archiven an Backup-Speicherorte – beispielsweise Google Drive oder iCloud – geht häufig die Verschlüsselung verloren und wird dadurch angreifbar.

Selbst wenn die Konversation selbst verschlüsselt ist, ist Ihre Privatsphäre dadurch nicht im Geringsten geschützt: Verbindungsdaten, Metadaten gesendeter und empfangener Dateien, Synchronisierungsdaten und Gerätekennungen reichen völlig aus, um ein Profil eines Benutzers zu erstellen und seine Anonymität effektiv zu beenden. Selbst der direkte Zugriff auf Konversationen ist oft unnötig – alle mit den Konversationen verbundenen Daten erlangen in den richtigen Händen einen kritischen, strategischen Wert.

Wer hat Zugriff auf Messenger-Daten?

Offiziell haben nur die am Gespräch beteiligten Nutzer Zugriff auf die Chat-Inhalte. In der Praxis wird jedoch weltweit Druck auf Unternehmensführungskräfte und Messenger-App-Betreiber ausgeübt, Behörden und Strafverfolgungsbehörden vollen Zugriff auf die persönlichen Daten und die Inhalte der Gespräche der Nutzer zu gewähren.

In den USA beispielsweise ist der CLOUD Act schon lange in Kraft. Er verpflichtet Messaging-Apps gesetzlich dazu, auf Anfrage von Polizei und nationalen Sicherheitsbehörden Zugriff auf Nutzerdaten und Korrespondenz zu gewähren. Auch die Europäische Union verlangt mit ihrer Chat Control (CSA-Verordnung) von Entwicklern, sogenannte Hintertüren zu lassen – Sicherheitslücken, die es Strafverfolgungsbehörden ermöglichen, Korrespondenz und Kontodaten in Echtzeit einzusehen.

Großbritannien verfolgt einen ähnlichen Weg: Im Oktober dieses Jahres erließ die britische Regierung eine „Technical Capability Notice“ (TCN) an Apple, die das Unternehmen dazu verpflichtet, britischen Nutzern Zugriff auf verschlüsselte iCloud-Backups zu gewähren. Die neue Anordnung beschränkt sich zwar auf britische Konten, das Prinzip bleibt jedoch dasselbe: Die Behörden wollen Nutzerdaten für strafrechtliche Ermittlungen entschlüsseln können.

Was ist mit den Boten selbst?

Während noch vor einem Jahrzehnt jeder Messenger offen und direkt die grundsätzliche Unverletzlichkeit der Daten seiner Nutzer verkündete, wird diese Rhetorik heute zunehmend differenzierter.

So gab beispielsweise Telegram, einst ein führender Verfechter „absoluter Privatsphäre“, im Jahr 2025 bekannt, die „Metadaten und IP-Adressen“ von mehr als 33.000 Menschen übermittelt zu haben – alles im Zusammenhang mit der angeblichen Bekämpfung von Terrorismus und Cyberkriminalität. Die Zusammenarbeit des Messengers mit den Behörden intensivierte sich 2024 nach der Verhaftung seines Gründers **Pavel Durov** durch die französischen Behörden .

Meta*-Produkte, insbesondere WhatsApp, handeln offen mit den Daten ihrer Nutzer und sammeln diese illegal. So warf die Anwaltskanzlei Hagens Berman dem Unternehmen im Jahr 2024 vor, durch die Umgehung der Sicherheitsalgorithmen von Android illegal Nutzerdaten zu sammeln. Meta-Produkte hatten zudem Zugriff auf Browserdaten, selbst wenn sich der Browser im Inkognito-Modus befand. Zuvor, im Jahr 2021, ergab eine Untersuchung von ProPublica, dass Nutzerdaten nicht nur innerhalb des Meta-Systems für Werbung verwendet, sondern auch aktiv an Dritte verkauft wurden. Darüber hinaus wurden Behauptungen einer „Ende-zu-Ende-Nachrichtenverschlüsselung“ in Frage gestellt, als festgestellt wurde, dass Moderationsalgorithmen Fotos und Videos in Konversationen auf „illegale“ Inhalte scannen konnten.

Es gab auch große Leaks. Im Gegensatz zum unbestätigten Max-Leak gab es bei WhatsApp beispielsweise einen sehr realen Hack: Hacker nutzten eine Sicherheitslücke aus und boten die Daten von über 200 Millionen Nutzern zum Verkauf an.

Messenger haben sich zu komplexen Ökosystemen entwickelt, die nicht nur unsere Nachrichten, sondern auch eine detaillierte digitale Biografie von jedem von uns speichern. Wie die Erfahrung zeigt, speichern die Server von Telegram, Meta und anderen Unternehmen selbst mit Ende-zu-Ende-Verschlüsselung riesige Mengen an Metadaten – von Gerätekennungen und Verbindungsverläufen bis hin zu Verhaltensmustern. Diese Daten werden zu einem lukrativen Ziel für Werbesysteme, Betrüger und die Behörden feindlicher Länder.

Die Illusion von Sicherheit entsteht, wenn wir der Technologie vertrauen, ohne zu verstehen, wie sie funktioniert, und ohne zu wissen, wer unter welchen Umständen auf unser digitales Leben zugreifen kann. Datenschutzerklärungen stehen zunehmend im Widerspruch zu Gesetzesinitiativen, die Unternehmen dazu verpflichten, Hintertüren für Geheimdienste zu öffnen. Aufsehenerregende Leaks – selbst unbestätigte – schüren das Misstrauen nur noch mehr.

Bleibt die Frage: Was tun? Heutzutage ist es fast unmöglich, komplett auf Messaging-Apps zu verzichten. Es ist jedoch möglich und notwendig, eine Plattform mit Bedacht auszuwählen, die Datenschutzrichtlinien sorgfältig zu prüfen, den Unterschied zwischen „Verschlüsselung während der Übertragung“ und „Ende-zu-Ende-Verschlüsselung“ zu verstehen und die Datenschutzeinstellungen regelmäßig zu aktualisieren.

Sicherheit liegt nicht nur in der Verantwortung der Entwickler, sondern auch in der Verantwortung jedes einzelnen Nutzers. Es ist an der Zeit, blindes Vertrauen hinter sich zu lassen und Technologie bewusst zu nutzen, ohne Komfort auf Kosten der Privatsphäre zu erkaufen. Nur so können wir Risiken, wenn nicht eliminieren, so doch zumindest minimieren und Schwachstellen in beherrschbare Bedrohungen verwandeln.

** in Russland als extremistisch anerkannt und verboten*