Chapter 5 Quiz

Due No due date **Points** 30 **Questions** 15 **Time Limit** None
Allowed Attempts Unlimited

Instructions

This quiz covers the content presented in **I2IoT 2.0 Chapter 5**. This quiz is designed for practice. You will be allowed multiple attempts and the grade does not appear in the gradebook.

There are multiple task types that may be available in this quiz. In some task types, partial credit scoring is allowed to foster learning. Please note that on tasks with multiple answers, points can be deducted for selecting incorrect options.

At the completion of the quiz, some items may display feedback. The feedback will reference the source of the content. Example: "Refer to curriculum topic: 1.2.3" - indicates that the source of the material for this task is located in chapter 1, section 2, topic 3.

Form: 35283

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	10 minutes	30 out of 30

Submitted Apr 10 at 3:10pm

Question 1 — 2 / 2 pts

How are USB flash drives a security risk?

- They contain a remote sensor.
- They cannot be encrypted.
- They have a controller that can be infected.

Correct!

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.

Question 2

2 / 2 pts

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

Correct!

- [x] Update firmware.
- [ ] Enable remote management.
- [ ] Locate the wireless router where it is accessible to users.

Correct!

- [x] Use WPA2-AES encryption.
- [ ] Use the default SSID.

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.

Question 3

2 / 2 pts

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?

Correct!

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

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.

Question 4

2 / 2 pts

What is a goal of performing a risk assessment?

- ( ) educating users in secure procedures
- ( ) restricting access to physical assets

Correct!

- (•) valuing assets to justify security expenditures
- ( ) outlining job duties and expectations

Refer to curriculum topic: 5.1.2
One of the goals of performing a risk assessment is to understand the value of protected assets so that security expenditurer are justified.

Question 5

2 / 2 pts

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

Correct!
- [x] bank account number
- [ ] home water usage

Correct!
- [x] birth date

Correct!
- [x] vehicle identification number
- [ ] home thermometer value
- [ ] vehicle fuel consumption

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.

Question 6

2 / 2 pts

How can a virtual assistant be a security risk?

Personal devices could be remotely seen.

Correct!

Personal information could be leaked.

Sensor options could be modified.

Encryption protocols are not supported.

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.

Question 7

2 / 2 pts

Why would an IT person use Zabasearch?

to research an IoT device

Correct!

to research a person

to research an app

to research a business

Refer to curriculum topic: 5.1.1
Zabasearch (www.zabasearch.com) is a comprehensive people search engine.

Question 8

2 / 2 pts

What is used to identify a wireless network?

Correct!

- (•) SSID
- ( ) MAC address
- ( ) IP address
- ( ) SPI

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.

Question 9

2 / 2 pts

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

- [ ] personal information
- [x] phrases

Correct!

- [ ] pet names
- [x] special characters

Correct!

- [ ] dictionary words
- [x] combinations of letters and numbers

Correct!

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.

Question 10

2 / 2 pts

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

Correct!

- [x] following email links that have already been scanned by the email server
- [ ] using a VPN to access the Internet from a Wi-Fi hot spot

Correct!

- [x] sharing information on social media
- [ ] 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

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.

Question 11

2 / 2 pts

Match the security best practice to the description.

Correct!	**implementing human resource security measures**	research and perform bacl ▾
Correct!	**employing access controls**	assign user roles and privi ▾
Correct!	**educating users**	train users on security pro ▾
Correct!	**regularly testing incident responses**	perform and test emergen ▾

Refer to curriculum topic: 5.1.2

Question 12

2 / 2 pts

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

Correct!

- (•) MAC address filtering
- ( ) disabling SSID advertisements
- ( ) enabling encryption
- ( ) 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.

Question 13

2 / 2 pts

Which action can help reduce online risk?

Correct!

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

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.

Question 14

2 / 2 pts

What is the goal of a white hat hacker?

stealing data

validating data

modifying data

Correct! 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.

Question 15

2 / 2 pts

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

Correct! 135792468

Ci3c0_RocK$

Correct! asdfghjkl

s3CurE_p@ss

34%cafe_!

Correct! randolph

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.