كيف تكتشف تطبيقات الهواتف الذكية المزيفة؟

الأحد 19 مارس 2017 10:03 م

تحفل متاجر الهواتف الذكية بما لا يحصيه العد من التطبيقات الحقيقية، لكن توجد أيضا المئات من التطبيقات المقلدة التي تبدو للوهلة الأولى كأنها أصلية.

ورغم أن مثل تلك التطبيقات يروج أصحابها أنها مرخصة فإنها في الواقع مجرد عبوات تطبيقات فارغة عديمة الفائدة، هدفها استدراج المستخدمين لجني أموالهم وأحيانا أخرى سرقة بياناتهم.

لا تؤثر هذه المشكلة فقط على أنظمة التشغيل آي.أو.إس وأندرويد وويندوز موبايل للأجهزة المحمولة، بل تؤثر أيضا على متاجر التطبيقات الخاصة بأنظمة تشغيل الحاسوب المكتبي مثل ويندوز 10 وماك أو.إس. ولحسن الحظ هناك طرق عديدة لاكتشاف هذه التطبيقات المزيفة.

أولى هذه الطرق النظر إلى العلامة التجارية الموجودة على التطبيق.

يقول تيم لوتر من اتحاد تكنولوجيا المعلومات الألماني "بيتكوم" إن على المستخدم إذا أراد اكتشاف التطبيق المزيف في متجر التطبيقات، أن ينظر بدقة وتمعن على العلامة التجارية. فرغم التشابه الكبير بين العلامة التجارية على التطبيق المقلد والتطبيق الأصلي، توجد غالبا فروق وخلافات دقيقة يمكن رصدها.

كما يقول الصحفي المتخصص في تكنولوجيا المعلومات ألكسندر سابير إن البحث عن العلامة التجارية للمنتجات الأصلية ومقارنتها بشكل العلامة الموجودة على التطبيقات الأخرى في المتجر يمكن أن تفيد في اكتشاف التطبيقات المزيفة.

"هناك تطبيقات أخرى للأجهزة المحمولة يسعى أصحابها لكسب المال بطرق أخرى، وهي التجسس على بيانات المستخدمين ثم ابتزازهم بعد ذلك"

والاختلاف بين اسم التطبيق المتاح للبيع والتطبيق الأصلي ولو كان يسيرا يشير لاحتمال أن يكون التطبيق مزيفا. ومن أدلة التزييف الأخطاء الإملائية في وصف التطبيق وعدم التطابق بين الوصف والخصائص.

ويضيف أن اسم الشركة المطورة للتطبيق إشارة مهمة للغاية لأصالة التطبيق. فإذا كان التطبيق مزيفا فغالبا لا يكون الاسم مطابقا لاسم الشركة على التطبيق الأصلي. كذلك يجب التعامل بحذر مع التعليقات والعروض الخاصة بالتطبيق، وحسب سابير فإن أي تقييمات إيجابية لا ترافقها تعليقات شارحة تثير الشكوك.

كما يحذر سابير من تطبيقات أخرى للأجهزة المحمولة يسعى أصحابها لكسب المال بطرق أخرى، وهي التجسس على بيانات المستخدمين ثم ابتزازهم بعد ذلك.

وعامة يجب إزالة أي تطبيق غير مفيد من الجهاز حتى إذا لم يكن ضارا، وإذا صودف مثل هذه التطبيقات يفضل عمل إعادة ضبط المصنع للجهاز، لأن بعض التطبيقات تعيد تثبيت نفسها بعد إزالتها.

وأخيرا، يمكن للمستخدم الذي اشترى تطبيقا مزيفا باستخدام بطاقة ائتمان الاتصال بالشركة المصدرة للبطاقة ومطالبتها بوقف تحويل المال إلى البائع، إلى جانب إبلاغ المتجر بوجود تطبيق مزيف لمساعدة المستخدمين الآخرين في عدم السقوط في هذا الفخ.