Security Training Review 2 – What do you know now?

SCRIPT - REVISED AUGUST 2025

Introduction

Welcome to the Security Training Review 2 module for all WIC Program staff provided by the Minnesota Department of Health WIC Program.

The purpose of this module is to see what you know now that you've reviewed the Security Training 2 module.

Overview

This module has at least one true/false, multiple choice, or fill-in-text question for each of the following topics: physical security and system security.

If you prefer to read the questions and answers yourself, feel free to mute the audio.

There is no requirement for how many questions you answer correctly.

Set a goal, 100% maybe, and see how you do.

Physical security

Review question 1

What do you know **now**? Multiple Choice. Select all that apply.

Which of the following statements are true about physical security?

A) CONTROL + L locks our computer.

B) A computer lock should be secured to a fixed, stationary object.

C) We should never leave our computer equipment in a car when traveling.

D) We should never send documents with private information to a personal or home printer.

E) Printed documents with private data should be recycled once were done reviewing/using them.

Answer 1

The answers are: B, C, and D.

Whenever we leave our computers, we should use Control + Alt + Delete or the Windows key + L (A) to lock our computers and if we have a physical lock, it should be secured to a fixed non-movable object (B).

When traveling, we should always keep our computer equipment with us and never leave it in the car, not even locked in the trunk (C).

As for printed documents with private information, they should **never** be sent to our personal or home printer (D) and once we are done with them, we should destroy them in the same way our agency destroys other confidential documents (E).

Review question 2

What do you know **now**? Enter 1 word into the text field (not case-sensitive) and click the Submit button.

Reports and documents with private data should always be stored in a secure place, such as a _____ drawer or file cabinet when not using or viewing them.

Answer 2

The answer is: locked

Documents must be secured just like access to our computer.

Leaving documents containing private data out for anyone to be able to view is neglecting our responsibility to our participants to protect their confidential information.

System security

Review question 3

What do you know **now**? Multiple choice. Select one.

Which of the following does **not** increase security?

A) Requiring full-disk encryption for all computers used for WIC.

B) Sharing our password with our supervisor in case they need to login to our computer.

C) Tracking system logins, logouts, and actions performed.

D) Limiting browser sessions to 30 minutes without a server call.

E) Requiring a certain level of password complexity.

Answer 3

The answer is: B.

Sharing our password? Never. It is private and should **never** be shared with **anyone** (B).

Requiring full-disk encryption (A), tracking our use of the information system (C), limiting inactive browser sessions (D), and ensuring our password meet basic requirements (E) are all ways that we increase security.

Review question 4

What do you know **now**? Multiple choice. Select all that apply.

What are some of the common pitfalls we should avoid when creating our passwords?

A) Using a passphrase that is easier to remember.

B) Using correctly spelled words.

C) Using names or pet names.

D) Using the first letters of words in a title, song, or poem.

E) Using celebratory dates, personal information, or favorites.

Answer 4

The answers are: B, C, and E.

Some of the common pitfalls when creating passwords include using correctly spelled words (B), names or pet names (C), keyboard sequences, personal info, celebratory dates (birthday, anniversary, etc.), favorite teams, numbers, and movies (E).

Using a passphrase (A) or the first letters of words in a title, song, or poem (D) are methods that use mnemonics to help us create and remember complex passwords.

Review question 5

What do you know **now**? True or false.

We should use the Remember Me toggle on the Multi-factor Authentication (MFA) page so that when our co-worker logs into our computer at lunch, she won't have to enter the MFA code.

Answer 5

The answer is: false**.**

The Remember Me toggle on the MFA page allows us to bypass the MFA process if we have to login more than once on a specific day (this "bypass" expires at midnight).

However, if we share our computer with others, we should not toggle on Remember Me. **We are all required to get the MFA the first time we login each day.**

Review question 6

What do you know **now**? A single word belongs in all three of the blank fields.

We must only ever be logged into “blank” environment at a time, have the information system open in “blank” browser window or tab at a time, and be logged into “blank” workstation at a time.

What is the word?

Enter the word into the field and click submit.

It is not case-sensitive.

Answer 6

The answer is: one.

To ensure user access security, we must never be logged into more than **one** environment at a time (such as Production and Training), have the information system open in more than **one** browser or browser tab at a time, or be logged into more than **one** workstation at a time.

Review question 7

What do you know **now**? Multiple choice. Select one.

Which of the following statements about deactivations is true?

A) Deactivation puts access on hold in case a staff person returns to WIC after leaving.

B) Deactivation is not a security measure.

C) We should deactivate users with planned absences lasting one week or longer.

D) Our Coordinator must call the MN Help Desk immediately if a staff person quits without notice.

E) We should submit a form and provide a date to deactivate our username if we decide to leave WIC.

Answer 7

The answer is: D.

Our coordinator should call the Help Desk to immediately deactivate a username if the person leaves WIC unexpectedly (D) since deactivation is a security measure (B) that safeguards the system by removing access (A).

Our coordinator should also submit a form when staff leave WIC to deactivate the username (E) and should request a “hold” be put on a username if a planned absence is going to last 4 weeks or more (C).

References

The following were referenced in this module.

Click the button to continue.

- 9.3 Information System Software (https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/chsctns/ch9/sctn9_3.pdf)
- 9.4 Network, Browser, and User Access Security (https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/chsctns/ch9/sctn9_4.pdf)

Thank you

How'd you do?

Continue your annual security training with Module 3: Access, Storage, Communications, and Sites with Data.

End Slide

Thank you for reviewing this security review module provided by the Minnesota Department of Health WIC Program.

Revisions

March 2026 – separated review module into 3 based on contents of training modules; added questions re: email and user access security.

August 2025 – updated for WINNIE information system.

*Minnesota Department of Health - WIC Program, 625 Robert St N, PO BOX 64975, ST PAUL MN 55164-0975; 1-800-657-3942, **health.wic@state.mn.us**, **www.health.state.mn.us**; to obtain this information in a different format, call: 1-800-657-3942.*