



Australian Government



உடனே செயல்படுங்கள்.  
பாதுகாப்பாக இருங்கள்.

# இணையத்தில் நீங்கள் எவ்வாறு பாதுகாப்பாக இருக்கலாம்

“எளிய வாசிப்பு” பதிப்பு



# இக்கையேட்டை எவ்வாறு பயன்படுத்துவது



நாங்கள் ஆஸ்திரேலிய அரசாங்கத்தைச் சேர்ந்தவர்கள்.

நாங்கள்தான் இக்கையேட்டை எழுதினோம்.



நாங்கள் சில வார்த்தைகளைத் **தடித்த** எழுத்துக்களில் எழுதியுள்ளோம்.

இந்த வார்த்தைகளின் அர்த்தம் என்ன என்பதை நாங்கள் விளக்குகிறோம்.

பக்கம் 32-ல் இந்த வார்த்தைகளின் பட்டியல் ஒன்றும் உள்ளது.



உங்களுக்கு நம்பிக்கை உள்ள ஒருவரிடம் பின்வருவனவற்றிற்கான ஆதரவுதவி கேட்கலாம்:

- இக்கையேட்டை வாசிக்க
- மேலும் தகவல்களைக் கண்டறிய.



இது மற்றொரு வழிகாட்டிக் கையேட்டின் 'எளிய வாசிப்பு' சுருக்கம்.

இது மிக முக்கியமான கருத்துக்களை மட்டுமே உள்ளடக்கியுள்ளது.



மற்றைய வழிகாட்டிக் கையேட்டை நீங்கள்  
எமது வலைத்தளத்தில் காணலாம்.

[www.actnowstaysecure.gov.au](http://www.actnowstaysecure.gov.au)

# இக்கையேட்டில் இருப்பது என்ன?

|                                                                     |    |
|---------------------------------------------------------------------|----|
| இக்கையேட்டைப் பற்றி                                                 | 5  |
| உங்கள் கணக்குகளைப் பாதுகாப்பாக வைத்திருங்கள்                        | 8  |
| உங்கள் தகவல்களைப் பாதுகாக்க உங்கள்<br>அமைப்புமுறைகளைச் சரிபாருங்கள் | 12 |
| உங்கள் சாதனங்களைப் பாதுகாத்துக் கொள்ளுங்கள்                         | 18 |
| மோசடிகள்                                                            | 23 |
| குரல் கொடுங்கள்                                                     | 29 |
| சொற்பட்டியல்                                                        | 32 |
| எங்களுடன் தொடர்பு கொள்ளுங்கள்                                       | 34 |

# இக்கையேட்டைப் பற்றி



இணையத்தில் நாம் எவ்வாறு பாதுகாப்பாக இருப்பது என்பது பற்றி நாம் அனைவரும் சிந்திக்க வேண்டும்.

இதனை நாம் **இணைய (சைபர்)** பாதுகாப்பு என்கிறோம்.



'சைபர்' என்பது இணையம் சம்பந்தப்பட்ட விடயம் ஒன்றைக் குறிக்கிறது.



இணையத்தில் உங்களைப் பாதுகாத்துக் கொள்ள உங்களால் செய்ய முடியுமான சில விடயங்களை இக்கையேடு விளக்குகிறது.

உதாரணமாக, '**சைபர்**' குற்றங்களிலிருந்து உங்களை எப்படிப் பாதுகாத்துக்கொள்வது.

குற்றவாளிகள் குற்றச் செயல்களுக்காக இணையத்தைப் பயன்படுத்துவது இணைய 'சைபர்' குற்றம் எனப்படுகிறது.



உதாரணமாக, அவர்கள் இணையத்தை பின்வருவனவற்றிற்காகப் பயன்படுத்தக்கூடும்:

- உங்கள் தனிப்பட்ட தகவல்களைத் திருடுவதற்காக
- உங்கள் இணையக் கணக்குகள் அல்லது சுயவிவரங்களைக் கையகப்படுத்துவதற்காக.

சைபர் குற்றம் எந்தவொரு சாதனம் மூலமாகவும் நடக்கலாம்.



இதில் அடங்குபவை, உங்களுடைய:

- கணினி
- 'ஸ்மார்ட்' கைபேசி
- 'ஸ்மார்ட் வாட்ச்'



'சைபர்' குற்றங்களிலிருந்து பாதுகாப்பாக இருக்க நீங்கள் செய்யக்கூடிய சில விடயங்கள் உள்ளன.



நீங்கள் என்ன செய்யலாம் என்பதை அடுத்து  
வரும் பக்கங்களில் விளக்குகிறோம்.

## உங்கள் கணக்குகளைப் பாதுகாப்பாக வைத்திருங்கள்



உங்கள் இணையக் கணக்குகளை எவ்வாறு  
பாதுகாப்பாக வைத்திருக்கலாம் என்பது பற்றி  
நீங்கள் சிந்திக்க வேண்டும்.

## வலுவான மற்றும் வெவ்வேறான கடவுச் சொற்றொடர்களைப் பயன்படுத்துங்கள்



கடவுச்சொற்றொடர் என்பது வலுவான  
ஒருவகை கடவுச்சொல் ஆகும்.

மற்றவர்களால் அதை யூகிப்பது மிகவும்  
கடினமானது.



வலுவான மற்றும் வெவ்வேறான  
கடவுச்சொற்றொடர்களைப் பயன்படுத்துவது,  
உங்கள் கணக்குகளைப் பாதுகாப்பதற்கான  
சிறந்த வழிகளில் ஒன்றாகும்.



உங்கள் ஒவ்வொரு இணைய கணக்கிற்கும்  
வெவ்வேறான கடவுச்சொற்றொடரைப்  
பயன்படுத்த வேண்டும்.



வலுவான கடவுச்சொற்றொடர்களில்  
அடங்குபவை:

- 4 அல்லது அதற்கு மேற்பட்ட தொடர்பற்ற  
சொற்கள்
- 15 அல்லது அதற்கு மேற்பட்ட  
எழுத்துக்கள் மற்றும் இலக்கங்கள்.



நீங்கள் சில பேரெழுத்துக்களைச் சேர்க்கலாம்.



நீங்கள் பின்வரும் குறியீடுகளையும்  
பயன்படுத்தலாம்:

- ஒரு இடைக்கோடு
- 'டொலர்' குறியீடு
- ஒரு மின்னஞ்சல் @ குறியீடு.



உங்கள் கடவுச்சொற்றொடர்களில் உங்களைப் பற்றிய எந்தவொரு தகவலையும் பயன்படுத்தக் கூடாது.



உதாரணமாக:

- உங்கள் பிறந்தநாள்
- உங்கள் குடும்ப உறுப்பினர்கள் அல்லது செல்லப்பிராணிகளின் பெயர்கள்.

## உங்கள் கணக்குகளில் உள்நுழைய கூடுதல் படிநிலைகளைச் சேருங்கள்



**‘பல படிநிலை உறுதிப்பாட்டு முறைமை’ (MFA)** மூலம் உங்கள் இணையக் கணக்குகளை நீங்கள் பாதுகாத்துக்கொள்ளலாம்.

MFA என்பது, நீங்கள் ஒவ்வொரு முறையும் உங்கள் கணக்கில் உள்நுழைய இரண்டு அல்லது அதற்கு மேற்பட்ட வெவ்வேறு வழிகளைப் பயன்படுத்துவதாகும்.



உதாரணமாக, நீங்கள் முதலில் உங்கள்  
கடவுச்சொற்றொடரை உள்ளிட  
வேண்டியிருக்கலாம்.

பிறகு உங்கள் தொலைபேசிக்கு வரும்  
குறியீட்டை உள்ளிடுங்கள்.

உங்களுக்கு பின்வரும் தெரிவுகள்  
இருக்கலாம்:



- குறியீட்டை உங்களுக்குக் கொடுக்கும்  
ஒரு செயலியை உங்கள் கைப்பேசியில்  
பெறும் தெரிவு



- குறியீட்டை மின்னஞ்சலில் பெறும்  
தெரிவு



- குறியீட்டை ஒரு குறுஞ்செய்தியில்  
பெறும் தெரிவு.



மற்றவர்கள் உங்களுடைய கணக்கிற்குள்  
நுழைவதை MFA கடினமாக்குகிறது.

அவர்கள் உங்களுடைய கடவுச்சொற்றொடரை  
கண்டுபிடித்தபோதிலும் கூட.

## உங்கள் தகவல்களைப் பாதுகாக்க உங்கள் அமைப்புமுறைகளைச் சரிபாருங்கள்



உங்கள் அமைப்புமுறைகள் இணையத்தில்  
உங்கள் தகவல்களைப் பாதுகாக்கின்றனவா  
என்பதை நீங்கள் சரிபார்க்கலாம்.



இதில், உங்கள் பின்வரும் அமைப்புமுறைகள்  
அடங்கும்:

- இணையக் கணக்குகள்
- சாதனங்கள்
- செயலிகள்.

நீங்கள்:



- உங்கள் அமைப்புமுறைகளை மாற்றலாம்
- உங்கள் தகவலை எந்த செயலிகள் பயன்படுத்த முடியும் என்பதைத் தெரிவு செய்யலாம்.

உங்கள் சாதனத்தில் உள்ள அமைப்புமுறைகளை பின்வரும் வழிகளில் கண்டறியலாம்:



- 'பல்-சக்கர' 'ஐகான்'-ஐத் தேடுவதன் மூலம் அல்லது
- உங்கள் சாதனத்தின் தேடல் பட்டியலில் 'settings' எனத் தட்டச்சு செய்தல் மூலம்.



'மெனு'வைத் திறப்பதன் மூலம் ஒரு செயலியில் அல்லது இணையக் கணக்கில் உள்ள அமைப்புமுறைகளை நீங்கள் கண்டறியலாம்.

'மெனு' பெரும்பாலும் மூன்று நேர்கோடுகள் போலத் தோற்றமளிக்கும்.

இந்த அமைப்புமுறைகளில் சிலவற்றினால் பின்வருவன பற்றிய தகவல்களைப் பகிர முடியும்:



- நீங்கள் யார்
- நீங்கள் எங்கே இருக்கிறீர்கள்
- நீங்கள் வசிக்கும் இடம்.



இந்தத் தகவலை இணையத்தில் பகிர்வது, சைபர் குற்றங்களுக்கு உங்களை ஆளாக்கக்கூடும்.



உங்கள் தகவல்களைப் பயன்படுத்தி, சைபர் குற்றவாளிகளால் உங்களைப் போல் நடிக்க முடியும்.

உதாரணமாக, அவர்கள் பின்வரும்  
தகவல்களைப் பயன்படுத்தலாம்:



- நீங்கள் வசிக்கும் இடம்



- உங்கள் குடும்ப உறுப்பினர்களின் பெயர்கள்



- உங்கள் செல்லப்பிராணிகளின் பெயர்கள்.



உங்களுக்குத் தெரிந்தவர்கள் மட்டுமே  
உங்கள் சமூக ஊடக சுயவிவரங்களைப்  
பார்க்க இயலுமாகும் விதத்தில் உங்கள்  
கணக்குகளை நீங்கள்  
அமைத்துக்கொள்ளலாம்.

உதாரணமாக, உங்கள் முகநூல் சுயவிவரம்.



இந்த அமைப்புமுறைகள் பொதுவாக  
அந்தரங்கப் பாதுகாப்பு அமைப்புமுறைகள்  
என்று சொல்லப்படுகின்றன.



உங்கள் **இருப்பிட அமைப்புமுறைகளையும்**  
நீங்கள் கட்டுப்படுத்தலாம்.

இருப்பிட அமைப்புமுறைகள் உங்கள் சாதனம்  
எங்குள்ளது என்பதைக் காட்டுகின்றன.



நீங்கள் இருப்பிட அமைப்புமுறைகளை 'ஆன்'  
அல்லது 'ஆஃப்' செய்யலாம்.

உங்கள் இருப்பிட அமைப்புமுறைகளை  
எந்தெந்த செயலிகள் பயன்படுத்தலாம்  
என்பதையும் நீங்கள் தேர்வு செய்யலாம்.



இதனை நீங்கள் உங்களது பின்வருவனவற்றில்  
செய்யலாம்:

- இணையக் கணக்குகள்
- சாதனங்கள்
- செயலிகள்.

சில செயலிகள், தாமாகவே  
பின்வருவனவற்றை செய்ய உங்களிடம்  
அனுமதி கேட்கக்கூடும்:



- உங்கள் 'கேமரா'வைப்  
பயன்படுத்தலாமா என்று



- உங்கள் புகைப்படங்களைப்  
பார்க்கலாமா என்று.



உங்களுக்குப் பரிச்சயமான செயலிகளை  
மட்டுமே உங்கள் 'கேமரா'வையும்  
புகைப்படங்களையும் பயன்படுத்த  
அனுமதிக்க வேண்டும்.

## உங்கள் சாதனங்களைப் பாதுகாத்துக் கொள்ளுங்கள்



இணையத்தில் உங்களைப் பாதுகாப்பாக  
வைத்திருக்க, உங்கள் சாதனங்களை  
எவ்வாறு பாதுகாக்கலாம் என்பதைப் பற்றி  
நீங்கள் சிந்திக்க வேண்டும்.

உதாரணமாக, உங்கள் கைபேசி அல்லது  
'ஸ்மார்ட் வாட்ச்'.



இணையத்துடன் இணைக்கும்  
சாதனங்களுக்கு இது முக்கியமானது.

## உங்கள் சாதனங்களை நடப்பு நாள் வரைக்குமானதாகப் புதுப்பியுங்கள்



உங்கள் சாதனங்களை இணையத்தில்  
பாதுகாப்பாக வைத்திருக்க, அவற்றை நீங்கள்  
புதுப்பிக்கலாம்.

உதாரணமாக, உங்கள் கைபேசி மற்றும்  
மடிக்கணினி.



உங்கள் சாதனம் இதனை ஒரு 'மென்பொருள்  
புதுப்பிப்பு' என்று அழைக்கக்கூடும்.



புதுப்பிப்புகள், 'சைபர்' குற்றங்களிலிருந்து  
ஒரு சாதனம் தன்னைத்தானே பாதுகாத்துக்  
கொள்ள உதவுகின்றன.



ஒரு சாதனத்தைத் தானாகவே புதுப்பிக்கும்  
வகையில் அதை அமைக்கலாம்.



உங்கள் சாதனங்களை எவ்வாறு புதுப்பிப்பது  
என்பது பற்றி எங்கள் வலைத்தளத்தில்  
மேலும் அறிந்துகொள்ளலாம்.

[www.actnowstaysecure.gov.au/  
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

## பொது 'வைஃபை' (Wi-Fi) நெட்வொர்க்குகள்



பொது 'வைஃபை' (Wi-Fi) யைப் பயன்படுத்தும்  
போது நீங்கள் கவனமாக இருக்க வேண்டும்.



பொது 'வைஃபை' (Wi-Fi) என்பது பொது  
இடங்களில் நீங்கள் பயன்படுத்தக்கூடிய  
இலவச கம்பியில்லா இணையமாகும்.

உதாரணமாக, ஒரு:



- சிற்றுண்டியகத்தில்
- விமான நிலையத்தில்
- உணவகத்தில்.



பொது 'வைஃபை' (Wi-Fi) யைப் பயன்படுத்தி ஒரு வலைத்தளத்தில் உள்ளிடும் தகவல்கள் குறித்து நீங்கள் கவனமாக இருக்க வேண்டும்.



உதாரணமாக, உங்களுடைய:

- வங்கி விபரங்கள்
- மின்னஞ்சல் கணக்குகள்
- சமூக ஊடக சுயவிவரங்கள்.



சில 'சைபர்' குற்றவாளிகள் பொது 'வைஃபை' (Wi-Fi) யை பின்வருவனவற்றிற்காகப் பயன்படுத்தலாம்:

- நீங்கள் இணையத்தில் என்ன செய்கிறீர்கள் என்பதைப் பார்ப்பதற்கு
- உங்கள் தகவல்களைத் திருடுவதற்கு.

இது ஏனெனில்:



- யார் வேண்டுமானாலும் இதைப் பயன்படுத்தலாம்



- உங்கள் சாதனங்களைப் பாதுகாப்பது அதிகடினமாகிவிடுகிறது.



பொது 'வைஃபை' (Wi-Fi) யைப் பாதுகாப்பாகப் பயன்படுத்துவது எப்படி என்பதை எங்கள் வலைத்தளத்தில் நீங்கள் அறிந்துகொள்ளலாம்.

[www.actnowstaysecure.gov.au/  
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

# மோசடிகள்



எவரேனும் ஒருவர் உங்களுக்கு பின்வரும் ஒன்றைச் செய்ய முயன்றால் அதை நாம் **மோசடி (scam)** என்போம்:

- உங்களைத் தந்திரமாக ஏமாற்றுதல்
- உங்கள் பணத்தை கையகப்படுத்துதல்.



மோசடிகள் செய்யும் நபர் ஒருவர் **மோசடியாளர் (scammer)** எனப்படுவார்.

'மோசடியாளர்கள்' பின்வரும் வழிகளில் உங்களை ஏமாற்ற முயற்சிக்கலாம்:



- ஒரு குறுஞ்செய்தி அல்லது தொலைபேசி அழைப்பு
- ஒரு மின்னஞ்சல்
- சமூக ஊடகங்கள்
- ஒரு வலைத்தளம்.



அவர்கள் நட்பாய்ப் பழகுவர்களாகத்  
தோன்றலாம்.

ஆனால், அவர்கள் உங்களை ஏமாற்றி உங்கள்  
தகவல்களைப் பெற்றுவிடக்கூடும்.

அவர்கள் இதனைப் பயன்படுத்தி:



- உங்கள் இணையக் கணக்குகளுக்குள்  
நுழையலாம்



- உங்களை போலவே நடிக்கலாம்



- உங்கள் பணத்தைத் திருடலாம்.

மோசடியாளர்கள் பின்வருவனவற்றையும்  
செய்யலாம்:



- உங்களை ஏமாற்றுவதற்காக போலிக் கணக்குகளை உருவாக்கலாம்



- நீங்கள் 'கிளிக்' செய்வதற்காக இணைப்புகளையும் விளம்பரங்களையும் பகிரலாம்.

## மோசடி(scam)-யை எவ்வாறு கண்டறிவது

ஒரு விடயம் பின்வரும் தன்மைகளைக் கொண்டிருந்தால், அது ஒரு மோசடி (scam) - யாக இருக்கலாம்:



- ஏதேனும் ஒன்றை விரைவாகச் செய்யும்படி உங்களை வேண்டினால்



- உங்களுக்கு நிறையப் பணம் கொடுக்க முன்வந்தால்



- உங்களிடம் பணம் கேட்டால்



- ஒரு இணைப்பைச் சொடுக்குமாறு உங்களிடம் கேட்டால்.



மோசடியாளர்கள், உங்களுக்குத் தெரிந்த மற்றும் உங்களது நம்பிக்கைக்குரிய ஒரு நிறுவனம் போலவும் நடிக்கக்கூடும்.

உதாரணமாக, உங்கள் வங்கி.



நீங்கள் உங்கள் தனிப்பட்ட தகவல்களை  
அவர்களுடன் பகிர்ந்துகொள்வதற்காகவே  
மோசடிக்காரர்கள் இதைச் செய்கிறார்கள்.



அந்த நபர் ஒரு மோசடியாளர் என்று நீங்கள்  
நினைத்தால், அவரிடம் பேசுவதை  
நிறுத்திவிட வேண்டும்.



அந்த நபர், தன்னை யார் என்று  
சொல்லிக்கொள்கிறாரோ அவர்தானா என்பதை  
நீங்கள் சரிபார்க்க வேண்டும்.

நீங்கள் நம்பும் மற்றும் நீங்களே கண்டறிந்த  
விவரங்களைப் பயன்படுத்தி அந்த நபருடனோ,  
அமைப்புடனோ தொடர்பு கொள்ளலாம்.



ஏதேனும் சரியில்லாதது போல் தோன்றினால்,  
உங்களைப் பாதுகாத்துக் கொள்ள  
உடனடியாகச் செயல்படுங்கள்.

## மோசடி (scam) பற்றிப் புகாரளித்தல்



'ஸ்கேம்வாட்ச்' (மோசடிக் கண்காணிப்பு) எனும் சேவை ஆஸ்திரேலியர்களுக்கு பின்வரும் வழிகளில் உதவுகிறது:

- மோசடிகளைப் (scams) புரிந்துகொள்ள
- மோசடிகள் (scams) பற்றி புகாரளிக்க.



மோசடி (scams) களுக்கு ஆளான ஆஸ்திரேலியர்களுக்கும் 'ஸ்கேம்வாட்ச்' உதவுகிறது.



'ஸ்கேம்வாட்ச்' வலைத்தளத்தில் நீங்கள் ஒரு மோசடி பற்றிப் புகாரளிக்கலாம்.

[www.scamwatch.gov.au/report-a-scam](http://www.scamwatch.gov.au/report-a-scam)

# குரல் கொடுங்கள்



இணையத்தில் மற்றவர்கள் தங்களை எவ்வாறு பாதுகாத்துக் கொள்ளலாம் என்பது குறித்து நீங்கள் குரல் கொடுக்க வேண்டும்.

இதில் அடங்குபவை:



- 'சைபர்' குற்றங்களைப் புகாரளித்தல்



- உங்களுக்குத் தெரிந்ததை குடும்பத்தினருடனும் நண்பர்களுடனும் பகிர்ந்துகொள்ளல்.



நீங்கள் எவ்வாறு குரல் கொடுக்கலாம் என்பதை பின்வரும் பக்கங்களில் விளக்குகிறோம்.

## 'சைபர்' குற்றத்தைப் புகாரளித்தல்

சைபர் குற்றங்களைப் புகாரளிப்பது பின்வரும் வழிகளில் அரசாங்கத்திற்கு உதவுகிறது:



- 'சைபர்' குற்றவாளிகள் சனங்களை எவ்வாறு தாக்க முயற்சிக்கிறார்கள் என்பதைத் தெரிந்துகொள்ளுதல்.



- இன்னும் அதிகமான சனங்களைப் பாதுகாத்தல்.



ReportCyber வலைத்தளத்தில் 'சைபர்' குற்றங்களைப் புகாரளிக்கலாம்.

[www.cyber.gov.au/report](http://www.cyber.gov.au/report)

## இணையத்தில் பாதுகாப்பாக இருப்பது பற்றி குடும்பத்தினரிடமும் நண்பர்களிடமும் கதைக்கவும்



இணையத்தில் பாதுகாப்பாக இருப்பது குறித்த உங்கள் ஆலோசனைகளை உங்கள் குடும்பத்தினருடனும் நண்பர்களுடனும் பகிர்ந்துகொள்ள வேண்டும்.

நீங்கள் அவர்களிடமிருந்தும் கற்றுக்கொள்ளலாம்.



இணையத்தில் பாதுகாப்பாக இருப்பது பற்றி உங்களுக்குத் தெரிந்தவற்றைப் பகிர்வதன் மூலம், உங்களையும் உங்களைச் சுற்றியுள்ளவர்களையும் நீங்கள் பாதுகாத்துக் கொள்ளலாம்.



நீங்கள் மற்றவர்களுடன் சாதனங்களைப் பகிர்ந்துகொள்பவர் என்றால், இதுவும் முக்கியமானது.

# சொற்பட்டியல்

இக்கையேட்டில் உள்ள **தடித்த** எழுத்துகளில் குறிப்பிடப்பட்டுள்ள சொற்களின் அர்த்தத்தை இந்தப் பட்டியல் விளக்குகிறது.



## 'சைபர்'

'சைபர்' என்பது இணையம் சம்பந்தப்பட்ட விடயம் ஒன்றைக் குறிக்கிறது.

## 'சைபர்' (இணைய) குற்றம்



குற்றவாளிகள் குற்றச் செயல்களுக்காக இணையத்தைப் பயன்படுத்துவதே 'சைபர்' குற்றம் ஆகும்.

உதாரணமாக, அவர்கள் இணையத்தை பின்வருவனவற்றிற்காகப் பயன்படுத்தலாம்:

- உங்கள் தனிப்பட்ட தகவல்களைத் திருட
- உங்கள் இணைய கணக்குகளைப் கைப்பற்ற.



### இருப்பிட அமைப்புமுறைகள்

இருப்பிட அமைப்புமுறைகள் உங்கள் சாதனம் எங்குள்ளது என்பதைக் காட்டுகின்றன.



### 'பல படிநிலை உறுதிப்பாட்டு முறைமை' (MFA)

MFA என்பது, நீங்கள் ஒவ்வொரு முறையும் உங்கள் கணக்கில் உள்நுழைய இரண்டு அல்லது அதற்கு மேற்பட்ட வெவ்வேறு வழிகளைப் பயன்படுத்துவதாகும்.



### கடவுச்சொற்றொடர்

கடவுச்சொற்றொடர் என்பது கடவுச்சொல்லின் ஒரு வலுவான வகையாகும்.

அதை மற்றவர்கள் யூகிப்பது மிகவும் கடினம்.



### பொது 'வைஃபை' (Wi-Fi)

பொது 'வைஃபை' (Wi-Fi) என்பது பொது இடங்களில் பயன்படுத்தக்கூடிய இலவச கம்பியில்லா இணையம் ஆகும்.

## மோசடிகள்



ஒருவர் பின்வருவனவற்றைச் செய்ய முயற்சிக்கும்போது அதை நாம் ஏமாற்று மோசடி (scam) என்று அழைக்கிறோம்:

- உங்களை ஏமாற்ற
- உங்கள் பணத்தை எடுத்துக்கொள்ள.



## மோசடியாளர்கள்

மோசடிகள் செய்யும் ஒரு நபர் 'ஸ்கேமர்' எனப்படுவார்.

## எங்களுடன் தொடர்பு கொள்ளுங்கள்



நீங்கள் 'ஆஸ்திரேலிய 'சைபர்' பாதுகாப்பு உதவி இலக்கத்தை' அழைக்கலாம்.

1300 292 371



நீங்கள் எங்கள் வலைத்தளத்தைப் பார்வையிடலாம்.

[www.actnowstaysecure.gov.au](http://www.actnowstaysecure.gov.au)



நீங்கள் ReportCyber வலைத்தளத்தில் சைபர் குற்றங்களைப் பற்றிப் புகாரளிக்கலாம்.

[www.cyber.gov.au/report](http://www.cyber.gov.au/report)



‘தகவல் அணுகல் குழு’ (Information Access Group), வணிக பயன்பாட்டு புகைப்படங்கள் மற்றும் வடிவமைக்கப்பட்ட படங்களைப் பயன்படுத்தி இந்த ‘எளிய வாசிப்பு’ பதிவேட்டை உருவாக்கியுள்ளது. அனுமதியின்றி இந்தப் படங்களை மீண்டும் பயன்படுத்தக் கூடாது. படங்கள் தொடர்பான ஏதேனும் விசாரணைகளுக்கு, [www.informationaccessgroup.com](http://www.informationaccessgroup.com) என்ற இணையதளத்தைப் பார்வையிடவும். ஜொப் இலக்கம் 6342 என்று எடுத்துரைக்கவும்.