CENTER FOR
DEMOCRACY
& TECHNOLOGY

Ransomware in Education - Review Quiz

Based on the material covered in the "Ransomware in Education" 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:
What is ransomware?

- ☐ A. A malware that takes over email accounts to send out fake ransom notes to random people in an attempt to extort money without revealing the attacker's identity.
- ☐ B. A cyberattack that locks users out of their own system by encrypting the data, and holds the key for a ransom.

Question 2:
Which of the following are useful preventative practices for ransomware attacks? *(choose all correct answers)*

- ☐ A. Maintaining robust backups of systems and data.
- ☐ B. Keeping security practices secret from non-expert users at the school to avoid attackers learning about them.
- ☐ C. Keeping an additional "off-line" backup to improve the likelihood that there is at least one backup that is safe from infection.

Question 3:
What is a WORM backup?

- ☐ A. A "write once, read many" backup that cannot be edited or changed once it is written.
- ☐ B. An infected backup that contains a malware "worm."

Question 4:
Should schools test their backups before using them to restore systems after an incident?

- ☐ A. No, time is of the essence after an attack and testing backups wastes valuable time.
- ☐ B. Yes, because the backup may be infected with the same virus, and restoring from an infected backup may further damage the system.

CENTER FOR
DEMOCRACY
& TECHNOLOGY

Ransomware in Education - Answers

Question 1:
What is ransomware?

☐ A. A malware that takes over email accounts to send out fake ransom notes to random people in an attempt to extort money without revealing the attacker's identity.
☒ **B. A cyberattack that locks users out of their own system by encrypting the data, and holds the key for a ransom.**

Answer: B

Question 2:
Which of the following are useful preventative practices for ransomware attacks? *(choose all correct answers)*

☒ **A. Maintaining robust backups of systems and data.**
☐ B. Keeping security practices secret from non-expert users at the school to avoid attackers learning about them.
☒ **C. Keeping an additional "off-line" backup to improve the likelihood that there is at least one backup that is safe from infection.**

Answers: A and C

Question 3:
What is a WORM backup?

☒ **A. A "write once, read many" backup that cannot be edited or changed once it is written.**
☐ B. An infected backup that contains a malware "worm."

Answer: A

Question 4:
Should schools test their backups before using them to restore systems after an incident?

☐ A. No, time is of the essence after an attack and testing backups wastes valuable time.
☒ **B. Yes, because the backup may be infected with the same virus, and restoring from an infected backup may further damage the system.**

Answer: B