هاتفك المحمول صندوق أسرارك واختراقه يعرضك للخطر !

هناك من يتجسس عليك دون علمك.. كيف تتفادى التعقب؟

ميزاتٌ كثيرةٌ تؤمنها هواتفنا المحمولة يُقابلها مخاطر على حياتنا وبياناتنا يمكن تجنبها أو التقليل منها من خلال اتباع خطوات عملية تُبعد عنا إمكانية تعقب موقعنا الجغرافي، أو التجسس عبر ميكروفون الهاتف أو التطبيقات التي نثبتها عليه، يأتي في مقدمتها الانتباه للأذونات التي تطلبها تلك التطبيقات، والتحديث المستمر لها ولنظام التشغيل، واستخدام برامج الحماية من الفيروسات، وتشفير الاتصال بالإنترنت عند الحاجة، خاصّة عند استخدام شبكات عامّة.

سهّلت الهواتف الذكية حياتنا وأتاحت أمامنا ميزات لا تُحصى مكّنتنا من الاستغناء عن الكثير من الأجهزة الأخرى، خاصة مع توفر خدمة الاتصال بالإنترنت وإمكانية تحميل تطبيقات لاستخدامات مختلفة كالتواصل الاجتماعي والتعليم وتسيير المعاملات البنكية وغيرها.

لكننا وأمام كل هذه الميزات، بتنا للاختراق بشكل كبير، ومع الكَمّ الهائل من المعلومات والبيانات التي تحفظها أجهزتنا عنا أصبح اختراقها كافياً للتسبب بالكثير من الضرر، خاصة في ظل وجود أنظمة ديكتاتورية وبوليسية

تتعقب كل من يحاول الخروج عن قبضتها الأمنية، وشركات تجارية تدفع مبالغ طائلة لتجميع أكبر قدر ممكن من المعلومات عن المستخدمين لتوظيفها في أعمالها.

ولأن أماننا وخصوصيتنا باتا على المحك، أصبح لزاماً علينا التعرف على طرق اختراق هواتفنا المحمولة واتخاذ الإجراءات المناسبة لتوفير الحماية لها، حتى لا ندفع ثمنًا باهظًا مقابل الميزات التي نحصل عليها منها.

○ ما هي المعلومات التي يمكن أن يكشفها عنك هاتفك المحمول في حال اختراقه؟

- ❖ معرفة المكالمات الصادرة والواردة وإمكانية التنصت عليها، إضافة إلى التعرف على الرسائل النصية المرسلة والمستقبلة.
- ❖ إمكانية الوصول إلى البيانات المخزنة بالجهاز مثل أرقام هواتف الأشخاص وعناوينهم، والملفات النصية، والصور ومقاطع الفيديو.
- ❖ مراقبة المواقع التي يتم تصفحها عبر الإنترنت، والبريد الإلكتروني، والخدمات المستخدمة عبر الهاتف.
- ❖ الوصول إلى معلومات شخصية عن المستخدم بما في ذلك تاريخ ميلاده، ومكان تواجده، وعمله، وهواياته، وحسابه المصرفي، ودوائر الاتصال الخاصة به.
- ❖ القدرة على اكتشاف رقم "PIN" الأمني الخاص بالمستخدم وكلمات المرور.
- ❖ معرفة نوع الجهاز المستخدم ومواصفاته.
- ❖ إمكانية زرع برامج تعقّب على الجهاز يمكنها التحكم فيه، وتشغيل بعض الخدمات دون معرفته، وإرسال بيانات مخزنة عليه، وأخذ صور للمستخدم وتسجيل صوته في البيئة المحيطة، كما يمكن توريط المستخدم بعمليات نصب واحتيال.

○ كيف يمكن تعقّب موقعك الجغرافي؟

- ✓ عبر النظام العالمي لتحديد المواقع "GPS" اختصار لـ"Global Positioning System": وهي أكثر الطرق دقة في تحديد مكان المستخدم، وتعتمد على استخدام موجات الراديو بين الأقمار الصناعية وجهاز الاستقبال داخل الهاتف وتصل دقتها إلى خمسة أمتار.
- ✓ من خلال معلومات عن موقع المستخدم تم الحصول عليها من بياناته الأخرى كالصور والرسائل القصيرة وطلبات الإنترنت التي يرسلها الهاتف.
- ✓ عن طريق إدخال المستخدم لمعلومات مكان تواجده "اسم الدولة أو المدينة أو الرقم البريدي" بناء على طلب بعض المواقع الإلكترونية التي تقدم خدمات تعتمد على عنوان المستخدم.
- ✓ عنوان الـ IP الخاص بالمستخدم: ومن خلاله يمكن تحديد الدولة أو المدينة التي يتواجد فيها.

- ✓ شبكات الـ "Wireless" أو الـ "Routers" المحيطة بالمستخدم: تمكن من معرفة مكان المستخدم حتى في حال كونه غير متصل بالإنترنت، أو كان جهازه دون شريحة.
- ✓ أبراج شركات الاتصالات: يمكن تحديد مكان المستخدم من خلال معرفة عدد أبراج الاتصالات التي تحيط به، وذلك حتى لو كان الجهاز دون شريحة ما دام به بطارية تعمل.[1]

○ ميكروفون هاتفك يتجسس عليك

يمكن للشخص أو الجهة المخترقة أن تعرف الكثير عن محادثات المستخدم ونشاطاته، من خلال سماع كل ما يقوله بواسطة ميكروفون هاتفه.

وفي الوقت الذي تُنكر الشركات استخدامها البيانات التي يتم جمعها من أصوات المستخدمين أو مشاركتها مع أطراف ثالثة، تبرز تساؤلات عن الآلية التي يتم من خلالها ظهور أحد الإعلانات المرتبطة بنشاط معين بمجرد حديثنا عنه مع أحد الأشخاص، فعلى سبيل المثال: عقب الحديث عن نيتنا السفر إلى وجهة معينة يبدأ ظهور إعلانات تتعلق بتلك الوجهة كالفنادق والمطاعم المتواجدة فيها وحجوزات الطيران وغيرها.

- **كيف يمكن تقليل احتمال هذا النوع من التجسس؟**

- ✓ تجنب التحدث عن الأمور الهامة بالقرب من الهاتف.
- ✓ الحذر من أذونات التطبيقات: بعض التطبيقات تتمكن من الحصول على أذونات لا تتوافق مع نشاطاتها، ولذلك يتوجب عند ملاحظة وجود تطبيق لا يحق له الوصول إلى الميكروفون، إزالة هذا الإذن والنظر في إمكانية مسح التطبيق من الهاتف خشية أن يكون ضاراً.

○ مخاطر التطبيقات

تطلب معظم التطبيقات الإذن للاستفادة من كميات كبيرة من بيانات المستخدم، كما أن بعض التطبيقات تحاول الوصول إلى البيانات التي لا علاقة لها بوظائفها، وهناك العديد من التطبيقات التي تقوم بجمع بيانات المستخدم على الرغم من تقييد الوصول إلى هذه البيانات.

ونقلت صحيفة "نيويورك تايمز" الأمريكية عن أحد المتمرسين في صناعة الإعلانات على الإنترنت قوله إنه من المحتمل أن يقوم تطبيق معين بتسريب البيانات إلى خمسة أو عشرة تطبيقات أخرى لمعرفة المزيد عن المستخدم، ومن شأن ذلك أن يحول أي تطبيق إلى أداة حاصدة للبيانات.

ومن هنا يتعين على المستخدم توخي الحذر عند تثبيت التطبيقات وأن يعمد إلى تنزيلها من مصادر موثوقة.

[1] "دليل الحماية لأجهزة الهاتف"، موقع البوصلة. 28 تموز/يوليو 2019. (آخر زيارة للرابط: 7 شباط/فبراير 2020). https://albosla.net/2704.

○ نصائح عملية لمنع التجسس على الهاتف المحمول أو اختراقه

1. تحديث نظام التشغيل والتطبيقات المُنصّبة على الهاتف بشكل دوري.
2. استخدام برامج الحماية من الفيروسات والبرمجيات الخبيثة.
3. استخدام التطبيقات التي توفر خدمة التعمية الكاملة لجميع المحادثات الصوتية والنصية مثل "WhatsApp,Signal".
4. استخدام "VPN" (الشبكة الخاصة الافتراضية) لتشفير الاتصال بالإنترنت عند الحاجة، وإغلاق الاتصال بالإنترنت في حال عدم الحاجة إليه.
5. استخدام غطاء لكاميرا الهاتف.

www.stj-sy.org
Syrians for Truth & Justice
editor@stj-sy.org
@STJ_SYRIA_ENG
syriaSTJ