Security Training 2 – Physical and System Security

SCRIPT - REVISED AUGUST 2025

Introduction

Welcome to the Security Training 2 module: Physical and System Security.

This training is for all MN WIC Program staff and is provided by the MN Department of Health WIC Program.

Overview 1

In this module, we'll take a look at physically securing our computer, practicing physical security to ensure data privacy, and system security, including logging in, user sessions, passwords, multi-factor authentication, and user deactivations.

Knowledge check 1

What do you know?

We perform security measures to protect participant information **and ourselves**. True or false.

Overview 2

Security measures have two primary purposes:

- Protect WIC participants' data and ensure they remain private.
- Attribute actions performed within the information system to the appropriate staff person.

Physical security

Common sense

Physical security is probably the easiest security measure to perform and also one of the easiest to neglect.

It is often a matter of practicing common sense.

Knowledge check 2

What do you know?

Securing our laptops or desktop computers with a Kensington Lock or equivalent locking mechanism to our desk chair is a simple way to practice physical security. True or False.

Lock computer

Using a Kensington Lock or equivalent locking mechanism to protect our laptops or desktop computers from theft is a simple way to practice physical security, and state-provided laptops and computers must be securely locked to a fixed stationary object (so not our chair).

Keys

This type of lock has two keys.

For desktops, **both** keys, and for laptops, one key, should be stored in a secure location separate from where the computer is being used.

For laptops, we should keep the second key on our person and **not** stored in a desk drawer or bag, where it might easily be found and used.

Knowledge check 3

What do you know?

It is OK to leave WIC hardware equipment in the car when traveling with a state-provided computer, scanner, or signature pad, as long as they are in a computer bag and locked in the trunk. True or False.

Traveling

Policy about traveling with our computer equipment has evolved to minimize risk.

Therefore, best practice, is to always keep our computer equipment with us when traveling.

We should never leave it in a vehicle, even if locked in the trunk.

Physical security & data privacy

Data protector

In WIC, one of our most important roles is data protector.

It is our responsibility to safeguard private data that are entrusted to us as part of our daily work in the WIC Program.

Knowledge check 4

What do you know?

Leaving our computer unlocked in our office or cube while “running to get something” is a security risk. True or false.

Locking computers

Locking our computers is one of the simplest ways to protect our participants’ data and ourselves.

We should make it a habit to always lock our computer before walking away from it by pressing Control Alt Delete and selecting lock computer or by pressing the Windows and L keys.

Knowledge check 5

What do you know?

It is OK to print a document with private participant information to a shared printer when working at our work site. True or false.

Printing materials

We should try to avoid printing reports or documents with private information.

However, this is sometimes necessary and unavoidable.

If using a shared printer at our work site, we should ensure we can pick up the document **immediately** after printing.

We should never send private information to a personal or home printer.

Printed materials

Never leave reports, or other documents with private data, in the open.

They should always be stored in a secure place, such as a locked drawer or file cabinet, when not using them.

Once printed materials are no longer being used, they should be destroyed and disposed of in the same manner our agency disposes of other private data.

Quick tip

Here is a quick tip: the State WIC ID is an anonymous individual identifier, and most reports and documents should have it.

We should always ask ourselves if we really need the private data, such as names, contact info, addresses, telephone #s, etc. before printing and remove them if we don’t.

We never know

We never know who may walk by our computer or our desk, whether it is a family member, a friend, a co-worker from a different department, another WIC participant, or office housekeeping staff, etc., none of whom is privy to information that may be displayed on our computer or printed documents.

Leaving our computer unlocked or documents containing private data exposed so that they can be viewed by anyone walking by is neglecting our responsibility as data protectors.

System security

Knowledge check 6

What do you know?

Our Windows login is a key to unlock encrypted information on our computer. True or false.

Windows login

We know our Windows login "unlocks" the computer so that we can use it and prevents access by other people, but it also acts as a key to unlock the encrypted information on our computer.

Any computer used for WIC must have "full-disk encryption".

This makes the information on the computer unreadable and unusable for anyone that does not have the Windows login “key” to unlock it.

Knowledge check 7

What do you know?

Which statement is NOT true about logging into the WIC information system? Select one.

A) The information system tracks when we log in and out.

B) It protects us from potential fraud.

C) The system only requires we login the first time we access it each day.

D) It protects private data from unauthorized access.

E) It is a security measure.

Logging in and browser session

We are required to log in with our unique username and individual passwords whenever we use the WIC information system.

This requirement is another security measure protecting WIC data from unauthorized access.

A browser session starts once we are logged in and sets a limit of 30 minutes.

This limit restarts each time we submit a server call (see WINNIE Tips - Session Settings on the MDH WIC website for more information about server calls).

This is another security measure that automatically logs us out if inactive, requiring us to login again if this occurs.

Click the button to continue.

User tracking

The system tracks when we are logged in, our computer's ID, our session duration(s), and when we logout, as well as many of the actions we perform while logged in, which means we can track fraudulent activities back to the user that performed them.

Keep passwords secret!

That is why it is so important that we don't share our passwords.

If anyone else were to learn our password, they could perform inappropriate actions, such as issuance fraud, that we could be held responsible for.

Knowledge check 8

What do you know?

After how many days does our WIC information system password expire?

Enter the number and click the Submit button.

Passwords

Our passwords expire every 90 days (another security measure).

Password requirements ensure a certain level of complexity, making it harder to guess and include 8 or more characters, one special character, one upper case, one lower case letter, and one number.

Use passphrases

Use a passphrase when creating a password.

These tend to be easier to remember, but more complex, which means harder to guess, and avoid the common pitfalls of using correctly spelled words, names or pet names, keyboard sequences, personal info, celebratory dates (birthday, anniversary, etc.), favorite teams, numbers, and movies.

Let's check out a couple of ways to make really strong passwords using phrases.

Click the Example #1 button.

Example #1

Choose the first letters of words in a title, song, or poem, such as:

Twas brillig and the slithy toves did gyre and gimble (from Jabberwocky by Lewis Carroll).

Swap out some of the first letters of each word for numbers and special characters and mix upper- and lower-case letters to create a really strong password: Tb@t$TD8aG.

Click the Example #2 button to see another method for creating passphrases.

Example #2

Choose an easy-to-remember phrase, such as “let’s get it done!”

Run the words together, add some capitals, swap symbols and numbers for a couple of letters, and we’ve made a really strong password: L3t$GEt!tD0n3!

Click the button to continue.

Knowledge check 9

What do you know?

We should develop a strong password, using a passphrase, and add a number at the end. Then we can just increase the number each time we need to change it so that it’s easier to remember after we change it. True or false.

Changing passwords

When we change our password, we should change it **significantly**.

The system will not let us reuse the last 9 passwords, but that doesn’t mean we should cheat the protective intention of this by just changing one letter or number.

That is not considered significant.

If you think your password has been compromised, be sure to change it immediately.

Remember, your password protects **you**!

Knowledge check 10

What do you know?

We can use a county-approved password manager software to save our passwords. True or false.

Password managers

Passwords must never be written down…we know we've all done it because in today's world we have so many passwords we need to remember, which is why we can use a **county-approved** password manager to help us out.

Password managers are a tool that requires one password to access its contents and allows us to store all of our usernames and passwords in one secure place.

Knowledge check 11

What do you know?

Multi-factor authentication, or MFA, is used to confirm our identity for our information system by sending an email to our own personal email account. True or false.

Multi-factor authentication (MFA)

Multi-factor authentication, or MFA, is also part of our daily login process and is used to confirm our identity by sending an email to our **individual county or agency-maintained email** address with a unique random code that must be entered to complete the login process for the information system each day.

Remember Me toggle

Our information system has a Remember Me toggle on the MFA page that, after entering our MFA code for that day, allows us to bypass the MFA process for any subsequent logins occurring on that same day. (The bypass expires at midnight.)

We should only toggle on Remember Me if no one else will be using our computer that day since every new login requires an MFA.

Knowledge check 12

What do you know?

As another security feature, WIC information system users have specific access to locations and are assigned roles that limit or allow access to system functions. True or false.

User access

In our information system, users have general access to participant information, but are assigned specific locations, the agencies and clinic we work at, and roles at those locations that limit where we can go and the functions we can perform, such as certification, benefit management, or agency administration (to name a very few).

All of this increases the system's security by limiting access to only what we need in order to do our job.

Click the button to continue.

User deactivations 1

When a staff person leaves WIC, we must deactivate their username to remove access to the information system.

This is to safeguard against potential malicious activities that could be performed in the information system to corrupt data, commit fraud, etc.

User deactivations 2

In the case of an unplanned staff departure, a Local Agency Coordinator or their designated alternate, **must call the Help Desk immediately** to have the username deactivated.

For planned absences lasting 4 weeks or longer, agency coordinators (or designated alternate) should submit a user request to place a temporary "HOLD" status on the staff person's username.

This "HOLD" can be removed once the staff returns.

Continue

We'll continue our security review for all WIC Program staff in the Security Training 3 module where we will look at access, storage, electronic communications, and sites with data.

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)

End Slide

Thank you for reviewing this Security Training 2 module provided by the MN Department of Health WIC Program.

Revisions

August 2025 – updated information and policies for new browser-based information system.

October 2020 – updated information and policies.

*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.*

This institution is an equal opportunity provider.