ಸೈಬರ್ ಮೋಸದ ಜಾಲ

ಎಚ್ಚರ! Apk ಫೈಲಿನ ಅಪಾಯಗಳಿಂದ ದೂರವಿರಿ

साइबर मायाजाल

.apk फाइल के खतरों से सावधान.

ನಿಮ್ಮ ಸುರಕ್ಷತೆಯೇ ನಮ್ಮ ಆದ್ಯತೆ

आपकी सुरक्षा हमारे साथ

ಸೈಬರ್ ಸುರಕ್ಷತೆಯ ಅತ್ಯುನ್ನತ ಕೇಂದ್ರ

साइबर सुरक्षा उत्कृष्टता केंद्र

यूनियन बैंक ऑफ इंडिया Union Bank of India

अच्छे लोग, अच्छा बैंक Good people to bank with

अंचल कार्यालय, बेंगलूरु / Zonal Office, Bengaluru

ರಮೇಶನ ಫೋನಿನಲ್ಲಿ ಯೂನಿಯನ್ ಬ್ಯಾಂಕಿನ ಹೆಸರಿನಲ್ಲಿರುವ .APKಯ ಬಹುಮಾನದ ಫೈಲನ್ನು ಡೌನ್ಲೋಡ್ ಮಾಡಲಾಗುತ್ತದೆ. ರಮೇಶ ಅದರ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಿದ್ದನ್ನು "ರಕ್ಷಕ" ನೋಡುತ್ತಾನೆ)
ಏನಪ್ಪಾ, ಏನು ಮಾಡ್ತಾ ಇದೀಯ? ಈ ಫೈಲಿನ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡ. (ಎಚ್ಚರಿಸುತ್ತ..)
U रKshak
U SuरKsha
ಯಾಕೆ ಮಾಡಬಾರದು? ಯೂನಿಯನ್ ಬ್ಯಾಂಕಿನಿಂದ ಎಷ್ಟು ದೊಡ್ಡ ಬಹುಮಾನಗಳು ಬಂದಿವೆ ಗೊತ್ತಾ?
ಅಲ್ಲ ಮಾರಾಯ! ಸ್ವಲ್ಪ ಗಮನ ಇಟ್ಟು ನೋಡು. ಇದೊಂದು ಮೋಸದ ಬಲೆ. ನೀನು ಕಷ್ಟಪಟ್ಟು ಸಂಪಾದಿಸಿದ ಹಣದ ಜೊತೆ ನಿನ್ನ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಕದಿಯಲು ಪ್ರಯತ್ನ ಇದು.
ಏನು?!! (ಗಾಬರಿಯಿಂದ) ನೀನ್ ಏನು ಹೇಳ್ತಾ ಇದ್ದೀಯಾ? ಈ ಫೈಲ್ ಬ್ಯಾಂಕಿನಿಂದ ಬಂದಿದೆ!
ಅಲ್ಲೆ ಇರೋದು ಮೋಸ! ಯೂನಿಯನ್ ಬ್ಯಾಂಕ್ ಎಂದಿಗೂ Apk ಅಥವಾ Ipa ಫೈಲನ್ನು ಅನ್ನು ಯಾವುದೇ ರೂಪದಲ್ಲಿ ಕಳುಹಿಸುವುದಿಲ್ಲ!
?

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 रKshak
U SuRKsha
पर क्यों? देखो न रिवार्ड्स का कितना बढ़िया ऑफर आया है- यूनियन बैंक की ओर से.
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.
?

ಒಂದು ನಿಮಿಷ. ಈ APK ಫೈಲ್ ಎಂದರೇನು? ಮತ್ತು ಬ್ಯಾಂಕಿನ ಹೆಸರಿನಲ್ಲಿ ಈ ಮೋಸ ಏಕೆ? ನನಗೆ ಇದೇನೂ ಅರ್ಥ ಆಗ್ತಿಲ್ಲ.
ಪೇಟೆಯಲ್ಲಿ ಯೂನಿಯನ್ ಬ್ಯಾಂಕಿನ ಹೆಸರಿನಲ್ಲಿ. apk/. ipa ನಡೆಯುತ್ತಿರುವ ಮೋಸದ ಬಗ್ಗೆ ನೀನು ಇನ್ನೂ ಕೇಳಿಲ್ಲವ?
U ₹Kshak
ಕೇಳಿಲ್ಲ, ಆದರೆ ನಿಮ್ಮಿಬ್ಬರ ಮಾತನ್ನು ಕೇಳಿದ ಮೇಲೆ ಕೆಲವು ಮೋಸಗಾರರು ಬ್ಯಾಂಕಿನ ಹೆಸರಿನಲ್ಲಿ ವಂಚನೆ ಮಾಡುತ್ತಿದ್ದಾರೆ ಅಂತ ಅನ್ನಿಸುತ್ತಿದೆ.
ಸರಿಯಾಗಿ ಅರ್ಥ ಮಾಡಿಕೊಂಡೆ ನೀನು! ಈಗ ನಿನಗೆ ತಿಳಿಯಿತು ನೋಡು!
ಈ ಮೋಸದ ವದಂತಿ ಮುಖ್ಯವಾಗಿ ಸಾಮಾಜಿಕ ಜಾಲತಾಣದಲ್ಲಿ ಹರಿದಾಡುತ್ತಿದೆ.

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 ₹Kshak
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.
ये फर्जीवाड़ा मुख्य रूप से सोशल मीडिया के माध्यम से प्रसारित हो रहा है.

ಓಹೋ ಸರಿ. ಅಂತೆಯೇ, ನನಗೆ ಗೊತ್ತಿರುವ ಒಬ್ಬರಿಗೆ ಆದಾಯ ತೆರಿಗೆ ಇಲಾಖೆಯ ರೂಪದಲ್ಲಿ ಮರುಪಾವತಿ ಸಂದೇಶ ಬಂದಿದೆ.
ಅಲ್ಲಿ ಕೂಡ. Apk ಲಿಂಕ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಕ್ಕೆ ಹೇಳಿದರು.
ಓ! ಹೌದಾ!
U ₹Kshak
ಆದರೆ ಸ್ವಲ್ಪ ಹೊತ್ತಿನಲ್ಲಿ ಅವರಿಗೆ ತನಗೆ ಯಾವ ಮರುಪಾವತಿಯೂ ಬರಲು ಬಾಕಿ ಇಲ್ಲ ಅಂತ ನೆನಪಾಯಿತು. ಆದ್ದರಿಂದ ಅವರು ಮೋಸದ ಬಲೆಯಿಂದ ತಪ್ಪಿಸಿಕೊಂಡರು.
ಸುರಕ್ಷಾ ಮತ್ತು ರಕ್ಷಕ ತಮ್ಮ ಸ್ನೇಹಿತನಿಗೆ ಈ ಸೈಬರ್ ಬೆದರಿಕೆಯ ಕಾರ್ಯವಿಧಾನ ಮತ್ತು ರಕ್ಷಣೆಯ ಅಂಶಗಳ ಬಗ್ಗೆ ಅರಿವು ಮೂಡಿಸುತ್ತಾರೆ)
ಇದು Spoofingನ ಒಂದು ಮಾದರಿ. ಇದು ಒಂದು ರೀತಿಯ ಸೈಬರ್ ಅಪರಾಧ.
U ₹Kshak
ಆದ್ದರಿಂದ ಈ ನಡುವೆ ಸೈಬರ್ ಭದ್ರತೆಯ ಬಗ್ಗೆ ಅಪ್ಡೇಟ್ ಆಗಿರುವುದು ಬಹಳ ಮುಖ್ಯ.

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.
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.
U रKshak
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.
इसीलिए आजकल साइबर सुरक्षा के बारे में अपडटेड रहना बहुत ज़रूरी है.

ಸರಿಯಾಗಿ ಹೇಳಿದೆ ಕಣೋ! ಈ ಬಗ್ಗೆ ನನಗೆ ಹೆಚ್ಚೇನೂ ಗೊತ್ತಿಲ್ಲ. ನಿನಗೆ ತಿಳಿದಿದ್ದರೆ ನನಗೆ ಹೇಳಿ ಕೊಡು. ನಾನು ಅದರ ಬಗ್ಗೆ ಎಲ್ಲವನ್ನೂ ತಿಳಿದು ಕೊಳ್ಳಬೇಕು.
ಈ ಎಪಿಕೆಯ ಮೋಸ ಹೇಗೆ ಕೆಲಸ ಮಾಡುತ್ತೆ? ಇದರಿಂದ ತಪ್ಪಿಸಿಕೊಳ್ಳಕ್ಕೆ ದಾರಿ ಯಾವುದು? ಮೋಸ ಆದರೆ ಯಾರನ್ನು ನೋಡಬೇಕು? ಎಲ್ಲ ಹೇಳು!
ಈಗ ಸರಿಯಾದ ಪ್ರಶ್ನೆ ಕೇಳಿದೆ!
ಇಲ್ಲಿ ಕೇಳು. ಮೊಬೈಲ್ ಕಂಪನಿಗಳು ಬಳಕೆದಾರರಿಗೆ ಥರ್ಡ್ ಪಾರ್ಟಿ ಆಪ್ ಗಳನ್ನು ಸ್ಥಾಪಿಸಲು ಅನುಮತಿ ನೀಡುತ್ತವೆ.
ಈ ಸೌಲಭ್ಯದಿಂದ ಮೋಸಗಾರರು ಲಾಭ ಪಡೆಯುತ್ತಾರೆ!

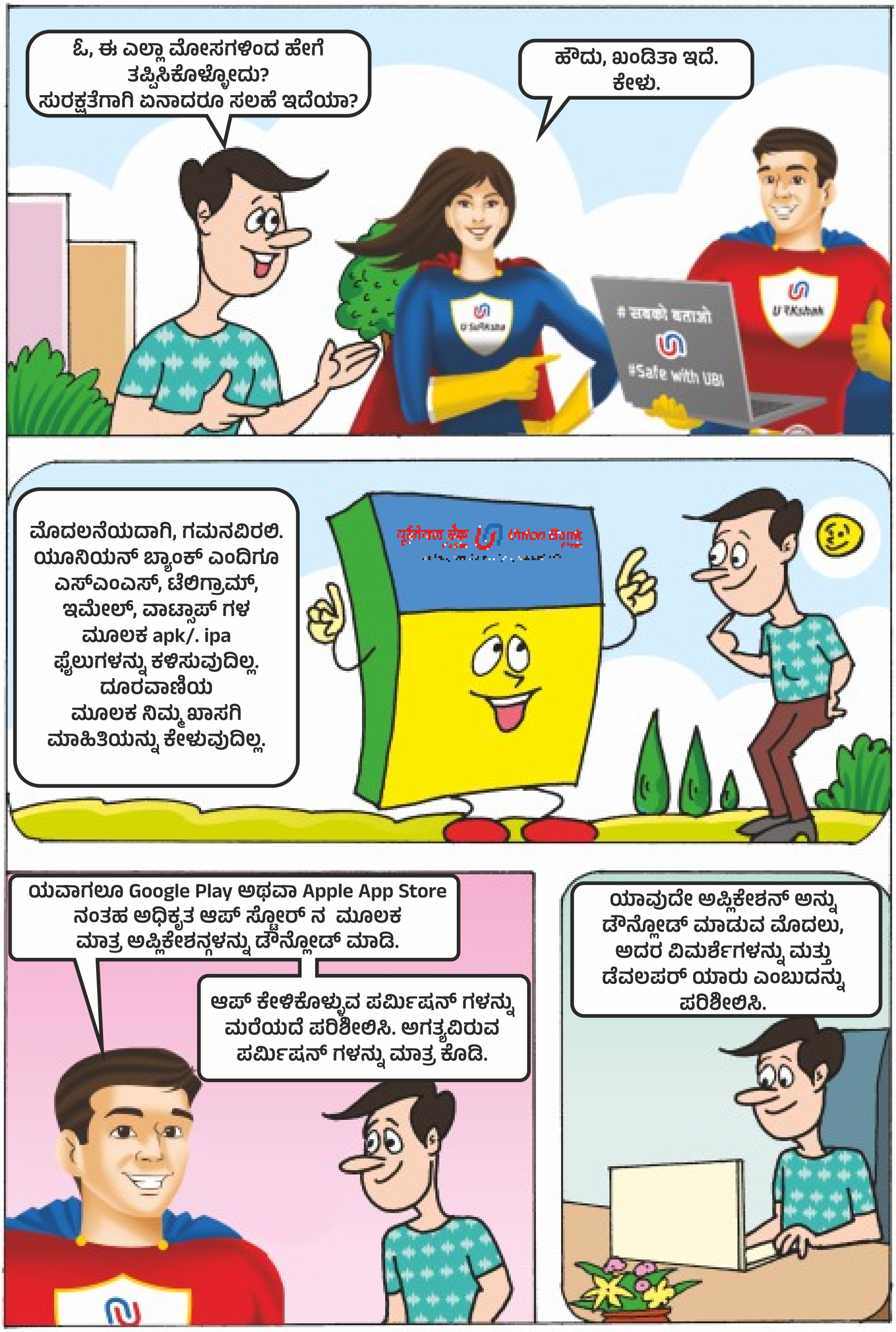
सही कहा यार. मुझे इस बारे में अधिक जानकारी नहीं है. अगर तुम्हें पता है तो तुम बताओ, मैं इसके बारे में सब कुछ जानना चाहता हूँ.
ये .apk धोखाधड़ी कैसे काम करती है? इससे बचने के तरीके क्या हैं ? इसका शिकार होने पर कहाँ संपर्क करना चाहिए.... सब कुछ ...
अब किया न तुमने सही सवाल!!
अरे सुनो, मोबाइल कंपनियाँ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

ಮೋಸ ಮಾಡುವ ಕೋಡ್ ನೊಂದಿಗೆ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಮಾಡಿ ಆ .APK ಫೈಲ್ ಗಳನ್ನು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮಗಳ ವೇದಿಕೆಗಳಲ್ಲಿ ಮತ್ತು ಬಳಕೆದಾರರ ಮೂಲಕ ಹಂಚುತ್ತಾರೆ ಇದರಿಂದ ತಿಳಿಯದವರು .APK ಫೈಲನ್ನು ತಮ್ಮ ಫೋನಿನಲ್ಲಿ ಹಾಕಿಕೊಳ್ಳುತ್ತಾರೆ.
ನಿನಗೆ ಗೊತ್ತು.. ಸ್ಪೂಫಿಂಗ್ ಕಳುಹಿಸುವವರ ಮಾಹಿತಿಯನ್ನು ಮರೆ ಮಾಡುತ್ತಾರೆ. ಇದು ಅಧಿಕೃತ ಮೂಲದಿಂದ ಬಂದಂತೆ ತೋರಿಸುತ್ತಾರೆ. ಇದರಿಂದಾಗಿ ಮಾಹಿತಿಯನ್ನು ಕದಿಯಬಹುದು ಅಥವಾ ಮಾಲ್ವೇರ್ ಹರಡಬಹುದು.
U SuRKsha
ನನಗೆ ಭಯ ಆಗ್ತಿದೆ! ಆದರೆ ಈ ವಂಚಕರು ಮೋಸ ಹೋದವರ ಫೋನ್ ಅನ್ನು ಹೇಗೆ ನಿಯಂತ್ರಿಸುತ್ತಾರೆ?
ಹೇಳ್ತೀನಿ! ಹೇಳ್ತೀನಿ! ನಕಲಿ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಸ್ಥಾಪಿಸಿದ ಮೇಲೆ ಅದು ಫೋನಿನ ಚಾಲನೆಯನ್ನು ಹ್ಯಾಕರ್ ಗೆ ನೀಡುತ್ತದೆ.
U SuRKsha
ಅಯ್ಯೋ!

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

ಹೀಗೆ ಮಾಡೋದರಿಂದ ಅ ಹ್ಯಾಕರ್ ಹಣಕಾಸಿನ ವ್ಯವಹಾರ ನಡೆಸಲು ಮತ್ತು ಹಣವನ್ನು ಕದಿಯಲು ಬೇಕಾಗುವ ಒಟಿಪಿ ಮತ್ತು ಪಿನ್ ಅನ್ನು ಕದಿಯುತ್ತಾನೆ.
ಈ ಇಡಿ ಪ್ರಕರಣ ಬರೀ ನಕಲಿ ಅಪ್ಲಿಕೇಶನ್ ಹಾಕಿಕೊಳ್ಳೋದರಲ್ಲಿ ನಿಲ್ಲಲ್ಲ!
ಅ ಹ್ಯಾಕರ್ ಗಳು ಇಮೇಲ್, ವಾಟ್ಸಾಪ್ ಸಂದೇಶ, ಫೋನ್ ಕರೆ, ವಿಡಿಯೋ ಕರೆ ಮತ್ತು ಡೀಪ್ ಫೇಕ್ ತಂತ್ರಗಳ ಮೂಲಕ ಸ್ಪೂಫಿಂಗ್ ಮಾಡಿ ಜನರನ್ನು ಬಲೆಗೆ ಹಾಕಿಕೊಳ್ಳುತ್ತಾರೆ.
ಅಯ್ಯಪ್ಪ! ಆಮೇಲೆ?
U SuRKsha
ಇದಾದ ಮೇಲೆ ನಿನ್ನ ಎಲ್ಲಾ ಖಾಸಗಿ ಮಾಹಿತಿಯನ್ನು ಅಂದರೆ ಬ್ಯಾಂಕ್ ವಿವರಗಳಿಂದ ಹಿಡಿದು ವೈಯುಕ್ತಿಕ ಮಾಹಿತಿಯವರೆಗೆ, ಎಲ್ಲವನ್ನೂ ಕಳವು ಮಾಡಬಹುದು.
ಇದರಿಂದಾಗಿ ಎಷ್ಟೋ ಸಲ ಜನರಿಗೆ ಸಿಕ್ಕಾಬಟ್ಟೆ ನಷ್ಟ ಆಗುತ್ತೆ.

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.


ಓ, ಈ ಎಲ್ಲಾ ಮೋಸಗಳಿಂದ ಹೇಗೆ ತಪ್ಪಿಸಿಕೊಳ್ಳೋದು? ಸುರಕ್ಷತೆಗಾಗಿ ಏನಾದರೂ ಸಲಹೆ ಇದೆಯಾ?
ಹೌದು, ಖಂಡಿತಾ ಇದೆ. ಕೇಳು.
सबको बताओ
#Safe with UBI
ಮೊದಲನೆಯದಾಗಿ, ಗಮನವಿರಲಿ. ಯೂನಿಯನ್ ಬ್ಯಾಂಕ್ ಎಂದಿಗೂ ಎಸ್‌ಎಂಎಸ್, ಟೆಲಿಗ್ರಾಮ್, ಇಮೇಲ್, ವಾಟ್ಸಾಪ್ ಗಳ ಮೂಲಕ apk/. ipa ಫೈಲುಗಳನ್ನು ಕಳಿಸುವುದಿಲ್ಲ. ದೂರವಾಣಿಯ ಮೂಲಕ ನಿಮ್ಮ ಖಾಸಗಿ ಮಾಹಿತಿಯನ್ನು ಕೇಳುವುದಿಲ್ಲ.
ಯವಾಗಲೂ Google Play ಅಥವಾ Apple App Store ನಂತಹ ಅಧಿಕೃತ ಆಪ್ ಸ್ಟೋರ್ ನ ಮೂಲಕ ಮಾತ್ರ ಅಪ್ಲಿಕೇಶನ್ಗಳನ್ನು ಡೌನ್ಲೋಡ್ ಮಾಡಿ.
ಆಪ್ ಕೇಳಿಕೊಳ್ಳುವ ಪರ್ಮಿಷನ್ ಗಳನ್ನು ಮರೆಯದೆ ಪರಿಶೀಲಿಸಿ. ಅಗತ್ಯವಿರುವ ಪರ್ಮಿಷನ್ ಗಳನ್ನು ಮಾತ್ರ ಕೊಡಿ.
ಯಾವುದೇ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಡೌನ್ಲೋಡ್ ಮಾಡುವ ಮೊದಲು, ಅದರ ವಿಮರ್ಶೆಗಳನ್ನು ಮತ್ತು ಡೆವಲಪರ್ ಯಾರು ಎಂಬುದನ್ನು ಪರಿಶೀಲಿಸಿ.

ओह, इन सब फर्जीवाड़े से कैसे बचा जाए? कोई सुरक्षा सुझाव?
हां, बिलकुल है. सुनो...
#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 जानकरियाँ 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.

ಮತ್ತು ಬ್ಯಾಂಕಿಂಗ್ ವಹಿವಾಟುಗಳಿಗಾಗಿ ಸಾರ್ವಜನಿಕ ಸ್ಥಳಗಳಲ್ಲಿ ಸಿಗುವ ಉಚಿತ ವೈ-ಫೈ ನೆಟ್ವರ್ಕ್ ಅನ್ನು ಯಾವತ್ತೂ ಬಳಸಬೇಡಿ!
ಯಾವುದೇ ಅಪರಿಚಿತರಿಂದ ಬಂದ ಲಿಂಕ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ. APK ಫೈಲ್ ಅನ್ನು ಡೌನ್ಲೋಡ್ ಮಾಡಬೇಡಿ.
ಬಲವಾದ ಪಾಸ್ವರ್ಡ್ ಅನ್ನು ಬಳಸಿ. ಸಾಧ್ಯವಾದಷ್ಟು ಮಲ್ಟಿಫ್ಯಾಕ್ಟರ್ ದೃಢೀಕರಣವನ್ನು ಬಳಸಿ.
U RKshak
U SaRKsha
ಫೋನ್ ಕಳುವಾಗುವ ಪರಿಸ್ಥಿತಿಯಲ್ಲಿದ್ದಾಗ ಅಥವಾ ಸಾಮಾನ್ಯ ಸಂದರ್ಭಗಳಲ್ಲಿ ಕೂಡ ನಿಮ್ಮ ಮೊಬೈಲ್ ನಲ್ಲಿ ಅನಧಿಕೃತ ಪ್ರವೇಶವನ್ನು ತಡೆಯಲು, ಸ್ಕ್ರೀನ್ ಲಾಕ್ನ ಬೇರೆ ಬೇರೆ ವೈಶಿಷ್ಟ್ಯಗಳಾದ ಪಿನ್, ಪ್ಯಾಟರ್ನ್, ಬಯೋಮೆಟ್ರಿಕ್ ಲಾಕ್ ಅನ್ನು ಸೆಟ್ಟಿಂಗ್ಗಳಲ್ಲಿ ಮೊದಲೇ ಹೊಂದಿಸಿ.
ಕಳ್ಳ.. ಕಳ್ಳ.. ಹಿಡಿಯಿರಿ.
ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಮೆಸೇಜಿಂಗ್ ಅಪ್ಲಿಕೇಶನ್ ಮೂಲಕ ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
ಆಧಾರ್
ಪಿನ್
ಕಾರ್ಡ್ ವಿವರ
C.V.V.

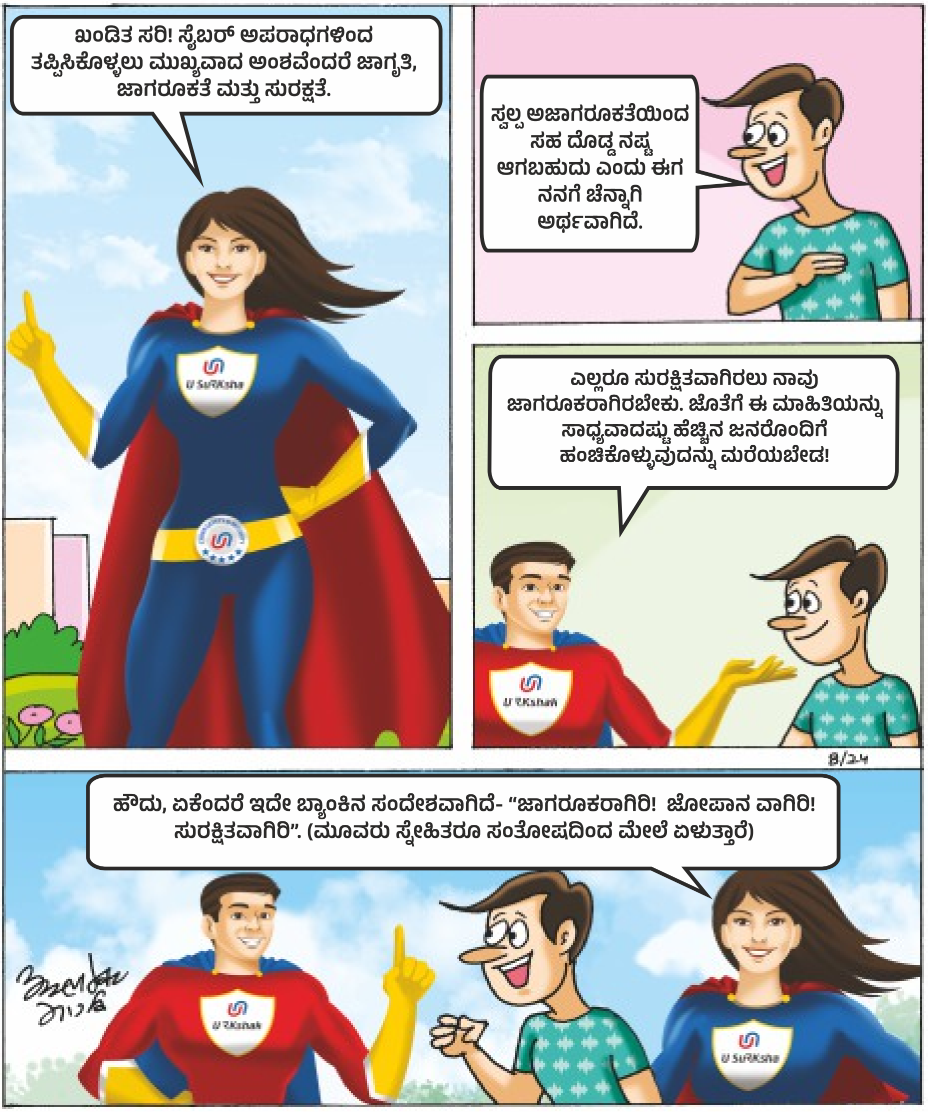
और बैंकिंग ट्रांजेक्शन के लिए सार्वजनिक स्थानों पर उपलब्ध फ्री वाई-फ़ाई नेटवर्क का प्रयोग न करें.
मॉल
किसी भी अज्ञात संपर्क से आए लिंक पर क्लिक न करें, .apk फाइल को कभी भी डाउनलोड न करें.
मजबूत पासवर्ड का उपयोग करें. यथा संभव मल्टीफैक्टर ऑथेंटिकेशन की सुविधा का ही उपयोग करें.
U रKshak
फोन चोरी या खो 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.
चोर..चोर.. पकड़ो पकड़ो..
कभी भी मैसेजिंग ऐप के माध्यम से अपनी व्यक्तिगत जानकारी साझा न करें.
आधार
पिन
कार्ड डिटेल्स
सीवीवी

ನಾನೂ ಈಗ ಒಂದು ಸುರಕ್ಷತೆಯ ಸಲಹೆಯನ್ನು ನೀಡಬಹುದೇ?... ನಿಮ್ಮ ಪಾಸ್ವರ್ಡ್ ಅಥವಾ ಒಟಿಪಿಯನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ, ಅಲ್ಲವೇ?
U SaRKsha
U ₹Kshak
ಸರಿಯಾಗಿ ಹೇಳಿದೆ ಕಣೋ!
ಇನ್ನೊಂದು ವಿಷಯ. ನಿಮ್ಮ ಲ್ಯಾಪ್ಟಾಪ್ ಮತ್ತು ಮೊಬೈಲ್ನಲ್ಲಿ ಅಧಿಕೃತವಾದ ಸಾಫ್ಟ್ವೇರ್ ಮತ್ತು ಆಂಟಿವೈರಸ್ ಅನ್ನು ಬಳಸಿ. ಮತ್ತು ಅದನ್ನು ಕಾಲಕಾಲಕ್ಕೆ ನವೀಕರಿಸಲು ಮರೆಯಬೇಡಿ.
ನನಗೆ ಇನ್ನೊಂದು ಪ್ರಶ್ನೆಯಿದೆ. ಯೂನಿಯನ್ ಬ್ಯಾಂಕಿನ ಹೆಸರಿನಲ್ಲಿ ಮೋಸದ ಗುಮಾನಿ ಇರುವ ಸಂದೇಶ ಬಂದರೆ ಅಂತಹ ಪರಿಸ್ಥಿತಿಯಲ್ಲಿ ನಾವು ಏನು ಮಾಡಬೇಕು?
U ₹Kshak

अब एक सुरक्षा टिप मैं भी दूँ? ... कभी भी अपना पासवर्ड या ओटीपी किसी के साथ साझा न करें, सही?
बिल्कुल सही कहा दोस्त!
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 ?

ಈ ಬಗ್ಗೆ ತಕ್ಷಣ ವರದಿ ನೀಡಬೇಕು. ಬ್ಯಾಂಕಿನ ಹೆಸರಿನಲ್ಲಿ ಎಸ್‌ಎಂಎಸ್, ವಾಟ್ಸಾಪ್ ಅಥವಾ ವಿಡಿಯೋ-ಆಡಿಯೊ ಕರೆಗಳ ಮೂಲಕ ಬಂದ ಮೋಸದ ಸಂದೇಶಗಳನ್ನು ಚಕ್ಷು ಪೋರ್ಟಲ್ ನಲ್ಲಿ ವರದಿ ಮಾಡಬಹುದು https://sancharsaathi.gov.in/sfc
ಮತ್ತು ಹಣಕಾಸಿನ ನಷ್ಟದ ಸಂದರ್ಭದಲ್ಲಿ, 1930 ಕ್ಕೆ ಕರೆ ಮಾಡುವ ಮೂಲಕ ಈ ಸೈಬರ್ ಅಪರಾಧವನ್ನು ತಕ್ಷಣವೇ ವರದಿ ಮಾಡಿ.
https://www.cybercrime.gov.in – ಇಲ್ಲಿ ನಿಮ್ಮ ದೂರನ್ನು ನೋಂದಾಯಿಸಿ. ಅಥವಾ ಸೈಬರ್ ಪೊಲೀಸರ ಸಹಾಯವನ್ನು ಪಡೆಯಿರಿ.
ಜೊತೆಗೆ, ಅಂತಹ ಅನೇಕ ಸೈಬರ್ ಭದ್ರತಾ ಜಾಗೃತಿ ಸಲಹೆಗಳನ್ನು ತಿಳಿಯಲು, www.unionbankofindia.co.in ಎಂಬ ಜಾಲತಾಣದಲ್ಲಿ ಮೆನು, ಕಸ್ಟಮರ್ ಕಾರ್ನರ್ ಗೆ ಹೋಗಿ ಬ್ಯಾಂಕ್ ಹೊರಡಿಸಿದ ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಅವೇರ್ನೆಸ್" ಗೈಡ್ ಅನ್ನು ಅವಶ್ಯವಾಗಿ ನೋಡಿ.
ಮಾಹಿತಿಗೆ ಧನ್ಯವಾದಗಳು. ಅಂದರೆ, ಜಾಗರೂಕತೆಯಿಂದ ಇರುವುದೇ ಉತ್ತಮ ಉಪಾಯ

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.
U रKshak
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 से राजभाषा कार्यान्वयन प्रभाग, मानव संसाधन विभाग, केंद्रीय कार्यालय, मुंबई द्वारा 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 .

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

संरक्षक

श्री नवनीत कुमार

अंचल प्रमुख, बेंगलूरु

उप संरक्षक

श्रीमती माधवी वी

उप अंचल प्रमुख, बेंगलूरु

उप संरक्षक

श्री सुधीर सी वी

उप अंचल प्रमुख, बेंगलूरु

प्रस्तुति

श्री जॉन ए अब्राहम

मुख्य प्रबंधक (राभा)