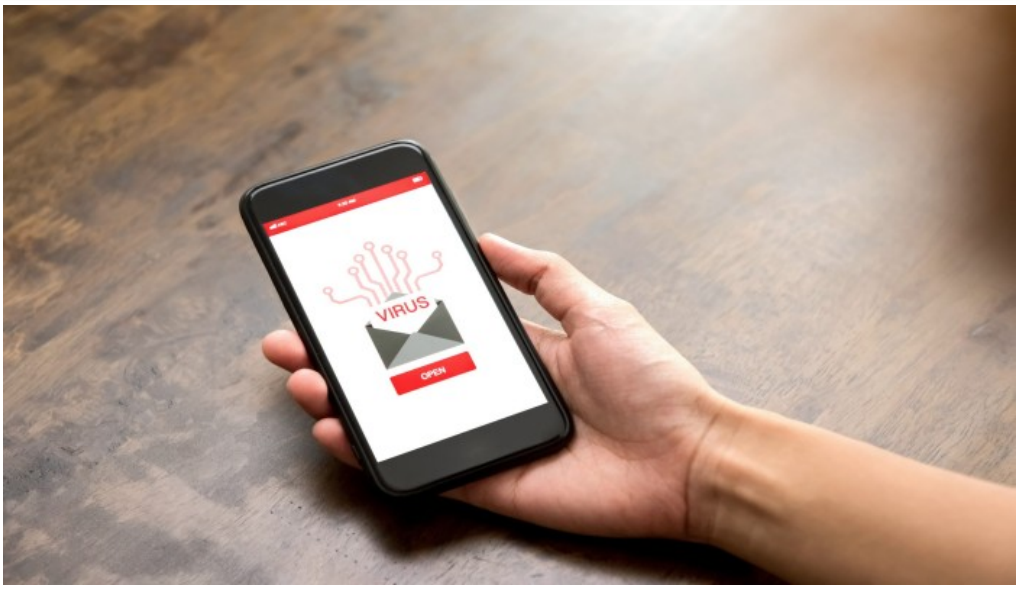
في 6 خطوات تخلص من الفيروسات على هاتفك



السبت 15 نوفمبر 2025 07:00 م

هل هاتفك يتباطأ أو يسخن؟، في حال لاحظت أن هناك شيئًا غير معتاد في جهازك قد يكون ذلك علامة على إصابته بالفيروسات التي تختبئ في الملفات والتطبيقات القابلة للتنزيل والتي يمكن تثبيتها على جهازك دون علمك

الطريقة الأسهل للتخلص من الفيروس من جهاز "أندرويد" هي استخدام برنامج مكافحة الفيروسات الموثوق به لمحاولة إزالة الفيروس يدويًا، قم بمسح بيانات المتصفح، وأعد التشغيل في الوضع الآمن، واحذف التطبيقات والملفات المشبوهة

يمكن أن يساعد تنشيط خدمة جوجل بلاي للحماية، وإجراء فحص أمان لحساب جوجل أيضًا في التعامل مع الفيروسات على هواتف أندرويد ويمكنك التخلص من الفيروسات على هاتفك بخطوات بسيطة

1. قم بتشغيل فحص مكافحة الفيروسات

يُمكن أن يساعدك تطبيق مكافحة الفيروسات مثل "نورتون موبايل سكيورتي" على التخلص من الفيروسات على جهاز الأندرويد غالبًا، يكفي فحص سريع لتحديد البرامج الضارة غير المرغوب فيها والتخلص منها

لإجراء فحص مضاد للفيروسات، افتح برنامج مكافحة الفيروسات، وانقر على زر الفحص، واتبع التعليمات التي تظهر على الشاشة تتيح لك بعض برامج مكافحة الفيروسات جدولة عمليات فحص دورية، بينما يوفر بعضها الآخر حماية فورية سيساعدك برنامج مكافحة فيروسات جيد على إزالة أي فيروس من جهازك

2. امسح ذاكرة التخزين المؤقت وملفات تعريف الارتباط

إذا كان هاتفك مصابًا بفيروسات ضارة، فعليك مسح ذاكرة التخزين المؤقت وملفات تعريف الارتباط (كوكيز) في متصفحك، حتى يساعدك في إزالة الملفات أو البيانات الضارة المخفية التي قد تستخدمها البرامج الضارة للعمل

إليك كيفية مسح ذاكرة التخزين المؤقت وملفات تعريف الارتباط على جوجل كروم، أحد أكثر المتصفحات شيوعًا لمستخدمي أندرويد:

افتح جوجل كروم

اضغط على قائمة النقاط الثلاث في الزاوية اليمنى العليا

حدد حذف بيانات التصفح

اختر "كل الوقت" من القائمة المنسدلة، ثم حدد "حذف البيانات" في الزاوية اليمنى السفلية

نصيحة سريعة: قد يؤدي مسح ذاكرة التخزين المؤقت وملفات تعريف الارتباط بالكامل إلى تسجيل خروجك من حساباتك النشطة، لذا كن مستعدًا لتسجيل الدخول مجددًا لاحقًا إذا كنت قلقًا بشأن نسيان كلمات المرور والحاجة إلى إعادة تعيينها، فيمكن أن يساعدك مدير كلمات المرور

3. أعد تشغيل جهازك في الوضع الآمن

إعادة تشغيل جهازك في الوضع الآمن - وهو إصدار مُخفّض من نظام التشغيل يُستخدم لاستكشاف الأخطاء وإصلاحها - يُعطّل تطبيقات الجهات الخارجية (التي ثبّتها بنفسك) ويمنعها من الوصول إلى ميزات مثل الكاميرا أو الخرائط. هذا يمنع البرامج الضارة، مثل برامج التجسس ، من اختراق هذه التطبيقات أثناء محاولة إزالتها.

إليك كيفية إعادة تشغيل جهاز أندرويد الخاص بك في الوضع الآمن:

استمر في الضغط على زر الطاقة الموجود على جانب جهازك.

اضغط مع الاستمرار على زر إيقاف التشغيل على الشاشة.

اضغط على موافق للتأكيد على رغبتك في الدخول إلى الوضع الآمن.

إذا كان هاتفك يعمل بشكل طبيعي في الوضع الآمن، فقد يشير ذلك إلى وجود برنامج ضار مخفي في تطبيق تابع لجهة خارجية. تشمل علامات البرامج الضارة بطء الأداء، وارتفاع درجة الحرارة، أو فتح التطبيقات وإغلاقها فجأة.

4. إزالة التطبيقات والملفات المصابة

ابحث عن الملفات أو التطبيقات غير المألوفة التي لا تعرفها - احذف أي شيء مشبوه. لإزالة التطبيق، اضغط عليه مطولًا حتى يبدأ بالاهتزاز، ثم انقر على "إلغاء التثبيت".

يجب إزالة التطبيقات المزيفة التي قد تحتوي على برامج ضارة أولًا. ابحث عن هذه العلامات عند مراجعة تطبيقاتك:

الأذونات غير المعتادة: تحقق من أذونات تطبيقاتك واسأل نفسك إن كنت قد منحتها بالفعل. إذا كان لتطبيق ما صلاحية وصول لا تتذكر موافقتك عليها، عليك بإزالته.

التطبيقات المكررة: إذا رأيت تطبيقين بنفس الاسم والأيقونة، فقد يكون أحدهما مزيفًا. أزلهما، ثم أعد تنزيل إصدار موثوق من متجر جوجل بلاي الرسمي.

مصادر غير رسمية: التطبيقات التي تُنزّل من مواقع غير موثوقة أكثر عرضة لاحتواء برامج ضارة. ابحث عن التطبيقات التي لم تُثبّتها من الموقع الرسمي للمطوّر أو من متجر جوجل بلاي.

تقييمات المستخدمين السلبية: تحقق من تقييمات العملاء لمعرفة ما إذا أبلغ آخرون عن برامج ضارة. في حال ذلك، ألغِ تثبيت التطبيق.

تصميم غير مألوف: قد تكون التطبيقات ذات التصميمات الغريبة، أو الميزات المعطوبة، أو التي تُقلّد تطبيقات أخرى مُزيّفة تحتوي على برامج ضارة، لذا يُفضّل حذفها.

بعد التحقق من وجود تطبيقات مشبوهة، انتقل إلى ملفاتك. يمكنك مراجعة ملفاتك باستخدام تطبيق "الملفات" المدمج من جوجل لاستكشاف مجلدات النظام.

إذا وجدتَ أي ملفات مشبوهة، ابحث عنها قبل حذفها، لأن حذف الملفات المهمة قد يُسبب مشاكل إضافية لهاتفك. إذا لم تكن متأكدًا مما إذا كان الملف برنامجًا ضارًا أم ملف نظام أساسيًا، فمن الأفضل استخدام برنامج مكافحة فيروسات مُخصص، مثل "نورتن موبايل سيكيورتي"، الذي سيساعدك في تحديد الملفات الضارة وإزالتها.

اكتشاف الملفات أو التطبيقات غير الآمنة لنظام أندرويد:

ابحث عن أسماء الملفات الغريبة.

تحقق من الملفات ذات الامتدادات مثل .exe أو .apk حيث يمكن للبرامج الضارة أن تختبئ فيها، ولكنها قد تكون شرعية، لذا تحقق من المصدر قبل إزالة أي منها.

ابحث عن المجلدات التي لا تتذكر إنشاءها، لكن عليك أن تنتبه إلى أن بعض مجلدات النظام غالبًا ما تبدو غير مألوفة.

في حالة الشك، استخدم برنامج مكافحة الفيروسات لتحديد التطبيقات أو الملفات الضارة.

5. قم بتفعيل جوجل بلاي للحماية

توفر لك خدمة جوجل بلاي للحماية طبقة حماية إضافية مجانية ضد البرامج الضارة الخفية. وهو نظام دفاعي مدمج يفحص التطبيقات ويحذرك في حال وجود أي شيء يبدو مريبًا. قد يساعدك على تجنب تثبيت تطبيقات خطيرة من البداية.

إليك كيفية تشغيل خدمة جوجل بلاي للحماية:

افتح جوجل بلاي وحدد رمز ملفك الشخصي في الزاوية اليمنى العليا.

حدد "بلاي للحماية"، ثم رمز الترس في الزاوية اليمنى العليا.

قم بتشغيل فحص التطبيقات باستخدام "بلاي للحماية" وتحسين اكتشاف التطبيقات الضارة.

سيؤدي تفعيل "تحسين اكتشاف التطبيقات الضارة" إلى فحص التطبيقات المُنزّلة مباشرةً من مواقع الويب. مع أن هذه الميزة تُضيف طبقة حماية إضافية، إلا أنه من الضروري التحقق من مطوّر التطبيق والتأكد من تنزيل التطبيقات من موقعه الرسمي.

نصيحة سريعة: أثناء تصفحك شاشة إعدادات خدمة جوجل بلاي للحماية، راجع أذونات التطبيقات غير المستخدمة ضمن " خصوصية التطبيقات". يمكن للبرامج الضارة استغلال الأذونات الممنوحة للتطبيقات القديمة، لذا فإن إلغاء أذونات التطبيقات أو إزالة التطبيقات غير المرغوب فيها يزيد من أمان هاتفك. كما أن حذف التطبيقات القديمة يُساعد في تسريع جهازك .

6. قم بإجراء فحص أمان لحساب جوجل

بعد التأكد من خلو جهازك من البرامج الضارة، قم بإجراء فحص أمان لحساب جوجل. يمكن للبرامج الضارة جمع بيانات اعتماد حسابك أو السيطرة عليه. قد يساعد الفحص السريع في تأمين حسابك والحفاظ على أمان معلوماتك.

فيما يلي ما يجب عليك مراجعته أثناء فحص أمان جوجل:

كلمات المرور المحفوظة: إذا كنت تستخدم مدير كلمات المرور من جوجل ، فراجع كلمات مرورك للتأكد من عدم وجود أي منها ضعيف أو مُعرَّض للخطر. غيِّرها إلى كلمات مرور قوية وفريدة للحفاظ على أمان كلمات مرورك .
الأجهزة المُسجّلة الدخول: راجع الأجهزة المتصلة بحسابك على جوجل. إذا وجدت جهازًا غير مُصرّح به، فأزله فورًا وحدّث كلمة مرور حسابك.

نشاط الأمان: تحقق من أي نشاط غير عادي، مثل محاولات تسجيل الدخول من مواقع غير معروفة. قد يكون هذا مؤشرًا على تعرض حسابك للاختراق من خلال برامج ضارة أو اختراق بيانات .

المصادقة الثنائية: فعِّل المصادقة الثنائية (2FA) لإضافة طبقة أمان إضافية، وحمايتك من الاستيلاء على حسابك. هذا يُصعّب على المتسللين الوصول إلى حسابك، حتى لو كانوا يعرفون كلمة مرورك.

تطبيقات الجهات الخارجية: راجع التطبيقات التي يمكنها الوصول إلى حسابك على جوجل. إذا لم تتعرف على أيٍّ منها أو لم تستخدمها منذ فترة، فألغِ وصولها لمنع جمع البيانات غير المرغوب فيها.

إعادة ضبط جهازك إلى إعدادات المصنع

إذا جربت كل شيء ولا يزال هاتفك مصابًا ببرامج ضارة، فأعد ضبط جهازك إلى إعدادات المصنع. سيؤدي هذا إلى حذف جميع التطبيقات والملفات على هاتفك ، لذا لا تنسَ نسخ بياناتك المهمة احتياطيًا أولًا.

إليك كيفية إعادة ضبط المصنع لهاتف أندرويد:

افتح الإعدادات، ثم قم بالتمرير لأسفل وانقر فوق النظام.

قم بالتمرير إلى الأسفل وحدد خيارات إعادة التعيين.

حدد مسح جميع البيانات (إعادة ضبط المصنع).

في حال فاتتك الخطوة الأولى، قم بإجراء فحص مضاد للفيروسات مثل نورتن موبايل سيكيورتي لأجهزة أندرويد قبل محاولة إعادة ضبط المصنع. قد يوفر عليك هذا فقدان جميع ملفات هاتفك ومتاعب إعادة ضبطه.

علامات تشير إلى أن هاتفك قد يحتوي على برامج ضارة

إذا كان هاتفك يسخن أو يعمل ببطء، أو تنفد بطاريته بسرعة، فقد يكون مصابًا ببرامج ضارة. تصرف فورًا لمنع المتسللين من جمع بياناتك أو تشفير ملفاتك والاستحواذ عليها مقابل فدية.

فيما يلي بعض العلامات التي تشير إلى وجود برامج ضارة في جهازك:

عندما يتصرف جهازك بشكل غريب: قد يكون تباطؤ الهاتف، أو ارتفاع درجة حرارته، أو استنزاف البطارية بسرعة علامات على أن البرامج الضارة تُسبب ضغطًا مفرطًا على جهازك. يُنصح بإعادة ضبط هاتفك في الوضع الآمن لمعرفة ما إذا كان أحد التطبيقات هو السبب.

ظهور الكثير من الإعلانات المنبثقة: قد يكون ظهور الكثير من الإعلانات المنبثقة علامة على إصابة هاتفك بنوع معين من البرامج الضارة يُعرف باسم برامج الإعلانات. يمكن لهذه البرامج جمع معلوماتك وبيعها لشركات أخرى وإغراقك بإعلانات مزعجة.

يحتوي هاتفك على تطبيقات غير معروفة: راجع قائمة التطبيقات لديك للتحقق من وجود أي تطبيقات لا تتذكر أنك ثبّتها بنفسك. قد تكون هذه برامج ضارة تسللت إلى هاتفك وثبّتها تلقائيًا دون علمك.

لديك استهلاك بيانات مرتفع بشكل غير معتاد: قد يكون الارتفاع المفاجئ في استهلاك البيانات علامة على أن البرامج الضارة ترسل معلومات من جهازك إلى الهاكرز. تحقق من استهلاكك للبيانات في إعدادات هاتفك أو في فاتورتك (إذا كانت لديك حدود بيانات)، وافصل الإنترنت إذا لاحظت أي مشكلة.

رسائل غير مرغوب فيها: قد يعني هذا أن برنامجًا ضارًا على جهازك قد شارك بعض بياناتك الشخصية مع مجرمي الإنترنت. قد تكون الرسائل غير المرغوب فيها جزءًا من هجمات الرسائل النصية القصيرة لخداعك للكشف عن معلومات أكثر حساسية.

رسائل من هاتفك: يمكن لبعض البرامج الضارة الوصول إلى تطبيق المراسلة على هاتفك وإرسال رسائل نصية إلى جهات اتصالك. إذا سألك أحدهم عن رسائل غريبة واردة من رقمك، فقد يكون ذلك علامة على تعرض جهازك للاختراق.

معرفة العلامات هي الخطوة الأولى للتخلص من البرامج الضارة على جهاز أندرويد. لضمان سلامتك، شغّل برنامج مكافحة الفيروسات فورًا لاكتشاف أي تهديدات وإزالتها.