

घोटालों से सुरक्षित रहना

CommBank में भरोसा और सुरक्षा हमारी सबसे बड़ी प्राथमिकता है। हमें ऐसे सेवार्थियों के उदाहरणों में वृद्धि होती हुई दिखाई दे रही है, जिनपर घोटालेबाजों द्वारा उन्हें पैसे भेजने के लिए दबाव डाला जाता है या जिन्हें धोखा दिया जाता है। ये घोटाले पेचीदा और अलग-अलग स्वरूपों में हो सकते हैं। इनके लिए ध्यान रखना महत्वपूर्ण है और यदि कुछ सही नहीं लगता है, तो हमें बताएँ। खुद को सुरक्षित रखने और किसी घोटाले की रिपोर्ट करने के तरीके के बारे में और अधिक जानकारी के लिए commbank.com.au/safe देखें।

प्रमाणीकरण और सत्यापन

- CommBank ऐप में सुरक्षा जांच पूरी करें।
- मल्टी-फैक्टर ऑथेंटिकेशन लागू करें, जो आपकी पहचान सिद्ध करने के लिए एक अतिरिक्त जांच करता है।
- बैंक से होने का दावा करने वाले कॉलकर्ताओं की पहचान को सत्यापित करने के लिए **CallerCheck** का उपयोग करें।
- हमारे कर्मियों के समक्ष खुद को सत्यापित करने के लिए शाखा में **CustomerCheck** का उपयोग करें।
- यदि पहली बार भुगतान करने पर खाते के विवरण सही नहीं लगते हैं, तो **NameCheck** आपको प्रॉम्प्ट करेगा।

डिवाइस और भुगतान सुरक्षा

- एँटी-वायरस सॉफ्टवेयर को अप-टु-डेट रखें और अपने कंप्यूटर को सामान्य खतरों से संरक्षित रखें।
- टैपिंग या अपना कार्ड इंसर्ट करने जैसी सुरक्षित भुगतान विधियों का उपयोग करें।
- जिन डिवाइसेज़ में आपका डिजिटल वॉलेट हो, उन्हें किसी के साथ साझा न करें।

पासवर्ड और व्यक्तिगत जानकारी

- कभी भी पासवर्ड या पिन साझा न करें, और व्यक्तिगत जानकारी साझा करते समय सतर्क रहें।
- कभी भी अपना NetCode किसी को न दें, जिसमें CommBank स्टाफ भी शामिल है।
- आप किसी भी समय NetBank और CommBank ऐप में अपना पासवर्ड बदल सकते/ती हैं।
- मजबूत पासवर्ड बनाएँ और इन्हें नियमित रूप से बदलते रहें। पासवर्ड बनाने के बारे में हमारे सुझावों के लिए commbank.com.au/password-security पर जाएँ।

ईमेल, एसएमएस और ऑनलाइन

- संदिग्ध ईमेल या एसएमएस में दिए गए लिंक्स पर क्लिक न करें।
- यदि आप किसी मैसेज के बारे में निश्चित नहीं हैं, तो किसी ऐसे व्यक्ति के साथ बात करें जिसपर आपको विश्वास है या फिर आधिकारिक संपर्क विवरणों के माध्यम से सीधे संगठन से संपर्क करें।
- तीसरे पक्षों से ऑटोमेटेड, संदिग्ध या धमकी भरी फ़ोन कॉलें आने पर फ़ोन काट दें।
- सोशल मीडिया और ऑनलाइन प्लेटफॉर्मों पर अज्ञात संपर्कों से सावधान रहें।

रुकें। जांच करें। अस्वीकार करें।

रुकें। क्या कुछ अजीब लग रहा है? संदेह होने पर रुकना ही सबसे अच्छा रहता है। गहरी सांस लें।

जांच करें। किसी ऐसे व्यक्ति से पूछें जिसपर आपको विश्वास है, या फिर आधिकारिक संपर्क विवरणों का उपयोग करके सीधे संगठन से संपर्क करें।

अस्वीकार करें। कॉलकर्ता का फ़ोन काट दें, ईमेल को डिलीट कर दें, फ़ोन नंबर को ब्लॉक कर दें। अपने पासवर्ड बदलें।

यदि आपको लगता है कि आप किसी घोटाले के शिकार हो गए/ई हैं, तो CommBank से तुरंत **13 22 21** पर संपर्क करें, अथवा विदेश से **+61 2 9999 3283** पर संपर्क करें।

यदि आपकी प्राथमिक भाषा अंग्रेज़ी नहीं है, तो सरकार की निःशुल्क अनुवाद और दुभाषिया सेवा (Translating and Interpreter Service) आपको हमारे साथ संवाद करने में मदद दे सकती है। यह सेवा 150 से भी अधिक भाषाओं में उपलब्ध है। जब आप हमें कॉल करते/ती हैं या हमसे शाखा में मिलते/ती हैं, तो हम इस सेवा की व्यवस्था कर सकते हैं।

आपको ये बातें पता होनी चाहिए: हम आपको कभी भी ऐसी कोई ईमेल या एसएमएस नहीं भेजेंगे, जिसमें आपका NetBank Client ID, पासवर्ड, या NetCode जैसी बैंकिंग जानकारी मांगी जाएगी; या जिसमें सीधे ईमेल या एसएमएस से लॉग ऑन करने के लिए लिंक शामिल होगा। हमेशा ब्राउज़र में commbank.com.au टाइप करें या अपनी बैंकिंग को सुरक्षापूर्वक एक्सेस करने के लिए CommBank ऐप का उपयोग करें। यदि CommBank की ओर से कुछ संदिग्ध लगता है, तो इसे hoax@cba.com.au पर फॉरवर्ड करें और फिर डिलीट कर दें। कॉमनवेल्थ बैंक ऑफ ऑस्ट्रेलिया एबीएन 48 123 123 124 एएफएसएल और ऑस्ट्रेलियन क्रेडिट लाइसेंस 234945.



घोटालों के बारे में उपभोक्ताओं के लिए महत्वपूर्ण जानकारी



निवेश (इसमें क्रिप्टो भी शामिल है)

घोटालेबाज लोगों को ऊँचे लाभ के वादे का लालच देते हैं, जिसमें अक्सर क्रिप्टो या निवेश के अन्य अवसर शामिल होते हैं। घोटालेबाज आपसे फ़ोन, ईमेल या सोशल मीडिया प्लेटफॉर्मों के माध्यम से संपर्क करने की कोशिश कर सकते हैं।

खुद को सुरक्षित रखने के सुझाव:

- यदि कुछ सच होने के लिए बहुत ही अच्छा लगता है, तो शायद यह सच नहीं है।
- अवांछित प्रस्तावों और निवेश करने या जल्दबाजी में कदम उठाने के दबाव के बारे में सतर्क रहें।
- पहले कंपनी या ब्रोकर की वैधता को ASIC वेबसाइट पर सत्यापित करें।



रिमोट एक्सेस

इसमें कोई घोटालेबाज आपको कॉल करता है और किसी विश्वसनीय कंपनी या संगठन की ओर से होने का दिखावा करते हुए आपके खातों या डिवाइस को एक्सेस करने की कोशिश करता है।

खुद को सुरक्षित रखने के सुझाव:

- किसी तीसरे पक्ष के कॉलकर्ता के निवेदन या दबाव में आकर कभी भी रिमोट एक्सेस सॉफ़्टवेयर डाउनलोड न करें।
- आप हमेशा किसी संगठन के वैध संपर्क विवरणों पर उन्हें वापिस कॉल कर सकते/ती हैं, जो उनकी आधिकारिक वेबसाइट पर उपलब्ध रहता है।
- यदि आपको CommBank की ओर से होने का दावा करने वाली कोई कॉल आती है, तो आप हमेशा इन-ऐप CallerCheck फीचर के माध्यम से हमें कॉल को सत्यापित करने के लिए कह सकते/ती हैं।

व्यापारिक ईमेल से छेड़छाड़



घोटालेबाज किसी छेड़छाड़ किए गए ईमेल पते या विश्वसनीय संपर्क की ओर से लगने वाली ईमेल के माध्यम से व्यवसायों को लक्षित कर सकते हैं, जैसे: आपके सहायक, ग्राहक, वकील, प्रबंधक या आपूर्तिकर्ता।

खुद को सुरक्षित रखने के सुझाव:

- पहली बार भुगतान करने या भुगतान विवरणों में बदलाव होने पर पहले विवरण की पुष्टि करने के लिए संगठन के आधिकारिक संपर्क नंबर पर उन्हें कॉल करें।
- भुगतान करते समय NameCheck फीचर का उपयोग करके यह देखें कि खाते का नाम दिए गए BSB और खाता नंबर से मेल खाता है या नहीं।
- फिशिंग के प्रयासों की पहचान करने और उनकी रिपोर्ट करने के लिए कर्मियों को प्रशिक्षित करें।

फिशिंग और स्मिशिंग



घोटालेबाज भ्रामक ईमेल या टेक्स्ट मैसेज का उपयोग करते हैं, जिनमें आपको धोखाधड़ी वाली वेबसाइट पर भेजने के लिए एक लिंक शामिल हो सकता है या संवेदनशील व्यक्तिगत जानकारी मांगी जा सकती है।

खुद को सुरक्षित रखने के सुझाव:

- संदिग्ध ईमेल या एसएमएस में दिए गए लिंक्स पर क्लिक न करें।
- संपर्क करने के उपलब्ध आधिकारिक तरीके इस्तेमाल करके आप सीधे संगठन से संपर्क करके संदेश की प्रामाणिकता की पुष्टि कर सकते/ती हैं।
- CommBank की ओर से आने वाले किसी भी संदिग्ध मैसेज की रिपोर्ट hoax@cba.com.au पर करें।



घोटालों के बारे में उपभोक्ताओं के लिए महत्वपूर्ण जानकारी



संबंध

घोटालेबाज संबंध बनाने के लिए नकली प्रोफाइल्स बनाते हैं और पीड़ितों को पैसे या व्यक्तिगत जानकारी भेजने के लिए उनके साथ चालाकी करते हैं।

खुद को सुरक्षित रखने के सुझाव:

- किसी ऐसे व्यक्ति को कभी भी पैसे न भेजें, या उसके साथ पासवर्ड, क्रेडिट कार्ड या खाता विवरण साझा न करें, जिसपर आपको भरोसा नहीं है।
- गूगल या सोशल मीडिया ऐप्स के माध्यम से अपने संभावित पार्टनर के बारे में ऑनलाइन जाँच-पड़ताल करें। यह पहचानने के लिए रिवर्स इमेज सर्च आजमाएँ कि आपको भेजी गई फोटो का मालिक कोई और है या नहीं।
- अपने ऑनलाइन संबंध के बारे में अपने परिवार और दोस्तों के साथ बात करें। वे दृष्टिकोण प्रस्तुत करने और चेतावनी संकेतों की पहचान करने में सक्षम हो सकते हैं, जिनपर शायद आपने ध्यान नहीं दिया होगा।



ऑनलाइन शॉपिंग

घोटालेबाज खरीदारों को लालच देकर काल्पनिक या नकली उत्पाद खरीदने के लिए ऑनलाइन स्टोर या विज्ञापन बनाते हैं।

खुद को सुरक्षित रखने के सुझाव:

- केवल प्रतिष्ठित और सुरक्षित वेबसाइटों पर ही खरीदारी करें और ऐसे किसी भी प्रस्ताव से सावधान रहें, जो सच होने के लिए बहुत अच्छा लगता है।
- सुरक्षित भुगतान विधियों का उपयोग करें और विक्रेताओं को सीधे पैसे न भेजने की कोशिश करें।
- 'लिमिटेड ऑफर्स' या बिक्री समाप्त होने के 'काउंटडाउन्स' की वजह से जल्दबाजी न करें या दबाव में न आएँ।

रोजगार के अवसर

इसमें रोजगार का प्रस्ताव ऐसा लगता है कि बहुत अधिक आर्थिक लाभ के बदले बहुत कम या कोई भी प्रयास न करना हो, अथवा यह जल्दी से पैसे कमाने का वादा करता है।

खुद को सुरक्षित रखने के सुझाव:

- कंपनी और प्रस्ताव को आधिकारिक माध्यमों से सत्यापित करें, और कंपनी के बारे में जाँच-पड़ताल करके सुनिश्चित करें कि वे वैध हैं और इस समय व्यापार कर रहे हैं।
- सोशल मीडिया, एन्क्रिप्टेड चैट, ईमेल, फ़ोन या ऐसे लोगों की ओर से आने वाले पत्र में रोजगार के प्रस्तावों से सावधान रहें, जिनसे आप मिले/ली नहीं हैं या जिन कंपनियों को आप जानते/ती नहीं हैं।
- एक वैध कंपनी आपको अग्रिम भुगतान करने या कंपनी के धन या व्यापार की सुविधा के लिए अपनी व्यक्तिगत बैंकिंग जानकारी इस्तेमाल करने की आवश्यकता कभी नहीं बनाएगी।



धमकी और जुर्माना

घोटालेबाज जुर्माना या कानूनी कार्रवाई की धमकी देकर पैसे निकलवाने के लिए अधिकारी या विश्वसनीय संगठनों की ओर से होने का दिखावा करते हैं।

खुद को सुरक्षित रखने के सुझाव:

- धमकी देने वाले कॉलकर्ताओं का फ़ोन काट दें और सीधे संगठन से संपर्क करें।
- कोई वैध संगठन आपको कभी भी असामान्य तरीकों से भुगतान करने के लिए नहीं कहेगा, जैसे गिफ्ट या स्टोर कार्ड्स, आईट्यून्स वाउचर्स, वायर ट्रांसफर्स या बिटकॉइन्स।
- यदि आप अपनी सुरक्षा को लेकर चिंतित हैं, तो पुलिस सहायता लाइन से संपर्क करें।

