Rethink your password habits to protect your accounts from hackers

CANADIAN CENTRE FOR CYBER SECURITY

April 2024 | 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 for multiple accounts might be convenient, but it makes it easier for hackers to gain access to your accounts and your personal information. With one password, 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.

Hackers target organizations and individuals, taking advantage of vulnerabilities in systems and software, sending phishing messages, and disguising malware as legitimate files. Hackers use these techniques 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, using it today 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.

According to the Cyber Centre 41% of Canadians say they use the same password for multiple accounts

Credential stuffing

In a credential stuffing attack, hackers use previously stolen log-in credentials from one website and then "stuff" them into the log-in pages of other websites and systems until matches are found. Hackers use tools such as botnets (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
- conduct other fraudulent activities

Websites like monitor.mozilla.org can tell you if your email address or password appear on a list of stolen credentials.

Password habits to adopt

A password is the first line of defence for your accounts. Adopting appropriate password habits can help you secure them effectively:

- Use a new and unique passphrase or complex password for every account.
- Activate 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 such as providing a security code or biometric.
  - For instructions on setting up MFA on popular online services, see the UK's National Cyber Security Centre's Tips for staying secure online—Turn on 2-step verification.
- Use a password manager (browser-based or stand-alone application) to help you remember your unique passphrases or complex passwords. Be sure to use a complex primary password and activate MFA on your password manager account.
- Keep your passwords and passphrases private. Do not share them with anyone and avoid storing them in a public place, such as taped to the side of your computer or under your keyboard.
- Avoid using the "remember me" or "save password" options when using public or shared computers and always log out of your account when finished

Steps to take if your account is compromised

1. Change your passphrase or password immediately.
2. If you have reused this password for other accounts, be sure to change the passwords for those accounts and never use the hacked password or passphrase again.
3. Check your account information carefully to make sure there are no unauthorized changes or transactions and. If applicable, change your security questions and answers.
4. Check your credit card and bank accounts for suspicious activity. If your credit card is linked to a compromised account, contact your bank.
5. Contact the Canadian Anti-Fraud Centre 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.
6. Inform contacts of the breach as your account may be used to send phishing messages that appear to come from you.

Learn More

Consult the following guidance to learn more about the key points we have identified:

- Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101)
- Protect your organization from malware (ITSAP.00.057)
- Best practices for passphrases and passwords (ITSAP.30.032)
- Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)
- Password managers: Security tips (ITSAP.30.025)

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Canada

Cat. No. D97-1/30-036-2024E-PDF ISBN 978-0-660-71283-3