May 2020

LONGWOOD UNIVERSITY

INFORMATION SECURITY

Are Passwords Leaving Us?

There are plenty of reasons to hate passwords. A recent Ponemon Institute study provides some insights into why many people have developed what has become known as *password fatigue:*

- Respondents reported having to spend an average of 12.6 minutes each week or 10.9 hours per year entering and/or resetting passwords. Most respondents also reported being unable to complete personal transactions because they had forgotten their passwords.

- About two-thirds (69 percent) admitted to sharing passwords with coworkers to access accounts, and more than half (51 percent) said they reuse an average of five passwords across work and personal accounts.

- Most respondents do not use a password manager and rely on human memory, spreadsheets, and sticky notes to manage passwords. Fewer than half (45 percent) use multifactor (or two-step) authentication in the workplace.[1]

It is increasingly clear that new security approaches are needed to help individuals manage and protect their passwords, and passwordless login technology could provide an option. A majority of IT security professionals and individual users believe that the use of biometrics or hardware tokens could offer better—and more user-friendly—security protections.

Several colleges and universities—including Duke[2] and Stanford[3]—are working to develop and deploy passwordless solutions. In the meantime, multifactor authentication and good password practices can help as we move toward a passwordless future.

Continued on page 3...

Inside this issue

Cybersecurity for Kids..... 2
Social Engineering Defense... 2
Passwords, Cont..... 3
Kids, Con't..... 4

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!

.

Cybersecurity for Kids

With school closures and subsequent transition to online learning (and summer just around the corner), kids are spending even more time on the internet. Keeping kids safe online is no small task for the parents who have been transitioning to remote work themselves. Here are a few tips to keep your kids safe online while everyone's home:

1. **SANS Institute**, an organization for security professionals, has recently released the "Securing Your Kids" webcast which provides a comprehensive overview of ways to secure kids online. It includes best practices, discusses recommendations for secure online learning, and provides some technology recommendations.
2. **NetSmartz**, an online safety education program, is a great resource for both parents and kids. For parents, check out the Resources section for fun and well-designed presentations you can show to your kids. For the kids, visit the library of video lessons, read e-books and download fun printable activities on many relevant topics for elementary, middle and high schoolers.

Continued on page 4…

This type of trick is much easier to fall for during a time of change and confusion.

Did You Know?

Check out these stats from CSO:

- 94% of malware is delivered via email.
- Phishing attacks account for more than 80% of reported security incidents.
- $17,700 is lost every minute due to phishing attacks.
- 60 percent of breaches involved vulnerabilities for which a patch was available but not applied.

Social Engineering Defense

Social Engineering is a psychological attack where attackers trick or fool their victims into making a mistake. This type of trick is much easier to fall for during a time of change and confusion. It is important to remain vigilant while working from home—keep your guard up when dealing with an unexpected email or phone call. Here are some tips to keep you safe:

Resist the Rush

Social engineers often create a tremendous sense of urgency, such as telling you there is a tight deadline, to trick you into making a mistake. Be suspicious if someone pressures you, intimidates you, or plays on emotions such as fear, curiosity, or excitement.

Think Before You Click

Social engineers want you to carelessly click on links and not think twice before opening attachments. Be cautious: one wrong move could infect your device and spread it to others.

Don't Just Download It or Plug It In

Social engineers count on you to download unapproved software or plug in infected USB drives or external devices. Only use authorized hardware and software. If you are not sure if something is authorized, just ask.

Ask Questions, and If It Feels Odd or Suspicious, Contact Security

If you are feel you are under attack, hang up the phone (or do not respond to the email), and contact security at infosec@longwood.edu right away.

Passwords, Con't.

Tips on protecting your digital identity:

- Use a fingerprint or biometric requirement to sign in when available. This provides an extra layer of protection for devices and apps.
- Whenever possible, take advantage of whatever two-factor authentication (2FA) methods are available for your service. View a list of websites that support two-factor authentication (2FA).
- Create a unique username and password or passphrase for each website or application.
- Use a password manager to help avoid password reuse, and protect it with a long passphrase. Some password managers are free, but you can also check with your IT department to find out which tool it recommends.
- Update to the latest security software, web browser, and operating system. Turn on automatic updates to help protect your personal information against new threats.

Stay protected when connecting to any public wireless hotspot. Use a virtual private network (VPN) client, which provides secure remote access to resources.

Notes

1. Ponemon Institute, *The 2019 State of Password and Authentication Security Behaviors Report,* January 2019.
2. Mary McKee and Shilen Patel, "Duke Unlock: One-step Multi-factor. Passwordless Authentication with Shibboleth and WebAuthn," *InCommon* (blog), InCommon/Internet2, December 2019.
3. "Cardinal Key: Simplicity and Security," *Stanford University IT* (website), March 13, 2020.

Resources

- World Economic Forum in collaboration with the FIDO Alliance: *Passwordless Authentication: The next breakthrough in secure digital transformation*
- National Cyber Security Alliance (NSCA): Passphrases and Securing Your Accounts and Devices
- National Institute of Standards and Technology Trusted Identities Group: Back to Basics: Multi-factor Authentication (MFA)
- NCSA: Credential Theft Isn't Going Away. Here's How You Can Fight It

Kids, 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. If your kids like **Garfield** (that naughty cat!), check out **these videos** from the Center for Cyber Safety and Education. You can watch the videos and then play games to reinforce the knowledge.
4. Check out **Google's Be Internet Awesome site**. It offers the Internet Code of Awesome that covers some good practices kids can use when using the Internet. For kids – and maybe adults! – play **the Interland game** to cross the Reality River testing your knowledge of true and false information on the Internet or visit the Kind Kingdom to share online kindness with fellow Internauts.
5. The Better Internet for Kids resource center provides **an online collection of videos** on a variety of topics. You can select the language of the videos or review other resources offered by different European Safer Internet Centres.

Longwood University

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

Fax: (434) 395-2035