How to be SECURE on Social Media

Select your level of anonymity

Before diving into social media, you should take the time to decide how anonymous you want to be. You could choose to exclude your last name or pictures of yourself and children, or you might choose to use social media to publish your life story. Pick a spot on this spectrum where you are comfortable and set yourself clear boundaries, such as “I will never post my address or phone number, but photos of my family are acceptable.”

Evaluate the platform and the settings available to you

You don’t have to use the default settings on your social media platforms. Before you start posting, customize the privacy settings to your level of comfort. On most sites, you can determine who you would like to share with, what information of yours is visible to others and if others can see your location. Be sure to review these settings often, especially when a social media platform goes through any major change.

Choose your friends wisely

Be selective when accepting friend requests and adding followers. Remember, when you share information on social media, it will be available to all those who follow you: friends, family, coworkers, future employers, etc. Keep in mind, your privacy depends on the actions of your least reliable friend!

Unique passwords are a must

To better protect your social media accounts from hackers, you should use strong passwords with a variety of characters. It is also best to create a unique password for social media instead of recycling the password you use for your bank accounts, your work computer or anything else. Also, although it can be inconvenient, it is best to fully log out of social media sites and log back in for each new session rather than remaining logged in.

Retain control of your personal brand

It’s easy enough to think before you post, but don’t forget to monitor what others say about you on social media. You can set up notifications to alert you of new posts and photos, and most social sites will give you the option to authorize any post or photo that tags you. Take advantage of these tools to keep your personal image and your private information secure.

Exert caution with third party apps and sites

If you want to sync an app to one of your social media sites, read the fine print carefully. Many apps want you to give them permission to post for you and access your friends or followers. Also, be wary of any sort of contest or giveaway on social media. Research the brand making the offer to make sure it is legit before you click. Phishing scams often look like they are coming from respectable brands or personalities.

Follow TechOhioState on social media for privacy tips, service offerings and much more!

Office of the Chief Information Officer