GEORGE MASON UNIVERSITY

Security Liaisons Newsletter

You are key to Internet safety and security at Mason

Information Technology Services | Security Office — itsoinfo@gmu.edu | MARCH 2018

Tips for Using Social Media Securely

Overview

Social media sites, such as Snapchat, Facebook, Twitter, Instagram, and LinkedIn, are amazing resources, allowing you to meet, interact, and share with people around the world.

However, with all this power comes risks — not just for you, but your family, friends, and employer. In this newsletter, we cover the key steps to making the most of social media securely and safely.

Posting

Be careful and think before posting. Anything you post will most likely become public at some point, impacting your reputation and future, including where you can go to school or the jobs you can get. If you don't want your family or boss to see it, you probably shouldn't post it. Also, be aware of what others are posting about you. You may have to ask others to remove what they share about you.

Privacy

Almost all social media sites have strong privacy options. Enable them when possible.

For example, does the site really need to be able to track your location? In addition, privacy options can be confusing and change often. Make it a habit to check and confirm they are working as you expect them to.

Passphrase

Secure your social media account with a long, unique passphrase. A passphrase is a password made up of multiple words, making it easy for you to type and remember, but hard for cyber attackers to guess.

Lock Down Your Account

Even better, enable two-factor authentication on all of your accounts. This adds a one-time code with your password when you need to log in to your account. This is actually very simple and is one of the most powerful ways to secure your account.

Scams

Just like in email, bad guys will attempt to trick or fool you using social media messages. For example, they may try to trick you out of your password or credit card. Be careful what you click on: If a friend sends you what appears to be an odd message or one that does not sound like them, it could be a cyber attacker pretending to be your friend.

Terms of Service

Know the site's terms of service. Anything you post or upload might become the property of the site.

Work

If you want to post anything about work, check with your supervisor first to make sure it is okay to publicly share.

Follow these tips to enjoy a much safer online experience. To learn more on how to use social media sites safely, or report unauthorized activity, check your social media site's security page.

Special announcement

2FA coming April 15 for Mason employees

Beginning April 15, all Mason employees will have to use two-factor authentication (2FA) to gain access to Patriot Web and all Banner-related applications.

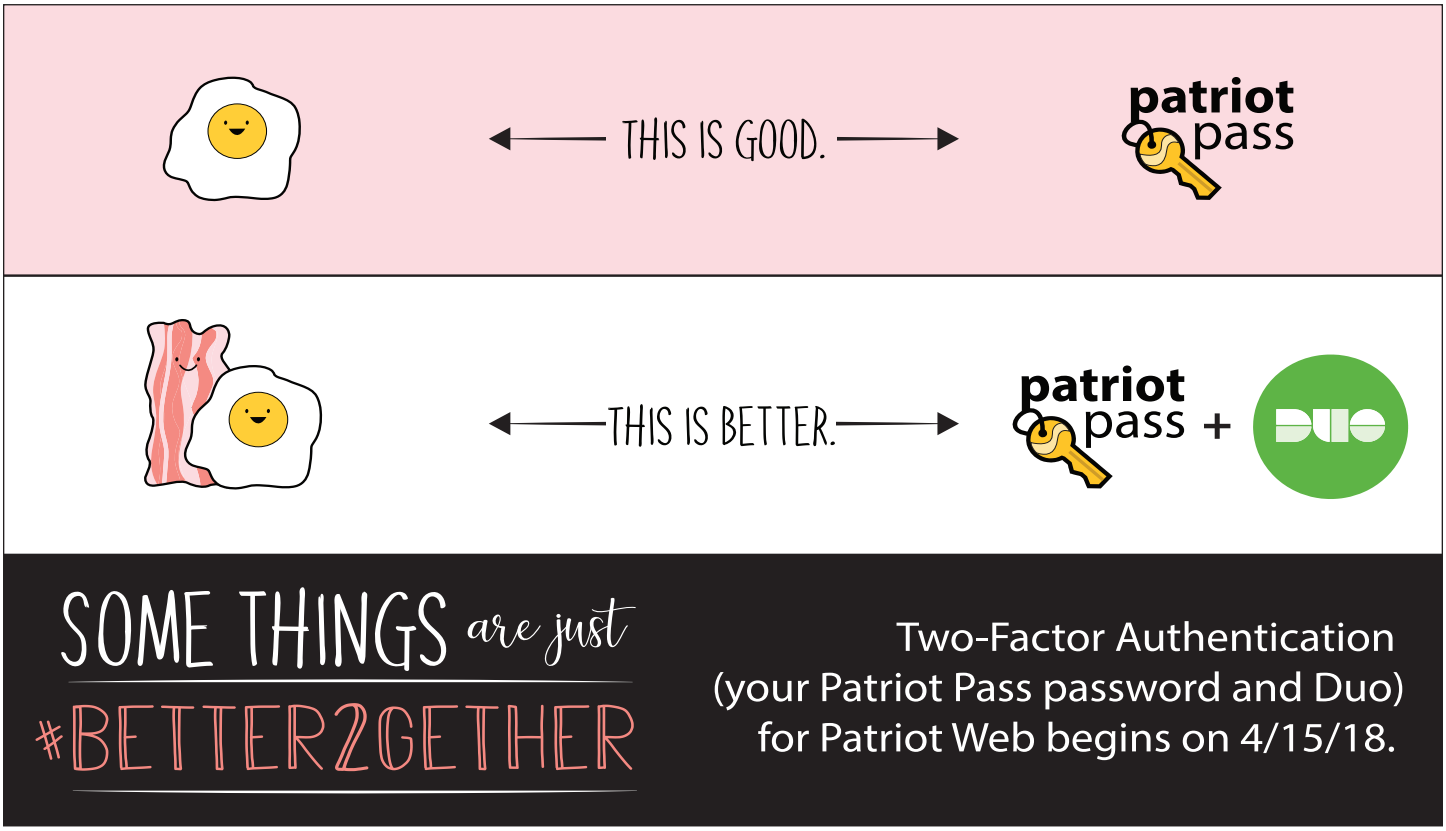
Employees not already enrolled in 2FA will be prompted to enroll when updating their Patriot Pass password.

However, you do not have to wait. You can enroll now. Instructions to enroll in 2FA are available at 2fa.gmu.edu.

Check with your co-workers to see if they are enrolled. If they are not, encourage them to enroll using the instructions at 2fa.gmu.edu.

If you have questions or need assistance, contact the ITS Support Center at 703-993-8870 or by email at support@gmu.edu

Because it is true: Some things are #Better2gether.



The information provided in the monthly newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall information security posture. Mason's IT Security Office brings you this information, produced by OUCH!, The SANS Securing The Human Program, The SANS Institute, 2018.