Instructional Design Blueprint: Cybersecurity Training

Developers: Aleyna Storms, Matthew A., and Katharine V.

Workplace Setting:	**Target Audience:**
An American school district's cybersecurity onboarding program for new faculty and staff members. The training is to be completed in school-based groups of 12-15 learners. New staff members will sign up for a synchronous class section specific to their campus or work site.	12-15 new faculty and staff members receiving onboarding training in cybersecurity.

Portrait and expectations of the target audience:
12-15 new faculty and staff members, with a variety of backgrounds, specializations, and ages. Learners will participate in a one-hour virtual training on the basics of cybersecurity. The course is intended for those with little to no background in cybersecurity and has no prerequisite requirements. Learners will sign up for a time slot to complete the training synchronously. Instructors will facilitate group interaction via Zoom and Zoom break out rooms.

Course Title: Cybersecurity Training

Learning Theory: Social exchange theory and group learning theory

Learning Theory Rational:
Group learning theory and social exchange theory are both centered on maximizing group strengths through collaboration and minimizing individual weaknesses. Social exchange theory capitalizes these synergistic relationships so that whole group process and product is greater than what the individuals could produce (Miller, 2022). Creating opportunities for group learning through this training will provide learners with the opportunity to share their understanding and contribute in a way that highlights and effectively increases the learning benefits of each member (Almuqrin, 2022). Because the goal of this training is for faculty and staff members to be able to recognize the importance of cybersecurity on a personal and collective level and be able to apply skills to their real-world circumstances, it is vital for them to have the opportunity do collaboratively learn through group engagement.

Learning Objectives:
Learners will be able to:

- Identify and define Personally Identifiable Information (PII) as information about a person that identifies, connects, relates, or describes them.
- Explain how different pieces of PII can be combined to identify people or deduce other personal information.
- Discuss the warning signs for these common security risks.
- Explain how these common security risks target people.
- Identify common security risks: phishing, keylogging, malware, rogue access points.
- Identify the best practices needed to protect themselves from security threats.
- Discuss and describe the importance of computer updates and virus scanning.
- Explain how multifactor authentication can be important and beneficial.

Timeframe and setting: One-hour synchronous virtual training, with an additional asynchronous post-course student reflection on changed practices.
Introduction: Learners will be welcomed to the Zoom meeting, and the instructor will begin the icebreaker script following along with the presentation and providing the opportunity for students to react. <u>Cybersecurity Ice Breaker:</u> Instructor script: “Look through the different pieces of information displayed and decide which ones do you think are too personal to share with just anyone?” Provide each piece of information and allow learners to use the scale feature in Mentimeter to react as “No,” “Maybe,” or “Yes”. (See Appendix A)
Materials: All learners must have internet access and a laptop or tablet with video and microphone capabilities for the training.
Meeting Platform: • Learners will meet through Zoom and instructors will utilize the breakout room feature to better facilitate discussion groups (Zoom Communications Software, 2023). • Presentation Material and Assessments will be presented and shared with the learners through Mentimeter (2014).
Learning Activities: • Cybersecurity Ice Breaker • Website Privacy Policy Breakout • Security Risk Jigsaw • Changed Practice Reflection

Module	Objectives	Resources/Technology	Learning Activities	Lesson Outline	Assessment
Privacy and Security	Learners will be able to: • Identify and define Personally Identifiable Information as information about a person that identifies, connects, relates, or describes them. • Explain how different pieces of Personally Identifiable Information can be combined to identify people or deduce other personal information.	Zoom: • Breakout Rooms for group conversations Websites: • Social Media • Search Engine • Online Shopping • Educational Website • Maps • Communication • Streaming • Gaming • Banking Video • How to Read Privacy Policies like a Lawyer. (The Verge, 2018). Presentation Material • Slides presentation about privacy and “the cost of free” (code.org, 2023).	Cybersecurity Ice Breaker: • Identify what information the learner would view as "personal” and would not want shared with just anyone. Presentation • Display Privacy Policy video (The Verge, 2018). Breakout Rooms • Learners will conduct website research in a randomized group. Mentimeter This or That • Indicate the least safe Social Media post. • Indicate the best privacy policy for the user’s needs. (See Appendix B)	Breakout Rooms • Learners will be given randomized grouping in Break Out Rooms • The Group will be given a website in a given category and read through the Privacy Policy. • Collectively, the group will answer the following questions: ○ What data is collected? ○ How is that data being used? ○ Is this data shared with a third party? ○ Do the benefits of the website outweigh privacy concerns? • Come back together to discuss results as a group: ○ Expected results: ▪ Every website that you use takes in data. ▪ Some websites are better with security than others.	Mentimeter This or That • Via Mentimeter.com This or That portion of the presentation. • Learners will be presented with multiple pairs of images, each pair accompanied by a question. • They will be asked to identify the more appropriate image/concept regarding Privacy and Security. • Results will be shown after each round of This or That. • The assessment will indicate whether the participants can identify the best practices for protecting their identity and privacy in a digital environment. (See Appendix B)

Security Risks	Learners will be able to: • Discuss the warning signs for these common security risks. • Explain how these common security risks target people. • Identify common security risks: phishing, keylogging, malware, rogue access points.	Zoom: • Breakout Rooms for group research. • Breakout Rooms for intergroup collaboration. Research Articles: • Keyloggers (Blue, 2017) • Phishing (Irwin, 2019) • Malware (Sectigo, 2020) Presentation Material: • Slides presentation about different security risks.	Breakout Rooms • Learners will conduct website research in a randomized pair for research. • Learners will bring their ideas together in a topic group break out room. Presentation • Topic Groups share their findings and additional important information. • Review of information in presentation • Display examples of the security risks. Mentimeter This or That • Indicate the most trustworthy email out of given examples. • Indicate the Malware notification. • Indicate the mouse movement that indicates keylogging. (See Appendix C)	Security Risk Jigsaw • Learners are given a partner in a breakout room and an article about one of the following topics: ○ Keylogging ○ Phishing ○ Malware • Partners will discuss the answers to the following questions. ○ What are the security risks? ○ How are people targeted? ○ What warnings are there? • Learners are brought back to the main group to be regrouped into topic-based breakout groups. • Learners discuss and elect three group leaders to present the information about the security topic. • Expected results ○ Keylogging is the unauthorized recording of keystrokes. ○ Phishing is an attempt to trick users into providing secure information.	Mentimeter This or That • Via Mentimeter.com This or That portion of the presentation. • Learners will be presented with multiple pairs of images, each accompanied by a question. • They will be asked to identify the more appropriate image/concept regarding Security Risks and other common scams and their indicators. • Results will be shown after each round of This or That. • The assessment will indicate whether the participants can identify the most common indicators for scams and possibly harmful activity online. (See Appendix C)

				○ Malware is software intended to harm a computing device.	
Best Practices	Learners will be able to: • Identify the best practices needed to protect themselves from security threats. • Discuss and describe the importance of computer updates and virus scanning. • Explain how multifactor authentication can be important and beneficial.	<u>Password Strength:</u> • Website to test passwords (*Password Strength Meter*, 2022). • Emphasize this is for testing and should not use actual password. <u>Presentation Material:</u> • Slides presentation about security best practices.	<u>Presentation</u> Presentation on the different practices one can use to be more secure: • Password Development • HTTPS vs. HTTP • Public Wi-Fi use. <u>Password Tester</u> • Learners will test different passwords (that are not their own) into the password tester to identify how long it would take for the password to be cracked. • Learners will read the tips provided as they attempt different passwords (2022). • Indicate the list of more acceptable password examples. • Indicate the secure website lists. • Indicate the most trustworthy Wi-Fi network connection to connect to. (See Appendix D)	<u>Password Tester</u> • The Module begins with using the password tester (2022) to test different passwords. • The password tester provides tips for the learners to explore best practices for password creation. <u>Changed Practices</u> • The course concludes with a post-course student reflection assignment on Changed Practices. • This will be completed asynchronously after the course and will follow the guiding questions provided in Appendix E.	<u>Mentimeter This or That</u> • Learners will be presented with multiple pairs of images, each accompanied by a question. • They will be asked to identify the more appropriate image/concept regarding all the concepts discussed in this training. • Results will be shown after each round of This or That. • The assessment will indicate whether the participants can identify the best practices for protecting valuable information and responsibly using the internet. (See Appendix D) <u>Post-Course Student Reflection:</u> <u>Changed Practices</u> • Learners will develop a plan using the provided template to make changes in their everyday and educational cyber use to better secure themselves online. (See Appendix E)

References

Almuqrin, A. H. (2022). Social exchange theory and theory of reasoned action affecting knowledge sharing: A case from Saudi Arabia. *Journal of Information Studies & Technology (JIS&T)*, *2022*(1), 1–16. https://doi.org/10.5339/jist.2022.5

Blue, V. (2017, June 28). *Keyloggers: Beware this hidden threat*. PCWorld. https://www.pcworld.com/article/406909/keyloggers-what-you-need-to-know-about-this-hidden-threat.html

Borky, J. M., & Bradley, T. H. (2018). Protecting information with cybersecurity. *Effective Model-Based Systems Engineering*, 345–404. NCBI. https://doi.org/10.1007/978-3-319-95669-5_10

Cybersecurity and Global Impacts ('23-'24). (2023). Studio.code.org; code.org. https://studio.code.org/s/csp8-2023

Interactive presentation software. (2014). Mentimeter. https://mentimeter.com

Irwin, L. (2019, June 6). *5 ways to detect a phishing email – with examples.* IT Governance UK ; IT Governance. https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email

Miller, S. P. (2022). Social exchange theory. *Salem Press Encyclopedia*.

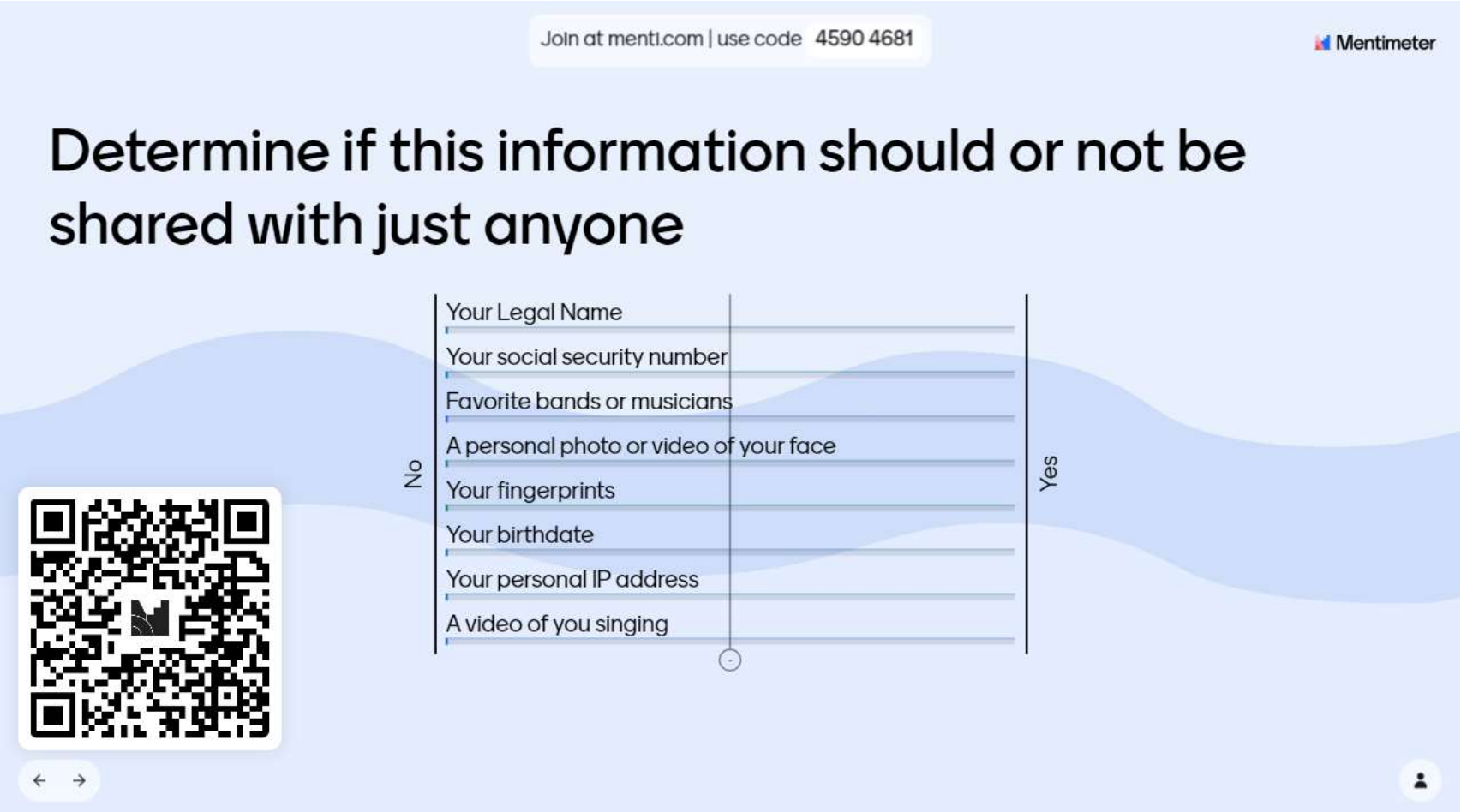
Password Strength Meter. (2022). PasswordMonster. https://www.passwordmonster.com/

Sectigo. (2020, September 23). *9 types of malware website owners need to know*. SiteLock. https://www.sitelock.com/blog/9-types-of-malware-all-website-owners-need-to-know/

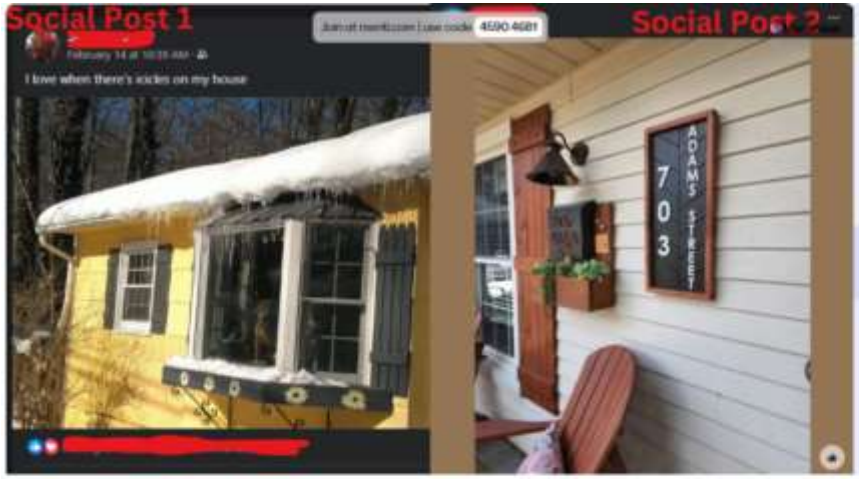
The Verge. (2018). How to read privacy policies like a lawyer. In *YouTube*. https://www.youtube.com/watch?v=zZkY3MLBGh8

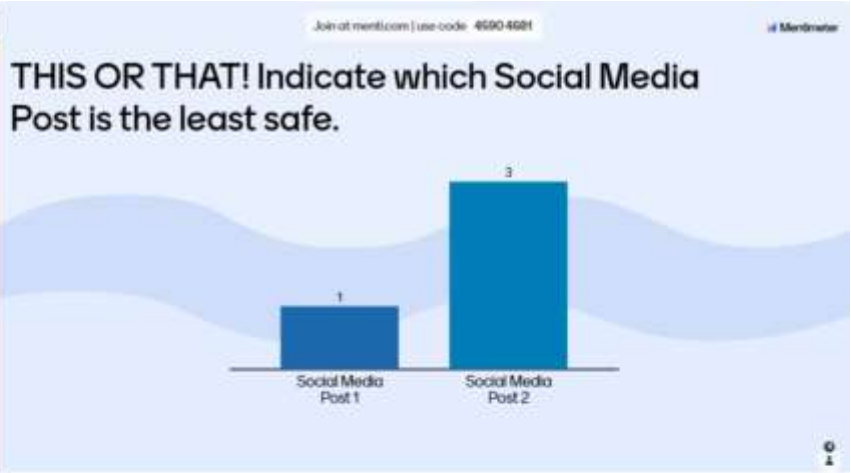
Zoom Video Communications. (2023). *Video Conferencing, Web Conferencing, Webinars, Screen Sharing*. Zoom Video. https://zoom.us

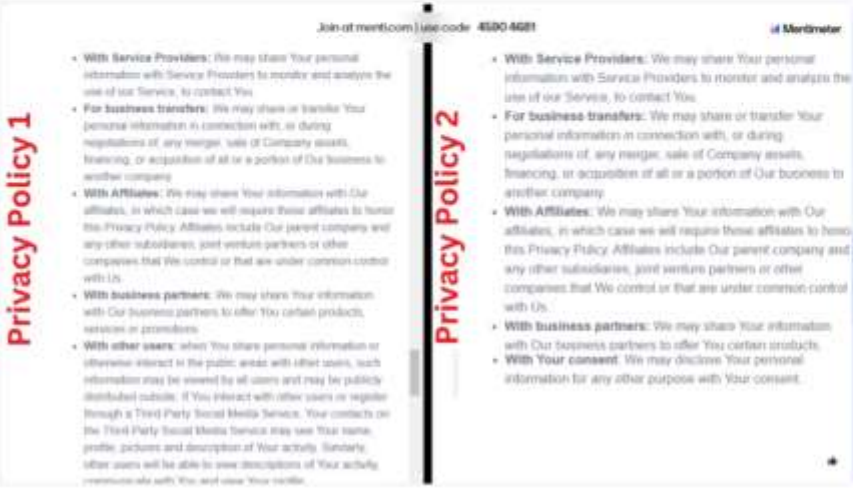
Appendix A


Join at menti.com | use code 4590 4681
Mentimeter
Determine if this information should or not be shared with just anyone
No
Yes
Your Legal Name
Your social security number
Favorite bands or musicians
A personal photo or video of your face
Your fingerprints
Your birthdate
Your personal IP address
A video of you singing

Appendix B


Social Post 1
Join at menti.com | use code 4590 4681
Social Post 2
I love when there's icicles on my house
703
ADAMS STREET


Join at menti.com | use code 4590 4681
Mentimeter
THIS OR THAT! Indicate which Social Media Post is the least safe.
1
3
Social Media Post 1
Social Media Post 2

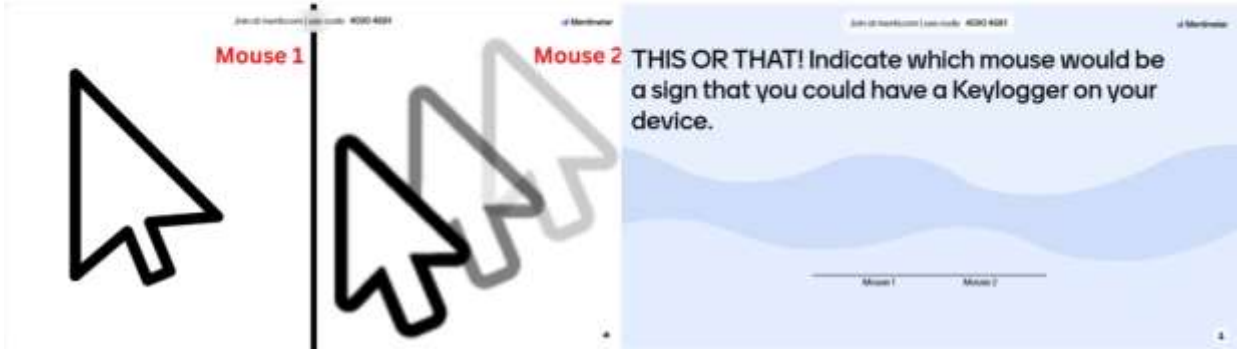

Join at menti.com | use code 4590 4681
Mentimeter
Privacy Policy 1
Privacy Policy 2
With Service Providers: We may share Your personal information with Service Providers to monitor and analyze the use of our Service, to contact You.
For business transfers: We may share or transfer Your personal information in connection with, or during negotiations of, any merger, sale of Company assets, financing, or acquisition of all or a portion of Our business to another company.
With Affiliates: We may share Your information with Our affiliates, in which case we will require those affiliates to honor this Privacy Policy. Affiliates include Our parent company and any other subsidiaries, joint venture partners or other companies that We control or that are under common control with Us.
With business partners: We may share Your information with Our business partners to offer You certain products, services or promotions.
With Your consent: We may disclose Your personal information for any other purpose with Your consent.


Join at menti.com | use code 4590 4681
Mentimeter
THIS OR THAT! Indicate which Privacy Policy has the best interest of the user.
Privacy Policy 1
Privacy Policy 2

Appendix C


Hulu Email 1
Hulu Email 2
We're Updating Our S
Agreement
THIS OR THAT! Indicate which email from Hulu is the email that can be taken seriously.


McAfee
462030
Virus Scan 2
THIS OR THAT! Indicate which McAfee display should be an indicator of Malware on your device?

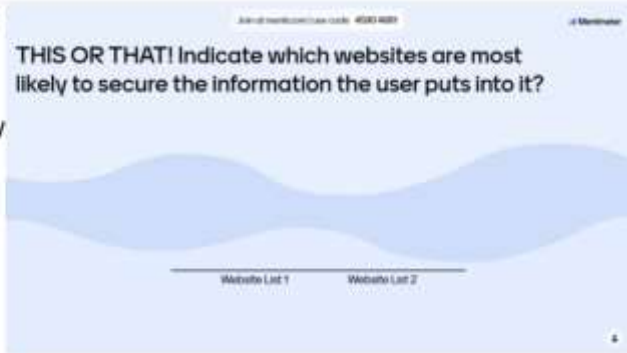

Mouse 1
Mouse 2
THIS OR THAT! Indicate which mouse would be a sign that you could have a Keylogger on your device.

Appendix D


Password List 1
1. 123123
2. abc123
3. qwerty123
4. 1q2w3e4r
5. adminHere
6. qwertyuiop
7. Amaz0nPa55w0rd!
8. AmericaTheBeautiful
9. iLov3U
10. pr1nc355
Disclaimer:
Do not use any of these passwords, even if they are declared "good". They are only for examples.
Password List 2
1. +his1sAl0ngPa55w0rd!
2. 0nc3Up0nA+iMe?
3. !0v3A!waY$
4. A74321%08005ms
5. $illygooseintheMeadow4e
6. pi3$cak3$pastreee$
7. AmazonDachshund254!
8. P!3as3!ov343v3r
9. PiQuadraticMathTeacher1!
10. JackofTradesMasterof0?


THIS OR THAT! Indicate the passwords that would be the most secure to use (as examples only).


Disclaimer:
These are real websites. Please be cautious.
Website Lists 1
• http://web.simmons.edu/~grovesd/comm244/notes/week2/links
• http://www.cs.sjsu.edu/~pearce/modules/lectures/web/html/HTTP.htm
• http://info.cern.ch/
Website Lists 2
• https://www.simmons.edu/
• https://www.sjsu.edu/cs/
• https://ace.edu/degree-programs/


THIS OR THAT! Indicate which websites are most likely to secure the information the user puts into it?


Network 1
Hidden Network
Network 2
Hidden Network


THIS OR THAT! Indicate which of these Wi-Fi networks will give the warning, "Other people might be able to see info you send over this network."

Appendix E

Module 3 Post-Course Student Reflection: Changed Practices Template

Use the questions below as a guide to develop a plan for what changes you will make in your everyday and educational cyber use.

1. Based on what you learned through this training, what are your current cybersecurity strengths?

2. Based on what you learned through this training, what areas do you currently have the most opportunity for growth?

3. What steps do you need to take to improve your cybersecurity practices?

4. What are 2-3 steps you can take to help create better cybersecurity practices for yourself and those around you?

5. What do you think is the most important aspect of this training for you personally and for those you work with?

6. If you were to lead a training course on cybersecurity, what topics or information would you need more support or resources for?