Security Training Module – Review Questions

REVISED OCTOBER 2020

Introduction

Welcome to the Security Review Questions, the purpose of which is to see what you've learned by viewing the Security Training Module.

Question #1

What do you know **now**?

The spare Kensington key for our laptop should be stored in our purse or laptop bag during the day. True or False.

Physical Security

The answer is False.

The spare Kensington key for our laptop should be stored in a secure location, such as a locked cabinet or drawer, preferably in a location separate from where the Kensington lock is used.

Question #2

What do you know **now**?

Which of the following increase the security of the system? Select all that apply.

A – Encryption

B – Roles and features

C – Use of a router

D – Passwords

E – Unique usernames

System Security

The answers are A, B, D and E.

Encryption, assigning roles and features, unique usernames, and passwords all increase the security of the system.

The purpose of a router is to direct information between webservers and computers in a wireless network.   Although the connection is encrypted, it does not function to increase the security of the system.

Question #3

What do you know **now**?

The safest place to save documents with private information on them is on your agency's Share or Network Drive. True or False.

Data Storage

The answer is False.

Share or Network drives allow all users who have rights to them to access the documents saved to them. Those with private WIC information should be stored in a place where they can be viewed only by WIC staff and not other agency staff.

Question #4

What do you know **now**?

It is OK to walk away from our computer without locking it because WIC computers are set to auto-lock after 10 minutes of inactivity. True or False.

Physical Security 1

The answer is False.

We should always lock our computers before walking away from them. Although WIC computers are set to auto-lock after 10 minutes of inactivity, we should never leave our screens unprotected from unauthorized people inadvertently viewing them.

Question #5

What do you know **now**?

The WIC Information System tracks when users log in and log out. True or False.

System Security 1

The answer is True.

The WIC Information System tracks actions performed by each user based on their username. It creates a log and records when each users logs in, the duration of their session, and when the user logs out, as well as the workstation ID.

Question #6

The State uses the FileZilla FTP Site… Select one.

A – …because it is a secure site

B – …to store documents and reports that have private information

C – …to provide secure, encrypted document transfer

D – Answers A and B

E – All of the above

Electronic Communication

The answer is E – All of the above.

The State uses the agencygateway on the secure FileZilla FTP site to store documents and reports that have private participant data. When you download a file from FileZilla to a location on your computer, the transfer is both secure and encrypted.

Question #7

What do you know **now**?

Which of the following is true for deactivating staff who are leaving the WIC Program? Select one.

A – You should call the MN Help Desk as soon as you learn a staff person is leaving WIC

B – You can submit a form to deactivate your access if you are leaving WIC

C – The coordinator should submit a form when they first learn staff is leaving

D – The coordinator should submit a form to indicate the date staff are leaving 3-5 business days before their exit date

E – All of the above

Deactivations

The answer is D.

A WIC Information System User Access Form should be submitted by the Coordinator to indicate the date of a staff person’s subsequent departure. The form should be submitted at least 3-5 business days prior to the staff person’s deactivation date.

Question #8

What do you know **now**?

Our Windows password unlocks the encryption on our hard drive. True or False.

System Security 2

The answer is True.

The function of the Windows password is two-fold: It locks the computer to prohibit access by unauthorized users and it acts as a key to unlock the encryption on the hard drive so that the information is readable and usable.

Question #9

What do you know **now**?

Which of the following are NOT examples of keeping data physically secure? Select all that apply.

A – Locking your laptop in the trunk when leaving it in the car for brief periods of time

B – Locking your computer before walking away from it

C – Storing private data on mobile storage devices, such as flash drives

D – Immediately picking up a report with participant information from the printer

E – Recycling printed materials with private information on them

Physical Security 2

The answers are C and E.

Since most removable storage media, such as flash drives, are not encrypted and can be lost or stolen relatively easily, storing private data on them does not keep that information physically secure.

Printed materials with private information should be destroyed as appropriate, by disposing of it in the same manner as your agency disposes of other private data.

Question #10

What do you know **now**?

VPN adds another layer of security and is therefore required when teleworking. True or False.

System Security 3

The answer is False.

When working remotely, while our home network may be secure, the additional use of VPN is preferable because it protects the transmitted data with an additional layer of security.

However, VPN is NOT required for teleworking.

Question #11

What do you know **now**?

We can lock our computers using CTRL + L. True or False.

Physical Security 3

The answer is False.

Computers can be locked using: Windows key + L or CTRL + Alt + Delete, then pressing the Enter key.

Question #12

What do you know **now**?

We can automatically provide participant information as long as we know the person making the request. True or False.

Social Engineering

The answer is False.

Whenever a request for private information is made, whether via e-mail, phone or in person, and regardless of whether the person is known to you, you must verify the person has been authorized to have access to the information.

Question #13

What do you know **now**?

A flash drive should be stored in a secure location even once private information previously saved to it has been deleted. True or False.

Data Storage

The answer is True.

Once private information has been stored on a flash drive, it must always be treated as if it still has private information on it. Nothing is ever truly deleted until the storage device is actually destroyed.

Question #14

What do you know **now**?

What are the requirements for WIC Information System passwords? Select one.

A – Up to 16 characters, upper/lower case, special character, number

B – 8 - 16 characters, upper/lower case, special character, number

C – Can’t be the same as last 3 passwords

D – Answers A and C

E – Answers B and C

Passwords

The answer is B.

HuBERT passwords must be at least 8 characters long and no more than 16. They must include upper/lower case letters, at least one number and one special character, and they cannot be the same as the last 9 passwords used by that user.

Question #15

What do you know **now**?

It is best practice to only send State WIC IDs, not names, when communicating about participants via e-mail. True or False.

Electronic Communications

The answer is True.

It cannot be assumed that e-mail is secure. In order to maintain privacy when communicating about participants via e-mail, we should never use names and always use the State WIC IDs (or Household IDs) when referring to participants in email.

End Slide

Thank you! You have completed the WIC Security Training provided by the MN Department of Health WIC Program.

Minnesota Department of Health - WIC Program 85 E 7th Place, PO BOX 64882, ST PAUL MN 55164-0882; 651-201-4444, health.wic@state.mn.us, www.health.state.mn.us; To obtain this information in a different format, call: 651-201-4444