CYBER ADVISORY

राज्य सायबर पुलिस मुख्यालय, भोपाल

भारत-पाक समाचार के रूप में छुपाई गई फ़िशिंग लिंक्स और APK फ़ाइलों के लिए उच्च सतर्कता

भारत-पाक संघर्ष के चलते साइबर हमले का जोखिम बढ़ गया है। इस स्थिति में भारतीय शासकीय एजेंसियां, सैन्य कर्मी/संस्थान और महत्वपूर्ण बुनियादी ढांचे को निशाना बनाया जा सकता है। भारत-पाक संघर्ष के संबंध में **WhatsApp, E-mail** और **Social Media Platform** के माध्यम से तेजी से फैल रही दुष्प्रचार सामग्री के बारे में सतर्क रहना आवश्यक है। इस सामग्री में भ्रामक **Videos, Images, '.exe/.apk'** और भारत-पाक संघर्ष से संबंधित समाचार या अपडेट के रूप में **Phishing emails, Fake Login Pages** और **Malicious Attachments** जैसी परिष्कृत रणनीति का उपयोग शामिल है।

साइबर अपराधी समाचार अथवा सूचनाओं से संबंधित विशेष अपडेट, संघर्ष से संबंधित कथन या लीक हुए फुटेज के बहाने दुष्प्रचार सामग्री प्रसारित कर रहे हैं, जिनमें मैलवेयर, स्पाइवेयर या फिशिंग वेबसाइट्स के लिंक होते हैं। यह सामग्री विभिन्न **URL** लिंक या अज्ञात नंबरों से भेजी गई तस्वीरों के रूप में भी हो सकती है जो कि **WhatsApp/Telegram**/अन्य सोशल मीडिया प्लेटफॉर्म के माध्यम से बड़ी सरलता से प्रेषित की जा सकती है।

साइबर हमला करने के तरीके:

1. दुष्प्रचार रूप से तैयार की गई **.apk** फाइल, **.exe** फाइल और वीडियो फाइल/लिंक को **WhatsApp, E-mail,** और अन्य सोशल मीडिया प्लेटफॉर्म पर निम्नलिखित तरीकों से साझा किया जा रहा है:
    - संदेशों में फिशिंग लिंक एम्बेड करना जो विश्वसनीय स्रोतों या समूहों के समान प्रतीत होते हैं। वैध समाचार या सरकारी स्रोतों की तरह दिखने के लिए डिजाइन की गई इन फिशिंग वेबसाइट्स के माध्यम से व्यक्तिगत डेटा को चुराया जा सकता है।
    - **App** या **Tool** (जैसे, **"Live war updates App"**) के रूप में लेबल की गई **APK** फाइल्स का प्रसार किया जा रहा है, जिसके माध्यम से डेटा चुराना या डिवाइस को लॉक करके फिरौती की मांग की जा सकती है। इसके अतिरिक्त इन **Tools** के माध्यम से बैंक खाते या सोशल मीडिया खाते आदि को भी हैक किया जा सकता है।

जनता के लिए सलाह:

WhatsApp और सोशल मीडिया उपयोग हेतु:

- कभी भी अनजान फोन नंबर से भेजे गए वीडियो या इमेज फाइल को **Open** न करें, भले ही ऐसी फाइल किसी ऐसे व्यक्ति द्वारा **Forward** की गई हो जिस पर आप भरोसा करते हैं।
- स्वयं भी ऐसे मैसेज/फाइल को कभी किसी को या किसी समूह को **Forward** न करें।
- केवल **Google Play Store** या अधिकृत ऐप स्टोर से ही किसी **App** को **Install** करें।
- विवादित अपडेट या संवेदनशील फुटेज दिखाने का दावा करने वाले **Forward** किए गए लिंक पर **Click** कर **Open** करने का प्रयास न करें।
- यदि आप किसी ऐसे समूह के सदस्य हैं जहां भड़काऊ या असत्यापित सामग्री शेयर की जा रही हो तो ऐसा करने वाले संदिग्ध **WhatsApp** ग्रुप से बाहर निकलें, रिपोर्ट करें और ऐसे ग्रुप को **Delete** करें।

WhatsApp में बेहतर सुरक्षा सेटिंग्स:

- ऑटो डाउनलोड **Disable** करें: **WhatsApp** की **Setting** में **-> Storage** और **Data ->** सभी **Media (Photo, Audio, Video, Documents)** के लिए **Auto-download** को **Disable** करें।
- अकाउंट हैक होने से बचाने के लिए हमेशा **WhatsApp** अकाउंट **Setting** में **2-step Verification Enable** करें।
- किसी भी दुष्प्रचार संदेश या समूह गतिविधि को सीधे **WhatsApp** पर **Report** करें या cybercrime.gov.in पर रिपोर्ट करें।
- **OTP** किसी के साथ साझा न करें।

E-mail उपयोगकर्ताओं के लिए:

- अज्ञात व्यक्ति द्वारा भेजे गए ईमेल न खोलें, खासकर वे जो भारत-पाक संघर्ष से संबंधित विषय वाले हों।
- अनचाहे ईमेल से आए **Attachments** को **Download** करने या लिंक पर **Click** कर **Open** करने से बचें।
- ईमेल **Address** की सावधानीपूर्वक जांच करें क्योंकि फिशिंग ईमेल भेजने के लिए साइबर अपराधी अक्सर असली जैसे दिखने वाले **Address** की नकल करते हैं।
- सभी ईमेल अकाउंट्स में **2-Factor Authentication (2FA) Enable** करें।
- **Updated Antivirus Software** का ही उपयोग करें और **Spam Filter** को **Enable** रखें।

सामान्य साइबर जागरूकता:

- भारत-पाक संघर्ष पर अपडेट या सूचनाएं जानने के लिए केवल सत्यापित समाचार चैनल और सोशल मीडिया हैंडल का ही उपयोग करें।
- संवेदनशील फर्जी समाचारों को **Forward** या **Download** करने से बचने के लिए **Fact Checkers** का उपयोग करें।
- **Cloud Storage** एवं महत्वपूर्ण डेटा का नियमित रूप से **Backup** लेते रहें।
- अपने **Antivirus** और **Mobile Security Software** को नियमित रूप से **Update** करें।
- विशेष रूप से संवेदनशील घटनाओं या सूचनाओं की असत्यापित सामग्री को **Share** करने से बचें।
- अधिकृत सरकारी वेबसाइटों और हैंडल के माध्यम से किसी भी ग्राफिक जानकारी को सत्यापित करें।

आपातकालीन स्थिति के लिए जरूरी सेटिंग्स:

1. **इमरजेंसी SOS फीचर (Emergency SOS)**
   - **Android:**
     सेटिंग्स > सेफ्टी और इमरजेंसी > इमरजेंसी SOS में जाकर इसे ऑन करें।
     (पावर बटन को 5 बार दबाकर SOS भेजें)
   - **iPhone:**
     सेटिंग्स > इमरजेंसी SOS > "साइड बटन से कॉल करें" और "ऑटो कॉल" चालू करें।
     (साइड बटन को 5 बार दबाकर SOS भेजें)

2. **इमरजेंसी कॉन्टैक्ट्स और मेडिकल ID**
   - **Android:** सेटिंग्स > सेफ्टी और इमरजेंसी > इमरजेंसी कॉन्टैक्ट्स में जोड़ें।
   - **iPhone:** हेल्थ ऐप > मेडिकल ID सेट करें और "लॉक स्क्रीन पर दिखाएं" चालू करें।

3. **इमरजेंसी अलर्ट ऑन करें**
   - **Android/iPhone:**
     सेटिंग **>** नोटिफिकेशन **>** वायरलेस अलर्ट्स → सभी चेतावनियाँ ऑन करें **(**भूकंप, सुनामी, आतंकी हमला आदि**)**।

रिपोर्टिंग:

यदि आप ऐसे किसी साइबर घोटाले का शिकार हुए हैं, तो कृपया हेल्पलाइन नंबर **1930** पर कॉल करें या www.cybercrime.gov.in पर अपनी शिकायत दर्ज करें। जनता से आग्रह है कि वे सतर्क रहें, संदिग्ध सामग्री को रिपोर्ट करें और गलत सूचना के प्रसार में योगदान न दें।