# Training Materials – Passwords

NORTHWEST TERRITORIES POWER CORPORATION
*Empowering Communities*

# Passwords are the last line of defense between a hacker and your personal information

## Most people use passwords to protect:

- Social media accounts (e.g. Facebook, Twitter, Instagram)
- Personal and corporate devices (e.g. laptops, cell phones)
- Email accounts (e.g. Gmail, Outlook, Yahoo)
- Online banking accounts
- Other third-party accounts (e.g. Amazon, PayPal, YouTube)

## Hackers can break your password by:

- Guessing common passwords: *123456*, *password*, *abc123*, and *qwerty* are among the most-used passwords.*
- Dictionary attacks against single common words or common passphrases
- Social engineering personal information to help guess passwords
- Monitoring Wi-Fi traffic: hackers connected to public Wi-Fi connections may be able to observe all information inputted by others connected to the same Wi-Fi, including user names and passwords.
- Sending phishing emails: hackers could send millions of emails that ask the victim to input their email user name and password.

*According to James Titcomb, Technology News Editor at *The Telegraph*

# Password requirements


NTPC requires every corporate password to:

- Contain at least 8 characters for standard accounts
- Contain at least 14 characters for privileged accounts (**Admin** and **OT access accounts**)
- Not contain the user's account name for parts of the full name that exceed two consecutive characters
- Contain characters from three of the following four categories
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)
- Be kept different from last 24 passwords
- Be kept different than any others used for services offered by the organization, or outside agencies.
- Be kept different from personal passwords.
- Not be shared with anybody else.

# Common mistakes


**Here are some common mistakes people make when creating passwords:**

- Simple passwords composed of common words are easy to guess.
  Examples: apple, rowboat, bumblebee, blizzard, password
- Passwords written down on a piece of paper or stored in plain text on a computer may be stolen by somebody with malicious intent.
- Using the same password for multiple websites is like having one key for multiple locks; if it's stolen, the thief can open them all.
- Using same password and incrementing numbers when changing.
  Examples: Snowmobiling!1, Snowmobiling!2, Snowmobiling!3

Are you guilty of making any of these mistakes?

# Password best practices

- ✓ Create passwords with a minimum length of 12 characters including complexity requirements of capitals, numbers and special characters
- ✓ Avoid using single common dictionary words or proper nouns
- ✓ Avoid using common passphrases such as iloveyou
- ✓ Never share your passwords with anybody, even if you trust them
- ✓ Keep your passwords secret by storing them only in your head *
- ✓ Use a different password for every website
- ✓ Don’t use common substitutions; i.e. 1 for l, 0 for o, @ for a, $ for s, etc.
- ✓ Use Multi-Factor Authentication (MFA) wherever possible

* Remembering multiple passwords can be difficult. Use a trusted password manager to keep track of your passwords for you.

# Creating a strong password


You can create a strong password in four steps:

| | | Example |
|---|---|---|
| 1 | Write down three common unrelated words<br>The more uncommon and unrelated the better | calcium pajamas certainly |
| 2 | Develop story to commit three unrelated words to memory easily | Should I apply calcium in my pajamas? Certainly! |
| 3 | Capitalize letters – random letters or whole words | calcium PAJAMAS certainly |
| 4 | Insert numbers and special characters to break up words and syllables, then add new capitals – mix it up, syllables are better to break up words used in dictionary attacks! | cal4cium8PAJAMAS*certainly<br>Or<br>calcium1PA-JA-MAS5cer&tainly<br>OR<br>calcium#P@JAMAS0cerTainly |

More-complex passwords may be harder to crack, but they are also harder to remember. Find the balance between these two factors when creating your passwords.

## RESOURCES

https://protonmail.com/blog/how-long-should-my-password-be/
https://protonmail.com/blog/protonmail-com-blog-password-vs-passphrase/
**Have I Been Pwned: Check if you have an account that has been compromised in a data breach**
**Simple Tricks to Remember Insanely Secure Passwords | PCMag**