DEC 20, 2017 3:07 AM PT | JR Raphael

1: Make sure your Android device is encrypted

It's an inevitable moment in the smartphone-owning cycle, the point at which a newer, shinier model comes along and your trusty old device is no longer needed.

Maybe your company bought you a new Android phone. Maybe your old one was getting too slow. Or maybe you just love electronics and couldn't resist the lure of whatever sexy new Android device your favorite manufacturer started selling.

[Further reading: 20 Android tips and tricks you shouldn't miss from 2017]

Whatever the case, it's common nowadays to find yourself with an extra phone. And while there are plenty of practical uses for an old Android device, there's also a time when the best choice is to sell, donate, or otherwise pass it along.

Before you do so, though, you'll want to be sure you've securely erased it and removed any traces of your past – because the last thing you'd want is for your phone's new owner to resurface your personal or corporate data.

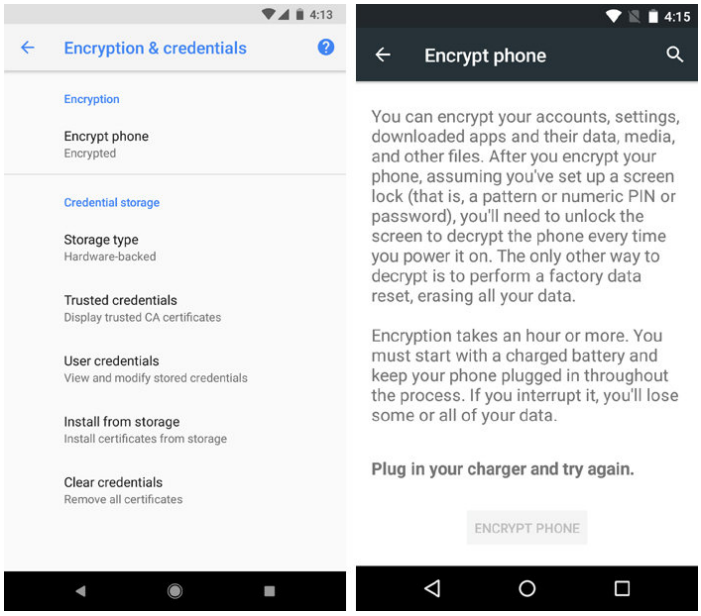
Follow the four steps below and you can let your Android device go without worry.

The biggest fear with wiping an Android device is the improbable but not *impossible* prospect of someone later using data recovery tools to find and assemble lingering bits of data.

That's why the first and most important step in securely erasing your Android device is to encrypt its local storage. That way, even if your phone makes its way into the hands of a shady character – and even if said scoundrel is able to recover the data you've erased – your sensitive info will remain virtually unreadable.

If your phone is relatively recent, there's a good chance it's already encrypted by default. But it's worth double-checking to make sure.

Head to the Security section of Android's system settings and look for the option labeled "Encryption." (The exact wording and placement may vary depending on your device's manufacturer and Android version, but it should be pretty easy to spot.) There, you'll be able to see if your phone is in fact already encrypted – and to start the encryption process if it isn't.



Google

The visuals will vary from one Android version to another, but your phone will either show you that it's encrypted or give you an option to encrypt it.

Be warned that the actual encryption process may take a while, and you won't be able to use your device while the process is under way. Once it's done, though, you can rest easy knowing your data has a powerful layer of protection from prying eyes in the unlikely event that it's even recovered.

2: Remove your SIM card and any storage cards

Now that your data is secure, take a moment to confirm that your carrier-issued SIM card and any external memory cards are removed from your device. (Not many devices have SD card slots these days, so don't fret if you don’t find one.)

Both cards can be tied to your identity and filled with private data, and there's no reason to keep either of them in a device that’s leaving your possession.

3: Perform a factory reset to fully erase your device

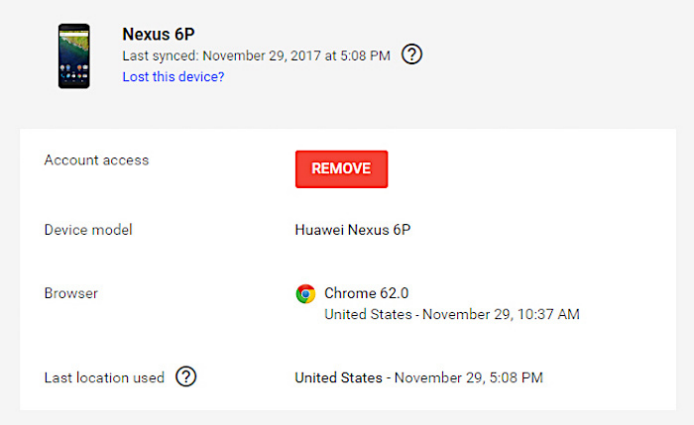
This part is the actual wipe of your Android phone: Go back into the system settings and look for a section called "Backup & reset." If you don't see that, try opening the System section and *then* look for either "Backup & reset" or just "Reset."

Find and select the option to perform a factory data reset and select any subsequent options to erase all types of data and accounts. The system will likely give you a confirmation screen or two and then ask you to input your PIN, pattern, or password for protection. Complete all those tasks, then sit back and wait while Android does its work.

4: Remove any remaining account associations

Last but not least, take a moment to manually remove the phone from your Google account and any other accounts that might be associated with it.

For Google, just visit this page, find the device in the list, then click it and click the red "REMOVE" button that appears. That'll ensure your Google account has no lingering connection to it.



Google

Severing the connection between a phone and your accounts is a smart final step to take.

Think through any other services that might have similar options – password managers like 1Password, Dashlane or LastPass, for instance, or multi-device authentication apps like Authy – and sign into their respective websites to sever any remaining connections.

And with that, you're all set: Your Android phone is securely erased and ready to move onto its new life.

Viewed using Just Read