September 2019

LONGWOOD UNIVERSITY

INFORMATION SECURITY

Information Security To Go!

Many people love the adventure that traveling provides: meeting new people, seeing new places, and having new experiences are part of the allure. Technology makes it easier than ever to satisfy our wanderlust. We can use our connected devices to discover the exotic locales we wish to visit, book tickets on planes and trains, practice driving virtually, and seamlessly navigate once we get to our final destination. For all this ease that technology brings, we should prepare our technology for travel as carefully as we plan our travel itineraries.

Travel tips

- **Back-up your data!** Backing up your data ensures that you won't lose information if your device is lost or stolen. Consider encrypting your data as well, but check with your IT support staff first about how best to implement encryption.
- **Protect your devices with a strong password or lengthy passcode.** Sometimes devices get lost or stolen, even when we are being careful. By protecting your device with a passcode or lengthy password, you make it harder for your device to be used and data to be accessed by others.
- **Make sure your devices and applications are up to date.** Keep your applications and devices up to date and patched. This helps protect your device and data from security vulnerabilities and threats.
- **Just say no to unsecured public Wi-Fi.** Having a wireless connection is almost a necessity for the modern traveler. However, using an unsecured public Wi-Fi hotspot can allow others to view the contents of your electronic activity. Never access your sensitive financial accounts from an unsecured network. If you must access sensitive data from an unsecured network, be sure that you use a VPN.

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.

Privileged Access

Privileged access is defined as a level of access above that of a normal user. For example, you have privileged access when you are made an administrator for certain systems on your computer. Here are some things to keep in mind about privileged access:

- Privileged access to IT resources and systems should only be used for official university business requiring the use of privileged access and should be consistent with a user’s role or job responsibilities.
- Privileged access will be granted on a system-by-system basis requiring approval from both the System Owner and the user’s supervisor, or designee (to include Third Party Contract Language).
- Supplementary and/or stronger authentication is required to utilize privileged access. Your privileged-access password should be unique.
- When a user’s role or job responsibilities change, privileged access should be promptly updated or removed.

You can read the full privileged access standard on Solomon.

Did You Know?

- **Least privilege** is the concept that users should run with the lowest level of access necessary to complete a task.
- For example, users should not run as administrators to check e-mail or search the web because completing those tasks doesn’t require administrator privileges.

Safe Searching

When searching the web, whether for business or personal reasons, you can run into sites that will attempt to trick you into downloading spyware, adware, viruses, etc. or collect your personal information without your consent. For safe searching, follow these tips:

- **Do not run as a local administrator on your computer.** At Longwood faculty and staff are required to run as users, not administrators, on their computers. If you have an administrator account for your computer, use it only when you need it to perform a specific administrator task. Also, keep your home computer safe by setting up an administrator account that is separate from your user account and use that account only when you need it.
- **Keep your antivirus up-to-date.** Never disable or reconfigure the security controls on your university computer. At home you should set your antivirus to auto-update so that you can keep your computer protected without having to think about it.
- **Be wary of prompts and pop-ups.** Accessing online multimedia resources is especially dangerous because you are often asked to install viewers or updates to access the content. Sometimes these installations are legitimate and sometimes they are malicious. Never update any software from a prompt from a pop-up window.

Information Security To Go! Con't.

- **Double check your MFA settings.** Many of us rely on multifactor authentication (MFA) to secure both personal and work-related accounts. Be sure that you know how (or if) that will work in the countries that you are visiting. For instance, if your MFA relies on SMS, be sure that you will be able to receive that message in the destination that you are visiting. If the option is available to you, consider using a physical token option to ensure you'll be able to login to your accounts.
- **Update your physical location with your password vault.** Many people use password vaults to manage all of their account passwords. Don't be surprised if your password vault requires additional verification steps when logging into it from a location that is not in your home country. (After all, we count on these vaults to be secure!) Check the vendor documentation or your account settings to make sure that there are no country restrictions or settings that you need to change before your trip. Also double-check that you're able to access your recovery/secondary email address just in case there is an issue.
- **Consider leaving your daily devices at home.** If you are traveling to a location where you are concerned about your individual privacy rights, consider leaving your primary mobile device at home and purchasing a replacement device to take with you instead. Put only the apps, services, and data that you need for that trip on the device. Some businesses and colleges and universities offer programs where a traveler can check out a "clean laptop" when traveling for business purposes. Using these types of devices help limit any exposure of your personal data. Check your data plan as well. A "burner phone" or car GPS may be cheaper.
- **Be smart about posting on social media.** It is always fun to post vacation pictures in the moment, but online postings on social networks (e.g., Twitter, Facebook, Instagram, Snapchat, etc.) can let other people know that you are not at home and that your home may be empty. Posting vacation pictures on social media once you are safely home helps protect your physical belongings.
- **Use hotel safes to protect your technology.** Here's another place where there is an overlap between online safety and physical safety. Just like you would put your passport, jewelry, and money in a hotel safe, consider using that safe to hold your electronic devices when you are not carrying them with you. Not only are the devices themselves expensive to replace, your personal data contained in the device can be irreplaceable (especially if you skipped the first tip on this list).
- **Remember your adapters!** Make sure you have power adapters that will work with three-prong plugs and that they fit the country's outlets. Some travel adapters only accept two-prong plugs. (If you're attending a conference, you may be able to borrow a charging cable temporarily.) Outlets also vary, even, for example, between the UK and Ireland. Your technology gadgets are not very helpful when they run out of charge or cannot be powered on. Charge and take a portable battery pack.
- **Mind your voltage!** Like plug types, different parts of the world use different voltages. Make sure that your technology devices can run on the voltage used at your destination. Getting shocked with 220V is not the same as 110V.

As surely as you can reduce wrinkles in your clothing with careful packing, so too can you avoid the most common technology travel woes by preparing before you leave home.

Resources

- Download the US Federal Bureau of Investigation Safety and Security for the Business Professional Traveling Abroad brochure.
- Review the US Federal Communications Commission Cybersecurity Tips for International Travelers.
- Download and read the US Customs and Border Protection's Inspection of Electronic Devices fact sheet.
- The Princeton University Information Security Office has published good guidelines for traveling abroad.
- Review the Cybersecurity While Traveling Tip Card, part of the STOP. THINK. CONNECT. Toolkit.
- Be prepared: Carry the Electronic Frontier Foundation's Border Search Pocket Guide.
- Learn more about Holiday Traveling with Personal Internet-Enabled Devices in this US-CERT guide.

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.

NCSAM

Do you know why we chose October 31 as the due date for your security training? October is National Cyber Security Awareness Month, or NCSAM. NCSAM is a collaborative effort between government and industry to raise cybersecurity awareness and encourage good habits.

This year's theme is "Own IT. Secure IT. Protect IT." It is important to understand, secure and maintain your digital profile:

- **Understand** your profile by knowing how your devices work—we are so connected and busy these days that sometimes convenience can overwhelm the details.
- **Secure** your profile by using strong passwords and 2-factor authentication and fending off social engineering attacks.
- **Protect** your digital profile by routinely checking privacy settings and shutting down accounts and apps you no longer use.

As October approaches, keep your eyes out for more communications about NCSAM!

Longwood University

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

Fax: (434) 395-2035

Info Sec