احذروا الوقوع بالمخاطر.. كيف يمكن تناقل المعلومات الحساسة عبر الإنترنت بشكل آمن؟

تطبيقات مراسلة مشفرة وموثوقة ينصح بها خبراء الأمن الرقمي

بات الحفاظ على خصوصية البيانات المرسلة عبر الإنترنت أمراً يشغل بال المستخدمين أكثر من أي وقت مضى، نظراً لتزايد الرقابة على المحتوى سواء من قبل حكومات دول العالم أو الشركات التي تجمع هذه البيانات بغرض بيعها إلى أطراف ثالثة لاستخدامها في أغراض البحث أو عرض إعلانات منسجمة مع اهتمامات المستخدمين أو توجيههم لاتخاذ آراء معينة، وهو الأمر الذي زاد المخاوف من تعرض المعلومات الشخصية والمكالمات والرسائل والصور للتجسس، ما دعا الشركات لإطلاق ميزات تضمن الخصوصية في تطبيقات المراسلة، من خلال إتاحة خدمات تشفير شاملة.

يتم التشفير بين طرفين عندما لا يحتفظ مزود الخدمة بنسخ من الرسائل التي يتم إرسالها على خوادمه، أي أن الشخص المرسَل له هو وحده من يتمكن من الوصول إلى الرسالة، ويتعذر ذلك على الحكومات أو المطورين أو أي طرف ثالث.

تزداد أهمية استخدام تطبيقات تراسل آمنة من قبل الناشطين والعاملين في مجالات الصحافة وحقوق الإنسان خاصة في فترات الحروب والنزاعات، إذ يكونون بأمس الحاجة للتعامل بوسائل لا تعرضهم لخطر كشف المعلومات والأسرار التي يتداولونها.

وينصح خبراء الأمن الرقمي بمجموعة من تطبيقات المراسلة المشفرة التي توفر درجات مقبولة من الأمان لبيانات المستخدمين، كما يحذرون من أخرى يسهل اختراقها.

1. **تلغرام Telegram**: يوفر هذا التطبيق أعلى درجات الحماية لمستخدميه على الإطلاق، إذ يمكّنهم من إجراء مراسلات سرية وعالية التشفير للصور والفيديوهات وجميع أنواع المستندات، ويمكن للرسائل أن تُدمّر ذاتها تلقائياً بعد فترة معينة، كما يُتاح تعيين خيار التدمير الذاتي للحساب في غضون زمن محدد.

ويعد مركز البيانات الذي يستقبل ويحتفظ بالرسائل في هذا التطبيق محجوب كلياً عن الحكومات، كما أنه يعمل بنظام متطور لمنع قرصنته.
وتعدّ جودة الاتصال الصوتي عبر "التلغرام" من داخل سوريا جيدة، مقارنة مع بقية برامج التراسل التي يشكوا بعض مستخدميها من رداءة الاتصال.
وهو تطبيق مجاني وسريع ومفتوح المصدر ومتعدد المنصات، ويمكّن من مزامنة رسائل المستخدم بسهولة عبر أجهزة مختلفة مرة واحدة.
يمكن تثبيته على Android و IOS

2. **سيغنال Signal**: وهو أحد أكثر التطبيقات أمناً من ناحية الخصوصية والحفاظ على سرية بيانات المستخدمين، ويمكن من خلاله إجراء مكالمات صوتية مشفرة للغاية، ومحادثات جماعية، وإرسال الصور والفيديوهات بسهولة وأمان، كما يمكن للرسائل التدمير الذاتي بعد فترة زمنية محددة.

وإضافة لذلك يمتاز البرنامج بأنه مجاني ومفتوح المصدر وسريع الأداء، ولا تحفظ الجهة المطورة رسائل أو صور وفيديوهات المستخدمين المرسلة والمستقبلة حتى لا تتعرض للاختراق بأي حال.
يمكن تنزيله على Android و IOS

3. **واتس آب WhatsApp**: من أكثر التطبيقات شعبية، ففي شهر نيسان/أبريل من عام 2016، أعلنت الشركة المطورة أن جميع المحادثات أصبحت مُشفرة تماماً، سواء كانت بين مستخدمَين، أو بين مجموعة[1]، وتضمن تقنية التشفير الخاصة بالتطبيق عدم تمكن أي جهة حتى الشركة نفسها من الاطلاع على الرسائل، لأن مفاتيح فك التشفير موجودة فقط على أجهزة المرسل والمستقبل.

[1] "WhatsApp's Signal Protocol integration is now complete". April 5, 2016. Last visited February 8, 2020. https://signal.org/blog/whatsapp-complete/.

لكن لا بد من الإشارة إلى أنه ووفقاً لسياسة الخصوصية تقوم الشركة بتسجيل رقم المرسل والمرسَل إليه ووقت إرسال الرسالة، وتحتفظ بهذا السجل في حال ورود أي طلب من جهات حكومية، لكن دون أن تحتفظ بمحتوى الرسالة.

ويتيح التطبيق القدرة على إرسال الصور ومقاطع الفيديو والرسائل الصوتية ومكالمات الفيديو إضافة لمحادثات المجموعة ومشاركة الموقع.

التطبيق مجاني وبسيط وسهل الاستخدام ويمكّن من إرسال واستقبال الرسائل من متصفح جهاز الحاسوب الخاص بالمستخدم.

يمكن تثبيته على **Android** و**IOS**

○ تشفير رسائل البريد الإلكتروني:

يوفر البريد الإلكتروني المشفّر القدرة على تشفير جسم ومرفقات الرسائل الإلكترونية، ويوجد العديد من البرامج التي تعمل على تشفير رسائل البريد الإلكتروني، الأمر الذي يقي من مخاطر كشف مضمونها أو حتى معرفة صيغة مرفقاتها الحقيقية.

ومن هذه البرامج:

- **برنامج تشفير الرسائل** Kleopatra

وهو برنامج مجاني مفتوح المصدر، يمكّن المستخدمين من نقل رسائل البريد الإلكتروني والملفات بشكل آمن مع مساعدة من التشفير والتوقيع الرقمي.[2]

○ احذروا تطبيق إيمو "IMO":

يحذر خبراء الأمن الرقمي من استخدام تطبيق "إيمو" للمراسلات بشكل عام، خاصة في سوريا، وذلك لكونه غير مشفر، إذ لا يقدم التطبيق التشفير المطلوب لأي نوع من البيانات المرسلة والمستقبلة، كما أنه يتبادل البيانات الشخصية مع شركات أخرى مثل "غوغل، تويتر، فيس بوك"، ويتضمن إعلانات لموقع طرف ثالث.[3]

لذا يُعتبر برنامج "تلغرام" بديلاً آمناً ومناسباً للمكالمات الصوتية داخل سوريا.

- **عيوب التطبيق:**

لا يؤمّن التطبيق حماية لخصوصية المستخدمين لعدم وجود ميزة التشفير بين طرفين، وهو ما يجعل إمكانية التجسس على المكالمات والمحادثات من قبل الحكومات أو المخترقين أو الشركة نفسها كبيرة جداً، كما أنه تطبيق مغلق المصدر وعلى عكس البرنامج مفتوح المصدر لا يمكن للمطورين الوصول لـ "الكود" الخاص به ومعرفة جميع تفاصيله.

---

[2] "خطوات عملية في الحماية الرقمية". سوريون من أجل الحقيقة والعدالة. 18 تشرين الثاني/نوفمبر 2018. (آخر زيارة للرابط: 11 شباط/فبراير 2020). https://stj-sy.org/ar/1029/.

[3] "مميزات وعيوب برنامج ايمو". 26 كانون الثاني/يناير 2020. (آخر زيارة للرابط: 11 شباط/فبرير 2020). http://bit.ly/2UImhGD.

وعلاوة على ذلك فإن سياسة الخصوصية تُشير بشكل صريح إلى أن أذونات التطبيق تُتيح الوصول إلى دفتر العناوين وسجل الاتصالات وأيضاً لمعلومات تفصيلية عن نوع الجهاز، وشريحة الـ (SIM)، ومشاركة هذه المعلومات مع أطراف ثالثة.

ويُضاف إلى ذلك أن احتفاظ خادم التطبيق ببيانات المستخدمين يدوم لمدة 90 يوماً وهو ما يعني أن جميع المكالمات والمحادثات والصور والفيديوهات ستكون عرضة للاستخدام في عمليات البحث والتحليل وغيرها.

- **نصائح للمستخدمين قبل تنزيل أي تطبيق للمزيد من الأمان:**

1. تحميل التطبيقات من المنصات الموثوقة مثل "Google play" و"Apple store"، إذ قد تتسبب التطبيقات التي يتم تثبيتها من مواقع غير رسمية بالوقوع في فخ البرمجيات الخبيثة وبرامج التجسس وغيرها.
2. التأكد من هوية منتِج التطبيق وسمعته، والبحث عن وجود علامة زرقاء بجانب اسمه تُعطى عادة للمطورين الموثوقين.
3. إلقاء نظرة على آراء وتقييمات المستخدمين خاصة المتعلقة منها بموضوعي الخصوصية والأمان.
4. التحقق من الأذونات التي يطلبها التطبيق عند تحميله، وما إذا كان من المنطقي طلبها، والامتناع عن تحميل التطبيقات التي تطلب أذونات قد تشكل مصدراً للخطورة على الخصوصية.[4]
5. حذف التطبيقات غير المستخدمة بشكل دوري.
6. التحديث المستمر للأجهزة قبل تحميل أي تطبيق لحماية البيانات من الفيروسات.[5]

[4] " تحذير! يتم تداول تطبيق مراسلة مزيّف في الشّمال السوري عبر واتس آب و تيليغرام، يجب عدم تنصيب التطبيق!". مشروع سلامتك. 23 تشرين الأول/اكتوبر 2019. (آخر زيارة للرابط: 11 شباط/فبراير 2020). http://bit.ly/39oT47I.

[5] "خطوات عملية في الحماية الرقمية". سوريون من أجل الحقيقة والعدالة. 18 تشرين الثاني/نوفمبر 2018. (آخر زيارة للرابط: 11 شباط/فبراير 2020). https://stj-sy.org/ar/1029/.