MN–ITS — Password Information

Revised: January 30, 2023

Review the information in the following sections to increase your MN–ITS password security:

- Password Do's
- Password Don'ts
- Creating Strong Passwords
- Avoiding Weak Passwords

When entering your User ID and password, the User ID is not case sensitive. The Password is case sensitive.

Do:

- Use a password that is easy to remember but hard to figure out, guess, or crack.
- Pick a password that you can type quickly without looking at the keyboard.
- Use a unique password for every password change.
- Memorize your passwords. The safest place to store your password is in your head.
- Lock your computer or use a password-protected screen saver before you leave your workspace.
- When receiving technological assistance, enter your password instead of telling it to your IT expert. Stay with your PC while receiving technical assistance.
- Change the password immediately if you have reason to believe that it has been disclosed to someone other than the authorized user or that security has been otherwise compromised.

Don't:

- Write down your computer password and post it on your monitor.
- Store your password in a computer file. Storing your password in a computer file, whether on your hard drive or on a floppy disk, can make it vulnerable to access by others.
- Share your password; you could be held responsible for any and all actions that someone else may take with your system privileges.
- Let anyone see your password or watch as you type it in.
- Use the same password for all your authentication needs.

Creating Strong Passwords

A strong password is one that is difficult for others to uncover or guess, but easy for you to remember. Follow these helpful hints to create a strong password:

- Use at least 8 characters (more characters used means a more secure password).
- Change your password annually.
- Do not use words that someone could guess as your password.
- Do not have more than three repeated characters.
- MN–ITS passwords must begin with an alphabetical character (A-Z, either upper or lower case).
- Use both alpha and numeric characters.
- Use upper and lower case characters in weird combinations.
- Combine punctuation or symbols with a particular word. For MN–ITS passwords:
  - Use these symbols: ! # $ % & ( ) * + , - . / : ; = ? @ [\ ] ^ { | } ~
  - Do not use these symbols: " ' < > &
- Combine misspelled words.
- Use a "passphrase" with numerical substitution. A passphrase is created by taking the first letter of every word in a phrase. For example, "I Do Not Like Green Eggs And Ham" would be

"IDNLGEAH." Now, if you substitute a number "3" for every "G" found in this phrase, you end up with a stronger password, "IDNL3EAH." (Do not use this example as your password.)
- Contain sounds of letters and numbers that, when spoken aloud, actually says something. The password "OU812" when spoken aloud says, "Oh, you ate one, too." Another example is "dbsabzb," that says, 'The bee is a busy bee."
- Embed words (fish and CRAB=fiCRABsh), unglue them (Ahmad=A+hmad) or interweave them ("cdaotg" interweaves "dog" and "cat").

Note: Do not use these examples as your password.

Avoiding Weak Passwords

- Avoid passwords that pertain to your personal life (the name of a family member or pet, your place of birth, your shoe size – your maternal grandmother's maiden name is a lot easier to find out than you think).
- Do not use numbers that someone could easily find out about you (your license plate, Social Security number, telephone numbers, or street address).
- Avoid the name of something that is important to you (your favorite food, recording artist, movie, TV character, place, sports team, hobby).
- Avoid names, numbers, people or other items associated with your organization.
- Avoid names of famous people, places, things, fictional characters, movies, TV shows, songs, slogans.
- Never use dictionary words from any language as the whole or part of your password. Most hacker programs are set up to try to guess dictionary words, and they use extensive dictionaries from dozens of languages. Even made-up languages or words from other published lists (like Tolkien's Elvish or Klingon) are vulnerable to hacker attacks.
- Passwords should not consist solely of a word in the dictionary (school, campaign) or the name of a person or place (mary, texas). You may base your password on a word or a name, but add some numbers, punctuation, or both within it. Don't put just one extra character at the beginning or the end (4mary, mary6, texas!).
- Avoid obvious replacements: s with $ (texa$), o with 0 (sch001), i or 1 with l (campalgn), e with 3 (tr33).
- Other common tactics that password-guessing programs try are reversing words (yram), duplicating (marymary), reflecting short words (maryyram), or playing games with upper or lower case (MARY, Yram, MaryyraM).
- Avoid making words plural, past tense, and removing the vowels.
- Avoid abbreviated words ("conseq" is just as bad as "consequence").
- Passwords that follow keyboard patterns (qwertyuiop) are weak choices. Not only do hackers know the common ones, but this class of passwords is vulnerable to "shoulder surfing." It is obvious to even a casual observer when a password like this is typed in.
- In choosing successive passwords, try to avoid falling into a recognizable pattern. If you always capitalize all the vowels, you effectively lose the value of the unusual capitalization. Do not always choose names of planets or other related themes for your passwords. Having two or three recognizable patterns is nearly as bad as sticking to one pattern all the time.

Return to MN–ITS: Home webpage
Return to the Minnesota Health Care Programs providers: Policies and procedures webpage