

NWOCA Tech Note

Protecting yourself with Strong Passwords

Here are some tips on selecting strong passwords to use for email and other sites that require a secure login. These tips were provided by Sophos.

Try to avoid using any of the following as your password

- Words that contain less than 10 characters
- Words found in the dictionary
- Names of family, pets, friends, co-workers or fantasy characters etc.
- Computer terms, names, commands
- Birthdays, addresses or phone numbers
- Word or number patterns like aaabbb, qwerty 000007 etc.
- Any of the above spelled backwards

Strong Passwords have the following characteristics

- Are at least ten characters long and is a passphrase (“Oh my, I stubbed my toe!”).
- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Contains numbers & punctuation characters.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored online

- Try to create passwords – or, preferably, passphrases - that can be easily remembered.

Creating Passphrases

- Passphrases (passwords based on a phrase rather than a single word) are a very good way to generate strong yet memorable passwords. Sophos strongly recommends the use of passphrases. These types of passwords can be used directly, such as: “Passphrases are memorable & secure.”, or shortened in a memorable way: “Passphrases R m&s”.

Did you know?

Your eSIS password will need to be changed every 90 days.

Your email password will need to be changed every 200 days.



Some Resources for you.

- Video on pass phrase creation by Sophos
 - <http://www.youtube.com/watch?v=VYzguTdOmmU>
- Guidelines for Strong Passwords (Wikipedia)
 - http://en.wikipedia.org/wiki/Password_strength#Guidelines_for_strong_passwords
- On line password strength checker by Microsoft:
 - <http://www.microsoft.com/protect/fraud/passwords/checker.aspx>