

7 علامات تحذرك بأن هاتفك "مخترق"



الخميس 16 أغسطس 2018 07:08 م

دفع التطور الكبير والمتلاحق للهواتف الذكية والأجهزة المحمولة الإنسان للاعتماد عليها بشكل متزايد في كل أمور حياته، حتى باتت تحمل معلوماتنا الشخصية الحساسة مثل التفاصيل المصرفية والرسائل الخاصة، والمكالمات، ورسائل البريد الإلكتروني، وتفاصيل حساباتنا الشخصية على وسائل التواصل الاجتماعي والعديد من المعلومات الأخرى، وهو ما يجعلها هدفاً لعمليات اختراق القرصنة

لذلك اليوم سنقدم لك 7 علامات تحذيرية إذا كان هاتفك يعاني منها، فمعناه أنه يتم اختراق هاتفك الذكي، وهي كالتالي:

1- الهاتف يعمل ببطء:

إذا كان أداء الهاتف أبطأ من المعتاد، قد يعود السبب إلى وجود برنامج ضار "malware"، ما يسبب بطء عمل الهاتف، حيث إن هذا النوع من الفيروسات يمكن أن يؤثر على أداء الجهاز، ويمكن أن يكون هذا البرنامج الضار برنامج تجسس يعمل على سحب بياناتك وملفاتك لجهاز آخر، ما يؤثر على عمل وحدة المعالجة الرئيسية التي من شأنها أن تبطئ عمل الجهاز

2- الهاتف يُعاني من نفاد شحن البطارية بسرعة:

إذا بدأت في ملاحظة أن البطارية بحاجة إلى الشحن بشكل متكرر على مدّ قصيرة، فعادةً ما يرجع ذلك إلى شيء يعمل في الخلفية على جهازك

في الحالات الأسوأ يرجع السبب في ذلك إلى قيامك بتنزيل نوع من البرامج الضارة التي تعمل في الخلفية وتعمل على إبطاء كل شيء، هذا ليس جيداً؛ حيث إنه -اعتماداً على نوع البرامج الضارة- قد تصبح ضحية لعملية اختراق من أجل سرقة الهوية أو الاستيلاء على ملفاتك

3- زيادة استهلاك باقة الإنترنت المُفعّلة على هاتفك:

شيء آخر يجب الانتباه إليه هو استخدامك للبيانات، إذا لاحظت أن استخدام بيانات الإنترنت قد زاد أو حتى أنك تجاوزت حد باقة البيانات المخصصة، فقد يكون هاتفك قد تعرض لعملية اختراق من بعض أنواع البرامج الضارة، وقد تشير الزيادة في استخدام البيانات إلى أن هناك أحدًا ينقل البيانات من جهازك إلى جهاز آخر

وبناء على ذلك احذف أي تطبيقات جديدة حقّلتها، وإذا استمر الأمر اعمل reset للهاتف

4- ارتفاع درجة حرارة الهاتف:

إذا لاحظت أن الجهاز ساخن للغاية فهذه إشارة سيئة، قد يكون ذلك بسبب تشغيل تطبيق خبيث في الخلفية، يمثل ضغطاً على وحدة المعالجة المركزية CPU.

5- ظهور رسائل مجهولة بكثرة وهو ما يُعرف بالتصيد Phishing:

أكثر أدوات عمل القرصنة تنوعاً ونجاحاً هي التصيد الاحتيالي phishing، وهي الطريقة التي يتظاهر فيها شخص ما بأنه شخص موثوق به أو شركة للوصول إلى معلوماتك الشخصية

غالباً ما تكون هذه الطريقة ممثلة في شكل رسائل بريد إلكتروني، وقد يكون من الصعب اكتشافها، ولكن هناك مؤشرات رئيسة تكشف عن أنك تقع ضحية عملية احتيال منها:

الأخطاء الإملائية، والأخطاء النحوية، والإفراط في استخدام علامات الترقيم مثل علامات التعجب، وتعدّ عناوين البريد الإلكتروني غير

الرسمية هي أيضًا إحدى العلامات الاحتياطية؛ لأن البنوك وشركات الطيران تحاول أن تكون رسمية وشفافة قدر الإمكان وتستخدم عناوين بريد إلكتروني رسمية ومثبتة على أسماء النطاقات الخاصة بها

كما أن النماذج المضمنة والمرفقات الغريبة وروابط مواقع الويب البديلة مربية أيضًا، لذلك فإن تجاهل هذه الرسائل الإلكترونية المشبوهة هي خطوة جيدة لمنعها من تحقيق هدفها

6- استخدام شبكات الواي فاي العامة Public Wi-Fi:

من أسهل الطرق التي تُسهل للقراصنة اختراق هاتفك والوصول إلى معلوماتك الشخصية هي استخدامك شبكات الواي فاي العامة للاتصال بالإنترنت

يستخدم المتسللون تقنيات مختلفة للحصول على بياناتك الحساسة أثناء الاتصال بشبكة الواي فاي العامة غير المشفرة، حيث يمكنهم تقديم موقع مزيف لك يطلب منك إدخال بياناتك وقد يكون ذلك مقنعًا وصعبًا الاكتشاف لحظتها، لذا ننصحك بعدم استخدام الخدمات المصرفية عبر الهاتف المحمول أو التسوق أثناء استخدامك شبكة واي فاي عامة

تذكر دائمًا أن تسجل الخروج بعد ذلك إنهاء اتصالك بشبكة الواي فاي العامة؛ لأنك إذا غادرت دون تنفيذ ذلك يمكن أن يتابع أحد المتسللين جلسة الويب الخاصة بك على الموقع الذي استخدمته مثل فيسبوك أو رسائل البريد الإلكتروني الخاصة بك، ويمكنهم فعل ذلك عبر ملفات تعريف الارتباط وحزم HTTP، لذلك تذكر دائمًا تسجيل الخروج

7- البلوتوث قيد التشغيل رغم أنك لم تشغله:

يمكن أن يسمح البلوتوث للمتسللين بالوصول إلى هاتفك دون حتى لمسك وهذا النوع من القرصنة يمكن أن يمر دون أن يلاحظه المستخدم، كما يمكن أن يصيب الأجهزة الأخرى المحيطة بك إذا كانت متصلة معهم عن طريق البلوتوث

أوقف تشغيل البلوتوث، وكن على دراية بأي تنزيلات مشبوهة أو روابط عناوين URL في النصوص ورسائل البريد الإلكتروني وخدمات المراسلة مثل فيسبوك أو واتساب، والتي يمكن أن تعطل هاتفك وتضر به

إذا لاحظت أن البلوتوث قيد التشغيل ولم تشغله، فأوقف تشغيله وشغل فحص الهاتف حتى تصل إلى الملفات الضارة التي تقوم بهذا الفعل وتقضي عليها