

هل يمكن التجسس على هاتفك عندما يكون مغلقًا؟

الجمعة 17 أكتوبر 2025 05:00 م

هل يمكن لشخص ما أن يتجسس على هاتفك عندما يكون مغلقًا؟، ربما دار في ذهنك هذا السؤال دون أن تتوصل إلى إجابة شافية حوله. وفقًا لشركة "سيرتو سوفت وير" البريطانية المتخصصة في أمن أجهزة الهواتف المحمولة، فإن بعض أنواع البرمجيات الخبيثة قد تجعل الهاتف يبدو وكأنه مُطْفَأ، بينما هو في الواقع لا زال نشطًا، مما يجعله عُرضة للتجسس. على سبيل المثال، Android/PowerOffHijack هو نوع من برامج التجسس التي تسيطر على عملية إيقاف تشغيل الهاتف. نتيجةً لذلك، قد يبدو هاتفك مُطْفَأ وهو لا زال يعمل. ولحماية نفسك من هذه المخاطر، توخَّ الحذر عند تثبيت التطبيقات من مصادر غير معروفة، وحافظ على تحديث برنامج هاتفك باستمرار.

ثغرات الأجهزة

يمكن للمهاجمين المتمرسين استغلال نقاط الضعف في أجهزة الهاتف لاعتراض البيانات أو التحكم في الجهاز عن بعد، حتى عندما يبدو أنه مغلق. وعلى الرغم من أنه من غير المرجح أن يمتلك القراصنة العاديون الأدوات والمهارات اللازمة لتنفيذ مثل هذه الهجمات، فإن منظمات مثل وكالة الاستخبارات والأمن البريطانية (GCHQ) ووكالة الأمن القومي الأمريكية قد طورت برامج قادرة على التنصت على الهواتف المغلقة. أفضل طريقة للدفاع عن نفسك من ثغرات الأجهزة هي الحفاظ على أمان هاتفك فعليًا.

العثور على جهاز في وضع الطاقة المنخفضة

عند إيقاف تشغيل هاتفك، قد تفترض أن جميع أنشطة الاتصال اللاسلكي تتوقف فورًا. لكن هذا ليس هو الحال دائمًا. غالبًا ما تدخل الهواتف الذكية الحديثة في وضع "الاحتياطي" منخفض الطاقة، مما يُبقي بعض الميزات نشطة جزئيًا، مما يُشكل ثغرة أمنية محتملة للمهاجمين المُحتَكِين. ويمكن لأجهزة آبل التي تعمل بنظام "آي أو إس 15"، أو أحدث أن تظل قابلة للبحث لمدة تصل إلى 24 ساعة بعد إيقاف تشغيلها. تستمر ميزة "العثور على شبكتي" في الاتصال بأجهزة "آبل" القريبة عبر البلوتوث، حتى عندما يبدو الهاتف مغلقًا تمامًا. تعمل أجهزة أندرويد بشكل مشابه، مع اختلاف ذلك باختلاف الشركة المصنعة. العديد من هواتف سامسونج وجوجل تحافظ على وظائفها عند إيقاف تشغيلها، بما فيها القدرة على الاستجابة لطلبات "العثور على جهاز" لفترة محدودة باستخدام طاقة البطارية الاحتياطية. على الرغم من أن هذه الميزات مصممة لمساعدتك في تحديد موقع أجهزتك المفقودة وتوفير الراحة، إلا أنها تتيح أيضًا فرصة للاستغلال. نظريًا، يمكن لمخترق محترف استغلال هذه الميزات للوصول إلى هاتفك حتى عندما تعتقد أنه مغلق تمامًا. لا يقتصر التهديد على القراصنة المحترفين فحسب. فأني شخص لديه حق الوصول إلى بيانات اعتماد حسابك على "آبل" أو "جوجل" - سواء كان شريكًا أو فردًا من عائلتك أو أي شخص شاركته بيانات تسجيل الدخول - يمكنه استخدام ميزات "العثور على جهاز" هذه لمراقبة موقعك دون علمك.

ثغرات البلوتوث

كشفت الأبحاث أن أجهزة "آي فون" الحديثة تحتفظ بوظائف لاسلكية مهمة حتى عند إيقاف تشغيلها. وأظهرت دراسة أُجريت عام 2022 أن شرائح "يو دبليو بي"، و"إن إف سي" و"بلوتوث" تستمر في العمل في وضع الطاقة المنخفضة لدعم ميزات مثل تتبع شبكة Find My. الأهم من ذلك، وجدت الدراسة أن برامج البلوتوث الثابتة على هذه الأجهزة غير موقَّعة ولا مُشَقَّرة، مما يجعلها عُرضة للتعديل. نجح الباحثون في تحميل برمجيات خبيثة مُخصَّصة على شريحة البلوتوث، واستمرت في العمل حتى مع ظهور هاتف الآيفون مُطْفَأ تمامًا. يمكن أن يقوم هذا البرنامج الخبيث بإرسال إشارات موقع غير مصرح بها، أو اعتراض اتصالات Secure Element - شريحة مخصصة في الهاتف الذكي تُستخدم لتخزين البيانات الحساسة والمعلومات المشفرة بشكل آمن للغاية، أو تنفيذ أنشطة ضارة أخرى.

تُثير هذه التداعيات قلقًا بالغًا بالنسبة للأهداف عالية القيمة، التي قد تُطفيئ أجهزتها مُتوقعةً صمَّمًا تأمُّنًا إذ يُمكن للمُهاجم الذي يتمتع بإمكانية الوصول إلى مستوى النظام تعديل البرامج الثابتة لوضع الطاقة المنخفضة للحفاظ على قدرات مراقبة مُستمرة تصمد أمام عمليات الإغلاق.

أفضل الممارسات لتأمين هاتفك

على الرغم من أن مخاطر التجسس على الهاتف - حتى مع إغلاق جهازك - قد تبدو مُقلقة، إلا أن هناك خطوات عملية يمكنك اتخاذها لحماية نفسك. يكمن السر في تطبيق طبقات متعددة من الأمان تعمل معًا لحماية بياناتك الشخصية واتصالاتك.

من خلال اتباع التدابير الوقائية التالية، يمكنك تقليل خطر المراقبة غير المصرح بها بشكل كبير والحفاظ على سيطرة أفضل على خصوصيتك:

استخدم كلمات مرور قوية وفريدة، وفُغل المصادقة الثنائية (2FA)

أنشئ كلمات مرور معقدة لجميع حساباتك، وتجنب إعادة استخدامها. فُغل المصادقة الثنائية كلما أمكن لإضافة طبقة حماية إضافية. فُكر في استخدام مدير كلمات مرور لتخزين كلمات مرور قوية لحساباتك بأمان وإنشائها.

حافظ على تحديث برامجك باستمرار

حدِّث نظام تشغيل هاتفك وتطبيقاته بانتظام لتجنب أي ثغرات أمنية محتملة. غالبًا ما تتضمن هذه التحديثات تصحيحات أمنية مهمة تحمي من التهديدات المكتشفة حديثًا.

راجع أذونات التطبيقات بعناية

توخَّ الحذر عند تثبيت تطبيقات جديدة، ولا تمنح الأذونات إلا عند الضرورة القصوى.

راجع بانتظام إعدادات الخصوصية وأذونات التطبيقات في هاتفك لتعطيل أي وصول غير ضروري إلى الكاميرا أو الميكروفون أو موقعك أو أي بيانات حساسة أخرى.

أغلق جهازك جيدًا. لتقليل خطر التجسس عندما يكون هاتفك مغلقًا، تأكد من إغلاقه تمامًا بدلًا من وضعه في وضع السكون.

اضغط باستمرار على زر التشغيل وأغد عملية الإغلاق للتأكد من أن الميكروفون والكاميرا في هاتفك غير نشطين.

تفعيل تشفير الجهاز

يُضيف تشفير هاتفك طبقة أمان إضافية من خلال طلب كلمة مرور أو رقم تعريف شخصي لفتح قفل الجهاز والوصول إلى البيانات المخزنة عليه.

فُغل التشفير باتباع التعليمات الخاصة بنظام تشغيل هاتفك.

استخدم شبكة VPN للأنشطة عبر الإنترنت. تُنشئ هذه الشبكة الافتراضية الخاصة، اتصالاً مشفّرًا بين جهازك والإنترنت، مما يساعد على حماية بياناتك واتصالاتك من المتنصتين والمخترقين المحتملين.

احتفظ بهاتفك في حقيبة فارادي عند الحاجة

للحصول على أقصى حماية من المراقبة اللاسلكية، استخدم حقيبة فارادي، وهي حقيبة متخصصة تحجب جميع الإشارات اللاسلكية، بما في ذلك الاتصالات الخلوية، والواي فاي، والبلوتوث، ونظام تحديد المواقع العالمي (GPS).