സൈബർ ഭ്രമം

.apk ഫയലുകളുടെ അപകടങ്ങളെ സൂക്ഷിക്കുക, കാർട്ടൂൺ പുസ്തകം: സ്ക്രിപ്റ്റ്

साइबर मायाजाल

.apk फाइल के खतरों से सावधान.

विवरण सामग्री संदर्भ साहित्य 2024

നിങ്ങളുടെ സുരക്ഷ ഞങ്ങളുടേതാണ്

आपकी सुरक्षा हमारे साथ

സൈബർ സുരക്ഷ മികവ് കേന്ദ്രം
साइबर सुरक्षा उत्कृष्टता केंद्र

यूनियन बैंक ऑफ इंडिया
Union Bank of India

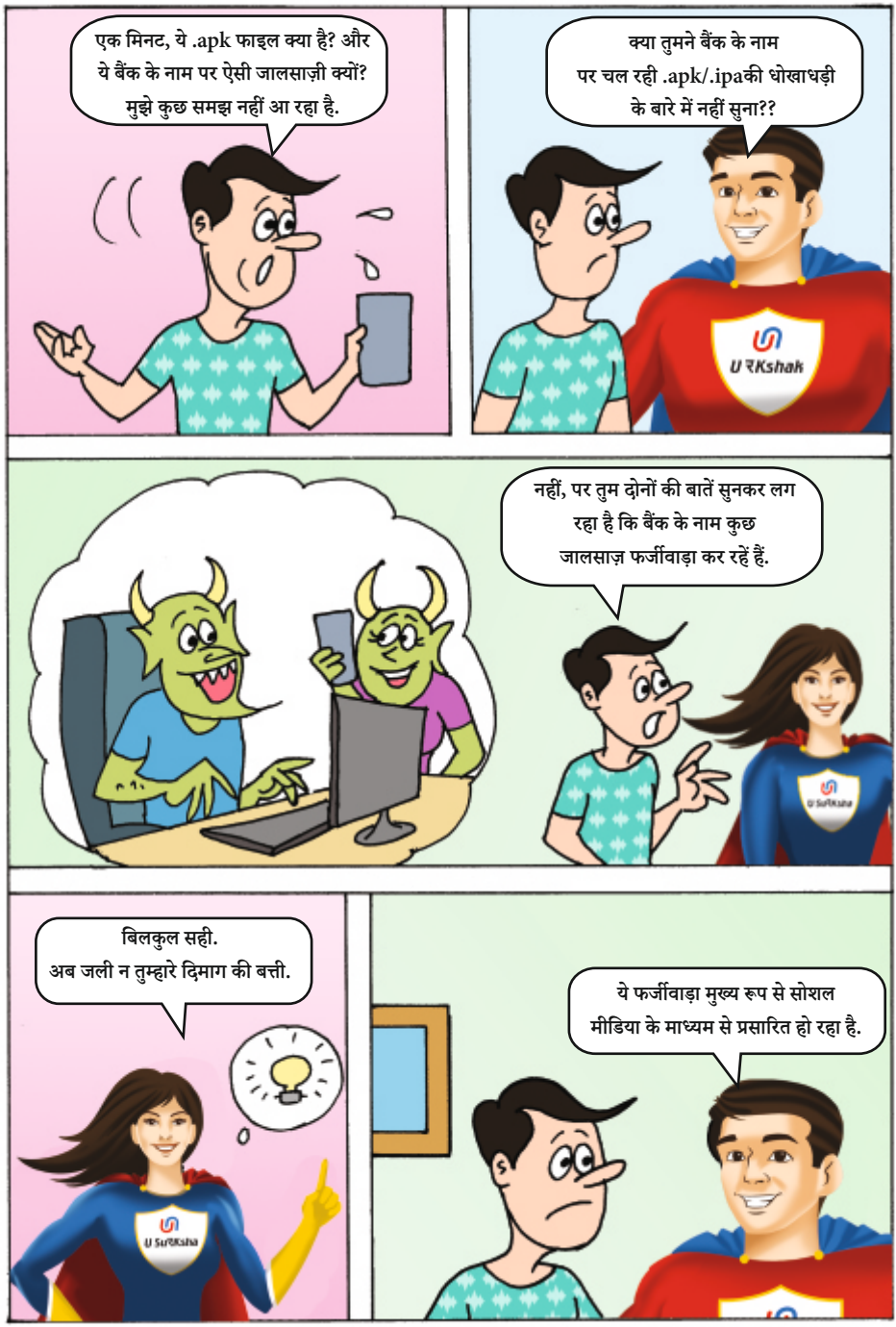
अच्छे लोग, अच्छा बैंक Good people to bank with

अंचल कार्यालय, मंगलूरु / ZONAL OFFICE, MANGALURU


.apk യുടെ ഒരു റിവാർഡ് ഫയൽ രമേശിന്റെ ഫോണിൽ യൂണിയൻ ബാങ്കിന്റെ പേരിൽ ലഭിക്കുന്നു, അത് രക്ഷക് ക്ലിക്കുചെയ്ത് കാണുന്നു)
ഹേയ്, നിങ്ങൾ എന്താണ് ചെയ്യുന്നത്? ഈ ഫയലിൽ ക്ലിക്ക് ചെയ്യരുത്. (ജാഗ്രതയോടെ പറയുന്നു)
U RKshak
U SuRksha
പക്ഷെ എന്തിന്? യൂണിയൻ ബാങ്കിൽ നിന്ന് എത്ര വലിയ റിവാർഡ് ഓഫർ വന്നിരിക്കുന്നുവെന്ന് നോക്കൂ.
U RKshak
ഹേയ് സർ, സൂക്ഷിച്ചു നോക്കൂ, ഇത് നിങ്ങളുടെ കഷ്ടപ്പെട്ട് സമ്പാദിച്ച പണവും മറ്റ് സ്വകാര്യ വിവരങ്ങളും മോഷ്ടിക്കാനുള്ള ഒരു കെണിയാണ്.
എന്ത്? (ആശ്ചര്യത്തോടെ) നിങ്ങൾ എന്താണ് സംസാരിക്കുന്നത്? എന്നാൽ, ഇത് ബാങ്കിൽ നിന്നാണ് വന്നത്.
ഇതാണ് വഞ്ചന. യൂണിയൻ ബാങ്ക് ഒരിക്കലും .apk/.ipa ഫയലുകൾ ഒരു രൂപത്തിലും അയയ്ക്കില്ല.
?
U SuRksha


रमेश के फोन पर यूनियन बैंक के नाम से .apk की रिवार्ड फ़ाइल प्राप्त की जाती है जिस पर क्लिक करते हुए रक्षक देख लेता है
अरे अरे, यह क्या कर रहे हो तुम ? इस फ़ाइल पर क्लिक मत करना.
U RKshak
U SuRKsha
पर क्यों? देखो न रिवार्ड्स का कितना बढ़िया ऑफर आया है- यूनियन बैंक की ओर से.
U RKshak
अरे महाशय, ध्यान से देखिए यह एक जाल है- तुम्हारी मेहनत की कमाई और अन्य निजी जानकारी चुराने का.
क्या? क्या बात कर रहे हो? पर, यह तो बैंक की तरफ से आया है.
यही तो धोखा है. यूनियन बैंक कभी भी .apk/.ipa फाइल्स किसी भी रूप में नहीं भेजता है.
U SuRKsha
?


ഒരു നിമിഷം, എന്താണ് ഈ .apk ഫയൽ? പിന്നെ എന്തിനാണ് ബാങ്കിന്റെ പേരിൽ ഇത്തരം തട്ടിപ്പ്? എനിക്ക് ഒന്നും മനസ്സിലാകുന്നില്ല (ആശങ്കയോടെ ചോദിക്കുന്നു)
യൂണിയൻ ബാങ്കിന്റെ പേരിൽ മാർക്കറ്റിൽ നടക്കുന്ന .apk/.ipa തട്ടിപ്പിനെക്കുറിച്ച് നിങ്ങൾ കേട്ടിട്ടില്ലേ??
U ₹Kshak
ഇല്ല, നിങ്ങൾ രണ്ടുപേരുടെയും വാക്കുകൾ കേട്ടപ്പോൾ ബാങ്കിന്റെ പേരിൽ ചില തട്ടിപ്പുകാർ തട്ടിപ്പ് നടത്തുന്നതായി തോന്നുന്നു.
കൃത്യമായി. ഇപ്പോൾ നിങ്ങളുടെ തലയില് വെളിച്ചം കത്തിയല്ലേ..
U SuRKsha
സോഷ്യൽ മീഡിയയിലൂടെയാണ് ഈ തട്ടിപ്പ് പ്രധാനമായും പ്രചരിക്കുന്നത്.

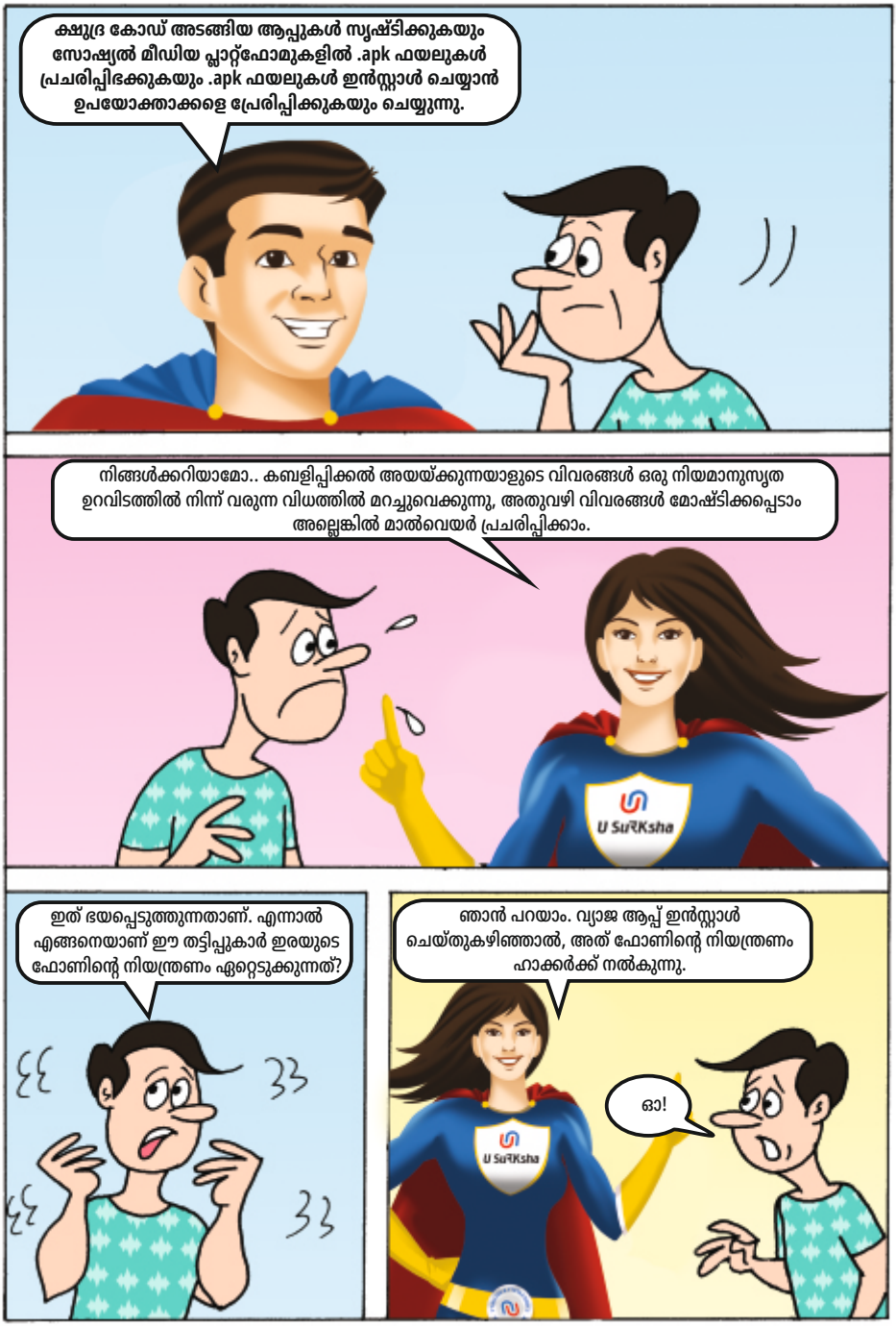

एक मिनट, ये .apk फाइल क्या है? और ये बैंक के नाम पर ऐसी जालसाज़ी क्यों? मुझे कुछ समझ नहीं आ रहा है.
क्या तुमने बैंक के नाम पर चल रही .apk/.ipaकी धोखाधड़ी के बारे में नहीं सुना??
U RKshak
नहीं, पर तुम दोनों की बातें सुनकर लग रहा है कि बैंक के नाम कुछ जालसाज़ फर्जीवाड़ा कर रहें हैं.
बिलकुल सही. अब जली न तुम्हारे दिमाग की बत्ती.
U SuRKsha
ये फर्जीवाड़ा मुख्य रूप से सोशल मीडिया के माध्यम से प्रसारित हो रहा है.


അതെ, ശരിയാണു, അതുപോലെ തന്നെ എന്റെ പരിചയക്കാരിൽ ഒരാൾക്ക് ആദായ നികുതി വകുപ്പിൽ നിന്ന് റീഫണ്ട് മെസ്സേജ് വന്നു.
അവനോടും .apk ലിങ്കിൽ ക്ലിക്ക് ചെയ്യാൻ ആവശ്യപ്പെട്ടു.
ഓ.
U ₹Kshak
എന്നാൽ കാലക്രമേണ, തനിക്കു റീഫണ്ട് ഇല്ലല്ലോന്നു അവൻ ഓർത്തു. അതിനാൽ വഞ്ചകരുടെ കെണിയിൽ അകപ്പെടാതെ രക്ഷപ്പെട്ടു.
സുരക്ഷയും രക്ഷകും ഈ സൈബർ ഭീഷണിയുടെ പ്രവർത്തനത്തെക്കുറിച്ചും സംരക്ഷണ പോയിന്റുകളെക്കുറിച്ചും അവരുടെ സുഹൃത്തിനെ അറിയിക്കുന്നു.)
ഇതൊരു കബളിപ്പിക്കൽ രീതിയാണ് - ഒരു തരം സൈബർ തട്ടിപ്പ്.
U ₹Kshak
അതുകൊണ്ടാണ് ഇന്നത്തേ കാലത്തു സൈബർ സുരക്ഷയെക്കുറിച്ച് അപ്ഡേറ്റ് ആവേണ്ടത് വളരെ പ്രധാനമാണ്.

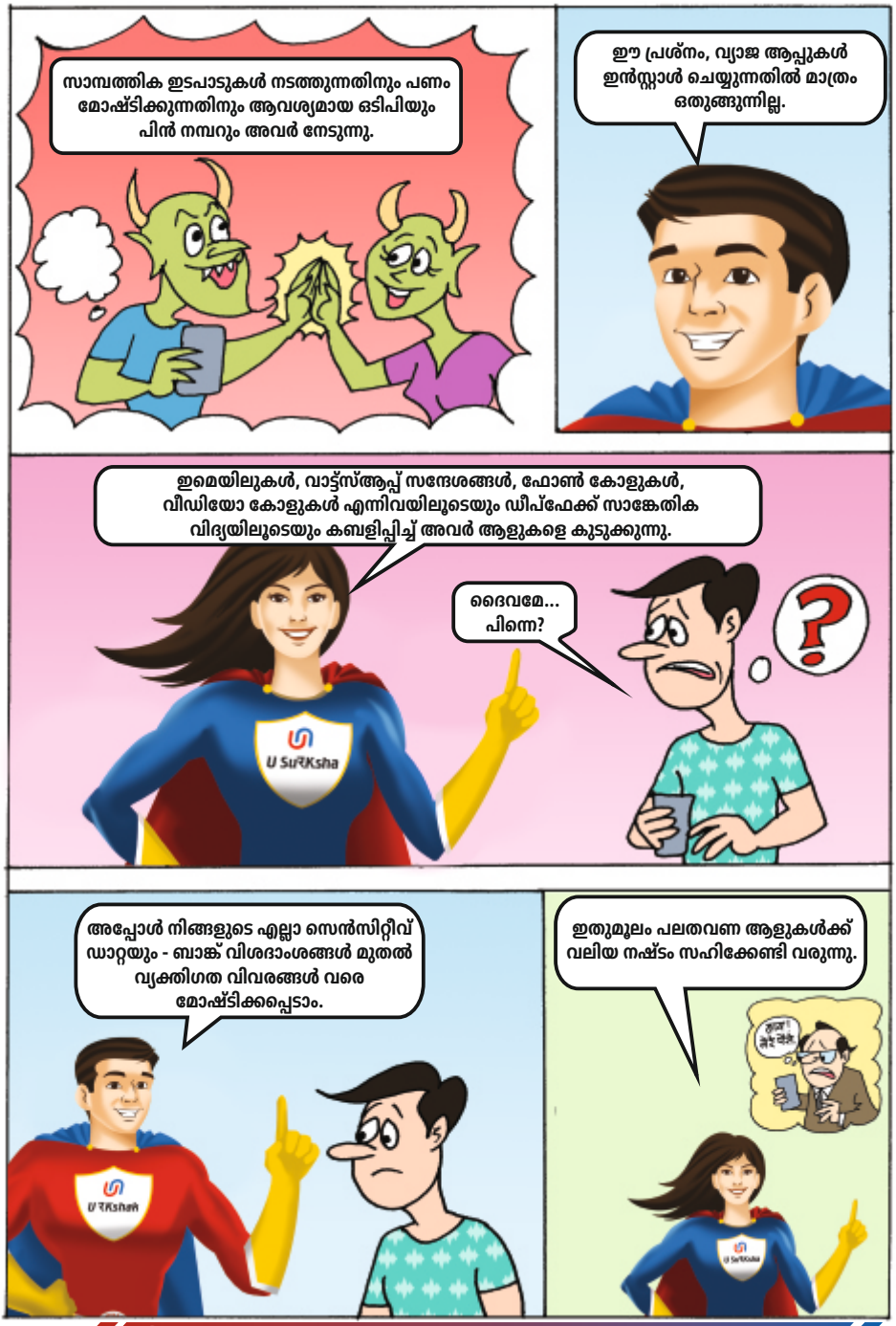

अच्छा, हाँ... ऐसे ही, मेरे एक जानकार को आयकर विभाग के रूप में रिफंड का संदेश आया था.
उसे भी .apk लिंक पर क्लिक करने को कहा गया था.
ओह.
U RKshak
लेकिन समय रहते उसे याद आ गया कि उसका रिफंड तो बनता ही नहीं है . इसलिए वह धोखेबाजों के जाल में फंसने से बच गया.
सुरक्षा और रक्षक अपने मित्र को इस साइबर खतरे की कार्य प्रणाली और बचाव के बिन्दुओं से अवगत करवाते हैं.
यह स्पूफिंग का तरीका है- जो एक प्रकार का साइबर फ्रौड है.
U RKshak
इसीलिए आजकल साइबर सुरक्षा के बारे में अपडटेड रहना बहुत ज़रूरी है.


നീ പറഞ്ഞത് ശരിയാണ്. എനിക്ക് ഇതിനെ കുറിച്ച് അധികം അറിയില്ല. നിങ്ങൾക്കറിയാമെങ്കിൽ എന്നോട് പറയൂ, എനിക്ക് അതിനെക്കുറിച്ച് എല്ലാം അറിയണം.
ഈ .apk തട്ടിപ്പ് എങ്ങനെയാണ് പ്രവർത്തിക്കുന്നത്? ഇത് ഒഴിവാക്കാനുള്ള വഴികൾ എന്തൊക്കെയാണ്? ഒരാൾ ഇതിന് ഇരയായാൽ എവിടെയാണ് ബന്ധപ്പെടേണ്ടത്... എല്ലാം...
ഇപ്പോൾ നിങ്ങൾ ശരിയായ ചോദ്യം ചോദിച്ചു!!
ഹേയ് കേൾക്കൂ, മൂന്നാം കക്ഷി ആപ്ലിക്കേഷനുകൾ ഇൻസ്റ്റാൾ ചെയ്യാൻ മൊബൈൽ കമ്പനികൾ ഉപഭോക്താക്കളെ അനുവദിക്കുന്നു.
തട്ടിപ്പുകാർ ഈ സവിശേഷത പ്രയോജനപ്പെടുത്തുന്നു..

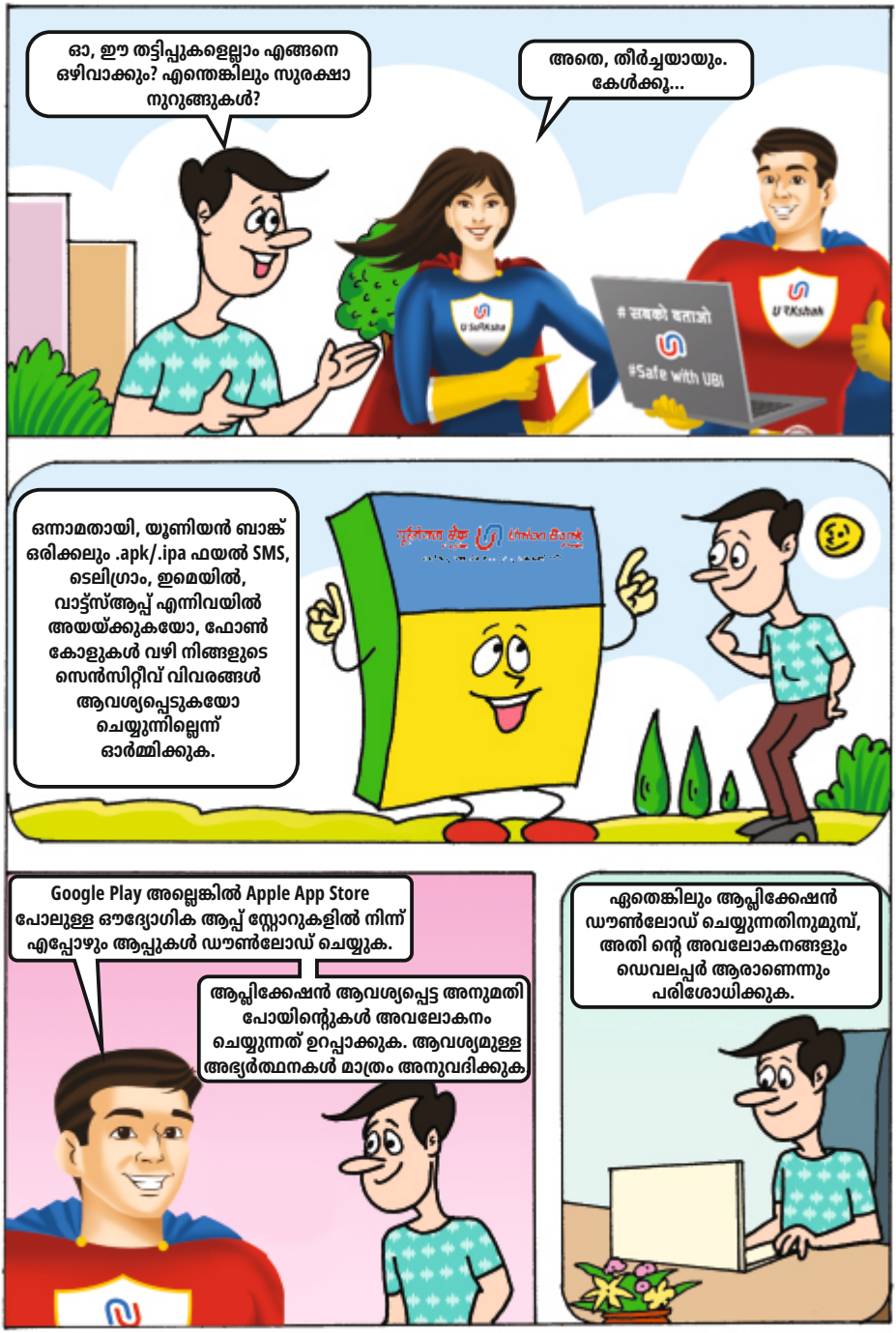

सही कहा यार. मुझे इस बारे में अधिक जानकारी नहीं है. अगर तुम्हें पता है तो तुम बताओ, मैं इसके बारे में सब कुछ जानना चाहता हूँ.
ये .apk धोखाधड़ी कैसे काम करती है? इससे बचने के तरीके क्या हैं ? इसका शिकार होने पर कहाँ संपर्क करना चाहिए.... सब कुछ ...
अब किया न तुमने सही सवाल!!
अरे सुनो, मोबाइल कंपनियाँ उपयोकर्ताओं को थर्ड पार्टी एप्लीकेशन इंस्टॉल करने की अनुमति देती है.
धोखेबाज इस सुविधा का फायदा उठाते हैं..


ക്ഷുദ്ര കോഡ് അടങ്ങിയ ആപ്പുകൾ സൃഷ്ടിക്കുകയും സോഷ്യൽ മീഡിയ പ്ലാറ്റ്ഫോമുകളിൽ .apk ഫയലുകൾ പ്രചരിപ്പിഭക്കുകയും .apk ഫയലുകൾ ഇൻസ്റ്റാൾ ചെയ്യാൻ ഉപയോക്താക്കളെ പ്രേരിപ്പിക്കുകയും ചെയ്യുന്നു.
നിങ്ങൾക്കറിയാമോ.. കബളിപ്പിക്കൽ അയയ്ക്കുന്നയാളുടെ വിവരങ്ങൾ ഒരു നിയമാനുസൃത ഉറവിടത്തിൽ നിന്ന് വരുന്ന വിധത്തിൽ മറച്ചുവെക്കുന്നു, അതുവഴി വിവരങ്ങൾ മോഷ്ടിക്കപ്പെടാം അല്ലെങ്കിൽ മാൽവെയർ പ്രചരിപ്പിക്കാം.
U SuRKsha
ഇത് ഭയപ്പെടുത്തുന്നതാണ്. എന്നാൽ എങ്ങനെയാണ് ഈ തട്ടിപ്പുകാർ ഇരയുടെ ഫോണിന്റെ നിയന്ത്രണം ഏറ്റെടുക്കുന്നത്?
ഞാൻ പറയാം. വ്യാജ ആപ്പ് ഇൻസ്റ്റാൾ ചെയ്തുകഴിഞ്ഞാൽ, അത് ഫോണിന്റെ നിയന്ത്രണം ഹാക്കർക്ക് നൽകുന്നു.
ഓ!
U SuRKsha


और मैलिशियस कोड युक्त ऐप बनाकर .apk फ़ाईलस को सोशल मीडिया के प्लैटफ़ार्मस् पर प्रसारित कर देते हैं और उपयोगकर्ताओं से .apk फाइलें इंस्टॉल करवा लेते हैं.
तुम्हें पता है.. स्पूफिंग सेंडर की जानकारी को इस तरह से छुपाता है कि यह वैध स्रोत से आया हुआ लगता है ताकि जानकारी चुराई जा सके या मैलवेयर फैलाया जा सके.
U SuRKsha
यह तो डरावना है. लेकिन ये धोखेबाज पीड़ित के फोन को कैसे नियंत्रित करते हैं?
बताती हूँ...बताती हूँ, एक बार जब नकली ऐप इन्स्टाल हो जाता है, तो यह फोन का नियंत्रण हैकर को दे देता है.
ओह !
U SuRKsha


സാമ്പത്തിക ഇടപാടുകൾ നടത്തുന്നതിനും പണം മോഷ്ടിക്കുന്നതിനും ആവശ്യമായ ഒടിപിയും പിൻ നമ്പറും അവർ നേടുന്നു.
ഈ പ്രശ്നം, വ്യാജ ആപ്പുകൾ ഇൻസ്റ്റാൾ ചെയ്യുന്നതിൽ മാത്രം ഒതുങ്ങുന്നില്ല.
ഇമെയിലുകൾ, വാട്ട്സ്ആപ്പ് സന്ദേശങ്ങൾ, ഫോൺ കോളുകൾ, വീഡിയോ കോളുകൾ എന്നിവയിലൂടെയും ഡീപ്ഫേക്ക് സാങ്കേതിക വിദ്യയിലൂടെയും കബളിപ്പിച്ച് അവർ ആളുകളെ കുടുക്കുന്നു.
U SuRKsha
ദൈവമേ... പിന്നെ?
?
അപ്പോൾ നിങ്ങളുടെ എല്ലാ സെൻസിറ്റീവ് ഡാറ്റയും - ബാങ്ക് വിശദാംശങ്ങൾ മുതൽ വ്യക്തിഗത വിവരങ്ങൾ വരെ മോഷ്ടിക്കപ്പെടാം.
ഇതുമൂലം പലതവണ ആളുകൾക്ക് വലിയ നഷ്ടം സഹിക്കേണ്ടി വരുന്നു.


जिससे वे वित्तीय लेन-देन करने और पैसे चुराने के लिए ज़रूरी ओटीपी और पिन हासिल कर लेता है.
यह पूरा प्रकरण केवल नकली ऐप इंस्टॉल करने तक सीमित नहीं रहता हैं.
वे ईमेल, व्हाट्सएप संदेशों, फोन कॉल, वीडियो कॉल और यहां तक कि डीपफेक तकनीक के माध्यम से भी स्पूफिंग का उपयोग करके लोगों को अपने जाल में फसा लेते हैं.
बाप रे... फिर?
U SuRKsha
फिर तुम्हारा सारा संवेदनशील डाटा- बैंक डिटेल्स से लेकर निजी जानकारी तक, सभी कुछ चुराया जा सकता है.
जिसकी वजह से कई बार लोगों को भारी नुकसान भी उठाना पड़ता है.


ഓ, ഈ തട്ടിപ്പുകളെല്ലാം എങ്ങനെ ഒഴിവാക്കും? എന്തെങ്കിലും സുരക്ഷാ നുറുങ്ങുകൾ?
അതെ, തീർച്ചയായും. കേൾക്കൂ...
सबको बताओ
#Safe with UBI
ഒന്നാമതായി, യൂണിയൻ ബാങ്ക് ഒരിക്കലും .apk/.ipa ഫയൽ SMS, ടെലിഗ്രാം, ഇമെയിൽ, വാട്ട്സ്ആപ്പ് എന്നിവയിൽ അയയ്ക്കുകയോ, ഫോൺ കോളുകൾ വഴി നിങ്ങളുടെ സെൻസിറ്റീവ് വിവരങ്ങൾ ആവശ്യപ്പെടുകയോ ചെയ്യുന്നില്ലെന്ന് ഓർമ്മിക്കുക.
Google Play അല്ലെങ്കിൽ Apple App Store പോലുള്ള ഔദ്യോഗിക ആപ്പ് സ്റ്റോറുകളിൽ നിന്ന് എപ്പോഴും ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യുക.
ആപ്ലിക്കേഷൻ ആവശ്യപ്പെട്ട അനുമതി പോയിന്റുകൾ അവലോകനം ചെയ്യുന്നത് ഉറപ്പാക്കുക. ആവശ്യമുള്ള അഭ്യർത്ഥനകൾ മാത്രം അനുവദിക്കുക
ഏതെങ്കിലും ആപ്ലിക്കേഷൻ ഡൗൺലോഡ് ചെയ്യുന്നതിനുമുമ്പ്, അതി ന്റെ അവലോകനങ്ങളും ഡെവലപ്പർ ആരാണെന്നും പരിശോധിക്കുക.


ओह, इन सब फर्जीवाड़े से कैसे बचा जाए? कोई सुरक्षा सुझाव?
हां, बिलकुल है. सुनो...
#सबको बताओ
#Safe with UBI
सबसे पहले यह ध्यान रखो कि यूनियन बैंक कभी भी एसएमएस, टेलीग्राम, ईमेल, व्हाट्सप्प पर .apk/.ipa फ़ाइल नहीं भेजता न ही फोन कॉल के माध्यम से आपकी संवेदनशील जानकारियां पूछता है.
हमेशा आधिकारिक ऐप स्टोर जैसे Google Play या Apple App Store से ऐप्स डाउनलोड करें.
एप्लिकेशन द्वारा अनुरोधित अनुमतियों की ज़रूर समीक्षा करें. केवल उन्हीं अनुरोधों को ही अनुमति दें जिसकी आवश्यकता है.
कोई भी एप्लिकेशन डाउनलोड करने के पहले उसके रिव्युज़ और डेवलपर कौन है, इसकी भी जाँच अवश्य करें.

കൂടാതെ ബാങ്കിംഗ് ഇടപാടുകൾക്കായി പൊതു സ്ഥലങ്ങളിൽ ലഭ്യമായ സൗജന്യ വൈഫൈ നെറ്റ്‌വർക്കുകൾ ഉപയോഗിക്കരുത്.

മുൻകരുതലുകൾ:.1.അജ്ഞാത കോൺടാക്റ്റുകളിൽ നിന്നുള്ള ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്, ഒരിക്കലും .apk ഫയലുകൾ ഡൗൺലോഡ് ചെയ്യരുത്.

ശക്തമായ പാസ്‌വേഡുകൾ ഉപയോഗിക്കുക. കഴിയുന്നത്ര മൾട്ടിഫാക്ടർ ഓതന്റിക്കേഷൻ ഉപയോഗിക്കുക.

ഫോൺ മോഷ്ടിക്കപ്പെടുകയോ നഷ്ടപ്പെടുകയോ അല്ലെങ്കിൽ സാധാരണ സാഹചര്യങ്ങളിൽപ്പോലും നിങ്ങളുടെ മൊബൈലിലേക്കുള്ള അനധികൃത ആക്സസ് തടയാൻ, സ്ക്രീൻ ലോക്കിന്റെ വിവിധ സവിശേഷതകൾ- പിൻ, പാറ്റേൺ, ബയോമെട്രിക് ലോക്ക് എന്നിവ ക്രമീകരണങ്ങളിൽ മുൻകൂട്ടി സജ്ജമാക്കുക.

മെസേജിംഗ് ആപ്പുകൾ വഴി നിങ്ങളുടെ സ്വകാര്യ വിവരങ്ങൾ ഒരിക്കലും പങ്കിടരുത്.

और बैंकिंग ट्रांजेक्शन के लिए सार्वजनिक स्थानों पर उपलब्ध फ्री वाई-फ़ाई नेटवर्क का प्रयोग न करें.

किसी भी अज्ञात संपर्क से आए लिंक पर क्लिक न करें, .apk फाइल को कभी भी डाउनलोड न करें.

मजबूत पासवर्ड का उपयोग करें. यथा संभव मल्टीफैकटर ऑथेंटिकेशन की सुविधा का ही उपयोग करें.

फोन चोरी या खो जाने की स्थिति में अथवा सामान्य परिस्थिति में भी अपने मोबाइल तक अनाधिकृत पहुँच को रोकने हेतु स्क्रीन लॉक की सुविधा को पिन,पैटर्न, बायोमेट्रिक लॉक जैसे माध्यमों से सेटिंग्स में पहले से ही सेट कर लें.

कभी भी मैसेजिंग ऐप के माध्यम से अपनी व्यक्तिगत जानकारी साझा न करें.


ഇനി ഞാനും ഒരു സേഫ്റ്റി ടിപ്പ് തരട്ടേ? ... നിങ്ങളുടെ പാസ്‌വേഡോ OTP യോ ഒരിക്കലും ആരുമായും പങ്കിടരുത്, അല്ലേ?
U SuRKsha
U RKshak
തികച്ചും ശരി സുഹൃത്തേ!
U SuRKsha
ഒരു കാര്യം കൂടി, നിങ്ങളുടെ ലാപ്‌ടോപ്പിലും മൊബൈലിലും യഥാർത്ഥ സോഫ്റ്റ്‌വെയർ, ആന്റിവൈറസ് എന്നിവ ഉപയോഗിക്കുക, അത് അപ്‌ഡേറ്റ് ചെയ്യാൻ മറക്കരുത്.
എനിക്ക് മറ്റൊരു സംശയം കൂടിയുണ്ട്, യൂണിയൻ ബാങ്കിന്റെ പേരിൽ ഞങ്ങൾക്ക് വ്യാജ ആശയവിനിമയം ലഭിച്ചാൽ, അത്തരമൊരു സാഹചര്യത്തിൽ നമ്മൾ എന്തുചെയ്യണം?
U RKshak


अब एक सुरक्षा टिप मैं भी दूँ? ... कभी भी अपना पासवर्ड या ओटीपी किसी के साथ साझा न करें, सही?
U SuRKsha
U RKshak
बिल्कुल सही कहा दोस्त!
U SuRKsha
एक बात और अपने लैपटाप और मोबाइल में जेनयुइन सॉफ्टवेयर, एंटीवायरस का उपयोग करें और उसे अपडेट करना न भूलें.
मेरी एक और जिज्ञासा है,अगर हमें यूनियन बैंक के नाम पर संदिग्ध धोखाधड़ी संचार प्राप्त होता है, तो ऐसी स्थिति में हमें क्या करना चाहिए ?
U RKshak

ഇത് ഉടൻ റിപ്പോർട്ട് ചെയ്യണം. ബാങ്കിന്റെ പേരിൽ SMS, വാട്ട്സ്ആപ്പ് അല്ലെങ്കിൽ വീഡിയോ-ഓഡിയോ കോൾ വഴി ലഭിക്കുന്ന വഞ്ചനാപരമായ ആശയവിനിമയം ചക്ഷു പോർട്ടലിൽ (https://sancharsaathi.gov.in/sfc) റിപ്പോർട്ട് ചെയ്യാം.

സാമ്പത്തിക നഷ്ടമുണ്ടായാൽ, 1930 എന്ന നമ്പറിൽ വിളിച്ച് ഈ സൈബർ കുറ്റകൃത്യം ഉടൻ അറിയിക്കുക

https://www.cybercrime.gov.in എന്നതിൽ നിങ്ങളുടെ പരാതി രജിസ്റ്റർ ചെയ്യുക അല്ലെങ്കിൽ സൈബർ പോലീസിന്റെ സഹായം തേടുക.

U RKshak

ഇത്തരം കൂടുതൽ സൈബർ സുരക്ഷാ അവബോധ നുറുങ്ങുകൾ അറിയാൻ, യൂണിയൻ ബാങ്കിന്റെ കോർപ്പറേറ്റ് സൈറ്റ് www.unionbankofindia.co.in - മെനു - കസ്റ്റമർ കോർണർ സന്ദർശിക്കുക, കൂടാതെ ബാങ്ക് നൽകുന്ന സൈബർ സുരക്ഷാ അവബോധ ഗൈഡ് സന്ദർശിക്കുക.

U SuRKsha

വിവരങ്ങൾക്ക് നന്ദി. ഇതിൽ നിന്നു മനസിലാക്കേണ്ടതു എന്തെന്നാൽ ജാഗ്രത മാത്രമാണ് പരിഹാരം.

इसे तुरंत रिपोर्ट करना चाहिए. बैंक के नाम से एसएमएस, व्हाट्सप्प या वीडियो-आडियो कॉल के माध्यम से प्राप्त धोखाधड़ी संचार को चक्षु पोर्टल (https://sancharsaathi.gov.in/sfc) पर रिपोर्ट कर सकते हैं.

और वित्तीय नुकसान होने की स्थिति में इस साइबर अपराध को तुरंत 1930 पर कॉल करके सूचित करें और

https://www.cybercrime.gov.in पर अपनी शिकायत दर्ज करें या साइबर पुलिस की सहायता लें.

और इस तरह की कई साइबर सुरक्षा जागरूकता टिप्स को जानने के लिए यूनियन बैंक की कॉर्पोरेट साइट (www.unionbankofindia.co.in)-मेनू -कस्टमर कॉर्नर पर जाकर बैंक द्वारा जारी साइबर सुरक्षा जागरूकता मार्गदर्शिका को ज़रूर देखें.

जानकारी के लिए धन्यवाद. मतलब, सतर्कता ही समाधान है.

आलोक भार्गव द्वारा रेखांकित व यूनियन बैंक ऑफ इंडिया, मुख्य सूचना सुरक्षा अधिकारी कार्यालय (सीआईएसओ) हैदराबाद के समन्वयन व राजभाषा कार्यान्वयन प्रभाग, मानव संसाधन विभाग, केंद्रीय कार्यालय, मुंबई के निर्देशानुसार अंचल कार्यालय, मंगलूरु द्वारा अनूदित तथा प्रकाशित.

- चक्षु पोर्टल (https://sancharsaathi.gov.in/sfc/): पिछले 30 दिनों के भीतर कॉल/ व्हाट्सप्प/ एसएमएस के माध्यम से प्राप्त किसी भी संदिग्ध धोखाधड़ी संचार को रिपोर्ट करें।
- 1930 पर कॉल: वित्तीय धोखाधड़ी हो जाने की स्थिति में या साइबर अपराध के मामले में 1930 पर कॉल करें अथवा www.cybercrime. gov.in पर अपनी शिकायत दर्ज करें.
- धोखाधड़ी युक्त या विवादास्पद लेनदेन के लिए यूनियन बैंक ऑफ़ इंडिया की हेल्पलाइन नं. 1800 2222 43 (टोल फ्री) पर संपर्क करें .

यूनियन बैंक ऑफ इंडिया Union Bank of India

अच्छे लोग, अच्छा बैंक Good people to bank with

आलोक भार्गव द्वारा रेखांकित व यूनियन बैंक ऑफ इंडिया, मुख्य सूचना सुरक्षा अधिकारी कार्यालय (सीआईएसओ) हैदराबाद के समन्वयन व राजभाषा कार्यान्वयन प्रभाग, मानव संसाधन विभाग, केंद्रीय कार्यालय, मुंबई के निर्देशानुसार अंचल कार्यालय, मंगलूरु द्वारा अनूदित तथा प्रकाशित.

- चक्षु पोर्टल (https://sancharsaathi.gov.in/sfc/): पिछले 30 दिनों के भीतर कॉल/ व्हाट्सप्प/ एसएमएस के माध्यम से प्राप्त किसी भी संदिग्ध धोखाधड़ी संचार को रिपोर्ट करें।
- 1930 पर कॉल: वित्तीय धोखाधड़ी हो जाने की स्थिति में या साइबर अपराध के मामले में 1930 पर कॉल करें अथवा www.cybercrime. gov.in पर अपनी शिकायत दर्ज करें.
- धोखाधड़ी युक्त या विवादास्पद लेनदेन के लिए यूनियन बैंक ऑफ़ इंडिया की हेल्पलाइन नं. 1800 2222 43 (टोल फ्री) पर संपर्क करें .

यूनियन बैंक ऑफ इंडिया Union Bank of India

अच्छे लोग, अच्छा बैंक Good people to bank with

LEAD

संवृद्धि की ओर | Towards Growth

दायित्व | आय | आस्ति | डिजिटलीकरण
Liability | Earnings | Assets | Digitization

संरक्षक
रेणू के. नायर
महाप्रबंधक
अंचल प्रमुख, मंगलूरू

संपादक
कृष्ण कुमार यादव
मुख्य प्रबंधक (राभा)
राजभाषा प्रभारी

सहयोग
श्रीकला एल.के.
उप महाप्रबंधक
उप अंचल प्रमुख