Privacy and Location Settings: They Know Your Every Move.

by The UTHSC Information Security Team

Where are you going? Where did you come from? Where do you live? What’s your most favorite restaurant? Where do you work? Where do you pick up your prescription? All of those questions can, not only, be answered by you, but by your mobile device or smartphone.

Privacy and location settings, natively located in your smartphone or mobile device or downloaded application may have the ability to track you 24/7/365. It tracks and stores your travel log daily. How does it know you are at home? Well, when you arrive at a destination and are there overnight based on your time zone more often, the app makes a calculated assumption that this is the place you rest your head, your home. It creates other frequently visited places using similar patterns; the same with you job.

Wondering how to ensure your privacy is unknowingly violating. Following this Privacy Checkup tips:

- Only turn on your location settings when using navigation system. You may turn it off when you arrive to your destination.
- Conduct a weekly Privacy Checkup on all of your apps and online social media networking sites like Facebook, Instagram, and Twitter.
- Be reminded that many apps must have access to your location in order to perform like Yik Yak and Shopkick.
- Instead of allowing an application to access your location, enter the closest zip code to satisfy location settings.
- Always read and review Privacy Statements and other information before downloading an app or signing up for a site. Some applications may be able to access information stored or cached on your device like your credit card number or other private data.

They Know Your Every Move...
In this article you’ll discover how to adjust the privacy settings on your social media sites and your devices, so you share only what you want with the people you want.

In this article, we will discuss the dangers of voluntarily uploading pictures and information online and how to use online social and professional networking more safely.
Google™ Yourself Today!

by Jessica McMorris & Ted Demopoulos

On the World Wide Web, who are you? Google yourself. Go ahead and do it! What is the first search result? Is it your place of employment? Is it one of your online social media pages? Is it your LinkedIn page?

If you do not know by now, 90% of your personal information is somewhere “out there” in the World Wide Web. Whether it be on the local receptionist’s computer at your doctor’s office or in the electronic database of your employer’s human resources offices. In the year of 2015, a majority of professional, medical, organizations utilize some form electric database and have access to the web. What can you do to minimize the amount of personal information that is on the World Wide Web?

A common concern about social networking sites is privacy protecting your personal information and the sensitive information of others. Potential dangers include:

**Impacting Your Future**

Many organizations search social networking sites as part of background checks. Embarrassing or incriminating posts, no matter how old, can prevent you from getting hired or promoted. In addition, many universities conduct similar checks for new student applications. Privacy options may not protect you, as these organizations can ask you to “Like” or join their pages prior to the application process.

**Attacks Against You**

Cyber criminals can harvest your personal information and use it for attacks against you. For example, they can use your information to guess the answers to your “secret questions” to reset your online passwords, create targeted email attacks called spear phishing or apply for a credit card using your name. In addition these attacks can spill into the physical world, such as identifying where you work or live.

**Harming Your Employer**

Criminals or competitors can use any sensitive information you post about your organization against your employer. In addition, your posts can potentially cause reputational harm for your organization. Be sure to check with your organization’s policies before posting anything about your employer.

The best protection is to limit the information you post. Yes, privacy options can provide some protection; however, keep in mind that privacy options are often confusing and can change frequently without you knowing. What you thought was private could become public for a variety of reasons. In addition, the privacy of your information is only as secure as the people you share it with. The more friends or contacts you share private information with, the more likely that information will become public. Ultimately, the best way to protect your privacy is to follow this rule: if you do not want your mother or boss to see your post, you most likely should not post it.

Also be aware of what information friends are posting about you. It can be just as damaging if they post private information or embarrassing photos of you. Make sure your friends understand what they can or cannot post about you.

If they post something you are not comfortable with, ask them to take it down. At the same time, be respectful of what you post about others.

Social networking sites are a powerful and fun way to communicate with the world. If you follow the tips outlined here, you should be able to enjoy a much safer online experience. For more information on how to use social networking sites safely or report unauthorized activity, be sure to review the security pages of the sites you are using.

For more information regarding encryption, contact the UTHSC Information Security Team at (901) 448-1579 or itsecurity@uthsc.edu.

**Resources**

Security Tips for Online Social Networking:
http://preview.tinyurl.com/b28a525

FB Security:
https://www.facebook.com/safety

Your FB Security Settings:
https://www.facebook.com/settings?tab=security

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp