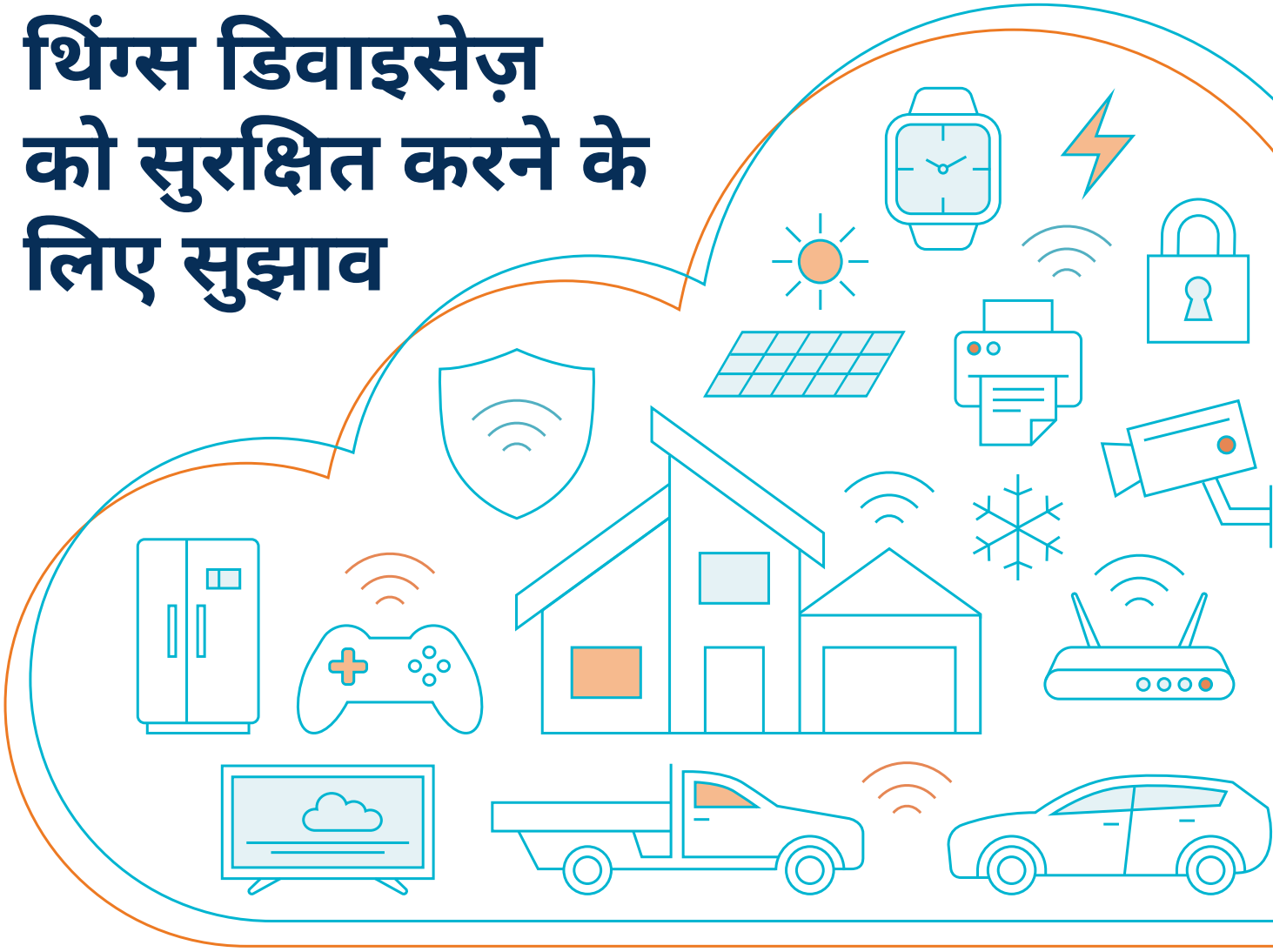
अपने इंटरनेट ऑफ थिंग्स डिवाइसेज़ को सुरक्षित करने के लिए सुझाव



ऑस्ट्रेलियाई साइबर सुरक्षा केंद्र ने समुदाय को इंटरनेट ऑफ थिंग्स (IoT) डिवाइसेज़ को सुरक्षित रूप से खरीदने और उपयोग करने में सहायता देने के लिए यह जानकारी विकसित की है। IoT डिवाइस एक ऐसी रोजमर्रा की वस्तु होती है, जिसमें इंटरनेट कनेक्टिविटी जोड़ी गई होती है। IoT डिवाइसेज़ के उदाहरणों में बेबी मॉनिटर्स, ड्रोन्स, सुरक्षा कैमरे, स्मार्ट टेलीविज़न्स और सोलर इनवर्टर्स शामिल हैं। आमतौर पर घरों और व्यवसायों में स्थित IoT डिवाइसेज़ इंटरनेट से कनेक्ट करने के लिए वाई-फाई अथवा 4G या 5G जैसे सेल्युलर नेटवर्क का उपयोग करते हैं।

आमतौर पर ऑस्ट्रेलिया में घरों और व्यवसायों में पाए जाने वाले कई IoT डिवाइसेज़ का डिज़ाइन सुरक्षा को ध्यान में रखकर नहीं किया गया है। इसके परिणामस्वरूप ये डिवाइसेज़ इंटरनेट के माध्यम से किए गए हमलों के प्रति अतिसंवेदनशील हैं। ऐसी घटनाएं साइबरअपराधियों को दुर्भावनापूर्ण उद्देश्यों के लिए आपके डिवाइस और व्यक्तिगत डेटा की अवांछित एक्सेस की अनुमति दे सकती हैं।

IoT डिवाइस खरीदने से पहले

डिवाइस खरीदने से पहले इसपर शोध करना महत्वपूर्ण है, क्योंकि निर्माता अलग-अलग स्तरों की सुरक्षा प्रदान करते हैं। डिवाइस खरीदने से पहले अलग-अलग निर्माताओं द्वारा बेचे जाने वाले इसके जैसे अन्य डिवाइसेज़ की तुलना करें। विचार करने योग्य बातों में शामिल हैं:

1. **क्या डिवाइस को किसी प्रसिद्ध प्रतिष्ठित कंपनी द्वारा बनाया जाता है और क्या इसे किसी प्रसिद्ध प्रतिष्ठित स्टोर द्वारा बेचा जाता है?** इस बात की संभावना अधिक है कि प्रसिद्ध प्रतिष्ठित कंपनियां सुरक्षा को ध्यान में रखते हुए डिवाइसेज़ का उत्पादन करेंगी। इस बात की संभावना भी अधिक है कि प्रसिद्ध प्रतिष्ठित स्टोर्स केवल प्रसिद्ध प्रतिष्ठित कंपनियों के डिवाइसेज़ बेचेंगे और उनके पास एक सख्त आपूर्ति-श्रृंखला होगी जो यह सुनिश्चित करती है कि निर्माता के इच्छित स्वरूप में ही आपको डिवाइस मिले।

2. **क्या पासवर्ड बदलना संभव है?** अपना पासवर्ड बदलना हमेशा अच्छा रहता है। यदि डिवाइस को एक कमजोर डिफ़ॉल्ट पासवर्ड के साथ भेजा जाता है, तो यह और भी अधिक महत्वपूर्ण है। अच्छी सुरक्षा वाले डिवाइस में अनन्य, अनुमान लगाने में कठिन, जटिल और अनुमान लगाने में अव्यवहार्य पासवर्ड होना चाहिए, क्योंकि किसी भी डिवाइस पर हमला करने का सबसे आसान तरीका एक कमजोर डिफ़ॉल्ट पासवर्ड होना है।

3. **क्या निर्माता अपडेट्स प्रदान करता है?** जैसे-जैसे कमजोरियां पहचान में आती हैं, यह महत्वपूर्ण है कि कंपनियां डिवाइस को दुरुस्त करने के लिए अपडेट्स प्रस्तुत करें। उदाहरण के लिए, यदि डिवाइस के सॉफ़्टवेयर में कोई ज्ञात अतिसंवेदनशीलताएं हैं या हैकर्स आपके डिवाइस पर हमला करने के नए तरीके विकसित करते हैं, तो दुरुस्त करने के लिए अपडेट्स की आवश्यकता होती है।

4. **डिवाइस क्या डेटा एकत्र करेगा और डेटा को किसके साथ साझा किया जाएगा?** क्या डेटा एकत्र किया जाएगा और उसका उपयोग कैसे किया जाएगा, इस बारे में जानकारी निर्माता की वेबसाइट पर या उनकी गोपनीयता नीति में आसानी से उपलब्ध होनी चाहिए। ऑनलाइन या मोबाइल एप्लिकेशन जो जानकारी एकत्र करती है, उसपर विचार करना हमेशा महत्वपूर्ण होता है।

5. **क्या डिवाइस केवल आपकी इच्छानुसार ही काम करता है?** अपनी आवश्यकता से अधिक काम करने वाले उपकरण खरीदने से आपकी सुरक्षा कम हो सकती है, जिसमें इंटरनेट से कनेक्ट करने वाले डिवाइस भी शामिल हैं। आप डिवाइस की जिन क्षमताओं का उपयोग नहीं करेंगे/गी, वे आपको कोई भी लाभ दिए बिना हमलों के प्रति डिवाइस की अतिसंवेदनशीलता बढ़ा सकती हैं।

IoT डिवाइस

अपने नेटवर्क और डेटा को अधिक सुरक्षित रखने में अपनी सहायता के लिए अपना डिवाइस सेट-अप करते समय कुछ आसान प्रश्नों को ध्यान में रखें।

1. **क्या डिवाइस को इंटरनेट से कनेक्ट करना आवश्यक है?** चूंकि इसे कनेक्ट किया जा सकता है, इसका मतलब यह नहीं है कि केवल इसी कारण से इसे कनेक्ट करना चाहिए। जो डिवाइस इंटरनेट से कनेक्ट नहीं होते हैं, उनपर हमला होने की संभावना बहुत कम होती है। यदि आप इंटरनेट कनेक्टिविटी की आवश्यकता वाले फीचर्स का उपयोग नहीं करने जा रहे/ही हैं, तो आपको इसे कनेक्ट करने की आवश्यकता के बारे में सोचना चाहिए।

2. **क्या डिवाइस सुरक्षित स्थान पर है?** यदि डिवाइस को किसी असुरक्षित क्षेत्र में इंस्टॉल करना आवश्यक नहीं है, तो इसे सुरक्षित स्थान पर इंस्टॉल करने से भौतिक रूप से हमला किए जाने का जोखिम कम हो सकता है।

3. **क्या मुझे डिफ़ॉल्ट यूज़रनेम और पासवर्ड बदलना चाहिए?** यह महत्वपूर्ण है कि आप एक मजबूत पासवर्ड या पासफ़्रेज़ का उपयोग करें। यदि आपके डिवाइस को अनन्य, अनुमान लगाने में कठिन, जटिल और अनुमान लगाने में अव्यवहार्य पासवर्ड के साथ नहीं भेजा गया है, तो इस पासवर्ड को बदलना आवश्यक है। डिफ़ॉल्ट यूज़रनेम और पासवर्ड एकत्र किए जाते हैं और ऑनलाइन पोस्ट किए जाते हैं, जिससे आपका डिवाइस असुरक्षित हो जाता है।

4. **क्या मेरा वाई-फाई नेटवर्क सुरक्षित रूप से सेट है, और क्या इसमें सुरक्षित पासवर्ड है?** हमलावरों के लिए आपके डिवाइस और आपके नेटवर्क को एक्सेस करना कठिन बनाने के लिए अपने वाई-फाई नेटवर्क और राउटर को संरक्षित करें।

अतिरिक्त कोशिश करें

अपने राउटर पर एक अतिरिक्त वाई-फाई नेटवर्क सेट-अप करें, जो केवल IoT डिवाइसेज़ के लिए ही हो। आपके वाई-फाई राउटर पर इसे 'गेस्ट' नेटवर्क का नाम दिया जा सकता है। यदि आपके IoT डिवाइसेज़ को एक-दूसरे के बीच संचार करने की आवश्यकता नहीं है, तो 'क्लाइंट आइसोलेशन' फीचर एनेबल करें। अपने IoT डिवाइसेज़ को अपने संवेदनशील डेटा से अलग रखने से यह सुनिश्चित होता है कि किसी एक IoT डिवाइस पर हमले से आपके अन्य डिवाइसेज़ या डेटा की एक्सेस उपलब्ध नहीं होती है।

5. **क्या अनावश्यक डिवाइस फीचर्स बंद हैं?** यदि आपके डिवाइस में अवांछित या अनावश्यक फीचर्स (जैसे कैमरे या माइक्रोफ़ोन) हैं, तो जहां संभव हो इन्हें अक्षम किया जाना चाहिए।

अतिरिक्त कोशिश करें

ऐसी कॉन्फ़िगरेशन सेटिंग खोजें, जिसमें डिवाइस के वेब एडमिनिस्ट्रेशन इंटरफ़ेस पर रिमोट एक्सेस को लोकल लैन या वैन/इंटरनेट से एनेबल किया जा सके। यदि आपको स्वयं रिमोट एक्सेस की आवश्यकता न हो, तो इसे लोकल लैन पर सेट करना सुनिश्चित करें।

IoT डिवाइस का रख-रखाव

एक बार आपका IoT डिवाइस सेटअप हो जाने और उपयोग शुरू करने के बाद याद रखने योग्य कुछ महत्वपूर्ण बातें होती हैं। इनमें शामिल हैं:

1. **अपने डिवाइसेज़ को नियमित रूप से रिबूट करें।** यदि आईओटी डिवाइस धीमा या निष्क्रिय होना शुरू हो जाता है, तो वायरस मौजूद हो सकते हैं। अधिकांश मैलवेयर मेमोरी में स्टोर होते हैं और डिवाइस रिबूट द्वारा आसानी से हटाए जा सकते हैं, यानि डिवाइस को बंद और चालू करके। यदि रिबूट के बाद डिवाइस धीमा या निष्क्रिय बना रहता है, तो फ़ैक्टरी रीसेट की कोशिश करें, किंतु इस बात का ध्यान रखें कि यह आपके सभी उपयोगकर्ता डेटा और वैयक्तिकृत सेटिंग्स को मिटा सकता है।

2. **नियमित रूप से अपडेट्स इंस्टॉल करें।** कुछ डिवाइसेज़ स्वत: अपडेट्स इंस्टॉल करते हैं। जो ऐसा नहीं करते हैं, उनके लिए नियमित रूप से निर्माता के पास जांच करें और उपलब्ध होने पर अपडेट्स इंस्टॉल करें। जब आपके डिवाइस के लिए आगे अपडेट्स उपलब्ध नहीं होते हैं, तो एक नए डिवाइस में अपग्रेड करने पर विचार करें जिसके लिए अपडेट्स उपलब्ध हैं। जिन डिवाइसेज़ के लिए सिक्योरिटी अपडेट्स की एक्सेस उपलब्ध नहीं है, उनके लिए नई कमजोरियों का पता चलने पर वे संरक्षित नहीं होंगे और ये डिवाइस आपके नेटवर्क, आपकी गोपनीयता और आपके डेटा के लिए जोखिम बन सकते हैं।

3. **जब आपका डिवाइस उपयोग में न हो, तो उसे बंद कर दें।** अप्रयुक्त और अनियंत्रित डिवाइसेज़ को विस्तारित अवधि के लिए अपने वाई-फाई नेटवर्क से पावर-ऑन और कनेक्टेड रखने से आपके डिवाइसेज़ पर हमला होने की संभावना बढ़ सकती है। स्वत: रूप से यह हासिल करने का एक विकल्प है कि केवल निर्दिष्ट घंटों के दौरान डिवाइस को पावर देने के लिए एक पावर आउटलेट टाइमर का उपयोग किया जाए।

4. **अपने मासिक इंटरनेट उपयोग या बिल में काफी बड़ी वृद्धि के लिए देखें।** इंटरनेट उपयोग या बिलिंग शुल्कों में काफी बड़ी वृद्धियाँ यह संकेत दे सकती हैं कि आपके डिवाइस के साथ छेड़छाड़ की गई है। यदि आपके व्यवसाय के आईटी विभाग द्वारा इसकी जांच न की जाए, तो फ़ैक्टरी रीसेट किया जाना चाहिए (लेकिन ध्यान रखें कि यह आपके सभी उपयोगकर्ता डेटा और व्यक्तिगत सेटिंग्स को मिटा सकता है), और उसके बाद आपको पासवर्ड बदलना चाहिए।

IoT डिवाइस का निपटान

किसी डिवाइस का निपटान करने (फेंकने या बेचने) से अन्य लोगों को आपकी व्यक्तिगत जानकारी या डेटा की आसान एक्सेस मिल सकती है।
इसकी रोकथाम के तरीकों में शामिल हैं:

1. **सभी डेटा और व्यक्तिगत जानकारी मिटा दें।** डिवाइस और संबंधित एप्लिकेशन्स, इन दोनों से आपके डेटा और व्यक्तिगत जानकारी को मिटाने के लिए निर्माता को एक तरीका उपलब्ध कराना चाहिए। अपनी व्यक्तिगत जानकारी को मिटाने से यह सुनिश्चित होता है कि आपके द्वारा डिवाइस का निपटान करने के बाद कोई भी उसकी एक्सेस हासिल नहीं कर सकता है। यदि आपको IoT डिवाइस के बिना अपने ऑनलाइन खाते की आवश्यकता नहीं है, तो इसे डिलीट कर दें।

2. **डिवाइस को फ़ैक्टरी रीसेट करें।** फ़ैक्टरी रीसेट को लोकल स्टोरेज में मौजूद डेटा को मिटाने और पासवर्ड्स, उपयोगकर्ता नामों और सेटिंग्स को डिफ़ॉल्ट रूप से रीसेट करने के लिए डिज़ाइन किया गया है। फ़ैक्टरी रीसेट करने के तरीके के बारे में जानकारी के लिए डिवाइस का उपयोगकर्ता मैनुअल या निर्माता की वेबसाइट देखें।

3. **डिवाइस को मोबाइल फ़ोन और अन्य डिवाइसेज़ से अलग करें।** ऐसे किसी डिवाइस का निपटान करने से दूसरों को एक्सेस हासिल करने की क्षमता मिल सकती है, जिसके पास अभी भी आपके अन्य डिवाइसेज़, नेटवर्क या ऑनलाइन खातों की एक्सेस है। अपने अन्य डिवाइसेज़ की जांच करना सुनिश्चित करें और आपके द्वारा निपटान किए जा रहे डिवाइस के साथ किसी भी पेयरिंग को हटा दें। जिन मोबाइल एप्लिकेशन्स की अब आवश्यकता नहीं है, उनके लिए उपलब्ध कराई गई सभी पर्मिशन्स को हटा दें ।

4. **डिवाइस से जुड़े किसी भी रिमूवेबल मीडिया (जैसे USB फ्लैश ड्राइव, मेमोरी कार्ड आदि) को हटा दें।** रिमूवेबल मीडिया में ऐसा व्यक्तिगत डेटा मौजूद हो सकता है जिसे फ़ैक्टरी रीसेट में हटाया नहीं गया है और इसे अलग से डिवाइस में से भौतिक रूप से हटाया जाना चाहिए, भौतिक रूप से नष्ट किया जाना चाहिए और फिर इसका निपटान किया जाना चाहिए।

सहायता

ऑस्ट्रेलियाई सिग्नल्स निदेशालय के ऑस्ट्रेलियाई साइबर सुरक्षा केंद्र से संपर्क करने के लिए asd.assist@defence.gov.au पर ईमेल भेजें या तत्काल सहायता के लिए 24/7 हॉटलाइन **1300 CYBER1 (1300 292 371)** पर कॉल करें।

ReportCyber पर साइबरअपराध की रिपोर्ट करें: www.cyber.gov.au/report

यदि आपको पहचान की चोरी का अनुभव हुआ है, तो उनकी वेबसाइट www.idcare.org के माध्यम से IDCARE से संपर्क करें।

अपने और अपने परिवार के लिए सलाह के उद्देश्य से www.cyber.gov.au पर जाएं। हाल के ऑनलाइन खतरों पर नि:शुल्क एसीएससी एलर्ट सेवा के लिए साइन अप करें।

आइए ऑस्ट्रेलिया को ऑनलाइन कनेक्ट करने के लिए सबसे सुरक्षित स्थान बनाएं।

साइबर सुरक्षा सलाह के लिए www.cyber.gov.au पर जाएं।

अस्वीकरण

इस संदर्शिका में दी गई सामग्री सामान्य प्रकृति की है और इसे कानूनी सलाह के रूप में नहीं लिया जाना जाना चाहिए अथवा किसी विशेष परिस्थिति या आपात स्थिति में इसपर सहायता के लिए भरोसा नहीं किया जाना चाहिए। किसी भी महत्वपूर्ण मामले में आपको अपनी परिस्थितियों के संबंध में उपयुक्त स्वतंत्र पेशेवर सलाह लेनी चाहिए।

इस संदर्शिका में निहित जानकारी पर निर्भरता के परिणामस्वरूप होने वाले किसी भी क्षति, हानि या खर्चे के लिए राष्ट्रमंडल कोई भी जिम्मेदारी या दायित्व को स्वीकार नहीं करता है।

कॉपीराइट

कोट ऑफ आर्म्स का उपयोग

जिन शर्तों के तहत कोट ऑफ आर्म्स का उपयोग किया जा सकता है, उनका विवरण प्रधान मंत्री एवं कैबिनेट विभाग की वेबसाइट पर यहाँ उपलब्ध है: Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au

और अधिक जानकारी या किसी साइबर सिक्योरिटी घटना की रिपोर्ट करने के लिए हमसे संपर्क करें:

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

यह नंबर केवल ऑस्ट्रेलिया में उपयोग के लिए उपलब्ध है।

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre