मितिः २०७८/०१/०९

साइबर सुरक्षाका लागि जनहितमा जारी सन्देश

सोसियल इन्जिनियरिंग (Social Engineering) संग सम्बन्धितः

(१) सोसियल इन्जिनियरिंग (Social Engineering) के हो?

यो एक प्रकारको साइबर हमला (Cyber Attack) हो जसमा साइबर आक्रमणकर्ता (Cyber Attacker) ले मनोवैज्ञानिक युक्तिहरू/रणनीतिहरू र मानिसहरूसँग भएको आफ्नो सम्बन्धको समेत प्रयोग गरेर पासवर्ड, बैंकको खाता नम्बर तथा पिन कोड, रकम प्राप्त गर्ने प्रयास गर्छन र सफल पनि हुन्छन् ।

समान्यतया ह्याक गर्ने तरिकाहरू पत्ता लगाउन भन्दा मानिसको आर्कषण/झुकाव लाई आफुतिर तानी उसको विश्वास जिल्न सजिलो हुने हुँदा आक्रमणकर्ता (Cyber Attacker) ले लोभ्याउने खालको सन्देश, संगीत, चलचित्रहरु सितैमा डाउनलोड गर्न दिने र सोही समयमा कम्प्युटरमा गोप्य रूपमा मालिसियस सफ्टवेयर स्थापना गरी कम्प्युटर प्रयोगकर्तासम्म पहुँच बनाउने गर्छन र कम्प्युटरलाई नियन्त्रण गर्ने गर्छन ।

त्यस्तै साइबर आक्रमणकर्ता (Cyber Attacker) ले इन्टरनेट प्रयोगकर्तालाई झुक्याई पासवर्ड दिनको लागि मूर्ख बनाई, डर धम्की देखाई बैंकबाट आफनो खातामा रकम जम्मा गर्न लगाउने जस्ता प्रयासहरु गर्छन् र सोझासाझा व्यक्तिहरुलाई त्यस्तो जालमा पार्न सफल पनि हुन्छन् ।

तसर्थ यसरी साइबर आक्रमणकर्ताहरुले इमेल पठाउने, असली जस्तै देखिने नक्कली वेबसाइटको (Fake Website) प्रयोग गर्ने, संदेश (Message) पठाउने र फोनकलको समेत प्रयोग गर्ने र मनोवैज्ञानिक संगत क्रियाकलापबाट मानिसको विश्वास जिल्न सफल भई सोझासाझा व्यक्तिहरुलाई ठगी गर्ने, डाटा चोर्ने तथा बेच्ने, संस्थाको मान प्रतिष्ठा तथा वित्तमा क्षति पुर्याउने जस्ता कार्य नै सोसियल इन्जिनियरिंग (Social Engineering) हो ।

(२) सोसियल इन्जिनियरिंग हमला (Social Engineering Attack) मा प्रयोग हुने माध्यम (Means) के के हुन सक्छन?

सोसियल इन्जिनियरिंग (Social Engineering Attack) मा प्रयोग हुने माध्यमहरुः-

१. इमेल (Phishing Email)
२. टेलीफोन/मोवाइल वार्ता (Vishing)
३. पेन ड्राइभ (USB Sticks)
४. वेभसाइट (Internet freebies)

५. भौतिक पहुँच (Physical impersonation)

६. इलेट्रोनिक फोहोर (Electronics Waste)

(३) सोसियल इन्जिनियरिंग हमला (Social Engineering Attack) बाट कसरी बच्ने ?

सोसियल इन्जिनियरिंग हमला (Social Engineering Attack) बाट बच्न निम्न उपायहरु अपनाऔ :-

(क) इमेल (Phishing Email)

१. शंकास्पद इमेललाई reply/response नगर्ने ।

२. इमेलको शंकास्पद attachments तथा प्राप्त भएका लिंकलाई नखोल्ने ।

३. Sender's email address तथा इमेलको embedded links लाई Cursor hovering गरी त्यसको आधिकारिकताको खोजविन तथा पहिचान गर्ने ।

(ख) टेलिफोन/मोवाइल वार्ता (Vishing)

१. सामान्यतया फोनमा संवेदनशील जानकारी प्रदान नगर्ने ।

२. उपहार(Gift)/चिठ्ठा (Lottery)/Working Visa बहाना फोन गर्नेलाई आफ्नो व्यक्तिगत विवरण नदिने।

३. Caller ID, Text Message Sender ID, Short Code उपर शंका लागेमा खोजविन तथा आधिकारिकता पहिचान गर्ने ।

४. फोन गर्नेको नाम, संगठनात्मक एकाई वा बाह्य कम्पनीको नाम शंका लागेमा केही समय लिई खोजविन तथा आधिकारिकता पहिचान गरेर मात्र आफ्नो विवरण पठाउने।

(ग) पेन ड्राइभ (USB Sticks)

१. पेन ड्राइभ (USB Sticks) मा Virus, Key loggers, Trojans, Ransomware जस्ता Malicious Software राखी हमला गर्न सक्ने भएकोले उक्त पेन ड्राइभ (USB Sticks) लाई Virus Scan गरेर मात्र प्रयोग गर्ने ।

२. अति महत्वपूर्ण पूर्वाधारहरु(Critical Infrastructures e.g. Server) मा सामन्यतया पेन ड्राइभ (USB Sticks) को प्रयोग नगर्ने ।

३. कुनै अपरिचित पेन ड्राइभ (USB Sticks) फेला परेमा त्यसलाई आफ्नो कम्प्यूटरमा प्रयोग नगर्ने, पेन ड्राइभ (USB Sticks) को फाइल (Contents) नखोल्ने ।

(घ) वेभसाइट (Internet freebies)

१. आधिकारिक वेभसाइटको पहिचान गरेर मात्र आफ्नो व्यक्तिगत विवरण प्रदान गर्ने ।

२. Cracked/Pirated Software Download गरी प्रयोग नगर्ने ।

३. असुरक्षित वेभसाइटहरु जस्तैः eMule, BitTorrent, Ares, etc. प्रयोग नगर्ने|

४. सितैमा विभिन्न offer हरु जस्तै movies, songs, music video, software, books etc. उपलब्ध गराउने असुरक्षित वेभसाइट (Internet freebies) प्रयोग नगर्ने ।

(ङ) भौतिक पहुँच (Physical impersonation)

१. कार्यस्थलको कम्प्युटर Password and Physical Lock गरेर राख्ने ।

२. कुनै पनि व्यक्तिलाई Access दिनु अगाडि त्यस व्यक्तिको सही पहिचान गर्ने ।

३. उचित सूरक्षागार्ड को व्यवस्था गरौ ।

(च) इलेट्रोनिक फोहोर डिस्पोजल (Electronics Waste disposal)

१. काम नलाग्ने इलेट्रोनिक सामग्रीहरुमा पनि संवेदनशील विवरणहरु हुन सक्ने भएकोले उक्त सामग्रीहरुलाई जथाभावी डिस्पोज नगर्ने । संवेदनशील विवरणहरुलाई नष्ट गरेर मात्र डिस्पोज गर्ने ।

२. म्याद सकिएको इलेट्रोनिक कार्डहरू (जस्तै आईडी कार्डहरू, एटीएम कार्डहरू, Access कार्डहरू) डिस्पोज गर्नु अघि उक्त कार्डहरुबाट कुनै पनि विवरण निकाल्न नमिल्ने गरी डिस्पोज गर्ने ।

३. काम नलाग्ने हार्ड डिस्क, पेन ड्राइभ, मेमोरी स्टिकहरू तथा USB फ्ल्यास ड्राईभहरूमा रहेको इलेक्ट्रॉनिक डाटा नष्ट गरेर मात्र डिस्पोज गर्ने ।

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