April 2020

LONGWOOD UNIVERSITY

INFORMATION SECURITY

Digital Decluttering

A few easy, actionable tips will help you stay cyber safe and protect your personal data and identity. The National Cyber Security Alliance (NCSA) and Better Business Bureau (BBB) are encouraging all consumers to freshen up their online lives by conducting a thorough cleaning of their cyber clutter. With preventing identity theft a top safety concern for Americans, NCSA and BBB encourage everyone to make "digital spring cleaning" an annual ritual to help protect valuable personal data.

Refreshing your online life is a relatively simple process. NCSA and BBB have identified the top trouble-free tips everyone should follow this spring and all year round.

KEEP A CLEAN MACHINE: Ensure all software on internet-connected devices – including PCs, smartphones and tablets – is up to date to reduce risk of infection from malware.

LOCK DOWN YOUR LOGIN: Your usernames and passphrase are not enough to protect key accounts like email, banking and social media. Begin your spring cleaning by fortifying your online accounts and enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device.

DECLUTTER YOUR MOBILE LIFE: Most of us have apps we no longer use and some that need updating. Delete unused apps and keep others current, including the operating system on your mobile devices.

Continued on page 3...

Inside this issue

Special points of interest

- Check out our Alerts page for the latest information about COVID-19 scams.
- If you have remote access to Longwood systems, you will have additional training in Securing the Human. Make sure your training is up to date!

.

Website Update

The Information Security Office has recently updated our website to provide support to Longwood employees during this challenging time. Our Security Alerts and Information page now includes information about the latest scams and malicious activities related to COVID-19. Check this page often for tips on protecting both your personal information and Longwood's data.

We have also added a Working Remotely page to support those of you who are working from home. Check out this page if you missed our email with tips for securing your devices and network while working remotely, including the following:

- Changing the default administrator password on your router
- Enabling automatic updates on your devices
- Familiarizing yourself with VPN policies and procedures

These are just a few of the tips you will find on the new page. Refer to this page when setting up your home work environment and engaging in online meetings.

It's much easier for cyberattackers to convey emotion or a sense of urgency over the phone.

Did You Know?

- Vishing stands for Voice Phishing
- Vishing is on the rise; it is important to detect and stop these attacks right away!
- If you did not initiate the phone call, protect yourself by not trusting the caller unless you know them.
- Scammers may be after your COVID-19 relief check! See tips to protect yourself from the FTC.

Vishing

Vishing (which stands for voice phishing) is when cyber criminals call you on the phone in an attempt to steal your money, to find out your personal information, or to gain access to your computer. These phone calls can either be from a real person or an automated voice message.

These criminals use vishing because there are far fewer security technologies that can detect and stop these attacks. Also, it's much easier for cyber attackers to convey emotion or a sense of urgency over the phone, thus rushing their targets into making a mistake.

Examples of Vishing

1. You receive an urgent phone call from the government telling you that your taxes are overdue and if you don't pay them right away you will be fined or go to jail. They then pressure you to pay them immediately with your credit card.
2. You receive a phone call from tech support, explaining that your computer is infected with malware and is actively scanning the internet. They then pressure you into buying their special security software that can get rid of the infection, or they demand remote access to your computer to fix it.
3. You receive an automated voicemail stating that your bank account has been compromised and are given a number to call back to update and secure your account.

Protecting Yourself from Vishing

1. If you suspect a phone call is a scam or attack, simply hang up.
2. If you are not sure if the call was legitimate, after you hang up, find a trusted phone number to call (such as from the organization's website) and call them back using that number. Never call back using information the cyber attacker gave you.

Continued on p. 4...

Digital Decluttering, Cont.

DO A DIGITAL FILE PURGE: Perform a good, thorough review of your online files. Tend to digital records, PCs, phones and any device with storage just as you do for paper files. Get started by doing the following:

- **Clean up your email:** Save only those emails you really need and unsubscribe to email you no longer need/want to receive.

- **Back it up:** Copy important data to a secure cloud site or another computer/drive where it can be safely stored. Passphrase protect backup drives. Always back up your files before getting rid of a device, too.

OWN YOUR ONLINE PRESENCE: Review the privacy and security settings on websites you use to ensure they're at your comfort level for sharing. It's OK to limit how and with whom you share information.

KNOW WHAT DEVICES TO DIGITALLY "SHRED": Computers and mobile phones aren't the only devices that capture and store sensitive, personal data. External hard drives and USBs, tape drives, embedded flash memory, wearables, networking equipment and office tools like copiers, printers and fax machines all contain valuable personal information.

CLEAR OUT STOCKPILES: If you have a stash of old hard drives or other devices – even if they're in a locked storage area – information still exists and could be stolen. Don't wait: wipe and/or destroy unneeded hard drives as soon as possible.

EMPTY YOUR TRASH OR RECYCLE BIN ON ALL DEVICES AND BE CERTAIN TO WIPE AND OVERWRITE: Simply deleting and emptying the trash isn't enough to completely get rid of a file. Permanently delete old files using a program that deletes the data, "wipes" it from your device and overwrites it by putting random data in place of your information – that then cannot be retrieved. For devices like tape drives, remove any identifying information that may be written on labels before disposal, and use embedded flash memory or networking or office equipment to perform a full factory reset and verify that no potentially sensitive information still exists on the device.

DECIDE WHAT TO DO WITH THE DEVICE: Simply deleting and emptying the trash isn't enough to completely get rid of a file. Permanently delete old files using a program that deletes the data, "wipes" it from your device and overwrites it by putting random data in place of your information – that then cannot be retrieved.

From the Tip Sheet "Do a Digital Declutter This Spring," available from Stop. Think. Connect.

Resources

- "How to Spring Clean Your Digital Clutter to Protect Yourself" from Wired.com.
- "Digital Spring Cleaning," from the Center for Internet Security.
- "Have You Done Your Digital Spring Cleaning?" from EdTechTeam.
- "Freshen Up Your Digital Space with a Spring Cleaning" from the National Initiative for Cybersecurity Careers and Studies.
- Video: Digital Spring Cleaning Checklist.

Vishing, Con't.

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.

3. Never allow a caller to take temporary control of your computer or trick you into downloading software.
4. Remember that, in most cases, government organizations will never call or email you; instead, they will contact you directly via old-fashioned mail.
5. If you receive a phone call from a number you do not know, let it go to voicemail. This will give you time to review the unknown caller's message on your own without any pressure.

This information is provided by SANS Security Awareness.

Longwood University

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

Fax: (434) 395-2035