

# आईओटी डिवाइस सुरक्षा

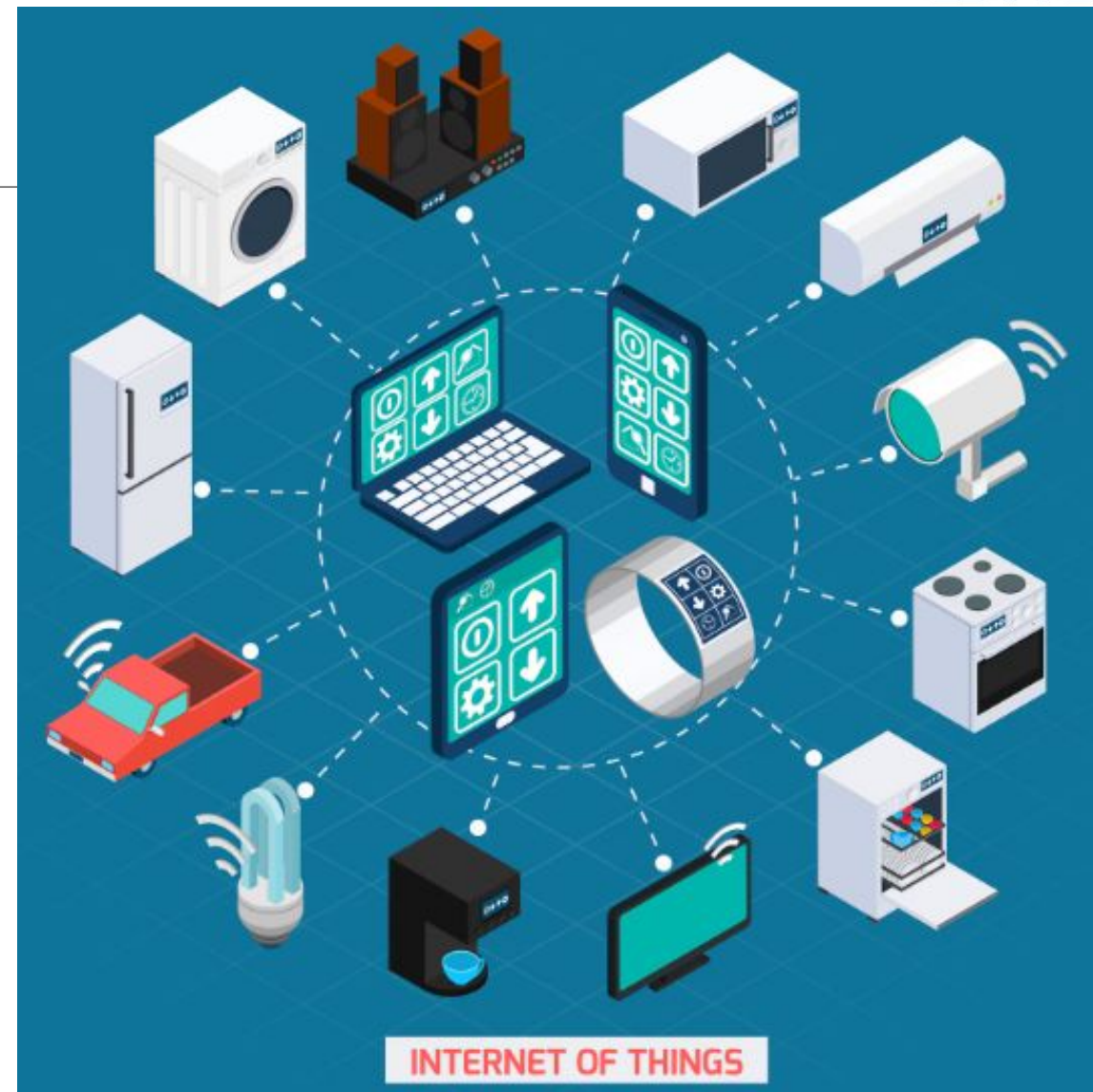
विश्वास आईओटी की नई मुद्रा है

---

द्वारा **सुमेरा फ़ारूक़**  
प्रोजेक्ट इंजीनियर  
सी-डैक मोहाली

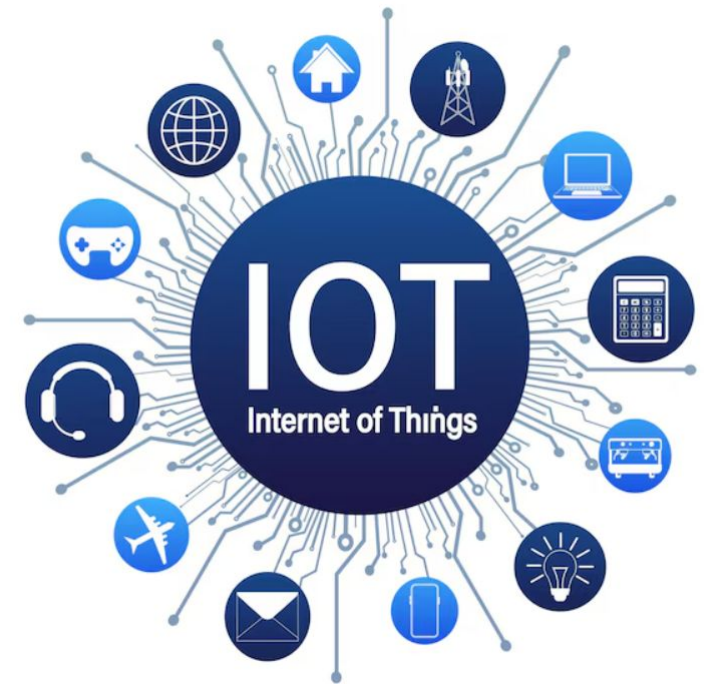
# अवलोकन

- IoT सुरक्षा का परिचय
- प्रमुख IoT सुरक्षा चुनौतियाँ
- वास्तविक जीवन का उदाहरण
- सामान्य IoT हमले
- IoT उपकरणों के लिए सुरक्षा उपाय



# आईओटी का क्या अर्थ है? किसी भी समय, कहीं भी, किसी भी चीज़ में कनेक्टिविटी।

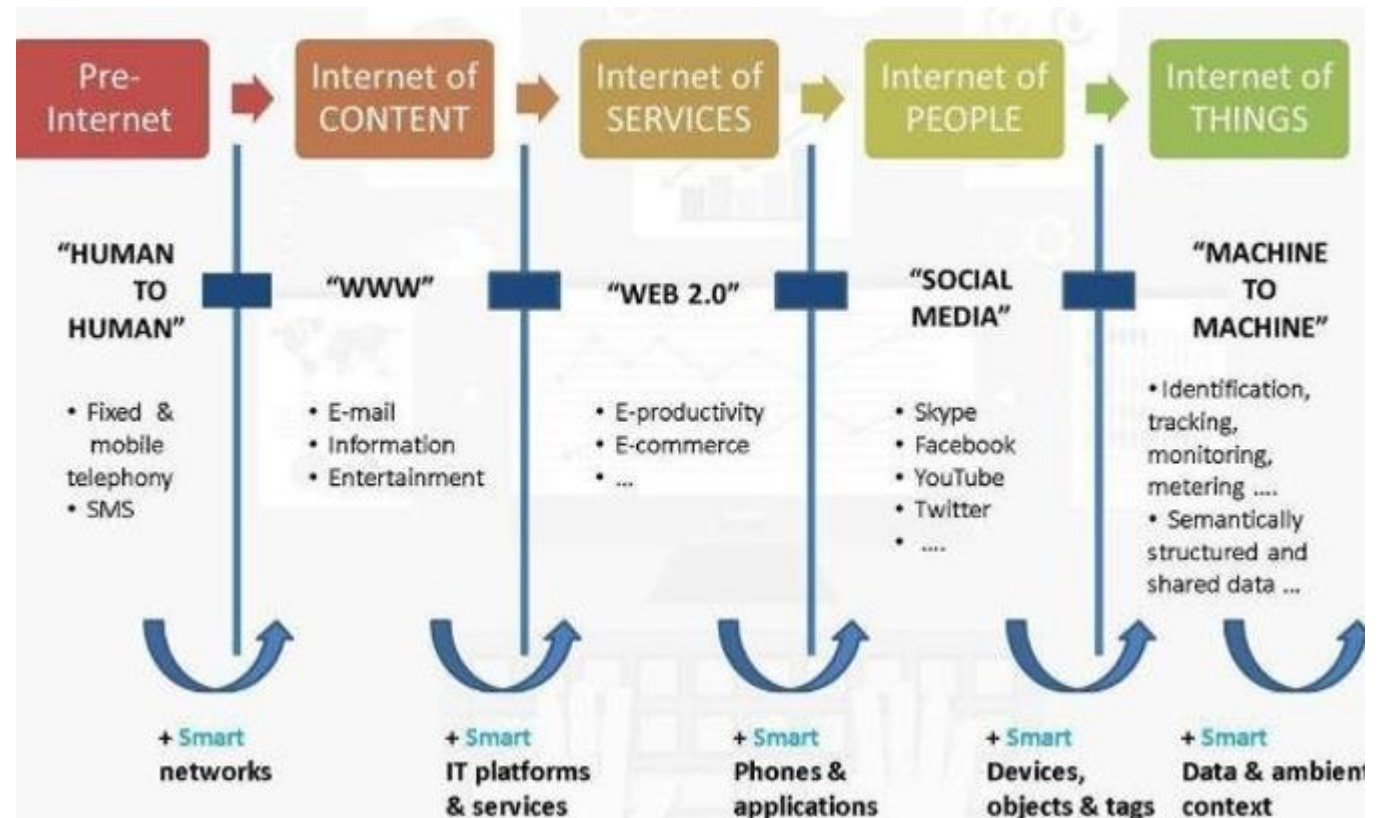
- ❖ The **इंटरनेट ऑफ थिंग्स (IoT)** क्लाउड में साधारण वस्तुओं को अन्य वस्तुओं और अनुप्रयोगों से जोड़ता है, जिससे वे बुद्धिमान और इंटरैक्टिव बन जाते हैं। ऐसे "स्मार्ट" उपकरण हमारे जीवन को समृद्ध और स्वस्थ बनाते हैं और सीमित संसाधनों के अधिकतम उपयोग में मदद करते हैं।
- ❖ "चीज़" कोई भी भौतिक इकाई हो सकती है जिसे एक विशिष्ट पहचान दी गई हो और नेटवर्क पर अन्य उपकरणों के साथ संचार या अंतःक्रिया करने की क्षमता दी गई हो। **उदाहरण** "चीजों" में वाहन, उपकरण, औद्योगिक मशीनें, पहनने योग्य उपकरण आदि शामिल हैं।
- ❖ **सेंसर** में स्थापित **भौतिक वस्तुओं** इसमें तापमान सेंसर, गति सेंसर, प्रकाश सेंसर, आर्द्रता सेंसर, जीपीएस सेंसर आदि शामिल हैं।



# आईओटी का विकास और क्रांति

इंटरनेट का विकास लोगों को जोड़ने से लेकर → सामग्री साझा करने → सेवाओं को सक्षम करने → लोगों को सामाजिक रूप से जोड़ने → और अब मशीनों को सीधे जोड़ने तक हुआ है, जो कि IoT का सार है।

आईओटी का विकास



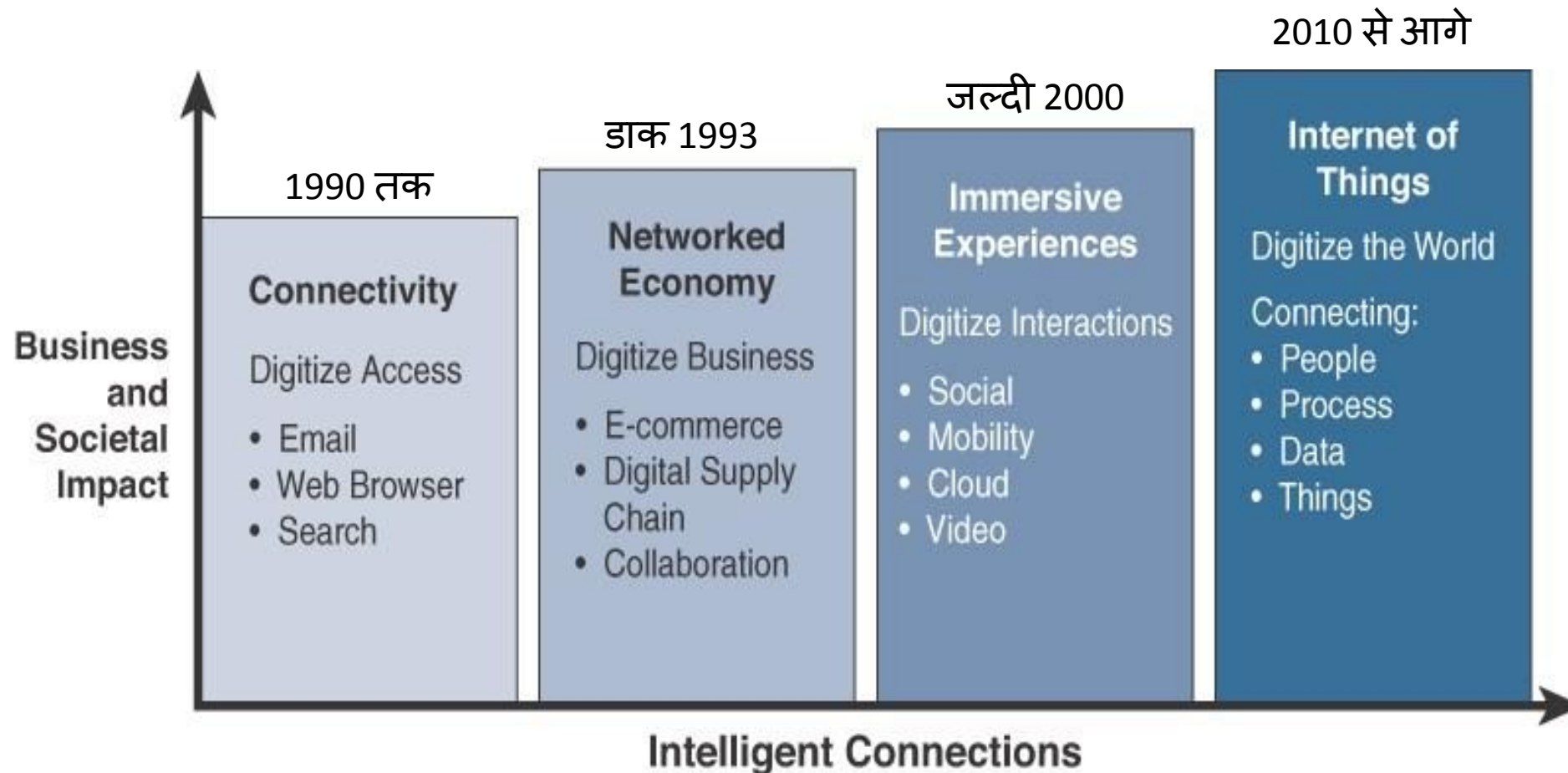
# "इंटरनेट ऑफ थिंग्स" का निर्माण

---

- केविन एश्टन द्वारा 1999 में प्रॉक्टर एंड गैम्बल में अपने कार्यकाल के दौरान किया गया ।
- एश्टन का काम आपूर्ति श्रृंखला दक्षता में सुधार करना था।
- यह शब्द इंटरनेट से वस्तुओं को जोड़ने की क्रांतिकारी अवधारणा का वर्णन करने के लिए उभरा।
- यह शब्द अपने प्रारंभिक संदर्भ से आगे बढ़ गया तथा प्रौद्योगिकी और उद्योगों को नया रूप देने लगा।



# संक्षिप्त इतिहास



# IIOT के चार प्रमुख घटक

## 1. संवेदन (उपकरण और सेंसर)

### IIOT की “आँखें और कान”

IIOT डिवाइस भौतिक वातावरण (तापमान, गति, स्थान, हृदय गति, आर्द्रता, आदि) से डेटा एकत्र करने के लिए सेंसर का उपयोग करते हैं।



**Sensors**  
Collecting data



**Connectivity**  
Sending data to cloud



**Data Processing**  
Making data useful



**User Interface**  
Delivering information to user

## 2. नेटवर्क कनेक्टिविटी

एकत्रित डेटा को अन्य उपकरणों, सर्वरों या क्लाउड पर प्रेषित किया जाना चाहिए

**कम दूरी**

**लंबी दूरी/कम शक्ति**

## 3. डेटा प्रोसेसिंग (एज/क्लाउड कंप्यूटिंग)

एक बार डेटा प्रेषित हो जाने पर, उसका विश्लेषण और प्रसंस्करण किया जाना चाहिए।

**डिवाइस पर ही (एज कंप्यूटिंग) → तेज़, कम बैंडविड्थ.**

**बादल में → शक्तिशाली विश्लेषण, बड़ा डेटा, एआई/एमएल।**

## 4. उपयोगकर्ता इंटरफ़ेस (एप्लिकेशन लेयर)

अंतिम चरण वह है जहां अंतर्दृष्टि को मनुष्यों के लिए उपयोगी बनाया जाता है।

**मोबाइल एप्लिकेशन** (अपने स्मार्ट एसी को नियंत्रित करने के लिए)।

**डैशबोर्ड** (फैक्ट्री मशीन की स्थिति दर्शाते हुए)

**स्वचालित अलर्ट/सूचनाएं.**



# आईओटी के लाभ

## 1. स्वचालन और नियंत्रण

ये उपकरण न्यूनतम मानवीय हस्तक्षेप के साथ स्वचालित रूप से काम कर सकते हैं।

## 2. दक्षता और उत्पादकता

दोहराए जाने वाले कार्यों को स्वचालित करके समय और संसाधनों की बचत होती है।

## 3. डेटा संग्रह और अंतर्दृष्टि

निरंतर निगरानी निर्णय लेने के लिए मूल्यवान डेटा प्रदान करती है।

## 4. लागत बचत

ऊर्जा-कुशल प्रणालियाँ उपयोगिता बिल कम करती हैं।

## 5. बेहतर सुरक्षा

IoT-सक्षम कैमरे, अलार्म और सेंसर बेहतर सुरक्षा सुनिश्चित करते हैं।

## 6. जीवन की बेहतर गुणवत्ता

स्मार्ट घर, स्मार्ट स्वास्थ्य सेवा, स्मार्ट परिवहन → अधिक सुविधा और आराम।

# आईओटी के नुकसान



## 1. सुरक्षा जोखिम

अरबों कनेक्टेड डिवाइस हमले की संभावना को बढ़ा देते हैं।

## 2. गोपनीयता संबंधी चिंताएँ

IoT डिवाइस संवेदनशील व्यक्तिगत डेटा एकत्र करते हैं।

## 3. जटिलता और अनुकूलता

विभिन्न डिवाइस, नेटवर्क और प्रोटोकॉल एक साथ सुचारू रूप से काम नहीं कर सकते हैं।

## 4. उच्च प्रारंभिक लागत

स्मार्ट डिवाइस और IoT अवसंरचना को स्थापित करना महंगा हो सकता है।

## 5. डेटा अधिभार

भारी मात्रा में डेटा के लिए मजबूत प्रसंस्करण और भंडारण की आवश्यकता होती है।

## 6. इंटरनेट पर निर्भरता

यदि नेटवर्क बंद हो जाए तो डिवाइस ठीक से काम नहीं कर पाएंगे।

# आधुनिक अनुप्रयोग

---

- स्मार्ट ग्रिड और ऊर्जा बचत
- स्मार्ट शहर
- स्मार्ट घर/होम ऑटोमेशन
- स्वास्थ्य देखभाल
- भूकंप का पता लगाना
- विकिरण का पता लगाना/खतरनाक गैस का पता लगाना
- स्मार्टफोन का पता लगाना
- जल प्रवाह निगरानी
- सुरक्षा
- यातायात निगरानी
- पहनने योग्य वस्तुएं
- स्मार्ट डोर लॉक सुरक्षा प्रणाली
- रोबोट और ड्रोन
- स्वास्थ्य सेवा और अस्पताल, टेलीमेडिसिन अनुप्रयोग
- बायोचिप ट्रांसपॉंडर (खेतों में पशुओं के लिए)
- हृदय निगरानी प्रत्यारोपण (उदाहरण पेसमेकर)
- कृषि
- उद्योग



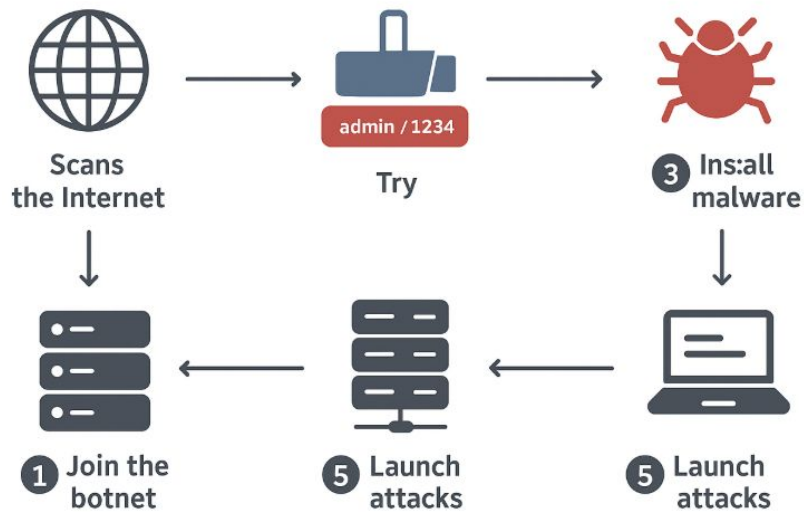
# अब यह महत्वपूर्ण क्यों है?

- IoT उपकरणों की संख्या में भारी वृद्धि हो रही है (वैश्विक स्तर पर अरबों में) → **आक्रमण की सतह बहुत बड़ी है.**
- कई IoT डिवाइस तैनात हैं **खराब नियंत्रण**, दूरस्थ, या बिना निगरानी वाली सेटिंग्स (जैसे क्षेत्र में सेंसर, उपभोक्ता घर)।
- IoT उपकरणों में अक्सर सीमित कंप्यूटिंग, मेमोरी, पावर और लागत संबंधी बाधाएँ होती हैं, जिससे मज़बूत सुरक्षा सुनिश्चित करना मुश्किल हो जाता है। चूँकि IoT उपकरण अक्सर महत्वपूर्ण प्रणालियों (जैसे औद्योगिक, स्वास्थ्य सेवा, उपयोगिताएँ) से जुड़े होते हैं, इसलिए उनके साथ छेड़छाड़ से गंभीर भौतिक या सामाजिक प्रभाव पड़ सकता है (सिर्फ़ डेटा उल्लंघन ही नहीं)।
- हमलावर तेजी से IoT उपकरणों का उपयोग नेटवर्क में प्रवेश बिंदु के रूप में या बड़े हमलों के लिए बिल्डिंग ब्लॉक (जैसे बॉटनेट) के रूप में कर रहे हैं।

इसलिए IoT को सुरक्षित करना वैकल्पिक नहीं है - इसे पूरे जीवनचक्र में अंतर्निहित किया जाना चाहिए।

# मिराई बॉटनेट

## HOW THE MIRAI BOTNET WORKED



मिराई ने इंटरनेट से जुड़े उपकरणों पर कमजोर/डिफॉल्ट पासवर्ड और खुली सेवाओं का फायदा उठाकर संक्रमित उपकरणों की एक विशाल सेना तैयार की और उनका उपयोग वेबसाइटों पर हमला करने के लिए किया - इसका समाधान बुनियादी स्वच्छता है: डिफॉल्ट पासवर्ड बदलें, फ़र्मवेयर अपडेट करें, और IoT उपकरणों को अलग करें।

# MIRAI बॉटनेट कैसे काम करता है

---

**इंटरनेट स्कैन करें:**मिराई ने उन उपकरणों की तलाश की जो इंटरनेट से जुड़े थे और सामान्य पोर्ट (जैसे टेलनेट) पर सुन रहे थे।

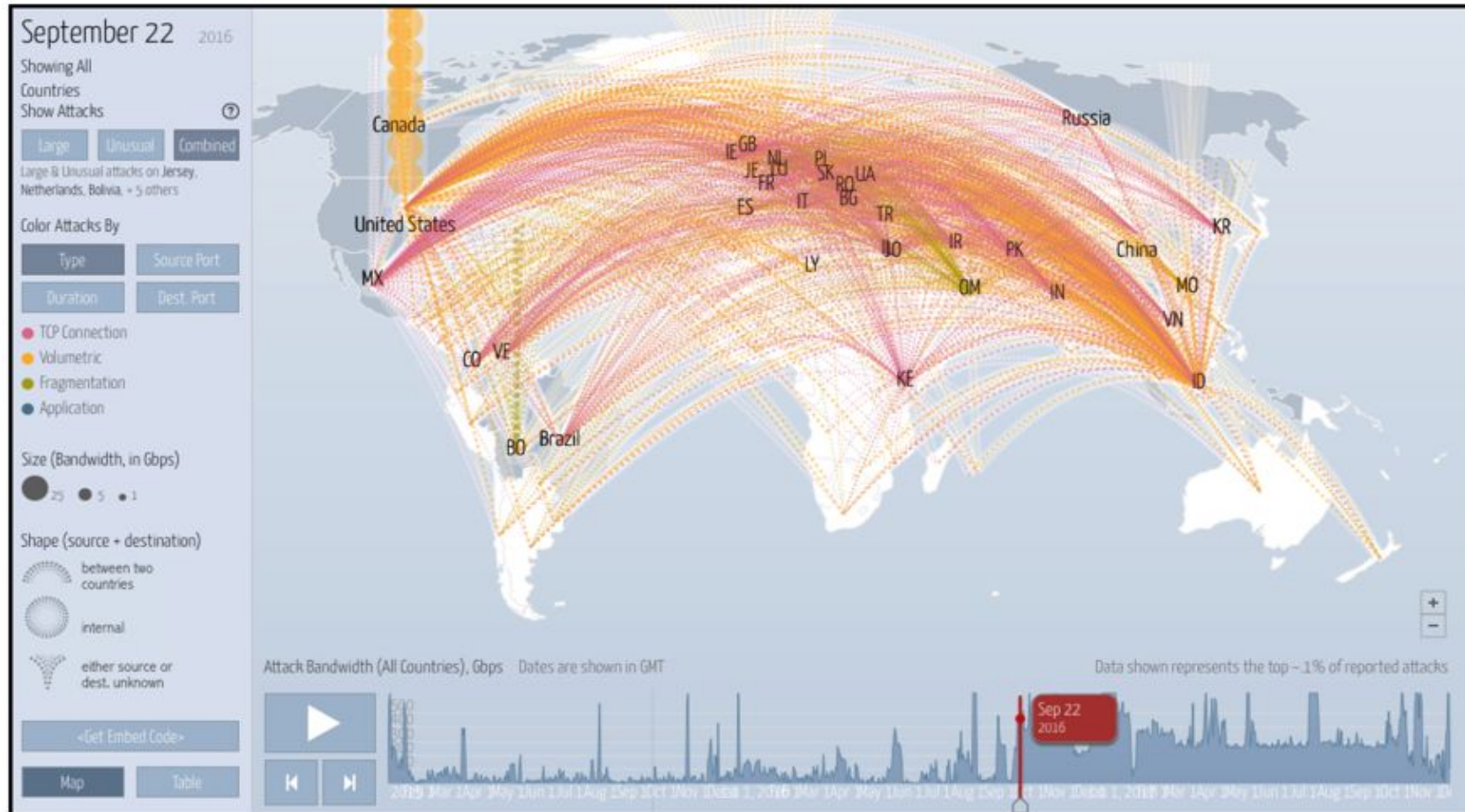
**डिफ़ॉल्ट पासवर्ड आजमाएँ:**प्रत्येक डिवाइस के लिए, मिराई ने सामान्य उपयोगकर्ता नाम और पासवर्ड (जैसे admin/admin) की एक लंबी सूची का उपयोग किया, जिसे निर्माता कभी-कभी डिफ़ॉल्ट के रूप में भेजते हैं।

**लॉग इन करें और स्वयं को स्थापित करें:**यदि डिवाइस ने इनमें से किसी उपयोगकर्ता नाम/पासवर्ड को स्वीकार कर लिया, तो मिराई ने लॉग इन किया, मैलवेयर डाउनलोड किया और उसे डिवाइस पर इंस्टॉल कर दिया।

**बॉटनेट में शामिल हों:**संक्रमित डिवाइस हमलावर के नियंत्रण सर्वर से जुड़ गया और आदेशों की प्रतीक्षा करने लगा।

**हमले शुरू करें:**आदेश मिलने पर, हमलावर ने उन सभी संक्रमित उपकरणों से एक चुने हुए लक्ष्य पर भारी मात्रा में ट्रैफिक भेज दिया - यह एक वितरित सेवा निषेध (DDoS) हमला है, जो किसी वेबसाइट या सेवा को अनुपयोगी बना सकता है।

# हमले के दौरान लिया गया वास्तविक समय का स्क्रीनशॉट



# चुनौतियां

## सुरक्षा

IoT उत्पादों और सेवाओं में मजबूत और आजीवन सुरक्षा कैसे सुनिश्चित करें?

## अंतरसंचालनीयता और मानक

IoT उपकरणों के लिए तकनीकी आधार के रूप में खुले, अंतर-संचालनीय और व्यापक रूप से उपलब्ध मानकों का स्वैच्छिक उपयोग अधिक लाभ प्रदान करेगा।



## गोपनीयता

ऐसी रणनीतियाँ विकसित करने की आवश्यकता है जो डेटा संग्रहण और प्रबंधन में पारदर्शिता, निष्पक्षता और उपयोगकर्ता विकल्प को बढ़ावा दें।

## नियामक, कानूनी और अधिकार संबंधी मुद्दे

परिवर्तन की तीव्र दर आईओटी प्रौद्योगिकी, संबद्ध नीति, कानूनी और विनियामक संरचनाओं की अनुकूलन क्षमता से आगे निकल सकती है।

## उभरती अर्थव्यवस्था और विकास के मुद्दे

IoT के लाभों को वास्तव में वैश्विक बनाने के लिए, कम विकसित क्षेत्रों में कार्यान्वयन की विशिष्ट आवश्यकताओं और चुनौतियों का समाधान करना होगा।

# प्रमुख आईओटी सुरक्षा चुनौतियाँ

- 1. विशाल आक्रमण सतह** अरबों IoT डिवाइस (सीसीटीवी कैमरे, पहनने योग्य उपकरण, स्मार्ट मीटर, कारें, आदि) जुड़े हुए हैं।
- 2. कमजोर प्रमाणीकरण और प्राधिकरण** कई IoT डिवाइस अभी भी उपयोग करते हैं **डिफॉल्ट पासवर्ड** (जैसे "admin/1234")। उचित जानकारी का अभाव **बहु-कारक प्रमाणीकरण** इससे डिवाइसों के साथ समझौता करना आसान हो जाता है।
- 3. डेटा गोपनीयता संबंधी चिंताएँ** IoT उपकरण लगातार संवेदनशील डेटा (स्वास्थ्य, स्थान, आवाज़, वीडियो) एकत्र करते रहते हैं। अनधिकृत पहुँच या दुरुपयोग से पहचान की चोरी, निगरानी या प्रोफाइलिंग हो सकती है।
- 4. असुरक्षित नेटवर्क संचार** कई डिवाइस डेटा संचारित करते हैं **बिना एन्क्रिप्शन के** (सादा पाठ)। इससे हमलावरों के लिए यह काम आसान हो जाता है **मैन-इन-द-मिडिल (MITM)** हमले।
- 5. सीमित डिवाइस संसाधन** IoT उपकरणों में **कम प्रसंस्करण शक्ति, मेमोरी और बैटरी** उन्नत सुरक्षा सुविधाएँ (जैसे फ़ायरवॉल, घुसपैठ का पता लगाना, या मजबूत एन्क्रिप्शन) चलाना मुश्किल है।

# जारी ...

---

## 6. असंबद्ध कमजोरियाँ

निर्माता अक्सर समय पर उत्पाद उपलब्ध नहीं कराते हैं। **सुरक्षा अद्यतन** या फ़र्मवेयर पैच। हैकर्स पुराने सिस्टम का फायदा उठाते हैं (उदाहरण के लिए, मिराई बॉटनेट ने असुरक्षित कैमरों का फायदा उठाया)।

## 7. भौतिक सुरक्षा जोखिम

कई IoT उपकरण सार्वजनिक क्षेत्रों (ट्रैफिक सेंसर, एटीएम, कैमरे) में लगाए जाते हैं। हमलावर डेटा निकालने या मैलवेयर इंस्टॉल करने के लिए उपकरणों के साथ भौतिक रूप से छेड़छाड़ कर सकते हैं।

## 8. आपूर्ति श्रृंखला जोखिम

उपकरण के पुर्जे अलग-अलग विक्रेताओं से लिए जाते हैं। डिवाइस के बिकने से पहले ही उसमें दुर्भावनापूर्ण चिप्स, बैकडोर या खराब फ़र्मवेयर डाले जा सकते हैं।

## 9. सुरक्षा की मापनीयता

कुछ उपकरणों के लिए काम करने वाले सुरक्षा तंत्र लाखों उपकरणों तक पहुँचने पर विफल हो सकते हैं। बड़े पैमाने पर क्रेडेंशियल, अपडेट और निगरानी का प्रबंधन एक बड़ी चुनौती है।

# सामान्य आईओटी हमले

## बॉटनेट / DDoS हमले

- हमलावर कई IoT उपकरणों से समझौता करते हैं और उनका उपयोग लक्ष्य पर भारी ट्रैफिक उत्पन्न करने के लिए करते हैं, जिससे वह लक्ष्य अभिभूत हो जाता है (वितरित सेवा अस्वीकार)। **मिराई** बॉटनेट इसका एक उत्कृष्ट उदाहरण है: यह डिफॉल्ट क्रेडेंशियल्स (टेलनेट) वाले उपकरणों को स्कैन करता है और उन्हें DDoS के लिए तैयार करता है।

## मैन-इन-द-मिडिल (MITM) / छिपकर सुनना / निगरानी

- उपकरणों, गेटवे और क्लाउड के बीच संचार को रोका जा सकता है; हमलावर इसे निष्क्रिय रूप से मॉनिटर कर सकते हैं या ट्रांसमिशन के दौरान डेटा बदल सकते हैं। अगर प्रोटोकॉल एन्क्रिप्टेड या ठीक से प्रमाणीकृत नहीं हैं, तो वे कमांड इंजेक्ट करके या डेटा को भ्रष्ट करके हमला कर सकते हैं।

## स्पूफिंग / पहचान / रीप्ले हमले

- एक हमलावर किसी वैध डिवाइस, सेंसर या गेटवे का भेष धारण कर सकता है। रीप्ले हमले सिस्टम को धोखा देने के लिए पहले से प्राप्त वैध संदेशों (जैसे कमांड) का पुनः उपयोग करते हैं।

## फ़र्मवेयर / सॉफ़्टवेयर शोषण / कोड इंजेक्शन

- फ़र्मवेयर या एप्लिकेशन कोड (बफर ओवरफ्लो, इंजेक्शन पॉइंट) में कमजोरियों का उपयोग हानिकारक कोड चलाने या नियंत्रण हासिल करने के लिए किया जाता है।

## सेंसर / साइड-चैनल हमले

- रहस्यों (जैसे क्रिप्टोग्राफिक कुंजी) का अनुमान लगाने के लिए साइड सूचना (जैसे बिजली की खपत, विद्युत चुम्बकीय उत्सर्जन, समय, थर्मल निशान) का उपयोग करना।

# जारी...

---

## सेवा अस्वीकार (DoS) / संसाधन समाप्ति

- सीमित क्षमता वाले उपकरणों पर अनुरोधों का बोझ डालें या उन्हें लगातार प्रतिक्रिया देने की स्थिति में लाएँ, जिससे बैटरी या सीपीयू की खपत हो। जैमिंग हमले (वायरलेस वातावरण में) संचार को अवरुद्ध या खराब भी कर सकते हैं।

## आपूर्ति श्रृंखला हमले / हार्डवेयर बैकडोर

- निर्माण के दौरान हानिकारक संशोधन या अंतर्निहित बैकडोर, या तैनाती से पहले हानिकारक फ़र्मवेयर का सम्मिलन। हमलावर अपडेट के बुनियादी ढाँचे से भी समझौता कर सकते हैं (उदाहरण के लिए, हानिकारक अपडेट भेजना)।

## डेटा / गोपनीयता हमले

- सेंसर डेटा, व्यक्तिगत जानकारी या नियंत्रण आदेशों तक अनधिकृत पहुँच (या रिसाव)। अखंडता हमले जो अनुप्रयोगों या ऑपरेटरों को गुमराह करने के लिए डेटा में हेरफेर करते हैं।

## रैंसमवेयर / जबरन वसूली के हमले

- अधिक परिष्कृत वातावरण में, हमलावर फिरौती वसूलने के लिए नियंत्रण प्रणालियों (जैसे ओटी/आईओटी संदर्भों में) को एन्क्रिप्ट या लॉक कर सकते हैं। ओटी/आईओटी रैंसमवेयर अधिक प्रचलित हो रहा है, खासकर महत्वपूर्ण बुनियादी ढाँचे को निशाना बनाकर।

# आईओटी सुरक्षा कुंजी अनुशंसा

## IoT Security Key Recommendations



# आईओटी सुरक्षा 6-कुंजी अनुशंसा

## IoT एंडपॉइंट सुरक्षा

सुरक्षित डिवाइस पोर्ट (TCP, UDP, वायरलेस)

अनएन्क्रिप्टेड संचार को ब्लॉक करें

कोड इंजेक्शन और मैलवेयर रोकें

कनेक्टेड डिवाइसों की पूर्ण दृश्यता

## IoT गेटवे सुरक्षा

उपयोग सुरक्षित वेब गेटवे (SWG)

विशेषताएं: ऐप नियंत्रण, HTTPS/SSL निरीक्षण, URL फ़िल्टरिंग

मैलवेयर और अनधिकृत पहुंच रोकें

VPN और निगरानी के साथ सुरक्षित दूरस्थ/क्लाउड कनेक्शन

## क्लाउड API को सुरक्षित करना

API = IoT और क्लाउड के बीच सेतु → सुरक्षित होना चाहिए

प्रमाणीकरण, एन्क्रिप्शन, टोकन, API गेटवे का उपयोग करें

बड़े पैमाने पर डेटा उल्लंघनों को रोकें

उदाहरण: REST API डिवाइस और सर्वर के बीच डेटा स्थानांतरण को सुरक्षित करता है

# IOT सुरक्षा 6-कुंजी अनुशंसा

## सुरक्षित नेटवर्क विकास

तैनात करना फ़ायरवॉल और MFA (बहु-कारक प्रमाणीकरण )

नेटवर्क पर केवल सत्यापित डिवाइसों को अनुमति दें

प्रमाणीकरण कुंजियों की सुरक्षा करें, एंटीवायरस/एंटीमैलवेयर अपडेट करें

नेटवर्क गतिविधि की निरंतर निगरानी

## अद्यतन डेटा एन्क्रिप्शन

एन्क्रिप्ट गतिशील डेटा (डिवाइस ↔ इंटरनेट)

सममित एन्क्रिप्शन → एकल कुंजी

असममित एन्क्रिप्शन → सार्वजनिक + निजी कुंजियाँ (अधिक सुरक्षित)

मजबूत रक्षा छिपकर सुनने और रीप्ले हमलों के खिलाफ

## संरक्षित डेटा संग्रहण

संवेदनशील जानकारी सुरक्षित करें (वित्तीय, व्यक्तिगत, बायोमेट्रिक)

अपडेट किए गए एंटीवायरस, एंटीमैलवेयर और स्कैनिंग टूल

वास्तविक समय खतरे की निगरानी + अलर्ट

दृश्यता और नियंत्रण के लिए केंद्रीकृत कंसोल

# IoT उभरते रूझान

---

**5G-संचालित IoT**– स्मार्ट शहरों, स्वायत्त वाहनों और औद्योगिक IoT को सक्षम करने वाली तेज़, कम विलंबता वाली कनेक्टिविटी।

**एआई + आईओटी (एआईओटी)**– पूर्वानुमानात्मक विश्लेषण, विसंगति का पता लगाने और स्वचालन के साथ बेहतर निर्णय लेना।

**एज कंप्यूटिंग** - वास्तविक समय की जानकारी और कम क्लाउड निर्भरता के लिए डिवाइस के करीब डेटा संसाधित किया जाता है।

**IoT सुरक्षा संवर्द्धन** – मजबूत एंडपॉइंट सुरक्षा, ब्लॉकचेन-आधारित प्रमाणीकरण और शून्य-विश्वास मॉडल।

**पहनने योग्य और स्वास्थ्य सेवा IoT**- स्मार्ट स्वास्थ्य निगरानी, दूरस्थ रोगी देखभाल और कल्याण ट्रैकिंग।

**टिकाऊ IoT**– स्मार्ट ग्रिड, कृषि और जलवायु निगरानी के लिए ऊर्जा-कुशल उपकरण और IoT समाधान।

# आईओटी भविष्य की दिशाएँ

---

**हाइपरकनेक्टेड स्मार्ट सिटीज़** – यातायात, उपयोगिताओं, अपशिष्ट और सुरक्षा प्रणालियों में IoT का निर्बाध एकीकरण।

**स्वायत्त IoT प्रणालियाँ** – AI/ML द्वारा संचालित स्व-शिक्षण IoT नेटवर्क।

**क्वांटम IoT (क्यूआईओटी)** – मजबूत IoT सुरक्षा और तीव्र डेटा विश्लेषण के लिए क्वांटम कंप्यूटिंग का लाभ उठाना।

**अंतरसंचालनीयता मानक** - विभिन्न उद्योगों में डिवाइस अनुकूलता के लिए सार्वभौमिक IoT प्रोटोकॉल।

**मानव-केंद्रित IoT** – उपयोगकर्ता की गोपनीयता, पहुंच और नैतिक IoT उपयोग पर ध्यान केंद्रित करें।

# सामान्य IoT उपयोगकर्ताओं के लिए सुरक्षा उपाय

## डिफॉल्ट पासवर्ड बदलें

अधिकांश IoT डिवाइस कमजोर डिफॉल्ट पासवर्ड (जैसे "admin123") के साथ आते हैं।

**क्या करें:** प्रत्येक डिवाइस के लिए हमेशा एक मजबूत, अद्वितीय पासवर्ड सेट करें।

**उदाहरण :** यदि कोई व्यक्ति डिफॉल्ट पासवर्ड का उपयोग करके आपके वाई-फाई कैमरे को हैक करता है, तो वह आपके घर पर जासूसी कर सकता है।

## डिवाइस को अपडेट रखें

निर्माता कमजोरियों को ठीक करने के लिए सुरक्षा अद्यतन जारी करते हैं।

**क्या करें:** स्वचालित अपडेट चालू करें या नियमित रूप से जांच करें।

**उदाहरण :** पुराने स्मार्ट टीवी आपके वाई-फाई के माध्यम से फैलने वाले मैलवेयर से संक्रमित हो सकते हैं।

## सुरक्षित वाई-फाई का उपयोग करें

IoT डिवाइस आपके घर के वाई-फाई के माध्यम से कनेक्ट होते हैं, इसलिए यदि वाई-फाई कमजोर है, तो सभी डिवाइस खतरे में हैं।

**क्या करें:** उपयोग WPA3 या WPA2 एन्क्रिप्शन, एक मजबूत वाई-फाई पासवर्ड सेट करें, और सार्वजनिक वाई-फाई से बचें।

**उदाहरण :** यदि आपका वाई-फाई खुला है तो आपके पड़ोस का कोई हैकर उससे कनेक्ट हो सकता है और आपके स्मार्ट डोर लॉक को नियंत्रित कर सकता है।

# सुरक्षा उपायजारी ...

## अलग IoT नेटवर्क

कई राउटर "अतिथि नेटवर्क" की अनुमति देते हैं। IoT उपकरणों के लिए इसका उपयोग करें।

**क्या करें** अपने लैपटॉप/फोन को एक नेटवर्क पर रखें और IoT डिवाइस को दूसरे पर।

**उदाहरण :** यदि कोई स्मार्ट बल्ब हैक हो जाता है, तो इसका लैपटॉप पर आपके बैंकिंग ऐप पर कोई प्रभाव नहीं पड़ेगा।

## उपयोग में न होने पर बंद कर दें

निष्क्रिय डिवाइस अभी भी डेटा का उपभोग करते हैं और हैक किए जा सकते हैं।

**क्या करें** जब आवश्यकता न हो तो IoT डिवाइस (जैसे स्मार्ट प्लग, कैमरा) को बंद कर दें।

**उदाहरण :** 24/7 चालू रहने वाले बेबी मॉनिटर को हमलावर आपके घर के अंदर सुनने के लिए अपहरण कर सकते हैं।

## अनुमतियों के साथ सावधान रहें

कई IoT ऐप्स अनावश्यक रूप से स्थान, संपर्क या कैमरा एक्सेस मांगते हैं।

**क्या करें:** केवल आवश्यक अनुमतियाँ दें।

**उदाहरण :** माइक्रोफोन एक्सेस मांगने वाला स्मार्ट टॉच ऐप जासूसी कर रहा हो सकता है।

# सुरक्षा उपायजारी ...

## दो-कारक प्रमाणीकरण (2FA) का उपयोग करें

IoT उपकरणों से जुड़े खातों के लिए सुरक्षा की अतिरिक्त परत।

**उदाहरण :** यदि आपका स्मार्ट लॉक ऐप हैक हो जाता है, तो भी हैकर आपके ओटीपी के बिना लॉग इन नहीं कर सकता है।

## सुरक्षा सॉफ़्टवेयर स्थापित करें

IoT को नियंत्रित करने के लिए अपने घर के वाई-फाई या स्मार्टफोन पर एंटीवायरस और फ़ायरवॉल का उपयोग करें।

**उदाहरण :** दुर्भावनापूर्ण ऐप्स को IoT लॉगिन विवरण चुराने से रोकता है।

## जागरूक रहें

हाल के IoT घोटालों (जैसे नकली ऐप्स या हानिकारक फ़र्मवेयर अपडेट) के बारे में जानें।

**उदाहरण :** ऐप स्टोर पर मौजूद नकली एलेक्सा ऐप लापरवाह उपयोगकर्ताओं से लॉगिन विवरण चुरा लेते हैं।

# मुख्य बिंदु: सभी के लिए IoT सुरक्षा

1. डिफ़ॉल्ट पासवर्ड बदलें
  - एक मजबूत, अनोखा पासवर्ड सेट करे
2. उपकरणों को अपडेट रखें
  - स्वचालित अपडेट सक्षम करें
3. सुरक्षित वाई-फाई इस्तेमाल करें
  - WPA3 या WPA2 एन्क्रिप्शन का उपयोग करें
4. IoT के लिए अलग नेटवर्क रखें
  - IoT उपकरणों के लिए गेस्ट नेटवर्क का प्रयोग करें
5. उपयोग न होने पर बंद कर दें
  - निष्क्रिय उपकरणों को बंद करें
6. अनुमतियों के साथ सावधान रहें
  - केवल आवश्यक अनुमतियाँ दें
7. दो-कारक प्रमाणीकरण उपयोग करें
  - सुरक्षा की एक अतिरिक्त परत जोड़ें
8. गोपनीयता नीतियाँ जाँचें
  - पारदर्शी नीतियों वाले ब्रांड प्राथमिकता दें
9. सतर्क रहें
  - नवीनतम IoT स्कैम और जोखिमों के बारे में जानें

---

# प्रश्नोत्तर (Q&A)

धन्यवाद  
(Thanks)