CENTER FOR DEMOCRACY & TECHNOLOGY

Cybersecurity in Education 101 - Review Quiz

Based on the material covered in the "Cybersecurity in Education 101" training material, select the best answer for each of the questions below and check yourself using the answer guide on the following pages.

Question 1:
Which of the following are benefits to keeping user accounts secure? (Select one)

- A. Malicious actors cannot steal a legitimate user's access to data or manipulate the system.
- B. IT and other technical staff can be confident they know who is accessing systems and their data and, in turn, ensure those users are properly trained.
- C. Security frameworks, like those that keep track of who accesses certain data, can be trusted to be accurate.
- D. All of the above.

Question 2:
What is a password manager? (Select one)

- A. A person who reviews all user passwords to ensure they are sufficiently strong.
- B. A tool that stores all of a user's passwords in one secure place so the user can select strong, unique passwords without having to memorize them all.
- C. Neither of the above.

Question 3:
What is OPSEC short for? (Select one)

- A. Opaque Secrecy - the practice of keeping security measures secret, rather than training staff on them, to avoid attackers from learning about the system.
- B. Operational Security - the practice of protecting systems against attacks that do not rely on software or hardware vulnerabilities, but rather on manipulating users or taking advantage of mistakes.
- C. Open Sector - the portion of a computer system that does not need to be secured because it does not contain important information.

Question 4:
What should you do if you think an email you got might be a phishing email? (Select one)

- A. Nothing, just delete it.
- B. Click on the link to see where it goes so you know for sure if it is a phish.
- C. Report it to IT staff.

Question 5:
Should you keep your software systems up-to-date by installing updates in a timely fashion? (Select one)

- A. Yes, because companies release patches that fix security flaws, and you want those fixes to be installed as soon as possible.
- B. No, because installing updates is annoying, and it doesn't make any difference to the security of a system.

Question 6:
Which of the following networks are too insecure to use for accessing sensitive information? (Select all that apply)

- A. A coffee shop wifi network with no password.
- B. A hotel wifi network with the password "jennysCoffee123".

CENTER FOR DEMOCRACY & TECHNOLOGY

Cybersecurity in Education 101 - Answer Guide

Question 1:
Which of the following are benefits to keeping user accounts secure? (Select one)

- ☐ A. Malicious actors cannot steal a legitimate user's access to data or manipulate the system.
- ☐ B. IT and other technical staff can be confident they know who is accessing systems and their data and, in turn, ensure those users are properly trained.
- ☐ C. Security frameworks, like those that keep track of who accesses certain data, can be trusted to be accurate.
- ☒ **D. All of the above.**

Answer: D
Explanation: Keeping individual accounts secure helps protect the overall systems by providing all three of the stated benefits.

Question 2:
What is a password manager? (Select one)

- ☐ A. A person who reviews all user passwords to ensure they are sufficiently strong.
- ☒ **B. A tool that stores all of a user's passwords in one secure place so the user can select strong, unique passwords without having to memorize them all.**
- ☐ C. Neither of the above.

Answer: B
Explanation: Password managers are tools that store all of a user's passwords in one secure place so the user can select strong, unique passwords without having to memorize every password. By making it easier to use strong passwords, password managers can help make systems more secure.

Question 3:
What is OPSEC short for? (Select one)

- ☐ A. Opaque Secrecy - the practice of keeping security measures secret, rather than training staff on them, to avoid attackers from learning about the system.
- ☒ **B. Operational Security - the practice of protecting systems against attacks that do not rely on software or hardware vulnerabilities, but rather on manipulating users or taking advantage of mistakes.**
- ☐ C. Open Sector - the portion of a computer system that does not need to be secured because it does not contain important information.

Answer: B

Explanation: OPSEC is short for "Operational Security," the practice of protecting systems against attacks that do not rely on software or hardware vulnerabilities, but rather on manipulating users or taking advantage of mistakes.

Question 4:
What should you do if you think an email you got might be a phishing email? (Select one)

- ▢ A. Nothing, just delete it.
- ▢ B. Click on the link to see where it goes so you know for sure if it is a phish.
- ☒ **C. Report it to IT staff.**

Answer: C
Explanation: Report phishes to IT staff right away so they can warn other users or try to block further phishes. Definitely do not click on any links, as this may introduce malware onto your system.

Question 5:
Should you keep your software systems up-to-date by installing updates in a timely fashion? (Select one)

- ☒ **A. Yes, because companies release patches that fix security flaws, and you want those fixes to be installed as soon as possible.**
- ▢ B. No, because installing updates is annoying, and it doesn't make any difference to the security of a system.

Answer: A
Explanation: Installing software updates in a timely way makes sure you always have the latest security fixes. Enabling automatic updates can make keeping your system up to date much more convenient.

Question 6:
Which of the following networks are too insecure to use for accessing sensitive information? (Select all that apply)

- ☒ **A. A coffee shop wifi network with no password.**
- ☒ **B. A hotel wifi network with the password "jennysCoffee123".**

Answers: A and B
Explanation: Both of these networks should be considered insecure, since a weak or easily-guessed password (like "jennysCoffee123") doesn't provide enough protection for sensitive data.