ما هي تطبيقات المراسلة الأكثر أمانًا؟.. هذه الخمسة أفضلها على الإطلاق

السبت 31 يناير 2026 08:00 م

توفّر تطبيقات المراسلة الوقت وتُسهّل التواصل، لكن البعض يخشى من إمكانية التعرض للاختراق، أو التجسس، حيث يمكن للهاكرز اختراق بعضها، مما يثير المخاوف بشأن أمان المحادثات، ويطرح التساؤل حول أكثرها أمانًا.

أكثر تطبيقات المراسلة أمانًا

تتمتع بعض التطبيقات بسمعة ممتازة في التصدي لعمليات الاختراق. ومن بين الأمور التي يجب البحث عنها: التشفير التام بين الطرفين، والمصادقة الثنائية لتسجيل الدخول، والبرمجيات مفتوحة المصدر، التي تخضع لمراقبة جهات متعددة وتعمل على تأمينها.

ومع أنّه لا يوجد نظام رقمي مضمون بنسبة 100 بالمائة، إلا أن اختيار إحدى هذه المنصات لإجراء المراسلات سيقلل من احتمالية تعرضك للاختراق، حيث يمكنك التحدث عن بياناتك الحساسة دون خوف من تنصت أحدهم عليك.

1. سيجنال

يُسوّق تطبيق سيجنال نفسه على أنه تطبيق "التحدث بحرية"، وقد أشاد به إدوارد سنودن كواحد من أكثر تطبيقات المراسلة أمانًا. إذ لا يستطيع مطورو التطبيق قراءة رسائلك أو التنصت عليها، ويعمل على منع الآخرين من فعل ذلك.

وتوفر هذه المنصة ميزة الدردشة الجماعية. ويضمن التشفير أن الرسائل النصية القصيرة لا يمكن رؤيتها إلا من قِبل الأشخاص الذين توافق عليهم. وهي متوافقة مع نظامي آي أو إس وأندرويد، واستخدامها مجاني.

2. فايبر

يملك تطبيق فايبر الذي شركة راكوتين، ويضم حوالي مليار مستخدم نشط شهريًا. سيتم تشفير جميع أجهزتك، بالإضافة إلى ميزة ترميز المحادثات بالألوان لتتمكن من معرفة مدى أمانها.

من مميزات فايبر الرائعة خاصية التدمير الذاتي، حيث يمكنك إجراء محادثات سرية للغاية دون القلق بشأن أي آثار متبقية على جهازك. مع ذلك، فإن المحادثاتهالجماعية أكثر عرضة للاختراق، لذا يُنصح بالالتزام بالمحادثات الفردية.

3. كليك

إذا كنت لا تمانع في دفع مبلغ بسيط مقابل خدمة مراسلة، فإن كليك من زوهو خيار ممتاز. يمكنك حتى تحديد عناوين IP التي يمكنها الوصول إلى المحادثة وحظر عناوين أخرى.

ما يميز هذه المنصة هو قدرتها على استخدام الذكاء الاصطناعي وإنشاء روبوت محادثة.

4. برايفت

كما هو الحال مع تطبيقات المراسلة الأخرى، يقوم تطبيق برايفت بتشفير الرسائل المرسلة لمنع اعتراضها. يُعدّ هذا البرنامج مثاليًا للفرق العاملة عن بُعد، حيث يتيح لك التواصل الصوتي، والدردشة، وإرسال رسائل الفيديو. وهو متوافق مع أجهزة أندرويد وآي أو إس.

ويعمل البرنامج على تشفير الاتصالات، ولا يتم الاحتفاظ بأي سجلات، وحتى لو تمكن الهاكرز من اختراق خوادم برايفت، فلن يتمكن من الحصول على معلوماتك الشخصية. تتوفر أربع باقات أسعار، تبدأ مجانية وتزداد تكلفتها حسب عدد المستخدمين.

5. مايكروسوفت تيمز

عندما تُناقش بيانات حساسة في المحاكم أو عبر القنوات التعليمية، غالبًا ما تجد قسم تكنولوجيا المعلومات يلجأ إلى "مايكروسوفت تيمز" كأحد أفضل الحلول المتاحة، حيث يحتفظ بسجل آمن للمحادثات.

ويمكنك استخدام تيمز مجانًا لجلسات تصل مدتها إلى 60 دقيقة مع 100 شخص أو أقل. ستحصل على 5 جيجابايت من مساحة التخزين لكل مستخدم، بالإضافة إلى دردشة غير محدودة، ومشاركة ملفات، ومهام. يتم تشفير البيانات. إذا كنت ترغب في مساحة تخزين أكبر، أو مدة اجتماعات أطول، أو عدد أكبر من المشاركين، فإن هناك ترقيات تبدأ من 4 دولارات لكل مستخدم شهريًا.

تجنب هذه التطبيقات

واجهت بعض شركات تطبيقات المراسلة مشاكل مع الهاكرز، لذا يُنصح بتجنب هذه التطبيقات حاليًا.

1. واتساب

إضافةً إلى تعريض أكثر من مليار مستخدم للاختراق، اكتسب واتساب سمعةً سيئةً بسبب تسريب البيانات الشخصية. ومع إعلان المنصة قبل سنوات عن نيتها نقل البيانات إلى فيسبوك، غادر المنصة العديد من المستخدمين إلى تطبيق آخر. وشهد تطبيق سيجنال زيادةً هائلة في عدد المستخدمين الجدد بلغت 4200 بالمائة في الأسبوع الذي تلى إعلان واتساب.

2. فيسبوك ماسنجر

يُعرف تطبيق ماسنجر بسماحه بنقل الفيروسات والرسائل من مرسلي الرسائل المزعجة والهاكرز. وعلى الرغم من أن الكثيرين يستخدمون ماسنجر للمحادثات الشخصية، فمن الحكمة تجنب أي شيء شديد الحساسية وعدم استخدامه لأغراض العمل.

لا يمكنك أبدًا معرفة من قد يتمكن من الوصول إلى ملفك الشخصي على فيسبوك، لذا من الأفضل إبقاء جميع المحادثات باستثناء المحادثات العادية جدًا بعيدة عن المنصة.

3. تيليجرام

تطبيق تيليجرام هو تطبيق مراسلة آخر يتعرض لانتقادات متكررة بسبب تسريب بيانات العملاء. فقد تمكن المخترقون من الوصول إلى بيانات العملاء برسالة نصية واحدة إلى الضحية الإلكترونية. ولم يقتصر تيليجرام على تسريب معلومات العملاء فحسب، بل شمل أيضًا أي شخص في قائمة جهات اتصال الضحية.

وإحدى مشاكل تطبيق تيليجرام هي طريقة تعامله مع التشفير. فهو يستخدم بروتوكولاً مغلقًا، لكنه لا يستخدمه إلا أثناء الإرسال وليس أثناء معالجة البيانات، مما يجعله عرضة للثغرات الأمنية في تخزين البيانات، وإطار عمل واجهة المستخدم، ومحادثات المجموعات.

يمكن اختراق أي تطبيق

على الرغم من أن بعض تطبيقات المراسلة توفر حماية أكبر من غيرها، لكن أي اتصال رقمي قابل للاختراق. لذا، من الأفضل الاحتفاظ بالمعلومات الحساسة للغاية للاجتماعات المباشرة فقط. وعليك أن تبذل قصارى جهدك لحماية المعلومات الشخصية وأسرار بشكل بالغ.