Written by **C. Mitchell Shaw** on August 17, 2015

How to Securely Remove All Data From Your Mobile Phone

Are you thinking about recycling or selling your old mobile phone? It's a good idea; but there are some serious security concerns you need to be aware of first.

Whether you are recycling, selling, or giving your phone away, you need to make sure that *all* personal data is securely removed first. Simply deleting the information on the phone will not remove the data securely enough. Even factory resetting the phone may not do the job. Time after time, security experts have shown that the data removed by deleting and factory resetting is still easily recoverable using simple software that anyone can get and use. Easy-to-use tools such as PhotoRec can recover deleted personal information in just a few steps.

This writer personally used PhotoRec to recover all the files and folders on a 1TB hard drive after mistakenly deleting all partitions and formatting the wrong drive. It took awhile because of the size of the drive, but eventually everything was recovered.

Imagine someone using that software to recover your photos, videos, address book, login information, and other personal items stored on your phone. These days users do everything on their phones: surf the web, pay bills online, take pictures and videos, use GPS to navigate, create and view documents, update their calendars, maintain their address books and social media accounts, and much, much more. The information someone could get would include all types of personally identifiable data that could be used to steal your identity, or worse.

In keeping with the trend of government being the most expensive, least efficient way to get anything done, the Federal Trade Commission (FTC) maintains a website page to advise citizens about how to to securely wipe the data on their devices before passing them along. The FTC's advice for phones? Factory reset your phone and remove the SD and SIM cards. According to the FTC website:

> First, try to use the factory reset. Many devices allow you to "wipe" your device and clear nearly all the information in its memory. Sometimes, this is called a "hard reset," or "factory reset." You may be able to save or transfer the information to your new device before you delete it from your old one. For detailed instructions on how to "wipe" your device, read your owner's manual or check the website of your mobile provider or the device manufacturer.
>
> Second, remove or erase SIM and SD cards. Many mobile devices store information on a SIM card or an external SD card as well as in the device's internal memory. If you're keeping your phone number, ask your mobile provider about transferring your SIM card to your new device. SD cards often contain photos and other sensitive information. Even when you "wipe" your device, your SIM card or SD cards may retain information about you. Remove them from your device or delete the

data that's stored on them.

Then, they say, you have a "clean" phone. It's to be hoped that the federal government isn't taking its own advice. While not totally off the mark, this assesment leaves out some vital information.

So what *is* the proper method for securely removing all data from your phone? It varies depending on your platform. One thing is the same, though: The methods outlined below will leave your phone as an amnesiac. It won't remember you or anything about you, so make sure you do a backup of all your data before you begin.

iPhone or iPad

Actually, if you are using an iPhone, the FTC is pretty accurate in its assessment. This is because Apple uses an encrypted file system to store all data on the iPhone's internal storage. By following the proper steps to factory reset the phone, the hardware-specific encryption key is securely wiped. Since this hardware-specific encryption key is only stored on the device, the data that is left is encrypted, but the key to decrypt it is lost. This leaves the data in a state that is unreadable. Even forensic software would be highly unlikely to ever recover the data.

To do this, choose "Settings," then "General," click "Reset," and choose "Erase all Content and Settings." It may take awhile depending on your model, which version of iOS you are running, and the amount of data on your device. When it is done, set your phone up again with a new long, random password. Write the password down in case you are interrupted and need to complete this later. Then, factory reset the device again. This will bury your data behind two layers of encryption. Once it finishes the second time, you're done. You can try to recover the data using PhotoRec or some similar tool, but you should be unable to see anything. Now destroy the password you wrote down. Your phone is ready to sell or donate.

Android Phone or Tablet

Android makes it a little harder, but the idea is exactly the same. You need to bury your data behind broken encryption. First, do a factory reset. Each manufacturer puts this in a different place in your settings, but it is typically found under a heading such as "Backup and Reset" under security. If you can't find it, do an Internet search for where it is on your particular model. Once you find it, click "Factory Reset" or "Factory Data Reset." Next, click all the options for erasing stored content and formatting SD card (if you have an SD card in the device). Then, click "Reset Device." You may receive one final warning that this will erase everything. Accept the warning and proceed to erase the device data.

Now, set the phone up again without setting up a Google account. Then set up a password for your lock screen. Make it long and random. Write it down. You won't keep it long. Next, depending on which version of Android you use, look in your settings for security and click on "Encrypt Device" or something similar. Again you may need to search the web for the location of this setting.

Once you click on "Encrypt Device," you will see a warning that your phone has to be fully charged and plugged in. Plug it in and charge it fully. Go through all the steps to fully encrypt your phone. It may take awhile. Do not interrupt it or unplug it during this process.

When it is finished, restart the phone and log in using the password that you created earlier. Do a factory reset and do not set the phone back up. That's it. Your data is buried beneath a layer of encryption that was formatted during the second factory reset. If you had really important or sensitive

data on the phone, repeat this process again. Or again and again, if you want to and have the time. Just use a different password each time and destroy all the passwords when you're done.

If you set your new Android device up with encryption right from the beginning, it will be much more secure and you can skip that step when wiping it in the future.

Just as with the iPhone, if you want to test the effectiveness of this process, you can download PhotoRec or a similar program, plug your phone in, and run the software. You should not be able to recover anything other than files that are part of the OS. Your personal data simply doesn't exist anymore. Even if you formatted your SD card, you should remove it — not sell or donate it with the phone unless you know how to securely wipe it, as well.

Photo of iphone: Kelvinsong