ब्लूबगिंग

डिफॉल्ट सेटिंग के रूप में प्रायः स्मार्टफोन की ब्लूटूथ सेटिंग्स अन्य उपकरणों को ढूँढने एवं उनसे कनेक्ट करने के मोड में होते हैं, इससे **ब्लूबगिंग** जैसे खतरों के प्रति वे अतिसंवेदनशील हो जाते हैं।

ब्लूबगिंग:

- **परिचय:**
  - यह **हैकिंग का एक रूप है** जो हैकर्स को **खोजे जा सकने योग्य चालू ब्लूटूथ कनेक्शन के माध्यम से डिवाइस तक पहुँच प्रदान करता है।**
  - ब्लूबगिंग के माध्यम से हैकर डिवाइस के ऐप्स तक अनधिकृत पहुँच प्राप्त कर सकता है और उन्हें अपनी इच्छा के अनुसार नियंत्रित कर सकता है।
  - ट्रू वायरलेस स्टीरियो (TWS) डिवाइस या ईयरबड सहित **कोई भी ब्लूटूथ-सक्षम डिवाइस ब्लूबगिंग के लिये अतिसंवेदनशील है।**
  - एक बार किसी डिवाइस या फोन के ब्लूबग हो जाने के बाद,**हैकर उसके कॉल सुन सकता है, संदेश पढ़ सकता है और संदेश भी भेज सकता है तथा संपर्कों के साथ छेड़छाड़ कर सकता है।**
  - यहाँ तक कि आईफोन जैसे सबसे सुरक्षित स्मार्टफोन भी इसकी चपेट में हैं।
- **सुरक्षात्मक उपाय:**
  - उपयोग में नहीं होने पर ब्लूटूथ को बंद रखना और युग्मित ब्लूटूथ उपकरणों को डिस्कनेक्ट करना।
  - ब्लूटूथ डिवाइस को ब्लूटूथ सेटिंग्स से बंद करना।
  - डिवाइस के सिस्टम सॉफ्टवेयर को नवीनतम संस्करण में अपडेट करना।
  - सार्वजनिक वाई-फाई का सीमित उपयोग करना।
  - अपनी डिवाइस में होने वाली संदिग्ध गतिविधियों के प्रति जागरूक रहना
  - डेटा उपयोग में अचानक हुई बढ़ोतरी की निगरानी करना।
  - आधुनिक एंटी-वायरस सॉफ्टवेयर का उपयोग करना।

संबंधित सरकारी पहलें:

- साइबर सुरक्षित भारत पहल
- साइबर स्वच्छता केंद्र
- ऑनलाइन साइबर अपराध रिपोर्टिंग पोर्टल
- भारतीय साइबर अपराध समन्वय केंद्र (I4C)
- राष्ट्रीय महत्तवपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC)
- सूचना प्रौद्योगिकी अधिनियम, 2000
- राष्ट्रीय साइबर सुरक्षा रणनीति 2020

UPSC सिविल सेवा परीक्षा, विगत वर्षों के प्रश्न (PYQs)

प्रश्न. भारत में निम्नलिखित में से किसके लिये साइबर सुरक्षा घटनाओं पर रिपोर्ट करना कानूनी रूप से अनिवार्य है? (2017)

1. सेवा प्रदाताओं
2. डेटा केंद्र
3. कॉर्पोरेट निकाय

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(a) केवल 1
(b) केवल 1 और 2

(c) केवल 3
(d) 1, 2 और 3

उत्तर: (d)

व्याख्या:

- सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act) की धारा 70B के अनुसार, केंद्र सरकार ने अधिसूचना द्वारा घटना प्रतिक्रिया के लिये राष्ट्रीय एजेंसी के रूप में कार्य करने हेतु भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम **(CERT-In)** नामक एक एजेंसी का गठन किया गया है।
- केंद्र सरकार ने आईटी अधिनियम, 2000 की धारा 70 B के तहत वर्ष 2014 में CERT-In के लिये नियम स्थापित और अधिसूचित किये। नियम 12 (1) (A) के अनुसार, **CERT-In** को साइबर सुरक्षा के संदर्भ में घटना होने के उचित समय के भीतर सेवा प्रदाताओं, मध्यस्थों, डेटा केंद्रों और कॉर्पोरेट निकायों द्वारा रिपोर्ट करना अनिवार्य है। **अतः 1, 2 और 3 सही हैं।**

अत: विकल्प (d) सही है।

स्रोत: द हिंदू

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/bluebugging