كيف تكتشف التجسس عليك من خلال كاميرا الهاتف؟

الجمعة 14 نوفمبر 2025 07:30 م

هل تخشى من أن كاميرا هاتفك قد تتجسس عليك؟، في الواقع فإن هذا ليس مستبعد تمامًا، في ظل وجود برامج التجسس يمكنها الوصول إلى هاتفك عن بعد، بالإضافة إلى نسخ شاشة جهازك وإظهار كل ما عليها
لكن من خلال التعرف على العلامات التحذيرية واتباع بعض الخطوات، فإنه يمكن اكتشاف تعرض كاميرا هاتفك للاختراق
وحددت شركة "إسيت" لتكنولوجيا المعلومات، قائمة بالمؤشرات التي قد تدل على تعرض هاتفك للتجسس عن طريق الكاميرا:

تصرفات مفاجئة

قد تشمل: تُشغّل الكاميرا تلقائيًا مع أن بعض برامج التجسس تُطفئ المؤشر الأخضر لإخفاء نشاطها، إلا أنه من الأفضل التحقق من ذلك
عدم القدرة على الوصول إلى الكاميرا إذا كان تطبيق آخر، مثل برامج التجسس، يصل إلى الكاميرا، فقد تتلقى رسالة تشير إلى أنه يحاول فتح الكاميرا

صور أو مقاطع فيديو غير معروفة

إذا وجدت صورًا أو مقاطع فيديو مخزنة في معرض الصور لديك ولا تتذكر التقاطها، فيجب أن يكون هذا بمثابة علامة تحذير على أن الكاميرا ربما تعرضت للاختراق

استنزاف البطارية وارتفاع درجة الحرارة

غالبًا ما تستهلك برامج التجسس المثبتة سرًا على هاتفك طاقةً أكثر من المعتاد، حتى في حال عدم استخدام الهاتف راقب استهلاك البطارية، واحتمالية ارتفاع درجة حرارة الجهاز

استخدام غير عادي للبيانات

عادةً ما يرغب المخترقون في الوصول إلى اللقطات التي سجلوها عبر كاميرتك؛ وفي هذه الحالة، سيحتاجون إلى إرسال هذه البيانات عبر الإنترنت لذا، قد تشير الارتفاعات المفاجئة في استخدام البيانات والفواتير إلى عمليات نقل ملفات كبيرة لا تعلم بها

مشاكل الأداء

لا تقتصر أضرار البرامج الضارة، مثل برامج التجسس، على استنزاف بطارية الجهاز فحسب، بل تستهلك أيضًا موارد النظام، مما قد يؤدي إلى تعطل التطبيقات أو تباطؤ أدائها وفي بعض الحالات القصوى، قد يتوقف الجهاز عن الاستجابة

سلوك غير متوقع للجهاز

مؤشر آخر على وجود برامج تجسس على هاتفك هو إعادة تشغيله فجأةً و/أو إضاءة شاشته دون سبب وجيه قد يكون أحدٌ ما هو السبب عن بُعد

تطبيقات جديدة غريبة

تُثبّت برامج التنصت نفسها على هاتفك كتطبيق، حيث يمتلك الكثير منا تطبيقات كثيرة لدرجة أننا قد لا نلاحظ تطبيقًا إضافيًا، لذا يُنصح بالانتباه

كيفية حماية كاميرا هاتفك من التجسس

باتباع بعض الخطوات البسيطة، يمكنك تجنب مشكلة أمنية وخصوصية محتملة كما أن النصائح التالية فعالة في منع انعكاس شاشة الهاتف:

مراجعة أذونات التطبيق بشكل منتظم

قد تحتوي التطبيقات التي تبدو وكأنها تطلب أذونات زائدة على برامج ضارة لذلك، يُنصح بمراجعتها من حين لآخر وإلغاء الأذونات الممنوحة لأي تطبيق لا يتطلب الوصول إلى التطبيق أو الميكروفون ليعمل بشكل صحيح

تثبيت برنامج أمان موثوق به

قم بتنزيل برنامج مكافحة البرامج الضارة من جهة خارجية موثوقة للكشف عن برامج التجسس وحذفها

حافظ على تحديث جهازك

يوصى بالتحديثات المنتظمة لنظام تشغيل هاتفك وجميع التطبيقات التي تعمل عليه لضمان حصولك على أحدث الإصدارات وأكثرها أمانًا في جميع الأوقات

يُفضّل دائمًا تنزيل التطبيقات من متاجر التطبيقات الرسمية فقط (جوجل بلاي، آبل آب ستور)، مما يقلل من احتمالية تنزيل تطبيق يحتوي على برامج تجسس

تجنب كسر الحماية/تجذير جهازك

قد يؤدي القيام بذلك إلى تعطيل تدابير أمنية مهمة (على جهاز آي فون)، وتقييد التحديثات التلقائية، وتعريضك لتطبيقات ضارة على متاجر التطبيقات التابعة لجهات خارجية

استخدم طرق المصادقة القوية

تأكد من تأمين جهازك بإنشاء رقم تعريف شخصي قوي ومصادقة بيومترية (مثل Face ID). تأكد من حماية أي تطبيقات من اختراق جهات خارجية بإنشاء كلمات مرور قوية وفريدة مُخزنة في مدير كلمات المرور

عزز أمان تسجيل الدخول بتفعيل المصادقة البيومترية، مما يعني أنه حتى لو تمكن أي شخص من الاطلاع على كلمات مرورك، فلن يتمكن من الوصول إلى تطبيقاتك وحساباتك

قم بتغطية الكاميرا عندما لا تكون قيد الاستخدام

إذا كنت تريد أن تكون حذرًا للغاية، فكر في وضع ملصق فوق الكاميرا لتغطية العدسة عندما لا تكون قيد الاستخدام

احذر من شبكات واي فاي العامة

غالبًا ما تكون شبكات الواي فاي العامة معرضة للاختراق إذا لم تكن البيانات على هذه الشبكات مشفرة، فقد يتمكن الهاكرز من التنصت على تصفحك للويب، بل وحتى إعادة توجيهك إلى مواقع خبيثة تُثبّت برامج تجسس أو قد تُسجّل دخولك عن طريق الخطأ إلى نقطة اتصال مشبوهة

احذر محاولات الاحتيال

تُعد محاولات الاحتيال أحد أهم أسباب إصابة الهاتف ببرامج التجسس لذا، انتبه لعلامات التحذير: رسائل بريد إلكتروني غير مرغوب فيها من شركات وهيئات تبدو موثوقة، تحثك على النقر على رابط أو فتح ملف مرفق غالبًا ما يحاولون فرض قرارات سريعة على أهدافهم من خلال خلق شعور بالإلحاح قاوم هذه الرغبة

ماذا تفعل إذا كنت تشك في وصول غير مصرح به إلى الكاميرا؟

إذا لم تتمكن من تنفيذ التدابير الوقائية بالسرعة الكافية، أو لم تنجح، ففكر في الخطوات التالية

قم بإجراء فحص للبرامج الضارة باستخدام تطبيق أمان موثوق به للعثور على أي تهديدات وحذفها

قم بفحص وإلغاء تثبيت أي تطبيقات مشبوهة أو تمت إضافتها مؤخرًا

تقييم أذونات التطبيق وإلغاء أي وصول "مطلوب" إلى الكاميرا لا يستند إلى سبب وجيه

قم بتحديث جميع برامجك ونظام التشغيل للتأكد من أنها تعمل على أحدث إصدار وأكثرها أمانًا، مما يجعل الحياة أكثر صعوبة للبرامج الضارة المحتملة على جهازك

راقب سلوك الجهاز عن كثب بحثًا عن علامات التحذير المذكورة أعلاه

إذا استمرت المشاكل، فقد يلزم إعادة ضبط المصنع أو استعادة البيانات من النسخة الاحتياطية في هذه الحالة، يُرجى التواصل مع خدمة عملاء الشركة المصنعة لجهازك للحصول على الإرشادات أولاً

يمكن أن تتعرض الهواتف الذكية للتهديدات من مصادر متنوعة قد يكون مجرمًا إلكترونيًا يسعى لسرقة معلوماتك الشخصية لبيعها على "الدارك ويب"، أو أن يسعى أحد الملاحقين للحصول على صور ومقاطع فيديو التقطتها كاميرتك وقد تكون أيضًا مراقبة من جهة أمنية لكن أيًا ما كان مصدر قلقك، فاليقظة هي الأساس