تطبيقات تخفي جوانب مظلمة.. كيف نتجنبها؟

الفضول قد يكلفنا التضحية بمعلوماتنا الخاصة .. إليكم خطوات عملية لتوخي الحذر

خلال السنوات الأخيرة، انتشرت العديد من البرامج والتطبيقات التي تُتيح ميزات فريدة للمستخدمين/ات مقابل جمع معلومات حساسة عنهم في الخفاء، ولاقت تلك التطبيقات رواجاً كبيراً لعدم معرفة معظم المستخدمين/ات ما قد يحلّ ببياناتهم ومعلوماتهم الشخصية إذا ما تمت سرقتها ومشاركتها مع أطراف ثالثة، قد تستخدمها لأغراض تجارية في غالب الأحيان، وهو ما يُبرز الحاجة لفهم آلية عمل تلك التطبيقات، ومراقبة الأذونات التي نمنحها لها، والشروط والأحكام التي نوافق عليها عند تثبيتها على أجهزتنا المحمولة.

تبدو مسلية ويدفعنا إليها الفضول أو ربما ننساق لتقليد ما يفعله الآخرون، نجربها عن حسن نية دون أن ندري ما قد تلحقه بنا من أذى.

تطبيقاتٌ كثيرةٌ انتشرت على أجهزتنا الذكية وعلى مواقع التواصل الاجتماعي، تبدو للوهلة الأولى أنها مدعاة للتسلية والمتعة وجلب الابتسامة إلا أن خبراء في الأمن الرقمي كشفوا ثغرات من شأنها انتهاك خصوصيتنا ووضعها تحت تصرف جهات لا نستطيع التكهن بنواياها.

تجمع بعض "اختبارات تحليل الشخصية" أو "تحديد نسبة الذكاء" أو "الصراحة" أو غيرها من التطبيقات المماثلة كميات هائلة من بياناتنا الحساسة بهدف تطوير ملفات رقمية تفصيلية عنا حتى دون موافقتنا.

كيف يحدث ذلك؟

تطلب تلك التطبيقات موافقة المستخدم/ة على الوصول لبياناته/ا الشخصية، كمعرض الصور أو قائمة الاتصال أو مكان التواجد (الموقع الجغرافي)، وبمجرد أن يحصل التطبيق على تصريح بجمع هذه البيانات، يمكنه أن يتداولها مع أيّ طرف ثالث، خاصة الشركات التي تتعقب وتجمع بيانات المستخدمين مثل هويتهم وأعمارهم وأماكن سكنهم واهتماماتهم لتوظيفها في أنشطة تجارية ولأغراض الدعاية والإعلان.

عادة ما تعلن التطبيقات والبرامج أو الخدمات عن "سياسة خصوصية" المستخدم عبر نصوص طويلة جداً تحتاج وقتاً طويلاً للقراءة والاطلاع، ولذلك يوافق عليها معظم المستخدمين دون أن يكون لديهم دراية بمضمونها.

نتيجة لذلك تضع الشركات ضمن أحكام الاستخدام وشروطه أكبر عدد ممكن من الحقوق لاستخدامها عند الحاجة، حتى لو لم تكن بحاجتها في الوقت الحالي.[1]

1. تطبيق "فيس آب" - Face App"

شهد تطبيق "فيس آب" إقبالًا جنونياً من قبل مرتادي الشبكة العنكبوتية في جميع أنحاء العالم حيث أشارت إحصائيات إلى أن نحو 150 مليون مستخدم استعملوا هذا التطبيق، وسط اتهامات وُجهت لشركة "وايرلس لاب - Wireless Lab" المطورة له باختراق خصوصية مستخدميه والتجسس عليهم.[2]

[1] "حقيقة تطبيق "فيس آب" الصادمة". موقع بي بي سي عربي. 19 يوليو/تموز 2019. (آخر زيارة للرابط: 5 شباط/فبراير 2020). http://tiny.cc/mphmjz.

[2] " هل تطبيق "فيس آب" خطير حقاً؟" – موقع DW. 18 تموز/يوليو 2019. (آخر زيارة للرابط: 5 شباط/فبراير 2020). http://tiny.cc/qlhmjz.

التطبيق الذي حظي بشعبية واسعة حول العالم يُتيح تعديل ملامح المستخدم عبر إضافة المكياج أو تغيير لون الشعر، أو تحويل تعابير الوجه إلى مبتسمة أو غاضبة، كما أنه يسمح للمستخدم بتعديل جنسه أو عرقه، ورؤية صورة تقريبية عن شكله بعد تقدمه بالسن أو فيما لو كان أصغر سناً، الأمر الذي أثار فضول ملايين المستخدمين.

أ. كيف يعمل التطبيق؟

يعتمد التطبيق على تقنية "الذكاء الاصطناعي"، والتي تعرف بـ "الخلايا العصبية الاصطناعية"، وهي عبارة عن تقنيات حسابية ذكية صُممت لتحاكي الطريقة التي يؤدي بها الدماغ البشري مهمة معينة، إذ تأخذ الخوارزمية صورة وجه المستخدم الداخلية وتقوم بتعديلها وفقاً لصور أخرى، من أجل تغيير الملامح بالشكل المطلوب.

ب. ما هي أبرز عيوب التطبيق؟

يطلب التطبيق عند تعديل الصورة منحه الإذن بالوصول إلى معرض الصور بالهاتف والتحكم به، وهو ما يتيح له الوصول إلى الكاميرا، والملفات الموجودة على الهاتف، وغيرها من الأمور التي تطال خصوصية المستخدم.

ت. حقائق حول تطبيق "فيس آب"

تطبيق مجاني، يمكن تحميله على الهواتف الذكية التي تعمل بنظامي "أندرويد Android" و"آي أو إس IOS "، تعود بداية انتشاره إلى العام 2017، حين كانت تملكه شركة "Face App Inc" وعملت على تطويره شركة "Wireless Lab " الروسية التي تتخذ من مدينة "سانت بطرسبرغ" مقراً لها.

تزامن انتشار التطبيق مع تحذيرات من قبل خبراء الأمن الرقمي من انتهاكه لخصوصية المستخدمين، خاصة وأنه يمكنه النفاذ إلى معرض الصور في الهاتف وتحميلها على خوادم الشركة دون أخذ إذن المستخدم، بما في ذلك الصور التي تُظهر معلومات شخصية وحساسة مثل البيانات المالية أو الصحية، أو أماكن التواجد.

كما انتشرت مخاوف حول ما يمكن أن يفعله القائمون على التطبيق بهذه الصور في المستقبل، ومن إمكانية وصول بيانات المستخدمين إلى الحكومة الروسية مثلاً.

وأشار موقع "BBC" إلى تخوف البعض من استخدم التطبيق للبيانات التي جمعها من المستخدمين من أجل التدرب على خوارزميات التعرف على الوجه، إذ يمكنه القيام بذلك حتى بعد حذف الصور نفسها لأن قياس الميزات على وجه الشخص يمكن استخراجها واستخدامها لمثل هذا الغرض.

ث. رد الشركة على الاتهامات

أصدرت شركة "Face App Inc" المالكة للتطبيق بياناً نفت فيه مشاركة أو بيع بيانات المستخدمين مع أطراف ثالثة، كما أكدت أنها تقوم بتحميل الصورة التي اختارها المستخدم فقط إلى خوادمها، وأنها تحذف كل الصور في مدة لا تتجاوز 48 ساعة من تاريخ التحميل.

ولكن يبرز التساؤل هنا عن سبب حاجة التطبيق إلى تحميل الصور أصلاً طالما أنه قادر على معالجتها على الهاتف دون الحاجة إلى تحميلها؟

2. تطبيق الصراحة

لاقى تطبيق "الصراحة" شعبية واسعة وانتشاراً كبيراً منذ إطلاقه عام 2017، خاصة بعد طرح نسخته الإنكليزية، إذ وصلت قاعدة مستخدميه إلى ملايين المستخدمين حول العالم، لكنه واجه في المقابل انتقادات من قبل خبراء الأمن الرقمي واتهامات بانتهاكه لخصوصية المستخدمين.[3]

أ. ما هو تطبيق "الصراحة"؟

يُتيح تطبيق "الصراحة" لمستخدمه استقبال رسائل من الأصدقاء قد تحمل انتقاداً أو مديحاً أو بوحاً بالمشاعر، دون الكشف عن هوية المرسل أو إمكانية الرد على تلك الرسائل.
وصمم هذا التطبيق المبرمج السعودي "زين العابدين توفيق"، دون أن يتوقع له هذا الكم من الانتشار أو الانتقادات.

ب. الانتقادات الموجهة للتطبيق

تعرض التطبيق لاتهامات تتعلق بانتهاك خصوصية المستخدمين، بعد اكتشاف إمكانية وصوله إلى الأسماء وجهات الاتصال الخاصة بالمستخدم، ووفقاً لموقع The Intercept يقوم التطبيق بتحميل تلك البيانات إلى خوادم الشركة دون وجود أي سبب وجيه لذلك.[4]

كما حذر خبراء أمن آخرون قاموا بتحليل نسخة "APK" للتطبيق باستخدام موقع "Virustotal" أن التطبيق يطلب استخدام الكاميرا لالتقاط الصور في أي وقت، والسماح له بقراءة البيانات من مستوعب حفظ خارجي، بالإضافة لصلاحيته بالكتابة على شريحة "SD"، وهي جميعها من المفترض ألا يحتاجها هذا النوع من التطبيقات.[5]

من جانب آخر يحذر الخبراء من إمكانية لجوء المخترقين إلى التطبيق من أجل تحقيق غاياتهم، فقد يعمد أحدهم إلى إرسال رسالة مرفقة برابط ملف تجسسي على أنه مرتبط بالتعليق الذي أرسله، وهنا سيقع الضحية بالفخ لمجرد فتحه الرابط دون أن يتمكن من معرفة المرسل.

ت. رد المطور

من جانبه رد مطور البرنامج، زين العابدين توفيق، على تلك الانتقادات بأن خوادم الموقع لا تحتفظ ببيانات المستخدمين أو جهات الاتصال الخاصة بهم، وأن طلب الوصول إلى الكاميرا سببه تأمين التقاط الصور للملف الشخصي.[6]

---

[3] "تطبيق "صراحة".. سعودي المنشأ يجتاح أمريكا والعالم". 10 كانون الثاني/يناير 2018. (آخر زيارة للرابط 5 شباط/فبراير 2020). http://tiny.cc/wkimjz.

[4] "Hit App Sarahah Quietly Uploads Your Address Book." August 27, 2017. Last visit February 5, 2020. https://theintercept.com/2017/08/27/hit-app-sarahah-quietly-uploads-your-address-book/ .

[5] "انتبهوا "صراحة" تطبيق بعيد عن الشفافية والصراحة يخرق خصوصية المستخدمين!". مونت كارلو الدولية. 3 آب/أغسطس 2017. (آخر زيارة للرابط 5 شباط/فبراير 2020). http://tiny.cc/2pimjz.

✓ نصائح لتقليل مخاطر اختراق التطبيقات للخصوصية:

- ❖ التحقق من الأذونات التي يطلبها التطبيق عند تحميله، وما إذا كان من المنطقي طلبها، وقراءة سياسة الخصوصية بدقّة.
- ❖ التحري حول سمعة التطبيق وموثوقيته قبل تحميله، بما في ذلك الانتباه لتفقد المعلومات حول المنتِج للتطبيق، وإلقاء نظرة على آراء وتقييمات المستخدمين.
- ❖ التحديث المستمر لنظام التشغيل قبل تثبيت أي تطبيق لحماية البيانات من الفيروسات.
- ❖ عدم تزويد التطبيق بأي تفاصيل شخصية حتى يتم التأكد من كيفية استخدامها.

منظمة "سوريون من أجل الحقيقة والعدالة" كانت قد أصدرت دليلاً خاصاً بحماية العاملين في مجال التوثيق والصحافة تحت اسم "خطوات عملية في الحماية الرقمية".