February 2020

LONGWOOD UNIVERSITY

INFORMATION SECURITY

Using Social Media for Good

Our social networks tell a story about us. You want to make sure that the story your social media tells about you is a good one. As articulated in a blog from the Digital Marketing Institute: "Sharing online allows you to craft an online persona that reflects your personal values and professional skills. Even if you only use social media occasionally, the content you create, share, or react to feeds into this public narrative. How you conduct yourself online is now just as important as your behavior offline."

A positive online reputation is vital in today's digital world. Like it or not, your information is out there. What you can do is help to control it and what it says about you.

Social media is so ingrained in our society that almost everyone is connected to it in some form. With every social media account you sign up for, every picture you share, and every post you make, you are sharing information about yourself with not only your friends and family but the entire digital world. How can you make sure your information and reputation stay safe online? Here are a few easy steps to get you started.

- **Keep it clean and positive.** Be entirely sure about what you're posting. Make sure to post content that you feel positively reflects you, your creativity, your values, and your skills. Remember that future employers may look at your social media accounts before hiring you. Questionable content can leave a bad impression; this can include pictures, videos, or even opinions that make you seem unprofessional or mean and may end up damaging your reputation.

Continued on page 3...

Inside this issue

Special points of interest

- We will soon be launching this year's training—introducing some new videos!
- Additional access may require additional training in Securing the Human; be prepared to finish new modules as they're assigned.

Are You Available?

It happens periodically at Longwood—you get an email from your supervisor or an administrator at the university asking *"Are you available?"* The message feels urgent. You want to be helpful—after all, that's your job, and this is your boss needing something. So in a split second, you decide to answer: *"Yes, I'm available. What do you need?"*

What happens next?

The good news is that just answering this particular email won't jeopardize you or Longwood. There is no link or attachment to click on, no malware to accidently trigger. This is a scam.

If you answer the email, you will likely get a reply. The scammer may ask you to go buy some gift cards at a store nearby, such as Walmart. Here's where you could get into trouble—if you actually go buy the gift cards and send the scammer information about them. Then you are out the money—you have been duped.

The only way this particular scam could harm the university is if you use a Longwood credit card to buy the gift cards, or if you give away your Longwood credentials during your exchanges with the scammer.

So, if you mistake the scammer for your boss at first, no worries. Just delete the email. And remember to be on the alert for strange email addresses or urgent messages. They are red flags that mean something is not quite right.

It happens periodically at Longwood—you get an email from your supervisor or an administrator at the university asking "Are you available?"

Did You Know?

- Concern about identity theft rates slightly higher than fears of job and healthcare loss.
- Nearly two-thirds of the American public have heard, read or seen something about online safety and security issues recently.
- When asked why they don't always do all the things they can or should do to stay safer online, 28 percent of Americans said they simply lacked the information or knowledge.

Attitudes Toward Security

In an effort to find out how people approach cybersecurity, the National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG) had Heart + Mind Strategies conduct two national surveys about online attitudes, behaviors and privacy. These surveys were conducted between 2010 and 2014 among people who self-selected to take them. The results, while not error-proof, reveal some surprising attitudes about cybersecurity.

Of the respondents:

- **93 percent** believe their online actions can protect not only friends and family but also help to make the web safer for everyone around the world.
- **61 percent** believe that much of online safety and security falls under their personal control, and consistent with those feelings, 90 percent said they want to learn more about keeping safer on the internet.
- **96 percent** feel a personal responsibility to be safer and more secure online.
- **48 percent** feel their actions to stay safe and secure can have a positive impact on financial, economic, and national security of the country, indicating Americans are open to making the bridge between their own safety and the nation's security.

For more information, see STOP. THINK. CONNECT.

Social Media, Con't.

Always think before you post or share negative or inappropriate content. Use the 24-hour rule before posting, allowing yourself 24 hours before posting any content that may be questionable to give yourself time to reflect on whether it is a good idea.

- **Oversharing and geotagging.** Never click and tell. It can seem like everyone posts personal information on social media all the time, including where they are and where they live. As noted on the DHS.gov site: "What many people don't realize is that these seemingly random details are all criminals need to know to target you, your loved ones, and even your physical belongings—online and in the real world. Avoid posting names, phone numbers, addresses, school and work locations, and other sensitive information (whether it's in the text or in the photo you took). Disable geotagging, which allows anyone to see where you are—and where you aren't—at any given time."

  If you really want to post that picture of your friends at brunch, consider following the concept of #latergram and post your content at a later time than when it actually happened. It is a win-win. You get to share your experience and at the same time still maintain the privacy of your location in real time.

- **Don't rely on privacy settings.** You have a private social media account so you can post anything you want? Nope. Privacy settings make it harder to see your full account, but it's not impossible. Also, there is always the chance that one of the people with access to your private account could screenshot and share the content.

  Make sure to keep your social media apps up to date and check the privacy settings frequently. Under no circumstances should you rely on privacy settings to shield inappropriate content. If there is any question that the content is inappropriate, don't post it.

- **Make sure you're professional.** Keep it classy! Every post is a reflection of you. Your social media accounts allow you to put your best foot forward or stumble if you aren't careful. A positive social media presence can help create both personal and professional opportunities. Promote your personal brand or what you want people to think of you. And, your high school English teacher was correct—proper spelling and grammar are always a plus.

- **Control your content.** Claim your identity on social media. Set up social media accounts and keep the profiles current. You don't have to join every platform; a few key ones will do. You can also look into apps that will cross post the content to all of your social media accounts, freeing up some of your valuable time. Use your accounts to engage professionally and personally in a positive way.

  Your social media accounts should tell the story of you that you want employers and others to see. Google your own name on a regular basis to make sure that that information out there is accurate. If you find incorrect information online, request that the website update it or take it down.

  If you follow these few simple recommendations, you are on your way to safely building a positive online reputation. Using social media positively doesn't mean you can't have fun and use it to express yourself; however, you want to ensure that you're okay with anyone seeing everything you post. Once you post something online, it's out there forever.

Resources

- Download the US Department of Homeland Security Social Media Guide.
- Learn how to manage your privacy settings with this Stay Safe Online Resource.
- Read this *EDUCAUSE Review* article to "Take Charge of Your Online Reputation."
- Read the Privacy Rights Clearinghouse guide, "Social Networking Privacy: How To Be Safe, Secure And Social."
- How Secure Are Your Social Privacy Settings? (video)
- Are You Sharing Too Much Information Online? (video)
- Considering Posting That Cute Vacation Selfie? (video)

External Emails

The Office of Information Security is responsible for developing and implementing campus-wide policies, controls and procedures to protect the university's information technology resources and systems from intentional or inadvertent modification, disclosure or destruction, as well as monitoring user adherence to these policies.

Last November, we began including an orange banner at the beginning of emails that originate outside of Longwood. The banner cautions you not to click links or open attachments unless you recognize the sender and know the content is safe.

We began this practice to help you be more secure, as external emails can sometimes come from malicious actors. However, it is important to note that any external email will have this notice, including emails from:

- The Commonwealth
- Students who use an @live.longwood.edu email address
- Gmail addresses
- Vendors
- Listservs

Because these emails are originating from a legitimate source, they may be safe—but it is always best to confirm that you were expecting the email and know the sender before proceeding.

Longwood University

Information Technology Services
French Hall
201 High Street
Farmville, VA 23909
(434) 395-4357
(434) 395-2034

Fax: (434) 395-2035