August 2019

LONGWOOD UNIVERSITY

INFORMATION SECURITY

Staying Safe Online

Shopping, surfing, banking, gaming, and connecting Internet of Things devices such as toasters and refrigerators are some of the many actions performed each minute in cyberspace. These common everyday activities carry the cyber threats of social engineering to gain unauthorized access to data, identity theft, bullying, location tracking, and phishing, to name just a few. How can we decrease our risk from these cyber threats without abandoning our online activities altogether? Here are some basic online tips everyone can follow to help stay secure while online.

- **Set up alerts.** Consider setting up alerts on your financial accounts. Many credit card companies and banks allow you to set up alerts on your accounts via their websites. These alerts range from sending you an email or text each time a transaction happens on your account to alerts when transactions meet or exceed a designated spending limit that you set. These alerts keep you in control of your accounts' activities. These types of alerts are useful because they make you aware of what's going on with your account quicker than waiting for monthly statements. When you receive an alert about a transaction that you did not authorize, you can reach out to the credit card company or bank immediately. Log into your credit card company and banking websites to set up alerts on your accounts.
- **Keep devices and apps up to date.** This familiar tip is useful even if you are just casually surfing the internet. Keeping your devices up to date (including apps and operating systems) ensures you have the latest security fixes.

.

Continued on p. 3

Inside this issue

Special points of interest

- Remember to complete Securing the Human by **10/31/19**.
- Additional access may require additional training; be prepared to finish new modules as they're assigned.

Acceptable Use

As we begin a new academic year, it's a good time to review Longwood's Acceptable Use policy, which covers what you can and can't do with Longwood's resources and systems. For use to be acceptable, it must demonstrate respect for:

1. The intent of the individual authorities granted the user;
2. The usage privileges of other authorized users;
3. The rights of others to privacy;
4. Intellectual property rights (e.g., as reflected in licenses and copyrights);
5. Ownership, confidentiality, integrity and availability of systems and data;
6. System mechanisms designed to limit, monitor and/or record use or access (Longwood University IT resources and systems activity are routinely monitored and recorded by technical support staff.);
7. Current network topology and configuration; and
8. Individuals' rights to be free of intimidation, harassment and unwarranted annoyance.

You can see the full policy on Solomon.

Not sharing your password is pretty straightforward, but what about the requirement to use different passwords for every site you access?

Did You Know?

There are many password managers to choose from. Here are some of the most popular:

- Keepass is open source and free to use.
- LastPass is another popular password manager.
- Zoho Vault works for teams.

To see a more complete list, check out this PC Mag article.

Password Managers

You've heard from your Securing the Human training and from communications from the Infosec Office that it isn't safe to share your password, or to use the same password on multiple sites.

Not sharing your password is pretty straightforward, but what about the requirement to use different passwords for every site you access, from work (using your LancerNet password on other sites is prohibited, as it could compromise Longwood's systems) to banking, credit card, and even social media sites? How can you possibly remember all those passwords, especially when each one is supposed to be long and complex enough to prevent a hacker from cracking the password?

Enter the password manager.

Password managers help you keep track of all those passwords. They can even create strong passwords! A password manager will help you access your sites without you having to remember anything but the one password to the password manager itself. This password should be extremely secure, as it holds all your other passwords. You might want to write it down and keep it in a secure place, like a lockbox or a locked file cabinet.

There are several password managers available, including KeePass, which is free and available at Longwood. See the sidebar on the left for more details.

Staying Safe Online, Continued

- **Don't use public Wi-Fi.** In addition to an updated device, the network the device is connected to is also important. Did you have to enter a password to connect to a Wi-Fi network? If you did, that network is more secure than an open one that any device within range can connect to. Whenever possible, use a secure network, especially when banking or shopping online.
- **Consider using a VPN.** VPN stands for virtual private network, and its main purpose is to provide a tunnel for encrypted internet traffic. If you are connected to the internet without using a VPN, your traffic is passed through the internet service provider's servers. The location of your device is known, and if you must connect to a public Wi-Fi network, there is a risk of snooping by other devices on the same network. Connecting to a VPN redirects your internet traffic to a remote server, encrypting the traffic, reducing the snooping risk. There are many options for VPN software today for consumers and businesses. Do your research and decide which one makes sense for your online needs.
- **Create unique passwords.** Here's another familiar tip. Using the same password for many sites is not a best practice. Suppose that one of your accounts suffered a data breach and your password was exposed. If you reused this password on other accounts, it's likely that someone would be able to access those accounts as well (especially if your user name is an email address). Consider using a password manager to manage all your passwords. Not only do these tools manage all your passwords, they can also create strong passwords and can even autofill your username and password as you go to websites on different browsers.
- **Be vigilant.** Be aware, there are fake websites out there waiting to collect your valuable information. Make sure you are on a legitimate site by double-checking the URL website address to make sure it is spelled correctly. Also make sure you see a padlock and https:// in the URL.

Remember that you are in control of your online activities. Following these security tips will give you peace of mind while online.

Resources

- Download the US Department of Homeland Security Social Media Guide.
- Learn about Password Managers.
- STOP. THINK. CONNECT.: The Basic Steps to Online Safety and Security
- STOP. THINK. CONNECT.: Tips for Passwords & Securing Your Accounts
- Are You Sharing Too Much Information Online? (video)
- Considering Posting That Cute Vacation Selfie? (video)

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.

A Note from Infosec

As we begin the 2019-2020 academic year we hope you will remember that it is our actions, as individual IT system users, that most greatly influence the security of Longwood University's information, resources and systems.

How can you help us keep Longwood secure? Stay informed by reading this newsletter and visiting our Solomon site (http://solomon.longwood.edu/information-security/) often. Review the materials in the current Social Engineering Fire Up campaign. Commit to learning something new when you complete Securing the Human this year.

Stay tuned throughout the year for more opportunities to help us keep Longwood secure!

Longwood University

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

Fax: (434) 395-2035