October 2019

LONGWOOD UNIVERSITY

INFORMATION SECURITY

Security is Everyone's Responsibility

Did you know? In 2017 the education industry (which includes K–12 and higher education institutions) had 7,837,781 records breached in 35 events. To put that into perspective, the healthcare industry had 6,058,989 records breached in 428 events, and the retail industry had 123,652,526 records breached across 33 events. (See Privacy Rights Clearinghouse Chronology of Data Breaches, 2017 data.)

More than half of the breaches in the education sector were caused by activities directly attributable to human error, including lost devices, physical loss, and unintended disclosure. These breaches were arguably preventable through basic information security protection safeguards.

What can you do every day to protect data? There are very few, if any, verticals such as higher education that transmit, process, access, and share such varying sensitive data elements. There is not a "one size fits all" blueprint for information security controls that all institutions can follow. Yet all campus members have a responsibility to know basic information security protections to safeguard data and prevent those data from being mishandled:

- **Update your computing devices:** Ensure updates to your operating system, web browser, and applications are being performed on all personal and institution-issued devices. If prompted to update your device, don't hesitate—do it immediately.

Continued on page 3.

Inside this issue

Safety Tips for NCSAM..... 2

IT MythBusters 2

Security is Everyone's Responsibility, Con't..... 3

IT MythBusters Continued 4

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.

Safety Tips for NCSAM

October is National Cyber Security Awareness Month, and that means this month is chock full of useful information to help keep you safe online, at Longwood and at home. Here are some safety tips from the National Cyber Security Alliance:

- **Double your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in.
- **Shake up your password protocol.** According to National Institute for Standards and Technology (NIST) guidance, you should consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cybercriminals from gaining access to these accounts and protect you in the event of a breach.
- **If you connect, you must protect.** Whether it's your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems.

If you connect, you must protect.

Did You Know?

- When you delete an email, you must delete it from your Trash and Sent folders to completely get rid of it.
- Servers are the best way to store information. The information is backed up, and it is secure. You should store restricted data on a server.
- Longwood emails will be written directly to you or to a group (such as Faculty or Staff) to which you belong.

IT MythBusters

Every discipline has its myths...ideas that circulate as true even though they aren't. This month, in honor of National Cyber Security Awareness Month, we will bust some of the most common myths about IT. Maybe you have heard some of these in the break room:

Myth: Everything on my hard drive is backed up.

Fact: Your hard drive is **NOT** backed up by ITS. You should save important data to a server, as servers are backed up each night .

Myth: Deleting documents from my hard drive gets rid of them.

Fact: To truly remove a document, you must use the Erase function available when you right-click in Windows.

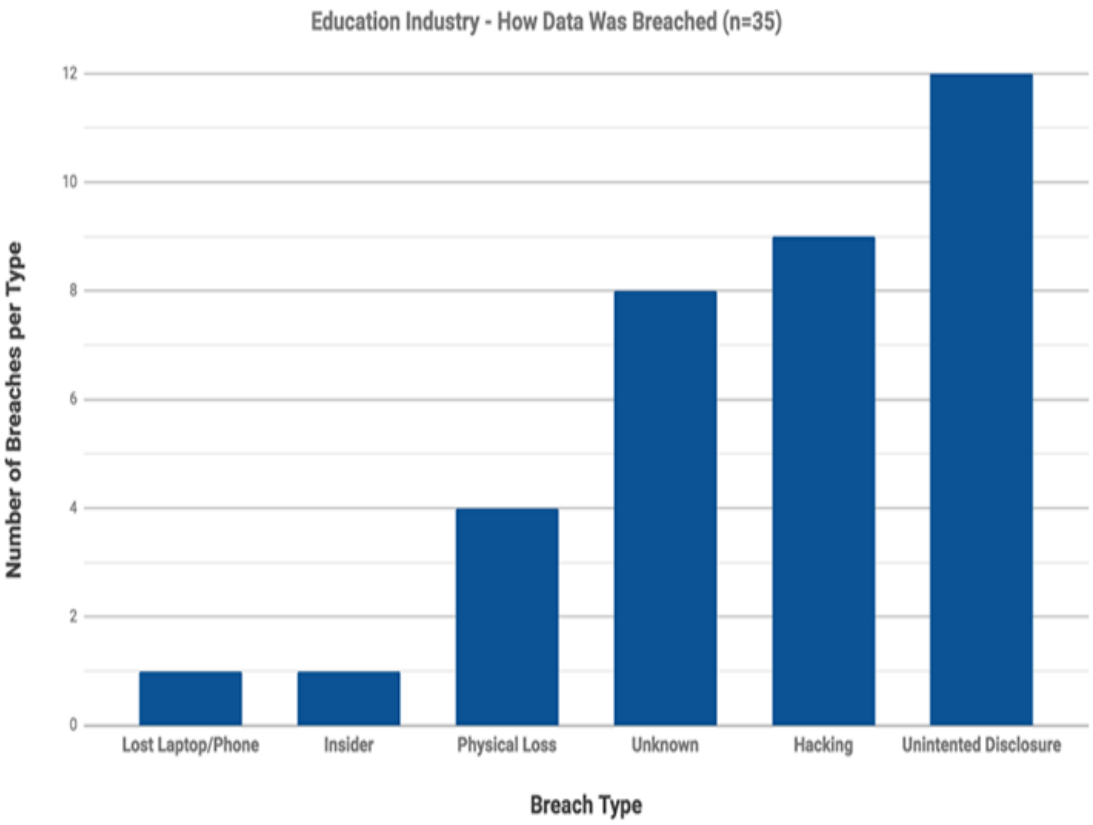
Myth: Important data should be backed up to my jump drive.

Fact: Important data should be stored on a server. Jump drives are easy to lose and easy to target with malware. You should **never** store FERPA or restricted data on a thumb drive.

Myth: I have virus protection software on my computer so it is not possible for me to get a virus.

Fact: Virus protection software can't protect against everything. It is important to have it installed and updated on your computer, but you still need to be cautious about opening attachments or clicking on links.

Continued on page 4.



Security is Everyone's Responsibility, Con't.

- **Enable two-factor authentication:** Whether for personal use or work, two-factor authentication can prevent unauthorized access even if your login credentials are stolen or lost.
- **Create really strong and unique passwords:** Create unique passwords for all personal and work accounts. In today's environment, one of the best ways to create a really strong password is to use a password manager for all of your accounts. A password manager will alleviate the burden of having to memorize all the different complex passwords you've created by managing them all in one "vault" and locking that vault with a single master password.
- **Protect your devices:** Using biometrics or six-digit passcodes on smartphones and tablets is critical to keeping curious minds from accessing personal information, work email, or retail/banking applications. It also helps protect your device if you lose or misplace it.
- **Understand where, how, and to whom you are sending data:** Many breaches occur because of "oopsie moments" where we accidently post sensitive information publicly, mishandle or send to the wrong party via publishing online, or send sensitive information in an email to the wrong person. Taking care to know how you are transmitting or posting data is critical.

Resources

- Practice good online safety habits with these tips and advice from Stop.Think.Connect.
- Stay informed with the monthly SANS OUCH! Security Awareness Newsletter.
- Check out the Data Security page on Solomon's Information Security pages for information about how to classify and handle Longwood's data.
- If your department handles restricted data—such as lists of names and Social Security Numbers—the Information Security department can provide training about the best way to classify and handle this data. Contact Liz Magill for more information.

IT MythBusters Continued

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.

Myth: If an email appears to be from someone I know, it is safe.

Fact: You must check the "from" address carefully, as many malicious actors will make the email appear to be from someone you know when it is actually from an outside email address.

Myth: It is okay for me to save work files to my personal computer.

Fact: Work files are internal data, and should be kept at work, preferably on a server.

Myth: If I put something on a share drive, everyone can see it.

Fact: Only people with permission to access that share drive will be able to see what you put on the drive.

Myth: Everything I do at work is private.

Fact: While IT does not watch everything each user does, it is possible for us to track what sites you visit and what you do on your computer.

Longwood University

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

Fax: (434) 395-2035