Passphrases make stronger Passwords

Move to a passphrase today

Since July 2018 we have communicated the requirement for staff to move to a Passphrase for logging into the Council network. With effect from August 27th 2019 technology will now enforce the requirement to use a passphrase for logging into your Council computer / laptop. This means the next time you are asked to change your password you will be required to select a passphrase.

Use the information and documents below to find out about using a Passphrase.

Passwords

Passwords are the primary element used to secure access to data and systems. It is therefore important that they are complex and secure enough to provide the protection required.

Staff are responsible for protecting their user credentials and ensuring that passwords created provide ongoing security for data and systems they access however passwords can be weak due to poor choices at creation for example by using:

- o Dictionary words;
- o Known names;
- o Using variants of the word 'Password';
- o Using variants of a day or month such as 'June-2018'.

Even with adding some numbers and a symbol such passwords provide very little protection for data and systems they intend to protect and in the majority of cases can be easily cracked in a matter of minutes.

What is a Passphrase?

With a minimum of 9 characters passphrases provide a more secure and user-friendly alternative to the traditional password approach and by using a combination of words within a phrase makes it easier to remember or by using 3 random words. You either use a phrase known to you or select some random words to use.

What does the new technology do?

You will no longer be able to use a dictionary word or known name as the basis of your password. For example the following would not be permitted:

- o 9Ilovecapetown

- o Husky0619!!
- o Samanthay06
- o NewYork123
- o HarryPotter3!
- o Waspnation11%&
- o GlasgowRangers123
- o GlasgowCeltic321

Syntax

Passphrases still have to:

- o be 9 characters minimum
- o not contain your login name or part thereof
- o contain 3 out of 4 of the following:
  1. Uppercase Character (A through Z)
  2. Lowercase Character (a through z)
  3. Digit (0 through 9)
  4. Special Character (i.e. !,$,%,#)

Quickly Change to a Passphrase

Press Ctrl, Alt, Del and select "Change a password"

Passphrase Hygiene

Remember to **never** reuse passphrases across internet based applications or systems. These should always be unique. Use the 'Background to Passphrases' document for hints and tips on how to achieve this and consider attending tutor led training for more guidance.

Account Security

Where an internet based system provides the ability to use two factor authentication (2FA, sometimes referred to as MFA) always ensure you apply this. Using an authenticator app as opposed to SMS messaging, where available, would be the preferred option.

Subscribe to this page

Related documents

- o Passphrase Examples [14kb] [Subscribe]

  Examples of how to create a passphrase using a phrase known to you

- o Background to Passphrases [270kb] [Subscribe]

  Why passphrases make better passwords

- o Passphrases using 3 random words [14kb] [Subscribe]