OMB Control Number: 1910-5160 Expiration: 2/28/2026

Paperwork Reduction Act Burden Disclosure Statement

This data is being collected to gather feedback and test knowledge of attendees for their understanding of the topic during the training session. The data you supply will be used for understanding where more training is needed and how to shape the content for future training sessions. The data will be collected through Menti, which is an online tool that is free for users and easy to use. This tool is also interactive, which is one of the goals of the training team to spark discussion and engagement with the content presented in the training.

Public reporting burden for this collection of information is estimated to average 1 minute per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of the Chief Information Officer, Enterprise Policy Development & Implementation Office, IM-22, Information Collection Management Program (1910-5160), U.S. Department of Energy, 1000 Independence Ave SW, Washington, DC 20585; and to the Office of Management and Budget (OMB), OIRA, Paperwork Reduction Project (1910-5160), Washington, DC 20503.

Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a currently valid OMB control number.

Submission of this data is voluntary.

Polling: Mentimeter

Set-Up Instructions:

1. Open your preferred web browser on your workstation or mobile phone.
2. Go to Menti.com.
3. Enter code.

Tips for Participating in Activities:

- Keep Menti open in the background for quick access.
- Adjust your screen to view both Teams & Menti (on workstation).
- Follow Menti prompts to participate!

Do not enter any PII (ex: full name).

Need Assistance?

Mentimeter

Use Teams Chat to send a direct message to the CSAT Team

Draft CAM gameshow questions

7/19/23

Passwords

- If you use a zero-knowledge password manager, who has access to the encryption keys needed to read your passwords? a) The password manager company b) Your employer c) Paying third-parties d) None of the above (Answer: D)

- According to a recent report from NordPass, what was the most popular password in the United States in 2022? a) Password b) 123456 c) guest d) a1b2c3 (Answer: C)

- Before computers, what word was synonymous with "password" in a military context? a) Passphrase b) Watchword c) Keyword d) Captcha (Answer: B -- Roman historians give detailed accounts about how the Roman military used passwords and watchwords 2,100 years ago)

- TRUE or FALSE: Passwords should have personal meaning to you (e.g. like a relative's birthday) so that you can remember them more easily. (Answer: False)

- The NCA says that it's ok to reuse a password how many times? a) 0 b) 2 c) About 10 d) You can reuse a strong password as many times as you want. (Answer: 0)

- TRUE or FALSE: A complex password is better than a long password. (Answer: False – length trumps complexity, but the best passwords are at least characters long, have a mix of characters and are unique to each account)

- What term refers to a hacking method where a cybercriminal attempts every possible combination of characters until the correct password is discovered? A) Guessatron B) Brute Force Attack C) Jiffying D) Reverse Human Determination Tactics (RHDT) (Answer: B)

- How long does the NCA recommend a master password for a password manager be? A) 8 characters B) 12 characters C) 15 characters D) 27 characters (Answer: C)

- How often will your bank email you and request a confirmation of your password? a) Once a month b) Once every 6 months c) Annually d) Never (Answer: D)

- Which of these passwords is the most secure? a) P@ssword b) p$$wo3d c) p8s$w0rD!! d) purple horse robin tree (Answer: D – length trumps complexity)

Phishing

- TRUE or FALSE: Phishing attacks are only delivered via email. (Answer: False – cybercriminals launch phishing attacks through phone calls, direct messaging, and text)

- What is the name of a software application that automatically downloads or displays marketing banners or pop-ups when a user is online? a) phishing b) update c) adware d) popware (Answer: C)

- If you click on the link in a phishing email sent to your work email address, what action should you take? a) Delete the email b) Unplug your device c) Report the incident to IT d) Change all your passwords (Answer: C -- reporting the incident should be your first step if you've already clicked on a malicious link)

- What is the cybersecurity term for when a fraudster uses a technique to disguise themselves as a known or trusted source? a) Spoofing b) Copycatting c) Match cutting d) Cybermirroring (Answer: A)

- TRUE or FALSE: The Internal Revenue Service will occasionally contact you via SMS text message? (Answer: False)

- A "smishing" attack is a phishing attack via what form of communication? a) Software b) Text message c) Snail mail d) None of the above (Answer: B -- the name comes from SMS text message phishing)

- What do cybercriminals call a phishing attack against senior executives or high-profile individuals? a) Crabbing b) Lobster-potting c) Phly Phishing d) Whaling (Answer: D)

- What two ingredients could a cybercriminal mix in 2023 to create a “spear-phishing” attack that targets you specifically? a) email and TikTok b) Apple Vision Pro and DMs c) social media and large language AI models d) LinkedIn and Taylor Swift’s *Eras* tour (Answer: C -- hackers can crawl through your public social media profiles, put them in ChatGPT, and it can create a super-believable tailored email)

MFA

- What is one of the “factors” used in multi-factor authentication? a) Your password b) Your credit card c) Your birthdate d) Your social security number (Answer: A)

- TRUE or FALSE: Multi-factor authentication can include biometric factors like fingerprint or facial scans. (Answer: True)

- What does the acronym 2FA stand for? a) Two-faced authenticator b) Two-factor authentication c) Two-facet administration d) Two-algorithm AI (answer: B -- it is another name for MFA)

- Which model of iPhone was the first to feature Face ID, Apple's facial recognition system that permits for biometric authentication? a) iPhone 3G b) iPhone 7 Plus c) iPhone X d) Face ID does not exist for iPhones (Answer: C -- the iPhone X was released in 2017, and all later models have this feature. Android first released a form of facial unlock in 2011)

- TRUE or FALSE: MFA is only available for highly sensitive accounts like banking, not more commonly used accounts like social media. (Answer: False)

- Which form of MFA is worse to use than having no MFA? a) Text message b) Stand-alone app c) Fingerprint scan d) None of the above (Answer: D -- any form of MFA is better than not having MFA)

- TRUE or FALSE: Captcha, like when a website asks you to identify all the stoplights in a photo, is a form of MFA. (Answer: False)

- According to CISA, how much can implementing MFA increase the security of an account? a) 43% b) 67% c) 89% d) 99% (Answer: D)

Software updates

- TRUE or FALSE: Setting your devices to automatically download and install updates can help prevent ransomware attacks? (Answer: True)

- As of 2022, what is the percentage of PCs in the world that still run Windows XP (released in 2001 and Microsoft officially ended support in 2009): a) 0% b) 0.4% c)7% d) 23% (Answer: B -- Windows XP is still used on the majority of PCs in certain countries, including Armenia)

- TRUE or FALSE: Software companies put out updates mostly to allow for more advertising. (Answer: False -- software updates typically include important security updates)

Identity theft

- Which credit bureau was the victim of a massive data breach in 2017? a) TransUnion b) Equifax c) Experian d) Chase (Answer: B -- the data of almost 148 million Americans was compromised)

- TRUE or FALSE: Freezing your credit is free. (Answer: True -- it also doesn't impact your credit score)

Other

- Social ___ is the name of a threat where a bad actors trick others into revealing sensitive information, like if a scammer posed as a tech support specialist to get access to a network. a) danger b) trending c) engineering d) response (answer: C)

- What federal agency is the parent executive department of the Cybersecurity and Infrastructure Security Agency (CISA)? a) State Department b) Department of Justice c) Department of Health and Human Services d) Department of Homeland Security (Answer: D)

- What toy was banned from National Security Agency premises in 1999 over concerns that it might be a surveillance device? a) Furby b) Tickle-Me Elmo C) Tamagotchi D) Beanie Babies (Answer: A -- the Furby actually had no recording technology, and Tiger Electronics president Roger Shiffman declared "Furby is not a spy!" The ban was later lifted, but later generations of Furby could connect to the internet and record audio)

- TRUE or FALSE: Web addresses that begin with HTTPS are more secure than ones that start with HTTP? (Answer: True -- HTTPS addresses are encrypted)

- What does the "I" in CISO stand for? a) Information b) Interim c) In-cybersecurity d) Internet (Answer: A -- CISO stands for Chief Information Security Officer)

- You can use a VPN (virtual private network) to replace your: a) Password manager b) Anti-virus software c) MFA d) None of the above (Answer: D)

- Turning off location tracking on your phone prevents it being tracked by: a) Cell phone towers b) Public Wi-Fi c) GPS d) All of the above (Answer: C)

- What insect shorted out an early supercomputer and inspired the term "computer bug"? a) Moth b) Roach c) Fly d) Japanese beetle (Answer: A)

- Which of these platforms is NOT a generative artificial intelligence (AI) program? a) Bard b) ChatGPT c) Midjourney d) MakeBelieve (Answer: D)

- TRUE or FALSE: It is better to back up your data to an external hard drive than the cloud. (Answer: False – neither external back ups nor the cloud is inherently better, as long as you remember to do it. In fact, we recommend backing up your data both ways!)

- Your home wireless network configuration should include: a) WPA2, unique password, and WPS disabled b) WEP, unique password, WPS enabled c) WPA2, default password, WPS disabled d) WPA, default password and WPS enabled (Answer: A -- WPA2 is an updated version of WPA, which stands for Wi-Fi Protected Access, and WPS stands for Wi-Fi Protected Setup)

Hackings

- What does the second "D" stand for in the cybercrime known as a DDoS attack? a) denial b) distributed c) drive d) desktop (Answer: A -- DDoS stands for "distributed denial-of-service")

- Which term describes the underlying cybersecurity structure of an organization, as well as the technology and policies that support it? a) lattice b) architecture c) edifice d) skeleton (Answer: B)

- What is BEC is an acronym for in a cybersecurity context? a) Baseless engineered cybersecurity b) Business email compromise c) Byte email context d) Blockchain exiting coin (Answer: B)

- TRUE or FALSE: If your data is encrypted due to a ransomware attack and you pay the ransom, the cybercriminals are required to decrypt your data and give you access again. (Answer: False)

- A joint report by IBM and the Ponemon Institute found that 82% of ransomware attacks were against companies with fewer than how many employees? a) 25 b) 100,000 c) 1 million d) 1,000 (Answer: D)

- What is the term for a collection of internet-connected devices, including computers, servers, smartphones, and smart devices, that are infected and controlled by malware, usually unbeknownst to their owner? a) Dark web b) Botnet c) DDoS d) Blockchain (Answer: B)

- TRUE or FALSE: If a public Wi-Fi network at a café requires a password to use it, it is safe to connect to it and access an online bank account. (Answer: False)

- When browsing online, a new window pops up stating that a virus has been found on your computer. The window provides a button to click offering to resolve the issue. Your best course of action is to: a) Click on the button to remove the virus. b) Place your cursor

over the button and check the link's website address (URL). If the address looks legitimate, click on it. If it looks like a scam link, close the window. c) Close both the original browser window and the new "pop-up" window. Do not return to that site. d) Hit the back button and see if it goes away. (Answer: C)

Non-scored poll questions

Icebreakers

- OPEN ENDED: What sort of pet did you have?
- OPEN ENDED: Tell us about your breakfast.
- What are you most interested in learning about today? a) MFA b) Strong passwords c) Avoiding phishing d) Installing updates

About NCA

- YES or NO: Have you participated in Cybersecurity Awareness Month before?
- The National Cybersecurity Alliance's content library at staysafeonline.org costs how much to use? a) $49.99 b) $599.99 c) $0 d) $3.74 per month (Answer: C)
- Including this October, how many Cybersecurity Awareness Months have there been? a) 1 b) 5 c) 11 d) 20 (Answer: D)
- How many organizations and individuals became Cybersecurity Awareness Month Champions and received a free toolkit from NCA in 2022? a) 6,255 b) 4,890 c) 744 d) 58 (Answer: A)

Oh Behave! Poll questions

- I find cybersecurity intimidating. a) Strongly disagree b) Somewhat disagree c) Neither agree nor disagree d) Somewhat agree e) Strongly agree
- What is the typical length of your passwords? a) Under 6 characters b) 7-8 characters c) 9-11 characters d) Over 12 characters
- What is your preferred method of remembering multiple passwords? a) I write them down in a notebook b) I write them down in a document on my computer c) I store them in my phone d)
- I store them in my email e) I just remember them (without writing them down) f) I save passwords in the browser g) I use a password manager application

Closing thoughts

- What behaviors do you think you'll change because of this fun, life-changing game? a) Start using MFA b) Be better at recognizing phishing c) Start saving passwords in a password manager d) Generate strong, unique passwords e) Regularly install updates f) Back up your data