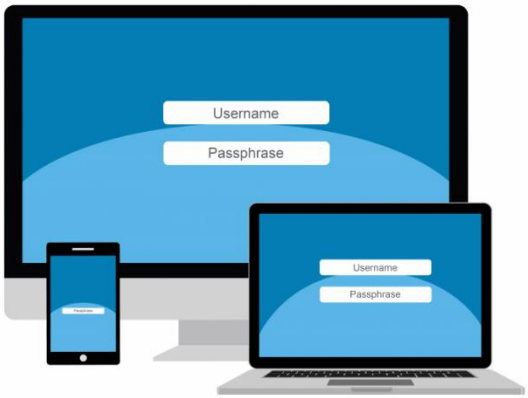
March 2018 Security Awareness
Using Passphrases Securely

Passphrases



Cyber attackers have developed sophisticated and effective methods to crack passwords using automated guessing techniques. That's why it is critical to use strong passwords. However, complex passwords can be hard to remember, confusing, and difficult to type.

Instead, we recommend using passphrases--a series of random words or a sentence. The more characters a passphrase has, the stronger it is. Passphrases are much easier to remember and type, but still hard for cyber attackers to hack.

Remember, your CWOPA password must be at least 12 characters long and contain at least three of the following types of characters: upper-case letters, lower-case letters, numbers and symbols.

Here are two examples:

Sentence or Phrase	Resulting Passphrase
I went on vacation to Jamaica in 2015 and the beach was beautiful.	iwovtji2015atbwb
My son was born at 1:23pm and weighed 8 pounds.	Mswba1:23pmaw8lb

While these passphrases are easy to remember and type, they are also strong because they use capital letters and symbols.

Using Passphrases Securely

Always be careful how you use passphrases. A passphrase is not helpful if it can be stolen or copied.

1. **Use a different passphrase for every account or device.** This way, if one of your accounts is hacked, the others are still safe. Considering using password manager program if you have a large number of passwords.

2. **Never share a passphrase or your strategy for creating them with anyone else, including coworkers or your supervisor.** If anyone else knows your passphrase, it is no longer secure. If you believe your passphrase may have been compromised or stolen, change it immediately. The only exception is if you want to share your key personal passphrases with a highly trusted family member in case of an emergency. In this case, it is a good idea to store passwords in a secure location and share that location with the family member.

3. **Do not use public computers to log in to your accounts.** Since anyone can use these computers, such as those at hotels or Internet cafes, they may be infected and capture all your keystrokes.

4. **Beware of websites that require you to answer personal questions.** These questions are used if you forget your passphrase and need to reset it. However, the answers can often be found on the Internet or social media. Use only information that is not publicly available or fictitious information that you can remember.

5. **Enable and utilize stronger authentication methods.** Many online accounts offer two-factor authentication, also known as two-step verification. This requires more than just your passphrase to log in, such as a passcode/PIN sent to your smartphone, and is much more secure than just a passphrase.

TIP: Make a passphrase even stronger by replacing letters with numbers or symbols. For example, replace the letter "A" with "@" or the letter "O" with the number zero. Additionally, always use the maximum number of characters allowed by a given website.

6. **Treat PINs as passwords.** Remember that a PIN, like the one on many mobile devices, is nothing more than a password. The longer a PIN, the more secure it is. Many mobile devices allow you to change your PIN number to an actual passphrase or use a biometric, such as your fingerprint.

7. **Close inactive accounts.** If you are no longer using an account, be sure to close, delete, or disable it.