नेपाल विधुत प्राधिकरण
साइबर सुरक्षा सचेतना

साइबर सुरक्षा (Cybersecurity) सचेतना महिना, जुन प्रत्येक अक्टोबरमा मनाइन्छ, नेपाल विधुत प्राधिकरण का लागि एक महत्वपूर्ण पहल हो किनभने यसले हाम्रो डिजिटल पूर्वाधारको सुरक्षाको महत्वलाई जोड दिन्छ। यो एक महिने अभियान, जसलाई विश्वव्यापी र स्थानिय रूपमा समर्थन गरिएको छ, NEA का सबै कर्मचारीहरूलाई मजबुत साइबर सुरक्षा अभ्यासहरू अपनाउन शिक्षा दिने र सक्षम बनाउने उद्देश्य राख्दछ। प्रभावकारी ऊर्जा व्यवस्थापनका लागि डिजिटल प्रणालीहरूमा हाम्रो बृद्धि भइरहेको निर्भरतालाई ध्यानमा राख्दै, साइबर खतराहरू विरुद्ध सतर्क रहनु अत्यावश्यक छ। यस माध्यमवाट साइबर सुरक्षाको हाम्रो बुझाइलाई बढावा दिन र उक्त जोखिमहरूलाई कम गर्न सकिने उपायहरूको बारेमा जानकारी प्रधान गरिनेछ। साइबर सुरक्षा सचेतनाको संस्कृति विकास गरेर, हामी हाम्रो विधुतीय प्रणालीहरूको लचकता र विश्वसनीयताको सुनिश्चितता गर्छौं, जसले अन्ततः हाम्रो राष्ट्रको महत्वपूर्ण पूर्वाधारको सुरक्षामा योगदान पुर्याउँछ।

साइबर सुरक्षा जागरूकता बढाउन र आफूलाई सुरक्षित राख्न प्रयोगकर्ताहरूले लिनुपर्ने दश व्यावहारिक कार्यहरू:

१. **मजबुत र फरक पासवर्डहरू प्रयोग गर्नुहोस्**: अक्षर, संख्या, र विशेष क्यारेक्टरहरूको मिश्रण गरेर जटिल पासवर्डहरू सिर्जना गर्नुहोस्, र विभिन्न खाताहरूमा एकै पासवर्ड पुन प्रयोग नगर्नुहोस्।

२. **मल्टिफ्याक्टर प्रमाणीकरण (MFA; Multi Factor Authentication) सक्षम गर्नुहोस्**: आफ्नो खाताहरूमा अतिरिक्त सुरक्षा थप्न MFA सक्षम गर्नुहोस्, जसले पासवर्डसँगै दोस्रो प्रमाणीकरणको सुरक्षा प्रधान गर्छ।

३. **फिशिङ्ग (Phishing) घोटालाहरू प्रति सतर्क हुनुहोस्**: नचाहिएको इमेल, सन्देश, वा लिङ्कहरू प्रति सावधान रहनुहोस्, विशेष गरी तिनीहरूले व्यक्तिगत जानकारी मागेमा। जवाफ दिनु अघि वा लिङ्कहरू क्लिक गर्नु अघि जाहाँ वाट जसले पठाएको हो, तिनको प्रामाणिकता सुनिश्चित गर्नुहोस्।

४. **सफ्टवेयर अद्यावधिक (Update) राख्नुहोस्**: आफ्नो अपरेटिङ प्रणाली (Operating System), सफ्टवेयर, र Application हरूलाई नियमित रूपमा अद्यावधिक गर्नुहोस् जसले गर्दा मालवेयर (Malware) विरुद्धको सुरक्षा गर्न सकियोस्।

५. **आफ्नो वाई-फाई (WIFI) नेटवर्क सुरक्षित गर्नुहोस्**: घर र कार्यालयमा वाई-फाई नेटवर्कहरूको लागि बलियो पासवर्ड प्रयोग गरेर अनधिकृत पहुँचबाट जोगिनुहोस्।

६. **आफ्नो डाटा ब्याकअप (Data Backup) गर्नुहोस्**: महत्वपूर्ण फाइलहरूको नियमित रूपमा बाह्य हार्ड ड्राइभ (External Hard Drive) वा क्लाउड (Cloud) सेवा *(जस्तै Google Drive, Drop Box, One Drive etc.)* मा ब्याकअप गर्नुहोस् ताकि साइबर आक्रमण वा हार्डवेयर विफलता (Hardware Failure) को अवस्थामा डाटालाई सजिलै पुनः प्राप्त गर्न सकियोस्।

७. **एन्टिभाइरस (Antivirus) र एन्टि-मालवेयर (Anti-malware) सफ्टवेयर प्रयोग गर्नुहोस्:** प्रतिष्ठित एन्टिभाइरस र एन्टि-मालवेयर सफ्टवेयर install गरेर नियमित रूपमा अपडेट गर्नुहोस् ताकि सम्भावित साइबर जोखिम पहिचान र रोकथाम गर्न सकियोस्।

८. **सुरक्षित ब्राउजिङ (Safe Browsing) अभ्यास गर्नुहोस्:** शंकास्पद वेबसाइटहरूमा नजानुहोस् र अविश्वसनीय स्रोतहरूबाट फाइलहरू डाउनलोड नगर्नुहोस्। सकेसम्म सुरक्षित, HTTPS encrypted वेबसाइटहरू प्रयोग गर्नुहोस्।

९. **आफ्ना खाताहरू नियमित रूपमा अनुगमन गर्नुहोस्:** वित्तीय र अनलाइन खाताहरूमा कुनै अनधिकृत लेनदेन वा परिवर्तनहरू भए/नभएको जाँच गर्दै शंकास्पद गतिविधि देखिएमा सम्बन्धित निकायमा तुरुन्त रिपोर्ट गर्नुहोस्।

१०. **साइबर सुरक्षा सम्बन्धि निरन्तर शिक्षा लिनुहोस्:** साइबर सुरक्षा खतराहरू र सर्वोत्तम अभ्यासहरूका बारेमा अद्यावधिक रहन तालिम सत्रहरूमा सहभागी हुनुहोस्, लेखहरू अध्ययन गर्नुहोस्, र साइबर सुरक्षा समाचारहरू नियमित रूपमा पढ्नुहोस्।

सूचना प्रविधि विभाग
नेपाल विद्युत प्राधिकरण