BRITISH COLUMBIA The Best Place on Earth | Ministry of Health Services

doctors of bc

Doctors Technology Office: Technical Bulletin

Creating Complex Passwords You Can Remember

DTO TB - #16-001	**Recommended Action re:** Use the following method to create complex passwords you can remember and write down.

Brief Description (Non-Technical): How long did it take for MS Word to let you know you have spelled a "WORD" wrong? With today's fast computers, it would not take long for a program to automatically try every word or names.
Until we have better and cheaper biometric security devices, passwords are still needed. The more complicated the password is, the harder it will be for hackers to discover it. The trouble is, how do we remember complex passwords, or come up with complex passwords.

Why are these two passwords very complex, and yet, hard for you to forget?
BCMA@6**04** and **DOBC@250.**

Solution: My personal encryption system to create complex passwords is to combine three unique parts that only I know very well. Each part must consist of data you **ALREADY know and remember**.

Personal Encryption: Combine part1 + part2 + part3 to create your password.

Examples of "Parts" You Can Use:

	Part 1	**Part 2**	**Part 3**
Definition	Use an Acronym	Use a special keyboard character	non-repeating, number (made up of)
E.g.	BCMA *	@	6 0 4
Denoted	**S1**	**WITH**	**1st; 2nd; 3rd**

This password can be written as **Part1 + Part2 + Part3** = **'S1 WITH 123'** to represent **'BCMA@604'**

The Key: (The non-repeating number should be **well known to you already**.)

- Vary the order of your non-repeating number.
  - 123 = 604
  - 321 = 406

Instead of using a three digit number, use a non-repeating **EIGHT** digit number.

If you have a system, when asked, you can make up complex passwords on the fly. Even write them down on Post-it notes. No one would understand your coding.

S1 WITH 12 = BCMA@60 or **S1 WITHout 23** = BCMA06

Author: Patrick Wong

Original Date Created: 2016-06-07 (updated 2016-12-08)

**Although using three separate encryption keys together makes hacking very difficult, avoid common acronyms such as BCMA. "BCMA" was used to make the example easier to follow. Instead, create unique acronyms as described on the top of page 2.*

Details and Additional Information (Technical):

Additional Examples of Part 1 (S1): (other ways to create part1)

- Using a phrase would be harder to guess. (avoid texting typed phrases)
  - E.g. [I love Paris in springtime (IlPis)]
- Unique industry acronym
  - PITO or p1T0 (old acronym no longer being used)
- Favorite city in another language
  - Cologne written as Koln or k0Ln (small k, zero, capital L, small n)

Additional Examples of Part 2 (WITH) (special characters): ~ ! @ # % ^ & * ( ) and so on.

Additional Examples of Part 3: (other ways to create the **8 digit number**)

- Portions of two membership numbers
- Old house number + new house number + street number
- Out of town area code + last 3 digits of a cell number + old apartment number
  - E.g. 1^{st}=**8**; 2^{nd}=**4**; 3^{rd}=**5**; 4^{th}=**3**; 5^{th}=**6**; 6^{th}=**7**; 7^{th}=**2**; 8^{th}=**1** = 84536721
    - NY city area code = 845
    - Portion of my cell number = 367
    - Old apartment number = 21

By using the more complex examples above, the passwords are now even harder to hack.

- S1with2345 = IlPis&4536
- S2with1234 = p1T0&8453
- S3without5678 = k0Ln6721

Having more than one Part 1 and Part 2 adds variety.

The key to the whole encryption system is Part 3, the eight digit, non-repeating number **that you must already know very well**. By changing which number you begin with, it's a totally different number.

Create a different pin for every card and token you have: (when you do not need all eight digits)

- My BMO credit card security number is 1234 = 8453
- My VISA bank card number is 2345 = 4536
- My HSBC debit card number is 123456 = 845367
- When I am given a temporary token number 6431, I write it on the back as 5248
  - When I have a chance, I change it to my first 4 numbers 1234 = 8453

If you have any questions or would like more information contact:
Doctors Technology Office, 604-638-5841, dtotechsupport@doctorsofbc.ca

Author: Patrick Wong *Original Date Created: 2016-06-07 (updated 2016-12-08)*

**Although using three separate encryption keys together makes hacking very difficult, avoid common acronyms such as BCMA. "BCMA" was used to make the example easier to follow. Instead, create unique acronyms as described on the top of page 2.*