July 2019

LONGWOOD UNIVERSITY

INFORMATION SECURITY

Mobile Device Security

With an increasing amount of sensitive data being stored on personal devices, the value and mobility of smartphones, tablets, and laptops make them appealing and easy targets. These simple tips will help you be prepared in case your mobile device is stolen or misplaced.

- **Encrypt sensitive information.** Add a layer of protection to your files by using the built-in encryption tools included on your computer's operating system (e.g., BitLocker or FileVault).
- **Secure those devices and backup data!** Make sure that you can remotely lock or wipe each mobile device. That also means backing up data on each device in case you need to use the remote wipe function. Backups are advantageous on multiple levels. Not only will you be able to restore the information, but you'll be able to identify and report exactly what information is at risk. (See Good Security Habits for more information).
- **Never leave your devices unattended in a public place or office**. If you must leave your device in your car, place it in the truck, out of sight, before you get to your destination, and be aware that the summer heat of a parked car could damage your device.
- **Password-protect your devices.** Give yourself more time to protect your data and remotely wipe your device if it is lost or stolen by enabling passwords, PINs, fingerprint scans, or other forms of authentication. (See Choosing and Protecting Passwords.) Do not choose options that allow your computer to remember your passwords.

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.

What is Ransomware?

Ransomware is a form of malware, or malicious software, that takes a computer system "hostage" by encrypting data. The malicious actors behind ransomware then demand a fee, or ransom, to unencrypt, and thus release, the data. The ransom is usually demanded in bitcoin, a form of cryptocurrency that can be hard to trace. Ransomware can cause quite a bit of havoc, as it has recently in the following cities:

- **Baltimore, MD:** In May, Baltimore city government computers were infected with ransomware. Critical systems were not affected, but most of the city's servers were shut down. The recovery is still ongoing. The attack has cost 10 million dollars so far, and the city expects damages to equal 18 million.
- **Lake City, FL:** The city's network was affected with ransomware in June, and the city paid a $500,000 ransom. An IT employee was later fired, and the IT department is being revamped.

Think of your password like a toothbrush: never share it with anyone and change it often.

Did You Know?

- You should use a different password for every account. It is especially important not to reuse your LancerNet password on another account.
- A password manager can keep track of all of your passwords for you. KeePass is a great one to use.
- ITS has created Minimum Password Standards, LancerNet Password Standards, and Password Creation Guidelines.

Safe Password Habits

We all know it—passwords can be a pain. They can be complicated to create and difficult to remember. However, they are necessary for keeping your information safe. And your Longwood password keeps university information safe. So it's a good idea to be familiar with the password management policy, as well as some safe password habits. Keep the following in mind when creating your passwords:

- **Your password should be strong.** Consider using a passphrase (such as *Where is my coffee?*) instead of a password. Or you can interweave two words or a word and a number sequence that is meaningful to you. For example, you can combine "kiwi" and "1987" to read *k1i9w8i7*.
- **Avoid writing down your password.** If you do write it down, keep it in a secure place (not on your desk).
- **Never share your password.** Don't even share it with the help desk—they will never ask for it. Neither will ITS. Your password or passphrase belongs to you and you alone—the minute you share it, it is insecure.
- **Change your password regularly.** At a minimum, it should be changed every 120 days.
- **Change your password if it has been compromised.** If your password has been compromised, notify the Help Desk and then change your password immediately.
- **Never use auto-logon or save password features** on websites or in programs.

Leaving your devices unlocked provides access to your data. Remember to lock your screen when you finish using your computer, laptop, or phone. For added security, set your device to automatically lock when it goes to sleep.

STOP | THINK CONNECT™

Mobile Device Security, Con't.

- **Put that shredder to work!** Make sure to shred documents with any personal, medical, financial, or other sensitive data before throwing them away.
- **Be smart about recycling or disposing of old computers and mobile devices.** Properly destroy your computer's hard drive. Use the factory reset option on your mobile devices and erase or remove SIM and SD cards.
- **Verify app permissions.** Don't forget to review an app's specifications and privacy permissions before installing it!
- **Be cautious of public Wi-Fi hot spots.** Avoid financial or other sensitive transactions while connected to public Wi-Fi hot spots.
- **Keep software up to date.** If the vendor releases updates for the software operating your device, install them as soon as possible. Installing them will prevent attackers from being able to take advantage of known problems or vulnerabilities. (See Understanding Patches and Software Updates.)

What can you do if your laptop or mobile device is lost or stolen? Report the loss or theft to the appropriate authorities. These parties may include representatives from law-enforcement agencies, as well as hotel or conference staff. If your device contained sensitive institutional or student information, immediately report the loss or theft to your organization so that they can act quickly.

Resources

The FTC provides guidance for securely disposing your mobile phone.

The DC Metropolitan Police Department provides helpful tips for preventing theft of laptops and personal electronics.

Learn how to get personal data off your devices (don't recycle, trade in, sell, or donate your device without wiping it clean).

Watch the short Federal Trade Commission video, "Back It Up: Don't Lose Your Digital Life."

See Educause's Campus Security Awareness Campaign blog on physical security, "May 2016: Preventing Device Theft."

Learn more about mobile device safety from the STOP.THINK.CONNECT. campaign.

Read tips from US-CERT, "Protecting Portable Devices: Physical Security."

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.

Longwood Smart Device Terms

In order to connect to Longwood email/calendaring with your smart device, you must abide by the following:

- **Device Lock -**A locking function (PIN, Password, Dot Pattern, etc.) **MUST** be set up on the device.
- **Idle Timeout** - Devices **MUST** be set to timeout/lock after no more than 15 minutes of inactivity.
- **Lost or Stolen Devices -** Lost or stolen devices **MUST** be reported to User Support Services, Information Security, or Campus Police (outside of regular business hours) immediately. **ALL Longwood and personal data (files, contact lists, etc.) on lost or stolen devices will be remotely wiped by ITS.**
- **Longwood-owned devices will be wiped** by ITS in the event that the user is no longer employed by the university or if the device is transferred to another user. This wipe will remove ALL Longwood and personal data (files, pictures, music, contact lists, etc.) from the device.
- **Upon separation, personal devices must be reconfigured.** Users must remove the ActiveSync configuration on their personal devices in the event that the user is no longer employed by the university.

Please contact User Support Services for the most up-to-date Terms of Use.

Longwood University

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

Fax: (434) 395-2035