

NCS A

Started on	Saturday, 14 January 2023, 4:24 PM
State	Finished
Completed on	Saturday, 14 January 2023, 4:40 PM
Time taken	16 mins 49 secs
Marks	24.00/24.00
Grade	100.00 out of 100.00

Question 1
Correct

Mark 2.00 out of 2.00

Flag
question

How can users working on a shared computer keep their personal browsing history hidden from other workers that may use this computer?

Select one:

- ☐ Reboot the computer after closing the web browser.
- ☐ Use only an encrypted connection to access websites.
- ☐ Move any downloaded files to the recycle bin.
- ☒ Operate the web browser in private browser mode.

Refer to curriculum topic: 3.2.2

When a computer user browses the web in private mode, the following occurs:

- Cookies are disabled.
- Temporary Internet files are removed after closing the window.
- Browsing history is removed after closing the window.

The correct answer is: Operate the web browser in private browser mode.

Mark 2.00 out of 2.00

Flag question


Select one:

- ☐ The user is on an unencrypted network and the password for the cloud storage service is viewable by the online printing service.
- ☐ The password entered by the user for the online printing service is the same as the password used on the cloud storage service.
- ☒ The cloud storage service is an approved application for the online printing service. ✓
- ☐ The account information for the cloud storage service was intercepted by a malicious application.

Refer to curriculum topic: 3.2.1

Open Authorization is an open standard protocol that allows end users to access third party applications without exposing the user password.

The correct answer is: The cloud storage service is an approved application for the online printing service.



A user is having difficulty remembering passwords for multiple online accounts. What is the best solution for the user to try?

Select one:

- ☐ Share the passwords with the network administrator or computer technician.
- ☐ Create a single strong password to be used across all online accounts.
- ☐ Write the passwords down and place them out of sight.
- ☒ Save the passwords in a centralized password manager program.

Refer to curriculum topic: 3.1.1


A password manager can be used to store and encrypt multiple passwords. A master password can be implemented to protect the password manager software.

Question 4

Correct

Mark 2.00 out of 2.00

Flag question



Which configuration on a wireless router is not considered to be adequate security for a wireless network?

Select one:

- ☒ prevent the broadcast of an SSID
- ☐ implement WPA2 encryption
- ☐ modify the default SSID and password of a wireless router
- ☐ enabling wireless security


Refer to curriculum topic: 3.1.1

A wireless router can be configured to not allow the SSID to be broadcast, but that configuration is not considered to be adequate security for a wireless network

Question 5

Correct

Mark 2.00 out of 2.00

 Flag question

Why do IoT devices pose a greater risk than other computing devices on a network?

Select one:

- ☐ IoT devices cannot function on an isolated network with only an Internet connection.
- ☒ Most IoT devices do not receive frequent firmware updates.
- ☐ IoT devices use unencrypted wireless connections.
- ☐ Most IoT devices do not require an Internet connection and are unable to receive new updates.

Refer to curriculum topic: 3.1.1

IoT devices commonly operate using their original firmware and do not receive updates as frequently as laptops, desktops, and mobile platforms.

The correct answer is: Most IoT devices do not receive frequent firmware updates.

Question 6

Correct

Mark 2.00 out of 2.00

Flag question

A user is surfing the Internet using a laptop at a public WIFI cafe. What should be checked first when the user connects to the public network?

Select one:

- ☐ if the laptop has a master password set to secure the passwords stored in the password manager
- ☐ if the laptop web browser is operating in private mode
- ☒ if the laptop requires user authentication for file and media sharing
- ☐ if the laptop Bluetooth adapter is disabled

Refer to curriculum topic: 3.1.1


When a user connects to a public network, it is important to know if the computer is configured with file and media sharing and that it requires user authentication with encryption.

The correct answer is: if the laptop requires user authentication for file and media sharing

Correct

Mark 2.00 out of 2.00

Flag question



As data is being stored on a local hard disk, which method would secure the data from unauthorized access?

Select one:

- ☒ data encryption
- ☐ two factor authentication
- ☐ a duplicate hard drive copy
- ☐ deletion of sensitive files

Refer to curriculum topic: 3.1.2

Data encryption is the process of converting data into a form where only a trusted, authorized person with a secret key or password can decrypt the data and access the original form.

Question 8

Correct

Mark 2.00 out of 2.00

Flag

question

What is the best method to prevent Bluetooth from being exploited?

Select one:

☐ Only use Bluetooth when connecting to a known SSID.

☒ Always disable Bluetooth when it is not actively used.

☐ Only use Bluetooth to connect to another smartphone or tablet.

☐ Always use a VPN when connecting with Bluetooth.

Refer to curriculum topic: 3.1.1

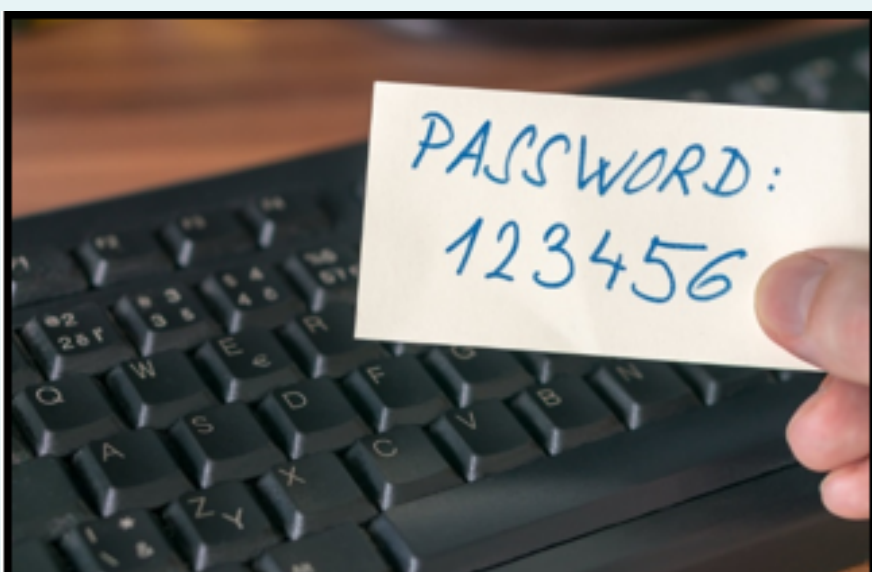
Bluetooth is a wireless technology that can be exploited by hackers to eavesdrop, establish remote access,

Question 9

Correct

Mark 2.00 out of 2.00

Flag question



A network administrator is conducting a training session to office staff on how to create a strong and effective password. Which password would most likely take the longest for a malicious user to guess or break?

Select one:

- ☐ drminjaphd
- ☐ super3secret12password1
- ☐ 10characters
- ☒ mk\$Scittykat104#

Refer to curriculum topic: 3.1.1

When choosing a good password:

Question 10

Correct

Mark 2.00 out of 2.00


Flag question

Do not use computer names or account names.

If possible use special characters, such as ! @ # \$ % ^ & * ().

Use a ten character password or more.

The correct answer is: mk\$Scitykat104#



How can a user prevent others from eavesdropping on network traffic when operating a PC on a public Wi-Fi hot spot?

Select one:

- ☐ Disable Bluetooth.
- ☐ Create strong and unique passwords.
- ☐ Use WPA2 encryption.
- ☒ Connect with a VPN service.

✓

Refer to curriculum topic: 3.1.1


When a user connects through an encrypted VPN tunnel on a public Wi-Fi network, any data being sent or

Question 11

Correct

Mark 2.00 out of 2.00

Flag question



Which type of technology can prevent malicious software from monitoring user activities, collecting personal information, and producing unwanted pop-up ads on a user computer?

Select one:

- ☒ antispyware
- ☐ firewall
- ☐ two factor authentication
- ☐ password manager

Refer to curriculum topic: 3.1.1

Antispyware software is commonly installed on a user machine to scan and remove malicious spyware software installed on a device.

Question 12

Correct

Mark 2.00 out of 2.00

🚩 Flag question

Which technology removes direct equipment and maintenance costs from the user for data backups?

Select one:

☐ an external hard drive

☒ a cloud service

☐ network attached storage

☐ a tape

Refer to curriculum topic: 3.1.2

The cost of cloud storage commonly depends on the amount of storage space needed. The cloud provider will maintain the equipment and the cloud user will have access to the backup data.

The correct answer is: a cloud service