

The Mosby Agency

Protection | Privacy | Education | Investigation

Cell Phones: The Little Device with a BIG Risk

This workshop discusses the potential risks of cell phone usage and popular phone apps. Everyone will leave the class knowing more about how apps, advertisers and cell phone companies exploit the data you use every day on your phone. We will review “best practices” for privacy settings and discuss some of the best and worst apps for protecting your personal information. Bring your cell phones because we will be making some quick, on the spot changes so you can leave Dare to Grow Texas feeling more secure.

Terms & Conditions:

We live in a world of instant gratification. When we download a new app to our smart phones most of us automatically click accept so we can begin using fun new filters or play that new popular game. Rarely do we stop to think about or read the terms and conditions for each app we have on our phone. Why would we? Developers and their legal teams purposefully use confusing and ambiguous language to dissuade consumers from researching what they are agreeing to. A consumer watchdog group recently tested how long it would take someone to read all the terms and conditions for some of the most popular smart phone apps. In total, there were over 900 pages of documents to read and it took over 31 hours to complete.

This workshop will highlight and decode language from the terms and conditions of some of the most popular apps. As a sample:

“_____ may also collect and gather user contents (e.g. photos, screenshots, comments, and other materials) that you create on the Service. Your photos can be captured by other users and if they use the capture function provided by _____, those photos will be stored and used for _____ and 3rd party’s service (eg, Facebook).”

“We may share user content and your information (including but not limited to, information from cookies, log files, device identifiers, location data, and usage data) with businesses that are legally part of the same group of companies that _____ is part of, of that become part of that group.”

Bluetooth, Sync, and the Internet of Things:

As more and more devices are requiring Wi-Fi connections we are at a higher risk for exploitation. The second half of this workshop will discuss the potential risks of every day devices and security systems. I will demonstrate how hackers are able to gain access to your devices, what they do once they have gained access, and how to stop them.

Common Devices that can be exploited:

Wi-Fi enabled home security cameras

Phones, Tablets, E-readers that automatically sync to your home network

Smart TVs

Amazon Firestick & Roku

Smart Fridges

The Mosby Agency aims to provide interactive workshops that ensure every participant leaves with the knowledge of how to remain safe while using their smart phones and internet connected devices. The goal is to provide easy to understand information that can then be passed along to friends and family.

Be sure to follow The Mosby Agency on LinkedIn, Twitter and Facebook to stay up-to-date on course offerings, tech trends and cyber security!

Website: www.mosbyagency.com

LinkedIn: www.linkedin.com/company-beta/19396911/

Facebook: www.facebook.com/mosbyagency

Twitter: [@mosbyagency](https://twitter.com/mosbyagency)