मितिः २०७८/०४/१५ (30 July, 2021)

साइबर सुरक्षाका लागि जनहितमा जारी सन्देश

म्यान इन द मिडल आक्रमण (Man in the Middle Attack: MITM) संग सम्बन्धितः

(१) म्यान इन द मिडल अट्याक के हो ?

म्यान-इन-द-मिडल अट्याकमा Sender तथा Receiver को विचमा तेश्रो पक्ष (hacker) ले प्रवेश गरी Sender को सबै Message (E.g. Password, Personally Identifiable Information, Credit Card number, Conversation etc.) प्राप्त गर्ने र सोलाई आफ्नो अनुकुल परिवर्तन गरेर Receiver लाई पठाइदिने गर्दछ । साथै, Receiver वाट प्राप्त भएको Message लाई पनि आफ्नो अनुकुल परिवर्तन गरी Sender लाई पठाइदिने गर्दछ । अर्थात, तेश्रो पक्ष (Hacker) ले Sender र Receiver वीचको सबै Message हरु प्राप्त गर्न र आफ्नो अनुकुल परिवर्तन गरी दुरुपयोग पनि गर्न सक्छ ।

(२) म्यान इन द मिडल अट्याकले कसरी काम गर्छ?

म्यान इन मिडल अट्याक दुई चरणमा हुने गर्छन।

क) **पहिलो चरणः** यस चरणमा साईबर अपराधी म्यान इन मिडल अटयाकको लागि इन्टरनेट ट्राफिकलाई गन्तव्यमा पुग्नु भन्दा पहिले प्राप्त गर्दछ, जसलाई Interception भनिन्छ । यो Interception कार्य पूरा गर्न साईबर अपराधीले IP Spoofing, ARP Spoofing, DNS Spoofing आदि तरिकाहरु अपनाउने गर्छन ।

ख) **दोस्रो चरणः** पहिलो चरणमा साईबर अपराधीले Interception कार्य पूरा गर्न सफल भए पछी उक्त Intercepted Traffic लाई दोस्रो चरणमा HTTPS

Spoofing, SSL Beast, SSL Hijacking, SSL Stripping लगायतका विधिहरुको प्रयोग गरी traffic को Original Content प्राप्त गर्दछ ।

(३) म्यान इन द मिडल अट्याकबाट कसरी बच्ने ?

म्यान-इन-द-मिडल अट्याकबाट बच्न निम्न उपायहरु अपनाऔ :-

१. आफ्नो डाटालाई सूरक्षित साथ स्थानान्तरण (Transfer) गर्न डाटालाई Secure Channel मार्फत Encrypt गरी पठाऔं ।
२. आफ्नो कम्प्यूटर/ल्याप्टप/मोबाइल तथा Network मा Firewall/IPS/IDS को प्रयोग गरौं ।
३. असुरक्षित सार्वजिनक वाईफाईको प्रयोग नगरौं । घरको वाईफाईमा समेत WPA2/3 को mode मा प्रयोग गरौं । साथै WPS Disable गरेर राखौं ।
४. Browser मा Force TLS (स्वतः रुपमा HTTPS प्रयोग हुने गरी) Plugin को प्रयोग गरेर मात्र अनलाइन कारोवार गरौं ।
५. सुरक्षित इमेलको लागि SSL/TLS/PGP/GPG encryption को Setting राखी प्रयोग गरौं ।
६. HTTPS वा Lock Icon सहित URL भएको वेबसाइटको प्रयोग गरौं ।
७. आफ्नो Software (Operating System, Application Software, Browser) लाई निरन्तर Update गरौं ।
८. आफ्नो कम्प्यूटर/ल्याप्टप/मोबाइल उपकरणमा मालवेयरको क्रियाकलाप अथवा Malicious Activities हुन नदिन Reputed Antivirus को प्रयोग गरौं ।
९. असुरक्षित सोफ्टवेयर, एप्स, फ्रीवेयर download नगरौं । साथै unencrypted/plain text messaging गर्ने एप्सको प्रयोग नगरौं ।
१०. इमेलबाट आफ्नो Password, OTP, Bank Account Number, PIN code जस्ता विवरणहरु नपठाऔं ।

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