OUCH! | December 2016

The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- Your Information
- Wiping Your Device
- SIM & External Cards

Securely Disposing of Your Mobile Device

Overview

Mobile devices, such as smartphones, smartwatches, and tablets, continue to advance and innovate at an astonishing rate. As a result, some people replace their mobile devices as often as every year. Unfortunately, too many people dispose of their devices with little thought on just how much personal data is on them. In this newsletter we will cover what types of personal information may be on your mobile device and how you can securely wipe it before disposing or returning it. If your mobile device was issued to you by your employer or has any organizational data stored on it, be sure to check with your supervisor about proper backup and disposal procedures before following the steps below.

Guest Editor

Heather Mahalik (**@HeatherMahalik**; **+HMahalik**) is a Principal Forensic Scientist leading the forensics effort for ManTech CARD. She is the course lead and co-author for the SANS Institute course Advanced Smartphone Forensics (FOR585) and instructor for Windows Forensic Analysis (FOR408). She blogs at **smarterforensics.com**.

Your Information

Mobile devices store far more sensitive data than you may realize, oftentimes more than even your computer. Typical information can include:

- Where you live, work, and places you frequently visit
- The contact details for everyone in your address book and applications, including family, friends, and coworkers
- Call history, including inbound, outbound, and missed calls
- SMS (texting), voice, and multimedia messages
- Chat sessions within applications like secure chat, games, and social media
- Location history based on GPS coordinates or cell tower history
- Web browsing history, search history, cookies, and cached pages
- Personal photos, videos, audio recordings, and emails
- Stored passwords and access to personal accounts, such as your online bank or email
- Access to photos, files, or information stored in the Cloud
- Any health-related information, including your age, heart rate, blood pressure, or diet

Securely Disposing of Your Mobile Device

Wiping Your Device

As you can see, there is most likely a tremendous amount of sensitive information on your mobile 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 of that sensitive information. You may not realize it, but simply deleting data is not enough; it can easily be recovered using free tools found on the Internet. Instead, you need to securely erase all the data on your device, which is called wiping. This actually overwrites the information, ensuring it cannot be recovered or rendering it unrecoverable. Remember, before you wipe all of your data, you most likely want to back it up first. This way, you can easily rebuild your new device.

When disposing of your mobile device, be sure to do a factory reset and remove the SIM and any SD cards if your device has them.

The easiest way to securely wipe your device is use its "factory reset" function. This will return the device to the condition it was in when you first bought it. We have found that factory reset will provide the most secure and simplest method for removing data from your mobile device. The factory reset function varies among devices; listed below are the steps for the two most popular devices:

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

Unfortunately, removing personal data from Windows Phone devices is not as simple as a factory reset. More research is being conducted on methods to ensure your personal data is wiped from the device. If you still have questions about how to do a factory reset, check your owner's manual or manufacturer's website. Remember, simply deleting your personal data is not enough, as it can be easily recovered.

SIM & External Cards

In addition to the data stored on 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 perform a factory reset on your device, the SIM card retains information about your account and is tied to you, the user. If you are keeping

Securely Disposing of Your Mobile Device

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, for example, if your new phone uses a different size SIM card, keep your old SIM card and physically shred or destroy it to prevent someone else from re-using it.

Finally, some mobile devices utilize a separate SD (Secure Digital) card for additional storage. These storage cards often contain pictures, smartphone applications, and other sensitive content. Remember to remove any external storage cards from your mobile device prior to disposal. (For some devices, your SD cards may be hidden in the battery compartment of your device, possibly beneath the battery.) 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 in this newsletter, take your mobile device to the store you bought it from and get help from a trained technician. Finally, if you are throwing your mobile device away, we ask you to consider donating it instead. There are many excellent charitable organizations that accept used mobile devices.

Security Awareness Training for Developers

Ensure your team can properly build defensible applications from the start by conducting security awareness training for developers, architects, managers, testers, business owners, and partners. https://securingthehuman.sans.org/u/nwb

Resources

Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Backup and Recovery:	https://securingthehuman.sans.org/ouch/2015#august2015
Advanced Smartphone Forensics Course:	https://sans.org/for585
OUCH! Newsletter Archives:	https://securingthehuman.sans.org/ouch/archives

License