

राजू और चालीस चोर



वित्तीय जालसाजों की
कार्यप्रणाली पर एक पुस्तिका

भारतीय रिज़र्व बैंक







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 जनसामान्य 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 सामान्य 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-मिजाज 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

क्रम सं	विषय	पृष्ठ संख्या
१	फ़िशिंग लिंक के माध्यम से धोखाधड़ी	१
२	विशिंग कॉल्स	३
३	ऑनलाइन मार्केटप्लेस का उपयोग करके धोखाधड़ी	५
४	क्रेडिट कार्ड वार्षिक शुल्क छूट- नकली ऑफर	७
५	एटीएम कार्ड स्किमिंग फ़ॉड	९
६	स्क्रीन शेयरिंग ऐप/रिमोट एक्सेस फ़ॉड का उपयोग कर धोखाधड़ी	११
७	सिम स्वैप/सिम क्लोनिंग	१३
८	सर्च इंजनों के माध्यम से प्राप्त रिज़ल्ट पर प्रमाणों के जोखिम से धोखाधड़ी	१५
९	क्यूआर कोड स्कैन के माध्यम से धोखाधड़ी	१७
१०	सोशल मीडिया के माध्यम से प्रतिक्रिया	१९
११	जूस जैकिंग - चार्जिंग केबल के माध्यम से डेटा की चोरी	२१
१२	लॉटरी धोखाधड़ी	२३
१३	ऑनलाइन नौकरी धोखाधड़ी	२५
१४	नकली खाता संख्या	२७
१५	ईमेल के माध्यम से धोखाधड़ी	२९
१६	मैसेज ऐप बैंकिंग फ़ॉड	३१
१७	चोरी के दस्तावेज़ों के साथ धोखाधड़ी वाले ऋण	३३
१८	सट्टेबाजी घोटाला	३५
१९	नकली टीकाकरण कॉल	३७
२०	कोविड टेस्टिंग- फ़र्जी ऑनलाइन साइट	३९



क्रम सं.	विषय	पृष्ठ संख्या
२१	रिकवरी एजेंट के बहाने जालसाज	४१
२२	समाज कल्याण योजना धोखाधड़ी	४३
२३	मल्टी लेवल मार्केटिंग (एमएलएम) घोटाले	४५
२४	वर्क फ्रॉम होम घोटाला	४७
२५	ऑनलाइन शॉपिंग धोखाधड़ी	४९
२६	सार्वजनिक वाई-फाई का उपयोग कर धोखाधड़ी	५१
२७	नकली विज्ञापन/प्रस्ताव	५३
२८	नकली ऋण प्रस्ताव	५५
२९	क्रेडिट कार्ड एक्टिवेशन धोखाधड़ी	५७
३०	क्रेडिट कार्ड सीमा उन्नयन धोखाधड़ी	५९
३१	आपके आधार कार्ड की सुरक्षा	६१
३२	कैशबैक ऑफ़र का उपयोग करके ऑनलाइन धोखाधड़ी	६३
३३	डिस्काउंट धोखाधड़ी	६५
३४	चैरिटी धोखाधड़ी	६७
३५	एफडी पर ओवरड्राफ्ट	६९
३६	मेलिशियस एप्लिकेशन का उपयोग कर धोखाधड़ी	७१
३७	अत्यधिक ब्याज दरों और उत्पीड़न की रणनीति के साथ अवैध ऋण वित्तपोषण ऐप्स	७३
३८	मर्चेन्ट आउटलेट्स पर कार्ड क्लोनिंग	७५
३९	ज्ञात व्यक्ति / परिवार / रिश्तेदारों के साथ साझा किए गए ब्योरे के माध्यम से धोखाधड़ी	७७
४०	भुगतान स्पूफिंग एप्लिकेशन	७९

१. फ़िशिंग लिंक के माध्यम से धोखाधड़ी

एक दिन, राजू को अपने फोन पर एक मैसेज प्राप्त हुआ:
प्रिय याहक,
यदि आपका केवाईसी ब्योरा दो दिनों के भीतर अपडेट नहीं किया जाता है,
तो आपका खाता ब्लॉक कर दिया जाएगा। ब्योरा
अपडेट करने के लिए नीचे दिए गए लिंक का उपयोग करें।
<http://updateKYC.ibank.com>

राजू: "अरे! मेरा सारा पैसा ब्लॉक कर दिया जाएगा;
मुझे अपना केवाईसी ब्योरा अपडेट करना होगा।"



राजू ने लिंक पर क्लिक किया,
लेकिन केवाईसी ब्योरा अपडेट करने का लिंक
काम नहीं किया। जल्द ही, उसे एक कॉल आता है।



जालसाज: "नमस्कार सर, मैं xyz बैंक से फोन कर
रहा हूँ। क्या आपको अपना केवाईसी ब्योरा अपडेट
करने में कोई दिक्कत आ रही है?"

राजू: "हाँ, लिंक काम
नहीं कर रहा है।"



जालसाज: "वेबसाइट पर ज्यादा लोड हो गया होगा;
मैं अपनी तरफ से ब्योरा अपडेट कर दूंगा।
कृपया अपना यूजर नेम,
पासवर्ड और ओटीपी साझा करें।"

click!
click!



क्या करें:

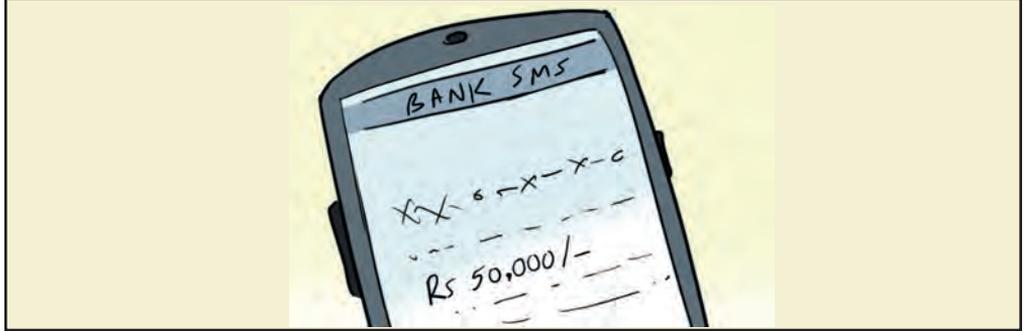
✓ जब भी आपको केवाईसी को अपडेट करने का अनुरोध करने वाले कॉल, लिंक या एसएमएस अज्ञात स्रोतों से प्राप्त हों, तो हमेशा अपनी होम ब्रांच या अपने रिलेशनशिप मैनेजर के माध्यम से केवाईसी स्थिति की जांच करें।

✓ 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

एक दिन राजू को फोन आया।

जालसाज: "नमस्कार सर,
मैं XYZ बैंक से फोन कर रहा हूँ।"

राजू: "जी, क्या बात है?"

जालसाज: "यह कॉल आपकी बीमा पॉलिसी के संबंध में है। आपकी पॉलिसी एक्टिवेट हो गई है, और आपको प्रिमियम के रूप में 18000/- रुपये का भुगतान करना होगा।"

राजू: "नहीं मेरे पास XYZ बैंक का कोई बीमा नहीं है।"

जालसाज: "सर, यह बहुत कम शुल्क पर प्रमोशनल ऑफर के रूप में एक्टिवेट हो गया। लेकिन अगर आपकी इसकी आवश्यकता नहीं है, तो मैं इसे डिएक्टिवेट कर दूंगा।"

राजू: "मुझे समझ में नहीं आता कि आपने मेरी सहायता के बिना पॉलिसी को कैसे एक्टिवेट किया, और मैं आप पर भरोसा क्यों करूँ?"

जालसाज: "सर, मैं आपके सोपे XYZ बैंक कस्टमर केयर से कॉल कर रहा हूँ। मेरे पास आरका नाम, पता, कर्डी प्योर, जन्म तिथि, कम्पनी का नाम और पदनाम जैसे सभी विवरण हैं।"

राजू: "ठीक है, तो मुझे बताओ कि पॉलिसी को कैसे डिएक्टिवेट किया जाए?"

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 बन की बाबी 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।



राजू तुरंत पास की XYZ शाखा में गया और लेन-देन के बारे में पूछताछ की।
राजू को अपनी गलती का अहसास हुआ: कॉल एक धोखेबाज का था;
उसे किसी अजनबी पर भरोसा नहीं करना चाहिए था।

क्या न करें:

- × गोपनीय जानकारी/धोरे 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।
- × विजिटल 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

राजू एक सोफा सेट को बेचना चाहता था। उन्होंने सेकेंड हैंड सामानों के लिए एक ऑनलाइन मार्केटप्लेस वाली वेबसाइट पर विज्ञापन पोस्ट किया।



Click!

विज्ञापन पोस्ट करने के तुरंत बाद, एक पोखेबाज द्वारा सोफा सेट के लिए 15,000/- रुपये का भुगतान करने की पेशकश की गई। प्रस्ताव पाकर राजू बहुत खुश हुआ।



जालसाज: "मैं फनीचर लेने से पहले ऑनलाइन भुगतान करूंगा।"

राजू: "ठीक है। बढ़िया।"



जालसाज: "कृपया अपना खाता नंबर साझा करें।"

राजू: "मेरा खाता नंबर 123XXX67 है।"

जालसाज: "मैं पहले खाते को सत्यापित करने के लिए अंतिम भुगतान करने से पहले 10/- रुपये भेजूंगा।"

जालसाज ने राजू के खाते में 10/- रुपये भेजे और अंतिम भुगतान करने के लिए पृष्ठ करने को कहा।

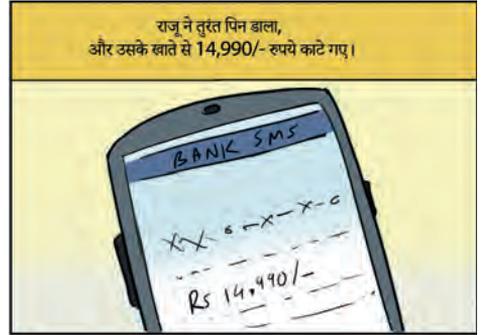


राजू: "हाँ, मुझे मिल गया।"

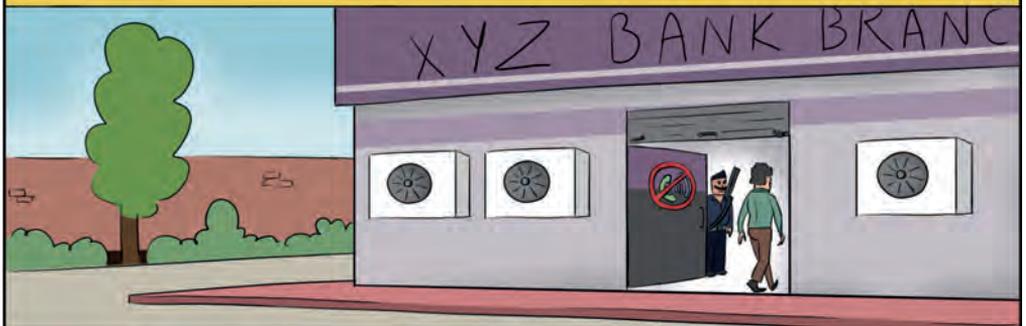
ध्यान दें:

- ✓ हमेशा याद रखें, UPI सिन 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।
- ✓ पटना 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।)



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 ब्योरे 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।

जालसाज: "गुड मॉर्निंग, मिस्टर राजू! मैं आपके बैंक कस्टमर केयर से रोहित कुमार बोल रहा हूँ। हमें आपको यह सूचित करते हुए खुशी हो रही है कि इस वर्ष के लिए आपके क्रेडिट कार्ड का वार्षिक शुल्क माफ़ कर दिया जाएगा क्योंकि आप हमारे सबसे मूल्यवान ग्राहकों में से एक हैं।"

राजू: "वाह! यह तो बहुत अच्छी खबर है!"

जालसाज: "मिस्टर राजू, कृपया आगे बढ़ने से पहले कुछ ब्योरों की पुष्टि करें। आपका कार्ड नंबर 42781234 XXXX है, और आपका पूरा नाम राजू देशपांडे है, है ना?"

(घोषेबाज ने पहले ही गैर-कानूनी श्रोतों से राजू के कार्ड का ब्योर एकत्र कर लिए थे।)

राजू: "हाँ, ये सही है।"

जालसाज: "मिस्टर राजू, अब आपको एक ओटीपी प्राप्त होगा। कृपया इसे हमारे साथ साझा करें ताकि हम अपनी ओर से शुल्क माफ़ कर सकें।"

क्या करें:

- ✓ आपके बैंक से होने का दावा करने वाले अज्ञात नंबरों से प्राप्त कॉल का जवाब देते समय सतर्क रहें।
- ✓ घोषापट्टी का पता चलने पर तुरंत अपनी होम ब्रांच को रिपोर्ट करें।
- ✓ आगे विदेशी 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 चूँकि कॉल करने वाले को पहले से ही उसके कार्ड का ब्योरे पता थे,
इसलिए कॉल वास्तविक होनी चाहिए। उसने तुरंत ओटीपी को जालसाज के साथ साझा कर दिया।

जालसाज: "धन्यवाद, मिस्टर राजू।
आपका वार्षिक शुल्क माफ कर दिया गया है।
आपका दिन अच्छा रहे!"



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 ब्योरे एकल 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 ट्रांज़ेक्शन ग्राह करने से पहले, पुनिष्ठित करें कि स्किमिंग डिवाइस मौजूद नहीं हैं। पोलेबाजों द्वारा स्किमिंग उपकरणों को कार्ड इंटरचेंज एरेंट के साथ ओवरलेप करके छिप दिया जाता है।
 - ✓ कार्ड स्किमिंग की घटना के 3 दिनों के भीतर बैंक को पोसाधही की रिपोर्ट करें। सभी ट्रांज़ेक्शन को ररवायित करने के लिए अपने पहले किए गए लेन-देन की बार-बार जांच करें।
 - ✓ घटना की रिपोर्ट निकलताम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (<https://cybercrime.gov.in>) पर करें।



क्या न करें:

- ✗ एटीएम परिसर में आपके एजेंट में लैन-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



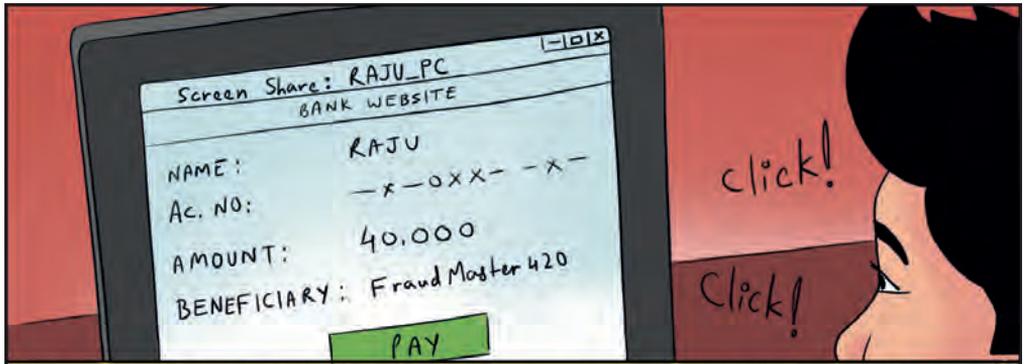
- क्या करें:
- ✓ संबंधित संस्था की आधिकारिक वेबसाइट पर प्रस्ताव की प्रामाणिकता सत्यापित करें।
 - ✓ अपने मोबाइल फोन में एंटीवायरस / स्पैम ब्लॉकिंग सॉफ्टवेयर इंस्टॉल करें।
 - ✓ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> पर करें।



(धोखापट्टी करने वाले ने राजू के मोबाइल में स्क्रीन-शेयरिंग ऐप को सफलतापूर्वक इंस्टॉल किया और उसके फोन तक पहुंच प्राप्त की। वह राजू के मोबाइल पर संदेशों को पढ़ सकता था और उनके की-पैड को ट्रैक कर सकता था।)



(राजू ने यह सोचकर कि यह सिर्फ 10/- रुपये की बात है, नेट बैंकिंग के माध्यम से राशि ट्रांसफर कर दी। जल्द ही उन्हें 35000/- रुपये, 20000/- रुपये और 40000/- रुपये के डेबिट संदेश प्राप्त हुए।)



(एक बार स्क्रीन-शेयरिंग एप्लिकेशन इंस्टॉल हो जाने के बाद, जालसाज के पास राजू द्वारा 10/- रुपये का भुगतान करने के लिए दर्ज किए गए नेट बैंकिंग पासवर्ड तक पहुंच थी।)

- 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 ऐस 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 ब्योरे साझा करता है।)



राजू: "मेरे मोबाइल को क्या हो गया है?
कोई नेटवर्क नहीं है, और मैं कॉल करने,
संदेश आदि भेज पाने में असमर्थ हूँ।"



(जालसाज नए सिम का उपयोग कर बैंकिंग एप्लिकेशन के लिए यूजर नेम पुनः प्राप्त करने के लिए 'फॉर्गेट यूजर 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 जांच 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, अनिवाह्य खरीदारी करने के लिए सिम को क्रेडिट किया गया था।



धया न करें:

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

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

राजू को क्रिकेट देखने का शौक है, और वह आगामी क्रिकेट मैच को लेकर बहुत उत्साहित था। लेकिन जैसे ही उसने स्पोर्ट्स ऐप खोला, उन्हें ज्ञात हुआ कि उसकी सबस्क्रिप्शन समाप्त हो गया है।



राजू सोचता है: "इसमें कौनसी बड़ी बात है! इंटरनेट है तो सारे समाधान हैं!"



वह सोचकर अपने इंटरनेट पर स्पोर्ट्स ऐप के सबस्क्रिप्शन को रिचार्ज करने का तरीका खोजा। काफी खोजबीन करने के बाद उसे एक जाल साज मिली। राजू ने तुरंत नंबर डायल किया।



क्या करें:

- ✓ हमेशा सेवा प्रदाता की आधिकारिक वेबसाइट से ही संपर्क करें / 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 जाँच किए बिना ओटीपी डाल कर भुगतान कर दिया।

राजू को एक एसएमएस मिला जिसमें कहा गया था कि उसके खाते से 40,000 रुपये डेबिट हो गए हैं।



(स्पॉट्स पेप को 1000 रुपये देने के बजाय, राजू जालसाज को 40000 रुपये ट्रांसफर कर बैठा था।)



क्या न करें:

- × नेब सर्च इंजन से प्राप्त यादृच्छिक फोन नंबरों पर संपर्क न करें शायद 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।

जालसाज: "नमस्ते, मैंने आपकी कार का विज्ञापन प्लेटफॉर्म पर देखा। मुझे कार पसंद आयी और मैं आपकी कार खरीदना चाहता हूँ।"



क्या करें:

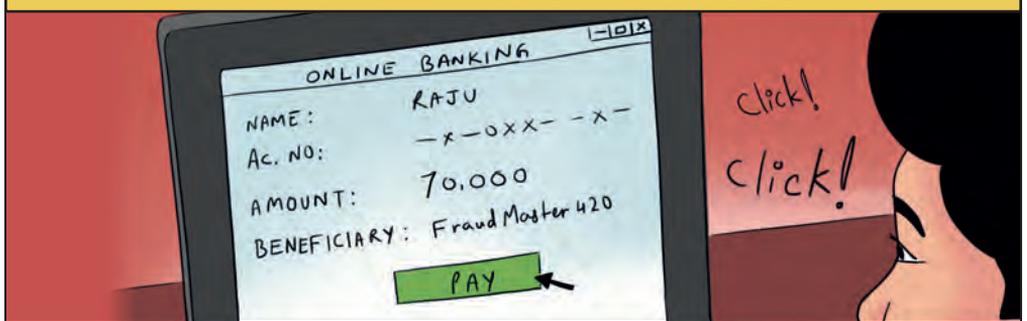
- ✓ क्यूआर कोड का उपयोग करने से पहले उसे उपयोग करना सीख लें।
- ✓ ट्रांजेक्शन की सूचना तुरंत अपने बैंक को दें।
- ✓ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> पर करें।



राजू क्यूआर कोड को स्कैन करता है और उसे यूपीआई पिन के लिए अप अनुरोध प्राप्त



(राजू ने उस पर विश्वास कर लिया और अपना यूपीआई पिन दर्ज किया। इसके बाद, उसके खाते से 70,000/- रुपये डेबिट हो गए। राजू को डेबिट का एसएमएस अलर्ट मिला। वह घबरा गया, और उसने जालसाज को कॉल करने की कोशिश की, लेकिन तब तक उसका फोन स्विच ऑफ हो गया था।)



क्या न करें:

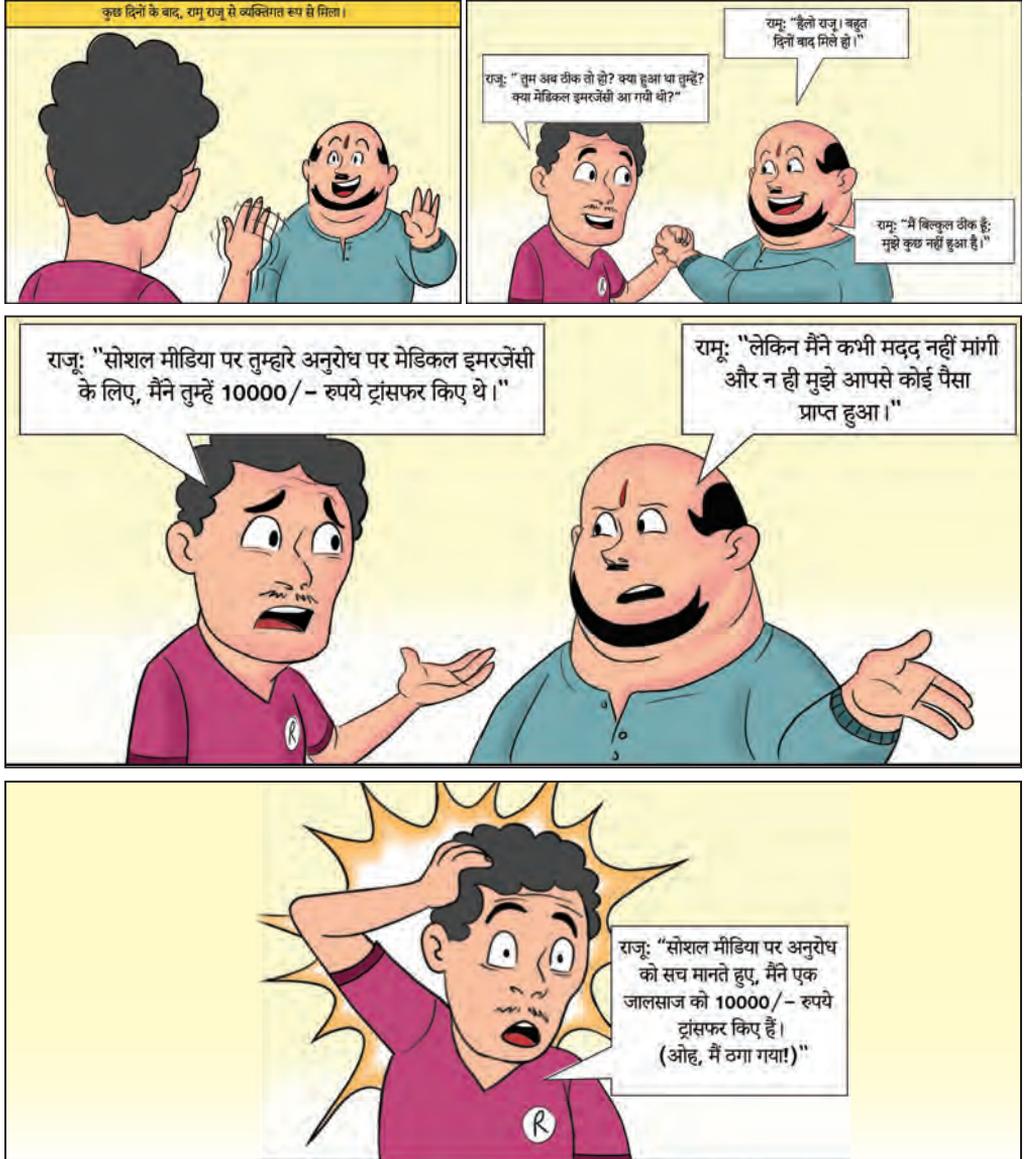
- × किसी अन्य व्यक्ति से पैसे प्राप्त करने के लिए अपना यूपीआई पिन दर्ज न करें। यूपीआई पिन केवल भुगतान करने के लिए आवश्यक है, धन प्राप्त करने के लिए नहीं।
- × भुगतान प्राप्त करने के लिए कोई क्यूआर कोड स्कैन न करें। पैसे प्राप्त करने के लिए क्यूआर कोड को स्कैन करने की आवश्यकता नहीं होती, / बल्कि भुगतान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

१०. सोशल मीडिया के माध्यम से प्रतिकारण



क्या करें:

- ✓ भगतान करने से पहले वास्तविक व्यक्ति को कॉल करके या प्रत्यक्ष मिलकर जांच करें।
- ✓ कोई भी भगतान करने से पहले हमेशा खाते के ब्यारे 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 मिल सूची को सच के लिए खुला न रखें।
- × उन लोगों के मिलता 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

मेडिकल इमरजेंसी के कारण राजू को जल्दी जाना पड़ा।
उसे ज्ञात होता है कि उसके फोन की बैटरी कम है।



राजू: "उफ़फ़! मेरी बैटरी खत्म हो गई
और मेरे पास चार्जर नहीं है।"

(एक जालसाज वायरस के साथ एक चार्जिंग केबल स्थापित करता है और उसे सार्वजनिक स्थान पर चार्जिंग प्वाइंट पर छोड़ देता है। राजू चार्जिंग केबल के साथ चार्जिंग प्वाइंट को नोटिस करता है और जालसाज से पूछता है कि क्या वह इसका इस्तेमाल कर सकता है।)



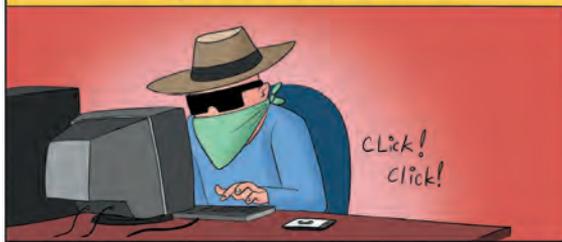
क्या करें:

- ✓ किसी भी अनधिकृत पहुंच से बचाने के लिए अपने मोबाइल फोन पर एंटी-वायरस सॉफ्टवेयर इनस्टॉल करें।
- ✓ घटना की रिपोर्ट किब्रोटवम 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, आलसाज ने राजू द्वारा दर्ज किए गए सभी विवरणों को अपने मोबाइल पर कैचर कर लिया और महत्वपूर्ण बैंक खातों जैसे यूजर नेम, पासवर्ड आदि को प्राप्त कर लिया।



एक दिन, राजू को अपने वचत 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।



ध्यान न करें:

- × अज्ञानबिंदुओं 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।



जालसाज: "हाय... मैं पंकज एबीसी से फोन कर रहा हूँ।
बधाई! आपने 10 लाख रुपये का एबीसी जैकपॉट जीता है।
मैंने आपको जैकपॉट ब्योरा भेज दिया है।
आप पुरस्कार का दावा करने के लिए उसमें दिए गए
नंबर पर संपर्क कर सकते हैं। जल्दी करें!"

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।

राजू: "हेलो, मैं राजू बोल रहा हूँ। मुझे एबीसी
जैकपॉट लेने के लिए आपसे संपर्क करने के लिए
कहा गया था।
मैं अपना जैकपॉट कैसे प्राप्त करूँ?"



जालसाज: "बधाई हो राजू! पुरस्कार प्राप्त करने के योग्य होने के लिए आपको 1000/- रुपये
का वितरण शुल्क देना होगा। मैं आपके संदेश पर नंबर पर हमारे शाले का ब्योरा भेजा है।
कृपया तुरंत राशि का भुगतान करें और मुझे वापस कॉल करें।"



(इस कथकपूर्ण गतिविधि से अनजान, राजू ने राशि का भुगतान किया और उसे वापस कॉल किया।)

राजू: "नमस्कार, मैंने राशि का भुगतान कर दिया है और आपको
ब्योरे भेज दिए हैं। मुझे अपना पुरस्कार कब मिलेगा?"

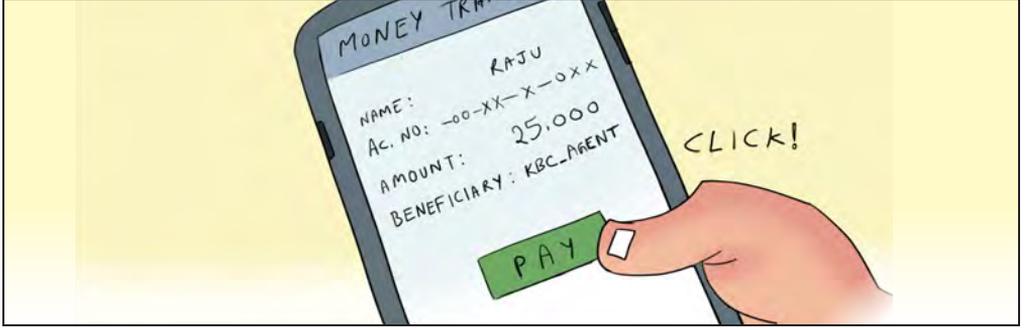


जालसाज: बहुत बढ़िया राजू! आपको 10 लाख
रुपये का जैकपॉट मिलने से पहले बस कुछ ही
और स्टेप्स पूरे करने हैं।
पुरस्कार राशि का दावा करने
के लिए आपको 25000/- रुपये
का बंधन देना होगा।

क्या करें:

- ✓ किसी भी कंपनी या प्राबंधन 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 अधिकार को हमेशा सत्यापित करें।
- ✓ घटना की रिपोर्ट निम्नलिखित साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रियॉर्टिंग 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:

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

१३. ऑनलाइन नौकरी धोखाधड़ी

राजू ने हाल ही में अपनी नौकरी खो दी थी और वह बहुत चिंतित था। उसने कई ऑनलाइन जॉब पोर्टल पर नौकरी की तलाश शुरू कर दी। उसने विभिन्न वेबसाइटों पर अपना बायोडाटा अपडेट किया।



एक दिन, उसे एक जालसाज का फोन आया, जो XYZ कंपनी का नकली व्यक्ति बनकर बात कर रहा था।

जालसाज: "क्या मैं मिस्टर राजू से बात कर रहा हूँ?"



राजू: "हाँ, क्या मैं जान सकता हूँ कि मैं किससे बात कर रहा हूँ?"

जालसाज: "हाय, राजू मैं XYZ कंपनी के मानव संसाधन विभाग से रोहित हूँ। आपके आवेदन के आधार पर आपको हमारी कंपनी में प्रबंधक पद के लिए चुना गया है।"



राजू: "वाह! मुझे चुनने के लिए धन्यवाद।"

जालसाज: "आपकी योग्यता ने आपको यह नौकरी पाने में मदद की है।"

राजू: "ठीक है, अच्छी बात है। अगला कदम क्या है?"



क्या करें:

- ✓ कोई भी पैसा देने से पहले कंपनी या भर्ती एजेंसियों की प्रामाणिकता सत्यापित करें।
भर्ती एजेंसिया 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 झासे 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

राजू अपने परिवार और अपने लिए एक परिवार बीमा पॉलिसी खरीदने की योजना बना रहा था।
ऑफिस से घर वापस जाते समय उन्होंने एबीसी इश्योरेंस कंपनी के नाम से एक छोटा सा स्टॉल देखा।

ABC INSURANCE COMPANY
INQUIRY BOOTH

राजू: "नमस्कार मैं अपने परिवार के लिए एक बीमा पॉलिसी खरीदने की योजना बना रहा हूँ।"

सेल्स एजेंट: "सर, आप सही जगह पर आए हैं। हमने इस आउटलेट को सार्वजनिक स्थानों पर विशेष रूप से नयी बीमा योजनाओं को शुरू करने के लिए शुरू किया है।"

राजू: "यह बहुत अच्छा है। क्या-क्या विकल्प उपलब्ध हैं?"

सेल्स एजेंट: "सर, परिवार के लिए सबसे अच्छा सुरक्षा प्लान है जिसमें आपको 10000/- रुपये के प्रीमियम पर 2 लाख का कवर मिलेगा।"

राजू: "ठीक है! मैं इस बारे में अपने परिवार से चर्चा करूँगा और आपको बताऊँगा।"

सेल्स एजेंट: "सर, हमने यह विशेष आउटलेट केवल आज के लिए खोला है। यदि आप अभी भुगतान करने के लिए तैयार हैं, तो हम पॉलिसी को 50% की छूट पर देने आपको केवल 5,000/- रुपये का भुगतान करना होगा।"

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।



(अगले दिन राजू ने देखा कि आउटलेट वहाँ नहीं था। 10 दिनों के बाद भी,
उसे कोई दस्तावेज नहीं मिला। राजू ने एबीसी बीमा कंपनी को फोन किया।)



एबीसी कंपनी: "हमारे पास ऐसा कोई आउटलेट नहीं है। इसके अलावा, हमारे पास हमारी
आधिकारिक वेबसाइट पर एक विशिष्ट भुगतान विकल्प है। हम स्थानांतरण के किसी अन्य
तरीके को नहीं अपनाते हैं। लगता है आपको ठग गया है।"



क्या न करें:

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

१५. ईमेल के माध्यम से धोखाधड़ी

एक बहुरूपिये जालसाज ने राजू को एक ईमेल भेजा, जिसमें उसने उसके दोस्त रमेश के नाम से अपनी मेडिकल इमरजेंसी के लिए आर्थिक मदद मांगी।



राजू ईमेल आईडी या खाते के ब्योरे की पृष्टि किए बिना तुरत राशि का भुगतान कर देता है।



एक दिन बाद, राजू ने रमेश को उसका स्वास्थ्य जानने के लिए कॉल किया।



रमेश: "नमस्कार राजू। मैं ठीक हूँ। क्या हाल है? तुमने मुझे बहुत दिनों बाद कॉल किया है।"



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।



यह जानकर राजू सदमे में था कि उसकी इस दयालुता के कार्य ने उसकी लापरवाही के कारण उसे धोखाधड़ी का शिकार बना दिया। उसे ईमेल आईडी सत्यापित करनी चाहिए थी।



क्या न करें:

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

१६. मैसेज ऐप बैंकिंग फ्रॉड

एक दिन राजू को एक अनजान नंबर से कॉल आया।

जालसाज: "नमस्कार सर। मैं XYZ बैंक के कस्टमर केयर सेंटर से कॉल कर रहा हूँ। हम एक नया उत्पाद, एक मैसेज ऐप लॉन्च कर रहे हैं। यह एक बैंकिंग सुविधा है जो आपके व्हाट्सएप के माध्यम से आसानी से 24x7 बैंकिंग सेवाएँ प्रदान करता है। जब आप इसे पहली बार इस्तेमाल करेंगे तो आपको एक गिफ्ट वाउचर भी मिलेगा। कृपया पृष्ठ करें कि 99****99 मैसेज ऐप के साथ रजिस्टर्ड किया हुआ मोबाइल नंबर है।"

NAME: RAJU
OCCUPATION: XOXO
ADDRESS: X-X-XX
00-X00A-X-0X
X-XA XOXO X-XX
CONTACT: 729256927
X-X-X-X

राजू: "वाह! यह बेहतरीन है। हाँ। यह मेरा मैसेज ऐप नंबर है।"

जालसाज: "ठीक है सर। हमने आपको पहले ही मैसेज ऐप पर एक वेलकम-मैसेज भेज दिया है। कृपया देखें।"

(राजू अपना मैसेज ऐप खोलता है और एक नंबर से एक स्वागत संदेश देखता है जिसमें उसकी प्रोफाइल पिक्चर में XYZ बैंक का पोस्टर और स्टैटस में बैंक का टैगलाइन होता है।)



जालसाज: "कृपया सत्यापन के लिए अपने डेबिट कार्ड का ब्योरा दर्ज करें। आपको मेरे साथ ब्योरे साझा करने की आवश्यकता नहीं है, लेकिन इसे आधिकारिक मैसेज ऐप नंबर पर ही दर्ज करें।"

राजू: "मैंने इसमें प्रविष्टि कर दी है।"

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।



(राजू ने अपने खाते में 20000/- रुपये का एक डेबिट संदेश देखा। वह तुरंत वापस कॉल करता है, लेकिन मोबाइल बंद हो जाता है। राजू को एहसास होता है कि उसे धोखा दिया गया है।)

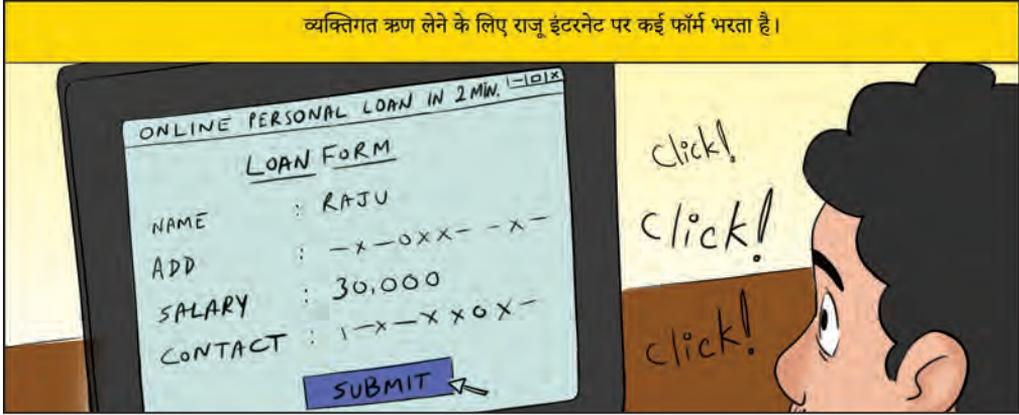


क्या न करें:

- ✗ आसान बैंकिंग सेवाओं की पेशकश करने वाले और मैसेजिंग ऐप 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 दस्तावेजों के साथ धोखाधड़ी वाले ऋण

व्यक्तिगत ऋण लेने के लिए राजू इंटरनेट पर कई फॉर्म भरता है।



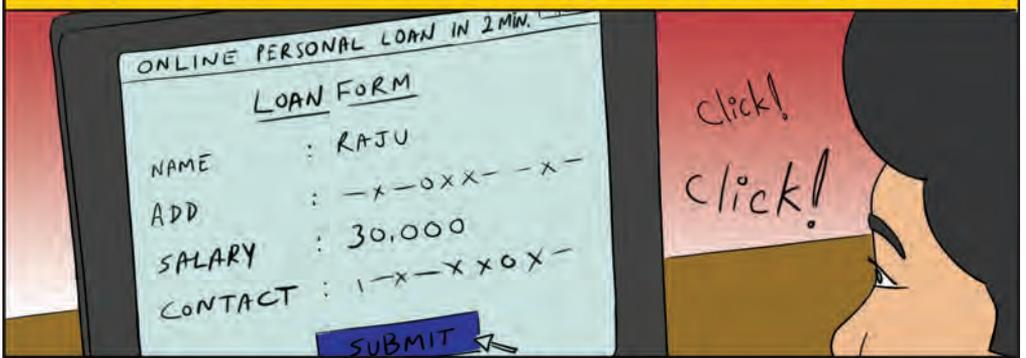
क्या करें:

- ✓ 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 सेवितरण 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 है.....



घोकत हुए, राजू ने बैंक का 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:
X 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

<p>राजू JKL क्रिकेट के नवीनतम सीज़न के लिए उत्साहित था।</p>	<p>राजू इंटरनेट पर JKL सट्टेबाजी समूहों की खोज करता है।</p>
<p>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।</p> 	
<p>जालसाज : स्वागत है, श्रीमान राजू। हमें खुशी है कि आपने सट्टेबाजी के बारे में पूछताछ की। मैं किस प्रकार आपकी मदद कर सकता हूँ?"</p> 	<p>राजू: "मैं इस JKL सीज़न के लिए एक शर्त लगाना चाहता हूँ।"</p> 
<p>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।"</p> 	
<p>क्या करें:</p> <ul style="list-style-type: none"> ✓ 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। 	



- क्या न करें:
- ✘ अनजान वेबसाइटों पर भुगतान नहीं करना चाहिए।

१९. नकली टीकाकरण कॉल

एक दिन राजू को एक अनजान नंबर से कॉल आया ।

जालसाज: "मैं स्थानीय स्वास्थ्य केंद्र से फोन कर रहा हूँ। हम आपके घर पर टीकाकरण की सुविधा उपलब्ध कराने के लिए कॉल कर रहे हैं।"



राजू: "अरे! ठीक। लेकिन हम इसे COWIN ऐप के जरिए ही कर सकते हैं, ठीक है ना?"



जालसाज: "हां सर, लेकिन ऐप पर घर पर टीकाकरण की सुविधा उपलब्ध नहीं है।"



राजू: "क्या कोई अतिरिक्त शुल्क है?"

जालसाज: "नहीं सर, यह नि:शुल्क है। मैं आपके पते की पुष्टि करूंगा, और आप टीके के लिए पंजीकृत हो जाएंगे। कृपया मुझे अपने आधार और पैन कार्ड के ब्यारे बताएं।"



क्या करें:

- ✓ ओटीपी जेनरेट करने का प्रयोजन समझने हेतु पूरा एसएमएस पढ़ें।
- ✓ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> पर करें।

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 हूँ, आपको एक पंजीकरण ओटीपी को प्राप्त होगा। कृपया इसे साझा करें।"

राजू को एक एसएमएस मिला- आपका सत्यापन कोड 1234 है

राजू: "हाँ, यह 1234 है।"

जालसाज: "धन्यवाद, सर। आपने वैकसीन 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

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।

'प्रिय ग्राहक, 50,000/- रुपये के व्यक्तिगत ऋण के लिए आपका अनुरोध सफलतापूर्वक स्वीकार कर लिया गया है।'

क्या न करें:

x 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

राजू घर पर ही कोविड-19 टेस्ट करना चाहते थे।

उन्होंने इंटरनेट पर उन डायग्नोस्टिक्स केंद्रों की खोज की जो घरेलू परीक्षण सुविधाएं प्रदान करते हैं।

राजू: "नमस्कार, मैं एक कोविड -19
टेस्ट बुक करना चाहता हूँ।"



जालसाज: "एबीसी डायग्नोस्टिक्स में आपका स्वागत है।
कृपया नमूना एकल करने के लिए अपना पता प्रदान करें।"



राजू: "मेरा पता 25,
एबीसी लेन, मुंबई, महाराष्ट्र है।
टेस्ट का शुल्क क्या होगा?"

जालसाज: "इसमें 1000/- रुपये खर्च होंगे और 100 रुपये
का होम कलेक्शन चार्ज होगा। साथ ही, आपको प्री-बुकिंग के
लिए 550/- रुपये का अग्रिम भुगतान करना होगा। मैं
आपके साथ प्री-बुकिंग के लिए भुगतान लिंक साझा करता हूँ।"



चूंकि राजू का परीक्षण करना जहरी था,

इसलिए वह अग्रिम राशि का भुगतान करने के लिए सहमत हो गया।

उन्होंने दिए गए लिंक पर अपने डेबिट कार्ड का उपयोग करके उक्त राशि का भुगतान किया।



क्या करें:

- ✓ किसी भी प्रकार के परीक्षण को हमेशा पंजीकृत पैथोलॉजी प्रयोगशालाओं के माध्यम से ही बुक करें।
- ✓ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> पर करें।

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
घोखा 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



राजू ने XYZ बैंक से लिए गए वाहन ऋण का उपयोग करके एक मोटरसाइकिल खरीदी थी। हालांकि, राजू की नौकरी चली गई और वह कर्ज की ईएमआई चुकाने के लिए संघर्ष कर रहा था। एक दिन एक घोखेबाज ने XYZ बैंक के रिकवरी एजेंट के वेश में राजू से उसके आवास पर संपर्क किया।

जालसाज: "मैं XYZ बैंक का एक रिकवरी एजेंट हूँ। यह देखा गया है कि आपने ऋण की बकाया चुकोती में चूक की है। मैं यहाँ आधिकारिक तौर पर आपका वाहन जब्त करने आया हूँ।"



जालसाज: "नहीं- नहीं! यह बैंक की प्रक्रिया है। आपके पास लगभग 20000/- रुपये बकाया हैं। आपको अभी कम से कम 5000/- का भुगतान करना होगा या मुझे वाहन लेना होगा।"



राजू: "अरे नहीं। कृपया मेरे वाहन को जब्त न करें। मेरी पिछली कुछ ईएमआई छूट गई है क्योंकि मेरी नौकरी चली गई थी। मेरे पास एक नई नौकरी का प्रस्ताव आया है और मैं अगले महीने से चुकाने का वादा करता हूँ।"



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 फॉर्म 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/एजेंसी फॉर्म 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 हूँ। 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 हूँ, 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 हूँ। देय राशि की वसूली के लिए कृपया मेरा आईडी कार्ड और बैंक का प्राधिकार पत्र देखें। क्या आपने उसकी आईडी देसी? क्या आपके पास भुगतान करने का कोई सबूत है?"



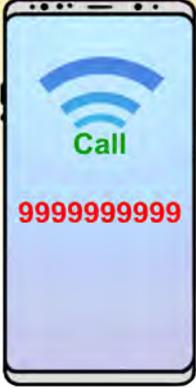
राजू: "अरे नहीं बाबा मैंने उस पर ऑन बंद करके भरोसा कर लिया।"

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

एक दिन राजू को एक अनजान नंबर से कॉल आया।



जालसाज - "मैं कृषि विभाग से फोन कर रहा हूँ। किसान योजना के लिए आपके खाते का विवरण अपडेट नहीं किया गया है, इसलिए आपकी लगभग 12000/- रुपये की सब्सिडी राशि हमारे पास बिना उपयोग के पड़ी है।"

राजू - "खाता अपडेट करने के लिए मुझे क्या करना चाहिए?"

जालसाज - "आप वेबसाइट पर जा सकते हैं और अपने आप अपडेट कर सकते हैं, अन्यथा, यदि आप मुझे अपने ब्योरे प्रदान करते हैं तो मैं इसे अपडेट कर दूंगा।"

क्या करें:

- ✓ सब्सिडी प्राप्त करने के लिए कोई भी भुगतान करने से पहले अपने ग्राम पंचायत या तहसीलदार कार्यालय से किसी भी सरकारी योजना के ब्योरे 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:

- ✗ कॉल पर सब्सिडी मिलने की ऐसी कहानियों पर कभी विश्वास न करें।
- ✗ पाल 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

राजू के मिल कृष्णा ने अच्छी कमाई की संभावना वाली एक योजना के बारे में समझाने के लिए उससे मुलाकात की।



कृष्णा: "हाई राजू! मुझे बहुत कम समय और निवेश के साथ पैसा कमाने का एक शानदार अवसर मिला।"



राजू: "ऐसा क्या? सुनने में अच्छा लग रहा है! मुझे इसके बारे में और बताएं। मुझे सब कुछ जानना है।"



कृष्णा: "आपको XYZ कंपनी के उत्पाद 20,000-रुपये में खरीदने होंगे, और आपको 10,000/- रुपये का मोबाइल फोन मुफ्त में मिलेगा। तीन और लोगों को नामांकित करने के बाद, आपको प्रति व्यक्ति 3,000/- रुपये का कमीशन मिलेगा, इसमें आप जितने अधिक लोगों को इस योजना के तहत लाते हैं उतना फायदा होगा।"



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। पॉजी 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 जरूरत 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 हूँ। 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।

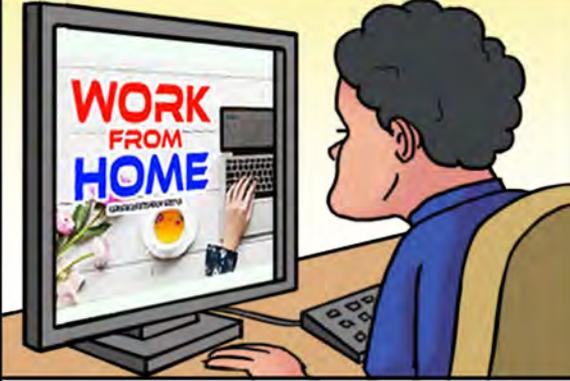
हालांकि, बिक्री निराशाजनक और अस्तिवहिन थी। वह 3 और एजेंटों की भर्ती के लिए कंपनी द्वारा निर्धारित लक्ष्यों को पूरा नहीं कर सका, और उसे 20000/ रुपये का नुकसान हुआ क्योंकि उसके द्वारा कंपनी से खरीदे गए उत्पाद नहीं बेचे जा सके। उसे कोई मोबाइल भी नहीं मिला।

क्या न करें:

✗ अज्ञात कंपनियों को पैसे न दें और अज्ञात योजनाओं में नामांकन न कराएं।

२४. वर्क फ्रॉम होम घोटाला

आकर्षक वेतन के साथ घर से काम करने के लिए एक जालसाज इंटरनेट और सोशल मीडिया पर नौकरियों का विज्ञापन करता है।
(घर से काम करके प्रतिदिन 1000/- रुपये कमाएँ)।



राजू विज्ञापन देखने के बाद बहुत उत्साहित है और वर्क फ्रॉम होमके लिए रजिस्टर करने के लिए लिंक पर क्लिक करता है।
राजू को एक अजनबी का फोन आता है।



जालसाज: "सर, हमारी एजेंसी के साथ पंजीकरण करने के लिए धन्यवाद। हमने आपके सीवी का अध्ययन कर लिया है, और आपको वर्क फ्रॉम होम जॉब के लिए चुना गया है। आपको अपना आधार और पैन कार्ड ब्योरा प्रदान करना होगा। आपको हमारी कंपनी की नीति के अनुसार कुछ फॉर्म भी भरने होंगे और कुछ दस्तावेजों पर हस्ताक्षर करने होंगे।"



राजू: "धन्यवाद। मैं सभी फॉर्म भरता हूँ और आपको अपना पता प्रमाण और पैन कार्ड ब्योरे भेजता हूँ।"



क्या करें:

- ✓ छोटे URL, अज्ञात स्रोतों से गूगल फॉर्म 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।



राजू धोखेबाज को सिक्क्योरिटी 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।



राजू को एक ही दिन में अलग-अलग नंबरों से कई उत्पीड़न और वसूली के कॉल आने लगे।



'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 फ्रम कभी सुरक्षा जमा राशि नहीं मांगती।

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।



राजू: "हैलो। मैंने आपकी वेबसाइट एबीसी देखी, और मैं एक नया स्मार्टफोन ढूंढ रहा हूँ।"



जालसाज: "सर, हमारी वेबसाइट में दिलचस्पी दिखाने के लिए धन्यवाद। हमारी कंपनी को फोन सीधे निर्माता से मिलता है, इसलिए आपको हमारी वेबसाइट पर सबसे अच्छी कीमत मिलेगी।"



राजू: "वाह! तब मैं एक वी20 मोबाइल फोन खरीदना चाहुंगा।"



जालसाज: "सर, मैं चाहुंगा कि आप इस साल के सबसे ज्यादा बिकने वाले फोन, यानी S20 FE को देखें। सर, यह बाजार में सबसे अच्छा स्मार्टफोन है। यदि आप पूरा भुगतान करके 1 घंटे के भीतर ऑर्डर देते हैं, तो आपको मोबाइल फोन की डिलीवरी के बाद कैशबैक के रूप में 50% राशि और मिलेगी।"



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' दिखाएँ, यह दर्शाता है कि लेनदेन सुरक्षित है।
- ✓ 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 फ्रीचर 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 ऑफर 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।"

जालसाज: "आपका फैसला बढ़िया है, सर। मैं आपको भुगतान के लिए एक लिंक भेज रहा हूँ। 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, घन 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।

सेल्स एजीक्यूटिव: "आपका कुल बिल 12000/- रुपये है,
सर। आप कैसे भुगतान करना चाहेंगे, कार्ड या नकद?"

RECEPTION

राजू: "मैं ऑनलाइन भुगतान करूंगा।"

राजू ने भुगतान शुरू किया लेकिन नेटवर्क की समस्या थी।

राजू: "मुझे लेन-देन के दौरान कनेक्टिविटी की समस्या का सामना
करना पड़ रहा है। क्या आप इसमें मेरी सहायता कर सकते हैं?"



सेल्स एजीक्यूटिव: "सर, अगर आपका नेटवर्क काम नहीं कर रहा है तो
आप फ्री वाई-फाई से जुड़ सकते हैं।"

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। "

सेल्स एग्जीक्यूटिव: "यहाँ खरीदारी के लिए
धन्यवाद, सर!"



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/- रुपये 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:

"दिवाली बंपर-ऑफर खरीदी गई
हर एक घड़ी के लिए - 2500/- रुपये
की तीन फ़ास्टट्रेक घड़ियाँ मुफ्त !
जल्दी करें ! ऑफर सीमित समय के लिए !
अधिक जानकारी के लिए कृपया
फोन करें: 90XXXXXXX99!"

राजू: 'वाह ! यह बहुत अच्छा लगता है! मैं एक घड़ी खरीदने पर
और 3 मुफ्त पा सकता हूँ! वैसे भी, मैं अपने चचेरे भाइयों को
इस दिवाली की छुट्टी में घर जाने पर उपहार देना चाहता था !
बेहतर होगा कि ऑफर खत्म होने से पहले मैं कॉल करूं।"



फोन पर राजू: "हैलो। मुझे आपका ब्रांडेड घड़ी
का ऑफर मिला। यह किस जगह है?
मैं खरीदारी के लिए आपके स्टोर
पर आ सकता हूँ।"



जालसाज: "सर! आप भाग्यशाली हैं।
हम ऑफर बस बंद करने जा रहे हैं।
आपको यहां आने की जरूरत नहीं है सर।
हम आपके पते पर माल पहुंचाएंगे।"



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।

राजू: "बहुत बढ़िया ! कृपया मुझे घड़ियों की तस्वीरें भेजें।"



जालसाज: "ज़रूर, सर। मैंने उन्हें पहले ही साझा कर दिया है। मैंने राशि के हस्तांतरण के लिए खाते का विवरण भी साझा किया है। ऑर्डर की पुष्टि के लिए आपको 3000/- रुपये का भुगतान करना होगा। भुगतान सफल होने के बाद, हम 3 दिनों के भीतर घड़ियाँ वितरित करेंगे। जल्दी करें सर। ऑफ़र अगले 30 मिनट में समाप्त हो जायेगा। दीपावली की हार्दिक शुभकामनाएं!!"



राजू: "ठीक है। मैंने अपना पता साझा कर दिया है। मैं अभी पैसे भेजता हूँ।"



3 दिन बाद:

राजू: "क्या हो गया? उन्होंने अभी तक घड़ियों की डिलीवरी क्यों नहीं की? उसका फोन स्विच ऑफ़ है। अब मैं उन्हें कैसे ट्रेस करूँ? मुझे लगता है कि मैंने पैसे खो दिए हैं।"

राजू ने वास्तव में अपना पैसा खो दिया।

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

राजू एक साधारण किसान है जो किसी तरह अपना गुज़ारा कर रहा है। एक दिन, उसे एक अजनबी का फोन आया।

जालसाज: "हैलो राजू। हम xyzy Pvt Ltd से कॉल कर रहे हैं। हमने आपके क्षेत्र के किसानों के लिए एक योजना शुरू की है। आपको हमारी कंपनी से रियायती दर पर ऋण लेने के योग्य पाया गया है।"



राजू: "अच्छा ! ठीक। इससे मुझे मदद मिलेगी। ऑफर क्या है?"



जालसाज: "हम केवल 3% की ब्याज दर पर 5 लाख रुपये तक का विशेष ऋण प्रदान करते हैं! इस ऋण का लाभ उठाने के लिए, आपको सत्यापन के लिए अपने बैंक खाते और आधार के ब्योरे साझा करने होंगे।"



राजू: "ठीक है। मैं इसके बारे में सोचूंगा और आपको बताऊंगा।"



क्या करें:

- ✓ ऋणदाता का ऋण लेने से पहले हमेशा उसके ब्योरे (जैसे उसका भौतिक पता / आधिकारिक वेबसाइट, आदि) की जाँच करें।
- ✓ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> पर करें।



राजू भुगतान करता है। हालाँकि, हफ्तों के बाद भी, उन्हें कंपनी की ओर से कोई जवाब नहीं मिला, और जिस नंबर से उन्हें कॉल आया, वह अब मौजूद नहीं है।



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।



जालसाज: "आपका कार्ड नंबर 45 से शुरू होता है। कृपया नंबर की पुष्टि करें।"

राजू: "ज़रूर। यह 4500 1000 1000 1000 है।"

जालसाज: "पुष्टि के लिए धन्यवाद। कृपया कार्ड के पीछे लिखी समाप्ति तिथि और कार्ड वेरिफिकेशन कोड (सीवीवी) की पुष्टि करें।"

राजू: "हाँ, समाप्ति तिथि 01/25 है और 111 सीवीवी नंबर है।"

राजू: "हाँ, यह 123456 है।"

जालसाज: "पुष्टि के लिए धन्यवाद, सर। आपको अंतिम एक्टिवेटण के लिए एक एसएमएस प्राप्त हुआ होगा। कृपया अपने फोन पर प्राप्त कोड की पुष्टि करें।"

जालसाज: "पुष्टि के लिए धन्यवाद। आपका कार्ड अब एक्टिवेट हो गया है, और आपको घंटे के भीतर इस संबंध में एक एसएमएस प्राप्त होगा। आपका दिन शुभ हो!"

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 ब्योरे 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 ब्योरे / ओटीपी किसी से साझा न करें, बैंक कभी भी ओटीपी नहीं मांगता।

३०. क्रेडिट कार्ड सीमा उन्नयन धोखाधड़ी

एक दिन राजू को एक बैंक से फोन आया।

जालसाज: हैलो, मिस्टर राजू। मैं XYZ बैंक से फोन कर रहा हूँ। बधाई हो, सर। आपका क्रेडिट कार्ड लिमिट अपग्रेड के योग्य है।"



राजू: "ओह, धन्यवाद। नई लिमिट क्या होगी?"



जालसाज: "नई लिमिट आपकी वर्तमान 1 लाख रुपये की सीमा से बढ़ाकर 5 लाख रुपये कर दी जाएगी।"



राजू: "ओह, यह बहुत अच्छा है!"



क्या करें:

- ✓ धोखाधड़ी का पता चलाने के बाद, आगे और ट्रैजिक्शन को रोकने के लिए बैंक को तुरंत कार्ड / खाता / यूपीआई सेवा को ब्लॉक करने के लिए क
- ✓ घटना की रिपोर्ट करने के लिए ईमेल / पत्र भेजें / अपनी गृह शाखा में जाएं।
- ✓ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> पर करें।



जालसाज: "सर, आपको फ्री लिमिट अपग्रेड कोड की पुष्टि करनी होगी जो आपको डिलीवर होगा। क्या मैं आगे बढ़ूं?"

राजू: "हाँ, प्लीज़।"

जालसाज: "आपका कार्ड नंबर 4500 1000 1000 1000 है। आपको एसएमएस में एक एक्टिवेशन कोड प्राप्त हुआ होगा। कृपया बताएं।"

राजू: "हाँ, यह 123456 है।"

जालसाज: "पुष्टि के लिए धन्यवाद। आपके कार्ड की सीमा अब अपग्रेड कर दी गई है, और आपको अगले 2 घंटों के भीतर इस संबंध में एक एसएमएस प्राप्त होगा। आपका दिन शुभ हो!"

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 व्योरे / ओटीपी किसी के साथ साझा न करें।

३१. आपके आधार कार्ड की सुरक्षा

एक दिन राजू अपने बैंक खाते से आधार कार्ड लिंक करवाने के लिए अपनी बैंक शाखा गया।

राजू: "मैं अपने आधार कार्ड को अपने बैंक खाते से जोड़ना चाहता हूँ।"



राजू आवश्यक दस्तावेज जमा करता है।

बैंक कर्मचारी: "कृपया आधार फॉर्म और अपने आधार कार्ड की फोटोकॉपी जमा करें। इसके अलावा, मुझे अपना असली आधार कार्ड दिखाएं।"

बैंक कर्मचारी: "मुझे अपने पंजीकृत मोबाइल नंबर पर प्राप्त ओटीपी बताएं।"



राजू: "मुझे कोई ओटीपी नहीं मिला।"

बैंक कर्मचारी: "ओटीपी आपके पंजीकृत मोबाइल नंबर पर भेजा गया था।"



राजू: "लेकिन मुझे कोई ओटीपी नहीं मिला। क्या आप कृपया मेरे बैंक खाते से जुड़े मोबाइल नंबर की जांच कर सकते हैं?"

बैंक कर्मचारी: "अभी देखती हूँ। आपके खाते से जुड़ा मोबाइल नंबर 98***25621 है।"



क्या करें:

- ✓ अपने बैंक खाते से जुड़े मोबाइल नंबर को सत्यापित करें।
- ✓ किसी भी संदिग्ध गतिविधि की पहचान करने के लिए नियमित रूप से अपने बैंक स्टेटमेंट और पासबुक की जांच करें।
- ✓ चटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> पर 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 ऑफर 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।

जालसाज: "नमस्कार सर! मैं ABC.com से कॉल कर रहा हूँ। सर, हमें आपको यह बताते हुए खुशी हो रही है कि हम आपको ABC.com से की खरीदारी पर 50% कैशबैक प्रदान कर रहे हैं।"



राजू: "ओह, सच में! 50% कैशबैक तो काफी बड़ा है। बहुत - बहुत धन्यवाद...!"



जालसाज: "सर, आप हमारे मूल्यवान ग्राहक हैं!"



राजू: "ठीक है, तो बताओ। कैशबैक मेरे खाते में कब जमा होगा?"



जालसाज: "सर, इसमें ज्यादा समय नहीं लगेगा। आपको ऐप खोलना होगा, और वहाँ कैशबैक के संबंध में एक पॉप-अप संदेश होगा।"



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।



राजू: "मैंने अपना ऐप खोला है। यह ABC.com को 20,000/रुपये का भुगतान अनुरोध दिखा रहा है।"

जालसाज: "यह सही है, सर। हमें आपके खाते में कैशबैक क्रेडिट करने के लिए आपकी स्वीकृति लेनी होगी। तो कृपया Y पर क्लिक करें।"

राजू: "ठीक है, अब यह मेरा यूपीआई पिनमांग रहा है।"

जालसाज: "कृपया अपना पिन दर्ज करें क्योंकि यह सिर्फ सत्यापन उद्देश्यों के लिए है।"

राजू: "ठीक है।"

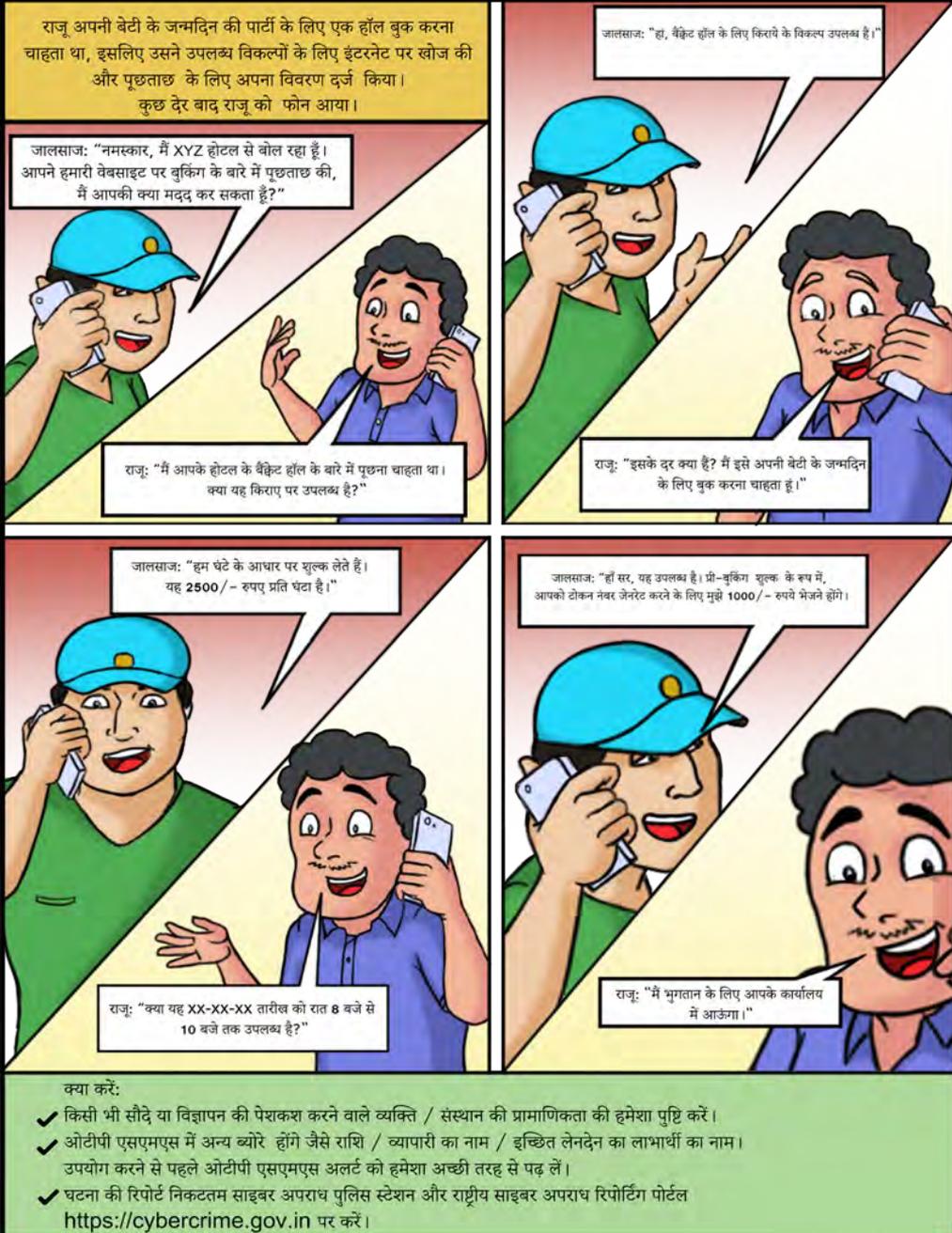
जालसाज: "धन्यवाद, सर। आपको शीघ्र ही आपके खाते में भुगतान प्राप्त होगा।"

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



राजू अपनी बेटी के जन्मदिन की पार्टी के लिए एक हॉल बुक करना चाहता था, इसलिए उसने उपलब्ध विकल्पों के लिए इंटरनेट पर खोज की और पूछताछ के लिए अपना विवरण दर्ज किया। कुछ देर बाद राजू को फोन आया।

जालसाज: "नमस्कार, मैं XYZ होटल से बोल रहा हूँ। आपने हमारी वेबसाइट पर बुकिंग के बारे में पूछताछ की, मैं आपकी क्या मदद कर सकता हूँ?"

राजू: "मैं आपके होटल के बैंक्रेट हॉल के बारे में पूछना चाहता था। क्या यह किराए पर उपलब्ध है?"

जालसाज: "हां, बैंक्रेट हॉल के लिए किराये के विकल्प उपलब्ध हैं।"

राजू: "इसके दर क्या हैं? मैं इसे अपनी बेटी के जन्मदिन के लिए बुक करना चाहता हूँ।"

जालसाज: "दुम घंटे के आधार पर शुल्क लेते हैं। यह 2500/- रुपये प्रति घंटा है।"

जालसाज: "हां सर, यह उपलब्ध है। प्री-बुकिंग शुल्क के रूप में, आपको टोकन नंबर जेनरेट करने के लिए मुझे 1000/- रुपये भेजने होंगे।"

राजू: "क्या यह XX-XX-XX तारीख को रात 8 बजे से 10 बजे तक उपलब्ध है?"

राजू: "मैं भगतान के लिए आपके कार्यालय में आऊंगा।"

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।



- 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।

NEWS REPORT

रिपोर्ट: 'अभिनेता मोनू ने सरकारी स्कूल के छात्रों को 100 स्मार्टफोन उपहार में दिए।'

राजू ने इंटरनेट पर अभिनेता के चैरिटी फाउंडेशन के बारे में खोजा और नंबर पर कॉल किया।

MONU
charity
Foundation

राजू: "नमस्कार, सर। क्या यह अभिनेता मोनू का चैरिटी फाउंडेशन है ?

जालसाज: "हां सर। यह उनके ऑफिस का नंबर है। मैं उनका निजी सचिव हूँ। मैं आपकी क्या मदद कर सकता हूँ?"

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: "सर मैं राजू हूँ, XXXX सरकारी स्कूल से फोन कर रहा हूँ। मैंने आपके द्वारा छात्रों को दान में स्मार्टफोन प्रदान करने वाले समाचार के बारे में देखा। सर, हमारे स्कूल में 100 गरीब छात्र हैं जो लैपटॉप/स्मार्टफोन नहीं खरीद सकते। क्या आप कृपया हमारी मदद कर सकते हैं?"

जालसाज: "जी हाँ! गरीब बच्चों की ओर से हमसे संपर्क करने के लिए आपका बहुत-बहुत धन्यवाद। मैं आपको मदद का आश्वासन देता हूँ।"

राजू: "यह बहुत ही अच्छा होगा! महोदय।"

जालसाज: "ठीक है। कृपया अपना पता साझा करें। हम आपको 100 स्मार्टफोन भेजेंगे। हालांकि, हमें फोन भेजने के लिए आपको आज ही 50,000/- रुपये का टोकन पंजीकरण शुल्क देना होगा। फोन एक हफ्ते में डिलीवर हो जाएंगे, और डिलीवरी के बाद हम रजिस्ट्रेशन फीस वापस कर देंगे।"

राजू: "ठीक है सर। मैं आपको तुरंत पंजीकरण शुल्क भेजता हूँ कृपया अपने खाते का ब्योरे साझा करें।"

जालसाज: "ठीक है सर। मैं आपको तुरंत पंजीकरण शुल्क भेजता हूँ कृपया अपने खाते का ब्योरे साझा करें।"

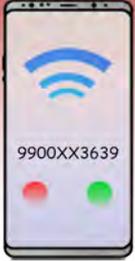
राजू ने पैसा ट्रांसफर कर दिया, लेकिन बाद में उन्हें पता चला कि सरकारी स्कूल के छात्रों को ऐसा कोई मोबाइल फोन दान नहीं किया गया था। राजू को अहसास हुआ कि दान के बहाने धोखेबाजों ने उसे ठगा है।

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

राजू एक वरिष्ठ नागरिक है, जो हाल ही में अपनी नौकरी से सेवानिवृत्त हुआ था और उसे एक बड़ी राशि मिली थी, जिसे वह निवेश करना चाहता था। एक दिन राजू को एक प्रतिष्ठित बैंक का कर्मचारी / एजेंट होने का दावा करने वाले व्यक्ति का फोन आया, जो ऊँचे ब्याज दरों वाली नयी योजना का प्रचार कर रहा था।



राजू: "नमस्कार! क्या यह पक्का है कि मुझे 9% ब्याज दर मिलेगा? क्योंकि कोई भी बैंक 7.1% से ज्यादा ब्याज नहीं दे रहा है।"

जालसाज: "हाँ सर, यह एक सीमित अवधि के लिए ही एक विशेष योजना है।"



राजू: "ठीक है, मैं बैंक जाऊंगा और सावधि जमा खोलूंगा।"



जालसाज: "सर, चूंकि आप एक वरिष्ठ नागरिक हैं, हमारा बैंक आपके घर एक प्रतिनिधि भेजेगा।"

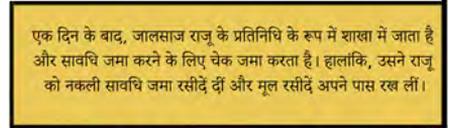


राजू: "नहीं, मैं अपना पैसा किसी अनजान व्यक्ति को नहीं सौंप सकता।"



क्या करें:

- ✓ हस्ताक्षर करने से पहले सभी दस्तावेजों की जांच करें।
- ✓ किसी ज्ञात व्यक्ति की सहायता से इंटरनेट बैंकिंग पर लेनदेन करना या बैंक शाखा में जाने को प्राथमिकता दें।
- ✓ साइबर अपराध के मामले में घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन या राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> पर करें।



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 रसीदें 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।

राजू: "नमस्ते, मुझे फ्रीलान्स काम करने के बारे में एक एसएमएस मिला। वर्क प्रोफाइल क्या है?"



राजू: (यह बहुत आसान है, यहाँ तक कि मेरा बेटा भी इसे कर सकता है।)
"ठीक है, मुझे इसमें दिलचस्पी है।"



एप्लिकेशन 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 एप्लिकेशन के माध्यम से राजू के डिवाइस से सभी गोपनीय जानकारी प्राप्त करने में सक्षम था। दुर्भाग्यपूर्ण 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 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

राजू और रामू सबसे अच्छे दोस्त थे। एक दिन, राजू रामू से मिला और उसे अपनी आर्थिक समस्याओं के बारे में बताया।

राजू: "मुझे तत्काल धन की आवश्यकता है; मैं क्या करूँ?"

रामू: "घबराने की जरूरत नहीं है मेरे दोस्त। कई मोबाइल ऐप बिना किसी दस्तावेज या सुरक्षा के तत्काल ऋण प्रदान करते हैं।"

राजू: "ओह, यह बहुत अच्छा है! बिना किसी दस्तावेज के जल्दी पैसा! क्रेडिट स्कोर भी चेक नहीं किया जा रहा है। मैं तुरंत 5000/- रुपये का ऋण लूंगा।"

राजू ऋण प्रदान करने वाली इकाई के पंजीकृत होने की पुष्टि किए बिना एक मोबाइल ऐप डाउनलोड करता है। उसके बैंक खाते में कुछ ही समय में 5000/- रुपये आ जाते हैं।

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 बैंड 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. मर्चेट आउटलेट्स पर कार्ड क्लोनिंग

एक दिन राजू अपने दोस्त के साथ एक रेस्टोरेंट में लंच करने गया। उसने वेटर को बुलाया।

वेटर: "स्वागत है, सर। कृपया बैठिए।"

राजू: "धन्यवाद।"

वेटर: "सर, मैं आपके लिए क्या कर सकता हूँ?"

राजू: "क्या मैं आपका मेन्यू कार्ड देख सकता हूँ?"

राजू ने खाना ऑर्डर किया और अपने दोस्तों के साथ भोजन का आनंद लिया।

वेटर: "ज़रूर सर। यह हमारा मेन्यू कार्ड है।"

राजू: "कृपया बिल लाएँ।"

क्या करें:

- ✓ डेबिट / क्रेडिट कार्ड से लेनदेन करते समय हमेशा अपना पिन नंबर छिपाएँ।
- ✓ समय-समय पर पिन बदलते रहें।
- ✓ व्यापारियों / डीलरों को हमेशा अपनी उपस्थिति में कार्ड स्वाइप करने के लिए कहें।
- ✓ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> पर करें।"



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 स्किमर 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

राजू एक बहुत ही मिलनसार और मददगार व्यक्ति है, लेकिन जब अपनी वित्तीय साख अथवा बैंक के ब्योरे की सुरक्षा करने की बात आती है तो इस मामले में वह लापरवाह है।

केशव: "नमस्कार, राजू! आप से बात कर सकता हूँ?"

राजू: "हाँ, केशव, बोलो"

राजू: "ठीक है मैं अपने कार्ड के ब्योरे भेजता हूँ।"

राजू ने अपने क्रेडिट कार्ड की एक फोटो अपने दोस्त के साथ शेयर की।

केशव: "xyz ई-कॉमर्स वेबसाइट पर एक रोमांचक ऑफर है। इसके लिए बैंक द्वारा जारी क्रेडिट कार्ड की आवश्यकता है। आप इस कार्ड का उपयोग कर रहे हैं। क्या आप मुझे फोन पर अपने क्रेडिट कार्ड का ब्योरे भेज सकते हैं? मैं आपको बाद में भुगतान करूँगा।"



राजू के दोस्त हमेशा ई-कॉमर्स वेबसाइटों द्वारा दी जाने वाली छूट का लाभ उठाने के लिए उसके कार्ड का उपयोग करते हैं, और वह अक्सर अपने कार्ड के ब्योरे अपने दोस्तों को फोन पर भेजता है।

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 कहाँ किया गया था।

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

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

राजू ने महसूस किया कि उसने खुद ऑनलाइन साइट पर कभी कोई भुगतान नहीं किया था, लेकिन उसने अपने कार्ड का ब्योरे 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।

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

क्या न करें:

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

४०. भुगतान स्पूफिंग एप्लिकेशन

राजू एक दोस्ताना मिजाज का खुदरा दुकान का मालिक है। वह अपनी दुकान पर बैठा था तभी एक ग्राहक आया और उसने कुछ खरीदा।



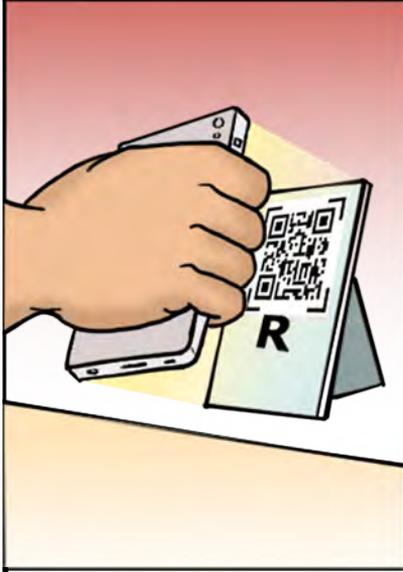
ग्राहक (जालसाज): "क्या मैं आपकी दुकान के क्यूआर कोड को स्कैन करके xyz एप्लिकेशन के माध्यम से भुगतान कर सकता हूँ?"



राजू: "हाँ, यह रहा कोड। कृपया स्कैन करें और भुगतान करें।"

क्या करें:

- ✓ जब भी कोई लेनदेन यूपीआई के माध्यम से किया जाता है तो हमेशा अपने बैंक खाते की जांच करके लेनदेन की जांच / पुष्टि करें।
- ✓ घटना की रिपोर्ट निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> पर करें।"



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।



- क्या न करें:
- ✗ फंड की वास्तविक प्राप्ति के बिना वित्तीय लेनदेन समाप्त न करें।







भारतीय रिज़र्व बैंक