मितिः २०७८/०२/१४ (28th May, 2021)

साइबर सुरक्षाका लागि जनहितमा जारी सन्देश

क) मालवेयर (Malware) के हो ?

मालवेयर (Malware: **Mal**icious Soft**ware**) ह्याकरद्वारा निर्माण भएको यस्तो प्रोग्राम हो जसलाई ह्याकर/साईबर अपराधीले ईमेल/इन्टरनेट तथा पेन ड्राइभ (USB Stick/Driver) वा संक्रमित (Infected) कम्प्युटरको माध्यमबाट अन्य कम्प्युटर तथा कम्प्युटर प्रणालीलाई बिगार्न तथा नष्ट गर्न प्रयोग गर्ने गर्छन | मालवेयर (Malware) विभिन्न प्रकारका हुन्छन् जस्तैः Spyware, Ransomware/Crypto-malware, Adware, Virus, Trojan, Worms, Bot & Botnets, Rootkits, Keyloggers, Spam/Phishing आदि |

ख) मालवेयर (Malware 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 वेभसाईट अन्तर्गत 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 मालवेयर (Malware) डाउनलोड तथा Install हुन्छ |

ग) मालवेयर (Malware) ले के हानी गर्न सक्छ ?

कम्प्युटरमा मालवेयर Install भए पछि यसले कम्युटर प्रयोगकर्ताको दैनिक क्रियाकलापलाई अवलोकन गरी प्रयोगकर्तालाई थाहै नदिई चल्ने र आर्थिक तथा व्यक्तिगत संवेदनशील डाटामा ह्याकर/ साईबर अपराधीलाई पहुँच पुर्याई दिने देखि सम्पूर्ण महत्वपूर्ण डाटालाई प्रयोग गर्न नसक्ने गरी Encryption गरी दिने र कम्प्युटर प्रणालीलाई नचल्ने गराई दिन सक्छ |

घ) मालवेयर (Malware) बाट कसरी सुरक्षित रहने ?

मालवेयर (Malware) बाट सुरक्षित रहन निम्न उपायहरु अपनाऔं।

१. Freeware, Pirated software/game, Free music/video, अश्लील सामग्री उपलब्ध हुने जस्ता असुरक्षित वेभसाइटहरुको प्रयोग नगरौ | 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 नगरौ |

२. सामाजिक संजाल (Social Media) जस्तैः Facebook, Twitter, LinkedIn तथा WhatsApp/Viber मा प्राप्त प्राप्त हुने शंकास्पद Attachment तथा लिंकलाई Click नगरौ |

३. कम्प्युटर तथा कम्प्युटर प्रणालीमा इमेल/इन्टरनेटको लिंक तथा Attachment लाई सहि पहिचान गरेर मात्र Click/open गरौ उक्त लिंक तथा Attachment शंकास्पद लागेमा नखोलौ |

४. असुरक्षित वेभसाइटहरुको Cookies Request लाई स्वीकार (Accept) नगरौ | त्यसलाई Ignore गरौ |

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

६. वेवारिसे रुपमा भेटिएको पेन ड्राइभ (USB Stick/Driver) लाई कम्प्युटर तथा कम्प्युटर प्रणालीमा प्रयोग नगरौ |

७. असुरक्षित वेभसाइटहरु पहिचान गर्ने Netcraft जस्ता Security Browser Add on Tools को प्रयोग गरौ |

८. कम्प्युटर तथा कम्प्युटर प्रणालीको भण्डारण हुने महत्वपूर्ण डाटा (Data) लाई नियमित backup राखौ |

९. कम्प्युटर तथा कम्प्युटर प्रणालीमा Anti-Virus/Anti-Malware/Spam Filter को प्रयोग गरी नियमित स्कान (Scan) गरौ |

१०. कम्प्युटर तथा कम्प्युटर प्रणालीको Firewall लाई सधै Active "ON" राखौ |

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

१२. सकेसम्म खुल्ला वाईफाई (असुरक्षित वाईफाई) को प्रयोग नगरौ |

१३. इमेल/इन्टरनेट मार्फत फैलिने नयाँ Virus/Cyber Attack बारेमा जानकारी राखौ | सो विषयमा अरुलाई समेत जानकारी गराऔ |

१४. कम्प्युटर, कम्प्युटर प्रणाली र डिजिटल खातामा बलियो पासवर्डको प्रयोग गरौ | उक्त पासवर्ड समय समय परिवर्तन अवस्य गरौ |

१५. कम्प्युटर र कम्प्युटर प्रणालीलाई सुरक्षित राख्र Multi-Factor Authentication (जस्तै Two Factor Authentication, Mobile Number, OTP, Fingerprint इत्यादी) को प्रयोग गरौ |

१६. इमेल/इन्टरनेट मार्फत पुरस्कार (Prize), उपहार (Gift), चिट्ठा (Lottery), भिषा (VISA) लगायत बिभिन्न प्रलोभन देखाएर पठाईएको वा डर धम्की दिई पठाईएको संदेश, फोनकल लगायतलाई Reply/Response नगरौं |

१७. इमेलबाट आफ्नो Password, OTP, Bank Account Number, PIN code जस्ता विवरणहरु नपठाऔ |

१८. कुनै पनि वेबसाइटको राम्रोसंग पहिचान नगरी Login Credentials (User Name and Password), बैंकको क्रेडिट कार्ड नम्बर, नागरिकता नम्बर लगायतका Personally Identifiable Information (PII) हरु Share नगरौं | आधिकारिक बेवसाइटको राम्रोसंग पहिचान गरेर मात्र आफ्नो विवरण Share गरौं |

१९. प्राप्त हुन आएको कुनै इमेल वा वेबसाइटको विषयमा शंका लागेमा सम्बन्धित संस्थामा फोन सम्पर्क गरेर, इमेल पठाउने व्यक्तिको वा संस्थाको राम्रोसंग पहिचान गरेर मात्र Reply/Response गरौं |

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