Australian Banking Association

अपने आप को सुरक्षित रखें: घोटालों और धोखाधड़ी से अवगत रहें

आगे आने वाले महीनों में COVID-19 से संबंधित घोटालों और धोखाधड़ी के प्रकरणों की बढ़ने की संभावना है।

घोटालेबाज व्यक्तिगत जानकारी प्राप्त करने लिए नकली ईमेल, फोन कॉल या टेक्स्ट संदेशों का उपयोग करते हैं। वे आपकी बैंक, विश्व स्वास्थ्य संगठन, सरकार, दान-सँस्थाओं या ट्रैवल एजेंट, बिजली, फोन या इंटरनेट प्रदाता, या आपके स्थानीय सुपरमार्केट जैसे वैध व्यवसायों की ओर से आपसे संपर्क का दिखावा करते हैं।

अपनी सुरक्षा करें

आपकी बैंक किसी भी खाते या वित्तीय विवरण के लिए आपको ईमेल या टेक्स्ट संदेश कभी नहीं भेजेगी, इसमें फोन, मोबाइल या इंटरनेट बैंकिंग के लिए अपना पता अपडेट करने या लॉगिन करने के लिए आग्रह करना शामिल है।

सरकारी और अन्य वैध संगठन आपको लिंक पर क्लिक करके विवरण अपडेट करने के लिए कभी नहीं कहेंगे। संदेह की स्थिति में किसी दोस्त या परिवार के सदस्य से बात करें, या सीधे संगठन से संपर्क करें और पूछें।

यदि आपको ऐसे किसी व्यक्ति से अपनी निजी जानकारी देने के लिए फोन कॉल प्राप्त होती है जिसे आप जानते/जानती नहीं हैं, तो फोन काट दें। सीधे कंपनी को कॉल करें और पूछें कि क्या उन्होंने फोन किया था।

ऐसे लोगों या संगठनों से प्राप्त हुए संलग्नक कभी न खोलें, जिन्हें आप जानते/जानती नहीं हैं। हमेशा ऐसे प्रस्तावों से सावधान रहें जो सच होने के लिए बहुत अच्छा लगता है या बहुत अधिक जानकारी मांगता है।

आपकी बैंक सहायता कर सकती है। उनसे तुरंत संपर्क करें, यदि:

- आपने धोखे से की गई फोन कॉल, ईमेल या टेक्स्ट संदेश के उत्तर में में अपने बैंकिंग विवरण प्रकट कर दिए हैं
- आपने गलती से किसी लिंक पर क्लिक कर दिया है या संलग्नक डाउनलोड कर लिए हैं
- आपके ध्यान में अपने खातों में किसी भी प्रकार का असामान्य लेन-देन आया है।

घोटाले की पहचान कैसे करें

- आपको व्यक्तिगत विवरण अपडेट करने या इसकी पुष्टि करने के लिए कहा जाता है, जिसमें पता, जन्मतिथि, बैंक खाते का विवरण, टैक्स फाइल नंबर अथवा कोई पिन या पासवर्ड भी शामिल है।
- ईमेल या टेक्स्ट संदेश में संदिग्ध दिखने वाले लिंक हैं। यदि आप सुनिश्चित नहीं हैं, तो सहायता के लिए किसी मित्र या परिवार के सदस्य से पूछें।
- आपको तत्काल भुगतान या अग्रिम राशि जमा करने के लिए कहा जाता है।
- यदि प्रस्ताव वास्तविकता के विपरीत बहुत अच्छा लगता है, तो संभावित रूप से यह घोटाला ही होता है।
- ईमेल पता कंपनी से मेल नहीं खाता है।
- कॉल करने वाला व्यक्ति आपके कंप्यूटर को दूरस्थ रूप से एक्सेस करने के लिए कहता है।

Australian Banking Association

www.ausbanking.org.au

अपनी वित्तीय जानकारी को घोटालों और धोखाधड़ी से सुरक्षित रखने के लिए शीर्ष के सुझाव

- संदिग्ध फोन कॉलों को काट दें, इसके बजाए कंपनी की वेबसाइट पर जाएँ या उनका नंबर खोजकर उन्हें सीधे कॉल करें।
- कभी भी पासवर्ड या पिनों को साझा न करें। अपने उपकरणों के लिए पासवर्ड बनाकर उन्हें सुरक्षित रखें। यदि आप एक साझा कंप्यूटर का उपयोग कर रहे/रही हैं, तो कभी भी पासवर्ड सेव न करें और हमेशा अपने खाते से लॉग आउट करें।
- अपने बैंक के खातों की नियमित रूप से जाँच करें ताकि आप किसी भी प्रकार का संदिग्ध लेनदेन तुरंत देख सकें।
- खरीदारी करते समय अपना कार्ड स्वाइप न करने का प्रयास करें। टैप या इंसर्ट करना अक्सर अधिक सुरक्षित होता है।
- क्रेडिट कार्डों से अग्रिम नकदी निकालने की सुविधा को ब्लॉक करें।
- अपने खाते को सुरक्षित रखने के सबसे अच्छे तरीके के बारे में अपनी बैंक से बात करें।
- अगर आपको लगता है कि आप किसी घोटाले के शिकार हो गए/गई हैं, तो इसके बारे में तुरंत अपनी बैंक को बताएँ।

आपसे चोरी करने के लिए बदमाश कई तरीके अपना सकते हैं, इनमें से प्रमुख तरीके यहाँ दिए गए हैं।

फिशिंग - आपकी व्यक्तिगत जानकारी प्राप्त करने के लिए बैंक, दान-संस्था या सरकार जैसे किसी विश्वसनीय स्रोत की ओर से प्रतीत होने वाली ईमेल या टेक्स्ट संदेश का उपयोग किया जाता है। यह संदेश वास्तविक प्रतीत होता है और अक्सर आपसे नकली वेबसाइटों पर व्यक्तिगत जानकारी एंटर करने या लिंक पर क्लिक करने के लिए कहा जाएगा - ऐसा करने पर बदमाश आपकी व्यक्तिगत जानकारी प्राप्त करने में सक्षम हो जाएँगे।

ऑनलाइन शॉपिंग घोटाले - घोटालेबाज नकली वेबसाइट या वास्तविक रिटेल साइट पर नकली विज्ञापन के माध्यम से एक वास्तविक ऑनलाइन दुकान होने का दिखावा करते हैं। नकली ऑनलाइन खरीदारी साइटें अक्सर मनी ऑर्डर, वायर ट्रॉंसफर, अंतर्राष्ट्रीय फंड ट्रॉंसफर या गिफ्ट कार्ड जैसे असामान्य तरीकों के माध्यम से अग्रिम भुगतान जमा करने का आग्रह करेंगी।

निवेश घोटाले - घोटालेबाज वित्तीय या निवेश से संबंधित सलाह देने वाला स्टॉकब्रोकर या पोर्टफोलियो प्रबंधक होने का दावा करता है। वे आपको एक निवेश के अवसर के लिए पैसे देने के लिए कहेंगे, जो वास्तविक हो सकता है या नहीं भी हो सकता है, और फिर वे आपके पैसे रख लेंगे।

रिमोट एक्सेस घोटाले - घोटालेबाज आपके कंप्यूटर या इंटरनेट कनेक्शन में कुछ समस्या होने या इसके मैलवेयर से संक्रमित होने का दावा करेगा। वे आपको कोई एप्लिकेशन इंस्टॉल करने या अपने कंप्यूटर तक पहुँच प्रदान करने के लिए मनाने की कोशिश करेंगे। इसके माध्यम से वे आपकी व्यक्तिगत जानकारी तक पहुँच प्राप्त करेंगे या समस्या को ठीक करने के लिए आपसे 'शुल्क' की माँग करेंगे।

संबंध और डेटिंग के घोटाले - घोटालेबाज आपसे पैसे या उपहार निकलवाने के लिए संबंध बनाता है। वे समय के साथ संबंध विकसित करते हैं और आपको अपनी संपत्ति उनके नाम करने के लिए कह सकते हैं या आपकी वसीयत के लाभार्थी बनने के लिए कह सकते हैं। अक्सर वे अपने स्वास्थ्य, यात्रा या परिवार में समस्या को हल करने के लिए पैसों की माँग करेंगे।

उपयोगी कड़ियाँ:

www.ausbanking.org.au/safe-savvy-a-guide-to-help-older-people-avoid-abuse-scams-and-fraud

www.esafety.gov.au/seniors/staying-safer-online

www.scamwatch.gov.au/

महत्वपूर्ण नोट: इस तथ्य पत्रक में सामान्य प्रकृति की जानकारी दी गई है और आपको किसी विशेष मामले में सलाह के लिए इसपर निर्भर नहीं करना चाहिए। आपको अपनी बैंक से संपर्क करके पता करना चाहिए कि यह जानकारी आपकी परिस्थितियों के लिए कैसे लागू हो सकती है।