هذه هي التنازلات التي تقدمها عند تنزيل تطبيق على هاتفك

ترجمة وتحرير نون بوست

هل عثرت على تطبيق أثار اهتمامك وقمت بتحميله على هاتفك، ولكن نظام الأندرويد أعلمك بأن هذا التطبيق يطلب الإذن للولوج إلى معلومات حساسة في الهاتف؟ هل نقوم فعلا بالتثبت من طلبات الإذن التي تعرضها علينا هذه التطبيقات قبل الضغط على زر الموافقة؟ وهل نهتم فعلا بما يقف وراء كل عملية تحميل للتطبيق؟

وفقا لتقرير جديد أصدرته شركة مخابر "كاسبرسكي" للسلامة المعلوماتية، فإن 47 بالمائة فقط من مستخدمي الهواتف الذكية يهتمون فعلا بتأثير هذه التطبيقات على هواتفهم، في حين أن 24 بالمائة منهم يمتنعون عن تحميل التطبيق إذا طلب منهم الإذن للولوج إلى معلومات شخصية يعتبرونها حساسة ولا يمكن المخاطرة بالكشف عنها.

بالإضافة إلى ذلك، أظهر هذا التقرير المنشور أن حوالي 83 بالمائة من هذه التطبيقات التي نقوم بتحميلها على هواتفنا الجوالة تقوم بالولوج إلى معلوماتنا الشخصية والحساسة على غرار أرقام الهواتف وأسماء الأشخاص، وسجلّ المكالمات التي قمنا بها فضلا عن الرسائل التي تبادلناها. وقد يصل الأمر إلى حد تحكمها في بعض إعدادات ضبط الهاتف على غرار أوقات غلقه وتشغيله، ومعلومات الاتصال بشبكة الإنترنت، ونظام تشغيل الهاتف بأكمله.

على الرغم من الغموض الذي لطالما لف سوق تطبيقات الأندرويد في العالم، فإن هناك نظام مراقبة ناجع يمكنه إما تنظيم عملية منح الإذن للتطبيقات أو القيام بعزلها ومنعها من الحصول على البيانات الحساسة

من جهتها، قامت مخابر "كاسبرسكي" للسلامة المعلوماتية بإجراء تجربة، تم خلالها تنزيل 66 من التطبيقات الأكثر شعبية بين مستخدمي نظام أندرويد، وتثبيتها على عدد من أجهزة الهواتف الذكية. وقد كانت النتيجة أن 54 من هذه التطبيقات كانت تعمل من تلقاء نفسها وتستهلك حوالي 22 ميغابايت من وحدات الإنترنت كل يوم، دون أن يفتحها المستخدم أو يكون على علم بذلك.

وعلى الرغم من الغموض الذي لطالما لف سوق تطبيقات الأندرويد في العالم، فإن هناك نظام مراقبة ناجع يمكنه إما تنظيم عملية منح الإذن للتطبيقات أو القيام بعزلها ومنعها من الحصول على البيانات الحساسة. وتجدر الإشارة إلى أنه يوجد دليل استخدام لنظام أندرويد لتشغيل الهواتف الجوالة، يحتوي على معلومات ونصائح عديدة، متعلقة بأنواع الأذون التي يتم منحها للتطبيقات عند تنزيلها، إلا أن الخبراء يحذرون من تسعة تطبيقات من شأنها أن تشكل خطورة كبيرة على الهواتف والأسرار. وبالتالي، يجب التعامل معها بحذر شديد، بما أنها تستهدف بشكل خاص ومباشر خصوصياتنا وأمن هواتفنا.

هذه أكثر المعلومات حساسية في هاتفك:

1-المفكرة:

تمكنك المفكرة من التعرف على التقويم أو التاريخ، وإدخال تغييرات على غرار إنشاء حدث جديد وحفظه للمستقبل. ويكمن الخطر هنا في أن التطبيقات الخبيثة التي تنزلها على هاتفك قد تغير من موعد مهم سجلته في المفكرة أو تقوم بمحوه تماما. بالإضافة إلى ذلك، قد تُستخدم للتجسس على صاحب الهاتف ومعرفة موعد لقاء أو نشاط معين سيقوم به.

2- قائمة الأسماء:

عندما يطلب منك تطبيق جديد الإذن بالدخول لقائمة الأسماء والأرقام في هاتفك وإدخال تغييرات عليها، فإنه يمكنه بعد ذلك إضافة أسماء جديدة والإطلاع على كل الأسرار حتى تلك المتعلقة بحسابات بنكية أو بخدمات أخرى تقوم بالحصول عليها عبر الهاتف. ومن الواضح أن ذلك يعدّ بمثابة الحيلة المفضلة بالنسبة للمتحيّلين الذين يتخذوم من سرقة معلومات الآخرين والتحيّل عليهم مورد رزق، حيث يمكنهم الولوج لحساباتنا في غفلة منا والقيام بأشياء مخالفة للقانون.

3- الكاميرا:

أحيانا نسمح لإحدى التطبيقات بالولوج لجهاز الكاميرا والتقاط الصور أو تسجيل مقاطع الفيديو من تلقاء نفسها، وهو ما يعد اعتداءً صارخا على خصوصيتنا، مما قد يسبب لنا مشاكل كبيرة في حال كان هذا التطبيق تحت تصرف أشخاص لا يضمرون نوايا طيبة.

صورة لوحة التحكم في تطبيقات الأندرويد

4- شريحة التخزين أو الذاكرة:

سواء يتم تخزين المعلومات في مساحة خارج الهاتف على غرار شريحة الذاكرة الرقمية الآمنة "SD card"، أو يتم تخزينها داخل نظام الهاتف نفسه، فإنه عندما يقوم تطبيق غريب بقراءة معلوماتك فإن الخطر يكمن في إمكانية قيامه بجمع المعلومات الحساسة ونسخها أو تدميرها وهو ما قد يسبب لنا مشاكل عديدة.

5- الميكروفون:

من خلال السماح لتطبيق جديد بالدخول إلى جهاز الميكروفون، فإننا نعرض أنفسنا لخطر التجسس على مكالماتنا وتسجيل المحادثات التي نجريها مع الأشخاص بينما يكون الهاتف موجودا في جيبنا.

6- الرسائل المكتوبة:

يعدّ السماح للتطبيقات بإرسال رسالة مكتوبة وقراءة أرشيف المحادثات بمثابة خطر كبير. لذلك، يجب الانتباه لهذه النقطة عند تحميل تطبيق جديد، لأن مجرمي الإنترنت يستعملون هذه الخاصية بالذات بهدف شراء أشياء من الإنترنت باستخدام حساب صاحب هذا الهاتف.

7- المجسات الموجودة في الهاتف:

يؤدي السماح بالإطلاع على عمل هذه المجسات التي تراقب جسم الإنسان وحركته، إلى الوصول إلى معلومات تُعتبر شخصية تقوم بعض الهواتف المتطورة بالتعرف عليها بشأن الحالة الصحية للمستخدم على غرار دقات القلب.

8- جهاز تحديد الأماكن:

إذا سمحنا لتطبيق معين بالتعرف على أماكن تواجدنا طوال الوقت، سواء عبر جهاز تحديد المواقع "GPS" أو خدمة عبر الإنترنت، فإنه يمكن لبعض المجرمين استخدام ذلك بهدف تحديد أماكن تواجدنا، واستغلال غيابنا عن البيت للقيام باقتحامه. علاوة على ذلك، يمكن لبعض الشركات إزعاجنا عن طريق إرسال دعايات ورسائل غير مرغوب فيها، على غرار تقييم الخدمة وجودة الطعام في مطعم كنا بصدد تناول العشاء فيه.

9- المكالمات:

يكمن الخطر هنا في أن التطبيق سوف يكون على إطلاع على جلّ المعلومات الصوتية التي مرّت عبر جهاز الهاتف المخترق

في حال تمّ اختراق نظام المكالمات الهاتفية، فإنه من الممكن معرفة نوعية الجهاز ورقم هاتف المستخدم والشبكة التي يستعملها. كما يمكن للمخترق إجراء مكالمات ومعرفة تاريخ المكالمات التي تم القيام بها في السابق، فضلا عن إضافة رسائل بريد صوتي وحتى التلاعب بالمكالمات الهاتفية الواردة على الجهاز أو إعادة توجيه بعضها نحو رقم آخر.

في الحقيقة، يكمن الخطر هنا في أن التطبيق سوف يكون على إطلاع على جلّ المعلومات الصوتية التي مرّت عبر جهاز الهاتف المخترق، وبالتالي استغلال ذلك لسرقة المعلومات أو الأموال. لذلك، ينصح الخبراء بالتعامل بحذر شديد والانتباه لكل التفاصيل عند تنزيل تطبيق جديد يطلب منا إذنا إضافيا للقيام بعملية خاصة، حيث أن ذلك يكون عادة تمهيدا لنشر فيروسات أو برمجيات خبيثة على هاتفنا.

تنظيم مسألة منح الإذن

يمكن التحكم في بعض التطبيقات من خلال لوحة الإعدادات على غرار تلك المتعلقة بالخيارات التي يتم ضبطها مسبقا للتعامل مع طلبات الإذن

يشغّل نظام أندرويد هواتفنا ويسمح لنا بالتعامل مع كل المحاولات الخطيرة التي تهدف لاختراق الجهاز. والجدير بالذكر أن هناك بعض التفاصيل التي تختلف من نظام محمول إلى آخر، ولكن يكفي في الغالب أن تدخل إلى صفحة الإعدادات ومنها إلى صفحة التطبيقات ثم الخيارات المتطورة، وهناك يمكن العثور على هذه الخيارات المتاحة أمامنا لحماية أنفسنا. فعند الدخول لأي تطبيق موجود على هاتفنا، يمكننا معرفة ما إذا كان يتمتع بإذن للإطلاع على بياناتنا الشخصية أو يكون من النوع الذي ينشط بشكل غير مرئي.

في المقابل، يطلب نظام "أندرويد 6" والنسخ التي جاءت بعده الإذن من صاحب الهاتف قبل إدخال أي تغييرات عليه، ويمكننا تفعيل أو تعطيل هذه الخاصية بشكل مباشر من خلال لوحة التحكم في

التطبيقات، وتعديل خيارات الضبط بالشكل الذي نريده.

من جهة أخرى، يمكن التحكم في بعض التطبيقات من خلال لوحة الإعدادات على غرار تلك المتعلقة بالخيارات التي يتم ضبطها مسبقًا للتعامل مع طلبات الإذن، مثل تحديد التطبيق التي سيقوم ببعث الرسائل والبريد الإلكتروني، والذي يقوم بفتح الصور المخزنة على الهاتف، أو الذي نعتمد عليه لتشغيل الموسيقى، أو المتصفح الذي نختاره لاستعمال الإنترنت.

كما أنه من الجلي أننا نحتاج للتعامل بحذر مع هذه التفاصيل ولا نترك لهذه التطبيقات المجال لتحدد هي لنفسها الصلاحيات التي تتمتع بها، نظرا لأننا في حال وقعنا في فخ برمجية خبيثة فإنها قد تسرق منا كلمات السر وتقوم بإرسال رسائل من هواتفنا دون علمنا.

علاوة على ذلك، يمكننا من خلال ضبط إعدادات التطبيقات، التحكم في عملية تراكم التطبيقات على شاشة الهاتف. بمعنى أننا لا نسمح لها بالظهور على الشاشة بالتزامن مع تطبيقات أخرى. وهو ما يعد أمرا بالغ الأهمية نظرا لأننا قد نتعرض أحيانا لعملية قرصنة تقوم خلالها إحدى البرمجيات الخبيثة بفتح صفحة مشابهة لصفحة فيسبوك أو مشابهة لموقع حسابنا البنكي. في هذه الحالة، نقع في الفخ ونقوم بإدخال اسم المستخدم وكلمة السر مما يجعلنا ضحية عملية تلاعب خطيرة.

يجبرنا استعمالنا للهاتف الذكي على البقاء في حالة يقظة طوال الوقت، إذا ما كنا نريد أن تسير الأمور كما نشاء كي لا نضطر لتغيير الهاتف بعد فترة أو نتعرض لعمليات احتيال

وأخيرا، يجب أن نتعامل بحذر خاص مع التطبيقات التي تمتلك الصلاحيات لتغيير إعدادات نظام تشغيل الهاتف، إذ أنه في حالة وقوعنا في فخ تطبيق خبيث، فإنه قد يتمكن من تغيير كلمات السر، أو يمنعنا من الولوج إلى حساباتنا إثر تشفيرها.

في هذا الصدد، تسمى هذه العملية في عالم القرصنة وجرائم الاحتيال الإلكترونية "بطلب الفدية في مقابل الإفراج عن البيانات"، حيث يجد صاحب الهاتف نفسه مجبرا على إرسال الأموال للشخص المحتال حتى لا يقوم هذا الأخير بمحو بياناته أو إغلاق حسابه. وقد مثلت هذه الظاهرة واحدة من أكبر المخاطر في العالم التي تنامت في مجال التكنولوجيا خلال السنوات الأخيرة، ويُنتظر أن يتنامى انتشارها في المستقبل.

من الواضح من خلال كل هذه المخاطر، أن عملية تحميل تطبيق جديد على هاتفنا تستحق منا كل الاهتمام والتدقيق. وفي حال وجود أدنى شك، يجب علينا البحث أكثر حول مصدر التطبيق وطبيعة نشاطه قبل تفعيله. ولكن تخضع هذه المسألة أيضا للتقدير المنطقي، فإذ قمت على سبيل المثال بتحميل تطبيق للبحث عن معلومات متعلقة بالسفر وحجوزات الفنادق، ثم طُلب منا الإذن لاستخدام جهاز تحديد المواقع، فإن العلاقة بين الأمرين تبدو واضحة وجليّة.

باختصار، يجبرنا استعمالنا للهاتف الذكي على البقاء في حالة يقظة طوال الوقت، إذا ما كنا نريد أن تسير الأمور كما نشاء كي لا نضطر لتغيير الهاتف بعد فترة أو نتعرض لعمليات احتيال. ولأجل ذلك، من الجيد أن نقوم بعملية مراقبة روتينية من حين لآخر، عبر تحديث التطبيقات الموجودة، وعدم تحميل أية تطبيقات من مصادر غير معروفة، فضلا عن استعمال تطبيقات لتنظيف الهاتف وتحسين أدائه ومنع إصابته بالفيروسات.

المصدر: البايس