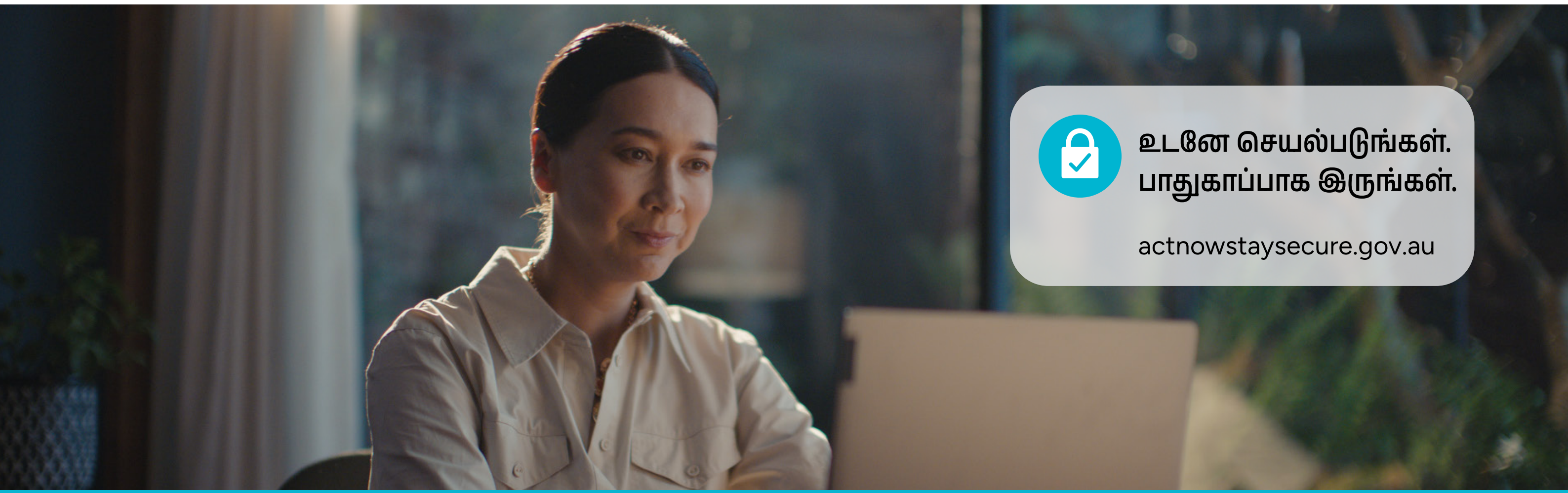
Australian Government

actnowstaysecure.gov.au



இணையத்தில் நீங்கள் எதிர்நோக்கும் ஆபத்துகள் என்ன?

தொழில்நுட்பம் வேகமாக முன்னேறி வருவதாலும், நாம் இணையத்தில் அதிக நேரம் செலவிடுவதாலும், ஆஸ்திரேலியர்கள் 'சைபர்' தாக்குதல்களுக்கு ஆளாகும் ஆபத்தில் உள்ளனர்.

'உடனே செயல்படுங்கள். பாதுகாப்பாக இருங்கள்' என்ற பிரச்சாரம், இணையத்தில் தங்களைப் பாதுகாத்துக் கொள்ள அனைவரும் எடுக்க முடியுமான எளிய இணையப் பாதுகாப்பு நடவடிக்கைகள் குறித்து ஆஸ்திரேலியர்களுக்கு அறிவுறுத்துகின்றது.

'உடனே செயல்படுங்கள். பாதுகாப்பாக இருங்கள்.'

இணையத்தில் பாதுகாப்பாக இருப்பது எப்படி

ஒவ்வொரு கணக்கிலும் தனித்துவமான மற்றும் வலுவான ஒரு கடவுச்சொற்றொடரைப் பயன்படுத்தவும்

உங்கள் ஒவ்வொரு இணையக் கணக்கிற்கும் தனித்துவமான மற்றும் வலுவான கடவுச்சொற்றொடரைப் பயன்படுத்துவது இணையத்தில் பாதுகாப்பாக இருக்க நீங்கள் எடுக்கக்கூடிய மிகவும் பயனுள்ள செயல்களில் ஒன்றாகும்.

கடவுச்சொற்றொடர் (passphrase) என்பது மிகவும் பாதுகாப்பான கடவுச்சொல் ஆகும். இது தொடர்பற்றதாக உருவாக்கப்பட்ட ஒரு சொற்றொடரைக் கொண்டிருக்கும். அதை நீங்கள் நினைவில் கொள்வது இலகுவாயிருக்கும், ஆனால் 'சைபர்' குற்றவாளிகளுக்கு யூகிக்கக் கடினமானதாக இருக்கும்.

உங்கள் கடவுச்சொற்றொடர்கள் வலுவாகவும் தனித்துவமாகவும் இருக்க, பின்வருவனவற்றை உறுதிப்படுத்திக் கொள்ளுங்கள்:

- ✓ நான்கு அல்லது அதற்கு மேற்பட்ட தொடர்பற்ற சொற்களைக் கொண்டிருத்தல்
- ✓ 15 அல்லது அதற்கு மேற்பட்ட எழுத்துக்களைக் கொண்டிருத்தல்
- ✓ ஒவ்வொரு கணக்கிற்கும் வெவ்வேறானதாக அவை இருத்தல்
- ✓ குடும்பப் பெயர்கள், பிறந்த திகதிகள் அல்லது முகவரிகள் போன்ற அடையாளம் காண முடியுமான தகவல்களைச் சேர்க்க வேண்டாம்.
- ✓ வலைத்தளத்தினால் அல்லது சேவையினால் கோரப்பட்டால், குறியீடுகள், பெரிய எழுத்துக்கள் அல்லது இலக்கங்களை சேர்க்கவும்.

உங்கள் தனித்துவமான கடவுச்சொற்றொடர்களை உருவாக்குவதற்கும், சேமிப்பதற்கும் கடவுச்சொல் நிர்வாகி (password manager) ஒன்றை பயன்படுத்த முயற்சி செய்யுங்கள்.

உங்கள் சாதனங்களைப் பாதுகாப்பாக வைத்திருக்க அனைத்து மென்பொருள் புதுப்பிப்புகளையும் நிறுவவும்.

'இண்டர்நெட்' இணைப்புள்ள உங்கள் அனைத்து சாதனங்களுக்கும் (உங்கள் தொலைபேசி, மடிக்கணினி அல்லது 'ஸ்மார்ட் 'கைக்கடிகாரம் போன்றவை) எப்போதும் மென்பொருள் புதுப்பிப்புகளை நிறுவுவது உங்களை இணையத்தில் பாதுகாப்பாக வைத்திருக்க மிகவும் அவசியம்.

மென்பொருள் புதுப்பிப்புகள் உங்கள் சாதனங்களின் பாதுகாப்பில் உள்ள குறைபாடுகள் அல்லது இடைவெளிகளை சரிசெய்கின்றன. வழக்கமான புதுப்பிப்புகளை நிறுவுவது உங்கள் சாதனங்களைப் பாதுகாப்பாக வைத்திருப்பதோடு 'சைபர் 'குற்றவாளிகள் அவற்றை அணுகுவதை கடினமாக்கும்.

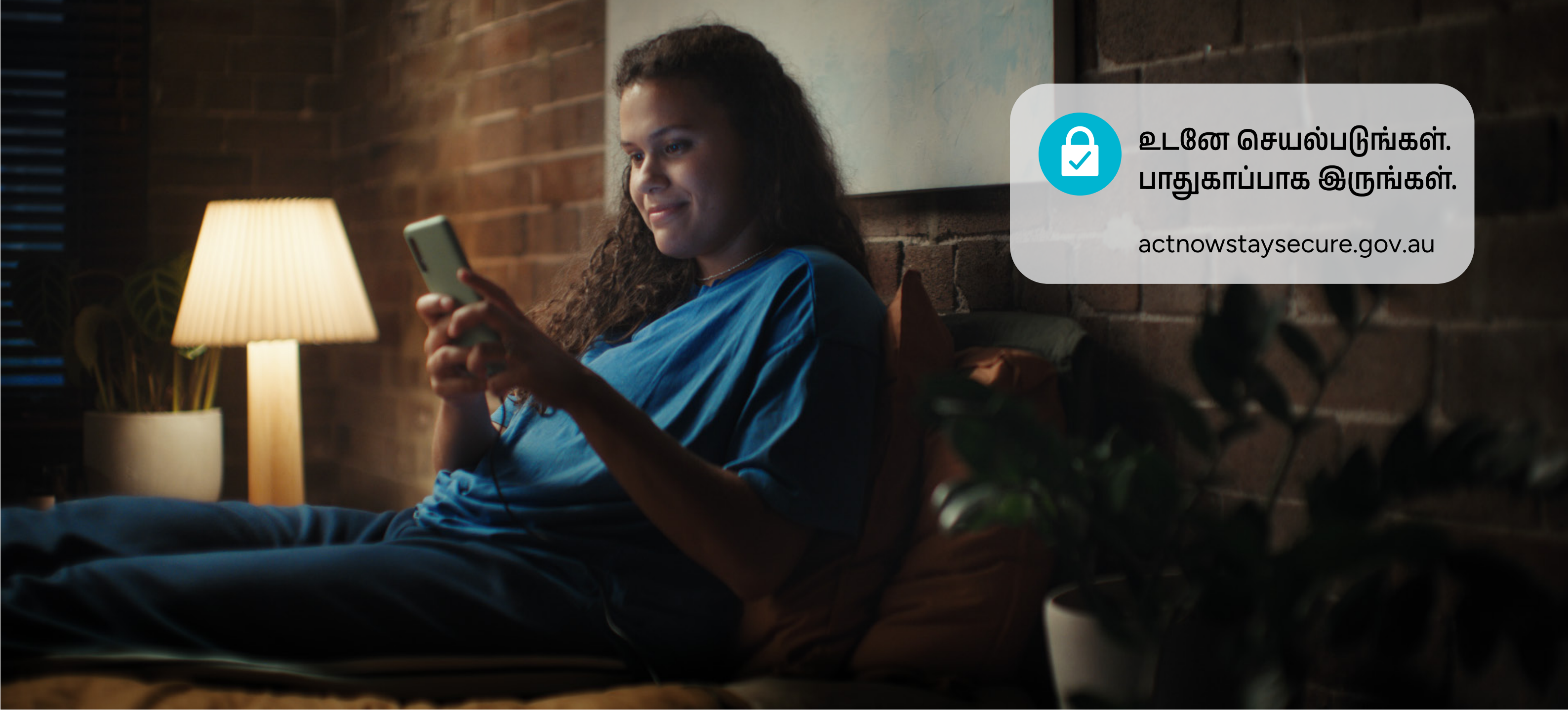
தானியங்கி புதுப்பிப்புகளை இயங்கும் நிலையில் வைத்திருங்கள், அத்துடன், வேண்டப்படும்போது அவற்றை நிறுவ மறக்காதீர்கள்.

எப்போதும் பல படிநிலைகளைக் கொண்ட உறுதிப்பாட்டு முறைமைகளை ஏற்படுத்திக்கொள்ளவும்.

உங்கள் அனைத்து இணையக் கணக்குகளுக்கும் கூடுதல் பாதுகாப்பைக் கொடுக்க, பல படிநிலைகளைக் கொண்ட உறுதிப்பாட்டு முறைமைகளை இயங்கும் நிலையில் வைத்திருங்கள்.

உங்கள் கணக்கில் உள்நுழைய பல படிநிலைகளைக் கொண்ட உறுதிப்பாட்டு முறைமை இரண்டு அல்லது அதற்கு மேற்பட்ட சரிபார்ப்பு முறைகளைக் கோரும். எடுத்துக்காட்டாக, உங்கள் கடவுச்சொல் அல்லது கடவுச்சொற்றொடரை உள்ளிட்ட பிறகு, ஒரு சரிபார்ப்புச் செயலி, மின்னஞ்சல் அல்லது குறுஞ்செய்தி வழியாக உங்களுக்கு அனுப்பப்பட்ட குறியீட்டை உள்ளிடுவது போன்ற இரண்டாவது சரிபார்ப்பை வழங்குமாறு உங்களிடம் கேட்கப்படும்.

உங்கள் உறுதிப்பாட்டு முறைமைகளில் ஒன்று (கடவுச்சொற்றொடர் போன்றவை) திருடப்பட்டாலும் கூட, பல படிநிலைகளைக் கொண்ட உறுதிப்பாட்டு முறைமை உங்கள் கணக்கைப் பாதுகாக்கும்.



இணையத்தில் பாதுகாப்பாக இருக்க மேலும் பல வழிகள் உங்களுக்கு வேண்டுமா?

‘சைபர்’ தாக்குதலில் இருந்து பாதுகாப்பாக இருக்க மேலும் வழிகளைத் தேடுகிறீர்களா? இணையத்தில் உங்களைப் பாதுகாத்துக் கொள்ள நீங்கள் எடுக்கக்கூடிய வேறு சில நடவடிக்கைகள் பின்வருமாறு.

பொது ‘வைஃபை’ (Wi-Fi) யை பயன்படுத்தும் போது கவனமாக இருங்கள்.

பொது ‘வைஃபை’ (Wi-Fi)-யை பயன்படுத்தும் போது, இணைப்பு பாதுகாப்பானதாக இருக்காது என்பதால், எந்தவொரு முக்கியமான அல்லது தனிப்பட்ட தகவலையும் அணுக வேண்டாம். இதில் உங்கள் சமூக ஊடகங்கள், மின்னஞ்சல் அல்லது இணையவழி வங்கிச் சேவைகளும் அடங்கும். நீங்கள் உள்ளிடும் எந்தத் தகவலும் ‘சைபர்’ குற்றவாளிகளால் அணுகப்படலாம்.

உங்கள் அந்தரங்கம் மற்றும் இருப்பிட அமைப்புகளை (location settings) தவறாமல் சரிபார்த்துப் புதுப்பிக்கவும்.

உங்களைப் பற்றிய தனிப்பட்ட அல்லது அடையாளம் காணக்கூடிய தகவல்களைப் பொதுமக்களுடன் தற்செயலாகப் பகிர்ந்துகொள்ளாமல் இருப்பதை உறுதிப்படுத்த, உங்கள் அந்தரங்கத் தன்மை மற்றும் இருப்பிட அமைப்புகளை அடிக்கடி சரிபார்க்கவேண்டியது முக்கியம்.

உங்கள் சமூக ஊடக கணக்குகளில் உள்ள அந்தரங்க அமைப்புகள் (privacy settings) மற்றும் உங்கள் செயலிகள், சாதனங்களில் உள்ள புவிஇருப்பிடக் கண்காணிப்பு ஆகியவை சரிபார்க்க வேண்டிய விடயங்களில் அடங்கும்.

‘சைபர்’ தாக்குதலில் இருந்து பாதுகாப்பாக இருப்பது எப்படி என்பது பற்றி நண்பர்கள் மற்றும் குடும்பத்தினருடன் கலந்துரையாடுங்கள்.

குறிப்பாக ‘இன்டர்நெட்’டுடன் இணைக்கப்பட்ட சாதனங்களைப் பகிர்ந்துகொள்ளும் பொழுது, உங்களையும், உங்கள் குடும்பத்தினரையும், நண்பர்களையும் இணையத்தில் பாதுகாப்பாக வைத்திருக்க இதைப் பற்றிய கல்வியறிவும், விழிப்புணர்வும் மிக முக்கியம். உங்களுக்கு நெருக்கமானவர்களுடன் இதைப் பற்றிப் பேசுவது ‘சைபர்’ பாதுகாப்பு மிக முக்கியமானது என்ற உணர்வை அவர்களுக்கு ஏற்படுத்தி இணையத்தில் தங்களை எவ்வாறு பாதுகாத்துக் கொள்வது என்பது குறித்த சமீபத்திய தகவல்களை அவர்கள் பெறுவதை உறுதி செய்யும்.

ஒரு ஏமாற்று மோசடியை எவ்வாறு அடையாளம் காண்பது என்பதை அறிந்து கொள்க.

ஏமாற்று மோசடி செய்பவர்கள் மக்களை ஏமாற்றி அவர்கள் பணத்தைச் செலுத்தவோ அல்லது அவர்களின் தனிப்பட்ட தகவல்களை வழங்கவோ செய்கிறார்கள்.

நீங்கள் யாருடன் தொடர்புகொள்கிறீர்கள் என்பது உறுதியாகத் தெரியாவிட்டால், யாருக்கும் பணத்தையோ அல்லது தனிப்பட்ட தகவல்களையோ கொடுக்காதீர்கள். அதிகாரப்பூர்வ வலைத்தளம் அல்லது செயலியில் இருந்து நீங்கள் கண்டறிந்த விவரங்களைப் பயன்படுத்தி அந்த நபர் அல்லது நிறுவனத்துடன் தொடர்புகொண்டு அவர்கள் யார் என்று தெரிந்துகொள்ளுங்கள்.

‘சைபர்’ தாக்குதல்கள் மற்றும் சம்பவங்களைப் புகார்ப்படுத்துங்கள்

புதிய போக்குகளைக் கண்டறியவும், சமூகத்தை எச்சரிக்கவும், ‘சைபர்’ சம்பவத்திலிருந்து நீங்கள் மீள்வதற்கு உதவவும் அரசாங்கத்திற்கு உதவ மோசடிகள் அல்லது ‘சைபர்’ சம்பவங்களைப் புகாரளிப்பது மிகவும் முக்கியமானது.

உங்களைப் பாதுகாத்துக் கொள்வதற்கான எளிய வழிமுறைகளை actnowstaysecure.gov.au -இல் அறிந்து கொள்ளுங்கள்

உடனே செயல்படுங்கள்.
பாதுகாப்பாக இருங்கள்.
actnowstaysecure.gov.au