Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Creating Strong Passphrases

DECEMBER 2020

Introduction

Multi-factor authentication (a combination of something that you know, something that you have or something that you are) is one of the most effective ways to protect against unauthorised access to valuable information and accounts. However, in cases where multi-factor authentication is not available, a strong passphrase can often be the only barrier between adversaries and your valuable information and accounts. Passphrases are most effective when they are long, complex, unpredictable and unique. By following this guidance, you can create stronger passphrases and avoid mistakes that adversaries exploit.

Passwords are passé - passphrases are longer and stronger

Passwords are passé. It's time to use passphrases instead. As we have increased our reliance on passwords, adversaries have developed increasingly sophisticated ways to crack them. In attempting to make passwords stronger, we have made them harder for humans to remember, and easier for machines to crack. Hence, the need for passphrases that are easy for humans to remember, and harder for machines to crack.

Principles for strong passphrases

Whenever you can, use a passphrase instead of a password. By following as many of these principles as you can, you will know you have created the most secure passphrase possible.

Create long passphrases

The longer your passphrase, the better. As adversaries can crack a short password with very little effort or time, you can increase the time and effort it takes by using a passphrase instead. Aim to make your passphrases at least 14 characters long, ideally as four or more random words whenever you can. For example, 'red house sky train', 'sleep free hard idea' or 'crystal onion clay pretzel'.

Create complex passphrases

Complexity is defined as using a combination of different character sets: capital letters, lowercase letters, numbers and special characters. Combining character sets can make a passphrase more difficult to guess and increases the time it takes to be cracked. For example, 'red House #sky train', 'Sleep free hard idea!' or 'crystal onion clay @Pretzel'.

Create unpredictable passphrases

The less predictable your passphrase, the better. A passphrase in the form of a lyric, quote or sentence, like 'I don't like pineapple on pizza.', uses spaces and punctuation, which adds complexity. However, a sentence could also be predictable, because the language you use will have grammar and punctuation rules to follow. In English sentences, for example, it is predictable to have spaces between words, a capital letter at the beginning and a single character of punctuation at the end, like a full stop. Sentences can also be predictable in the placement of nouns, adjectives, verbs and so on.

Using a random mix of unrelated words is far more unpredictable, and will produce a stronger passphrase. There are many ways to create a mix of random words. There are tools available on the internet that can help[1], or you could open to random pages in a dictionary or another book to select unrelated words.

Create unique passphrases

Use a unique passphrase for every valuable account. Reusing a passphrase makes each account that uses it more vulnerable. This is particularly important for valuable accounts like email, financial accounts and those that store banking details. Often email addresses are reused as usernames to log into multiple accounts, and the accounts are often used to store valuable personal information, making your email account a valuable resource. If adversaries have cracked your passphrase, they will attempt to use it for every account they find that is associated with you, and even change your passphrase so that you can't regain access to your accounts. Inconveniencing adversaries trying to steal from you is worth having unique passphrases for every valuable account.

One way that you can reduce the burden of having unique passphrases for every valuable account is to use modifiers for each one based on the service that it relates to. For example, 'crystal onion clay @Pretzel faceb00k' or '#insta crystal onion clay @Pretzel'.

Protect your passphrases

Secure your passphrases

Password managers (which can also be used to store passphrases as well) enable good cyber security habits. Having a unique passphrase for every valuable account may sound overwhelming; however, using a password manager to save your passphrases will free you of the burden of remembering which passphrase goes where.

A lot of web browsers provide an in-built password manager. You might have noticed the pop-up window asking to store your password when logging into accounts. Password managers are also sold separately, however, quality and security may vary.

When using a password manager:

- conduct research to ensure the password manager is from a reputable vendor
- conduct research to ensure the password manager is maintained by the vendor with regular security updates
- protect the password manager with its own strong and memorable passphrase.

You may choose to keep track of your passphrases in a notebook rather than a password manager. No matter how you keep track of your passphrases, ensure you have a secure storage method.

[1] https://www.eff.org/dice

Protect what protects you

Remember adversaries are opportunistic. Store and handle your passphrases carefully to avoid being compromised. Do not share your passphrases with anyone and be aware of your surroundings when using them in public. Use trusted Wi-Fi, trusted telecommunication networks or a Virtual Private Network (VPN) when accessing valuable accounts. Free public Wi-Fi, without the use of a VPN, can potentially expose your browsing activity. Log off and sign out of accounts when you finish using them.

Think critically when answering phone calls, messages and emails. Are the senders really who they say they are[2]? Be wary of requests for personal details, passphrases or financial details, particularly if the message sounds urgent. If you doubt the communicator's identity, delay immediate action. Re-establish communication later with the organisation using contact details you have found independently, using trusted sources.

If a passphrase has been compromised, change it immediately and never use it again. One way to check your credentials is by going to 'Have I Been Pwned'[3].

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.

[2] https://www.cyber.gov.au/acsc/view-all-content/publications/detecting-socially-engineered-messages
[3] https://haveibeenpwned.com/