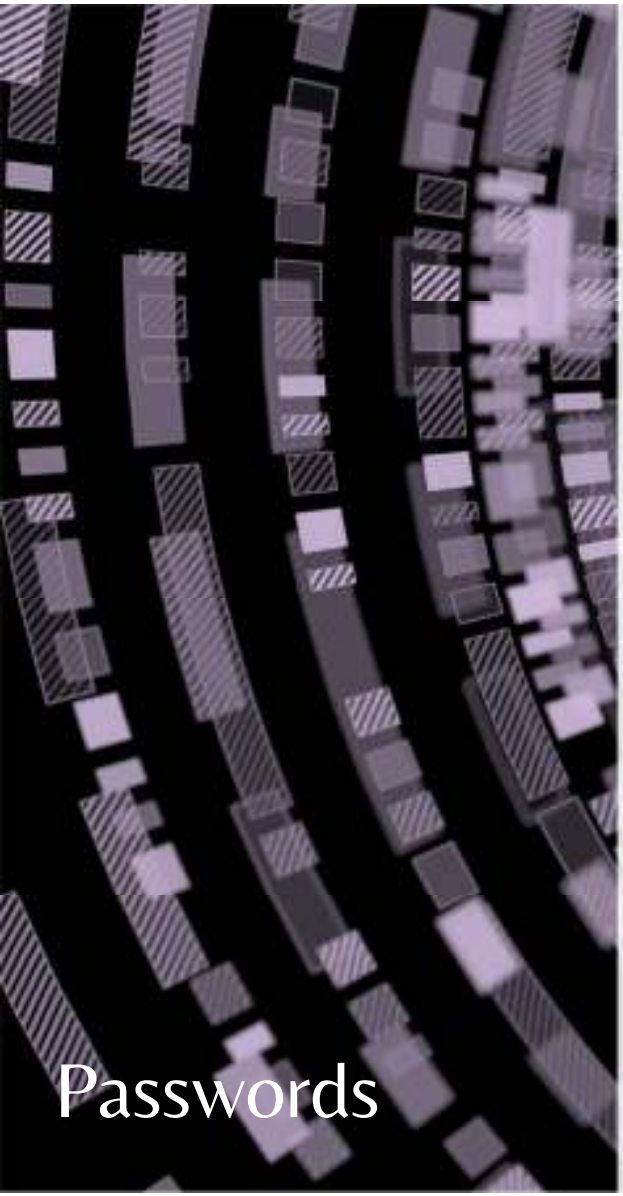
Heather Noggle

Cybersecurity for People

Level 1 Series

What to Do And Why

What	Why
Make a unique password per website/application	If someone gets your credentials for one site, the credentials for other sites are safe: (Twitter, Jan 2023)
12 or more characters, each password. Mix of letters, numbers, and symbols (oh, my)	Computing power is increasing, making “brute force” attempts to discover (crack) passwords faster and simpler. Complexity and length are your friend.
Use a Password Manager	Remember one “supersecure” password – a passphrase. Manage the rest.



Passwords

Curious? Discover More

https://www.haveibeenpwned.com

Check to see if your phone number or any of your email addresses are associated with a data breach...and when.

https://www.hivesystems.io

Download the password table. They update it each year.

Challenge

Make all passwords 20 characters or more. Plan to increase the length next year, if not sooner. The longer the password, the better.

https://www.heathernoggle.com

What to do and Why

Because password books are so 1992 (and insecure).

What	Why
Make a great passphrase to secure your other passwords.	A passphrase is a long but memorable structured password. The memorable part is key.
Use your password manager to create your other passwords – make them as long as possible.	Little effort on your part – great payoff. You don't need to know and remember these passwords.
Make account set-up and password storage in your manager a reminder to ALSO set multifactor authentication on accounts.	MFA + strong passwords and good management practices bolster your personal cybersecurity to strong, intentional levels.

Example Passphrases

Spinner8PieceContrail_Garden9StrikeBall*GreenSphere

MondayNote9Cannon1)FinchMornay@BeefGreatTitleChickpea

LessHill92BeltwayGritPancakeNutcracker*BrownDanderCollie

Chain7Headphone+CampLeg3PowerMoneyBiscuitLankyPear

Practicing out loud helps you memorize.
Words with loose affiliation (to you) but not next to each other also helps.

Password Managers

Curious? Discover More

1Password

My recommendation – ease of use + security, reasonable.

https://www.1password.com

Bitwarden

Another alternative, less expensive, not as user-friendly.

https://www.bitwarden.com

Challenge

Research Alternative Password Managers

https://www.cnet.com/tech/services-and-software/best-password-manager/

What and Why

Approach MFA with humor. Every extra step you take magnifies security.

What	Why
Multifactor authentication – MFA. One or more additional steps you take to authenticate - prove that you're you.	Someone who's not you but has your credentials is frustrated and moves on to the next target.

Examples		
"Security Questions"	An older method, not the most effective option.	Make it better - give fake answers to the questions.
A code in text or email	Better	But there's a better option…
An authentication app	Even better	Google Authenticator, others

Multifactor authentication https://www.heathernoggle.com

Multifactor Authentication

Curious? Discover More

2FA and MFA

2FA is two-factor authentication. Username + password AND one additional step to authenticate. These terms are often interchangeable.

Categories

Consider 3 categories of MFA: something you know, something you are, and something you have.

Challenge

Use a FIDO Device – MFA with Less Hassle

WOOF! FIDO is Fast ID Online. Device-based (something you have) MFA. An example? Yubikey from Yubico: https://www.yubico.com/

https://www.heathermoggle.com

What to do and Why

If you back it up, you can restore it!

What	Why
Back up your important data!	If you lose your data (or it's encrypted/destroyed), you can get one or more files from your backups.
Be intentional about backup.	What files do you need to keep? How frequently do you need to back up files?
Follow the 3-2-1 Backup Method, especially if you're an organization. https://www.veeam.com/blog/321-backup-rule.html	Eventually build 3 different backups, two different media. 2 onsite backups, 1 offsite (cloud/online).

Backup Resources

USB External drive – without backup software. (Seagate, 2 TB)

USB External drive – with configurable backup software (Western Digital iPassport, 2TB)

IDrive Online Service

https://www.heathermoggle.com/videoresources

Curious? Discover More

Practice Restoring Backups

Restore to another computer, manually or automatically.
Perhaps both.

Review What you Backup and Why Regularly

- Organize your data well
- Be intentional!

Challenge

Write Your Own Script

Powershell in Windows – research why this works

```
j:
xcopy /y /s /d *.* z:\backups\
pause
```

https://www.heathermoggle.com

MALWARE

Malware is a compound word

Mal = Bad

Ware = Software that runs on computers and other devices

Types: Worms, Trojans, Adware, Bots, Spyware, RANSOMWARE $$$$$

Choose Your Defense

Antimalware Recommendations

Scan Daily, Preferably Automatically
Run a “Deep Scan” at Least Monthly
Purchase a Full Package from a Reputable Vendor
Remember to Protect Your Mobile Devices and Tablets!

I Recommend One of These

- Bitdefender
- Malwarebytes
- McAfee
- Norton

https://www.cnet.com/tech/services-and-software/best-antivirus/

Curious? Discover More

History of Malware

https://www.lifewire.com/brief-history-of-malware-153616

WannaCry?

https://www.malwarebytes.com/wannacry

Challenge

Learn Malware Specific Examples

https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/

Antimalware

https://www.heathernoggle.com

What to Do And Why

Click intentionally. #ownyourclicks

What	Why
PAUSE if something seems off.	Your senses are probably right. Scammers want you to ACT NOW in the QUICKEST WAY possible – their way. A link, a phone call.
Verify independently. Search the information in another, separate way if you are curious.	Using that convenient link or phone number is the goal of the scammer.
BREATHE. And tell someone what happened.	We don't want anyone to fall for a scam. Share your stories.

Social Engineering

Curious? Discover More

Learn the Difference Between Phishing, Spear Phishing, and Whaling

Scammers target people differently with these varied social engineering attacks.

Watch This TED Talk

Search for it on the TED site or YouTube: Christopher Hadnagy - How phishing scammers manipulate your amygdala and oxytocin

Challenge

Think Like a Scammer to Defeat a Scammer

What would a phishing email, voice mail, or text from you look like? One you think would work.

What would it say? Be devious in your thinking.

https://www.heathermoggle.com

What to Do And Why

Here's a Bad Pun about Being Left to Your Own Devices

What	Why
Know what you have. When was each device last updated? Are updates waiting?	Devices that need updates to their operating systems have exploitable vulnerabilities. You don't want that.
Look for unused software and remove it from computers and other devices. Ensure the software you use is up to date.	It's easier to manage your devices' operations if you remove what you're not using.
Set computers and mobile devices to auto-update their operating systems.	Set it once, and it runs. You can always install it sooner if you see a message online about the update being available.

Device Management

Curious? Discover More

Learn about Data Destruction and Device EOL

EOL = End of Life. There are safe ways to destroy data and decommission devices.

Search “destroy data” and then search “decommission devices.”

Consider Powering Down Devices Not In Use

If you use a device only occasionally, take it offline and turn it off.

Challenge

Learn How to Monitor Network Traffic

It’s good to check if your devices might not be behaving.

https://www.makeuseof.com/windows-11-set-data-usage-limit/#third-party-tools-to-monitor-data-usage

https://www.heathermoggle.com

Heather Noggle

Cybersecurity for People Series

Level 1

YouTube
https://www.youtube.com/@heathernoggle

LinkedIn
https://www.linkedin.com/in/heathernoggle/

Website
https://www.heathernoggle.com/

Twitter
https://twitter.com/heather_noggle

Share knowledge