Passwords vs. Passphrases

While you probably have a good idea of what constitutes a password, you may still be scratching your head over passphrases. Passphrases use a series of words, separated by spaces, dashes, or other separator characters, or not (it doesn't really matter) making them harder to guess than a single password. "correct horse battery staple" is an example of a passphrase. Although passphrases often contain more characters than passwords do, passphrases contain fewer "components" (four words instead of, say, 12 random characters); this makes them phrases easier to remember.

The key to picking a good passphrase is to pick words that are both uncommon and easy to remember. Movie, TV, or quotes from popular culture or famous people are also not good to use as they can be easy for attackers to guess or brute force.

Examples of weak passphrases:

- "I have a dream"
- "nice jazz play here"
- "The cake is a lie"
- "I am Iron Man"

Examples of strong passphrases:

- "brothers question retained signs"
- "invoices fidelity races lifting"
- "Formerly lived in West Edmonton

Both passwords and passphrases can be secure, and if you are using a password manager, the security and usability differences between passwords and passphrases will not be significant. However, if you are setting a password that you must remember by heart, for usability reasons, we recommend using passphrases.

When you use passphrases, also keep the following in mind:

- Four words should be sufficient. Five words is better.
- Don't choose from the most common words, and don't choose quotes or sayings. The words should be as random as possible.
- Use a unique passphrase for every account you own. That way, if one passphrase is ever exposed, the other accounts remain secure.
- Keep in mind that spaces are valid characters.
- Use a mix of lower and upper cases, numbers, or special characters to replace some of the letters.

You should take a few minutes and complete the GoA Cyber Security eCourse on Secure Passwords by logging in [here](#) if you haven't already and also check out our Passwords [tip sheet](#).

Have more questions on passphrases? Drop your [Corporate Information Security Office](#) a line.

*Note: please do not use any of the sample passphrases provided!