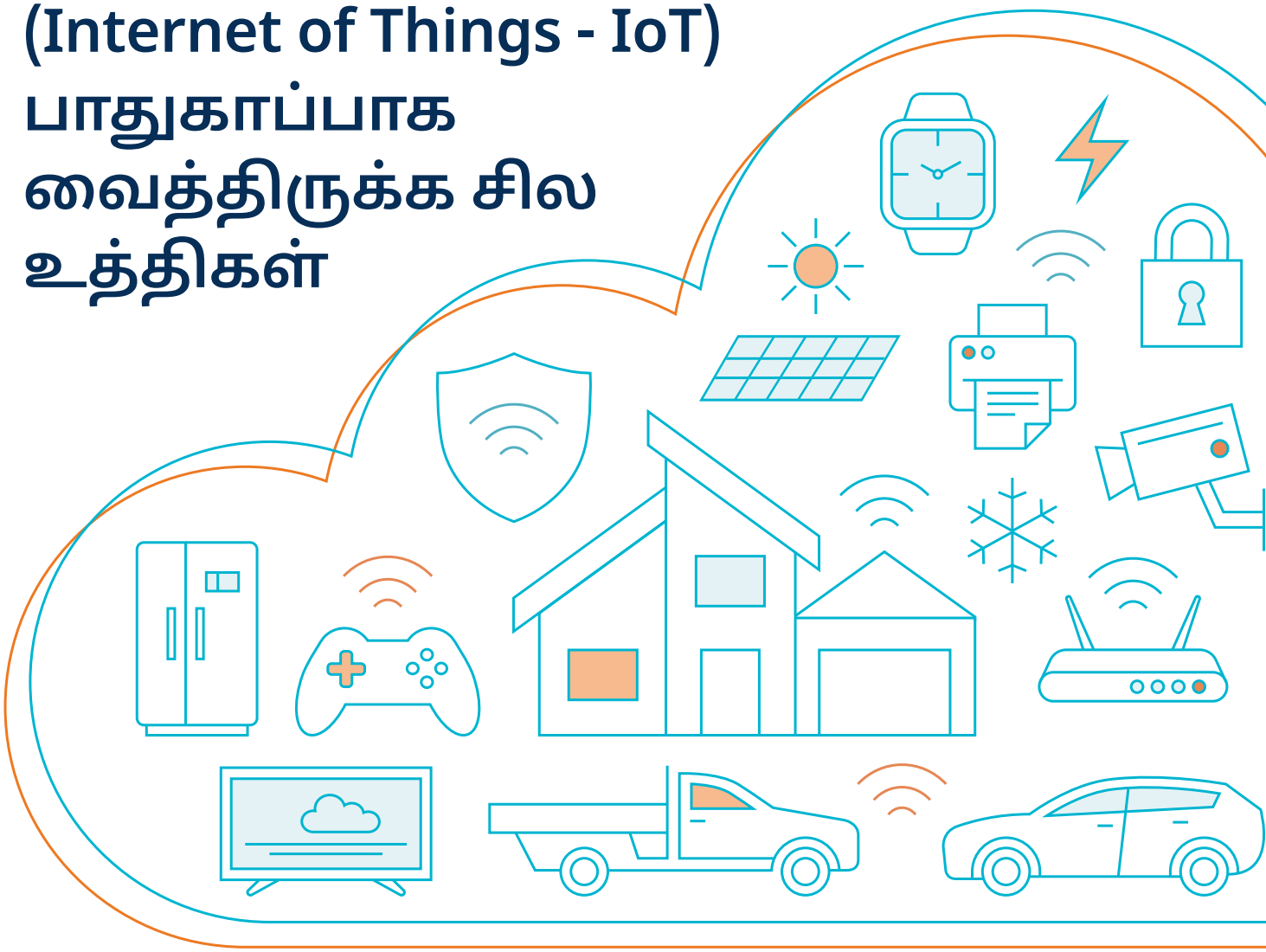
இணைய சாதனங்களை (Internet of Things - IoT) பாதுகாப்பாக வைத்திருக்க சில உத்திகள்



இணைய வலைத்தளத்துடன் இணைக்கப்படும் சாதனங்களை (IoT) வாங்கி, பாதுகாப்பாகப் பயன்படுத்த உதவும் வகையில் ஆஸ்திரேலிய சைபர் பாதுகாப்பு மையம் இந்த ஆவணத்தை உருவாக்கியுள்ளது. ஒரு IoT சாதனம் என்பது இணைய வலைத்தளத்துடன் இணைக்கப்பட்ட ஒரு அன்றாடப் பொருளாகும். குழந்தைகளைக் கண்காணிக்கப் பயன்படுத்தப்படும் கருவிகள், ட்ரோன்கள், பாதுகாப்பு கமராக்கள், ஸ்மார்ட் தொலைக்காட்சிகள் மற்றும் சூரிய ஒளியிலிருந்து மின்சாரம் உற்பத்தி செய்யும் கருவிகள் IoT சாதனங்களின் எடுத்துக்காட்டுகளில் அடங்கும். வீடுகள் மற்றும் வணிக நிறுவனங்களில் பயன்படுத்தப்படும் IoT சாதனங்களை இணையத்துடன் இணைக்க Wi-Fi அல்லது 4G அல்லது 5G போன்ற நெட்வொர்க்குகள் பயன்படுத்தப்படுகின்றன.

ஆஸ்திரேலிய வீடுகள் மற்றும் வணிக நிறுவனங்களில் பொதுவாகப் பயன்படுத்தப்படும் பல IoT சாதனங்கள் பாதுகாப்பைக் கருத்தில் கொண்டு வடிவமைக்கப்படவில்லை. இதன் விளைவாக, இணைய வலைத்தளத்துடன் இணைக்கப்படும் சாதனங்கள் பாதிக்கப்படும் அபாயம் ஏற்பட்டுள்ளது. தீங்கிழைக்கும் நோக்கங்களுக்காக, சைபர் குற்றவாளிகள் உங்கள் சாதனம் மற்றும் தனிப்பட்ட தரவை அனுமதியின்றி அணுக இதுபோன்ற சம்பவங்கள் அனுமதிக்கும்.

ஒரு IoT சாதனத்தை வாங்குவதற்கு முன்

சாதனங்களை உற்பத்தி செய்பவர்கள் பல்வேறு அளவிலான பாதுகாப்பை வழங்குவதால், அவற்றை வாங்குவதற்கு முன் அது குறித்து ஆராய்வது முக்கியம். ஒரு சாதனத்தை வாங்குவதற்கு முன், வெவ்வேறு உற்பத்தியாளர்களால் விற்கப்படும் ஒத்த சாதனங்களை ஒப்பிட்டுப் பாருங்கள். நீங்கள் கருத்தில் கொள்ள வேண்டிய விடயங்களில் சில:

1. **அந்த சாதனம் ஒரு பிரபலமான நிறுவனத்தால் தயாரிக்கப்பட்டு, ஒரு பிரபலமான விற்பனையாளரால் விற்கப்படுகிறதா?** நன்கு அறியப்பட்ட நற்பெயர் பெற்ற நிறுவனங்கள் சாதனங்களைத் தயாரிக்கும் போது, பாதுகாப்பைக் கருத்தில் கொண்டு தயாரிப்பதற்கான வாய்ப்புகள் அதிகம். நன்கு அறியப்பட்ட, புகழ்பெற்ற விற்பனையாளர்கள், நன்கு அறியப்பட்ட புகழ்பெற்ற நிறுவனங்களின் சாதனங்களை மட்டுமே விற்பனை செய்வதற்கான வாய்ப்புகள் அதிகம், மேலும் உற்பத்தியாளரின் நோக்கத்தின்படி சாதனம் உங்களுக்குக் கிடைப்பதை உறுதிசெய்யும் கடுமையான விநியோகச் சங்கிலியைக் கொண்டுள்ளன.

2. **கடவுச்சொல்லை மாற்ற முடியுமா?** உங்கள் கடவுச்சொல்லை மாற்றுவது எப்போதும் நல்லது. அதே வேளை, பலவீனமான இயல்புநிலை கடவுச் சொல்லுடன் சாதனம் அனுப்பப்பட்டால், கடவுச்சொல்லை மாற்றுவது மிகவும் முக்கியமானதாகிறது. நல்ல பாதுகாப்பு உள்ள ஒரு சாதனம் தனித்துவமான, கணிக்க முடியாத, சிக்கலான மற்றும் ஊகிக்க முடியாத கடவுச் சொற்களைக் கொண்டிருக்க வேண்டும், ஏனெனில் பலவீனமான இயல்புநிலை கடவுச் சொற்கள் ஒரு சாதனத்தைத் தாக்க எளிதான வழிகளாகும்.

3. **புதுப்பிப்புகளை உற்பத்தியாளர் வழங்குகிறாரா?** சாதனங்கள் பாதிப்புக்குள்ளாகின்றன என கண்டறியப்படும்போது, அவற்றை சரிசெய்ய புதுப்பிப்புகளை நிறுவனங்கள் வழங்குவது முக்கியம். எடுத்துக்காட்டாக, சாதனத்தில் உள்ள மென்பொருளில் அறியப்பட்ட பாதிப்புகள் இருந்தால் அல்லது உங்கள் சாதனத்தை சமரசம் செய்வதற்கான புதிய வழிகளை இணையவழி திருடர்கள் உருவாக்கினால், திருத்தங்களை வழங்க புதுப்பிப்புகள் தேவை.

4. **என்ன தரவுகளை சாதனம் சேகரிக்கும், அந்தத் தரவுகள் யாருடன் பகிரப்படும்?** என்ன தரவு சேகரிக்கப்படும், அது எவ்வாறு பயன்படுத்தப்படும் என்பது பற்றிய தகவல்கள் உற்பத்தியாளரின் வலைத்தளத்திலோ அல்லது அவர்களின் தனியுரிமைக் கொள்கையிலோ உடனடியாகக் கிடைக்க வேண்டும். இணைய வழியாக அல்லது செயலிகளூடாக என்ன தரவுகள் சேகரிக்கப் படுகின்றன என்பதைக் கருத்தில் கொள்வது மிகவும் முக்கியம்.

5. **நீங்கள் விரும்புவதை மட்டும்தான் அந்த சாதனம் செய்கிறதா?** இணையத்துடன் இணைப்பது உட்பட உங்களுக்குத் தேவையானதை விட அதிகமாகச் செய்யும் சாதனத்தை வாங்குவது உங்கள் பாதுகாப்பைக் குறைக்கக்கூடும். நீங்கள் பயன்படுத்தாத சில சாதனத் திறன்கள், உங்களுக்கு எந்தப் பலனையும் வழங்காமல், சாதனத்தைத் தாக்குதல்களுக்கு உட்படுத்தும் பாதிப்பை அதிகரிக்கக்கூடும்.

இணைய வலைத்தளத்துடன் இணைக்கப்படும் சாதனம் (IoT)

உங்கள் நெட்வொர்க் மற்றும் தரவை மிகவும் பாதுகாப்பாக வைத்திருக்க உதவும் வகையில், உங்கள் சாதனத்தை இணைக்கும் போது சில எளிய கேள்விகளை மனதில் கொள்ளுங்கள்.

1. **இந்த சாதனம் அவசியம் இணையத்துடன் இணைக்கப்பட வேண்டுமா?** இணையத்துடன் இணைக்க முடியும் என்பதற்காக, அதனை அவசியம் இணைக்க வேண்டியது அவசியமல்ல. இணையத்துடன் இணைக்கப்படாத சாதனங்கள் பாதிக்கப்படுவதற்கான வாய்ப்புகள் மிகக் குறைவு. இணையத்துடன் இணைப்பதால் கிடைக்கும் செயற்பாடுகளை நீங்கள் பயன்படுத்தப் போவதில்லை என்றால், அந்த சாதனத்தை இணையத்துடன் இணைக்க வேண்டுமா என்பதை நீங்கள் கருத்தில் கொள்ள வேண்டும்.

2. **சாதனம் பாதுகாப்பான இடத்தில் உள்ளதா?** பாதுகாப்பற்ற ஒரு இடத்தில் சாதனத்தை நிறுவ வேண்டிய அவசியமில்லை என்றால், அதை பாதுகாப்பான இடத்தில் நிறுவுவதன் மூலம் அது சமரசமாகும் அபாயத்தைக் குறைக்கலாம்.

3. **இயல்புநிலை பயனர் பெயர் மற்றும் கடவுச்சொல்லை நான் மாற்ற வேண்டுமா?** வலுவான கடவுச்சொல் அல்லது கடவுச் சொற்றொடரைப் பயன்படுத்துவது முக்கியம். தனித்துவமான, கணிக்க முடியாத, சிக்கலான மற்றும் ஊகிக்க முடியாத கடவுச் சொல்லுடன் உங்கள் சாதனம் அனுப்பப்படவில்லை என்றால், அந்தக் கடவுச்சொல்லை மாற்ற வேண்டும். இயல்புநிலை பயனர் பெயர்கள் மற்றும் கடவுச் சொற்கள் சேகரிக்கப்பட்டு ஆன்லைனில் இடுகையிடப்படுகின்றன என்பதனால் உங்கள் சாதனம் பாதிக்கப்படக் கூடியதாக இருக்கும்.

4. **எனது Wi-Fi நெட்வொர்க் பாதுகாப்பாக அமைக்கப்பட்டுள்ளதா, அத்துடன் அதற்குப் பாதுகாப்பான கடவுச்சொல் இருக்கிறதா?** உங்கள் சாதனத்தையும் உங்கள் நெட்வொர்க்கையும் தாக்க முயல்பவர்கள் அணுகுவதை கடினமாக்கும் வகையில் உங்கள் Wi-Fi நெட்வொர்க் மற்றும் routerரைப் பாதுகாக்கவும்.

மேலும் பாதுகாப்பை விரும்பினால்

IoT சாதனங்களுக்கு மட்டும் என்று உங்கள் routerரில் பிறிதொரு Wi-Fi நெட்வொர்க்கை அமைக்கவும். இது உங்கள் Wi-Fi routerரில் 'விருந்தினர்' நெட்வொர்க் என்று அறியப்படலாம். உங்கள் IoT சாதனங்கள் ஒன்றுக்கொன்று தொடர்பு கொள்ளத் தேவையில்லை என்றால், 'client isolation' என்று தனிமைப்படுத்தி இயக்கவும். உங்கள் முக்கியமான தரவுகளிலிருந்து IoT சாதனங்களைத் தனிமைப்படுத்துவதன் மூலம், ஒரு IoT சாதனம் சமரசம் செய்யப்பட்டாலும், உங்களது பிற சாதனங்கள் அல்லது தரவுகளுக்கான அணுகல் இருக்காது என்பதை உறுதி செய்கிறது.

5. **தேவையற்ற செயல்பாடுகள் சாதனத்தில் முடக்கப்பட்டுள்ளனவா?** (கமராக்கள் அல்லது ஒலிவாங்கிகள் போன்ற) தேவையற்ற விடயங்கள் உங்கள் சாதனத்தில் இருந்தால், முடிந்தவரை அவற்றின் செயல்பாட்டை முடக்கி விட வேண்டும்.

மேலும் பாதுகாப்பை விரும்பினால்

உங்களது LAN அல்லது WAN கட்டமைப்பு, இணையத்துடன் இணைக்கப்படக்கூடிய சாதனங்களைத் தொலைவிலிருந்து அணுகுவதற்கு அனுமதி வழங்கியுள்ளதா என்று அதன் உள்ளமைவில் தேடுங்கள். தொலைவிலிருந்து உங்கள் சாதனங்களை அணுகும் தேவை உங்களுக்கு இல்லையென்றால், அது Local LAN என்று அமைக்கப்பட்டிருக்கிறது என்பதை உறுதிப்படுத்தவும்.

ஒரு IoT சாதனத்தைப் பராமரித்தல்

உங்கள் IoT சாதனம் இணைக்கப்பட்டு, பயன்பாட்டில் இருக்கும் போது நினைவில் கொள்ள வேண்டிய சில முக்கியமான விடயங்கள் உள்ளன. அவற்றில் சில:

1. **உங்கள் சாதனங்களை, தவறாமல் மறுதொடக்கம் (reboot) செய்யுங்கள்.** IoT சாதனம் மெதுவாக இயங்கினால் அல்லது செயல்பட முடியாமல் போயிருந்தால், வைரஸ்கள் இருக்க வாய்ப்பிருக்கிறது. பெரும்பாலான தீம்பொருள் சாதனத்தின் நினைவகத்தில் சேமிக்கப்படுகிறது என்பதால், சாதனத்தை மறுதொடக்கம் செய்வதன் மூலம் இது எளிதாக அகற்றப்படலாம், அதாவது, சாதனத்தை அணைத்து மீண்டும் இயக்குவதன் மூலம். மறுதொடக்கத்திற்குப் பின்னரும் சாதனம் மெதுவாக இயங்கினால் அல்லது செயலற்றுப் போனால், factory reset என்ற ஆரம்ப நிலைக்கு சாதனத்தை மீட்டமைக்க முயற்சிக்கவும். ஆனால் ஒரு எச்சரிக்கை, இப்படி செய்வதால் உங்கள் பயனர் தரவு மற்றும் தனிப்பயனாக்கப்பட்ட விடயங்கள் அழிக்கப்பட்டுவிடக்கூடும் என்பதை மனதில் கொள்ளுங்கள்.

2. **வழமையான புதுப்பிப்புகளைப் பயன்படுத்தவும்.** சில சாதனங்கள் தானாகவே புதுப்பிப்புகளைப் பயன்படுத்துகின்றன. அவ்வாறு செய்யாதவர்கள் சாதனத்தை உற்பத்தி செய்தவருடன் ஒப்பிட்டுப் பார்த்து, புதுப்பிப்புகள் கிடைக்கும் போது அவற்றைப் பயன்படுத்துங்கள். உங்கள் சாதனத்திற்கு புதுப்பிப்புகள் இனி கிடைக்காது என்ற நிலை வரும்போது, புதுப்பிப்புகள் கிடைக்கக்கூடிய புதிய சாதனத்திற்கு மேம்படுத்துவதைக் கருத்தில் கொள்ளவும். சாதனங்களைப் பாதிக்கக்கூடிய விடயங்கள் புதிதாகக் கண்டுபிடிக்கப்பட்டால், அவற்றிலிருந்து பாதுகாப்பு புதுப்பிப்புகளுக்கான அணுகல் இல்லாத சாதனங்கள் பாதுகாக்கப்படாது. அத்துடன், உங்கள் நெட்வொர்க், உங்கள் தனியுரிமை மற்றும் உங்கள் தரவுகளுக்கு, இந்த சாதனம் ஆபத்தானதாக மாறக்கூடும்.

3. **உங்கள் சாதனம் பயன்பாட்டில் இல்லாதபோது அதை அணைத்து வைக்கவும்.** பயன்படுத்தப்படாத மற்றும் கண்காணிக்கப்படாத சாதனங்களை உங்கள் Wi-Fi நெட்வொர்க்குடன் நீண்ட காலத்திற்கு இணைத்து வைத்திருந்தால் உங்கள் சாதனங்கள் தாக்கப்படுவதற்கான வாய்ப்பு அதிகரிக்கும். இதனை நீங்கள் தலையிடாமல் தானாகவே அணைத்து வைப்பதற்கு அந்த சாதனத்திற்குக் குறிப்பிட்ட சில நேரங்களுக்கு மட்டும் சக்தியை வழங்க, timer போன்றவற்றைப் பயன்படுத்துவது ஒரு வழி.

4. **உங்கள் மாதாந்தர இணைய பயன்பாடு அல்லது இணைய சேவைக்கான கட்டணத்தில் குறிப்பிடத்தக்க அதிகரிப்பு இருக்கிறதா என்று அவதானியுங்கள்.** இணைய பயன்பாடு அல்லது இணைய சேவைக்கான கட்டணத்தில் குறிப்பிடத்தக்க அதிகரிப்பு இருந்தால், உங்கள் சாதனம் சமரசம் செய்யப்பட்டுள்ளது என்பதைக் குறிக்கலாம். உங்கள் வணிக நிறுவனத்தின் தகவல் தொழில்நுட்பத் துறையால் ஆராயப்படாவிட்டால், factory reset என்ற ஆரம்ப நிலைக்கு சாதனத்தை மீட்டமைக்க வேண்டும். (ஆனால் ஒரு எச்சரிக்கை, இப்படி செய்வதால் உங்கள் பயனர் தரவு மற்றும் தனிப்பயனாக்கப்பட்ட விடயங்கள் அழிக்கப்பட்டுவிடக்கூடும் என்பதை மனதில் கொள்ளுங்கள்.) அதைத் தொடர்ந்து உங்கள் கடவுச்சொல்லை மாற்றவும்.

ஒரு IoT சாதனத்தை அப்புறப்படுத்துதல்

(அதை எறிவது அல்லது விற்பதன் மூலம்) ஒரு சாதனத்தை அப்புறப்படுத்தும் போது உங்கள் தனிப்பட்ட தகவல் அல்லது தரவை மற்றவர்கள் எளிதாக அணுகலாம். இதைத் தடுப்பதற்கான வழிகள் சில:

1. **எல்லா தரவையும் தனிப்பட்ட தகவலையும் சாதனத்திலிருந்து அழிக்கவும்.** சாதனம் மற்றும் தொடர்புடைய செயலிகள் இரண்டிலிருந்தும் உங்கள் தரவு மற்றும் தனிப்பட்ட தகவல்களை எவ்வாறு அழிப்பது என்பதற்கான ஒரு முறையை சாதனத்தின் உற்பத்தியாளர் வழங்கியிருக்க வேண்டும். உங்கள் தனிப்பட்ட தகவல்களை அழிப்பதன் மூலம் நீங்கள் சாதனத்தை அப்புறப்படுத்திய பிறகு யாருக்கும் அந்த தகவல்கள் கிடைக்காது என்பதை உறுதி செய்யலாம். அந்த IoT சாதனம் இல்லாமல் உங்களுக்கு அந்த ஆன்லைன் கணக்கு இனி தேவையில்லை என்றால் அந்தக் கணக்கை நீக்கவும்.

2. **சாதனத்தை factory reset என்ற ஆரம்ப நிலைக்கு மீட்டமைப்பு செய்யவும்.** Factory reset என்பது சாதனத்தின் சேமிப்பகத்தில் வைக்கப்பட்டுள்ள தரவை அழிக்கவும், கடவுச் சொற்கள், பயனர் பெயர்கள் மற்றும் அமைப்புகளை இயல்பு நிலைக்கு மீட்டமைக்கவும் வடிவமைக்கப்பட்டுள்ளது. Factory reset என்ற ஆரம்ப நிலைக்கு மீட்டமைப்பு செய்வது எப்படி என்பதை சாதனத்தின் பயனர் கையேடு அல்லது உற்பத்தியாளரின் இணையத்திலிருந்து பெறலாம்.

3. **பாவனையில் இல்லாத சாதனத்தை, மொபைல் போன்கள் மற்றும் பிற சாதனங்களிலிருந்து துண்டிக்கவும்.** உங்கள் பிற சாதனங்களுடன் தொடர்பு பட்ட ஒரு சாதனத்தை அப்புறப்படுத்தும் போது, நெட்வொர்க் அல்லது இணைய கணக்குகளை மற்றவர்கள் இன்னும் அணுகக்கூடிய சாத்தியக் கூறுகளைக் கொண்டுள்ளது. நீங்கள் அகற்றும் சாதனத்துடன் உங்கள் பிற சாதனங்களில் எந்தவித இணைப்பும் இல்லையென்பதை உறுதி செய்க. இனி தேவைப்படாத செயலிகளுக்கு வழங்கப்பட்ட அனைத்து அனுமதிகளையும் அகற்றவும்.

4. **சாதனத்துடன் இணைக்கப்பட்டுள்ள (USB flash drives மற்றும் memory card) போன்ற உதிரிகளை அகற்றவும்.** சாதனத்திலிருந்து அகற்றக் கூடிய உதிரிகள் factory reset மீட்டமைப்பில் நீக்கப்படாத தனிப்பட்ட தரவைக் கொண்டிருக்கலாம், எனவே அவை சாதனத்திலிருந்து அகற்றப்பட்டு, தனியாக எறியப் பட வேண்டும் அல்லது அழிக்கப்பட வேண்டும்.

உதவி

ஆஸ்திரேலிய சமிக்ஞைகள் இயக்குநரகத்தின் ஆஸ்திரேலிய சைபர் பாதுகாப்பு மையத்தை asd.assist@defence.gov.au என்ற மின்னஞ்சல் மூலம் தொடர்பு கொள்ளவும் அல்லது அவசர உதவிக்கு, ஒரு நாளில் 24 மணி நேரமும், வாரத்தில் 7 நாட்களும் **1300 CYBER1 (1300 292 371)** என்ற எண்ணை அழைக்கவும்.

பாதுகாப்பு முறியடிக்கப்பட்ட நிகழ்வு குறித்து ReportCyber இல் புகாரளிக்க, www.cyber.gov.au/report என்ற இணையத் தளத்திற்கு செல்லவும்.

உங்களுக்கு அடையாளத் திருட்டு ஏற்பட்டிருந்தால், IDCARE ஐ அவர்களின் இணையதளம் www.idcare.org மூலம் தொடர்பு கொள்ளவும்.

உங்களுக்கும் உங்கள் குடும்பத்தினருக்கும் தேவையான ஆலோசனை பெற www.cyber.gov.au ஐப் பார்வையிடவும். சமீபத்திய ஆன்லைன் அச்சுறுத்தல்கள் குறித்த இலவச ACSC எச்சரிக்கை சேவைக்கு பதிவு செய்க.

ஆன்லைனில் இணைந்திருக்க ஆஸ்திரேலியா மிகவும் பாதுகாப்பான இடம் என்று மாற்றுவோம்.

சைபர் பாதுகாப்பு ஆலோசனைக்கு, www.cyber.gov.au ஐப் பார்வையிடவும்

பொறுப்புத் துறப்பு

இந்த வழிகாட்டியில் கூறப்பட்டுள்ள விடயங்கள் பொதுவானவை. அவை சட்ட ஆலோசனையாகக் கருதப்படக்கூடாது. மேலும், எந்தவொரு குறிப்பிட்ட சூழ்நிலையில் அல்லது அவசரகால சூழ்நிலையில் நேரடியாக உதவும் என்று நம்பக்கூடாது. எந்தவொரு முக்கியமான விடயத்திலும், உங்கள் சொந்த சூழ்நிலைகள் தொடர்பாக தகுந்த சுயாதீனமான தொழில்முறை ஆலோசனையை நீங்கள் நாட வேண்டும்.

இந்த வழிகாட்டியில் உள்ள தகவல்களை நம்பியதன் விளைவாக ஏற்படும் எந்தவொரு சேதம், இழப்பு அல்லது செலவுக்கும் ஆஸ்திரேலிய காமன்வெல்த் அரசு எந்த பொறுப்பையும் ஏற்காது.

பதிப்புரிமை

ஆஸ்திரேலிய அரசின் Coat of Arms வகை இலச்சினையின் பயன்பாடு

ஆஸ்திரேலிய அரசின் Coat of Arms வகை இலச்சினை எந்தெந்த விதிமுறைகளின் கீழ் பயன்படுத்தப்படலாம் என்பது பிரதமர் துறை மற்றும் அமைச்சரவையின் Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au என்ற இணையதளத்தில் விரிவாக உள்ளது.

மேலும் தகவலுக்கு அல்லது இணைய பாதுகாப்பு முறியடிக்கப்பட்ட நிகழ்வு குறித்துப் புகாரளிக்க, எங்களைத் தொடர்பு கொள்ளவும்:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

இந்த எண்ணை ஆஸ்திரேலியாவிற்குள் மட்டுமே பயன்படுத்த முடியும்.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre