ARE YOUR DEVICES SECURE?

Best practices for password security

2 OR MORE

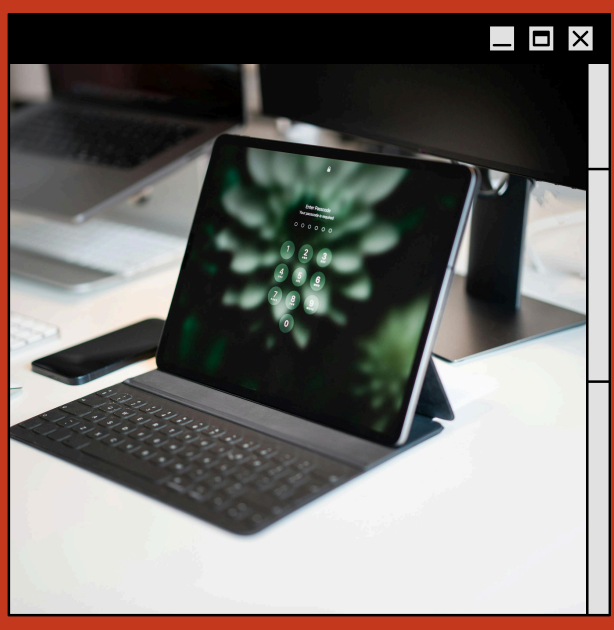
Implement multi-factor (MFA) authentication where possible (e.g., a password, an authentication app, and/or your fingerprint)

AT LEAST 14

Use complex passphrases that are unique to each account and contain at least 4 unrelated words or 14+ characters

DON'T RECYCLE

Don't reuse passwords or passphrases that you've previously used



BE CAUTIOUS

Use a VPN when connecting to public Wi-Fi and don't share your passwords with anyone

USE A VAULT

Generate and store complex passphrases using a reputable password manager

PROTECT THE VAULT

Use your strongest passphrase to secure access to your password manager

References

Australian Cyber Security Centre (ACSC

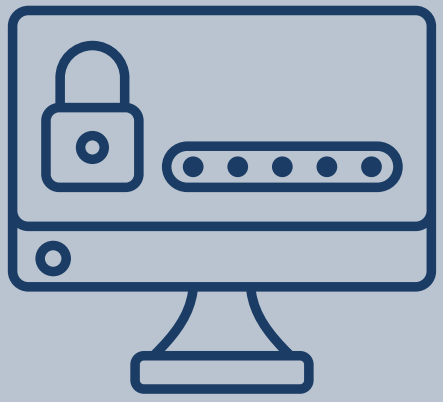
Created by Ariel Bethea

SECURING ACCOUNTS AND DEVICES

Top Tips for Password Security

ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Enable MFA where possible, which uses something you know (e.g., a password), something you have (e.g. an authentication app) and/or something you are (e.g. your fingerprint)

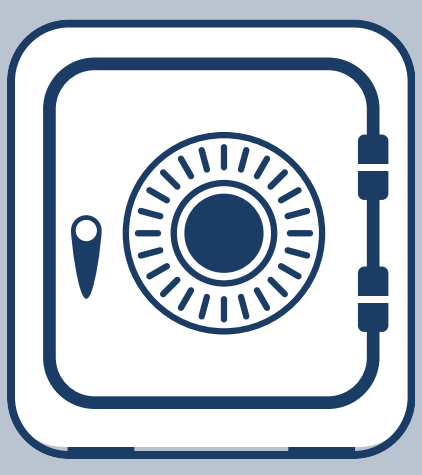


USE STRONG PASSPHRASES

Use complex passphrases that are unique to each account and contain at least 4 unrelated words or a minimum of 14 characters

EXERCISE CAUTION

- Use a VPN when connecting to public Wi-Fi networks
- Log out of devices when stepping away and don't share your passwords with anyone



SELECT A PASSWORD MANAGER

Generate and store complex passphrases using a reputable password manager and ensure your strongest passphrase is reserved for accessing the password manager. Avoid the "Remember Me?" feature when using a public or shared computer.

REFERENCES

AUSTRALIAN CYBER SECURITY CENTRE (ACSC)

Read more at https://www.cyber.gov.au

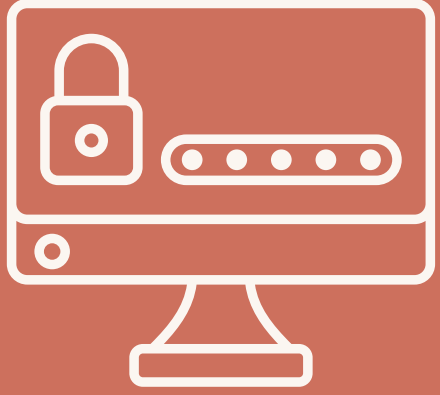
Created by Ariel Bethea

SECURING ACCOUNTS AND DEVICES

Top Tips for Password Security

ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Enable MFA where possible, which uses something you know (e.g., a password), something you have (e.g. an authentication app) and/or something you are (e.g. your fingerprint)

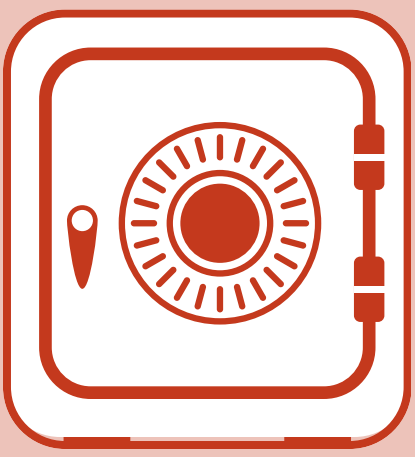


USE STRONG PASSPHRASES

Use complex passphrases that are unique to each account and contain at least 4 unrelated words or a minimum of 14 characters

EXERCISE CAUTION

- Use a VPN when connecting to public Wi-Fi networks
- Log out of devices when stepping away and don't share your passwords with anyone



SELECT A PASSWORD MANAGER

Generate and store complex passphrases using a reputable password manager and ensure your strongest passphrase is reserved for accessing the password manager. Avoid the "Remember Me?" feature when using a public or shared computer.

REFERENCES

AUSTRALIAN CYBER SECURITY CENTRE (ACSC)

Read more at https://www.cyber.gov.au

Created by Ariel Bethea