

# معلومات و أفكار

## كيفية إزالة المتسلل من هاتفك الذكي

كيف تحمي هاتفك من الاختراق

?

?

?

يمكن أن يؤدي اختراق الهاتف إلى تعريض هويتك وخصوصيتك للخطر دون علمك. يقوم المحتالون باستمرار بتطوير وتحسين أساليب القرصنة ، مما يزيد من صعوبة اكتشافهم. هذا يعني أن المستخدم العادي قد يكون أعمى بسبب أي عدد من الهجمات الإلكترونية. لحسن الحظ ، يمكنك حماية نفسك من خلال مواكبة آخر المستجدات

## لماذا هواتفنا هدف للقرصنة

جلبت الهواتف الذكية جميع حساباتنا وبياناتنا الخاصة إلى موقع واحد مناسب – مما يجعل هواتفنا الهدف المثالي للمتسلل. كل شيء من الخدمات المصرفية إلى البريد الإلكتروني ووسائل التواصل الاجتماعي مرتبط بهاتفك. مما يعني أنه بمجرد وصول المجرم إلى هاتفك ، تفتح جميع تطبيقاتك أبوابًا للسرقة الإلكترونية.

# ماهي قرصنة الهاتف

يتضمن اختراق الهاتف أي طريقة يفرض فيها شخص ما الوصول إلى هاتفك أو اتصالاته. يمكن أن يتراوح هذا من الخروقات الأمنية المتقدمة إلى الاستماع ببساطة إلى اتصالات الإنترنت غير الآمنة. يمكن أن يتضمن أيضًا سرقة ماديًا لهاتفك واختراقه بالقوة عبر أساليب مثل القوة الغاشمة. يمكن أن تحدث قرصنة الهاتف لجميع أنواع الهواتف ، بما في ذلك أجهزة iPhone و Android. نظرًا لأن أي شخص يمكن أن يكون عرضة لاختراق الهاتف ، فإننا نوصي بأن يتعلم جميع المستخدمين كيفية التعرف على الجهاز المخترق.



# كيفية معرفة ما إذا كان شخص ما يقوم باختراق هاتفك

قد يكون واحدًا أو أكثر من هذه العلامات الحمراء على أن شخصًا ما قد اخترق هاتفك:

- 1- يفقد هاتفك الشحن بسرعة. تستخدم البرامج الضارة والتطبيقات الاحتيالية أحيانًا تعليمات برمجية ضارة تميل إلى استنزاف قدر كبير من الطاقة.
- 2- هاتفك يعمل ببطء بشكل غير طبيعي. قد يمنح الهاتف الذي تم اختراقه كل قوة المعالجة الخاصة به لتطبيقات المخترق المشبوهة. يمكن أن يتسبب هذا في بطء هاتفك إلى حد الزحف. يمكن أن يكون التجميد غير المتوقع ، والأعطال ، وإعادة التشغيل غير المتوقعة من الأعراض في بعض الأحيان.
- 3- لاحظت نشاطًا غريبًا على حساباتك الأخرى عبر الإنترنت. عندما يدخل أحد المتسللين إلى هاتفك ، سيحاولون سرقة الوصول إلى حساباتك القيمة. تحقق من الوسائط الاجتماعية والبريد الإلكتروني بحثًا عن مطالبات إعادة تعيين كلمة المرور أو مواقع تسجيل الدخول غير المعتادة أو عمليات التحقق من الاشتراك في الحساب الجديد.
- 4- إذا ظهرت مكالمات أو مكالمات في سجلاتك. قام المتسللون بالتنصت على هاتفك باستخدام حضان طروادة SMS. بدلاً من ذلك ، قد ينتحلون هويتك لسرقة معلومات شخصية من أحبائك. ترقب ، لأن الأتريقتين تترك فتات الخبز مثل الرسائل الاحكام

# ماذا تفعل إذا تم اختراق هاتفك الذكي

كيفية إزالة الهاكر من هاتفك

أولاً ، عليك التخلص من أي برامج ضارة اخترقت جهازك. بمجرد استئصال خرق البيانات ، يمكنك البدء في حماية حساباتك وإبعاد المتسللين عن هاتفك.

قد تشمل هذه:

لقد تعلمت كيفية تحديد ما إذا كان شخص ما يخترق هاتفك. الآن ، أنت مستعد للرد. وإليك كيفية استبعاد مجرمي الإنترنت هؤلاء من التكنولوجيا الشخصية الخاصة بك.

الخدمات المصرفية عبر الإنترنت

البريد الإلكتروني (العمل والشخصي)

معرف Apple أو حساب Google

رمز مرور الهاتف

جميع وسائل التواصل الاجتماعي

أولاً ، عليك التخلص من أي برامج ضارة اخترقت جهازك. بمجرد استئصال خرق البيانات ، يمكنك البدء في حماية حساباتك وإبعاد المتسللين عن هاتفك.

تابع أيضاً مع أي خدمات مالية أو خدمات تسوق عبر الإنترنت حفظت بطاقات الائتمان أو التفاصيل المصرفية الخاصة بك (مثل Amazon و eBay وما إلى ذلك) وهذا سيساعدك على تحديد أي معاملات احتيالية وتأكيد من الإبلاغ عن هذه الرسوم والاعتراض عليها مع البنك الذي تتعامل معه

# كيفية منع شخص ما من اختراق هاتفك مرة أخرى

تزداد أهمية أمان القرصنة على الهاتف نظرًا لأن المزيد من معلوماتنا الشخصية أصبحت رقمية ومتصلة بالهاتف المحمول. نظرًا لأن الأساليب تتطور باستمرار ، فسيتعين عليك أن تكون يقظًا دائمًا فيما يتعلق بالأمان.

إن مراعاة سلوكك الرقمي هو أفضل طريقة لحماية نفسك ولحسن الحظ ، هناك العديد من الممارسات المعروفة التي ثبت أنها تقلل من مخاطر القرصنة.

كيف تحمي هاتفك من الاختراق

لا تقم بتنزيل تطبيقات سطحية أو غير مرغوب فيها. انظر إلى المراجعات والبحث قبل التثبيت إذا لم تكن متأكدًا. إذا لم تكن واثقًا من أمان التطبيق ، فلا تثبته.

لا تقم بعمل جيلبريك لهاتفك. على الرغم من أنه يتيح لك التنزيل من متاجر التطبيقات غير الرسمية ، إلا أن كسر الحماية يزيد من خطر تعرضك للاختراق عن غير قصد. بصرف النظر عن البرامج الضارة أو برامج التجسس ، فهذا يعني أنك ستفقد تصحيحات الأمان في آخر تحديثات نظام التشغيل. يتخطى جيلبريك التحديثات للحفاظ على عمل جيلبريك. هذا يجعل مخاطر تعرضك للاختراق أعلى من المعتاد.