OUCH! December 2022

OUCH!

The Monthly Security Awareness Newsletter for You

SANS SECURITY AWARENESS

Disposing of Your Mobile Device

Overview

Mobile devices, such as smartphones, smart watches, and tablets, continue to advance and innovate at an astonishing rate. As a result, you may be replacing a new device as often as every year. Unfortunately, you may not realize just how much personal data are on your devices — far more than your computer. Below we cover the different types of data on your mobile devices and how you can securely wipe your device before disposing or replacing it. If your mobile device was issued to you by work, check with your supervisor about disposal procedures first.

Your Information

Your mobile devices store more sensitive data than you realize, to include . . .

Where you live and work, and your daily travel habits.
The contact details for everyone in your address book, including family, friends, and co-workers.
Phone call history including inbound, outbound, voicemail, and missed calls.
Texting or chat sessions within applications like secure chat, games, and social media.
Personal photos, videos, and audio recordings.
Stored passwords and access to your accounts, such as your bank, social media, or email.
Health related information, including your age, heart rate, or exercise history.
Financial information including credit cards, payment methods, and transactions.

Erasing Your Device

Regardless of how you dispose of your mobile device, such as donating it, exchanging it for a new one, giving it to someone, reselling it, or even recycling it, first erase all of your sensitive information. Do not assume that the next owner will “do the right thing.” The first step is to back up your device so you can recover and transfer all your data and settings to your new device. Once backed up, you will want to reset your device, as this wipes your data and resets it to factory default. During the reset process you may be prompted to enter your cloud password to break any links with that device to the Cloud; be sure to do this. The reset steps below are for the two most common devices — Apple and Android.

Apple iOS Devices: Settings | General | Transfer or Reset | Erase All Content and Settings.

Android Devices: Settings | System | Reset Options | Erase All Data (these options vary depending on your device manufacturer).

SIM & External Cards

In addition to resetting your device, also consider what to do with your SIM (Subscriber Identity Module) card. This is the little card in your phone issued to you by your phone carrier; it's what identifies your device and enables it to make a cellular or data connection. When you wipe your device, the SIM card retains information about your account and is tied to you. If you are keeping your phone number and moving to a new device, talk to your phone service provider about transferring your SIM card. If this is not possible, keep your old SIM card and physically destroy it. Many of today's modern smartphones having something called an eSIM, which is a virtual SIM card as opposed to a physical SIM. The eSIM is wiped during the reset process.

Finally, some Android mobile devices utilize a removable SD (Secure Digital) card for additional storage. Remove these external storage cards from your mobile device prior to disposal. These cards can often be re-used in new mobile devices, or can be used as generic storage on your computer with a USB adapter. If reusing your SD card is not possible, then just like your old SIM card, we recommend you physically destroy it.

If you are not sure about any of the steps covered above, or if your device reset options are different, take your mobile device to the store from which you bought it from and get help. Finally, if you are throwing a device away, consider donating it instead. There are many excellent charitable organizations that accept used mobile devices, and many mobile providers have drop-off bins in their stores to recycle them.

Guest Editor

Heather Mahalik (@HeatherMahalik) Is the Sr. Dir of Digital Intelligence at Cellebrite and SANS DFIR Curriculum Lead, FOR585 Author and Faculty Fellow Instructor at SANS. Heather's career has been based upon forensic research and 20 years of case work.
She blogs at www.smarterforensics.com/blog.

Resources

Securely Using Mobile Apps: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Securing Your Mobile Devices: https://www.sans.org/newsletters/ouch/securing-mobile-devices/
Donating Your Cellphone: https://www.makeuseof.com/best-places-to-donate-your-old-phone/
SANS Course: Advanced Smartphone Forensics Course: https://sans.org/for585