Lakehead Public Schools

Password Best Practices

Passwords are part of our daily lives. We use them for school, work and throughout our personal life. This info graphic will cover best practices for creating a strong password, making sure your password is safe and what to do when you think and or know it's been compromised.

To learn more, visit: www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032

Creating A Strong Password

Knowing how to make a strong password is the first step in making sure your information is safe. The more complex your password is, the harder it is for someone to guess.

- **DON'T** use predictable phrases or dates (i.e. your birthday, family names, pet names.).
- **ADD** symbols, numbers and a combination of capital letters to add complexity.
- **USE** a password manager to help create and store your passwords.
- **CHANGE** default passwords to devices and accounts when required (I.e. admin/admin, 0000)

Taking Care Of Your Passwords

Using a password manager allows you to keep strong and unique passwords for all our accounts without having to remember them all!

- Use a journal or notebook and write your passwords down. Make sure to keep them in a safe and secure.
- You can download a password manager that has extensions for your browser, app for your phone, etc.
- **DON'T** Log into your password manager on public devices like school laptops, library computers, etc.

HOW DO CYBER CRIMINALS GET YOUR PASSWORDS?

Passwords are often acquired during data breaches. This is when a Cyber criminal attacks an organization and gets a hold of account information. Typically, this information is bought and sold around the Internet or held for ransom. Your stolen information can be used in trying to access your accounts.

Other ways include:

- Trying to access accounts using common known passwords (i.e. 000000, admin, 1234, and so on)
- Impersonating legitimate companies or people in your life to gain your password or account recovery information.
- Creating phishing emails (or text messages) leading you to fake websites that look legitimate. These sites will ask you for personal information.

Having different passwords for every account prevents a Cyber criminal from having larger reach into your accounts. This allows you to be able to stop them in their tracks faster!

WHY Protecting Your Accounts Is Important

Protecting your passwords for emails, banking and work is crucial. The following points are examples of risks associated with an account breach:

- Accessing other accounts of yours
- Using your accounts to message co-workers, family and friends pretending to be you
- Accessing personal information

What is a phishing attack?

"Phishing" refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information, or other important data in order to utilize or sell the stolen information. By masquerading as a reputable source with an enticing request, an attacker lures in the victim in order to trick them, similar to how a fisherman uses bait to catch a fish.

What To Do If Your Password Has Been Stolen

- **For work accounts** contact your IT department or Cybersecurity team to get help recovering your account.
- **For personal accounts:**
  - Change your password
  - Set up 2FA (Two-factor authentication)
  - Use a passkey (a secure, password-free authentication method allowing users to sign in to apps and websites using device-level biometrics [face/fingerprint], PIN, or screen lock.)
  - Make sure your passwords aren't part of any known password lists.