मितिः २०७८/०४/०१ (16th July, 2021)

साइबर सुरक्षाका लागि जनहितमा जारी सन्देश

फारमिंग आक्रमण (Pharming Attack) संग सम्बन्धित :

क) फारमिंग आक्रमण (Pharming Attack) के हो ?

फारमिंग आक्रमण (Pharming Attack) एक प्रकारको अनलाइन ठगी (Online Fraud) हो जसमा साइबर अपराधीहरु (Pharmers/Cyber Criminals) ले प्रयोगकर्ताको कम्प्युटर तथा सर्भर (Server) मा Malicious Code install गरी प्रयोगकर्तालाई थाहै नदिई हेर्न खोजेको Website को **IP Address परिवर्तन** (Computer Local Host File वा DNS Cache Corruption/ DNS server Poisoning) गरी कुनै Click विना नै प्रयोगकर्तालाई Fake/Bogus/Fraudulent Website मा स्वतः निर्देशित (Auto-direct) गराई उक्त Fake/Bogus/Fraudulent Website को माध्यमबाट प्रयोगकर्ताको व्यक्तिगत संवेदनशील विवरणहरु जस्तै PIN Code, Payment Card Details, Password आदि प्राप्त गर्ने गर्दछन । तत्पश्चात् अपराधीहरुले उक्त व्यक्तिगत विवरण पासवर्ड तथा पिन कोड प्रयोग गरी वित्तीय ठगी (Financial Fraud) अर्थात रकम तथा व्यक्तिगत विवरण चोर्ने गर्दछन ।

ख) फारमिंग आक्रमण (Pharming Attack) भएको कसरी थाहा पाउने ?

- यदि हेर्न खोजिएको वेबसाइटमा https को सट्टा http देखियो भने,
- यदि वेबसाइटमा अस्वभाविक त्रुटीहरु (जस्तैः spelling error, unfamiliar font or color) देखिने, वास्तविक भन्दा भिन्न लाग्ने, वैध (legitimate) साइट जस्तो नदेखिने भयो भने

फारमिंग आक्रमण (Pharming Attack) भएको हुन सक्छ ।

ग) फारमिंग आक्रमण (Pharming Attack) बाट कसरी बच्ने?

फारमिंग आक्रमण (Pharming Attack) बाट बच्न निम्न उपायहरु अपनाऔं।

१. Https भएको secure वेबसाइटमा मात्र Visit गरौं । जस्तैः **https**://www.nta.gov.np

२. विश्वासिलो तथा सुरक्षित (Trusted and Safe) Browser (जस्तै Mozilla Firefox etc.) को प्रयोग गरौं ।

३. शंकास्पद वेबसाइटको Visit नगरौं ।

४. कुनै पनि वेबसाइट Navigate गर्दा उक्त वेबसाइट Completely load हुन दिई उक्त वेबसाइटको URL (जस्तैः https://nta.gov.np/) मा spelling error/swapping letters भए नभएको कुरा ध्यान पुर्वक जांच गरौं ।

५. कारोवार गर्नु भन्दा अगाडि आधिकारिक वेभसाइट भए/नभएको पहिचान गरेर मात्र कारोवार गरौं ।

६. Consumer-grade Routers र Access Points (AP) मा रहेको default password लाई परिवर्तन गरौं ।

७. प्राय अपराधीहरु (Pharmers) ले सस्तो अथवा offer दिने जस्ता लोभ्याउने Commercial fake Site प्रयोग गर्ने भएकोले अधिकारिक Commercial Site मा मात्र आफ्नो व्यक्तिगत संवेदनशील विवरण share गरौ र त्यस्ता अधिकारिक Commercial Site बाट मात्र अनलाइन सपिंग/कारोवार गरौं ।

८. Secure Browsing को लागि Reputed DNS Servers भएको VPN सेवा मात्र प्रयोग गरौं ।

९. अपरिचित व्यक्तिबाट प्राप्त इमेलको Attachment तथा link लाई Click नगरौं |

१०. Two Factor Authentication वा Multi Factor Authentication को प्रयोग गरौं|

११. आधिकारिक तथा Reputed Anti-virus/Anti-malware तथा Firewall सफ्टवेयरको प्रयोग गरौं|

Nepal Telecommunications Authority (NTA)

Cyber Security Task Force (NTACERT)

Jamal, Kathmandu, Nepal

Email: cert@nta.gov.np, Website: www.nta.gov.np