RETHINK YOUR PASSWORD HABITS TO PROTECT YOUR ACCOUNTS FROM HACKERS

August 2020 ITSAP.30.036

You have online accounts for everything ranging from government services to online shopping. Each time you create a new account, you need to create a username and a password. Reusing these credentials (i.e. your username or email address and 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 they need is one password, and then they have the key to multiple accounts.

PASSWORD REUSE PUTS YOU AT RISK

User credentials are a high-value target because hackers know that people tend to use their passwords more than once. But how do they get access to your passwords in the first place? Hackers target organizations and individuals, taking advantage of vulnerabilities in systems and software, sending phishing messages, and disguising malware as legitimate files, all in an attempt to steal sensitive information like user credentials. Once they have this information, they can sell or post it online, making it widely available to other hackers. 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**. To protect yourself, avoid reusing a password, even if you think it's complex and difficult to guess.

CREDENTIAL STUFFING

In a credential stuffing attack, hackers use previously stolen log-in credentials (i.e. your username or email address and password) from one website and then "stuff" these credentials into the log-in pages of other websites and systems until matches are found. Hackers use tools such as botnets, which are collections of Internet robots or Internet-connected devices, and account checker apps to automate these attacks and test credentials on many websites. Once a hacker has access to an account, they can change your password, steal any associated credit card information, make unauthorized transactions, or conduct other fraudulent activities.

PASSWORD HABITS TO ADOPT

A password is the first line of defence for your accounts. Review the following password habits to make sure you are securing them effectively:

- Use a unique passphrase or password for every account.
- Enable multi-factor authentication (MFA) on your accounts where possible. MFA adds a layer of protection by requiring that you prove your identity in multiple ways when logging in (e.g. providing a security code or biometric). For instructions on setting up MFA on popular online services, see the following website: www.telesign.com/turnon2fa/tutorials
- Use a password manager (browser-based or stand-alone application) to help you remember your unique passphrases or passwords. Be sure to use a complex master password and enable MFA on your password manager account.

STEPS TO TAKE IF YOUR ACCOUNT IS COMPROMISED

If you suspect your account has been compromised, take the following steps to protect yourself:

1. Change your passphrase or password immediately. If you have reused this password for other accounts, be sure to change the passwords for those accounts.
2. Check your account information carefully. Make sure there are no unauthorized changes or transactions and, if applicable, change your security questions and answers.
3. Check your credit card and bank accounts for suspicious activity. If your credit card is linked to a compromised account, contact your bank.
4. Contact the Canadian Anti-Fraud Centre (www.antifraudcentre-centreantifraude.ca) and your local police if you suspect any fraudulent activity or if you are concerned about identity theft. You may also want to notify a credit bureau.

Visit the Cyber Centre website (cyber.gc.ca) to find related publications: *ITSAP.30.032 Best Practices for Passphrases and Passwords*, *ITSAP.30.030 Secure Your Accounts and Devices with Multi-Factor Authentication*, and *ITSAP.30.025 Password Managers—Security*.

AWARENESS SERIES