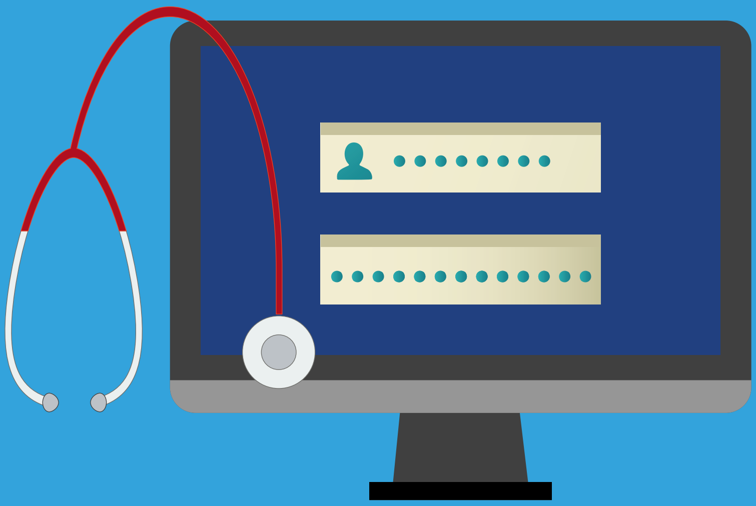
Australian Government
Australian Digital Health Agency

Supporting a positive security culture

PASSWORDS



Fact sheet

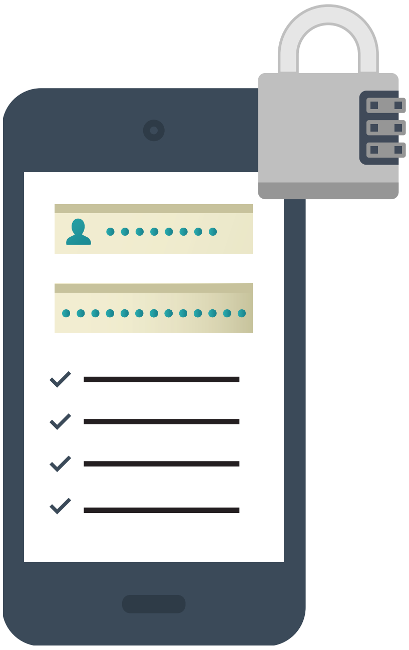
This document has been prepared to assist healthcare organisations to develop a positive security culture. It provides general guidance in relation to password management and is not intended to be comprehensive.

Your password – the key to your information

When accessing online services for work or personal activities, your password is the first line of defence for keeping your accounts secure.[1] Similar to a lock on the front door of your home, a password helps to prevent unauthorised access.

As passwords protect important information, it's essential to use a long, complex and unique password on each account. This prevents something known as the 'domino effect', where someone obtains or guesses the password for one account and they can then gain access to other accounts that use the same password.

A strong password is long (for example 14 characters or more) and includes a combination of upper and lower-case letters, numbers and special characters. It is important to make sure your passwords are hard for someone else to guess.



Passphrases

One way to set a strong password is to use a passphrase. A passphrase is a set of letters, numbers and symbols that is easy for you to remember, but difficult for a cyber criminal to crack.

Choose a passphrase that combines at least four words and is not related to you, your work or your immediate family. Once you have selected four or more words that you can remember, incorporate some numbers or symbols.

Tips for setting strong passwords or passphrases

Follow these tips to create a strong password or passphrase:

✓	consider creating a longer passphrase by combining at least four unrelated words	✗	don't include names of pets or immediate family members, or their dates of birth
✓	use a combination of characters that are easy for you to remember	✗	don't choose a password that is easy for others to guess
✓	use a separate password for each account and device	✗	never share your passwords
✓	enable multi-factor authentication if it is available – for example, use of a password plus a finger print scan or single use code	✗	avoid using repeated characters, numeric sequences (e.g. 1234), single dictionary words, and your address

How do cyber criminals crack passwords?

There are a number of approaches that cyber criminals use to ‘crack’ passwords. Some of the common attack methods include:[2]

- **Phishing and social engineering** – these are two ways of tricking unsuspecting users into divulging credentials or providing unauthorised access. Phishing relates to sending messages with malicious content, whereas social engineering describes live or in-person misrepresentations.
- **Brute force attack** – a trial and error method that involves trying all possible combinations of characters in sequence. Cyber criminals use high powered computers to test billions of passwords every second.
- **Dictionary attack** – a more sophisticated form of brute force attack in which common words are entered into password fields. Automated software is used to crack passwords that are based on dictionary words, slang terms, common misspellings, words spelled backward and well-known passwords, such as ‘password123’. A variation of this is known as ‘credential stuffing’ where leaked or stolen credentials are tried.

To reduce the likelihood of your password being cracked, it is important to ensure that you use a long, complex password that is hard for someone else to guess. Always use unique passwords for every account.

Password Managers

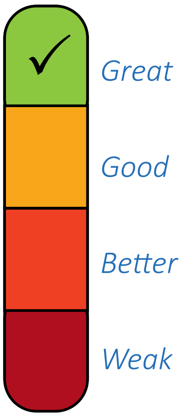
When you set strong and unique passwords on multiple accounts, it can be challenging to remember all of them. However, it is critical that passwords are *not* written down and left near your device, or stored in a ‘notes’ application on your device or online.

Instead, you may wish to consider using a password manager.[3] This is a software application that stores and manages your passwords in an encrypted database. It enables you to:

- generate random, complex, unique passwords using a password generator function
- store your passwords and protect them with encryption
- reduce the number of passwords you have to remember.

Password managers store your passwords in an encrypted database, which is protected with your ‘master password’. Therefore, it is essential that the master password you use to access the password manager is very strong.

There are risks involved with using a password manager and it is advisable to consider these risks when deciding whether to use a password manager, for example:



Master password strength indicator

- If someone guesses your master password, they will have access to all of your passwords – so make sure you use a very long, strong, unique passphrase that is easy for you to remember, but difficult for someone else to guess.
- If you forget your master password, there is no way to recover it, so you will lose access to all of your passwords.
- Password managers can be an attractive target for cyber criminals – if your password manager is compromised, all of your passwords will be compromised too. Choosing a

standalone password manager, rather than a cloud-based service can help to reduce the risk of a web-based attack.

In addition to choosing a strong master password, ensure your devices are also password protected, and turn on multi-factor authentication for your password manager and your devices, where available.

Multi-factor Authentication

A password helps to protect against unauthorised access, however if this password becomes known it no longer provides effective protection. Multi-factor Authentication (MFA), also known as Two Factor authentication (2FA), provides added protection.

With MFA, instead of just entering a username and password, you also need to provide another method of identification – known as another ‘factor’. This reduces the chance of a cyber criminal gaining unauthorised access if they have discovered your password.

The factors that may be used to confirm your identity include:

- Something you *know* – such as your username and passphrase
- Something you *have* – such as a code from a token, SMS, or mobile app
- Something you *are* – such as your fingerprint or a facial scan.

Using multiple secret pieces of information to identify yourself can protect against many types of password attacks.

Good password practices

In summary, below are five tips to remember when it comes to setting a good password:

1. Don’t share your passphrase with others as you could be held responsible for their actions, which could result in disclosure of sensitive information.
2. Always use a unique passphrase for each account to help prevent the ‘domino effect’. This is where all accounts using the same password are compromised, when the password is discovered.
3. Consider using a password manager if you have trouble remembering your passwords, but make sure you use a very strong master password to avoid compromise and risking the domino effect.
4. If you suspect someone knows your password, choose a new password immediately to reduce the likelihood of unauthorised access to information.
5. A strong password is long, for example 14 characters or more, and includes a combination of upper and lower-case letters, numbers and special characters.

Further information

To find out more about how you can protect information that you access online, visit the Agency's Cyber security page.

You can also choose to receive free updates about the latest information security risks by registering at the Australian Cyber Security Centre and Scamwatch.

Visit the Australian Digital Health Agency's website for additional guides and information on information security at https://www.digitalhealth.gov.au/healthcare-providers/cyber-security.

References

1 Australian Cyber Security Centre, Get smarter with passwords. Available from: https://www.cyber.gov.au/acsc/view-all-content/news/get-smarter-passwords

2 ITPro, The top 12 password-cracking techniques used by hackers. Available from: https://www.itpro.co.uk/security/34616/the-top-password-cracking-techniques-used-by-hackers

3 CERTNZ, Keep your data safe with a password manager. Available from: https://www.cert.govt.nz/individuals/guides/keep-your-data-safe-with-a-password-manager/

4 Australian Cyber Security Centre, Multi-factor authentication. Available from: https://www.cyber.gov.au/mfa

Publication date: September 2021

Contact for enquiries

Telephone: 1300 901 001 or **email:** help@digitalhealth.gov.au

Disclaimer
The Australian Digital Health Agency ("the Agency") makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control
This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

Acknowledgements

Council of Australian Governments
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Australian Government

Australian Digital Health Agency

digitalhealth.gov.au