NPC Smarter Computing™

Cyber criminals are always looking for the weakest point of entry into our accounts. When your accounts contain your business data including clients' personally identifiable information (PII), it's even more important that your passwords not be the weak link.

The following eight tips will help you better secure your accounts by creating and managing the strongest possible passwords, and by adding a second layer of security so that your password alone isn't enough to gain access.

1 Use Passwords That Favour Length Over Complexity

Complex passwords are less secure than you might think because cyber criminals use automated processes to crack passwords; *brute force attacks* try every combination of characters to find the right one and *dictionary attacks* compare passwords against common words for a faster match.

Replacing letters with symbols makes it harder for humans to guess a password but won't slow down a computer that's trying to crack it. The amount of time it takes a computer to crack a password increases exponentially with each additional character, so longer passwords are much more secure.

Use a password with at least 14 characters when possible.

2 Use Passphrases for Convenience

Using a longer password could be more convenient and easier to remember than using a complex password. Try making your longer password into a phrase to make it easier to type and remember.

COMPLEX PASSWORD **Melis3a!**	LONG PASSPHRASE **melissa skate f@ll up**
8 characters	21 characters
Can be cracked in: **59.36 seconds**	Can be cracked in: **30 centuries**

3 Use a Secure Password Manager

When you have a long password for each of your accounts, you will probably want to use a password manager. Find one that is secure and reputable before trusting them with all of your logins.

We'd recommend using one that stores passwords locally (instead of in the cloud) and is locked by a fingerprint reader for added security and easier access.

4 Change Your Passwords Regularly, Every 90-120 Days

If a cyber criminal does obtain your password, they may be able to access your account and remain undetected for a period of time. Changing passwords regularly denies further access to anyone who may have been in your account without your knowledge.

5 Never Send Your Username and Password Together

If you do need to share login credentials or the password to an encrypted file, send both elements (username/password or file/password) separately, preferably using different methods of communication — share one via email and the other by phone call, for instance.

You should also never share or confirm a password through an unfamiliar website, email, text message, or phone call.

6 Never Use the Same Password Twice or In More Than One Place

When a cyber criminal does obtain a username and password, they will try to log in to other major websites using the credentials. Create a different password for each of your accounts, even seemingly less important ones like social media and streaming services.

91% of people know the risks of reusing passwords between online accounts. 66% of people do it anyway.[1]

7 Careful What Info You Share Online

Cyber criminals use social media and personal websites to crack passwords faster by scouring them for personal details that might be used in a password (like your birthdate or favourite sports team) or to bypass security questions (like your childhood pet's name or the model of your first car).

8 Enable Multi-Factor Authentication (MFA)

Account hacks often occur because of weak passwords that are easy to crack or passwords that have been exposed in a cyber attack. Enabling a second layer of security can prevent access to your account no matter how your password could be obtained.

Multi-factor authentication (MFA) is the use of two or more identification methods to verify your identity. These "factors" include something that only you *know*, like a password or PIN; something that only you *have*, like your phone or USB security key; and something that only you *are*, like your voice or fingerprint.

MFA can block over 99.9 percent of online account compromise attacks.[2]

Watch our Safe Computing Webinar, Enhancing Password Security and the Power of Multi-Factor Authentication, for more information and other tips to improve your password security.

NPC DataGuard

NPC specializes in secure managed computing solutions to help every business professional stay firmly ahead of emerging cyber threats. Let NPC alleviate the pressure on you to protect client data so that you can focus on building your business.

Sources:
(1) "Psychology of Passwords: The Online Behavior That's Putting You at Risk," Report by LogMeIn, Inc., March 13, 2020
(2) Melanie Maynes, "One simple action you can take to prevent 99.9 percent of attacks on your accounts," Microsoft Security, August 20, 2019

NPC DataGuard, a division of Compugen Inc.
1-855-667-2642
info@npcdataguard.com
www.npcdataguard.com