Home / I'm Learning / Introduction to IoT / Introduction to IoT - Chapter 5 / Chapter 5 Quiz

Introduction to IoT

Started on	Saturday, 26 November 2022, 1:39 PM
State	Finished
Completed on	Saturday, 26 November 2022, 1:44 PM
Time taken	5 mins 6 secs
Marks	29.00/30.00
Grade	**96.67** out of 100.00

Question 1

Correct

Mark 2.00 out of 2.00

What is a goal of performing a risk assessment?

Select one:

○ valuing assets to justify security expenditures   ✔

○ restricting access to physical assets

○ outlining job duties and expectations

○ educating users in secure procedures

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.

The correct answer is: valuing assets to justify security expenditures

---

Question 2

Correct

Mark 2.00 out of 2.00

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

Select one or more:

   personal information

   dictionary words

✓ combinations of letters and numbers   ✔

✓ special characters   ✔

   pet names

✓ phrases   ✔

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 **3**

Correct

Mark 2.00 out of 2.00

How are USB flash drives a security risk?

Select one:

○ They contain a remote sensor.

◉ They have a controller that can be infected.   ✔

○ They contain wireless antennas.

○ They cannot be encrypted.

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 **4**

Correct

Mark 2.00 out of 2.00

How can a virtual assistant be a security risk?

Select one:

○ Encryption protocols are not supported.

○ Sensor options could be modified.

◉ Personal information could be leaked.   ✔

○ 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 **5**

Correct

Mark 2.00 out of 2.00

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:

○ Verify the name of the sender of emails before opening them.

○ Only click on embedded links in email messages from trusted colleagues.

○ Encrypt traffic through a VPN.   ✔

○ Scan emails with antivirus software.

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 **6**

Correct

Mark 2.00 out of 2.00

What is used to identify a wireless network?

Select one:

○ SPI

○ SSID   ✔

○ IP address

○ MAC address

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**

Partially correct

Mark 1.00 out of 2.00

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

Select one or more:

✓ sharing information on social media   ✔

□ following email links that have already been scanned by the email server

□ verifying a banking site URL before entering information

□ creating a very complex password for a new account and storing it in a password manager service

□ using a VPN to access the Internet from a Wi-Fi hot spot

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

Question **8**

Correct

Mark 2.00 out of 2.00

What is the goal of a white hat hacker?

Select one:

○ validating data

○ stealing data

◉ protecting data   ✔

○ modifying 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 **9**

Correct

Mark 2.00 out of 2.00

Match the security best practice to the description.

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

Refer to curriculum topic: 5.1.2

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

Question **10**

Correct

Mark 2.00 out of 2.00

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

Select one:

◉ 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.

The correct answer is: MAC address filtering

Question 11

Correct

Mark 2.00 out of 2.00

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

Select one or more:

✓   birth date   ✔

     home water usage

     home thermometer value

✓   vehicle identification number   ✔

     vehicle fuel consumption

✓   bank account number   ✔

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 12

Correct

Mark 2.00 out of 2.00

Which action can help reduce online risk?

Select one:

○   only download programs with the most positive reviews on 3rd party websites

○   only click embedded links in email messages from friends

○   only conduct transactions on websites after verifying the URL is correct   ✔

○   only accept unsolicited software updates when logged into a secure network

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 **13**

Correct

Mark 2.00 out of 2.00

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 **14**

Correct

Mark 2.00 out of 2.00

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

Select one or more:

Use the default SSID.

✓ Use WPA2-AES encryption.   ✓

✓ Update firmware.   ✓

Enable remote management.

Locate the wireless router where it is accessible to users.

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 **15**

Correct

Mark 2.00 out of 2.00

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

Select one or more:

✓ 135792468 ✔

Ci3c0_RocK$

34%cafe_!

✓ randolph ✔

s3CurE_p@ss

✓ asdfghjkl ✔

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.

The correct answers are: randolph, 135792468, asdfghjkl

◄ Chapter 5: Terms and Concepts Practice

Jump to...

Read Chapter 6: Educational and Business
Opportunities ►

Terms and Conditions

Privacy Statement

Cookie Policy

Data Protection

Trademarks

Data Protection

Accessibility