मितिः २०७८/०५/११ (27 August, 2021)

साइबर सुरक्षाका लागि जनहितमा जारी सन्देश

इमेल सुरक्षा (Email Security) संग सम्बन्धितः

(१) इमेल सूरक्षा (Email Security) के हो?

Email Communication, इमेलमा अनाधिकृत पहुँच, Email Data Loss, इमेलमा प्राप्त हुने Spam Message, Phishing Message आदि लाई रोक्नको लागि वा आफ्नो इमेल खातामा अनावश्यक वा Threat Message हरुलाई आउनबाट रोक्न अपनाइने विभिन्न सूरक्षाका विधि तथा उपायहरु नै इमेल सूरक्षा भनिन्छ ।

साइबर अपराधीले मालवेयर, स्पाम र फिशिंग आक्रमण (attacks) को लागि ईमेललाई एक लोकप्रिय माध्यमको रुपमा प्रयोग गर्ने गर्छन । इमेलमा भ्रामक सन्देशहरु पठाई, Attachment खोल्न लगाई वा लिंकमा क्लिक गर्न लगाई प्रयोगकर्ताको उपकरणमा मालवेयर स्थापित (Install) गर्ने गर्दछन् ।तत्पश्चात प्रयोगकर्ताको क्रियाकलापलाई अनुगमन गर्ने, व्यक्तिको Financial विवरण चोर्ने, कम्पनीको गोप्य तथा संवेदनशील विवरण सार्वजनिक गरिदिने जस्ता अपराधिक क्रियाकलापहरु गर्छन् ।

तसर्थ ईमेल सुरक्षा व्यक्तिगत र व्यापारिक ईमेल खाताहरु दुबैको लागि नै आवश्यक हुन्छ।

(२) प्राप्त इमेल असुरक्षित इमेल (Unsecure Email) हो वा होइन कसरी छुट्टाउने?

इमेल मेसेजमा निम्न बमोजिमको संकेत देखिएमा असुरक्षित इमेल हुन सक्छ ।

- अपरिचित व्यक्तिबाट आएको अस्वभाविक किसिमको इमेल भएमा ।
- Prize, VISA, Lottery जस्ता लोभ्याउने खाले Content भएको इमेल भएमा ।
- अस्वाभाविक किसिमको लिंक तथा Attachment पठाइएको इमेल भएमा ।
- आकर्षक विज्ञापन भएको इमेल भएमा ।
- आफुसंग असम्बन्धित मान्छेको इमेल प्राप्त भएमा ।
- untrusted Domain जस्तै ....@afhdo3e.com देखिएमा ।

(३) इमेल (Email) कसरी सुरक्षित बनाउने ?

इमेल सुरक्षित बनाउन निम्न उपायहरु अपनाऔ :

१. इमेल सुरक्षाको लागि Email Service Provider ले प्रदान गरेको Security Features लाई Enable गरौ |

२. अनलाइन registration गर्दा Business वा आफ्नो महत्वपूर्ण इमेलको प्रयोग नगरौ |

३. सकभर व्यक्तिगत इमेल सार्वजिनक नगरौ | भिन्न भिन्न उदेश्यको लागि फरक फरक इमेलको प्रयोग गरौ | साथै Social Media मा राखिएको इमेल लगायतका व्यक्तिगत विवरणलाई private गरेर राखौ |

४. शंकास्पद देखिने इमेलबाट Phishing/ Malware/Social Engineering लगायतका सूरक्षा जोखिम हुन सक्ने भएकोले त्यस्ता शंकास्पद इमेल, SPAM/Junk इमेललाई नखोलौ | साथै उक्त इमेलको reply नगरौ |

५. अनावश्यक इमेल आएमा त्यस्तो इमेललाई SPAM वा junk मा जाने वा Block गर्ने गरी Configure/Setting गरौ |

६. अनावश्यक वेबसाइटमा Subscribe नगरौ | यदि Subscribed गरेको भए उक्त वेबसाइटबाट प्राप्त इमेलमा दिईएको unsubscribe लिंक मार्फत unsubscribe गरौ |

७. इमेल सुरक्षाको लागि SPAM Filter तथा Antivirus को प्रयोग गरौ |

८. सार्वजिनक स्थानमा राखिएको कम्प्यूटरबाट इमेल login गर्दा उक्त कम्प्यूटरमा भएको Keylogger को प्रयोग गरी Username तथा password चोरी हुन सक्ने भएकोले त्यस्ता कम्प्यूटरबाट सकेसम्म login नगरौ | यदि गरेको भए पनि आफ्नो व्यक्तिगत कम्युटरबाट पासवर्ड यथासिघ्र पासवर्ड परिवर्तन गरौ |

९. शंकास्पद इमेलको लिंक तथा Attachment लाई Click नगरौ |

१०. आफ्नो इमेलमा बलियो पासवर्ड राखौ र समय समयमा पासवर्ड परिवर्तन गरौ | साथै इमेल Recovery को लागि Multifactor Authentication को समेत प्रयोग गरौ |

११. Business इमेल वा आफ्नो महत्वपूर्ण इमेल सार्वजिनक वाईफाईबाट नखोलौ |

१२. Remotely कम्पनीको इमेल खोल्दा VPN को प्रयोग गरौ |

१३. सुरक्षित इमेल प्राप्त गर्नको लागि SSL/TLS/PGP/GPG encryption Solution को प्रयोग गरौ |

१४. कम्पनी/संस्थाको लागि Secure email gateway को प्रयोग गरौ |

१५. Email Security Policy तर्जुमा गरी सो को कार्यान्वयन गरौ |

Nepal Telecommunications Authority (NTA)
Cyber Security Task Force (NTACERT)
Jamal, Kathmandu, Nepal
Email: cert@nta.gov.np, Website: www.nta.gov.np