

# समाचार वाणी

## खबर जो करें असर !

नाशिक | Friday, 25 September 2026

### भारत में साइबर सुरक्षा पर बढ़ती सतर्कता : चीन और पाकिस्तान से खतरे के बीच डिजिटल सुरक्षा पर ज़ोर

Publisher

Published on 21 Aug 2025



#### भारत में साइबर सुरक्षा पर बढ़ती सतर्कता : चीन और पाकिस्तान से खतरे के बीच डिजिटल सुरक्षा पर ज़ोर

लखनऊ स्थित उत्तर प्रदेश इंस्टीट्यूट ऑफ फॉरेंसिक साइंसेज़ (UP SIFS) में आयोजित तीन दिवसीय राष्ट्रीय सेमिनार ने भारत की साइबर सुरक्षा स्थिति पर गहन चर्चा की। इस सेमिनार में देश-विदेश के साइबर सुरक्षा विशेषज्ञों, सरकारी अधिकारियों, और तकनीकी विशेषज्ञों ने भाग लिया। चर्चा का मुख्य विषय रहा—भारत की डिजिटल सुरक्षा को मजबूत बनाना और पड़ोसी देशों से बढ़ते साइबर खतरों का समाधान।

#### भारत के सामने साइबर खतरे

भारत दुनिया की सबसे तेजी से डिजिटल होती अर्थव्यवस्थाओं में से एक है। लेकिन जैसे-जैसे डिजिटल ढांचा विस्तारित हो रहा है, साइबर अपराध और हैकिंग की घटनाएं भी तेजी से बढ़ रही हैं।

विशेषज्ञों ने बताया कि चीन और पाकिस्तान से साइबर हमलों का खतरा लगातार बढ़ रहा है। पिछले कुछ वर्षों में कई बार भारतीय रक्षा, बिजली आपूर्ति, रेलवे नेटवर्क और बैंकिंग सेक्टर पर साइबर हमले देखने को मिले हैं।

इन हमलों का मकसद केवल डेटा चोरी करना नहीं, बल्कि भारत की आर्थिक और रणनीतिक सुरक्षा को प्रभावित करना भी है। विशेषज्ञों ने चेताया कि ऐसे हमले भविष्य में और भी गंभीर हो सकते हैं यदि साइबर सुरक्षा की तैयारी मजबूत नहीं की गई।

#### साइबर सुरक्षा पर सरकार का फोकस

भारत सरकार पहले ही राष्ट्रीय साइबर सुरक्षा नीति 2020 लेकर आ चुकी है, जिसका उद्देश्य डिजिटल ढांचे को सुरक्षित करना है। अब 2025 में इसे और व्यापक रूप दिया जा रहा है।

नई नीति में—

- क्रिटिकल इंफ्रास्ट्रक्चर (बिजली, जल आपूर्ति, रक्षा, बैंकिंग आदि) को साइबर हमलों से सुरक्षित रखने के उपाय
- साइबर अपराध की जांच के लिए फॉरेंसिक प्रयोगशालाओं को आधुनिक तकनीक से लैस करना
- एथिकल हैकर्स और साइबर विशेषज्ञों की भर्ती और प्रशिक्षण
- आम नागरिकों को साइबर साक्षरता (Cyber Literacy) से जोड़ना शामिल किया गया है।

### बढ़ते साइबर अपराध और उनके प्रकार

भारत में साइबर अपराध अब केवल हैकिंग और डेटा चोरी तक सीमित नहीं रह गया है। विशेषज्ञों ने बताया कि अब इसमें—

- रैनसमवेयर हमले (जहां हैकर्स सिस्टम को लॉक कर फिरोती मांगते हैं),
- फिशिंग अटैक (ई-मेल या मैसेज के जरिए धोखाधड़ी),
- सोशल मीडिया हैकिंग,
- आर्टिफिशियल इंटेलिजेंस आधारित साइबर फ्रॉड जैसी चुनौतियाँ भी शामिल हो गई हैं।

पिछले एक साल में ही भारत में साइबर अपराधों की दर में **25% की वृद्धि** दर्ज की गई है। इसमें सबसे ज्यादा मामले बैंकिंग फ्रॉड और डिजिटल पेमेंट से जुड़े हैं।

### अंतरराष्ट्रीय सहयोग की आवश्यकता

सेमिनार में विशेषज्ञों ने इस बात पर भी ज़ोर दिया कि साइबर सुरक्षा केवल राष्ट्रीय मुद्दा नहीं है, बल्कि यह **अंतरराष्ट्रीय सहयोग** का विषय भी है।

भारत को अमेरिका, यूरोपीय देशों, और एशियाई साझेदारों के साथ मिलकर **ग्लोबल साइबर सिक्योरिटी नेटवर्क** का हिस्सा बनने की ज़रूरत है। इससे भारत को नई तकनीक, इंटेलिजेंस शेयरिंग और आधुनिक सुरक्षा सिस्टम अपनाने में मदद मिलेगी।

### विशेषज्ञों की राय

UP SIFS में आयोजित इस सेमिनार में प्रमुख साइबर सुरक्षा विशेषज्ञों ने कुछ महत्वपूर्ण सुझाव रखे—

1. हर सरकारी और निजी संगठन में साइबर सुरक्षा ऑडिट अनिवार्य किया जाए।
2. डिजिटल पेमेंट और ऑनलाइन ट्रांजेक्शन पर दोहरी सुरक्षा प्रणाली (Two-Factor Authentication) लागू हो।
3. साइबर सुरक्षा शिक्षा को कॉलेज और विश्वविद्यालय स्तर पर अनिवार्य किया जाए।
4. साइबर सुरक्षा स्टार्टअप्स और इनोवेशन को प्रोत्साहन दिया जाए।
5. आम नागरिकों को जागरूक करने के लिए साइबर जागरूकता अभियान चलाए जाएं।

### भारत का भविष्य और साइबर सुरक्षा

भारत में तेजी से बढ़ती डिजिटलीकरण की प्रक्रिया के साथ यह सुनिश्चित करना अनिवार्य हो गया है कि देश का डिजिटल ढांचा किसी भी तरह की साइबर जंग में सुरक्षित रह सके।

चीन और पाकिस्तान जैसे पड़ोसी देशों से आने वाले खतरों के मद्देनज़र, यह साफ है कि आने वाले समय में साइबर सुरक्षा उतनी ही महत्वपूर्ण होगी जितनी रक्षा और आंतरिक सुरक्षा।

विशेषज्ञों का मानना है कि अगर भारत ने समय रहते **मजबूत साइबर सुरक्षा प्रणाली** विकसित कर ली, तो यह न केवल देश की **राष्ट्रीय सुरक्षा को सुरक्षित रखेगी**, बल्कि डिजिटल अर्थव्यवस्था को भी मजबूती प्रदान करेगी।

#### **निष्कर्ष:**

भारत के लिए साइबर सुरक्षा आज केवल तकनीकी आवश्यकता नहीं, बल्कि **राष्ट्रीय सुरक्षा की अनिवार्यता** बन चुकी है। चीन और पाकिस्तान जैसे देशों से आने वाले साइबर खतरों को देखते हुए, भारत को न केवल अपनी आंतरिक सुरक्षा मजबूत करनी होगी बल्कि अंतरराष्ट्रीय स्तर पर भी सहयोग बढ़ाना होगा।

---

DISCLAIMER: the views/contents expressed/presented herein, within this advertorial and promotional feature are the sole and exclusive responsibility of individual clients/expert/their authorised representative/Publisher, to which effect, publication house/its representative/affiliates are not responsible/liable whatsoever.