



Calendar

Question 1

Correct

Mark 2.00 out of 2.00

Flag question

Which two online activities pose high security risks? (Choose two.)

Select one or more:

- ☒ following email links that have already been scanned by the email server ✓
- ☐ creating a very complex password for a new account and storing it in a password manager service
- ☐ verifying a banking site URL before entering information
- ☒ sharing information on social media ✓
- ☐ using a VPN to access the Internet from a Wi-Fi hot spot

Refer to curriculum topic: 5.1.3

The two most risky online behaviors listed are these:

- Sharing news articles only with friends and family on social media. The more information shared on social media, the more an attacker can learn.
- Following email links that have already been scanned by the email server. Scanned emails can still contain forged links to malicious sites.

The correct answers are: sharing information on social media, following email links that have already been scanned by the email server

Show one page at a time

Finish review

Question 2

Correct

Mark 2.00 out of 2.00

Flag question

Which three passwords are the least secure? (Choose three.)

Select one or more:

- ☒ asdfghjkl ✓
- ☐ Ci3c0_Rock\$
- ☒ 135792468 ✓
- ☒ randolph ✓
- ☐ s3CurE_p@ss
- ☐ 34%cafe_!

Refer to curriculum topic: 5.1.3

Strong passwords should be at least 8 characters in length and include upper and lower case characters, numbers, and special characters.

Question **3**

Correct

Mark 2.00 out of
2.00

🚩 Flag
question

Which action can help reduce online risk?

Select one:

- ☒ only conduct transactions on websites after verifying the URL is correct
- ☐ only download programs with the most positive reviews on 3rd party websites
- ☐ only accept unsolicited software updates when logged into a secure network
- ☐ only click embedded links in email messages from friends



Refer to curriculum topic: 5.1.3

Malicious websites can easily be made to mirror official bank or financial institution websites. Before clicking the links or providing any information, double-check the URL to make sure it is the correct web page for the institution.

The correct answer is: only conduct transactions on websites after verifying the URL is correct

Question **4**

Correct

Mark 2.00 out of
2.00

🚩 Flag
question

What is a wireless router security best practice that limits access to only specific internal hosts?

Select one:

- ☐ disabling SSID advertisements
- ☐ enabling encryption
- ☒ MAC address filtering
- ☐ enabling the built-in firewall



Refer to curriculum topic: 5.1.3

Media Access Control (MAC) address filtering enables a wireless router to check the MAC addresses of internal devices trying to connect to it. This allows connections to be limited to only devices with MAC addresses known to the router.

The correct answer is: MAC address filtering

Question **5**

Correct

Mark 2.00 out of 2.00

Flag question

Match the security best practice to the description.

regularly testing incident responses	perform and test emergency response scenarios	✓
educating users	train users on security procedures	✓
employing access controls	assign user roles and privilege levels	✓
implementing human resource security measures	research and perform background checks on employees	✓

Refer to curriculum topic: 5.1.2

The correct answer is: regularly testing incident responses → perform and test emergency response scenarios, educating users → train users on security procedures, employing access controls → assign user roles and privilege levels, implementing human resource security measures → research and perform background checks on employees

Question **6**

Correct

Mark 2.00 out of 2.00

Flag question

What is used to identify a wireless network?

Select one:

- ☐ SPI
- ☐ MAC address
- ☐ IP address
- ☒ SSID



Refer to curriculum topic: 5.1.2

A wireless network is identified by a name which is known as the service set identifier or SSID.

The correct answer is: SSID

Question **7**

Correct

What is the goal of a white hat hacker?

Question 7

Correct

Mark 2.00 out of 2.00

Flag question

What is the goal of a white hat hacker?

Select one:

- ☐ validating data
- ☐ modifying data
- ☐ stealing data
- ☒ protecting data



Refer to curriculum topic: 5.1.1

White hat hackers are actually "good guys" and are paid by companies and governments to test for security vulnerabilities so that data is better protected.

The correct answer is: protecting data

Question 8

Incorrect

Mark 0.00 out of 2.00

Flag question

What are three examples of personally identifiable information? (Choose three.)

Select one or more:

- ☒ birth date
- ☒ vehicle fuel consumption
- ☐ home thermometer value
- ☒ bank account number
- ☐ vehicle identification number
- ☐ home water usage



Refer to curriculum topic: 5.1.1

Personally identifiable information is any data that is related to an actual person that when used on its own or in combination with other information can identify, contact, or locate a specific individual.

The correct answers are: bank account number, birth date, vehicle identification number

Question 9

Correct

Mark 2.00 out of 2.00

Flag question

What are two recommended steps to protect and secure a wireless network? (Choose two.)

Select one or more:

- ☐ Use the default SSID.
- ☐ Enable remote management.
- ☒ Update firmware. ✓
- ☐ Locate the wireless router where it is accessible to users.
- ☒ Use WPA2-AES encryption. ✓

Refer to curriculum topic: 5.1.2

Two best practices for securing wireless networks are to encrypt the wireless traffic with WPA2 encryption and to keep the wireless router firmware updated. This prevents data from being readable by an attacker and fixes any known bugs and vulnerabilities in the router.

The correct answers are: Update firmware., Use WPA2-AES encryption.

Question 10

Correct

Mark 2.00 out of 2.00

Flag question

Why would an IT person use Zabasearch?

Select one:

- ☐ to research an IoT device
- ☐ to research a business
- ☐ to research an app
- ☒ to research a person ✓

Refer to curriculum topic: 5.1.1

Zabasearch (www.zabasearch.com) is a comprehensive people search engine.

The correct answer is: to research a person

Question 11

Correct

Mark 2.00 out of 2.00

Flag question

Which three elements should be combined when creating a strong password? (Choose three.)

Select one or more:

- ☐ personal information
- ☒ combinations of letters and numbers
- ☐ pet names
- ☐ dictionary words
- ☒ phrases
- ☒ special characters



Refer to curriculum topic: 5.1.3

Strong passwords should have combined letters, numbers, special characters, phrases, and be at least eight (8) characters long.

The correct answers are: combinations of letters and numbers, special characters, phrases

Question 12

Correct

Mark 2.00 out of 2.00

Flag question

An employee is using a coffee shop Wi-Fi hotspot to access corporate email. What action can the employee take to reduce the security risk of using a hotspot?

Select one:

- ☐ Only click on embedded links in email messages from trusted colleagues.
- ☐ Scan emails with antivirus software.
- ☒ Encrypt traffic through a VPN.
- ☐ Verify the name of the sender of emails before opening them.



Refer to curriculum topic: 5.1.3

Attackers will often deploy fake Wi-Fi hotspots in public locations, such as coffee shops, to lure users. The attacker has access to all the information exchanged via the compromised hotspot, putting the unsuspecting users at risk. For this reason, always send data through an encrypted VPN when using a hotspot.

The correct answer is: Encrypt traffic through a VPN.

Question 13

Incorrect

Mark 0.00 out of 2.00

Flag question

How can a virtual assistant be a security risk?

Select one:

- ☐ Personal information could be leaked.
- ☐ Sensor options could be modified.
- ☐ Encryption protocols are not supported.
- ☒ Personal devices could be remotely seen.



Refer to curriculum topic: 5.1.3

The sensors could be used to access a home network and gain access to PCs and data. Personal information such as passwords or credit card information could be compromised.

The correct answer is: Personal information could be leaked.

Question 14

Correct

Mark 2.00 out of 2.00

Flag question

How are USB flash drives a security risk?

Select one:

- ☐ They cannot be encrypted.
- ☒ They have a controller that can be infected.
- ☐ They contain a remote sensor.
- ☐ They contain wireless antennas.



Refer to curriculum topic: 5.1.3

USB and thumb drives include a tiny controller that can be infected with malware. No antivirus scanning will detect the malware because it is contained in the controller and not in the data area.

The correct answer is: They have a controller that can be infected.

Question 15

Correct

Mark 2.00 out of 2.00

Flag question

What is a goal of performing a risk assessment?

Select one:

- ☒ valuing assets to justify security expenditures

