Verificación de dispositivos para detector el Root o Jailbreak

Si le preocupa la privacidad y seguridad de su dispositivo, puede ser importante verificar regularmente los teléfonos, tabletas y dispositivos que transmiten o hacen '*streaming*' para ver si han sido sometidos a Root o Jailbreak.

> "Root" significa que alguien ha adquirido la capacidad de administrar o gestionar el sistema operativo del dispositivo. El sistema operativo soporta las funciones básicas del dispositivo y permite ejecutar aplicaciones y programas. Someter un dispositivo al Root puede poner en peligro el sistema operativo, lo que hace que su teléfono sea menos seguro y más vulnerable a spyware y stalkerware.
>
> "Jailbreak" significa que alguien ha eliminado las limitaciones que el fabricante del dispositivo puso para mantenerlo seguro. Por ejemplo, el Jailbreak permite instalar en un iPhone aplicaciones que no proceden de la Apple Store o descargar ilegalmente contenidos protegidos por derechos de autor.

Antes de empezar: Priorizar la seguridad

La situación y los riesgos de cada persona sobreviviente son diferentes, y no hay una forma "correcta" de responder a un incidente, solamente formas que se ajustan o no a su situación... Saber la manera de cómo verificar si un dispositivo ha sido sometido al Root o Jailbreak puede ayudarle a identificar si una persona agresora puede haber manipulado ese dispositivo y pensar en diversas ideas sobre cómo hacerlo, así como a planificar qué actividades realizar en qué dispositivos. La verificación puede ser útil, pero no garantiza la seguridad por sí sola. Si una persona agresora vigila regularmente sus

dispositivos y cuentas, y usted decide efectuar cambios, esto puede alertarla. La persona puede saber que un dispositivo se ha restablecido a la configuración de fábrica o que se ha eliminado una aplicación no autorizada o una tienda de aplicaciones, y puede ser capaz de hacer el Root o Jailbreak de nuevo, coaccionarle u obligarle a darle acceso a su configuración, instalar spyware o stalkerware de forma remota, o intensificar el abuso. En algunas situaciones, hacer cambios también podría borrar pruebas.
Siempre dé prioridad a la seguridad y confíe en sus instintos. Puede que estas medidas de seguridad le resulten útiles:

- Utilice dispositivos y cuentas más seguros para las conversaciones y actividades delicadas. Si cree que alguien está vigilando su teléfono, computadora o cuentas, utilice un dispositivo diferente (como la computadora de la biblioteca o el teléfono de una amistad) y una cuenta a la que esa persona no pueda acceder (y a la que no haya tenido acceso en el pasado). Para obtener más información sobre dispositivos y cuentas más seguros, consulte nuestro recurso sobre seguridad de dispositivos y cuentas.
- Obtenga más información. Enfrentarse a la violencia, el abuso y el acoso puede ser difícil y peligroso. Las personas intercesoras pueden ayudarle a descubrir opciones y recursos locales y a crear un plan para su seguridad. Puede ponerse en contacto con una línea de ayuda nacional para que le pongan en contacto con recursos locales.

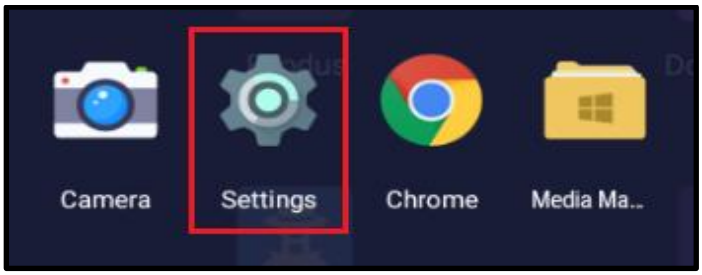
Verificación de dispositivos Android y Chromebooks

El Root es un proceso que se suele llevar a cabo en dispositivos Android a los que alguien tiene acceso físico y que otorga a otra persona el control del dispositivo a nivel de administrador. Con el control a nivel de administrador, esa persona puede desinstalar aplicaciones que deberían ser imposibles de desinstalar, cambiar los permisos de las aplicaciones, desactivar las funciones de seguridad del dispositivo, etc.

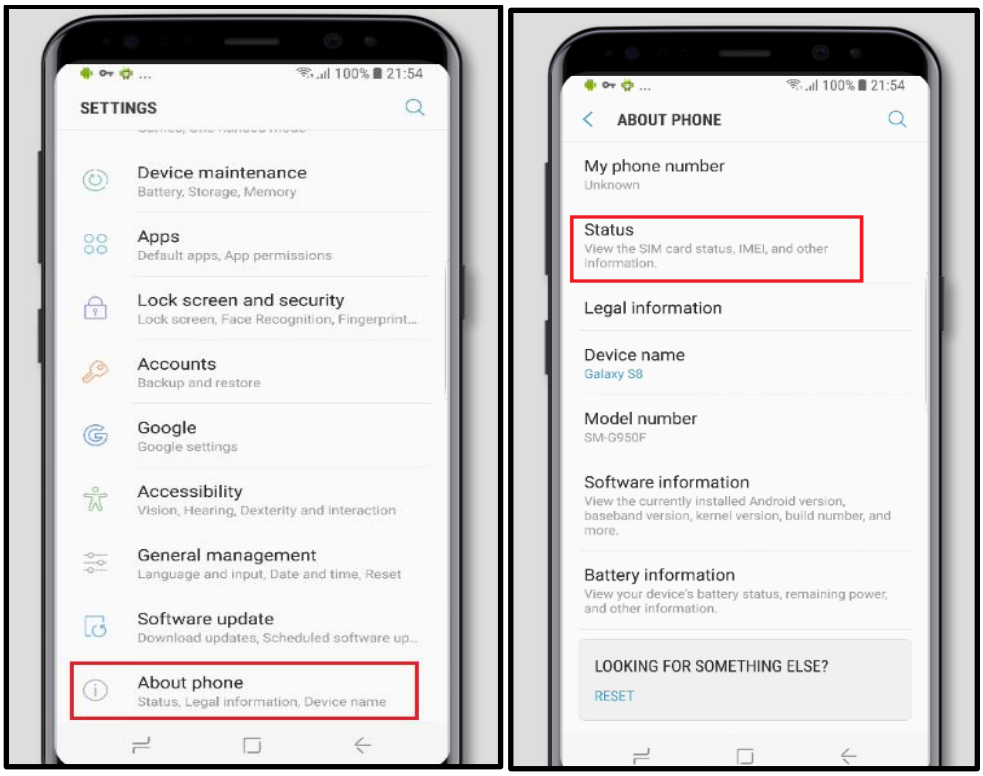
Dispositivos Android

Los dispositivos Android pueden ser teléfonos o tabletas que utilizan el sistema operativo Android, como las tabletas Amazon Fire o Google Pixel C. Esta sección se aplica a cualquier dispositivo Android.

Abra la configuración del dispositivo, que normalmente se indican con un ícono de engranaje.



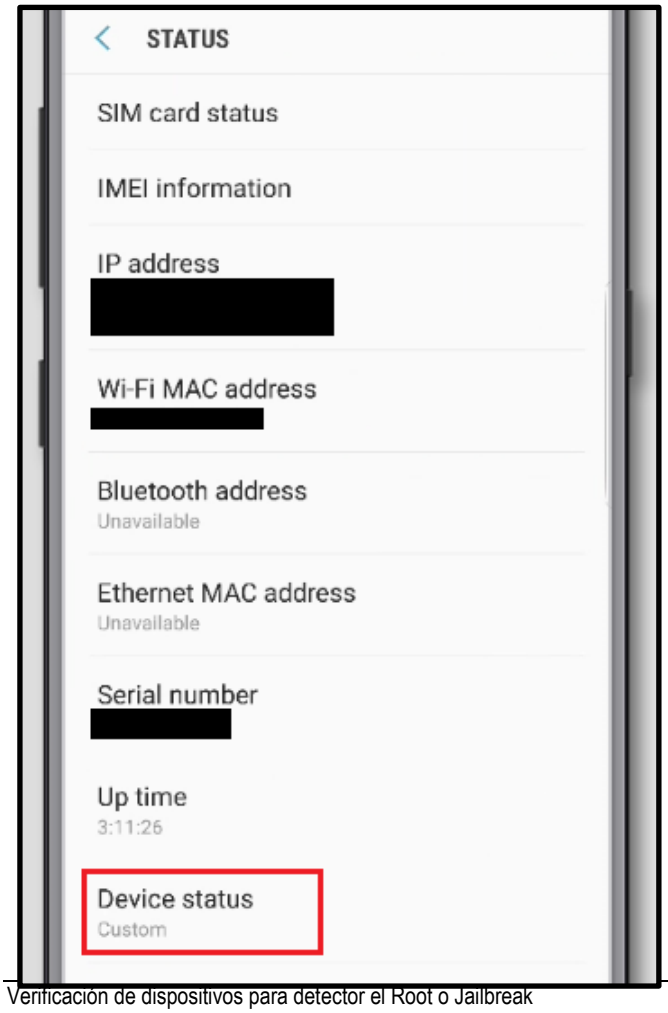
En configuración (*settings)*, busque la opción "Acerca del teléfono" (*About Phone)* (imagen inferior izquierda). Pulse "Acerca del teléfono" *(About phone)* y busque la opción "Estado" *(Status)* (los menús y opciones concretas pueden variar según el dispositivo y la versión de Android). Pruebe a pulsar la lupa para buscar si tiene problemas para encontrarlo.



Una vez en el menú Estado, desplácese hacia abajo hasta que encuentre un elemento "Estado del dispositivo" *(Device Status)* o "Estado del teléfono" *(Phone Status)*. Si está en "Personalizado" *(Custom)* - como se muestra en la imagen de abajo - significa que su dispositivo puede estar sometido al Root. Si muestra "Oficial" *(Official)* el teléfono no ha sido sometido al Root.

Desafortunadamente, es difícil deshacerse del Root de un dispositivo por su cuenta a menos que tenga muchos conocimientos técnicos. Un restablecimiento de fábrica no eliminará el Root del dispositivo. Puede llevar el dispositivo a una tienda de reparación de teléfonos y explicar el problema, y es posible que puedan ayudarle o remitirle a alguien que pueda hacerlo. Una persona representante de la tienda de su operador de telefonía también puede ser capaz de ayudar, pero tenga en cuenta que si su teléfono ha sido sometido al Root, esto podría anular la garantía del teléfono.

Si, y solamente si, se siente con la comodidad de intentar algo un poco más avanzado, puede instalar la aplicación de gestión Root SuperSU a través de un archivo APK (aplicación), y utilizarla para deshacer el Root del dispositivo (esto podría borrar todos sus archivos de la misma forma que lo haría un restablecimiento de fábrica). En esta página se explica cómo instalar un APK. Es muy importante tener cuidado con esto, porque podría hacer que su dispositivo sea menos seguro si se hace incorrectamente. Si decide seguir adelante, descargue e instale la última versión de SuperSU en su dispositivo (no instale ninguna aplicación que diga ser SuperSU a través de Google Play Store, ya que no es la aplicación real y podría ser un peligro para la seguridad o la privacidad, o simplemente no funcionaría). Abra SuperSU y pulse la pestaña Configuración, luego pulse "Deshacer Root completo" (*Full unroot)* y luego "Continuar" *(Continuar)* cuando se abra el cuadro de diálogo. Si la aplicación le pregunta si desea "¿Intentar restaurar la imagen de arranque de fábrica?" *(Attempt to restore stock boot image?)* o "¿Intentar restaurar la imagen de recuperación de fábrica?" (Attempt *to restore stock recovery image?)*, seleccione sí. Una vez que haya terminado, reinicie el dispositivo.



Dispositivos ChromeOS (Chromebooks)

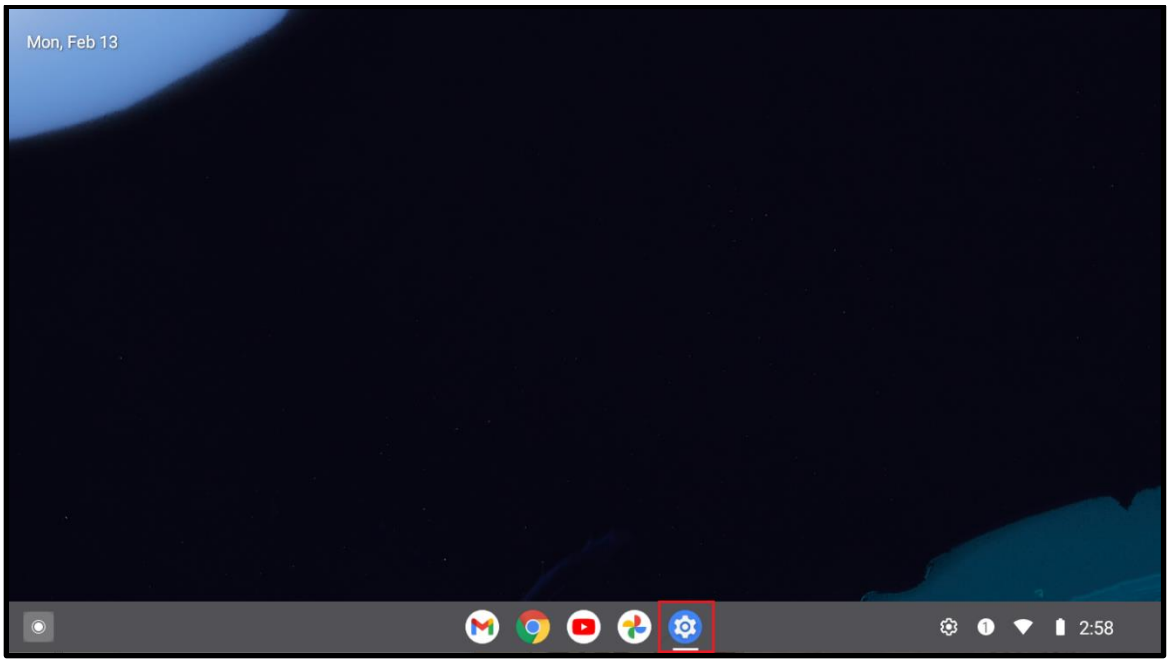
Los Chromebooks utilizan un sistema operativo llamado ChromeOS. Es relativamente fácil comprobar si un

Chromebook moderno está sometido al Root, pero tenga en cuenta que tanto hacer el Root como deshacerlo eliminará todos sus archivos y cuentas. Si decide deshacer el Root en un Chromebook sometido a Root, es recomendable que primero haga una copia de seguridad de todos los archivos y decida qué es lo que desea conservar.
Los siguientes son indicios de que su Chromebook podría estar sometido a Root:

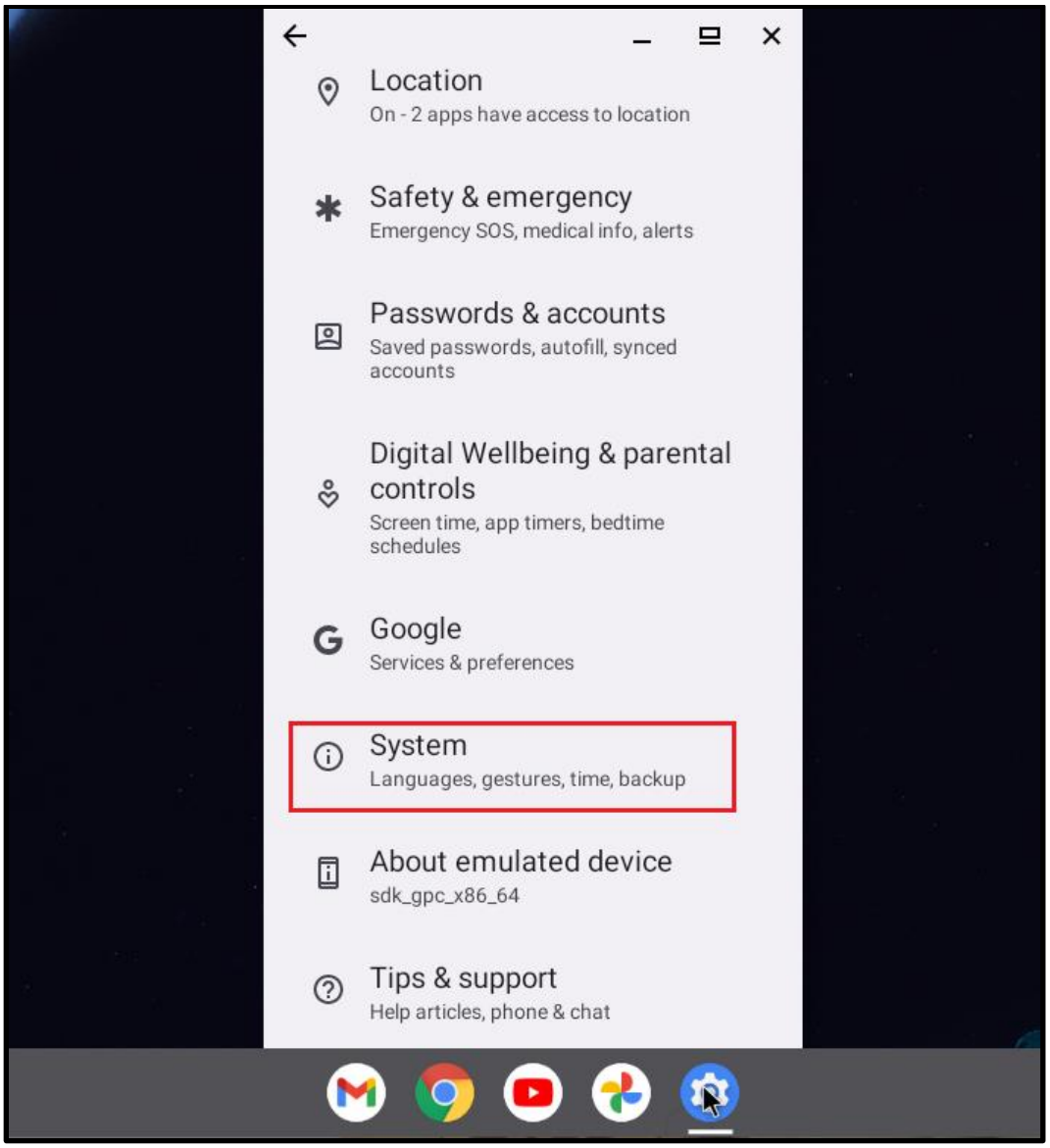
- Emite dos pitidos al encenderlo.
- Cuando lo reinicia muestra cualquier tipo de pantalla de advertencia, en lugar de la pantalla de inicio normal.

Si la pantalla dice "La verificación de OS está apagada *(OS Verification is off*): Pulse ESPACIO para volver a habilitar" y si se siente con la seguridad de deshacer el Root de su dispositivo (recuerde que esto puede borrar todos los archivos), puede hacerlo pulsando la barra espaciadora mientras se muestra esta pantalla.

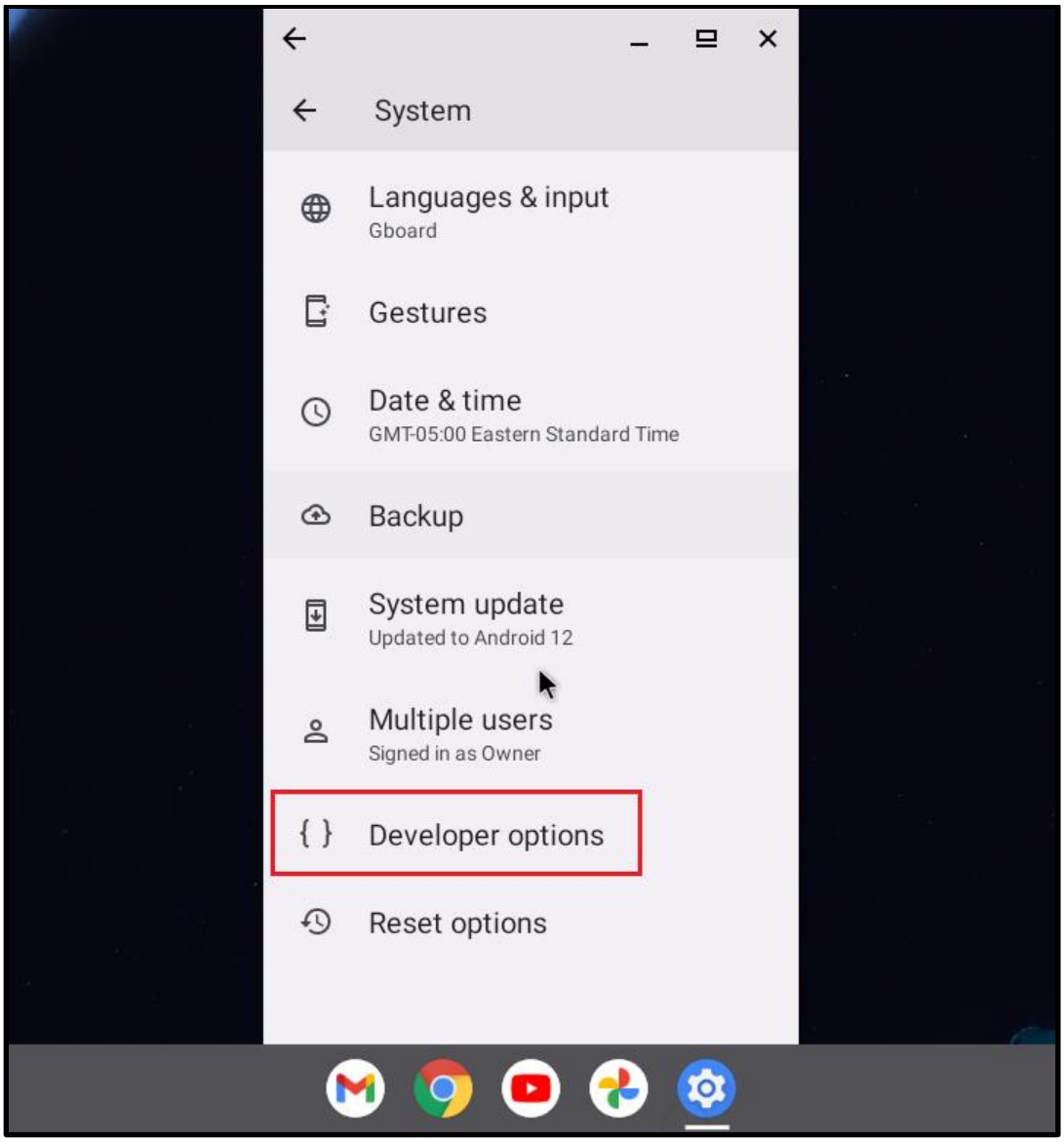
Si estas cosas no suceden, su Chromebook podría todavía estar sometido a Root. Para que un Chromebook esté sometido al Root, el usuario debe primero habilitar las "Opciones de desarrollador" *(Developer Options)*, y usted puede comprobar fácilmente si están activadas y desactivarlas. Abra la Configuración (un ícono de engranaje, que se muestra en el recuadro rojo en la imagen de abajo).



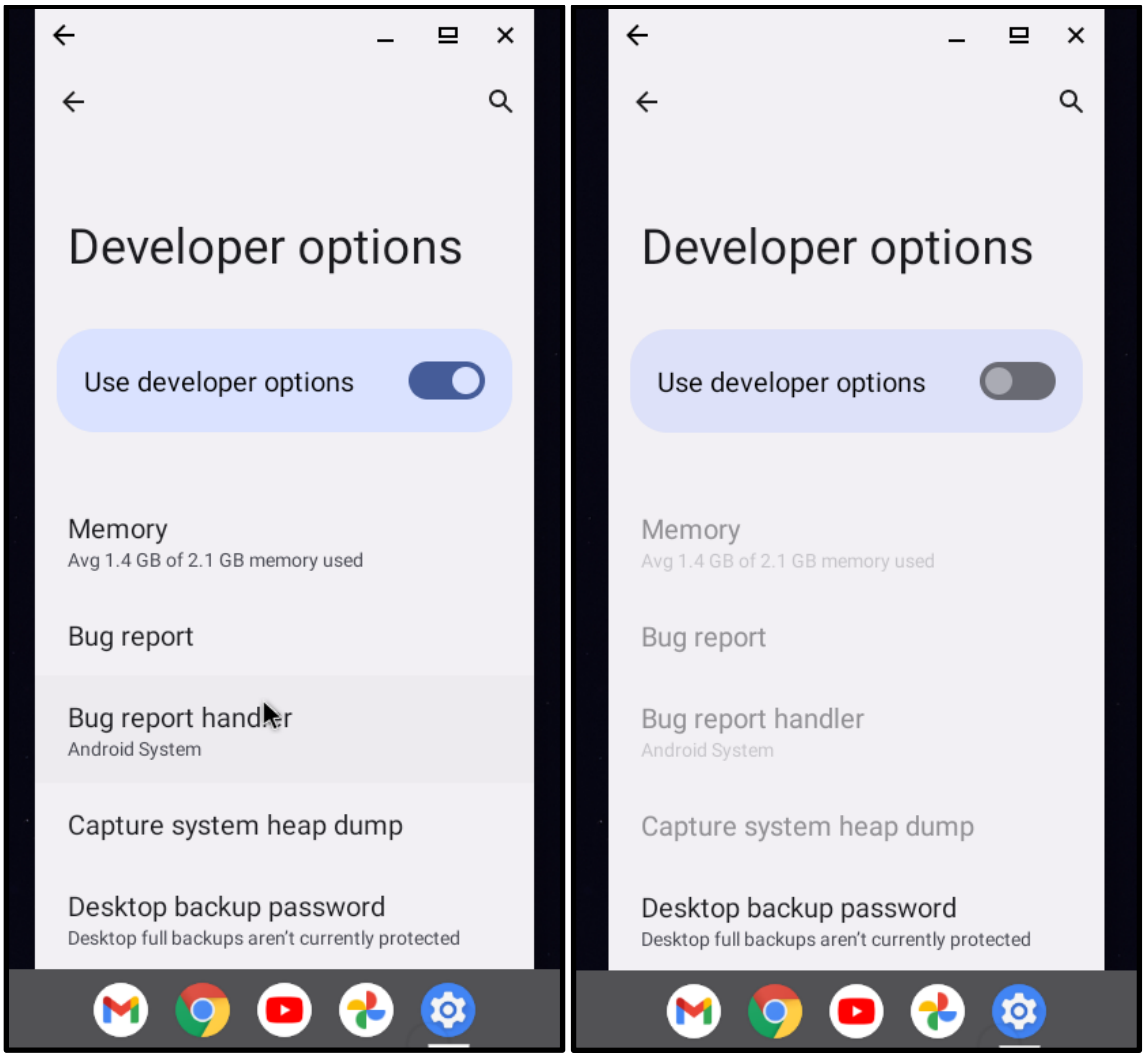
Al abrir la aplicación Configuración *(Settings)*, aparecerá un menú. Desplácese hasta el elemento Sistemas *(System)*, que aparece en rojo en la imagen siguiente, y púlselo.



Aparecerá otro menú. Desplácese por todo el menú. Si ve un elemento "Opciones de desarrollador" *(Developer Options)*, es posible que el Chromebook esté sometido a Root. Habilitar las opciones de desarrollador es solamente un paso necesario para el proceso de Root, pero a menos que esté desarrollando aplicaciones para Chromebook, hay pocas razones para tenerlo habilitado.



Si siente la seguridad de desactivar esta función, es fácil hacerlo con algunos Chromebooks, dependiendo del modelo. Pruebe a pulsar "Opciones de desarrollador" *(Developer Option)*. Si hay un interruptor con la etiqueta "Usar opciones de desarrollador" *(Use Developer Option)* (imagen inferior izquierda) gírelo a la posición "desactivado" *(off)* (imagen inferior derecha). Una vez que salga del menú de opciones de desarrollador, este debería desaparecer, lo que significa que ha retirado el Root del Chromebook.



Si no tiene la opción de hacer esto, y cree que el Chromebook está sujeto a Root porque emitió dos pitidos al arrancar pero sin otros indicadores, o si simplemente no quiere hacerlo por su cuenta, considere llevarlo a una tienda de reparaciones.

Verificación de los dispositivos iOS para el Jailbreak

El averiguar con seguridad si un dispositivo iOS (iPhone o iPad) está sometido a Jailbreak, puede requerir la ayuda de un especialista. Sin embargo, si utiliza los dos métodos siguientes, puede detectar la mayoría de los casos de Jailbreak.

Método 1: Busque aplicaciones que requieran Jailbreak

Puede utilizar la barra de búsqueda de su dispositivo para buscar aplicaciones que solamente pueden instalarse en dispositivos iOS con Jailbreak. La más conocida es Cydia, una tienda de aplicaciones alternativa, que alguien podría haber instalado en su dispositivo para instalar aplicaciones que Apple no permite en su tienda. Sin embargo, hay otras aplicaciones populares que normalmente requieren Jailbreak, incluyendo AppCake, Frida y PowerModule. La imagen de abajo muestra una búsqueda de Cydia que no encuentra resultados, lo que significa que Cydia no está instalado en el teléfono. Si encuentra alguna de estas aplicaciones, esto indica que el dispositivo está sometido a Jailbreak. ***AVISO:*** *Hay tiendas de aplicaciones alternativas que no requieren que su dispositivo esté sometido a Jailbreak, por lo que incluso si su dispositivo no lo está, alguien podría haber instalado una tienda de aplicaciones alternativa con el fin de instalar aplicaciones en su dispositivo que no están permitidas por Apple.*

Método 2: *Ejecutar aplicaciones incompatibles con Jailbreak*
Algunas aplicaciones, especialmente en el sector financiero, manejan datos delicados y son desarrolladas por empresas con fuertes preocupaciones de seguridad y cumplimiento legal. Estas aplicaciones a veces están diseñadas para no poder ejecutarse en dispositivos que están sometidos a Jailbreak, debido a los riesgos de seguridad que plantea el Jailbreak. Barclay's US, una aplicación bancaria y de tarjetas de crédito, es un ejemplo de aplicación diseñada de este modo.

Si decide probar este método, instale aplicaciones, como Zelle, Payoneer o Barclay's, que estén diseñadas de esta manera (no importa si realmente tiene una cuenta con ellos; de hecho, si le preocupa que una persona agresora tenga acceso a su dispositivo, puede que no quiera iniciar sesión en sus cuentas financieras en ese dispositivo de cualquier manera). Después de instalarlas, intente abrirlas. Si recibe un mensaje de cualquiera de ellos diciendo que no se pueden ejecutar porque el dispositivo está en Jailbreak, eso significa que el dispositivo está sometido a Jailbreak.

Verificación de los dispositivos de transmisión (streaming)

Un dispositivo de transmisión o streaming, o reproductor multimedia de streaming, le permite transmitir películas, música u otros contenidos a su televisión, utilizando su red WiFi. Algunos ejemplos son Fire TV, Roku, Chromecast y Apple TV.

Si bien hay muchas opciones para los dispositivos de streaming, este recurso discute dos populares que son relativamente más fáciles de someter a Root. Si usted piensa elegir un nuevo dispositivo de streaming, considere seleccionar aquél que sea más difícil a someterse al Root.

Amazon FireStick (Fire TV Stick)

Para verificar si un Amazon FireStick podría estar sometido a Root, haga clic en el botón Configuración (el ícono que parece un engranaje, normalmente en la parte derecha de la pantalla). Vaya a "Mi Fire TV". *(My Fire TV).* Se abrirá una ventana con un menú. Si "Opciones de desarrollador" *(Developer Options)* es un elemento del menú, es posible que el FireStick esté sometido a Root. Esto no significa necesariamente que lo esté, porque activar las opciones de desarrollador es solamente un paso para hacer Root en un FireStick. Desde un principio, en la mayoría de los FireSticks, las opciones de desarrollador están desactivadas, y a menos que usted sea un desarrollador de aplicaciones para FireStick, hay pocas razones para tenerlas activadas. Si siente la seguridad de cómo hacerlo, puede desactivar las opciones de desarrollador haciendo clic en él, y luego girando el interruptor en la parte superior de la pantalla a la posición "*off*".

Roku

Antes era posible someter el Root en un dispositivo Roku, pero a partir de la primavera de 2021, una vez que Roku se enteró de esto, actualizó su sistema operativo, haciendo que ya no fuera posible hacer el Root. Sin embargo, si ha tenido un Roku desde antes de mayo de 2021 y no ha

actualizado su sistema operativo desde entonces, es posible que pueda ser sometido al Root. Para comprobarlo, intente actualizar cualquier aplicación que tenga instalada en el dispositivo, o descargue una nueva, utilizando la tienda Roku. Si no puede hacerlo, el Roku está sometido a Root. Si siente inseguridad para poder deshacer el Root, puede hacerlo con un restablecimiento de fábrica (esto borrará sus datos y preferencias personales, y desvinculará su cuenta del dispositivo - será como si acabara de recibirlo). Si quiere evitar que el dispositivo sea sometido a Root en el futuro, actualice su software.

Apoyado por US DOJ-OVW Subvención #15JOVW-21-GK-02255-MUMU. Las opiniones, resultados y conclusiones o recomendaciones expresadas son de los autores y no representan necesariamente los puntos de vista del Departamento de Justicia de los Estados Unidos.

Actualizamos nuestros materiales con frecuencia. Visite TechSafety.org para consultar la última versión de este y otros materiales.