IT Risk Bulletin

The University of Alabama System

A joint publication of the UA, UAB, UAB Health System, and UAH Chief Information Security Officers and The University of Alabama System

Summer 2015 Issue No. 8

FOR MORE INFORMATION:

ASHLEY EWING
Information Security Officer
UA
205-348-6524
aewing@ua.edu

CHIEF INFORMATION SECURITY OFFICER
UAB
205-975-3117
CISO@uab.edu

CHIEF INFORMATION SECURITY OFFICER
UAB Health System
205-996-3328
CISO@uabmc.edu

RUSS WARD
Chief Information Security Officer
UAH
256-824-2623
ciso@uah.edu

CHAD TINDOL
Director of Risk Management
UA System
205-348-5889
ctindol@uasystem.ua.edu

MURIEL FOSTER
Director of IT Audit
Office of Internal Audit, UA System
205-934-4105
mjfoster2@uasystem.ua.edu

To access current and past IT Risk Bulletins, go to the "Office of Risk Management" page on www.uasystem.ua.edu.

Are Those Apps Safe?

These days, the assumed answer to every inconvenience or obstacle in life is **"there's an app for that."** Some are work-related, but many are personal. How safe are these apps when they have access to so much personal or work information on our devices? And how does that fit our risk tolerance? According to a recent report by McAfee:

- 80% of apps collect your location
- 82% of apps track something
- 57% of apps track when you use your devices
- 36% of apps know your account information

Here are a few tips to safely using your next app:

1. **If you don't want your location shared by an app, you must turn off location services under Privacy Settings.** Location services are required by many apps to provide you with location-specific data such as maps, and store details. However, your location may also be shared with advertisers.

2. **Before downloading an app, pay attention to the disclosures about personal information that can be accessed by the app, e.g. location of the device, or contacts.** The developer should be clear about this. If not, that may be a red flag.

3. **Always update your apps.** Many app updates contain security patches that will prevent your information from being accessed by malware.

4. **Be careful when reading app reviews to decide on whether to download.** Some app developers may pose as consumers and write positive reviews to persuade you to download their app.

For more information on mobile security for consumers:

- "Who's Watching You: McAfee Mobile Security Report" (Feb 2014).
- Twitter accounts: EduCause and EdTech Higher Ed.

Sources:

- "Understanding Mobile Apps," Federal Trade Commission Consumer Information.