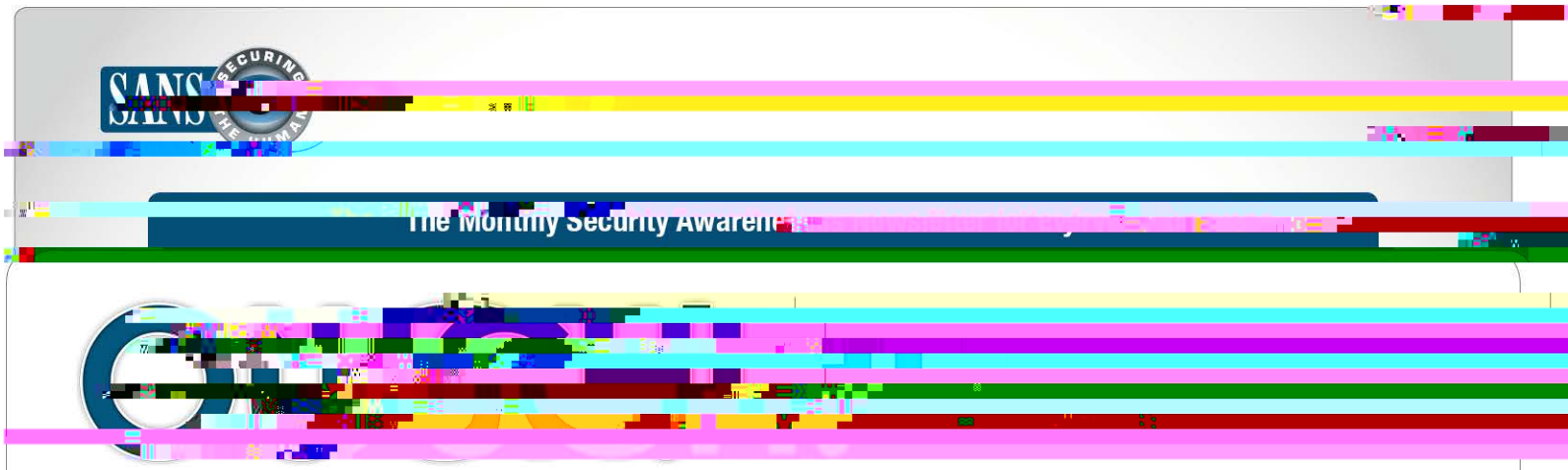

Overview

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

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
-
- 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
-

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 ýrst 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 ýrst. 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 ýrst 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

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