UTHSC G.U.A.R.D.

April 2017

Protect Yourself and Your Identity

by Valerie Vogel, Educause

Identity theft is a real threat; it can happen to anyone, and it can be challenging for victims to deal with the fallout.

According to the US Department of Justice, more than 17 million Americans were victims of identity theft in 2014. EDUCAUSE research shows that 21 percent of respondents to the annual ECAR student study have had an online account hacked, and 14 percent have had a computer, tablet, or smartphone stolen. Online fraud is an ongoing risk. The following tips can help you prevent identity theft.

- Read your credit card, bank, and pay statements carefully each month.
- Review your health insurance plan statements and claims.
- Shred it! Shred any documents with personal, financial, or medical information before you throw them away.
- If a request for your personal info doesn't feel right, do not feel obligated to respond! Legitimate companies won't ask for personal information such as your social security number, password, or account number in a pop-up ad, e-mail, text, or unsolicited phone call.
- Limit the personal information you share on social media.
- Put a password on it. Protect your online accounts and mobile devices with strong, unique passwords or passphrases.
- Limit use of public Wi-Fi. Be careful when using free Wi-Fi, which may not be secure.
- Secure your devices. Encrypt your hard drive, use a VPN, and ensure that your systems, apps, antivirus software, and plug-ins are up-to-date.

If you become a victim of identity theft:

- File a report with the US Federal Trade Commission at IdentityTheft.gov.
- Use the identity theft report to file a police report. Make sure you keep a copy of both reports in a safe place.
- Flag your credit reports by contacting the fraud departments of any one of the three major credit bureaus: **Equifax** (800-525-6285), **Experian** (888-397-3742), or **TransUnion** (800-680-7289).

IN THIS ISSUE

Securely Disposing of Your Mobile Device

by Heather Mahalik, Guest Editor for the SANS Institute

Mobile devices, such as smartphones, smartwatches and tables 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.

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

- Where you live, work and places you frequently visit
- 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

As you can see, there is most likely a tremendous amount of sensitive information on your mobile device. Regardless of how you dispose of it, 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 devise, 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.

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. Factory reset will provide the most secure and simplest method of 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

For any information security concerns, contact the Information Security Team at itsecurity@uthsc.edu or (901)-448-1579.