Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

cyber.gov.au

আপনার ইন্টারনেট অফ থিংস ডিভাইসগুলিকে সুরক্ষিত করার টিপস

অস্ট্রেলিয়ান সাইবার সিকিউরিটি সেন্টার এই তথ্যটি তৈরি করেছে যাতে কমিউনিটি নিরাপদে ইন্টারনেট অফ থিংস (IoT) ডিভাইস কিনতে এবং ব্যবহার করতে পারে। IoT ডিভাইস হলো একটি নিত্যপ্রয়োজনীয় জিনিস যার সাথে ইন্টারনেট সংযোগ যুক্ত হয়েছে। IoT ডিভাইসের কয়েকটি উদাহরণ হল বেবি মনিটর, ড্রোন, সিকিউরিটি ক্যামেরা, স্মার্ট টেলিভিশন এবং সোলার ইনভার্টার। বাড়ি এবং ব্যবসার মধ্যে IoT ডিভাইসগুলি সাধারণত ইন্টারনেটের সাথে সংযোগ স্থাপনের জন্য Wi-Fi বা সেলুলার নেটওয়ার্ক, যেমন 4G বা 5G ব্যবহার করে।

অস্ট্রেলিয়ার বাড়ি এবং ব্যবসায় সাধারণত পাওয়া যায় এমন অনেক IoT ডিভাইস নিরাপত্তার কথা মাথায় রেখে ডিজাইন করা হয়নি। এর ফলে ইন্টারনেটের মাধ্যমে ডিভাইসগুলি ঝুঁকির মুখে পড়েছে। এই ধরনের ঘটনাগুলি সাইবার অপরাধীদের ক্ষতিকারক উদ্দেশ্যে আপনার ডিভাইস এবং ব্যক্তিগত ডেটাতে অযাচিত অ্যাক্সেসের সুযোগ করে দিতে পারে।

একটি IoT ডিভাইস কেনার আগে

কেনার আগে ডিভাইসগুলি নিয়ে খোঁজ খবর নেয়া গুরুত্বপূর্ণ, কারণ নির্মাতারা বিভিন্ন স্তরের নিরাপত্তা প্রদান করে। একটি ডিভাইস কেনার আগে, বিভিন্ন নির্মাতার দ্বারা বিক্রি হওয়া একই ধরণের ডিভাইসগুলির তুলনা করুন। যেসকল বিষয় বিবেচনা করবেন তার মধ্যে রয়েছে:

1. **ডিভাইসটি কি কোন সুপরিচিত নামী কোম্পানির তৈরি এবং কোন সুপরিচিত নামী দোকানে বিক্রি করা হয়?** সুপরিচিত নামী কোম্পানিগুলি খুব সম্ভবত নিরাপত্তার কথা মাথায় রেখে ডিভাইস তৈরি করে। সুপরিচিত নামীদামী দোকানগুলি কেবল সুপরিচিত নামীদামী কোম্পানিগুলির ডিভাইস বিক্রি করার সম্ভাবনা বেশি, এবং তাদের একটি কঠোর সরবরাহ-শৃঙ্খল থাকে যাতে ডিভাইসটি প্রস্তুতকারকের ইচ্ছানুযায়ী আপনার কাছে পৌঁছায়।

2. **পাসওয়ার্ড কি পরিবর্তন করা সম্ভব?** সবসময়ই আপনার পাসওয়ার্ড পরিবর্তন করে নেয়া ভালো। তবে, যদি ডিভাইসটি একটি দুর্বল ডিফল্ট পাসওয়ার্ড দিয়ে পাঠানো হয়, তাহলে এটি আরও গুরুত্বপূর্ণ হয়ে ওঠে। একটি সুরক্ষিত ডিভাইসে এমন পাসওয়ার্ড ব্যবহার করা উচিত যা ব্যতিক্রমী, অনিয়মিত, জটিল এবং যা অনুমান করা অসম্ভব, কারণ দুর্বল ডিফল্ট পাসওয়ার্ডগুলি কোনও ডিভাইস আক্রমণ করার সবচেয়ে সহজ উপায়।

3. **প্রস্তুতকারক কি আপডেট প্রদান করে?** যখনই কোন দুর্বলতা আবিষ্কৃত হয়, কোম্পানিগুলোর উচিত দ্রুত সফটওয়্যার আপডেট দেওয়া—কারণ এসব আপডেট ডিভাইসকে সুরক্ষিত রাখার ক্ষেত্রে গুরুত্বপূর্ণ। উদাহরণস্বরূপ, যদি ডিভাইসের সফ্টওয়্যারে জ্ঞাত দুর্বলতা থাকে অথবা হ্যাকাররা আপনার ডিভাইসে ঢুকার নতুন উপায় বের করে, তাহলে সমাধান প্রদানের জন্য আপডেটের প্রয়োজন হয়।

4. **ডিভাইসটি কোন ডেটা সংগ্রহ করবে এবং কাদের সাথে এই ডেটা শেয়ার করা হবে?** কোন তথ্য সংগ্রহ করা হবে এবং কীভাবে ব্যবহার করা হবে সে সম্পর্কে তথ্য প্রস্তুতকারকের ওয়েবসাইটে বা তাদের গোপনীয়তা নীতিতে সহজেই পাওয়া উচিত। অনলাইন বা মোবাইল অ্যাপ্লিকেশন যে তথ্য সংগ্রহ করে তা সর্বদা বিবেচনা করা গুরুত্বপূর্ণ।

5. **ডিভাইসটি কি কেবল আপনি যা করতে চান তাই করে?** এমন একটি ডিভাইস কেনা যা আপনার প্রয়োজনের চেয়ে বেশি কাজ করে, যার মধ্যে ইন্টারনেট সংযোগও অন্তর্ভুক্ত, তা আপনার নিরাপত্তা হ্রাস করতে পারে। আপনি ডিভাইসের যে সক্ষমতাগুলি ব্যবহার করবেন না তা আপনাকে কোনও সুবিধা না দিয়েই ডিভাইসে আক্রমণের ঝুঁকি বাড়িয়ে তুলতে পারে।

IoT ডিভাইস

আপনার ডিভাইস সেট আপ করার সময় কয়েকটি সহজ প্রশ্ন মনে রাখবেন, যা আপনার নেটওয়ার্ক এবং ডেটা আরও সুরক্ষিত রাখতে সাহায্য করবে।

1. **ডিভাইসটি কি ইন্টারনেটের সাথে সংযুক্ত থাকা প্রয়োজন?** কেবল ইন্টারনেটের সাথে সংযুক্ত হতে পারে বলেই যে এটি সংযুক্ত হওয়া উচিত তা নয়। যেসব ডিভাইস ইন্টারনেটের সাথে সংযুক্ত নয়, সেগুলোর ঝুঁকির সম্ভাবনা অনেক কম। যদি আপনি ইন্টারনেট সংযোগের প্রয়োজনীয় ফিচারগুলো ব্যবহার না করেন, তাহলে ডিভাইসটি ইন্টারনেটে সংযুক্ত করা উচিত কি না—সেটা ভেবে দেখা দরকার।

2. **ডিভাইসটি কি নিরাপদ স্থানে আছে?** যদি ডিভাইসটি কোনও অনিরাপদ স্থানে ইনস্টল করার প্রয়োজন না হয়, তবে এটি একটি নিরাপদ স্থানে ইনস্টল করলে ফিজিক্যাল ক্ষতির ঝুঁকি কমানো যেতে পারে।

3. **আমি কি ডিফল্ট ব্যবহারকারীর নাম এবং পাসওয়ার্ড পরিবর্তন করব?** আপনার একটি শক্তিশালী পাসওয়ার্ড বা পাসফ্রেজ ব্যবহার করা গুরুত্বপূর্ণ। যদি আপনার ডিভাইসে ব্যতিক্রমী, অনিয়মিত, জটিল এবং অনুমান করা অসম্ভব এমন একটি পাসওয়ার্ড না থাকে তবে সেই পাসওয়ার্ডটি পরিবর্তন করতে হবে। ডিফল্ট ব্যবহারকারীর নাম এবং পাসওয়ার্ড অনলাইনে সংগ্রহ করে প্রকাশ করা হয়, যার ফলে আপনার ডিভাইসটি ঝুঁকির মুখে পড়ে।

4. **আমিআমার ওয়াই-ফাই নেটওয়ার্ক নিরাপদে সেট আপ করেছি, এবংএটির কি কোন নিরাপদ পাসওয়ার্ড আছে?** আক্রমণকারীদের আপনার ডিভাইস এবং নেটওয়ার্ক অ্যাক্সেস করা কঠিন করে তুলতে আপনার ওয়াই-ফাই নেটওয়ার্ক এবং রাউটার সুরক্ষিত করুন।

অতিরিক্ত চেষ্টা করুন

শুধুমাত্র IoT ডিভাইসের জন্য আপনার রাউটারে একটি অতিরিক্ত Wi-Fi নেটওয়ার্ক সেট আপ করুন। এটি আপনার ওয়াই-ফাই রাউটারে 'অতিথি' নেটওয়ার্ক হিসাবে পরিচিত হতে পারে। যদি আপনার IoT ডিভাইসগুলির মধ্যে একে অপরের সাথে যোগাযোগের প্রয়োজন না হয়, তাহলে 'ক্লায়েন্ট আইসোলেশন' বৈশিষ্ট্যটি সক্ষম করুন। আপনার IoT ডিভাইসগুলিকে আপনার সংবেদনশীল ডেটা থেকে আলাদা রাখলে নিশ্চিত হয় যে IoT ডিভাইসের সাথে আপস করলে আপনার অন্যান্য ডিভাইস বা ডেটাতে অ্যাক্সেস পাওয়া যাবে না।

5. **অপ্রয়োজনীয় ডিভাইস বৈশিষ্ট্যগুলি কি বন্ধ করা আছে?** যদি আপনার ডিভাইসে অবাঞ্ছিত বা অপ্রয়োজনীয় বৈশিষ্ট্য থাকে (যেমন ক্যামেরা বা মাইক্রোফোন), তাহলে সম্ভব হলে এগুলি নিষ্ক্রিয় করা উচিত।

অতিরিক্ত চেষ্টা করুন

এমন একটি কনফিগারেশন সেটিং খুঁজুন যেখানে স্থানীয় LAN বা WAN/ইন্টারনেট থেকে ডিভাইসের ওয়েব অ্যাডমিনিস্ট্রেশন ইন্টারফেসে রিমোট অ্যাক্সেস সক্ষম করার কথা উল্লেখ করা আছে। যদি আপনার নিজে রিমোট অ্যাক্সেসের প্রয়োজন না থাকে, তাহলে ডিভাইসটি শুধু লোকাল LAN-এ সেট করা আছে কি না তা নিশ্চিত করুন।

একটি IoT ডিভাইস রক্ষণাবেক্ষণ করা

আপনার IoT ডিভাইসটি সেট আপ এবং ব্যবহারের পরে কিছু গুরুত্বপূর্ণ বিষয় মনে রাখা উচিত। এর মধ্যে রয়েছে:

1. **আপনার ডিভাইসগুলি নিয়মিত রিবুট করুন।** IoT ডিভাইসটি ধীরগতির বা অকার্যকর হয়ে গেলে ভাইরাস উপস্থিত থাকতে পারে। বেশিরভাগ ম্যালওয়্যার মেমোরিতে সংরক্ষিত থাকে এবং ডিভাইস রিবুট করে, অর্থাৎ ডিভাইসটি বন্ধ এবং চালু করে সহজেই অপসারণ করা যায়। রিবুট করার পরেও যদি ডিভাইসটি ধীর গতিতে চলতে থাকে বা অকার্যকর হয়ে পড়ে, তাহলে ফ্যাক্টরি রিসেট করার চেষ্টা করুন, তবে মনে রাখবেন এতে আপনার সমস্ত ব্যবহারকারীর ডেটা এবং ব্যক্তিগত সেটিংস মুছে যেতে পারে।

2. **নিয়মিত আপডেট প্রয়োগ করুন।** কিছু কিছু ডিভাইস স্বয়ংক্রিয়ভাবে আপডেট প্রয়োগ করে। যেসব ডিভাইস স্বয়ংক্রিয়ভাবে আপডেট প্রয়োগ করে না, সেগুলর ক্ষেত্রে নিয়মিতভাবে প্রস্তুতকারকের সঙ্গে চেক করতে হবে এবং নতুন আপডেট এলে তা প্রয়োগ করতে হবে। যখন আপনার ডিভাইসে আপডেট আর পাওয়া না যায়, তখন এমন একটি নতুন ডিভাইসে আপগ্রেড করার কথা বিবেচনা করুন যেখানে আপডেট পাওয়া যায়। যেসব ডিভাইসের নিরাপত্তা আপডেটে অ্যাক্সেস নেই, সেগুলি নতুন দুর্বলতা আবিষ্কৃত হলে সুরক্ষিত থাকবে না এবং এই ডিভাইসগুলি আপনার নেটওয়ার্ক, আপনার গোপনীয়তা এবং আপনার ডেটার জন্য ঝুঁকিপূর্ণ হতে পারে।

3. **আপনার ডিভাইসটি ব্যবহার না করার সময় বন্ধ করে দিন।** অব্যবহৃত এবং নজরদারিবিহীন ডিভাইসগুলিকে দীর্ঘ সময় ধরে আপনার ওয়াই-ফাই নেটওয়ার্কের সাথে সংযুক্ত রেখে দিলে আপনার ডিভাইসগুলিতে আক্রমণের সম্ভাবনা বেড়ে যেতে পারে। এই কাজটি স্বয়ংক্রিয়ভাবে সম্পন্ন করার একটি উপায় হলো পাওয়ার আউটলেট টাইমার ব্যবহার করা, যাতে শুধু নির্দিষ্ট সময়েই ডিভাইসটি বিদ্যুৎ পায়।

4. **আপনার মাসিক ইন্টারনেট ব্যবহার বা বিল উল্লেখযোগ্যভাবে বৃদ্ধির দিকে লক্ষ্য রাখুন।** ইন্টারনেট ব্যবহার বা বিলিং চার্জ উল্লেখযোগ্যভাবে বৃদ্ধি পেলে বোঝা যেতে পারে যে আপনার ডিভাইসটি ক্ষতিগ্রস্ত হয়েছে। যদি না আপনার ব্যবসার আইটি বিভাগ এটি তদন্ত করতে চায়, তাহলে ফ্যাক্টরি রিসেট প্রয়োগ করা উচিত (তবে মনে রাখবেন এটি আপনার সমস্ত ব্যবহারকারীর ডেটা এবং ব্যক্তিগত সেটিংস মুছে ফেলতে পারে)। এরপর অবশ্যই পাসওয়ার্ড পরিবর্তন করতে হবে

ফেলে দেয়া একটি IoT ডিভাইস

কোনও ডিভাইস বাতিল করার সময় (এটি ফেলে দেওয়া বা বিক্রি করে দেয়ার মাধ্যমে) অন্যদের কাছে আপনার ব্যক্তিগত তথ্য বা ডেটা সহজেই পৌঁছে যেতে পারে।
এটি প্রতিরোধের উপায়গুলির মধ্যে রয়েছে:

1. **সমস্ত ডেটা এবং ব্যক্তিগত তথ্য মুছে ফেলুন।** ডিভাইস এবং সংশ্লিষ্ট অ্যাপ্লিকেশন উভয় থেকে আপনার ডেটা এবং ব্যক্তিগত তথ্য কীভাবে মুছে ফেলা যায় তার জন্য প্রস্তুতকারকের উচিত একটি পদ্ধতি প্রদান করা। আপনার ব্যক্তিগত তথ্য মুছে ফেললে নিশ্চিত করা যায় যে ডিভাইসটি বাতিল করার পর কেউই সেই তথ্যের অ্যাক্সেস পাবে না। IoT ডিভাইস ছাড়া যদি আপনার অনলাইন অ্যাকাউন্টের আর প্রয়োজন না হয়, তাহলে তা মুছে ফেলুন।

2. **ডিভাইসটির ফ্যাক্টরি রিসেট করুন।** ফ্যাক্টরি রিসেট স্থানীয় স্টোরেজে রাখা ডেটা মুছে ফেলার জন্য এবং পাসওয়ার্ড, ব্যবহারকারীর নাম এবং সেটিংস ডিফল্ট অবস্থায় ফিরিয়ে আনার জন্য ডিজাইন করা হয়েছে। ফ্যাক্টরি রিসেট কীভাবে করতে হয় সে সম্পর্কে তথ্যের জন্য ডিভাইসের ব্যবহারকারী ম্যানুয়াল বা প্রস্তুতকারকের ওয়েবসাইট দেখুন।

3. **মোবাইল ফোন এবং অন্যান্য ডিভাইস থেকে ডিভাইসটি বিচ্ছিন্ন করুন।** আপনার অন্যান্য ডিভাইস, নেটওয়ার্ক বা অনলাইন অ্যাকাউন্টগুলিতে এখনও অ্যাক্সেস আছে এমন কোনও ডিভাইস বাতিল করে দিলে অন্যরা অ্যাক্সেস পেতে পারে। আপনি যে ডিভাইসটি বাতিল করছেন, সেটার সঙ্গে যুক্ত অন্য ডিভাইসগুলোর পেয়ারিং বাতিল করা হয়েছে কি না, সেটা অবশ্যই চেক করুন। মোবাইল অ্যাপ্লিকেশনে প্রদত্ত যে কোনও অনুমতি যা আর প্রয়োজন নেই তা সরিয়ে ফেলুন।

4. **ডিভাইসের সাথে সংযুক্ত যেকোনো অপসারণযোগ্য মিডিয়া (যেমন USB ফ্ল্যাশ ড্রাইভ, মেমোরি কার্ড ইত্যাদি) সরিয়ে ফেলুন।** অপসারণযোগ্য মিডিয়াতে এমন ব্যক্তিগত তথ্য থাকতে পারে যা ফ্যাক্টরি রিসেটে মুছে যায় না এবং তা ডিভাইস থেকে আলাদাভাবে অপসারণ, ধ্বংস এবং বাতিল করা উচিত।

সাহায্য

জরুরি সহায়তার জন্য অস্ট্রেলিয়ান সিগন্যালস ডিরেক্টরেটের অস্ট্রেলিয়ান সাইবার সিকিউরিটি সেন্টারের সাথে asd.assist@defence.gov.au ঠিকানায় ইমেল করে যোগাযোগ করুন অথবা **1300 CYBER1 (1300 292 371)** নম্বরে ২৪/৭ হটলাইনে কল করুন।

সাইবার অপরাধের অভিযোগ www.cyber.gov.au/report ঠিকানায় রিপোর্টসাইবারকে জানান।

যদি আপনার পরিচয় চুরি হয়ে থাকে, তাহলে IDCARE-এর ওয়েবসাইট www.idcare.orgএর মাধ্যমে তাদের সাথে যোগাযোগ করুন।

আপনার এবং আপনার পরিবারের পরামর্শের জন্য www.cyber.gov.au দেখুন। সাম্প্রতিক অনলাইন হুমকি সম্পর্কে বিনামূল্যে ACSC সতর্কতা পরিষেবার জন্য সাইন আপ করুন।

আসুন অস্ট্রেলিয়াকে অনলাইনে সংযোগ স্থাপনের জন্য সবচেয়ে নিরাপদ স্থান করে তুলি।

সাইবার নিরাপত্তা পরামর্শের জন্য, www.cyber.gov.au দেখুন।

দাবিত্যাগ

এই নির্দেশিকার তথ্য সাধারণ প্রকৃতির এবং কোনও বিশেষ পরিস্থিতিতে বা জরুরি পরিস্থিতিতে আইনি পরামর্শ হিসেবে বিবেচনা করা উচিত নয় অথবা সহায়তার জন্য এর উপর নির্ভর করা উচিত নয়। যেকোনো গুরুত্বপূর্ণ বিষয়ে, আপনার নিজের পরিস্থিতির ভিত্তিতে উপযুক্ত স্বাধীন পেশাদার পরামর্শ নেওয়া উচিত।

এই নির্দেশিকায় থাকা তথ্যের উপর নির্ভর করার কারণে যে কোনও ক্ষয় ক্ষতি বা ব্যয়ের জন্য কমনওয়েলথ কোনও দায়বদ্ধতা বা দায় স্বীকার করে না।

আরও তথ্যের জন্য, অথবা সাইবার নিরাপত্তা সংক্রান্ত কোনও ঘটনার প্রতিবেদন করতে, আমাদের সাথে যোগাযোগ করুন:

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

এই নম্বরটি শুধুমাত্র অস্ট্রেলিয়ার মধ্যে ব্যবহারের জন্য উপলব্ধ।

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre