वित्तीय जानकारी इकाई-नेपाल

काठमाडौं

आम नागरिक तथा वित्तीय सेवा प्रदायकहरूका लागि अनलाइन ठगी (Online Scams/Fraud) सम्बन्धी विशेष सतर्कताको सूचना (Advisory)

१. उद्देश्य

वित्तीय जानकारी इकाई (FIU-Nepal) ले बैंकिङ कारोबार विश्लेषणको क्रममा अनलाइन ठगीका घटनाहरूमा वृद्धि भएको पाएको छ। नेपालीहरूको महान चाड दसैं, तिहार, नेपाल संवत् तथा छठ जस्ता उत्सवहरूको समयमा अनलाइन अकाउन्ट सिर्जना, डिजिटल बैंकिङ, इ-कमर्स (Online Shopping) र डिजिटल भुक्तानीको प्रयोग व्यापक रूपमा बढ्ने हुँदा यसै मौकाको फाइदा उठाई आपराधिक मानसिकता भएका व्यक्ति तथा समूहहरूले सर्वसाधारण र वित्तीय प्रणालीलाई लक्षित गरी विभिन्न प्रकारका डिजिटल तथा वित्तीय ठगी (Online Frauds) गर्ने जोखिम उच्च देखिएको छ। यस सूचनाको मुख्य उद्देश्य आम उपभोक्ता, बैंक तथा वित्तीय संस्थाहरू र अनलाइन सेवा प्रदायकहरूलाई सम्भावित जोखिमहरू पहिचान गर्न र त्यस्ता ठगीबाट बच्नका लागि मार्गदर्शन प्रदान गर्नु रहेको छ।

२. चाडपर्वमा देखिन सक्ने प्रमुख अनलाइन ठगीका प्रकारहरू

- **नक्कली चाडपर्व अफर र चिट्ठा (Fake Festival Offers & Lotteries)**
  "दसै धमाका", "तिहार छठ बम्पर उपहार" वा "तपाईंले आकर्षक उपहार जित्नुभयो" भन्दै सामाजिक सञ्जाल (Facebook, WhatsApp, Viber, Messenger आदि) मा नक्कली लिङ्कहरू पठाउने र सेवा शुल्क वा करको नाममा अग्रिम रकम माग गर्ने।

- **फिसिङ र बैंकिङ ठगी (Phishing & Banking Scams)**
  बैंक वा डिजिटल वालेटको नक्कली वेबसाइट/वेबपेज बनाएर ग्राहकलाई केवाइसी (KYC) अपडेट नगरे अकाउन्ट ब्लक हुने डर देखाई पासवर्ड, ओटिपी (OTP) र व्यक्तिगत विवरणहरू चोरी गरी बैंक तथा वित्तीय संस्थामा रहेको खाताबाट रकम ठगी गर्ने।

- **नक्कली अनलाइन सपिङ पेजहरू (Fake e–commerce Pages)**
  सामाजिक सञ्जालमा ब्रान्डेड सामानहरूको तस्बिर राखी भारी छुटको विज्ञापन गर्ने र अग्रिम भुक्तानी (Advance Payment) माग गर्ने। अग्रिम भुक्तानी पश्चात सामान नपठाई ग्राहकलाई ब्लक गरी ठगी गर्ने।

- **नक्कली पहिचान र कागजपत्रको दुरुपयोग (Identity Theft & Document Fraud)**
  सामाजिक संजालहरूमा अरू कसैको नागरिकता, फोटो वा कीर्ते (Photo–shopped) गरिएका कागजपत्रहरू राखी नक्कली खाता (जस्तै fake facebook account) खोलेर आपराधिक गतिविधि सञ्चालन गर्ने।

३. आम नागरिक तथा उपभोक्ताहरूका लागि सुरक्षित रहने उपायहरू:

- **ओटिपी र पासवर्ड गोप्य राख्नुहोस्:** आफ्नो मोबाइलमा आउने ओटिपी (OTP), बैंक खाताको पासवर्ड, वा वालेटको पिन (PIN) कसैलाई पनि सेयर नगर्नुहोस् ।
- **नक्कली लिङ्कहरू क्लिक नगर्नुहोस्:** सामाजिक सञ्जालमा आउने "फ्री रिचार्ज", "चिट्ठा पर्यो" वा "नक्कली उपहार" दाबी गरिएका शङ्कास्पद लिङ्कहरू (Links) खोल्दै नखोल्नुहोस् ।
- **अग्रिम भुक्तानी गर्दा सचेत रहनुहोस्:** अनलाइनबाट सामान खरिद गर्दा आधिकारिक र विश्वसनीय वेबसाइटहरू मात्र प्रयोग गर्नुहोस् । सामाजिक सञ्जालका नयाँ वा अपरिचित पेजहरूबाट सामान किन्दा सकेसम्म 'पे अन डेलिभरी' (Pay on Delivery) को विकल्प रोज्नुहोस् ।
- **यूआरएल (URL) को आधिकारिकता जाँच गर्नुहोस्:** डिजिटल भुक्तानी गर्नु अघि सम्बन्धित वेबसाइटको वेब ठेगाना (URL) सही छ कि छैन सुनिश्चित गर्नुहोस् ।

४. बैंक तथा वित्तीय संस्था र डिजिटल सेवा प्रदायकहरूका लागि सुझाव

- **सशक्त ग्राहक पहिचान (Robust KYC Verification):** डिजिटल माध्यमबाट खाता खोल्दा पेस गरिएका परिचयको विवरण (Identification details) verify गर्नुहोस् ।
- **शङ्कास्पद ठेगाना र विवरणको निगरानी:** एउटै ठेगाना वा एउटै मोबाइल नम्बर प्रयोग गरेर फरक-फरक नाममा धेरै खाताहरू खोलिएका छन् भने त्यस्ता खातामा हुने कारोवारलाई लामो सार्वजनिक विदाको समयमा निरन्तर अनुगमन र निगरानी हुनेगरी 'रेड फ्ल्याग' (Red Flag) दिने संयन्त्र सुचारु राख्ने ।
- **प्रविधिको प्रयोग:** ठूलो मात्रामा हुने शङ्कास्पद कारोबार, अस्वाभाविक नगद स्थानान्तरण, वा छोटो समयमा धेरै खाताहरूमा पैसा पठाउने (Layering) प्रवृत्ति पत्ता लगाउन निगरानी प्रणाली (Transaction Monitoring System) चुस्त राख्नुहोस् ।
- **कर्मचारी तथा ग्राहक सचेतना:** चाडपर्व सुरु हुनु अगावै आफ्ना फ्रन्टलाइन कर्मचारीहरूलाई सम्भावित ठगीका ढाँचाहरू पहिचान गर्ने तालिम दिनुहोस् र सामाजिक सञ्जाल एवं एसएमएस (SMS) मार्फत ग्राहकहरूलाई सचेत गराउनुहोस् ।

५. ठगी वा शङ्कास्पद गतिविधि भएमा कहाँ सम्पर्क गर्ने?

यदि तपाईं कुनै पनि प्रकारको अनलाइन ठगीमा पर्नुभएको छ, वा तपाईंको परिचय दुरुपयोग भएको शङ्का लागेमा ढिला नगरी तत्काल सम्बन्धित बैंक तथा वित्तीय संस्था वा डिजिटल वालेट प्रदायकको ग्राहक सेवा केन्द्र (आफ्नो खाता वा वालेट तत्काल ब्लक गर्नका लागि), नेपाल प्रहरी साइबर ब्यूरो, नजिकैको जिल्ला प्रहरी परिसर वा प्रहरी कार्यालयमा जानकारी गराउनुहोस् ।

***