CHECKING DEVICES FOR ROOTING OR JAILBREAKING

techsafety.org.au

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of January 2025.

If you are concerned about your device's privacy and security, it can be important to regularly check phones, tablets, and streaming devices to see whether they have been rooted or jailbroken.

"Rooted" means that someone has gained the ability to administer or manage the device's operating system. The operating system supports the device's basic functions and allows apps and programs to run. Rooting a device can compromise the operating system, making your phone less secure and more vulnerable to spyware and stalkerware.

"Jailbroken" means that someone has removed the limitations that the device's manufacturer put in place to keep the device secure. For example, jailbreaking makes it possible to install apps on an iPhone that do not come from the Apple Store, or to illegally download copyrighted content.

Before We Start: Prioritise Safety

Each survivor's situation and risks are different, and there isn't one "right" way to respond to an incident, only ways that do or don't fit your situation. Knowing how to check whether a device has been rooted or jailbroken can help you identify whether and brainstorm how an abusive person may have exploited that device, and plan which activities to do on which devices. Checking may be helpful, but won't ensure safety by itself. If an abusive person regularly monitors your devices and accounts, making changes may alert them. They may know that a device has been reset to factory settings or that an unauthorised app or app store has been deleted, and may be able to root or jailbreak it again, coerce or force you to give them access to the your settings, install spyware or stalkerware remotely, or escalate the abuse. In some situations, making changes could also erase evidence. Always prioritise safety and trust your instincts. You may find these safety steps useful:

- Use safer devices and accounts for sensitive conversations and activities. If you think that someone is monitoring your phone, computer, or accounts, use a different device (such as a library computer or a friend's phone) and an

account that the person cannot access (and that they have not had access to in the past). For more information about safer devices and accounts, see our resource on securing devices and accounts.

- Get more information. Navigating violence, abuse, and stalking can be difficult and dangerous. DFV practitioners can help you figure out options and local resources and help you create a plan for your safety. You can call 1800RESPECT on 1800 737 732 to be connected with local resources.

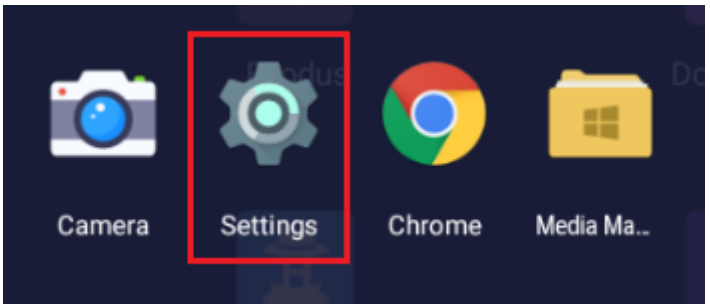
Checking Android Devices and Chromebooks

Rooting is a process, usually performed on Android devices to which someone has physical access, that gives someone administrator-level control of a device. With administrator-level control, that person can uninstall apps that were intended to be impossible to uninstall, change permissions on apps, disable the device's security features, and more.

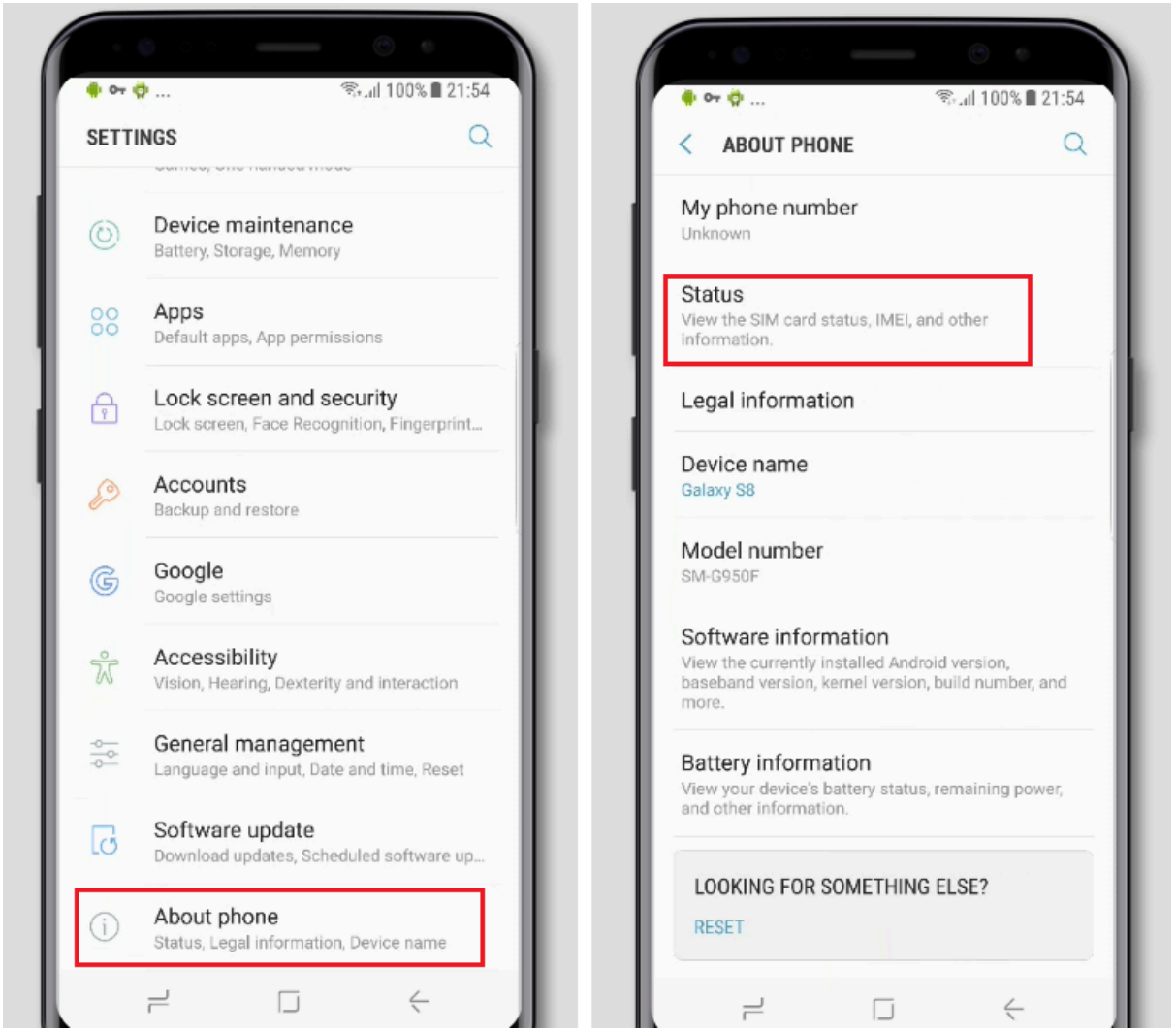
Android Devices

Android devices can be phones or tablets that use the Android operating system, such as Amazon Fire or Google Pixel C tablets. This section applies to any Android device.

Open the device's Settings, which is usually indicated by a gear icon.



Under settings, look for the "About Phone" option (below left image). Press "About Phone" and look for the "Status" item (the specific menus and options may vary depending on the device and version of Android). Try pressing the magnifying glass to search if you are having trouble finding it.

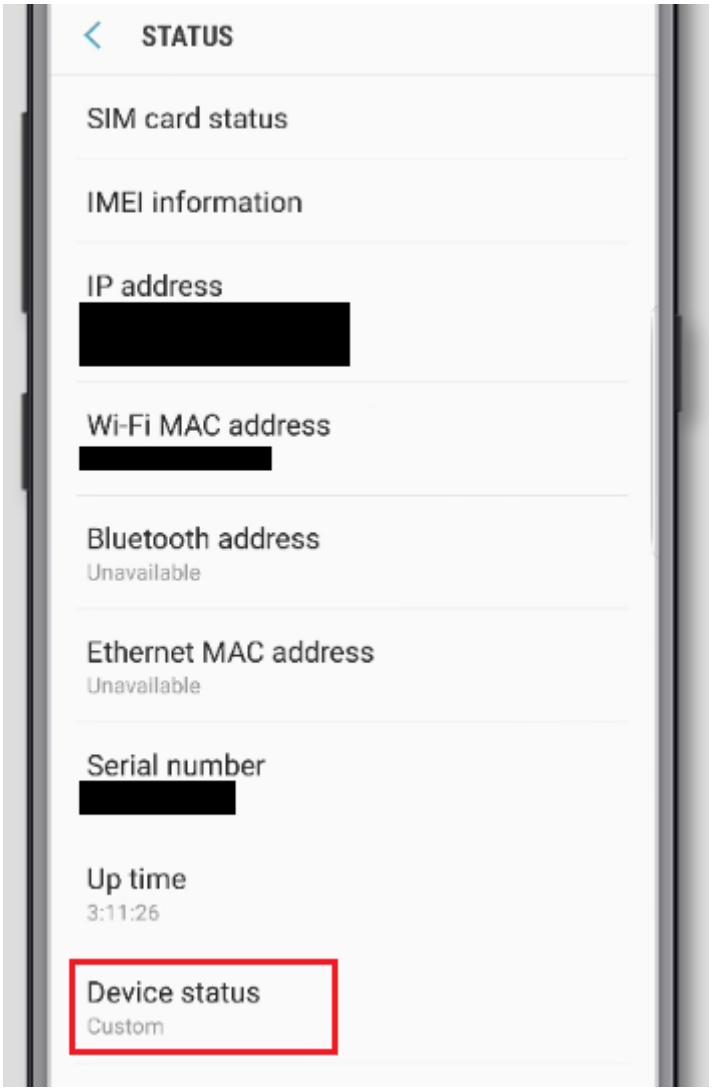


Once in the Status menu, scroll down until you find a "Device status" or "Phone status" item. If this is set to "Custom" – as shown in the below image – that means that your device may be rooted. If it says "Official" the phone has not been rooted.

Unfortunately, it is difficult to unroot a device on your own unless you have a lot of technical expertise. A factory reset will not unroot the device. You can take the device to a phone repair store and explain the problem, and they may be able to help you or refer you to someone who can. A representative from your carrier's store may also be able to help, but keep in mind that if your phone has been rooted it could void your phone's warranty.

If, and only if, you are comfortable trying something a little more advanced, you can install the SuperSU root management app through an APK (application) file, and use it to unroot the device (this could erase all of your files in the same way that a

factory reset would). This page explains how to install an APK. It is very important to be careful with this, because you could make your device less secure if it's done incorrectly. If you decide to go ahead, download and install the latest version of SuperSU on your device (do not install any apps claiming to be SuperSU through the Google Play Store, as they are not the real app and could be a security or privacy hazard, or just not work). Open SuperSU and press the Settings tab, then press "Full unroot" and then "Continue" when the dialogue box opens. If the app asks you whether to "Attempt to restore stock boot image?" or "Attempt to restore stock recovery image?" select yes. Once you are finished, restart the device.



ChromeOS Devices (Chromebooks)

Chromebooks use an operating system called ChromeOS. It is relatively easy to check whether a modern Chromebook is rooted, but be aware that either rooting it or unrooting it will delete all its files and accounts. If you decide to unroot a rooted Chromebook, you may want to first back up all files and accounts that you want to keep.

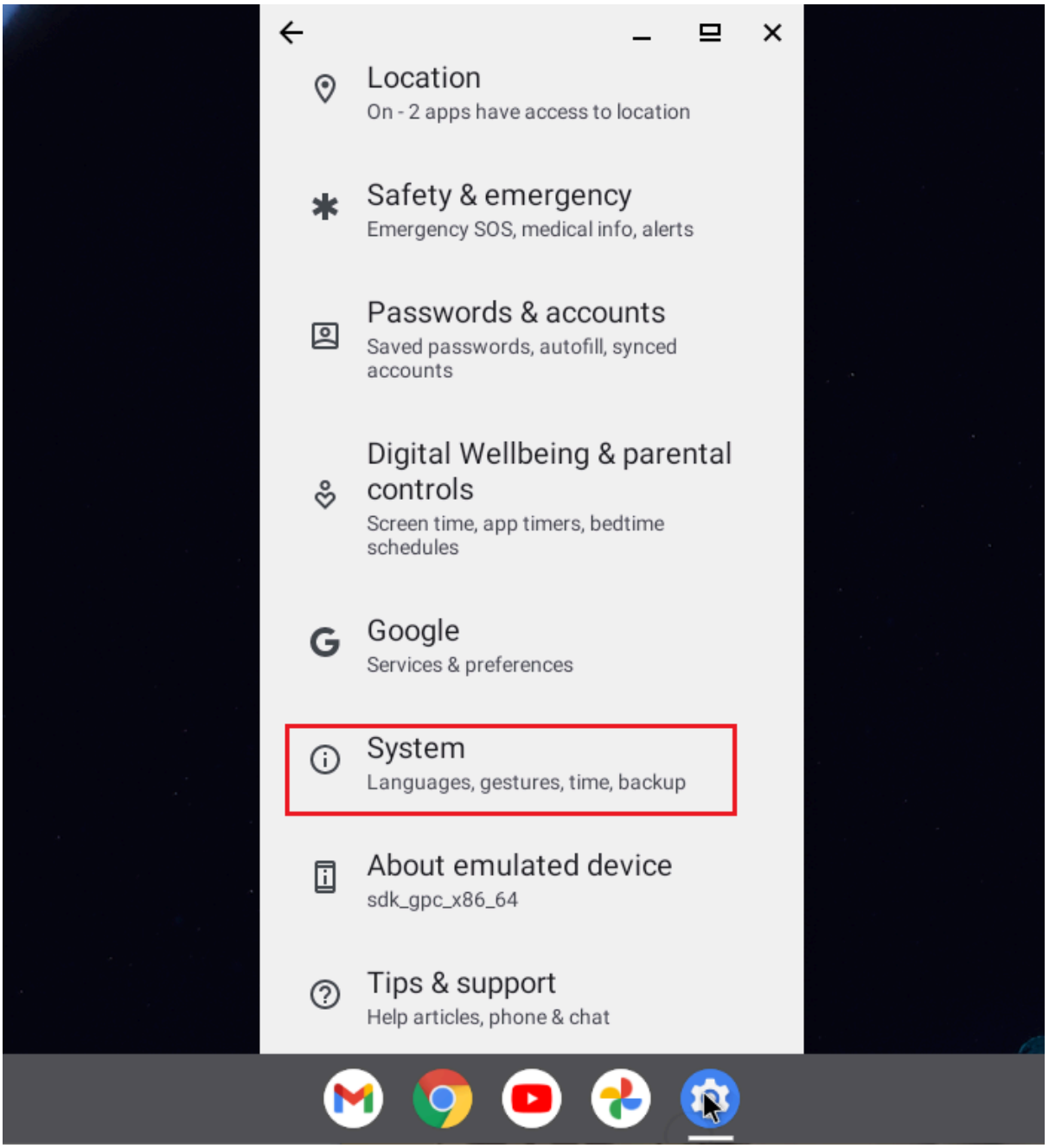
The below are indications that your Chromebook could be rooted:

- It beeps twice when you turn it on.
- It shows any sort of warning screen, instead of the normal startup screen, when you restart it.

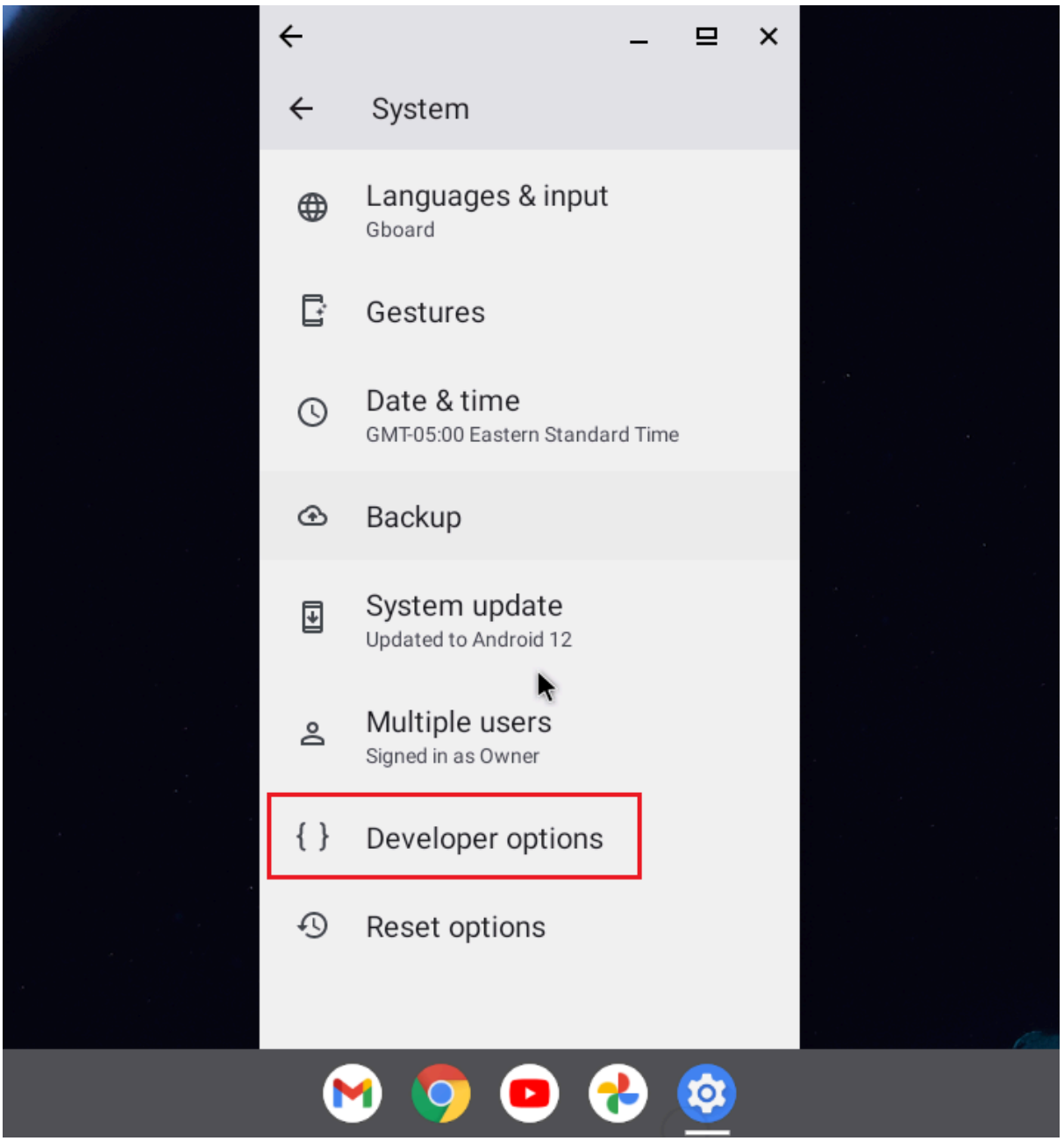
If the screen says "OS Verification is off: Press SPACE to re-enable," and you feel safe unrooting your device (remember this can delete all files), you can do so by pressing the space bar while this screen is showing.

If these things are not happening, your Chromebook could still be rooted. To root a Chromebook, the user must first enable "Developer options." You can easily check whether these are enabled, and disable them. Open Settings (a gear icon, shown in the red box in the image below).

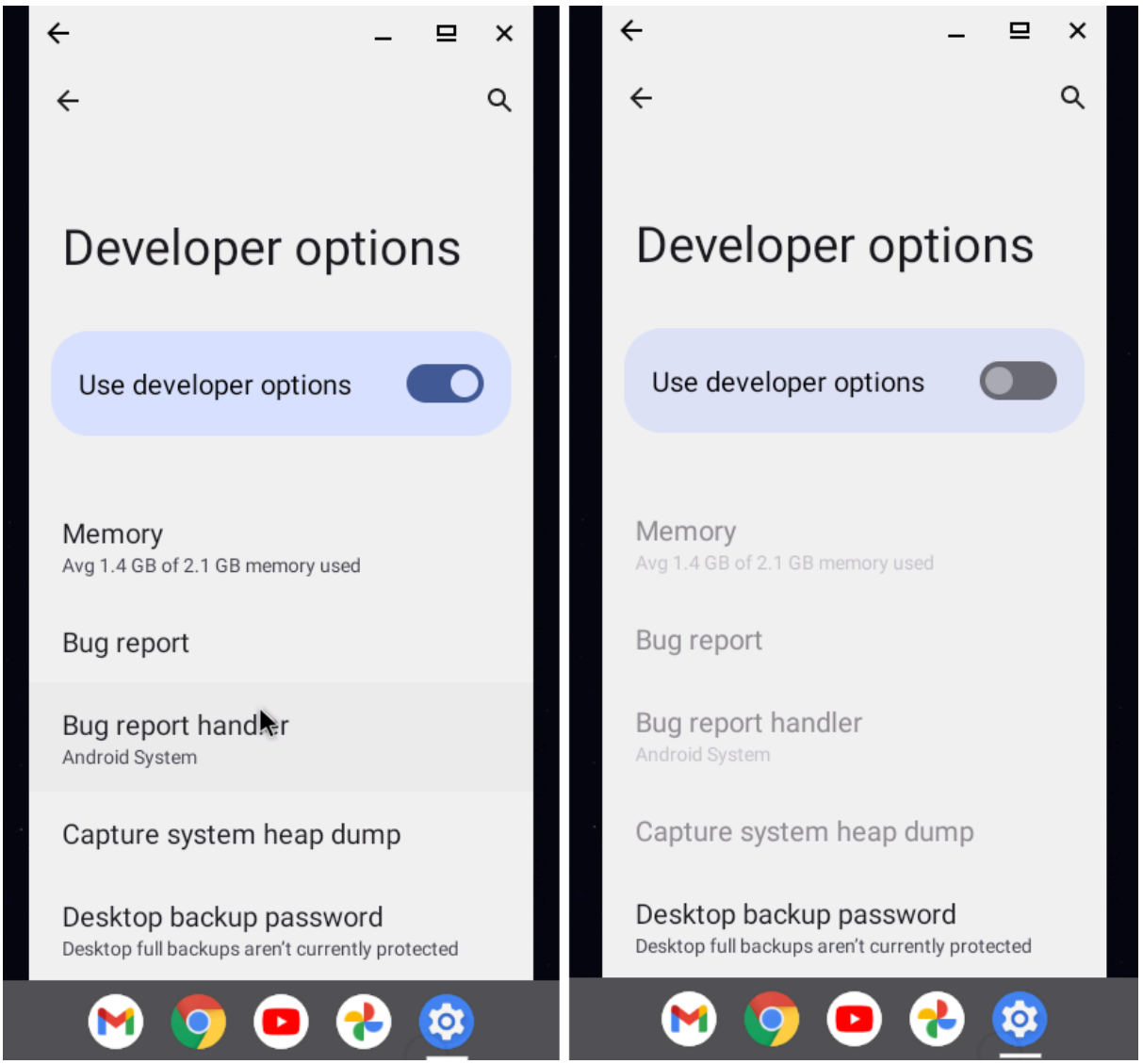
When you open the Settings app, it will display a menu. Scroll down to the Systems item, which is boxed in red in the image below, and press it.



This should display another menu. Scroll down the whole menu. If you see a "Developer options" item, the Chromebook may be rooted. Enabling Developer options is only one step required for the rooting process, but unless you are developing Chromebook apps, there is little reason to have it enabled.



If you feel safe disabling this feature, it is easy to do that with some Chromebooks, depending on the model. Try pressing "Developer options." If there is a switch labeled "Use developer options" (below left image) turn it to the "off" position (below right image). Once you leave the Developer options menu, it should disappear, which means that you have unrooted the Chromebook.



If you do not have an option to do this, and you believe the Chromebook is rooted because it beeped twice on startup but with no other indicators, or if you simply don't want to do this yourself, consider taking it to a repair store.

Checking iOS Devices for Jailbreaking

Finding out for sure whether an iOS device (iPhone or iPad) is jailbroken, may require help from a specialist. However, if you use both of the following two methods, you can detect most cases of jailbreaking.

Method 1: Look for Apps that Require Jailbreaking

You can use your device's search bar to search for apps that can only be installed on jailbroken iOS devices. The best-known is Cydia, an alternate app store, which someone could have installed on your device in order to install apps that Apple doesn't allow into their store. However, there are other popular apps that typically require jailbreaking, including AppCake, Frida, and PowerModule. The image below shows a search for Cydia that finds no results, meaning that Cydia is not installed on the phone. If you do find any of these apps, this indicates a jailbroken device.

NOTE: There are alternate app stores that do not require jailbreaking, so even if your device is not jailbroken, someone could still have installed an alternate app store in order to install apps onto your device that are not allowed by Apple.

Method 2: Run Jailbreak-Incompatible Apps

Some apps, especially in the financial sector, handle sensitive data and are developed by companies with strong security and legal compliance concerns. These apps are sometimes designed to not be able to run on jailbroken devices, because of the security risks posed by jailbreaking. Macquarie Mobile Banking is one example of a banking app which is designed this way.

If you choose to try this method, install apps, such as the Macquarie Banking app, Up- Easy Money, CommBank Banking App, We Money and Frollo, that are designed this way (it doesn't matter whether you actually have an account with them – in fact, if you are concerned about an abusive person having access to your device, you may not want to log into your financial accounts on that device anyway!). After you have installed them, try to open them. If you get a message from any of them saying that they can't be run because the device is jailbroken, that means that the device is jailbroken.

Checking Streaming Devices

A streaming device, or streaming media player, lets you stream movies, music, or other content, to your TV, using your WiFi network. Some examples include Fire TV, Roku, Chromecast, and Apple TV.

While there are many options for streaming devices, this resource discusses two popular ones that are relatively easier to root. If you are choosing a new streaming device, consider selecting one that is more difficult to root.

Amazon FireStick (Fire TV Stick)

To check whether an Amazon FireStick could be rooted, click the Settings button (the icon that looks like a gear, usually on the right side of your screen). Go to "My Fire TV." This will open a window with a menu. If "Developer options" is a menu item, the FireStick may be rooted. It does not necessarily mean that it has been, because turning on Developer options is only one step in rooting a FireStick. Developer options are disabled by default on most FireSticks, and unless you are a FireStick app developer, there is little reason to have them enabled. If you feel safe doing so, you can disable Developer options by clicking on it, and then turning the switch at the top of the screen to the "off" position.

Roku

It was possible to root a Roku device as of spring 2021. Once Roku learned about this, they updated the Roku operating system, making it no longer possible to root. However, if you have a Roku from May 2021 or earlier, and you have not updated its operating system since then, it is possible that it could be rooted. To check, try updating any app that you have installed on the device, or downloading a new one, using the Roku store. If you cannot do this, the Roku is rooted. If you feel safe unrooting it, you can do so with a factory reset (this will erase your data and personal preferences, and unlink your account from the device – it will be like you just got it). If you want to prevent any future rooting of the device, update its software.

Acknowledgement

This handout has been created by Wesnet under licence from the National Network to End Domestic Violence.