मितिः २०७८/०१/०२

साइबर सुरक्षाका लागि जनहितमा जारी सन्देश

फिशिंग स्क्याम (Phishing scam) संग सम्बन्धितः

(१) फिशिंग स्क्याम (Phishing Scam) अथवा फिशिंग हमला (Phishing Attack) के हो?

यो एक प्रकारको साइबर हमला (Cyber Attack) हो जसको प्रयोग गरेर साइबर अपराधीहरुले (Cybercriminals) इन्टरनेट प्रयोगकर्ताहरुको (Internet users) व्यक्तिगत विवरण, इमेल तथा पासवर्ड, बैंकको खाता नम्बर तथा पिन कोड आदि प्राप्त गर्ने, साथै कुनै प्रलोभन वा डर धम्की देखाई बैंकबाट आफनो खातामा रकम जम्मा गर्न लगाउने जस्ता प्रयासहरु गर्छन् र सोझासाझा व्यक्तिहरुलाई त्यस्तो जालमा पार्न सफल पनि हुन्छन् | यसको लागि साइबर अपराधीहरुले इमेल पठाउने, असली जस्तै देखिने नक्कली वेबसाइटको (Fake Website) प्रयोग गर्ने, संदेश (Message) पठाउने र फोनकलको समेत प्रयोग गर्छन् |

(२) फिशिंग स्क्याम(Phishing scam) अथवा फिशिंग हमला (Phishing Attack) बाट कसरी बच्ने ?

त्यसकारण फिशिंग स्क्याम(Phishing scam) अथवा फिशिंग हमला (Phishing Attack) बाट बच्न निम्न उपायहरु अपनाऔं :-

१. अपरिचित व्यक्ति वा ठेगानाबाट आएको शंकास्पद इमेललाई नखोलौं |

२. अपरिचित व्यक्ति वा ठेगानाबाट आएको शंकास्पद इमेलको **Attachment** लाई नखोलौं |

३. अपरिचित व्यक्ति वा ठेगानाबाट आएको इमेलमा रहेको **Link** हरुमा **Click** नगरौं र नखोलौं |

४. अपरिचित व्यक्ति वा ठेगानाबाट आएको इमेल वा शंकास्पद इमेललाई तत्काल **Delete** अथवा **Block** गरौं ।

५. इमेल **Reply/Response** नै गर्नु परे **Browser** मा वेबसाइटको नाम **Type** गरेर मात्र गरौं ।

६. पुरस्कार(Prize), उपहार (Gift), चिट्ठा (Lottery) लगायत बिभिन्न प्रलोभन देखाएर पठाईएको वा डर धम्की दिई पठाईएको इमेल, संदेश, फोनकल लगायतलाई **Reply/Response** नगरौं ।

७. चिनेको व्यक्ति/संस्था वा नचिनेको व्यक्ति/संस्थाबाट आएको **Email** मा **PDF, TEXT, CSV** जस्ता **Standard Format** बाहेकका **exe, vbs** जस्ता **extension** का **File** हरु **Click** नगरौं र नखोलौं ।

८. आफूसंग सम्बन्धित नभएका Country domain/sub-domain बाट आएका इमेलहरुलाई नखोलौं र **Delete** गरौं ।

९. अनावश्यक Mailing List मा Subscribe नगरौं र अनावश्यक Mailing list मा Subscribed भएमा Unsubscribe गरौं ।

१०. इमेलबाट आफ्नो Password, OTP, Bank Account Number, PIN code जस्ता विवरणहरु नपठाऔ ।

११. 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 गरेरमात्र आफ्नो विवरण Share गरौं** ।

१२. 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 ।

१३. आफ्नो Computer/Laptop/Mobile Device आदिमा Antivirus को प्रयोग 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