eHealth Saskatchewan

Enterprise Security Services

Reusing Passwords Puts You At Risk

RETHINK YOUR PASSWORD HABITS

Reusing credentials (i.e username, email, password) for multiple accounts might be convenient, but you are actually making it easier for hackers to gain access to your accounts and your personal information. All hackers need is one password, then they have the key to multiple accounts.

Even if a password was stolen years ago, you may still be using it today, which puts you at risk of cyber attacks like credential stuffing.

Hackers will use previously stolen log-in credentials and "stuff" them into websites and systems until a match is found.

Think Twice!

Avoid reusing a password, even if you think it's complex and difficult to guess.

Be the strong link!

- ☑ Always use unique passphrases or complex passwords. Don't use the same password for multiple accounts, websites, or devices.
- ☑ Enable multi-factor authentication (MFA) on your accounts where possible. MFA adds an additional layer of protection to help prove your identity.
- ☑ Follow the password standards and guidelines as set out in the policy: "CP606-2020 - Security - Password Management"
- ☑ Never share your password, or write it down.

If you suspect you've received a suspicious email, forward it (as an attachment) to emailsecurity@eHealthSask.ca and delete it from your inbox. Report any security-related incidents immediately to ServiceDesk@eHealthSask.ca

We appreciate your help in protecting the Saskatchewan health network.