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, some people replace their mobile devices as frequently as every year. Unfortunately, people often do not realize how much personal data is on these devices. Below we cover what may be on your mobile device and how you should securely wipe it before disposing of it. If your mobile device was issued to you by your employer, or has any work data stored on it, be sure to check with your supervisor about proper backup and disposal procedures first.

Your Information

Mobile devices store more sensitive data than many people realize, often far more than your computer, including:

- **Where you live, work, and places you visit**
- **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**
- **Web browsing history, search history, cookies, and cached pages**
- **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, exercise history, or blood pressure**

Wiping Your Device

Regardless of how you dispose of your mobile device, such as donating it, exchanging it for a new one, giving it to another family member, reselling it, or even throwing it out, you need to be sure you first erase all that sensitive information. Simply deleting data is not enough, instead you should securely erase all the data on your device. The easiest way to do this is to reset your device. The reset function varies among devices; listed below are the steps for the two most common devices. An even more secure step is to make sure you have encryption enabled on your device before resetting it. On most recent mobile devices, the easiest way to do this is to simply enable a screen lock (which hopefully you have enabled already). Finally, we highly recommend you backup your device before resetting it.

- Apple iOS Devices: Settings | General | Reset | Erase All Content and Settings
- Android Devices: Settings | Privacy | Factory Data Reset

SIM & External Cards

In addition to your device, you also need to consider what to do with your SIM (Subscriber Identity Module) card. A SIM card is what a mobile device uses 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 to prevent someone else from reusing it to impersonate you and gain access to your information or accounts. 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 reused 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 you bought it from and get help from a trained technician. 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.

Subscribe to OUCH! and receive the latest security tips in your email every month - www.sans.org/security-awareness/ouch-newsletter.

Guest Editor

Christopher Crowley *(@CCrowMontance) is an independent consultant in the Washington, DC area, focusing on security operations. He tweets and blogs occasionally. Keep an eye out for his forthcoming book on Security Operations Centers. He's a Senior Instructor at the SANS Institute.*

Resources

SANS Course:	https://sans.org/sec575
SANS Course:	https://sans.org/for585
FTC Advice on Disposing Your Mobile Device:	https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device

OUCH! is published by SANS Security Awareness and is distributed under the Creative Commons BY-NC-ND 4.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley