OUCH! | June 2014

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- Your Information
- Wiping Your Device
- SIM / External Storage Cards

Disposing of Your Mobile Device

Overview

Mobile devices, such as smartphones and tablets, continue to advance and innovate at an astonishing rate. As a result, many of us replace our mobile devices as often as every 18 months. Unfortunately, too many people simply dispose of their older mobile devices with little thought on just how much personal data their devices have accumulated. 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 of it 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

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) is a consultant based in the Washington, DC area. He is the lead instructor for the SANS Institute course Mobile Device Security and Ethical Hacking (SEC575) and an author of Incident Response Team Management (MGT535).

Your Personal Information

Mobile devices store far more sensitive data than you may realize, most likely even more than your computer does. Typical information stored by a mobile device can include:

- Where you live, work and places you frequently visit
- The contact details for everyone in your address book, including family, friends and coworkers
- Call history, including inbound, outbound and missed calls
- Text and voice messages
- Chat sessions within applications like games and social media
- Location history based on GPS coordinates or cell tower history
- Web browsing history, cookies and cached pages
- Personal photos, videos, audio recordings and email
- 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 heart rate, blood pressure or diet

Disposing of Your Mobile Device

Wiping Your Device

As you can see, there may be a tremendous amount of sensitive information on your mobile device. Regardless of how you dispose of your mobile device, such as donating it, giving it to another family member, reselling it or even throwing it out, you need to be sure that you first erase all of your sensitive information. In addition, you need to erase your information if you are returning your mobile device or exchanging it for a new one. If you do not, whoever ends up with your mobile device may be able to easily access it. However, before you begin wiping your data, you most likely need to backup all of your data, including photos, videos, or any other information. Once you wipe your device, you will not be able to recover any of your data stored on it.

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

Once you have backed up your data, you then need to securely erase it. Simply deleting files, photos or data is not enough. Data that has been deleted can be easily recovered using free tools found on the Internet. Instead, you want to securely erase all the data on the device, which is called wiping. This actually overwrites the information, ensuring it cannot be recovered. The easiest way to do this is to use your device's "factory reset" function. This will return it to the condition it was in when you first bought it. We have found that a 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 three most popular devices:

- Apple iOS Devices: Settings | General | Reset | Erase All Content and Settings
- Android Devices: Settings | Privacy | Factory Data Reset
- Windows Phones: Settings | About | Reset Your Phone

If you still have questions about how to do a factory reset, check your owner's manual or manufacturer's website. Remember that 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 phone or data connection. When you perform a factory reset on your device, the SIM card retains information about your account. If you are keeping your phone number and moving to a new device, talk to the phone salesperson about transferring your SIM card. If this is not possible (for

Disposing of Your Mobile Device

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 reusing it.

Finally, some mobile devices utilize a separate SD (Secure Digital) card for additional storage. These storage cards often contain pictures, smart phone 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 as generic storage on your computer with a USB adapter. If reusing your SD card is not possible, then we recommend you physically destroy it, just like your old SIM card.

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 that you consider donating it instead. There are many excellent charitable organizations that accept used mobile devices.

SANS Security Awareness Summit - 10 Sep, Dallas TX

Attend the SANS Security Awareness Summit & Training premier event in Dallas on September 10th, 2014. It is the only event that combines hands-on classroom training with discussions amongst the most innovative minds in the Security Awareness industry. Choose from 5 training classes and add on the one-day action-packed Summit that will help you build your next generation security awareness program. Register and learn more:
http://www.sans.org/event/security-awareness-summit-and-training-2014

Resources

NIST SP800-88 Rev. 1:	http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf
OUCH! Backups:	http://www.securingthehuman.org/ouch/2013#september2013
Common Security Terms::	http://www.securingthehuman.org/resources/security-terms

License