

كل ما تريد معرفته عن كيفية اختراق هاتفك ببرامج التجسس

الأربعاء 15 أكتوبر 2025 01:30 م

يمكن أن يتعرض هاتفك للتجسس عن طريق الخطأ دون علمك، عن طريق الإنترنت، لذا يتعين على أي شخص يمتلك هاتفًا ذكيًا الحذر من برامج التجسس، خاصةً إذا كان هاتفك قديمًا. ويمكنك معرفة ما إذا كان برنامج التجسس مثبتًا على هاتفك من خلال تشغيل الكاميرا والميكروفون بشكل عشوائي، أو سماع تشويش أثناء المكالمات، أو رؤية تطبيقات وملفات غير مألوفة على هاتفك. وكشفت رانزا تريفينو من شركة كيبير سيكيوريتي المهتمة بالأمن السيبراني عن قائمة بأهم العلامات التي قد تشير إلى تعرض الهاتف للتجسس، وكيفية التخلص من برامج التجسس، والحيلولة دون تعرض الهاتف للاختراق عن طريقها.

تشغيل كاميرا الهاتف والميكروفون بشكل عشوائي

إذا لاحظت تشغيل كاميرا وميكروفون هاتفك عشوائيًا، فقد يشير ذلك إلى اختراق هاتفك ببرامج تجسس. يمكن لبرامج التجسس استخدام كاميرا وميكروفون هاتفك سرًا للتنصت على مكالماتك، أو تسجيل الصوت، أو حتى التقاط الصور ومقاطع الفيديو دون علمك، مما يؤثر مخاوف جدية، ويُعرض خصوصيتك وسلامتك للخطر، حيث يمكن لقراصنة الإنترنت جمع معلوماتك الشخصية، وتتبع موقعك، والتنصت على مكالماتك، أو حتى مضايقتك.

سماع أصوات أثناء المكالمات الهاتفية

من العلامات الأخرى لاختراق هاتفك باستخدام برامج التجسس سماع أصوات غريبة أثناء المكالمات الهاتفية، مثل الصفير والأصوات البعيدة والتشويش. على الرغم من أن هذه المشاكل قد يكون سببها أحيانًا ضعف الإشارة، لكنها قد تشير أيضًا إلى أن اختراق هاتفك ومراقبة مكالماتك سرًا.

مشاكل في الأداء

إذا لاحظت ثمة مشكلة مفاجئة في أداء هاتفك، مثل أو ارتفاع درجة الحرارة أو استنزاف البطارية بسرعة، أو فترات تحميل طويلة أو مشاكل في إيقاف التشغيل أو إعادة التشغيل، فقد يكون ذلك علامة على اختراق جهازك. تعمل برامج التجسس في خلفية هاتفك، مستهلكة موارد النظام، مما يجعل الهاتف بطيئًا أو غير مستجيب أو حتى غير قابل للاستخدام.

تطبيقات أو ملفات غير مألوفة على هاتفك

من الدلائل الواضحة على احتمال تعرض هاتفك لبرامج تجسس ملاحظة تطبيقات أو ملفات غير مألوفة لا تعرفها أو تتذكر تنزيلها. قد تبدو هذه التطبيقات والملفات شرعية، لكنها في الواقع برامج ضارة تعمل في الخلفية دون علمك. بمجرد تثبيتها، يمكنها جمع معلومات حساسة، مثل تفاصيل حسابك المصرفي وكلمات مرورك وحتى موقعك، سرًا.

رسائل غير عادية

إذا بدأت بتلقي رسائل غير عادية على هاتفك، مثل نصوص غريبة أو رسائل خطأ متكررة أو إعلانات منبثقة، فقد يكون هاتفك تم اختراقه ببرامج تجسس. غالبًا ما تكون هذه الرسائل محاولات لإغرائك بالنقر على روابط ضارة تُطلب منك إدخال معلوماتك الشخصية.

كيف يمكنك إزالة برامج التجسس من هاتفك؟

في بعض الحالات، لا يمكن إزالة برامج التجسس يدويًا أو باستخدام برنامج مكافحة فيروسات. إذا لم تتمكن من إزالة برامج التجسس بعد اتباع الخطوات التالية، فقد تحتاج إلى إعادة ضبط هاتفك إلى إعدادات المصنع، مما يؤدي إلى مسح جميع التطبيقات والملفات والمستندات وبرامج التجسس من الهاتف تمامًا. قبل إعادة ضبط هاتفك، تأكد من نسخ بياناته احتياطيًا لتجنب فقدانها.

إزالة برامج التجسس من هاتفك، اتبع الخطوات التالية:

أعد تشغيل هاتفك في الوضع الآمن:

أول ما عليك فعله هو فصل هاتفك عن الإنترنت وإعادة تشغيله في الوضع الآمن. يعمل الوضع الآمن فقط على البرامج الأساسية، مما يؤدي إلى قطع اتصال برامج التجسس بقراصنة الإنترنت، ويسمح بإعادة تشغيل هاتفك دون أي تدخل.

احذف التطبيقات والملفات غير المألوفة:

بعد إعادة التشغيل في الوضع الآمن، راجع التطبيقات والملفات على هاتفك. ابحث عن التطبيقات والملفات التي لا تتذكر تنزيلها أو التي تبدو مشبوهة. احذف أي عناصر ضارة، وامسح ذاكرة التخزين المؤقت للمتصفح لإزالة أي مواقع ويب ضارة.

شغل برنامج مكافحة فيروسات:

قد تظهر بعض برامج التجسس كتطبيقات أو ملفات رسمية، مما يصعب اكتشافها. لتحديد أي برامج تجسس مخفية وإزالتها، ثبت برنامج مكافحة فيروسات على هاتفك. يخصص برنامج مكافحة الفيروسات هاتفك بحثًا عن أي برامج تجسس مخفية، ثم يزيلها. كما أن تثبيته على هاتفك سيساعد في منع الإصابات المستقبلية.

أعد تشغيل هاتفك بشكل طبيعي:

بعد إتمام الخطوات السابقة، يمكنك إخراج هاتفك من الوضع الآمن وإعادة تشغيله بشكل طبيعي بعد تشغيل هاتفك، يجب عليك منع تثبيت برامج التجسس عليه مستقبلاً بتحديث برنامجك واتباع أفضل ممارسات الأمن السيبراني .

كيفية منع برامج التجسس من الوصول إلى هاتفك؟

يمكنك حماية هاتفك من التعرض لبرامج التجسس، من خلال الخطوات التالية:

لا تقم بتنزيل التطبيقات من مواقع الويب غير الموثوقة

لتجنب تثبيت برامج التجسس عن طريق الخطأ، لا تُنزل التطبيقات من مواقع ويب غير موثوقة أو إعلانات مشبوهة. نزل التطبيقات فقط من مصادر موثوقة، مثل متجر تطبيقات "آبل ومتجر جوجل بلاي".

تجنب النقر على الرسائل غير المرغوب فيها

يمكن أن تنتشر برامج التجسس عبر رسائل التصيد الاحتيالي الإلكترونية التي تحتوي على مرفقات ضارة أو النقر على رابط ضار . تجنب التفاعل مع الرسائل غير المرغوب فيها التي تحتوي على مرفقات أو روابط مشبوهة، وإذا لم تكن متأكدًا، فافحص المرفقات بحثًا عن برامج ضارة أو تحقق من وجود أي تناقضات في الروابط باستخدام أداة فحص عناوين URL.

تصفح فقط المواقع الآمنة

يمكن لقراصنة الإنترنت تثبيت برامج تجسس على هاتفك عبر عمليات تنزيل عشوائية، حيث قد يؤدي مجرد زيارة موقع غير آمن إلى إصابة هاتفك بالبرمجيات الخبيثة. لحماية نفسك، التزم بالمواقع الموثوقة، واكتب عناوين URL مباشرة في متصفحك، وتجنب النقر على الروابط المشبوهة. توخ الحذر عند استخدام محركات البحث، فقد تظهر بعض الإعلانات الضارة أو المواقع المزيفة في نتائج البحث.

حافظ على تحديث برنامج هاتفك

يستغل قراصنة الإنترنت ثغرات أمنية في برامج أو تطبيقات هاتفك لإصابته ببرامج تجسس. يُعدّ تحديث برنامج هاتفك باستمرار من أكثر الطرق فعالية لحماية نفسك. فالتحديثات لا تُضيف ميزات أمان جديدة فحسب، بل تُصحّح أيضًا أي ثغرات أمنية قد يستغلها قراصنة الإنترنت. كما أن التأكد من تشغيل هاتفك بأحدث إصدار من نظام التشغيل يُقلّل من خطر الإصابة ببرامج التجسس وغيرها من أنواع البرامج الضارة.

استخدم مدير كلمات المرور

مع أن مدير كلمات المرور لا يحظر برامج التجسس مباشرةً، إلا أنه يُقلّل من خطر التعرض لهجمات مُعينة. فمن خلال إنشاء كلمات مرور وتخزينها وتعبئتها تلقائيًا، يُقلّل من الحاجة إلى كتابتها يدويًا، مما يُوفر حمايةً من مُسجلات ضغطات المفاتيح، وهي نوع من برامج التجسس التي تُسجل ضغطات المفاتيح. كما يُحافظ على بيانات اعتمادك مُخزنةً بأمان في خزانة مُشفرة، مما يُصعّب سرقة بيانات اعتمادك حتى في حال اختراق جهازك.

تثبيت برنامج مكافحة الفيروسات

يكتشف برنامج مكافحة الفيروسات البرامج الضارة المعروفة ويمنعها ويزيلها من جهازك. يُنصح بتثبيت برنامج موثوق لمكافحة فيروسات الأجهزة المحمولة، إذ يساعد في الكشف عن برامج التجسس المخفية، وحظر التهديدات المحتملة، وتنبهك إلى المواقع الضارة أو التنزيلات الضارة.