मितिः २०७८/०३/११ (25th June, 2021)

साइबर सुरक्षाका लागि जनहितमा जारी सन्देश

रान्समवेयर (Ransomware) संग सम्बन्धित :

क) रान्समवेयर (Ransomware) के हो ?

रान्समवेयर (Ransomware) एक प्रकारको मालवेयर (Malware: **Mal**icious Soft**ware**) हो जसको प्रयोग गरेर ह्याकर/साईबर अपराधीले ईमेल/इन्टरनेट तथा पेन ड्राइभ (USB Stick/Driver) वा संक्रमित (Infected) कम्प्युटरको माध्यमबाट महत्वपूर्ण डाटा तथा कम्प्युटर प्रणालीलाई बिगार्न तथा नष्ट गर्न प्रयोग गर्ने गर्छन । साथै कम्प्युटर प्रयोगकर्ताबाट फिरौती रकम प्राप्त नगरेसम्म कम्प्युटर प्रयोगकर्ताको डाटालाई सार्वजनिक गर्ने वा महत्वपूर्ण डाटालाई प्रयोग गर्न नसक्ने गरी Encryption/Lock गरी दिने गर्छन । कतिपय अवस्थामा म्याद तोकी ह्याकर/साईबर अपराधीले कम्प्युटर प्रयोगकर्ताबाट रकम/विट क्वाइन (Crypto Currency) माग्ने तर उक्त समयावधि भित्र भुक्तानी नगर्दा महत्वपूर्ण डाटालाई सधैको लागि नष्ट (Delete) गरी दिनुको साथै ह्याकर/साईबर अपराधीले सामान्यता मागेको रकम/विट क्वाइन (Crypto Currency) भुक्तानी पाए पनि प्रयोगकर्ताको डाटालाई उपलब्ध गराउदैन । रान्समवेयर (Ransomware) धेरै प्रकारका हुन्छन् जस्तैः WannaCry, UIWIX CryptoLocker, NotPetya, Bad Rabbit, Cerber, Crysis, CryptoWall, GoldenEye, Jigsaw, Locky आदि ।

ख) रान्समवेयर आक्रमण (Ransomware Attack) कहाँबाट आउँछ ?

इन्टरनेट प्रयोगकर्ताले

- इमेल मार्फत प्राप्त असुरक्षित फाइल Attachment तथा लिंकलाई Click गर्दा,
- संक्रमित (Infected) पेन ड्राइभ (USB Stick/Driver) लाई फाइल स्थानान्तरण(Transfer/Copy) गर्नको लागि प्रयोग गर्दा,
- Visit गरिएको असुरक्षित वेभसाईटमा आएको Pop-Up Window/Banner मा Click गर्दा,
- सामाजिक संजाल (Social Media) जस्तैः Facebook, Twitter, LinkedIn तथा WhatsApp/Viber मा प्राप्त प्राप्त असुरक्षित Attachment तथा लिंकलाई Click गर्दा,
- Freeware/shareware तथा Pirated Software, Music/Video डाउनलोड गर्दा,

प्रयोगकर्ताको कम्प्युटर/मोवाईलमा रान्समवेयर (Ransomware) डाउनलोड भई Install हुन्छ ।

ग) रान्समवेयर आक्रमण (Ransomware Attack) बाट कसरी सुरक्षित रहने ?

रान्समवेयर (Ransomware Attack) बाट सुरक्षित रहन निम्न उपायहरु अपनाऔं।

१. कम्प्युटर तथा कम्प्युटर प्रणालीको भण्डारण हुने महत्वपूर्ण डाटा (Data) लाई नियमित backup राखौं ।

२. कुनै कारणबश कम्प्युटर तथा कम्प्युटर प्रणाली ह्याक भई ह्याकरले डाटा (Data) Encryption गरी उक्त Data Decryption को लागि पैसा भुक्तानी माग गरेमा त्यस्ता ह्याकरलाई भुक्तानी नगरौ। ह्याकरलाई भुक्तानी गर्दैमा उक्त Data Decryption हुने सम्भावना हुदैन ।

३. कम्प्युटर, कम्प्युटर प्रणाली र डिजिटल खातामा बलियो पासवर्डको प्रयोग गरौं । उक्त पासवर्ड समय समय परिवर्तन गरौं ।

४. कम्प्युटर र कम्प्युटर प्रणालीलाई सुरक्षित राख्न Multi-Factor Authentication (जस्तै Two Factor Authentication, Mobile Number, OTP, Fingerprint आदि) को प्रयोग गरौं ।

५. कम्प्युटर तथा कम्प्युटर प्रणालीमा Anti-Virus/Anti-Malware/Spam Filter को प्रयोग गरी नियमित स्कान (Scan) गरौं ।

६. कम्प्युटर तथा कम्प्युटर प्रणालीमा प्रयोग भएका Software लगायत Operating System, Anti-Virus/Anti-Malware/Spam Filter लाई नियमित अद्यावधिक (Update) गरौं ।

७. Freeware, Pirated software/game, Free music/video, अश्लील सामग्री उपलब्ध हुने जस्ता असुरक्षित वेभसाइटहरुको प्रयोग नगरौं । त्यस्ता असुरक्षित वेभसाइटहरु Visit गर्दा Pop-Up Window/Banner मा प्रचारको लागि आउने लिंकमा Click नगरौ र त्यस्ता वेभसाइटहरुबाट Freeware/shareware तथा Pirated Software, Music/Video/games डाउनलोड नगरौं ।

८. सामाजिक संजाल (Social Media) जस्तैः Facebook, Twitter, LinkedIn तथा WhatsApp/Viber मा प्राप्त हुने शंकास्पद Attachment तथा लिंकलाई Click नगरौं ।

९. कम्प्युटर तथा कम्प्युटर प्रणालीमा इमेल/इन्टरनेटको लिंक तथा Attachment लाई सहि पहिचान गरेर मात्र Click/open गरौ उक्त लिंक तथा Attachment शंकास्पद लागेमा नखोलौं ।

१०. वेवारिसे रुपमा भेटिएको पेन ड्राइभ (USB Stick/Driver) लाई कम्प्युटर तथा कम्प्युटर प्रणालीमा प्रयोग नगरौं ।

Nepal Telecommunications Authority (NTA)

Cyber Security Task Force (NTACERT)

National Theatre Building, Jamal

Kathmandu, Nepal

Email: cert@nta.gov.np, URL: www.nta.gov.np