एनएचपीसी लिमिटेड
(भारत सरकार का एक नवरत्न उद्यम)
NHPC Limited
(A Government of India Navratna Enterprise)

ITUWTSA NEW DELHI 2024

सूचना प्रोद्योगिकी एवं संचार विभाग
IT & C Department
एनएचपीसी ऑफिस कॉम्प्लेक्स, सैक्टर-33,
फ़रीदाबाद (हरियाणा)-121003
NHPC Office Complex, sector-33,
Faridabad (Haryana)-121003
फोन/Phone: 0129-2256576
वैबसाइट/Website: www.nhpcindia.com

संदर्भ संख्या:-एनएच/आई टी एवं सी/2024/ 956 **दिनांक : 11/10/2024**

परिपत्र

विषय: साइबर सुरक्षा – क्या करें एवं क्या न करें।

सूचना और संचार प्रौद्योगिकी (ICT) हमारे रोजमर्रा के जीवन में सर्वव्यापी हो गई है। आईसीटी की बढ़ती स्वीकार्यता और बढ़ते उपयोग ने साइबर हमलों की संभावनाओं को बढ़ा दिया है, इसलिए NHPC के सभी कर्मचारियों से अनुरोध है कि वे साइबर सुरक्षा के लिए नीचे दिए गए निर्देशों का पालन सुनिश्चित करें:

क्या करें:

- सभी ऑनलाइन सेवाओं के लिए कैपिटल लेटर, स्मॉल लेटर, नंबर और स्पेशल कैरेक्टर के संयोजन का उपयोग करते हुए कम से कम 8 अक्षरों वाले जटिल पासवर्ड का उपयोग करें।
- जहाँ भी उपलब्ध हो, Multi-Factor Authentication का उपयोग करें।
- अपने महत्वपूर्ण डेटा का ऑफ़लाइन बैकअप जरूर रखें।
- **केवल अधिकृत और लाइसेंस प्राप्त सॉफ़्टवेयर का उपयोग करें।**
- जब आप अस्थायी रूप से अपना डेस्क छोड़ते हैं, तो हमेशा अपने कंप्यूटर को लॉक/लॉग-ऑफ करें।
- जब आप कार्यालय छोड़ते हैं, तो सुनिश्चित करें कि आपके कंप्यूटर और प्रिंटर ठीक से बंद हैं।
- अपने कंप्यूटर और मोबाइल फोन पर GPS, Bluetooth, NFC और अन्य सेंसरों को disable रखें। उन्हें केवल आवश्यकता पड़ने पर ही enable करें।
- केवल Google Play store (Android के लिए) और Apple App store (iOS के लिए) के आधिकारिक ऐप स्टोर से ऐप डाउनलोड करें।
- ऐप डाउनलोड करने से पहले, ऐप की लोकप्रियता की जाँच करें और उपयोगकर्ता समीक्षाएँ पढ़ें। किसी भी ऐसे ऐप को डाउनलोड करने से पहले सावधानी बरतें जिसकी प्रतिष्ठा खराब हो या जिसका यूजर बेस कम हो, आदि।
- किसी भी छोटे यूनिफ़ॉर्म रिसोर्स लोकेटर (URL) (उदाहरण: tinyurl.com/ab534/) को खोलते समय सावधानी बरतें। कई मैलवेयर और फ़िशिंग साइट URL शॉर्टनर सेवाओं का दुरुपयोग करते हैं।
- SMS या सोशल मीडिया आदि के ज़रिए शेयर किए गए किसी भी लिंक को खोलते समय सावधानी बरतें, विशेष रूप से जहाँ लिंक के पहले रोमांचक ऑफ़र/छूट आदि दिए गए हों या किसी करंट अफेयर्स के बारे में जानकारी देने का दावा किया गया हो। ऐसे लिंक फ़िशिंग/मैलवेयर वेबपेज पर ले जा सकते हैं, जो आपके डिवाइस को खतरे में डाल सकता है।
- किसी भी संदिग्ध ईमेल प्राप्त होने की स्थिति में तुरंत IT&C डिवीज़न को रिपोर्ट करें।

सूचना प्रोद्योगिकी एवं संचार विभाग
IT & C Department
एनएचपीसी ऑफिस कॉम्प्लेक्स, सैक्टर-33,
फ़रीदाबाद (हरियाणा)-121003
NHPC Office Complex, sector-33,
Faridabad (Haryana)-121003
फोन/Phone: 0129-2588239
वैबसाइट/Website: www.nhpcindia.com

क्या न करें:

- एक से ज़्यादा सेवाओं/ वेबसाइटों/ ऐप्स में एक ही पासवर्ड का इस्तेमाल न करें।
- अपने पासवर्ड को ब्राउज़र या किसी असुरक्षित दस्तावेज़ में सेव न करें।
- किसी भी पॉप अप / ऐड पर क्लिक न करें।
- किसी भी व्यावसायिक क्लाउड सेवा (जैसे: गूगल ड्राइव, ड्रॉप बॉक्स, आदि) पर कोई आधिकारिक डेटा या फ़ाइल अपलोड या सेव न करें।
- किसी भी तीसरे पक्ष की अनामीकरण सेवाओं (जैसे नॉर्ड वीपीएन, एक्सप्रेस वीपीएन, टोर, प्रॉक्सी, आदि) का इस्तेमाल न करें।
- अपने इंटरनेट ब्राउज़र में किसी तीसरे पक्ष के टूलबार (जैसे डाउनलोड मैनेजर, वेदर टूल बार, आस्कमी टूल बार, आदि) का इस्तेमाल न करें।
- **कोई भी pirated सॉफ़्टवेयर (जैसे: क्रैक, कीजेन, आदि) इंस्टॉल या इस्तेमाल न करें।**
- किसी भी अज्ञात प्रेषक द्वारा भेजे गए ईमेल में शामिल किसी भी लिंक या अटैचमेंट को न खोलें।
- सिस्टम पासवर्ड या प्रिंटर पासकोड या वाई-फ़ाई पासवर्ड को किसी भी अनधिकृत व्यक्ति के साथ साझा न करें।
- सोशल मीडिया या थर्ड पार्टी मैसेजिंग ऐप पर कोई भी संवेदनशील जानकारी साझा न करें।
- किसी भी अनधिकृत बाहरी डिवाइस को प्लग-इन न करें, जिसमें किसी अज्ञात व्यक्ति द्वारा साझा की गई USB ड्राइव शामिल है।
- **किसी भी अनधिकृत रिमोट एडमिनिस्ट्रेशन टूल (जैसे टीमव्यूअर, एमी एडमिन, एनीडेस्क, आदि) का उपयोग न करें।**
- **आधिकारिक दस्तावेज़ों को स्कैन करने के लिए किसी भी बाहरी मोबाइल ऐप आधारित स्कैनर सेवाओं (जैसे कैमस्कैनर आदि) का उपयोग न करें।**
- **किसी भी आधिकारिक दस्तावेज़ को संपादित/ परिवर्तित/ संपीड़ित करने के लिए किसी भी बाहरी वेबसाइट या क्लाउड-आधारित सेवाओं का उपयोग न करें (जैसे वर्ड टू पीडीएफ या फ़ाइल आकार संपीड़न)।**
- किसी भी अनधिकृत या अज्ञात व्यक्ति के साथ टेलीफोन या किसी अन्य माध्यम से कोई भी संवेदनशील जानकारी साझा न करें।

11/10/2024

(विभोर)
महाप्रबंधक (आई टी)
मुख्य सूचना सुरक्षा अधिकारी

वितरण:- इंट्रानेट पर। इस परिपत्र की कोई हार्ड कॉपी जारी नहीं की जाएगी ।

एनएचपीसी लिमिटेड
(भारत सरकार का एक नवरत्न उद्यम)
NHPC Limited
(A Government of India Navratna Enterprise)

ITUWTSA NEW DELHI 2024

सूचना प्रोद्योगिकी एवं संचार विभाग
IT & C Department
एनएचपीसी ऑफिस कॉम्प्लेक्स, सैक्टर-33,
फ़रीदाबाद (हरियाणा)-121003
NHPC Office Complex, sector-33,
Faridabad (Haryana)-121003
फोन/Phone: 0129-2588239
वैबसाइट/Website: www.nhpcindia.com

संदर्भ संख्या:-एनएच/आई टी एवं सी/2024/ दिनांक : 11/10/2024

परिपत्र

Subject: Cyber Security Do's and Don'ts.

Information and Communication Technologies (ICT) have become ubiquitous in our everyday life. The increasing adoption and use of ICT has increased the attack surface. All the NHPC employees are requested to follow below cyber security Do's and Don'ts to remain cyber safe:

DO's:

- Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters for all online services.
- Use multi-factor authentication, wherever available.
- Maintain an offline backup of your critical data.
- **Use authorized and licensed software only.**
- When you leave your desk temporarily, always lock/log-off from your computer session.
- When you leave office, ensure that your computer and printers are properly shutdown.
- Keep the GPS, bluetooth, NFC and other sensors disabled on your computers and mobile phones. These may be enabled only when required.
- Download Apps from official app stores of google (for android) and apple (for iOS) only.
- Before downloading an App, check the popularity of the app and read the user reviews. Observe caution before downloading any app which has a bad reputation or less user base, etc.
- Observe caution while opening any shortened uniform resource locator (URLs) (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortener services.
- Observe caution while opening any links shared through SMS or social media, etc., where the links are preceded by exciting offers/discounts, etc., or may claim to provide details about any current affairs. Such links may lead to a phishing/malware webpage, which could compromise your device.
- Immediately report any suspicious email to IT&C Division.

DON'TS:

- Don't use the same password in multiple services/websites/apps.
- Don't save your passwords in the browser or in any unprotected documents.
- Don't click on random popups/ ads while browsing internet.
- Don't upload or save any official data or files on any commercial cloud service (ex: google drive, drop box, etc.).
- Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies, etc.).

सूचना प्रोद्योगिकी एवं संचार विभाग
IT & C Department
एनएचपीसी ऑफिस कॉम्प्लेक्स, सैक्टर-33,
फ़रीदाबाद (हरियाणा)-121003
NHPC Office Complex, sector-33,
Faridabad (Haryana)-121003
फोन/Phone: 0129-2588239
वैबसाइट/Website: www.nhpcindia.com

- Don't use any 3rd party toolbars (ex: download manager, weather tool bar, askme tool bar, etc.) in your internet browser.
- **Don't install or use any pirated software (ex: cracks, keygen, etc.).**
- Don't open any links or attachments contained in the emails sent by any unknown sender.
- Don't share system passwords or printer passcode or Wi-Fi passwords with any unauthorized persons.
- Don't disclose any sensitive details on social media or 3rd party messaging apps.
- Don't plug-in any unauthorized external devices, including USB drives shared by any unknown person.
- **Don't use any unauthorized remote administration tools (ex: Teamviewer, Ammy admin, anydesk, etc.)**
- **Don't use any external mobile App based scanner services (ex: Camscanner etc.) for scanning official documents.**
- **Don't use any external websites or cloud-based services for editing/converting/compressing any official document (ex: word to pdf or file size compression).**
- Don't share any sensitive information with any unauthorized or unknown person over telephone or through any other medium.

11/10/2024

(विभोर)
महाप्रबंधक (आई टी)
मुख्य सूचना सुरक्षा अधिकारी

वितरण:- इंट्रानेट पर। इस परिपत्र की कोई हार्ड कॉपी जारी नहीं की जाएगी ।