राजू और चालीस चोर

वित्तीय जालसाजों की कार्यप्रणाली पर एक पुस्तिका

भारतीय रिज़र्व बैंक

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA


भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

प्रस्तावना

भारतीय वित्तीय प्रणाली की तकनीकी और डिजिटल क्रांति के दौर में भारतीय रिजर्व बैंक (बैंक) जनसामान्य के मध्य 'निवारक वित्तीय जागरूकता' के प्रसार की आवश्यकता को महसूस करता है, विशेष रूप से डिजिटल वित्तीय विश्व में प्रवेश करने वाले नए लोगों के लिए, जो ऑनलाइन धोखाधड़ी लेनदेन की बारीकियों से भलीभांति परिचित नहीं हैं और डिजिटल धोखाधड़ी के शिकार हो सकते हैं। बैंक ने मार्च 2022 में अपनी ग्राहक जागरूकता पहल के भाग के रूप में धोखेबाजों द्वारा उपयोग की जाने वाली सामान्य कार्यप्रणाली और विभिन्न वित्तीय लेनदेन करते समय बरती जाने वाली सावधानियों पर 'बी (ए) वेयर' नामक पुस्तिका प्रकाशित की थी। पुस्तिका को जनसमान्य और अन्य हितधारकों से सकारात्मक प्रतिक्रिया प्राप्त हुई।

विभिन्न शैक्षिक स्तर वाले सभी आयु वर्ग के व्यक्तियों तथा ग्राहकों जिसमें स्कूली बच्चे, युवा, वयस्क, अर्ध-साक्षर और वरिष्ठ नागरिक आदि शामिल हैं, के बीच जागरूकता उत्पन्न करने हेतु बी (ए) वेयर की अवधारणा को सचित्र रूप में विस्तारित करते हुए 'राजू और चालीस चोर' नामक एक अन्य पुस्तिका जारी की गई है। पुस्तिका में धोखाधड़ी वाली वित्तीय घटनाओं में देखी गई कार्यप्रणाली का एक स्पष्ट चित्रात्मक वर्णन है। इसका उद्देश्य समान्य गलतियों से सीखने में मदद करना और अपनी मेहनत की कमाई और खुद को धोखेबाजों से सुरक्षित रखने के लिए कदम उठाना है।

जैसा कि नाम से ही स्पष्ट है 'राजू और चालीस चोर' पुस्तिका में ऐसी चालीस कहानियां शामिल हैं, जो आरबीआई लोकपाल और उपभोक्ता शिक्षण और संरक्षण विभाग (सीईपीडी) सहित बैंक को सूचित की गई धोखाधड़ी की घटनाओं की झलक दिखाती है और इस प्रकार की घटनाओं से बचाव के लिए क्या करें और क्या न करें के बारे में सरल उपाय प्रदान करती है। राजू एक भोला-भाला नागरिक है जो इन कहानियों में वरिष्ठ नागरिक, किसान या एक खुश-मिज़ाज व्यक्ति आदि विभिन्न पात्रों / भूमिकाओं में नजर आता है ताकि विभिन्न हितधारक जीवन के विभिन्न क्षेत्रों में उसके रूप में स्वयं को पहचान सकें।

इस पुस्तिका को तैयार करने में आरबीआई लोकपाल, मुंबई -II, महाराष्ट्र और गोवा की टीम द्वारा किए गए रचनात्मक प्रयासों को कृतज्ञतापूर्वक स्वीकार किया जाता है।

हम पाठकों से आग्रह करते हैं कि वे धोखेबाजों द्वारा इस्तेमाल की जाने वाली ऐसी कार्यप्रणाली से स्वयं को अवगत कराएं और हमारे आसपास के लोगों को शिक्षित कर इस प्रकार की जागरूकता का प्रचार-प्रसार करें।

पाठकों से अनुरोध है कि वे अपनी प्रतिक्रिया / सुझावों को cgmcepd@rbi.org.in पर साझा करें।

सावधान रहें और जागरूक रहें!

क्रम-सूची

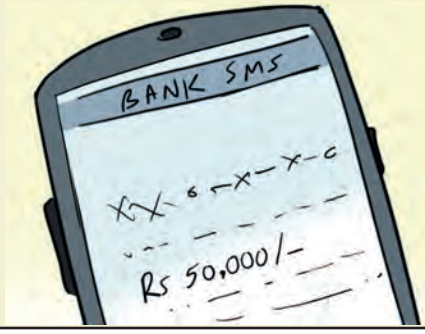
१. फ़िशिंग लिंक के माध्यम से धोखाधड़ी

क्या करें:

✔ जब भी आपको केवाईसी को अपडेट करने का अनुरोध करने वाले कॉल,लिंक या एसएमएस अज्ञात स्रोतों से प्राप्त हों,तो हमेशा अपनी होम ब्रांच या अपने रिलेशनशिप मैनेजर के माध्यम से केवाईसी स्थिति की जांच करें।

✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

कुछ समय बाद, राजू को उसके फोन पर मैसेज आया जिसमें कहा गया था
कि उसके खाते से **50,000 /-** रुपये डेबिट हो गए हैं।



राजू ने तुरंत उस व्यक्ति को फोन किया,लेकिन उसने कॉल का जवाब नहीं दिया।
राजू को अहसास हुआ कि वह व्यक्ति धोखेबाज था और राजू को उसके साथ कोई व्यक्तिगत ब्योरे साझा नहीं करना चाहिए था।

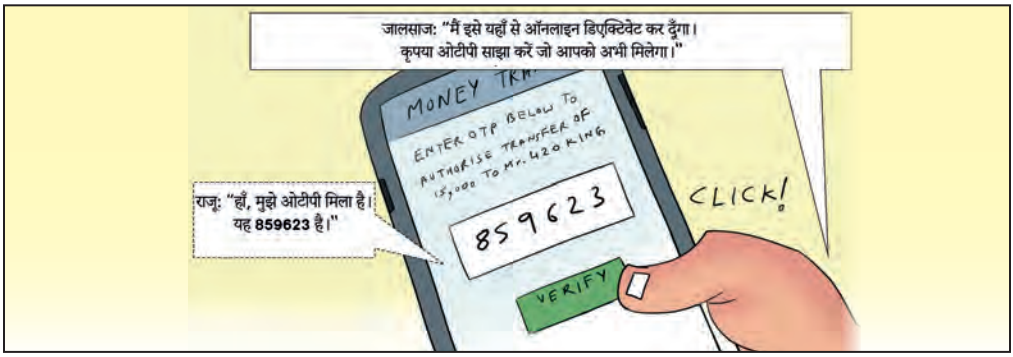
क्या न करें:

- ✕ फोन / ईमेल पर प्राप्त अज्ञात/अवांछित लिंक्स को सत्यापित किए बिना क्लिक न करें।
- ✕ अपनी गोपनीय जानकारी अजनबियों के साथ साझा न करें।

२. विशिंग कॉल्स

क्या करें:

- ✔ किसी पर भी भरोसा करने से पहले किसी भी मुद्दे के बारे में हमेशा अपने रिलेशनशिप मैनेजर या बैंक शाखा से क्रॉस-चेक करें।
- ✔ ओटीपी आपके सुरक्षित धन की चाबी की तरह है, इसलिए इसे धोखेबाजों से हमेशा दूर रखें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।



क्या न करें:

× गोपनीय जानकारी/ब्यौरे मांगने वाले अज्ञात कॉलर्स जो बैंकों की ओर से बोलने का दावा करते हैं उन पर भरोसा न करें। बैंक फोन पर इस तरह की जानकारी नहीं मांगते।

× डिजिटल दुनिया में अजनबियों पर आसानी से भरोसा न करें और अनजान नंबरों से प्राप्त कॉल का जवाब देते समय सतर्क रहें।

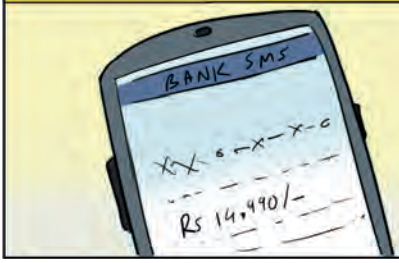
३. ऑनलाइन मार्केटप्लेस का उपयोग करके धोखाधड़ी

क्या करें:

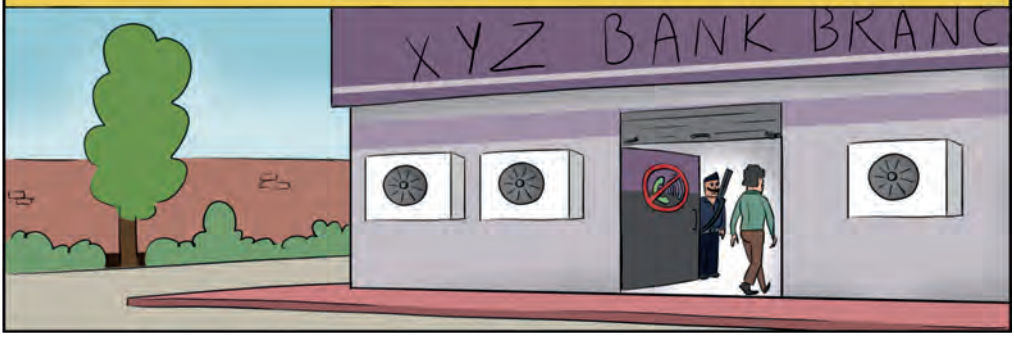
- ✔ हमेशा याद रखें, UPI पिन केवल भुगतान करने के लिए आवश्यक है और कोई भुगतान प्राप्त करने के लिए आवश्यक नहीं है।
- ✔ भुगतान शुरू करने से पहले हमेशा यूपीआई एप्लिकेशन में मोबाइल नंबर सत्यापित करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

(तब धोखेबाज ने राजू को भुगतान करने के बजाय 14,990/-
रुपये का भुगतान प्राप्त करने के लिए एक upi अनुरोध भेजा।)

राजू ने तुरंत पिन डाला,
और उसके खाते से 14,990/- रुपये काटे गए।



यह अहसास होते ही कि उसे धोखा दिया गया है, राजू ने तुरंत ही बैंक शाखा में संपर्क किया और उसी दिन शिकायत दर्ज की।

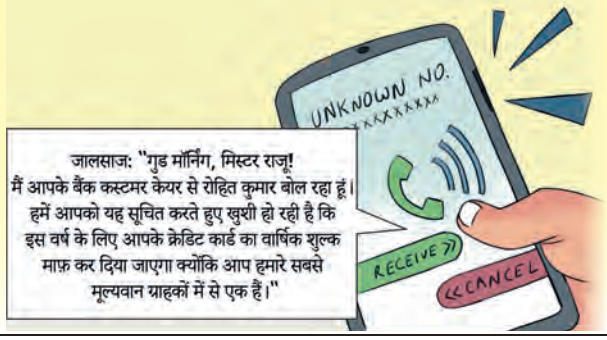


क्या न करें:

- ✗ अजनबियों के साथ ओटीपी या गोपनीय खाता ब्यौरे साझा न करें।
- ✗ किसी अन्य व्यक्ति से भुगतान प्राप्त करने के लिए यूपीआई पिन दर्ज न करें।

४. क्रेडिट कार्ड वार्षिक शुल्क छूट- नकली ऑफर

एक दिन राजू को एक अनजान नंबर से कॉल आया।



क्या करें:

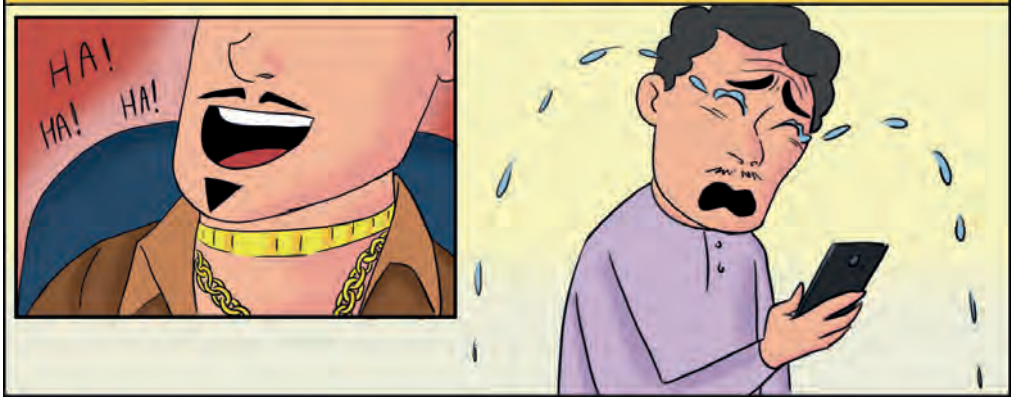
- ✔ आपके बैंक से होने का दावा करने वाले अज्ञात नंबरों से प्राप्त कॉल का जवाब देते समय सतर्क रहें।
- ✔ धोखाधड़ी का पता चलने पर तुरंत अपनी होम ब्रांच को रिपोर्ट करें।
- ✔ आगे वित्तीय नुकसान को रोकने के लिए अपने कार्ड को ब्लॉक करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

राजू ने सोचा कि चूंकि कॉल करने वाले को पहले से ही उसके कार्ड का ब्यौरे पता थे,
इसलिए कॉल वास्तविक होनी चाहिए। उसने तुरंत ओटीपी को जालसाज के साथ साझा कर दिया ।

कॉल डिस्कनेक्ट हो गया ।
जल्द ही, राजू को एक एसएमएस मिला जिसमें कहा गया था कि
उसके क्रेडिट कार्ड खाते से 12,000/- रुपये डेबिट हो गए हैं।

राजू ने तुरंत जालसाज को फोन किया, लेकिन उसका फोन स्विच ऑफ था।

राजू को अहसास हुआ कि वह व्यक्ति धोखेबाज था,
और उसे उसके साथ ओटीपी साझा नहीं करना चाहिए था।



क्या न करें:

× अपना ओटीपी किसी के साथ साझा न करें। धोखेबाज आपके खाते का ब्यौरे एकत्र करने में सक्षम हो सकते हैं, लेकिन लेनदेन केवल तभी हो सकता है जब आप आपके फोन पर भेजे गए गोपनीय ओटीपी को साझा करते हैं।

५. एटीएम कार्ड स्किमिंग फ्रॉड

क्या करें:

- ✔ एटीएम मशीनों में कोई भी ट्रांज़ैक्शन शुरू करने से पहले, सुनिश्चित करें कि स्किमिंग डिवाइस मौजूद नहीं हैं। धोखेबाजों द्वारा स्किमिंग उपकरणों को कार्ड इंसर्शन स्लॉट के साथ ओवरलैप करके छिपा दिया जाता है।
- ✔ कार्ड क्लोनिंग की घटना के 3 दिनों के भीतर बैंक को धोखाधड़ी की रिपोर्ट करें। सभी ट्रांज़ैक्शन को सत्यापित करने के लिए अपने पहले किए गए लेन-देन की बार-बार जांच करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (https://cybercrime.gov.in) पर करें।

क्या न करें:

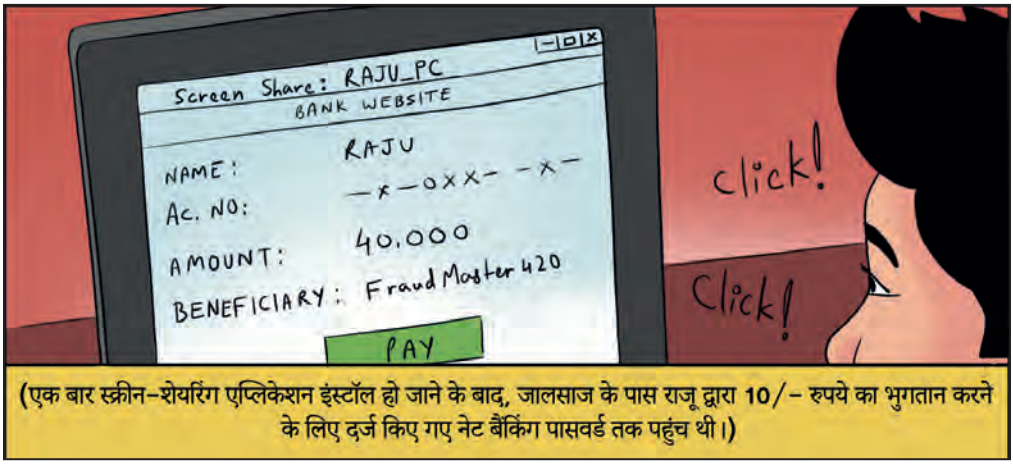
× एटीएम परिसर में आपके एवज में लेन-देन(ट्रांज़ेक्शन) करने के लिए अपना एटीएम कार्ड किसी को न दें।

इस प्रकार की सोशल इंजीनियरिंग का उपयोग वरिष्ठ नागरिकों / अर्ध-शिक्षित व्यक्तियों को लक्षित करने के लिए किया जा रहा है, जिन्हें एटीएम का प्रयोग करने में कठिनाई होती है।

६. स्क्रीन शेयरिंग ऐप/रिमोट एक्सेस फ्रॉड का उपयोग कर धोखाधड़ी

क्या करें:

- ✔ संबंधित संस्था की आधिकारिक वेबसाइट पर प्रस्ताव की प्रामाणिकता सत्यापित करें।
- ✔ अपने मोबाइल फोन में एंटीवायरस / स्पैम ब्लॉकिंग सॉफ्टवेयर इंस्टॉल करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।



क्या न करें:

× एसएमएस, ईमेल या इंस्टेंट मैसेजिंग एप्लिकेशन के माध्यम से भेजे गए लिंक पर कोई भी एप्लिकेशन डाउनलोड न करें।

× किसी अज्ञात व्यक्ति द्वारा साझा किए गए स्क्रीन-शेयरिंग एप्लिकेशन को डाउनलोड न करें। इन ऐप्स द्वारा उत्पन्न स्क्रीन शेयरिंग कोड अज्ञात व्यक्तियों के साथ साझा ना करें।

७. सिम स्वैप/सिम क्लोनिंग

क्या करें:

- ✔ अज्ञात कॉल करने वालों पर विश्वास करने के बजाय संदेह होने पर अपने दूरसंचार सेवा प्रदाता के साथ सिम कार्ड की स्थिति सत्यापित करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

(राजू कॉलर के साथ ब्यौरे साझा करता है।)

(जालसाज नए सिम का उपयोग कर बैंकिंग एप्लिकेशन के लिए यूज़र नेम पुनः प्राप्त करने के लिए 'फॉर्गॉट यूज़र नेम, 'पासवर्ड रीसेट करें' आदि जैसे विकल्पों का उपयोग करता है और सभी पैसे अपने खाते में स्थानांतरित कर देता है।)

कुछ मिनटों के बाद, जब राजू को अपने बैंक खाते से नकद डेबिट दिखाते हुए ईमेल प्राप्त हुए, तो उसने अपने बैंक खाते की शेष राशि की जाँच की। उसने देखा कि उसके खाते से कुछ अनधिकृत डेबिट किए गए थे, जिसके लिए उनके पंजीकृत मोबाइल नंबर पर कोई एसएमएस प्राप्त नहीं हुआ था क्योंकि फंड ट्रांसफर करने, ऑनलाइन खरीदारी करने के लिए सिम को कंप्रोमाइज़ किया गया था।

क्या न करें:

× अपना आधार नंबर और सिम नंबर जैसे गोपनीय ब्यौरे अज्ञात कॉल करने वालों के साथ साझा न करें।

८.सर्च इंजनों के माध्यम से प्राप्त रिज़ल्ट पर प्रमाणों के जोखिम से धोखाधड़ी

क्या करें:

- ✔ हमेशा सेवा प्रदाता की आधिकारिक वेबसाइट से ही संपर्क ब्योरे / ग्राहक सेवा नंबर आदि प्राप्त करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

राजू ने लिंक पर क्लिक किया और राशि की जांच किए बिना ओटीपी डाल कर भुगतान कर दिया।

क्या न करें:

× वेब सर्च इंजन से प्राप्त यादृच्छिक फोन नंबरों पर संपर्क न करें खास कर वित्तीय लेन-देन करने के लिए।

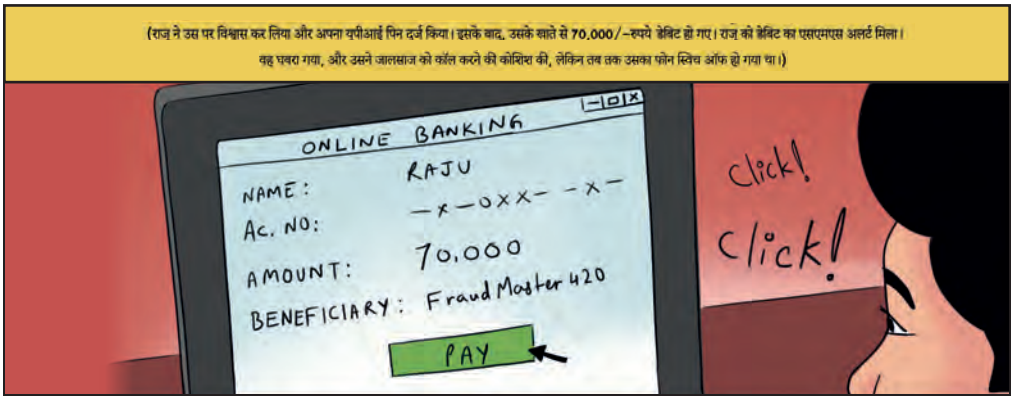
९.क्यूआर कोड स्कैन के माध्यम से धोखाधड़ी

राजू ने अपनी पुरानी कार को बेचने के लिए एक ऑनलाइन वेबसाइट पर पंजीकृत कराया।

कुछ ही घंटों में एक व्यक्ति (जालसाज) ने उससे संपर्क किया।

क्या करें:

- ✔ क्यूआर कोड का उपयोग करने से पहले उसे उपयोग करना सीख लें।
- ✔ ट्रांज़ेक्शन की सूचना तुरंत अपने बैंक को दें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।



क्या न करें:

× किसी अन्य व्यक्ति से पैसे प्राप्त करने के लिए अपना यूपीआई पिन दर्ज न करें। यूपीआई पिन केवल भुगतान करने के लिए आवश्यक है, धन प्राप्त करने के लिए नहीं।
× भुगतान प्राप्त करने के लिए कोई क्यूआर कोड स्कैन न करें। पैसे प्राप्त करने के लिए क्यूआर कोड को स्कैन करने की आवश्यकता नहीं होती, / बल्कि भुगतान भेजने के लिए होती है।

१०. सोशल मीडिया के माध्यम से प्रतिरूपण

क्या करें:

- ✔ भुगतान करने से पहले वास्तविक व्यक्ति को कॉल करके या प्रत्यक्ष मिलकर जांच करें।
- ✔ कोई भी भुगतान करने से पहले हमेशा खाते के ब्यौरे की जांच करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

क्या न करें:

- × अपनी व्यक्तिगत जानकारी जैसे मोबाइल नंबर, ईमेल आईडी और मित्र सूची को सब के लिए खुला न रखें।
- × उन लोगों के मित्रता अनुरोध स्वीकार न करें / फॉलो न करें जिनसे आप कभी व्यक्तिगत रूप से नहीं मिले हैं।

११. जूस जैकिंग - चार्जिंग केबल के माध्यम से डेटा की चोरी

क्या करें:

- ✔ किसी भी अनधिकृत पहुंच से बचाने के लिए अपने मोबाइल फोन पर एंटी-वायरस सॉफ़्टवेयर इन्स्टाल करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

चार्ज करते समय चार्जिंग केबल राजू के मोबाइल में वायरस इंजेक्ट कर देता है।

अगले कुछ दिनों के दौरान, जालसाज ने राजू द्वारा दर्ज किए गए सभी विवरणों को अपने मोबाइल पर कैप्चर कर लिया और महत्वपूर्ण बैंक क्रेडेंशियल जैसे यूज़र नेम, पासवर्ड आदि को प्राप्त कर लिया।

एक दिन, राजू को अपने बचत खाते में अनधिकृत निकासी का संकेत देने वाले एसएमएस / ईमेल प्राप्त होते हैं

और उन्हें ज्ञात होता है कि उनके खाते से कहीं छेड़छाड़ की गई है।

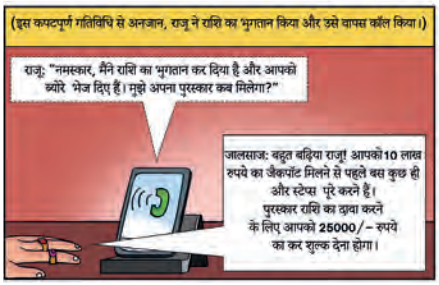
क्या न करें:

× अजनबियों द्वारा दिए गए / सार्वजनिक स्थानों पर उपलब्ध चार्जिंग अडैप्टर/ केबल का उपयोग न करें।

१२. लॉटरी धोखाधड़ी

राजू को एक ऑडियो संदेश मिला जिसमें कहा गया था कि उसने एबीसी जैकपॉट जीता है।

उत्साहित, राजू ने उस नंबर पर कॉल किया जो जैकपॉट संदेश में था
जिसमें एक सुपरस्टार द्वारा पुरस्कार पर बधाई देने वाला एक नकली वीडियो दिखाया गया था।
उसने दिए गए नंबर पर संपर्क किया।



क्या करें:

- ✔ किसी भी कंपनी या प्रबंधन टीम के सदस्यों के रूप में उन पर भरोसा करने से पहले अज्ञात नंबरों से प्राप्त संदेश को सत्यापित करें।
- ✔ ऐसे आयोजनों की आधिकारिक वेबसाइटों के साथ लॉटरी ऑफ़र को हमेशा सत्यापित करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

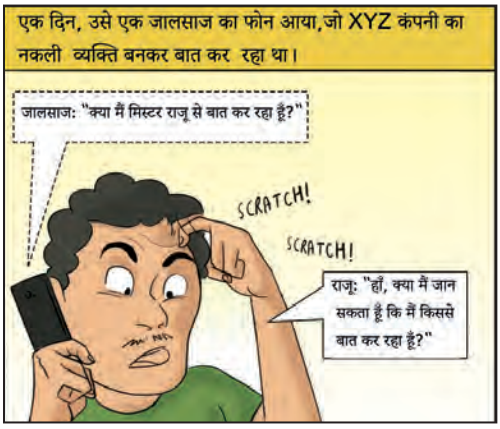
दुबारा बिना सोचे समझे राजू दुबारा भुगतान कर देता है।

.....बाद में, उसे अहसास होता है कि उसके साथ धोखा हुआ है।

क्या न करें:

× बहुत अधिक रिटर्न की उम्मीद में सत्यापन के बिना भुगतान न करें।

१३. ऑनलाइन नौकरी धोखाधड़ी



क्या करें:

- ✔ कोई भी पैसा देने से पहले कंपनी या भर्ती एजेंसियों की प्रामाणिकता सत्यापित करें।
  भर्ती एजेंसियां आमतौर पर काम दिलाने के लिए उम्मीदवारों से शुल्क नहीं लेती हैं।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

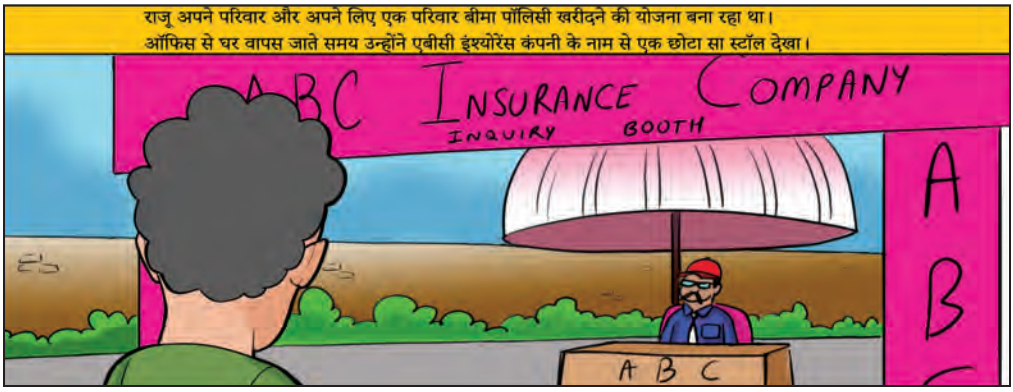
उत्साह से भरपूर राजू बताए गए खाते में 5,000/- रुपये का भुगतान करता है

(कई दिनों तक प्रतीक्षा करने के बावजूद, राजू को कोई लैपटॉप नहीं मिला। उसने नंबर पर कॉल करने की कोशिश की, लेकिन नंबर हमेशा बंद रहता था। उसने कंपनी का नाम ऑनलाइन खोजा लेकिन कुछ भी नहीं मिला। राजू को अंततः अहसास हुआ कि उसकी मेहनत की कमाई के साथ धोखाधड़ी की गई है।)

क्या न करें:

✕ नौकरी के झांसे में किसी को भुगतान न करें। एक वैध कंपनी नौकरी की पेशकश के लिए संभावित उम्मीदवार से कभी भी भुगतान नहीं मांगेगी।

१४. नकली खाता संख्या



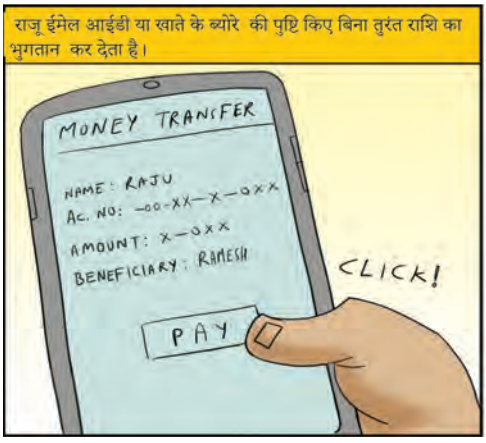
क्या करें

- ✔ किसी ज्ञात डेटाबेस पर किसी संगठन के क्रेडेंशियल्स को क्रॉस-चेक करके जाँचे कि क्या वे वास्तविक हैं।
- ✔ उत्पादों का लाभ उठाने के लिए हमेशा पंजीकृत कार्यालयों से संपर्क करें।
- ✔ राशि केवल खाता संख्या के आधार पर ही स्थानांतरित की जाती है।
- ✔ जालसाज कंपनी का असली नाम दे सकते हैं लेकिन खाता नंबर अपना दे सकते हैं, भुगतान करने से पहले हमेशा कंपनी के साथ खाता संख्या सत्यापित करें
- घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
- ✔ https://cybercrime.gov.in पर करें।

क्या न करें:

✕ कंपनी की प्रामाणिकता की पुष्टि किए बिना किसी को भुगतान न करें।

१५. ईमेल के माध्यम से धोखाधड़ी



क्या करें:

- ✔ प्राप्त ईमेल के आधार पर कोई भी भुगतान करने से पहले संबंधित व्यक्ति से सत्यापित करें।
- ✔ ईमेल आईडी सत्यापित करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

क्या न करें:

✕ यादृच्छिक ईमेल या समान दिखने वाली ईमेल आईडी से अनुरोध प्राप्त होने पर भुगतान न करें।

१६. मैसेज ऐप बैंकिंग फ्रॉड

क्या करें:

- ✔ आपके खाते का ब्योरा मांगने वाले अज्ञात नंबरों से प्राप्त कॉल का जवाब देते समय सतर्क रहें।
- ✔ धोखाधड़ी का पता चलने पर तुरंत अपनी होम ब्रांच को रिपोर्ट करें। आगे और वित्तीय नुकसान को रोकने के लिए अपने खाते को ब्लॉक करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

क्या न करें:

✗ आसान बैंकिंग सेवाओं की पेशकश करने वाले और मैसेजिंग ऐप्स के माध्यम से टेक्स्ट भेजने वाले अनजान कॉलर्स पर भरोसा न करें।

✗ कार्ड ब्योरे और ओटीपी किसी के साथ साझा न करें।

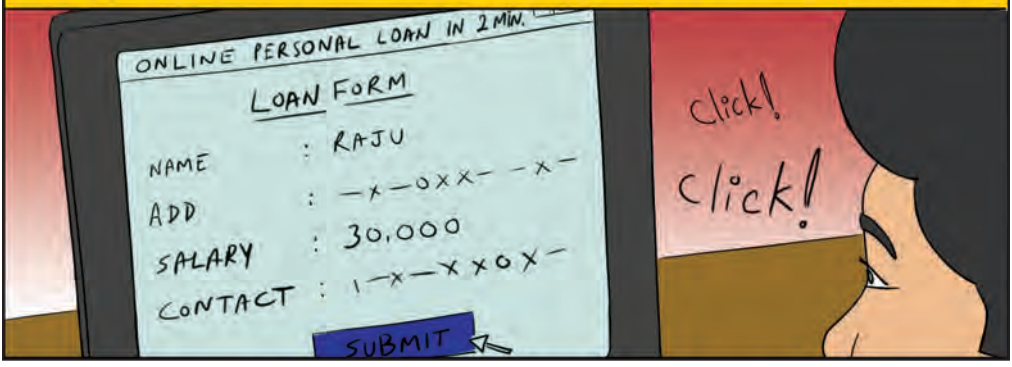
१७. चोरी के दस्तावेज़ों के साथ धोखाधड़ी वाले ऋण

क्या करें:

- ✔ दस्तावेजों को प्रस्तुत करते समय हमेशा अंतिम उपयोग की निगरानी करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

राजू अपने सभी विवरणों के साथ ऋण आवेदन पत्र भरता है और प्रतिनिधि को रद्द चेक प्रदान करता है।

जालसाज राजू के दस्तावेजों का उपयोग करके ऋण के लिए आवेदन करता है लेकिन ऋण के संवितरण के लिए अपना खाता नंबर देता है।



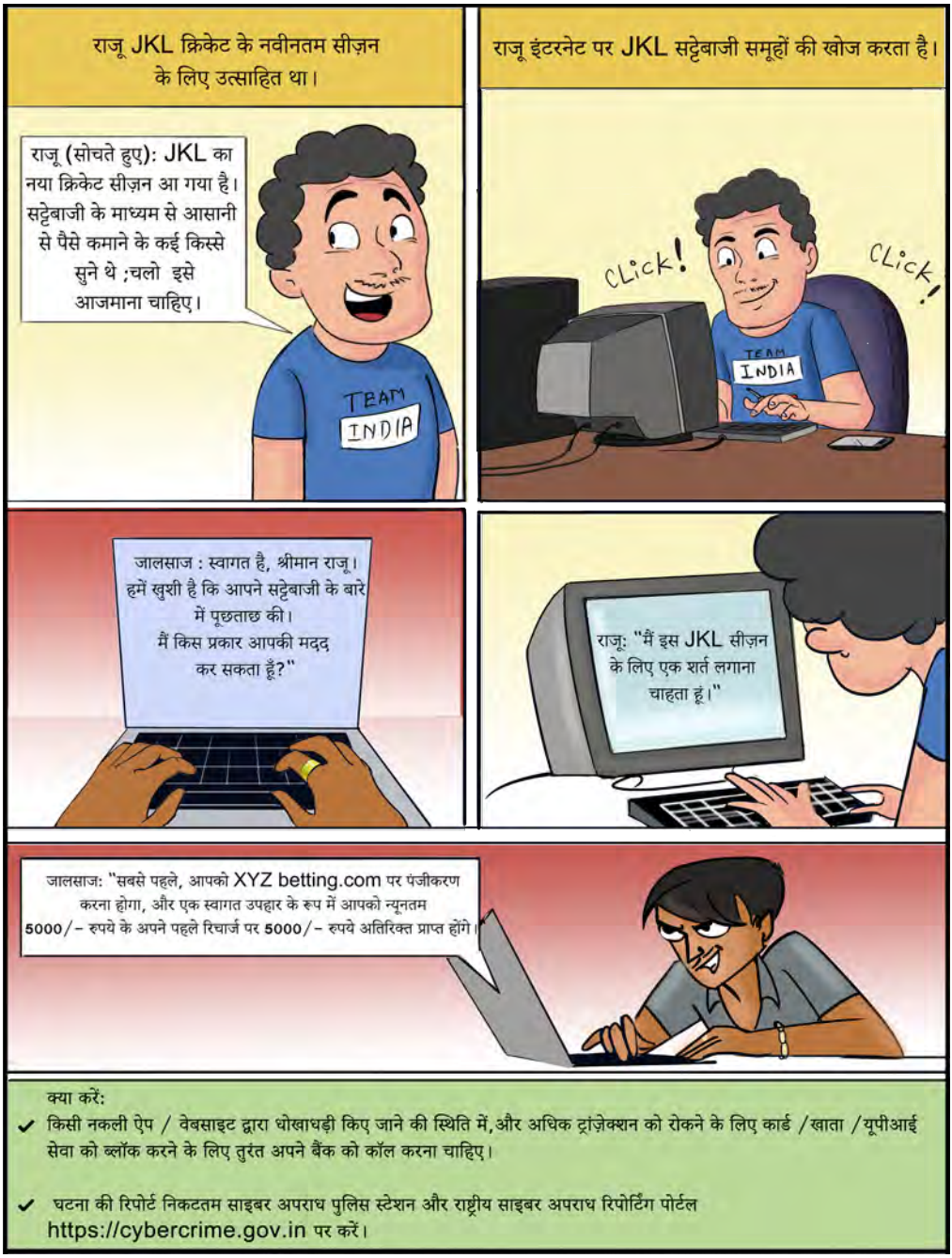
राजू: एक महीने के बाद, राजू को एक पत्र प्राप्त होता है जिसमें सूचित किया जाता है कि ऋण के लिए 10,000/- रुपये बकाया हैं.....

चौंकते हुए, राजू ने बैंक को फोन करके सूचित किया कि उसने कोई ऋण नहीं लिया है। लेकिन बैंक उसके द्वारा भरा गया ऋण आवेदन पत्र दिखाता है

क्या न करें:

✕ कभी भी अपना गोपनीय ब्योरा जैसे कि आधार नंबर, पैन नंबर, चेक बुक या चेक अज्ञात व्यक्तियों के साथ साझा न करें।

१८. सट्टेबाजी घोटाला


राजू JKL क्रिकेट के नवीनतम सीज़न के लिए उत्साहित था।
राजू (सोचते हुए): JKL का नया क्रिकेट सीज़न आ गया है। सट्टेबाजी के माध्यम से आसानी से पैसे कमाने के कई किस्से सुने थे ;चलो इसे आजमाना चाहिए।
TEAM INDIA
राजू इंटरनेट पर JKL सट्टेबाजी समूहों की खोज करता है।
CLICK!
CLICK!
TEAM INDIA
जालसाज : स्वागत है, श्रीमान राजू। हमें खुशी है कि आपने सट्टेबाजी के बारे में पूछताछ की। मैं किस प्रकार आपकी मदद कर सकता हूँ?"
राजू: "मैं इस JKL सीज़न के लिए एक शर्त लगाना चाहता हूं।"
जालसाज: "सबसे पहले, आपको XYZ betting.com पर पंजीकरण करना होगा, और एक स्वागत उपहार के रूप में आपको न्यूनतम 5000/- रुपये के अपने पहले रिचार्ज पर 5000/- रुपये अतिरिक्त प्राप्त होंगे।
क्या करें:
✔ किसी नकली ऐप / वेबसाइट द्वारा धोखाधड़ी किए जाने की स्थिति में, और अधिक ट्रांज़ेक्शन को रोकने के लिए कार्ड /खाता /यूपीआई सेवा को ब्लॉक करने के लिए तुरंत अपने बैंक को कॉल करना चाहिए।
✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।


(राजू आकर्षक डेकोरेटेड ऐप इंस्टॉल करता है और केवल होम स्क्रीन को देखकर आश्वस्त हो जाता है कि यह एक बड़ी कंपनी है।)
राजू: "मुझे ऐप इंस्टॉल करने के लिए लिंक भेजें।"
XYZ
betting.com
जालसाज: "हमें आपकी राशि प्राप्त नहीं हुई है। विशेष ऑफर का लाभ उठाने के लिए कृपया जल्दी भुगतान करें।"
राजू: "हां, मैंने ऐप इंस्टॉल कर लिया है और निर्देश के अनुसार अभी ही 5000/- रुपये का भुगतान किया है। मुझे अपने वॉलेट में अतिरिक्त क्रेडिट कब मिलेगा?"
जालसाज: "आपको कल तक क्रेडिट मिल जाएगा।"
राजू (सोचते हुए): "यह थोड़ा संदिग्ध लगता है, लेकिन मैं सुबह तक इंतजार करूंगा।"
हालाँकि, राजू ठगा गया और धोखेबाज से फिर कभी बातचीत नहीं हुई।
क्या न करें:
✕ अनजान वेबसाइटों पर भुगतान नहीं करना चाहिए।

१९. नकली टीकाकरण कॉल


राजू: "मेरा आधार नंबर 1234455 है,
और मेरा पैन नंबर adf1234 है।"
जालसाज: "धन्यवाद, सर। कृपया प्रतीक्षा करें। मैं आपका आधार और पैनपंजीकृत कर रहा हूं,
आपको एक पंजीकरण ओटीपी कोड प्राप्त होगा । कृपया इसे साझा करें।'
राजू को एक एसएमएस मिला– आपका सत्यापन कोड 1234 है
your verification code is 1234
राजू: "हाँ,यह 1234 है।"
जालसाज: "धन्यवाद, सर। आपने वैक्सीन के लिए सफलतापूर्वक पंजीकरण कर लिया है, और आपको जल्द ही इसकी पुष्टि मिल जाएगी। जब हमारे स्वास्थ्य अधिकारी आपको टीका लगाने के लिए आयें तब कृपया कोड साझा करें। "
कॉल डिस्कनेक्ट हो गई। कुछ समय बाद, राजू को एक एसएमएस आया
'प्रिय ग्राहक, 50,000/– रुपये के व्यक्तिगत ऋण के लिए आपका अनुरोध सफलतापूर्वक स्वीकार कर लिया गया है।'
जालसाज ने राजू की ओर से 50,000/– रुपये का कर्ज लेने के लिए राजू को अपना पैन नंबर और ओटीपी साझा किए जाने के कारण धोखा दिया। राजू के पैन नंबर के आधार पर ऋण लेना राजू को XYZ कंपनी को ऋण वापस करने के लिए उत्तरदायी बनाता है।
क्या न करें:
× अपना आधार, पैन कार्ड का ब्योरा और ओटीपी अजनबियों के साथ साझा न करें। बैंक खातों से नकद निकासी सहित विभिन्न वित्तीय सेवाओं के लिए पैन कार्ड–आधारित ओटीपी का उपयोग किया जाता है।
इसलिए,अपना गोपनीय ब्योरा जैसे आधार और पैन नंबर को धोखेबाजों से बचाना बेहद जरूरी है।

२०. कोविड टेस्टिंग- फर्जी ऑनलाइन साइट

इसके बाद उस व्यक्ति ने फोन काट दिया और अपना नंबर स्विच ऑफ कर दिया।

राजू परेशान हो गया, और उसने एबीसी डायग्नोस्टिक्स साइट पर हेल्पलाइन नंबर खोजा,लेकिन वह नहीं मिला

राजू को अंततः अहसास हुआ कि उसे धोखा दिया गया था।

क्या न करें:

✕ संदेह होने पर अग्रिम भुगतान न करें। यदि कोई अग्रिम भुगतान मांगता है, तो इस स्थिति में सतर्क रहने की बात है और आवश्यक सावधानी के साथ ही उन लेनदेन को आगे बढ़ाना चाहिए।

२१. रिकवरी एजेंट के बहाने जालसाज

क्या करें:

- ✔ कोई भी भुगतान/प्रतिबद्धता करने से पहले हमेशा वसूली एजेंटों की पहचान सुनिश्चित करें। जाँच करें कि क्या एजेंट के पास बैंक या एजेंसी फर्म द्वारा जारी किए गए पहचान पत्र के साथ बैंक से वसूली नोटिस और प्राधिकार पत्र की एक प्रति है। आप फोन पर होम ब्रांच से क्रॉस वेरिफाई भी कर सकते हैं।
- ✔ घटना की सूचना निकटतम पुलिस स्टेशन और अपने बैंक/एजंसी फ़र्म की गृह शाखा को दें।


जालसाज पैसा लेता है।
राजू: "ठीक है। मैं अभी 5000/- रुपये का भुगतान करता हूँ और शेष अगले कुछ महीनों में।"
जालसाज: "ठीक है सर। मैं आपके लिए एक विशेष अनुग्रह के रूप में कर रहा हूं। आप सीधे बैंक शाखा से रसीद और लंबित बकाया की स्थिति प्राप्त कर सकते हैं"
कुछ दिनों के बाद एक और रिकवरी एजेंट राजू के घर उसके पास जाता है:
रिकवरी एजेंट: "गुड इवनिंग सर। मैं रवि हूं, XYZ बैंक का रिकवरी एजेंट। कृपया बैंक द्वारा जारी इस वसूली नोटिस को देखें जिसमें कहा गया है कि आप अपनी पिछली तीन ईएमआई चूक गए हैं और बैंक आपके वाहन की जब्ती कर सकता है।आप या तो सीधे बैंक में भुगतान कर सकते हैं या रसीद के बदले मुझे भुगतान कर सकते हैं।"
राजू हैरान होकर "कैसे हो सकता है? मैंने आपके एजेंट को कुछ दिन पहले ही 5000/- रुपये का भुगतान कर दिया है"
रिकवरी एजेंट: "यह संभव नहीं है सर। मैं इस क्षेत्र में XYZ बैंक का अधिकृत एजेंट हूं। देय राशि की वसूली के लिए कृपया मेरा आईडी कार्ड और बैंक का प्राधिकार पत्र देखें। क्या आपने उसकी आईडी देखी? क्या आपके पास भुगतान करने का कोई सबूत है?"
राजू: "अरे नहीं बाबा मैंने उस पर आँख बंद करके भरोसा कर लिया।"
क्या न करें:
× कभी भी बैंक / वसूली एजेंटों को रसीद की उचित पावती के बिना कोई नकद भुगतान न करें।

२२. समाज कल्याण योजना धोखाधड़ी


राजू– "कृपया इसे अपनी तरफ से अपडेट करें।"
जालसाज – "कृपया अपने बैंक खाता और डेबिट कार्ड के ब्योरे प्रदान करें।"
जालसाज "आपको एक ओटीपी प्राप्त होगा; प्रक्रिया को पूर्ण करने के लिए कृपया इसे साझा करें।"
राजू अपने बैंक खाते और डेबिट कार्ड के ब्योरे प्रदान करता है और धोखेबाज के साथ ओटीपी साझा करता है।
राजू–"बहुत बहुत धन्यवाद।"
कुछ मिनट बाद, राजू को बैंक से एक एसएमएस मिला जिसमें कहा गया था कि उसके बैंक खाते से 25,000/– रुपये डेबिट हो गए हैं।
INR 25,000/00
DEBITED FROM
Ac-No:xxxx070
ON 0X-X1-22
राजू को समाज कल्याण योजना में नाम दर्ज कराने के बहाने से ठगा गया।
क्या न करें:
✕ कॉल पर सब्सिडी मिलने की ऐसी कहानियों पर कभी विश्वास न करें।
✕ पात्र लाभार्थी डेटा राज्य सरकार के पास पहले से ही उपलब्ध है।
✕ आपके जिले या ग्राम पंचायत में आपके तहसीलदार कार्यालय के जन सेवा केंद्र में अपना पंजीकरण कराने के बाद सरकार आपको लाभ प्रदान करेगी।
✕ अपना ओटीपी कभी किसी के साथ साझा न करें।

२३. मल्टी लेवल मार्केटिंग (एमएलएम) घोटाले

क्या करें:

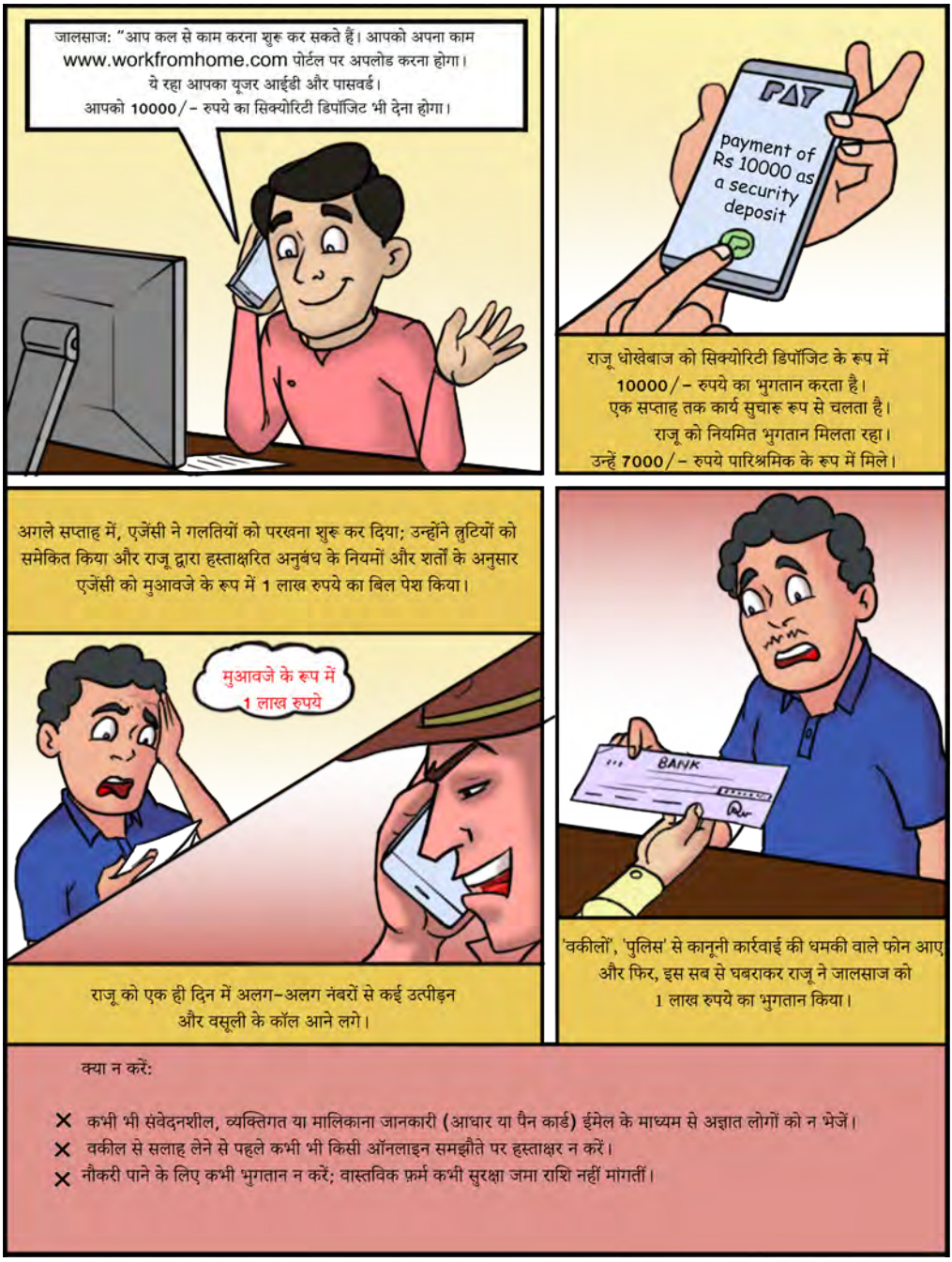
- ✔ इस प्रकार की योजनाओं में आपको शामिल करने की कोशिश करने वाले लोगों से दूर रहें।
- ✔ मल्टी लेवल मार्केटिंग योजना की प्रामाणिकता की पुष्टि करें। पोंजी स्कीम, पिरामिड स्कीम आदि जैसी कुछ नेटवर्क मार्केटिंग स्कीम प्रत्यक्ष बिक्री दिशानिर्देश, 2016 और इनामी चिट और धन परिचालन स्कीम (पाबंदी) अधिनियम, 1978 के तहत भारत में अवैध हैं।
- ✔ यदि ऐसी किसी स्कीम का प्रस्तावक आपका मित्र या रिश्तेदार है, तो भी उसे विनम्रता पूर्वक मना करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन तथा राष्ट्रीय साइबर अपराध पोर्टल https://cybercrime.gov.in पर करें।


राजू: "यह पैसा कमाने का एक शानदार तरीका है। मुझे हर दिन काम करने की ज़रूरत नहीं है क्योंकि मेरे द्वारा भर्ती किए गए एजेंट मेरी ओर से काम करेंगे, और मुझे उनके द्वारा की गई बिक्री पर कमीशन मिलेगा।"
कृष्णा: "हाँ, राजू। इसलिए मैं आपसे मिल रहा हूं। आप मेरे एजेंट के रूप में मेरी टीम में शामिल हो सकते हैं।"
राजू ने तुरंत फॉर्म भरा और मल्टी लेवल मार्केटिंग कंपनी का डायरेक्ट सेलिंग एजेंट बनने के लिए तैयार हो गया।
हालांकि, बिक्री निराशाजनक और अस्तित्वहीन थी। वह 3 और एजेंटों की भर्ती के लिए कंपनी द्वारा निर्धारित लक्ष्यों को पूरा नहीं कर सका,और उसे 20000/ रुपये का नुकसान हुआ क्योंकि उसके द्वारा कंपनी से खरीदे गए उत्पाद नहीं बेचे जा सके। उसे कोई मोबाइल भी नहीं मिला।
क्या न करें:
✕ अज्ञात कंपनियों की पैसे न दें और अज्ञात योजनाओं में नामांकन न कराएं।

२४. वर्क फ्रॉम होम घोटाला

क्या करें:

- ✔ छोटे URL, अज्ञात स्रोतों से गूगल फ़ॉर्म पर मांगी गई जानकारी से सावधान रहें।
- ✔ ईमेल, एसएमएस और पोर्टल में वर्तनी और व्याकरण संबंधी गलतियों को ध्यान पूर्वक देखें ।(क्योंकि जालसाज वास्तविक कंपनियों की नकल कर सकते हैं
- ✔ व्यक्तिगत जानकारी मांगने वाले लिंक / फॉर्मों से सावधान रहें।
- ✔ ऑफ़र या इकाई की वास्तविकता को सत्यापित करने के लिए हमेशा ईमेल के हेडर की जांच करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।


जालसाज: "आप कल से काम करना शुरू कर सकते हैं। आपको अपना काम www.workfromhome.com पोर्टल पर अपलोड करना होगा। ये रहा आपका यूजर आईडी और पासवर्ड। आपको 10000/- रुपये का सिक्योरिटी डिपॉजिट भी देना होगा।
PAY
payment of Rs 10000 as a security deposit
राजू धोखेबाज को सिक्योरिटी डिपॉजिट के रूप में 10000/- रुपये का भुगतान करता है। एक सप्ताह तक कार्य सुचारू रूप से चलता है। राजू को नियमित भुगतान मिलता रहा। उन्हें 7000/- रुपये पारिश्रमिक के रूप में मिले।
अगले सप्ताह में, एजेंसी ने गलतियों को परखना शुरू कर दिया; उन्होंने त्रुटियों को समेकित किया और राजू द्वारा हस्ताक्षरित अनुबंध के नियमों और शर्तों के अनुसार एजेंसी को मुआवजे के रूप में 1 लाख रुपये का बिल पेश किया।
मुआवजे के रूप में 1 लाख रुपये
राजू को एक ही दिन में अलग-अलग नंबरों से कई उत्पीड़न और वसूली के कॉल आने लगे।
BANK
'वकीलों', 'पुलिस' से कानूनी कार्रवाई की धमकी वाले फोन आए और फिर, इस सब से घबराकर राजू ने जालसाज को 1 लाख रुपये का भुगतान किया।
क्या न करें:
✕ कभी भी संवेदनशील, व्यक्तिगत या मालिकाना जानकारी (आधार या पैन कार्ड) ईमेल के माध्यम से अज्ञात लोगों को न भेजें।
✕ वकील से सलाह लेने से पहले कभी भी किसी ऑनलाइन समझौते पर हस्ताक्षर न करें।
✕ नौकरी पाने के लिए कभी भुगतान न करें; वास्तविक फ़र्म कभी सुरक्षा जमा राशि नहीं मांगतीं।

२५. ऑनलाइन शॉपिंग धोखाधड़ी

एक दिन राजू को एक अनजान नंबर से मैसेज आया जिसमें बहुत सस्ते दाम पर मोबाइल फोन का विज्ञापन था। उत्सुकतावश, राजू ने लिंक पर क्लिक किया और स्मार्टफोन को **50%** की छूट पर देखकर हैरान रह गया। राजू ने वेबसाइट पर दिए नंबर पर संपर्क किया।

क्या करें:

- ✔ हमेशा सुरक्षित वेबसाइटों से खरीदारी करें। यह सुनिश्चित करने की अनुशंसा की जाती है कि वेबसाइट चेक आउट ब्राउज़र में एक छोटा लॉक आइकन या 'https' दिखाएं, यह दर्शाता है कि लेनदेन सुरक्षित हैं।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।


राजू: "ठीक है। फोन की कीमत क्या है ??"
जालसाज: "सर, बाजार में इसके समान फ़ीचर वाले फोन की मौजूदा कीमत एक लाख से अधिक है, लेकिन हम इसे केवल 50,000/- रुपये में बेच रहे हैं। आपको 25,000/- रुपये का कैशबैक मिलेगा।"
राजू: "ठीक है। मैं इसके बारे में सोचूंगा और आपको बताऊंगा ।"
जालसाज: "सर, यह ऑफर केवल अगले 50 मिनट के लिए वैध है, और कुछ ही फोन स्टॉक में बचे हैं आपको तुरंत ही ऑर्डर करना होगा और ऑफ़र का लाभ उठाने के लिए भुगतान करना होगा।"
राजू ने सोचा कि वह 50000/- रुपये की कीमत वाला फोन नहीं खरीद सकता, लेकिन उसने फिर से सोचा कि मोबाइल फोन की डिलीवरी के बाद उसे 50% कैशबैक के रूप में मिलेगा, इसलिए यह उसके लिए एक उत्कृष्ट सौदा है।
राजू: "ठीक है, मैं तुरंत भुगतान कर दूंगा।"
50000
जालसाज: ""आपका फैसला बढ़िया है, सर। मैं आपको भुगतान के लिए एक लिंक भेज रहा हूं। कृपया अपना भुगतान जल्द से जल्द करें।"
राजू ने भुगतान किया और उत्पाद की डिलीवरी का इंतजार किया, लेकिन उसे कभी कोई मोबाइल नहीं मिला।
क्या न करें:
✕ अनजान वेबसाइटों से कभी भी ऑनलाइन शॉपिंग न करें।
✕ ऑनलाइन विक्रेताओं से कभी भी कुछ भी न खरीदें जो केवल उपहार कार्ड, धन हस्तांतरण आदि द्वारा भुगतान स्वीकार करते हैं क्योंकि ऐसे भुगतानों का पता लगाना और रिवर्स करना लगभग असंभव है।
✕ अज्ञात साइटों को कभी भी अग्रिम भुगतान न करें, क्योंकि भुगतान हो जाने के बाद उत्पाद मिलने की संभावना न के बराबर होती है।

२६. सार्वजनिक वाई-फाई का उपयोग कर धोखाधड़ी

रविवार का दिन था। राजू और उसका परिवार शॉपिंग मॉल में थे।
राजू ने कुछ कपड़े और किराने का सामान खरीदा और भुगतान करने के लिए रिसेप्शन पर गया।

राजू ने भुगतान शुरू किया लेकिन नेटवर्क की समस्या थी।

क्या करें:

- ✔ हमेशा एक सुरक्षित वाई-फाई नेटवर्क का उपयोग करना चाहिए।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

राजू मुफ्त वाई-फाई से जुड़ा और लेन-देन पूरा किया।"

राजू खुश था कि उसका दिन अच्छे से बीता। कुछ समय बाद, उसे अपने बैंक से एसएमएस अलर्ट मिलने लगे। '14,000/- और 10,000/- रुपए आपके खाते से डेबिट किए गए।' राजू भ्रमित था।

आखिरी बार उसने मॉल में 12,000/- रुपये का लेन-देन किया था, और ये लेनदेन अलग थे। उसने अपने बेटे को संदेशों के बारे में बताया।

"आखिरी लेन-देन क्या था, पिताजी, और आपने वह कहाँ किया?"

राजू: "मैंने आखिरी लेन-देन शॉपिंग मॉल में किया था; मैंने बिल का भुगतान ऑनलाइन कर दिया। मेरा नेटवर्क काम नहीं कर रहा था इसलिए मैंने फ्री वाई-फाई से कनेक्ट किया और भुगतान किया।

बेटा: आपने वित्तीय लेनदेन के लिए मुफ्त वाई-फाई का इस्तेमाल किया? यह सुरक्षित नहीं है, पिताजी। हैकर्स इस वाई-फाई का इस्तेमाल यूजर के डेटा तक पहुंचने और अवैध उद्देश्यों के लिए इसका इस्तेमाल करने के लिए करते हैं।"

राजू: "सच? मुझे इसकी जानकारी नहीं थी बेटा।

बेटा: "जब आपने वित्तीय लेनदेन के लिए वाई-फाई नेटवर्क का इस्तेमाल किया, तो कुछ हैकर्स ने आपके व्यक्तिगत डेटा तक पहुंच प्राप्त की और इसे आपके बैंक खाते से अनधिकृत लेनदेन के लिए इस्तेमाल किया। इसलिए आपको ये संदेश मिल रहे हैं।"

राजू: "हे भगवान! मैंने बहुत बड़ी गलती की। हम अब क्या कर सकते हैं?"

बेटा: "हमें तुरंत आपके बैंक जाना चाहिए और उनसे आपका खाता ब्लॉक करने के लिए कहना चाहिए।"

वित्तीय लेनदेन के लिए सार्वजनिक वाई-फाई का इस्तेमाल कर राजू हैकर्स का शिकार हो गया।

क्या न करें:

✕ सार्वजनिक वाई-फाई का उपयोग न करें, खासकर वित्तीय लेनदेन करते समय। ऐसे लैपटॉप या मोबाइल डिवाइस को हैक करना आसान है जो बिना किसी सुरक्षा के सार्वजनिक वाई-फाई कनेक्शन पर है। हैकर्स आपके ईमेल पढ़ सकते हैं, पासवर्ड और अन्य क्रेडेंशियल चुरा सकते हैं।

२७. नकली विज्ञापन/प्रस्ताव

पोस्टर:

क्या करें:

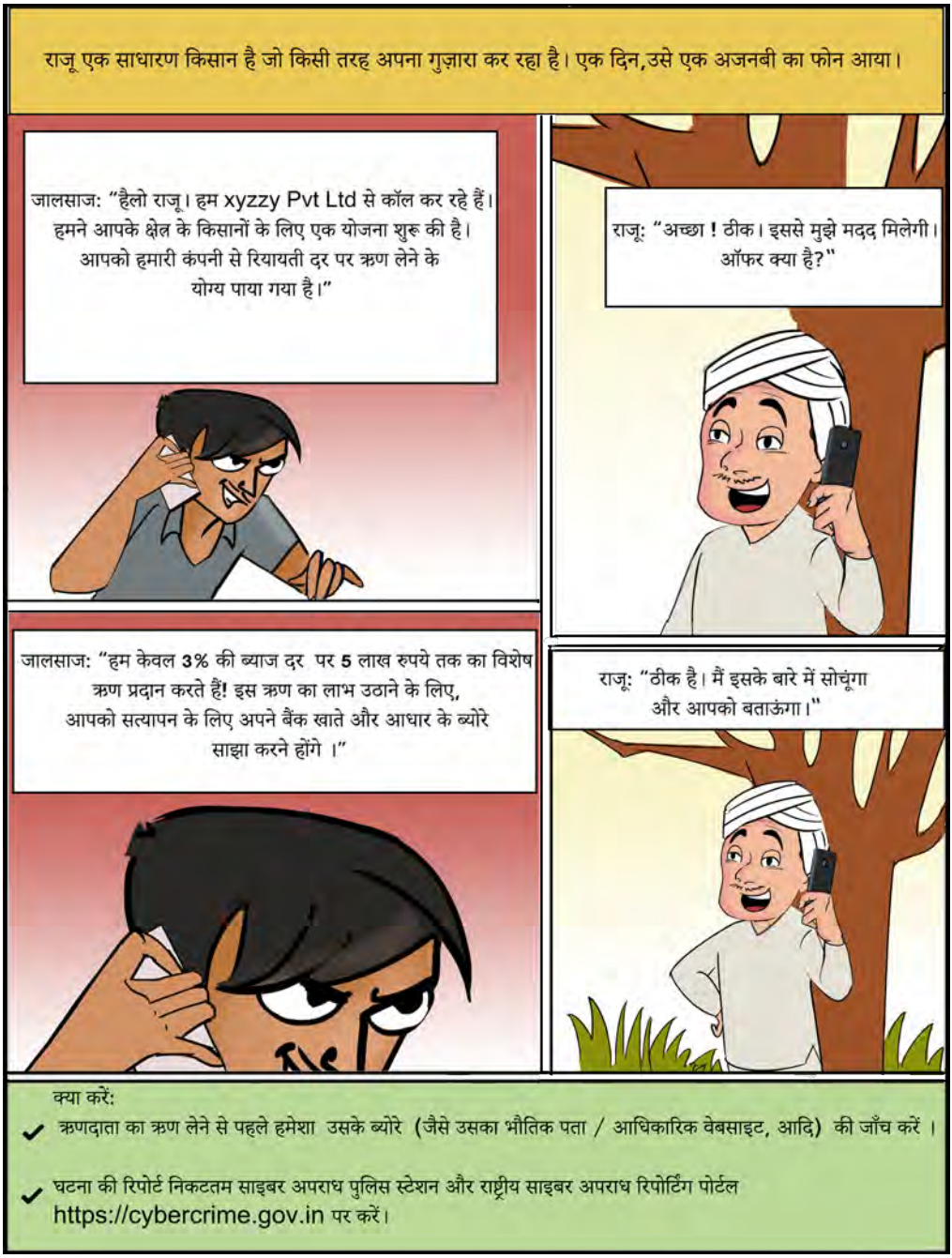
- ✔ ब्रांडेड उत्पादों के मामले में, आधिकारिक वेबसाइटों के माध्यम से विज्ञापनों को सत्यापित करें।
- ✔ गैर-ब्रांडेड उत्पाद विज्ञापनों के लिए, दुकान पर व्यक्तिगत रूप से आने या डिलीवरी के बाद ही भुगतान करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

क्या न करें:

✕ विज्ञापनों में किए गए बड़े-बड़े दावों के बहकावे में न आएं। अपनी मेहनत की कमाई को देने से पहले जांच लें और सत्यापित करें।

✕ जब तक आप उत्पाद प्राप्त न करें तब तक किसी भी राशि का भुगतान न करें। (यदि असत्यापित स्रोतों से खरीद रहे हैं)

२८. नकली ऋण प्रस्ताव



क्या न करें:

✕ ऋण स्वीकृत कराने के लिए कभी भी कोई अग्रिम भुगतान न करें। बैंक और वित्तीय संस्थान कभी भी ऋण स्वीकृति के लिए अग्रिम शुल्क नहीं मांगते हैं। शुल्क, यदि कोई हो, आपके ऋण राशि से काट लिया जाएगा और शेष राशि आपके खाते में स्थानांतरित कर दी जाएगी।

२९. क्रेडिट कार्ड एक्टिवेशन धोखाधड़ी

राजू को उनके बैंक से एक एसएमएस आया कि उनके क्रेडिट कार्ड से **1.2** लाख रुपये डेबिट हो गए हैं।यहाँ, क्रेडिट कार्ड एक्टिवेट कराने के बहाने राजू से ठगी की गई।

क्या न करें:

- ✕ कभी भी अपने कार्ड के ब्यौरे और ओटीपी किसी के साथ साझा न करें।
- ✕ अपने क्रेडिट कार्ड एक्टिवेशन के लिए अज्ञात कॉल करने वालों पर भरोसा न करें। क्रेडिट कार्ड आपके मोबाइल बैंकिंग एप्लिकेशन से एक्टिवेट किया जा सकता है।
- ✕ कभी भी अपने कार्ड के ब्यौरे /ओटीपी किसी से साझा न करें, बैंक कभी भी ओटीपी नहीं मांगता।

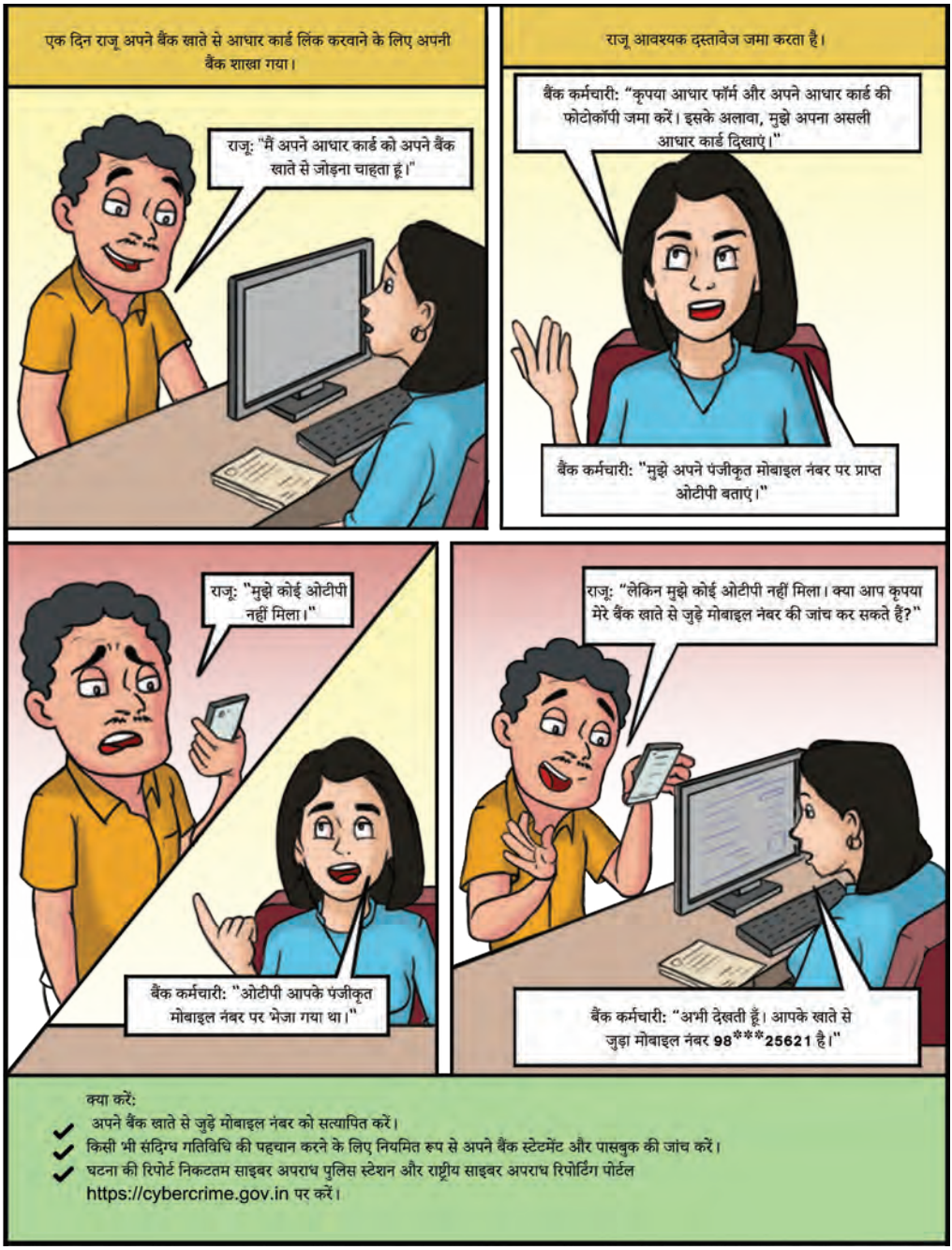
३०. क्रेडिट कार्ड सीमा उन्नयन धोखाधड़ी

कुछ समय बाद, राजू को उनके बैंक से उनके क्रेडिट कार्ड से 70000/- रुपये डेबिट होने के बारे में एक एसएमएस मिला। जालसाज ने उसके साथ धोखाधड़ी की।

क्या न करें:

- ✕ क्रेडिट कार्ड एक्टिवेशन / सीमा बढ़ाने के लिए अनजान कॉल करने वालों पर भरोसा न करें।
- ✕ अपने कार्ड का ब्यौरे / ओटीपी किसी के साथ साझा न करें।

३१. आपके आधार कार्ड की सुरक्षा




राजू: "लेकिन यह मेरा मोबाइल नंबर नहीं है।"
बैंक कर्मचारी: "आप पिछले हफ्ते बैंक आए थे।"
राजू: "पिछली बार जब मैं अपना केवाईसी फॉर्म जमा करने के लिए बैंक गया था, तो बैंक के एक सज्जन ने मुझे फॉर्म भरने में मदद की और मेरे पैसे जमा कर दिये थे ।"
बैंक कर्मचारी: "आपके द्वारा जमा किए गए फॉर्म में उसका मोबाइल नंबर हो सकता है, और आपका बैंक खाता उस नंबर से जुड़ा हुआ है। वह आसानी से आपके बैंक खाते का दुरुपयोग कर सकता है। जमा करने से पहले आपको उस फॉर्म की जाँच कर लेनी चाहिए थी ।"
राजू: "मुझे इस बारे में कोई जानकारी नहीं थी। मैंने इतनी बड़ी गलती कर दी। अब मै क्या कर सकता हूँ?"
बैंक कर्मचारी: कृपया अपना पंजीकृत मोबाइल नंबर बदलने के लिए एक फॉर्म जमा करें।
क्या न करें:
✕ अपने गोपनीय ब्योरे जैसे आधार और बैंक खाते का ब्योरे अजनबियों के साथ साझा न करें।
लेन-देन / बैंक में फॉर्म जमा करने के लिए अजनबियों की मदद न लें। केवल बैंक अधिकारियों की सहायता लें और जमा करने से पहले विवरण सत्यापित करें।

३२. कैशबैक ऑफ़र का उपयोग करके ऑनलाइन धोखाधड़ी

राजू इंटरनेट पर बहुत सक्रिय रहता है और हमेशा ऑनलाइन शॉपिंग को प्राथमिकता देता है क्योंकि ई-कॉमर्स वेबसाइटें अपने उत्पादों पर आकर्षक ऑफर प्रदान करती हैं।

क्या करें:

- ✔ धोखाधड़ी का पता चलने के बाद, अपनी होम ब्रांच को सूचित करें और अपने खाते को ब्लॉक कर दें ताकि और वित्तीय नुकसान न हो
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

जैसे ही राजू ने अपना UPI पिन डाला, उसके खाते से **20,000/-** रुपये की राशि डेबिट हो गई।
राजू ने जालसाज को कॉल करने की कोशिश की, लेकिन कनेक्ट नहीं हो सका।

क्या न करें:

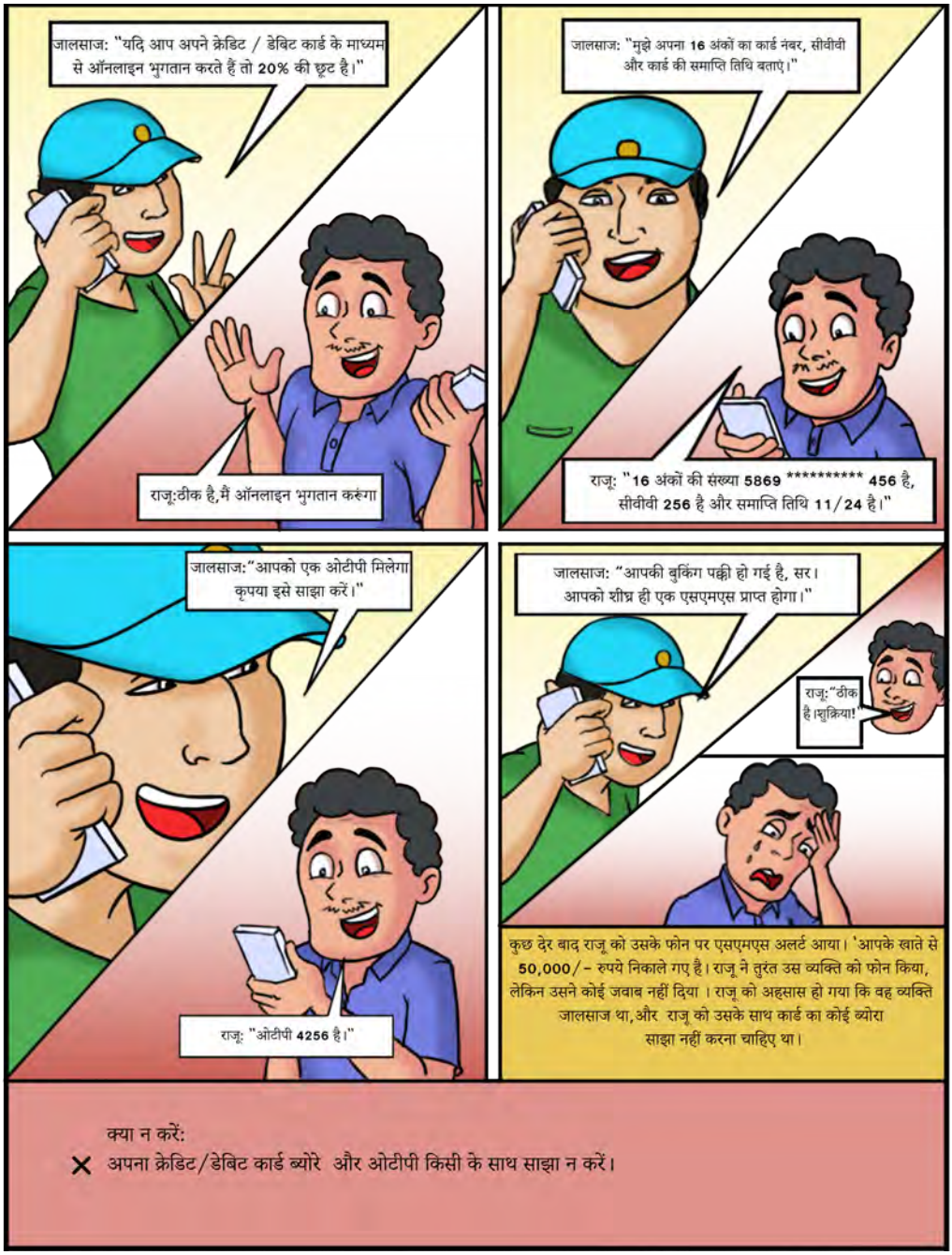
✕ फोन करने वाले पर आंख मूंदकर विश्वास न करें; प्रस्ताव की प्रामाणिकता की जांच करने के लिए कंपनी की आधिकारिक वेबसाइट को सत्यापित करना चाहिए।

✕ भुगतान प्राप्त करने के लिए यूपीआई पिन दर्ज या साझा न करें क्योंकि यह केवल भुगतान भेजने के लिए आवश्यक है।

३३. डिस्काउंट धोखाधड़ी

क्या करें:

- ✔ किसी भी सौदे या विज्ञापन की पेशकश करने वाले व्यक्ति / संस्थान की प्रामाणिकता की हमेशा पुष्टि करें।
- ✔ ओटीपी एसएमएस में अन्य ब्योरे होंगे जैसे राशि / व्यापारी का नाम / इच्छित लेनदेन का लाभार्थी का नाम। उपयोग करने से पहले ओटीपी एसएमएस अलर्ट को हमेशा अच्छी तरह से पढ़ लें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।


जालसाज: "यदि आप अपने क्रेडिट / डेबिट कार्ड के माध्यम से ऑनलाइन भुगतान करते हैं तो 20% की छूट है।"
राजू:ठीक है,मैं ऑनलाइन भुगतान करूंगा
जालसाज: "मुझे अपना 16 अंकों का कार्ड नंबर, सीवीवी और कार्ड की समाप्ति तिथि बताएं।"
राजू: "16 अंकों की संख्या 5869 ********** 456 है, सीवीवी 256 है और समाप्ति तिथि 11/24 है।"
जालसाज:"आपको एक ओटीपी मिलेगा कृपया इसे साझा करें।"
राजू: "ओटीपी 4256 है।"
जालसाज: "आपकी बुकिंग पक्की हो गई है, सर। आपको शीघ्र ही एक एसएमएस प्राप्त होगा।"
राजू:"ठीक है।शुक्रिया!"
कुछ देर बाद राजू को उसके फोन पर एसएमएस अलर्ट आया। 'आपके खाते से 50,000/- रुपये निकाले गए है। राजू ने तुरंत उस व्यक्ति को फोन किया, लेकिन उसने कोई जवाब नहीं दिया । राजू को अहसास हो गया कि वह व्यक्ति जालसाज था,और राजू को उसके साथ कार्ड का कोई ब्योरा साझा नहीं करना चाहिए था।
क्या न करें:
✕ अपना क्रेडिट/डेबिट कार्ड ब्योरे और ओटीपी किसी के साथ साझा न करें।

३४. चैरिटी धोखाधड़ी

राजू सरकारी स्कूल में शिक्षक है। उन्हें एक खबर मिली कि अभिनेता मोनू सरकारी स्कूल के छात्रों को स्मार्टफोन गिफ्ट कर रहे हैं।

क्या करें:

- ✔ हमेशा सरकारी वेबसाइट डेटाबेस पर चैरिटी संगठनों की साख की जांच करें कि वे असली हैं या नकली।
- ✔ हमेशा सतर्क रहें क्योंकि नकली वेबसाइट केवल दान भेजने के स्थान का ब्योरे बदलते हुए लगभग एक वास्तविक चैरिटी साइट के समान दिख सकते हैं, ।
- ✔ स्कैमर्स अक्सर उच्च दबाव वाली रणनीति का उपयोग करते हैं, जैसे कि तात्कालिकता पर जोर देना और अत्यधिक भावनात्मक भाषा का उपयोग करना। किसी ऐसे व्यक्ति से हमेशा सावधान रहें जो यह दावा करता हो कि दान तत्काल होना चाहिए।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।

राजू ने पैसा ट्रांसफर कर दिया, लेकिन बाद में उन्हें पता चला कि सरकारी स्कूल के छात्रों को ऐसा कोई मोबाइल फोन दान नहीं किया गया था। राजू को अहसास हुआ कि दान के बहाने धोखेबाजों ने उसे ठगा है।

क्या न करें:

✕ बिना सत्यापन के गूगल खोज के आधार पर रैंडम नंबरों पर कॉल न करें।

✕ दावे की प्रामाणिकता / वास्तविकता की पुष्टि किए बिना अग्रिम धनराशि न भेजें।

३५. एफडी पर ओवरड्राफ्ट


जालसाज: "सर, कोई पैसा देने की जरूरत नहीं है। आपको बस एक क्रॉस चेक देना होगा मैं यह सुनिश्चित करूंगा कि आपका पैसा नकद नहीं निकाला जाएगा और केवल सावधि जमा खाते में जमा किया जाएगा।"
राजू: "ठीक है उसे चेक लेने के लिए कहो
जालसाज चेक लेने के लिए राजू के घर जाता है और अलग-अलग फॉर्म पर हस्ताक्षर लेता है, जिसे राजू हस्ताक्षर करने से पहले नहीं देखता है।
एक दिन के बाद, जालसाज राजू के प्रतिनिधि के रूप में शाखा में जाता है और सावधि जमा करने के लिए चेक जमा करता है। हालांकि, उसने राजू को नकली सावधि जमा रसीदें दीं और मूल रसीदें अपने पास रख लीं।
FAKE F.D
₹
जालसाज खुद को राजू के प्रतिनिधि के रूप में बताता है और राजू द्वारा हस्ताक्षरित ओवरड्राफ्ट फॉर्म का उपयोग करता है, जिसमें ओवरड्राफ्ट के क्रेडिट के लिए उसका फ्रॉड बैंक खाता नंबर होता है
एक दिन के बाद, राजू को एफडी के बदले जारी किए गए ओवरड्राफ्ट के बारे में एक एसएमएस मिला और शाखा में जाने पर, वह यह जानकर चौंक गया कि उसे जो एफडी रसीद मिली थी, वह नकली थी।
क्या न करें:
× महत्वपूर्ण दस्तावेज / चेक अज्ञात व्यक्तियों को न सौंपें।

३६. मेलिशियस एप्लिकेशन का उपयोग कर धोखाधड़ी

एक दिन, राजू को एक संदेश मिला कि क्या वह फ्रीलान्स काम करने की इच्छा रखता है। चूंकि राजू बेरोजगार था, उसने तुरंत एसएमएस में उल्लिखित नंबर डायल किया।

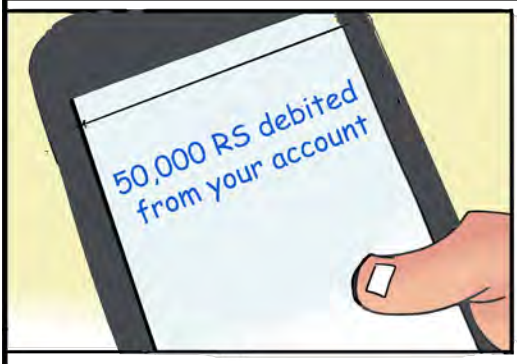
एप्लीकेशन डाउनलोड करने के बाद राजू ने काम करना शुरू कर दिया। काम वास्तविक लग रहा था; हालांकि, वह नहीं जानता था कि जालसाज उसकी सारी गतिविधियों को अपने लैपटॉप पर देख रहा था।

समय के साथ,जालसाज अपने एप्लीकेशन के माध्यम से राजू के डिवाइस से सभी गोपनीय जानकारीप्राप्त करने में सक्षम था। दुर्भावनापूर्ण इरादे से अनजान, राजू एप्लिकेशन का उपयोग करना जारी रखता है। जालसाज राजू के ईमेल पर भेजे गए ओटीपी को भी प्राप्त करने में सक्षम था क्योंकि धोखेबाज को उसके ईमेल तक पहुंच मिल गयी थी।

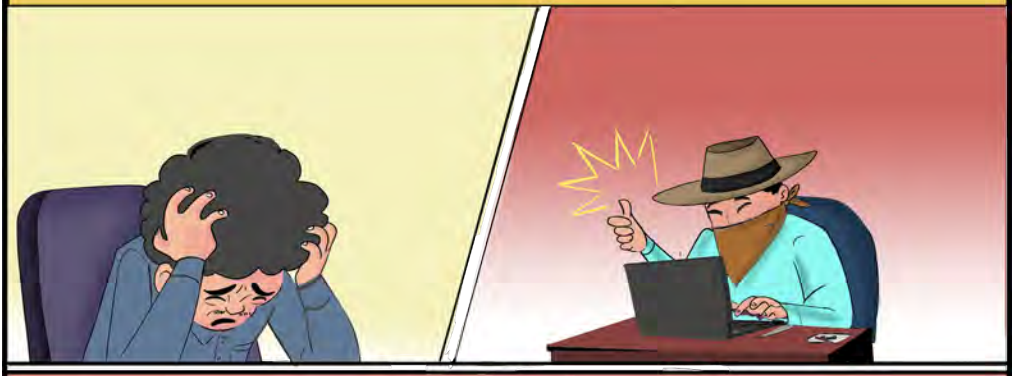
क्या करें:

- ✔ नौकरियों की पेशकश करने वाली संबंधित संस्था की आधिकारिक वेबसाइट पर ऑफ़र की प्रामाणिकता को सत्यापित करें।
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।"

कुछ दिनों के बाद, राजू को एसएमएस अलर्ट मिला जिसमें बताया गया था कि उसके खाते से
50,000/रुपये डेबिट हो गए हैं
राजू को इस बात की भनक तक नहीं थी कि उसके खाते से कैसे छेड़छाड़ की गई या पैसे कैसे डेबिट किए गए।



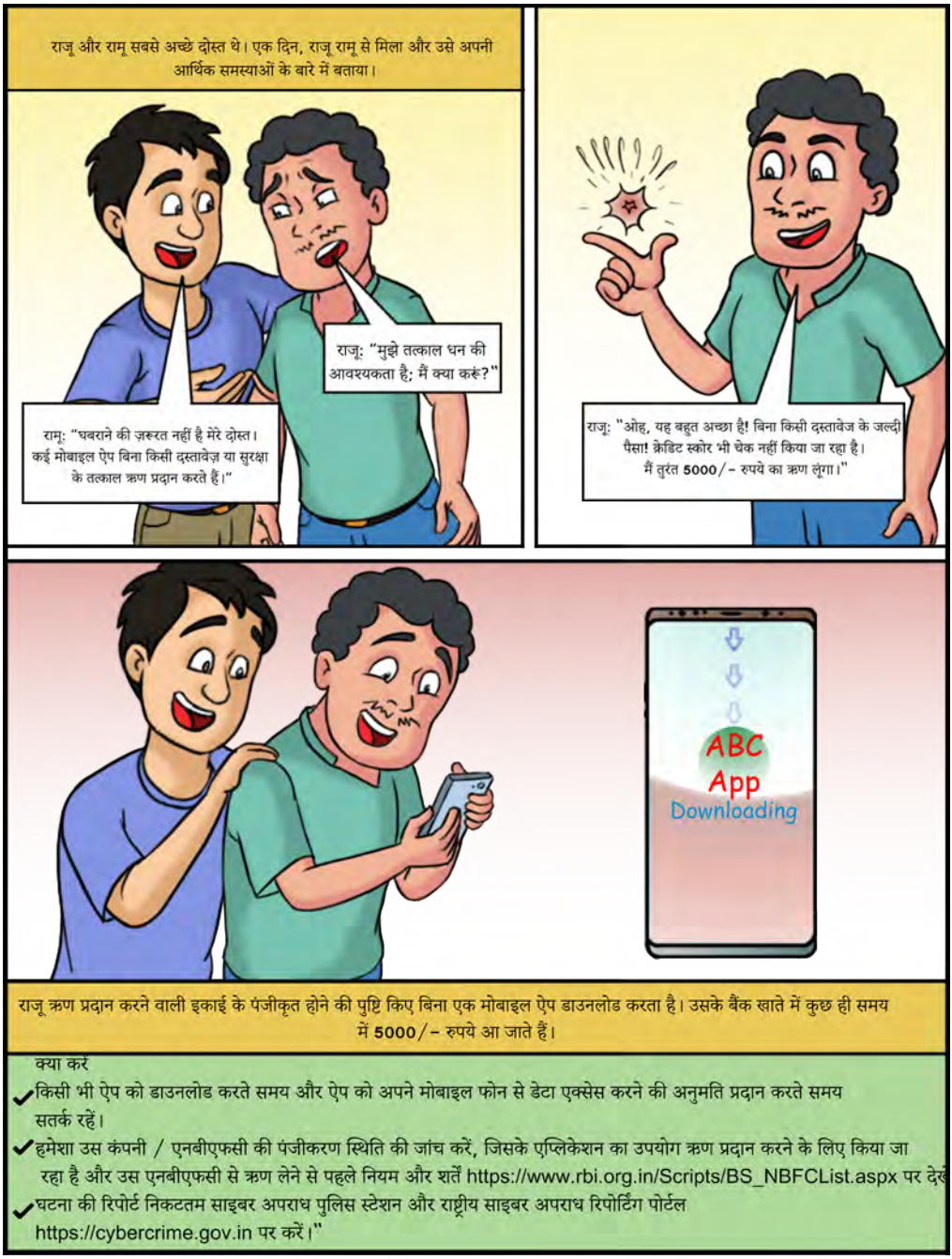
जांच के बाद, यह पाया गया कि उसके डिवाइस में एक दुर्भावनापूर्ण एप्लिकेशन था,
जिससे उसकी सभी गतिविधियों को देखा जा रहा था और पासवर्ड को स्किम् किया जा रहा था।



क्या न करें:

✕ एसएमएस, ईमेल या इंस्टेंट मैसेजिंग एप्लिकेशन के माध्यम से भेजे गए लिंक, विशेष रूप से अजनबियों से प्राप्त किसी भी एप्लिकेशन की प्रामाणिकता की पुष्टि किए बिना उसे डाउनलोड न करें।

३७. अत्यधिक ब्याज दरों और उत्पीड़न की रणनीति के साथ अवैध ऋण वित्तपोषण ऐप्स



क्या करें

- ✔ किसी भी ऐप को डाउनलोड करते समय और ऐप को अपने मोबाइल फोन से डेटा एक्सेस करने की अनुमति प्रदान करते समय सतर्क रहें।
- ✔ हमेशा उस कंपनी / एनबीएफसी की पंजीकरण स्थिति की जांच करें, जिसके एप्लिकेशन का उपयोग ऋण प्रदान करने के लिए किया जा रहा है और उस एनबीएफसी से ऋण लेने से पहले नियम और शर्तें https://www.rbi.org.in/Scripts/BS_NBFCList.aspx पर देखें
- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।"


7 दिनों के भीतर, राजू को 7500/- रुपये के पुनर्भुगतान के लिए कॉल आने लगे। राजू ने अभी भी पुराने ऋण को चुकाने के लिए पैसे की व्यवस्था नहीं की थी और 5000 / ऋण के पुनर्भुगतान के रूप में 7500 / - की मांग से चौंक गया था। राजू एक और दोस्त लक्ष्मण के पास पहुंचा।
राजू: "मैं इस धारणा में था कि मैं अपनी ऋण राशि को मामूली ब्याज शुल्क के साथ चुकाऊंगा, लेकिन यह ऐप अत्यधिक ब्याज और कई अन्य शुल्क ले रहा है। अब मुझे क्या करना चाहिये?"
लक्ष्मण : ओह! क्या आपने सत्यापित किया कि कंपनी भारतीय रिज़र्व बैंक के साथ पंजीकृत थी या कोई अन्य वैध पंजीकरण है? अन्यथा, वे किसी भी नियम के तहत कवर नहीं होंगे, और आप केवल समझौते के अनुसार भुगतान करने के लिए बाध्य हैं। हमेशा भारतीय रिज़र्व बैंक की वेबसाइट देखें, कि क्या वित्त कंपनी (एनबीएफसी) भारतीय रिज़र्व बैंक द्वारा पंजीकृत और लाइसेंस प्राप्त है।
क्या न करें:
× अगर कोई मोबाइल ऐप बिना किसी दस्तावेज़ और क्रेडिट स्कोर की जांच किए त्वरित ऋण प्रदान कर रहा है तो सतर्क रहें और हमेशा ब्याज दर की जांच करें।

३८. मर्चेंट आउटलेट्स पर कार्ड क्लोनिंग

वेटर ने कार्ड लिया, राजू से दूर चला गया और जब राजू ध्यान नहीं दे रहा था तो कार्ड को स्किमर में स्वाइप कर दिया।

बाद में, कार्ड का स्किम्ड ब्योरे एक जालसाज को दिया गया, जिसने कार्ड को सभी कार्ड विवरणों के साथ क्लोन किया और उन विवरणों का उपयोग राजू के खाते से पैसे निकालने के लिए किया।

क्या न करें:

✕ अपना क्रेडिट कार्ड / डेबिट कार्ड पिन किसी के साथ साझा न करें।

✕ क्रेडिट और डेबिट कार्ड को अपनी नजरों से ओझल न होने दें।

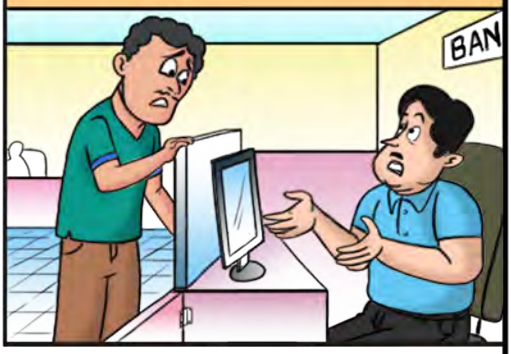
३९. ज्ञात व्यक्ति / परिवार / रिश्तेदारों के साथ साझा किए गए ब्योरे के माध्यम से धोखाधड़ी

क्या करें:

- ✔ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in पर करें।"
- ✔ समय-समय पर पिन बदलते रहें।

एक महीने के बाद, राजू को उसके मोबाइल नंबर पर एक एसएमएस आया और वह यह पता नहीं लगा पाया कि कार्ड का इस्तेमाल कहां किया गया था।

राजू ने बैंक में शिकायत दर्ज कराई। बैंक ने उन्हें आगे बताया कि विवादित लेनदेन एक ऑनलाइन मर्चेंट साइट पर किया गया था।



केशव: "राजू, अभी कुछ दिन पहले, मैंने अपना मोबाइल फ़ोन खो दिया था और मेरे फ़ोन में आपके कार्ड का ब्यौरे है। मुझे डर है कि इससे ये लेन-देन हो सकता है।

राजू: "अरे! केशव, तुम्हें मुझे इस घटना के बारे में बताना चाहिए था। मैंने कार्ड ब्लॉक कर दिया होता। मुझे अपने कार्ड के ब्यौरे फोन पर साझा नहीं करने चाहिए थे।"

राजू ने महसूस किया कि उसने खुद ऑनलाइन साइट पर कभी कोई भुगतान नहीं किया था, लेकिन उसने अपने कार्ड का ब्यौरे अपने दोस्तों के साथ साझा किया था। राजू ने तुरंत अपने सभी दोस्तों से संपर्क किया, लेकिन सभी ने उन्हें सूचित किया कि उन्होंने लेन-देन नहीं किया है।

क्या न करें:

✕ अपने कार्ड का ब्यौरे सोशल मीडिया या मैसेजिंग ऐप पर साझा न करें, भले ही प्राप्तकर्ता आपका मित्र/रिश्तेदार/परिवार ही क्यों न हो।

४०. भुगतान स्पूफिंग एप्लिकेशन


R
ग्राहक ने नकली xyz ऐप के तहत कोड को स्कैन किया।
उसने एक नकली भुगतान सूचना/स्क्रीनशॉट तैयार किया और राजू को दिखाया।
XYZ
"ठीक है। शुक्रिया।"
दिन के अंत में, राजू ने मिलान के लिए अपने दुकान खाते की जांच की और पाया कि उसके खाते में एक भुगतान अभी तक प्राप्त नहीं हुआ है।
अब उसे अहसास हुआ कि फर्जी स्क्रीनशॉट दिखाकर उसे ठगा गया है।
XYZ
इस स्पूफिंग पर, राजू बैंक से शिकायत भी नहीं कर सकता या धोखाधड़ी की रिपोर्ट नहीं दे सकता, क्योंकि वास्तविक फंड ट्रांसफर कभी हुआ ही नहीं, और राजू के पास ग्राहक का कोई ब्योरे भी नहीं है।
क्या न करें:
× फंड की वास्तविक प्राप्ति के बिना वित्तीय लेनदेन समाप्त न करें।


भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA


भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

भारतीय रिज़र्व बैंक