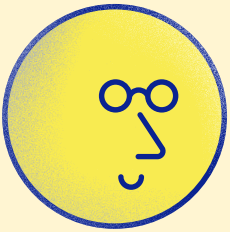
घोटालों का पता कैसे लगाएँ और उनसे सुरक्षित कैसे रहें



घोटालों से स्वयं को सुरक्षित रखने के लिए आपकी संदर्शिका

Australian Government

National Anti-Scam Centre

ScamWatch
Stop. Better safe than scammed.

स्वदेशी भूमि के प्रति अभिस्वीकृति

ACCC पूरे ऑस्ट्रेलिया-भर में स्वदेशी भूमि के पारंपरिक स्वामियों और संरक्षकों के प्रति अभिस्वीकृति व्यक्त करता है और भूमि, समुद्र एवं समुदाय के साथ उनके निरंतर संबंध को मान्यता देता है। हम उनके और उनकी संस्कृतियों के प्रति तथा अतीत, वर्तमान एवं भविष्य में उनके बुजुर्गों के प्रति अपना सम्मान व्यक्त करते हैं।

Australian Competition and Consumer Commission
Ngunnawal
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

© ऑस्ट्रेलिया राष्ट्रमंडल 2023

यह कार्य कॉपीराइट है। *कॉपीराइट अधिनियम 1968* के तहत अनुमत किसी भी उपयोग के अतिरिक्त इस कार्य में निहित सभी सामग्री क्रिएटिव कॉमन्स एट्रिब्यूशन 4.0 ऑस्ट्रेलिया लाइसेंस के तहत प्रदान की जाती है, जिसमें निम्नलिखित के लिए अपवाद है:

- कॉमनवेल्थ कोट ऑफ आर्म्स
- ACCC और AER के लोगो
- ऐसा कोई भी चित्रण, आरेख, तस्वीर या ग्राफिक जिसके लिए Australian Competition and Consumer Commission के पास कॉपीराइट नहीं है, लेकिन जो इस प्रकाशन का हिस्सा हो सकता है या इसमें निहित हो सकता है।

संगत लाइसेंस शर्तों का विवरण तथा CC BY 4.0 AU लाइसेंस के लिए संपूर्ण कानूनी कोड क्रिएटिव कॉमन्स की वेबसाइट पर उपलब्ध है।

पुन:प्रकाशन और अधिकारों से संबंधित निवेदनों व पूछताछ को इस पते पर भेजा जाना चाहिए: Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

महत्वपूर्ण सूचना

इस प्रकाशन में दी गई जानकारी केवल सामान्य मार्गदर्शन के लिए ही है। यह कानूनी या कोई अन्य पेशेवर सलाह का गठन नहीं करती है, और इसपर किसी भी न्यायाधिकार-क्षेत्र में कानूनी वक्तव्य के रूप में भरोसा नहीं किया जाना चाहिए। चूंकि इसका उद्देश्य केवल एक सामान्य संदर्शिका के रूप में है, इसलिए इसमें सामान्यीकरण हो सकते हैं। यदि आपको कोई विशिष्ट चिंता है, तो आपको पेशेवर सलाह लेनी चाहिए।

ACCC ने वर्तमान और सटीक जानकारी प्रदान करने के लिए हर उचित प्रयास किया है, लेकिन यह उस जानकारी की सटीकता, वर्तमानीयता या संपूर्णता के बारे में कोई गारंटी नहीं देता है।

जो पक्ष इस प्रकाशन में दी गई जानकारी का पुन:प्रकाशन या अन्यथा उपयोग करना चाहते हैं, उन्हें प्रकाशन से पहले इस जानकारी की वर्तमानीयता तथा सटीकता की जाँच करनी होगी। प्रत्येक प्रकाशन संस्करण से पहले ऐसा किया जाना चाहिए, क्योंकि ACCC मार्गदर्शन और प्रासंगिक पारगमनकालीन कानून अक्सर बदलते रहते हैं। पक्षों के पास निहित सभी प्रश्नों को इस पते पर भेजा जाना चाहिए: Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 05/24_24-13

www.accc.gov.au

सामग्री

सहायता उपलब्ध है 1

घोटाला क्या होता है 3

घोटालों का पता लगाने और उनसे सुरक्षित रहने के लिए आसान कदम 4

टेक्स्ट या एसएमएस घोटाले 7

ईमेल घोटाले 11

फोन घोटाले 15

वेबसाइट घोटाले 19

सोशल मीडिया, ऐप-आधारित और ऑनलाइन मैसेजिंग घोटाले 23

प्रमुख घोटाले, जिनके बारे में आपको पता होना चाहिए 27

घोटालों की रिपोर्ट कहाँ करें 31

और अधिक सहायता एवं समर्थन 33

यह मार्गदर्शिका National Anti-Scam Centre द्वारा निर्मित की गई है और यह आपको घोटालों से होने वाले नुकसान की पहचान करने तथा स्वयं को सुरक्षित रखने में सहायता करेगी।

घोटाला एक अपराध होता है और घोटाले करने वाले लोग अपराधी होते हैं। ऑस्ट्रेलिया में बहुत से लोगों के साथ घोटाले किए जा रहे हैं और वे अपने पैसे खो रहे हैं, जो कभी-कभी उनके पूरे जीवन-भर की बचत होती है। घोटालों से लोगों के जीवन को नुकसान पहुंचता है।

घोटालों का पता लगाना कठिन होता जा रहा है, इसलिए इन्हें रोकने के लिए हमें साथ-मिलकर काम करने की आवश्यकता है।

National Anti-Scam Centre ऑस्ट्रेलियावासियों को घोटालों से सुरक्षित रखने के लिए काम करता है।

हम घोटालेबाजों को ऑस्ट्रेलियावासियों के पैसे और व्यक्तिगत जानकारी की चोरी करने से रोकने के नए तरीके खोजने के लिए सरकार और उद्योग के साथ-मिलकर काम करते हैं। हम यह कैसे हासिल करते हैं, यहाँ इसके कुछ तरीके दिए गए हैं।

हम लोगों को घोटालों की पहचान करने और इनसे सुरक्षित रहने में सहायता देते हैं

Scamwatch के माध्यम से हम घोटालों और ऐसे तरीकों के बारे में अप-टु-डेट जानकारी साझा करते हैं, जिनसे आप स्वयं को घोटालों से सुरक्षित रख सकते/ती हैं।

हम घोटालेबाजों को बाधित करते हैं

खुफिया जानकारी को एकत्र करके और उसे सरकार व उद्योग के बीच साझा करके हम घोटालेबाजों के लिए उनके अपराधों को जारी रख पाना कठिन बनाते हैं और लोगों के लिए घोटालों की रिपोर्ट करना आसान बनाते हैं।

सहायता उपलब्ध है

यदि आप यह पढ़ रहे/ही हैं, तो संभव है कि आपके, या आपके किसी परिचित के साथ घोटाला किया गया है। दुर्भाग्यवश आप अकेले/ली नहीं हैं। घोटाले और भी अधिक जटिल बनते जा रहे हैं, जिसका अर्थ है कि किसी के साथ भी घोटाला किया जा सकता है।

यदि आपके साथ घोटाला किया गया है, तो यह महत्वपूर्ण है कि आप जल्दी कदम उठाएँ।

यदि किसी घोटालेबाज के कारण आपका पैसा डूब गया है, तो अपनी बैंक या कार्ड प्रदाता से संपर्क करें।

संपर्क करें: IDCARE, 1800 595 160, www.idcare.org

घोटाले इसलिए सफल होते हैं क्योंकि वे असली तथ्य की तरह प्रतीत होते हैं। घोटालेबाज इस बात पर निर्भर करते हैं कि आप जल्दबाज़ी के कारण चेतावनी के संकेतों का पता नहीं लगा पाते/ती हैं, कुछ ऐसा प्रतीत होता है जिससे आप चूकना नहीं चाहते/ती हैं, अथवा यह आपके किसी भरोसेमंद व्यक्ति की ओर से प्रतीत होता है।

इन 3 कदमों का पालन करके स्वयं को घोटालों से सुरक्षित रखें:

रुकें

अनिश्चित होने पर किसी को भी पैसे या व्यक्तिगत जानकारी न दें।

घोटालेबाज आपकी सहायता करने का प्रस्ताव देंगे या आपकी पहचान सत्यापित करने के लिए आपसे पूछेंगे। वे ऐसे संगठनों की ओर से होने का दिखावा करेंगे, जिनसे आप परिचित हैं और जिनपर आप भरोसा करते/ती हैं, जैसे सेवा प्रदाता, पुलिस, आपकी बैंक या सरकारी सेवाएँ।

जाँच करें

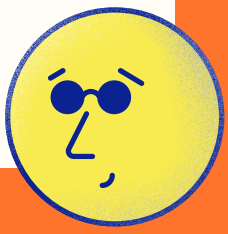
स्वयं से पूछें - क्या मैसेज या कॉल नकली हो सकते हैं?

मैसेज में दिए गए किसी भी लिंक पर कभी भी क्लिक न करें। व्यवसायों या सरकार से संपर्क करने के लिए केवल उसी संपर्क जानकारी का उपयोग करें, जो आपको स्वयं उनकी आधिकारिक वेबसाइट या ऐप पर मिलती है। यदि आप सुनिश्चित नहीं हैं, तो 'नहीं' कहें, हैंग अप करें या डिलीट करें।

सूचना दें

यदि कुछ गलत लगता है, तो जल्दी कदम उठाएँ।

यदि आपको कोई असामान्य गतिविधि दिखाई देती है अथवा यदि किसी घोटालेबाज को आपके पैसे या जानकारी प्राप्त हो जाती है, तो अपनी बैंक से संपर्क करें। सहायता लें और ReportCyber तथा Scamwatch के पास घोटाले की रिपोर्ट करें। जब आप घोटालों की रिपोर्ट करते/ती हैं, तो घोटालों के विरुद्ध हमारे संरक्षण को निर्मित करके आप सभी ऑस्ट्रेलियावासियों की सहायता करते/ती हैं।



घोटाला क्या होता है

जब कोई आपके पैसों या व्यक्तिगत जानकारी की चोरी करने के लिए आपको धोखा देता है, तो यह घोटाला होता है।

घोटाले अपराधियों द्वारा संचालित किए जाने वाले आर्थिक अपराध हैं, जो अक्सर बहुत संगठित और जटिल होते हैं।

घोटाले:

- अपराधियों द्वारा संचालित किए जाते हैं
- वास्तविक प्रतीत होते हैं
- विश्वसनीय कहानियों के साथ आते हैं
- आपके ऊपर कदम उठाने के लिए दबाव डालते हैं

घोटाला यह नहीं होता है:

- कंप्यूटर हैकिंग
- अनुबंध में अनुचित शर्तें
- परेशान करने वाले मार्केटिंग के तरीके

यह याद रखना महत्वपूर्ण है कि सभी नकारात्मक अनुभव घोटाले नहीं होते हैं। हो सकता है कि आपने ऐसे उत्पाद के लिए भुगतान किया हो जो आपको कभी मिला ही नहीं, या आपने कुछ खरीदा हो और बाद में पता चला कि उसकी गुणवत्ता खराब थी। यह निराशाजनक तो होता है, किंतु यह आवश्यक नहीं है कि ये घोटाले ही हों। Australian Consumer Law इस प्रकार के मामलों में ऑस्ट्रेलियाई उपभोक्ताओं को संरक्षण प्रदान करता है।

और अधिक जानकारी के लिए www.accc.gov.au/consumers पर जाएँ।

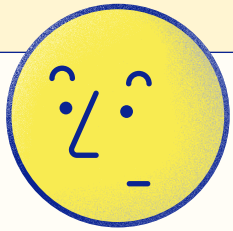
घोटालों का पता लगाने और उनसे सुरक्षित रहने के लिए आसान कदम

हम सभी के साथ घोटाले हो सकते हैं। घोटाले इसलिए कारगर होते हैं क्योंकि घोटालेबाज आपके पैसों की चोरी करने और आपकी व्यक्तिगत जानकारी प्राप्त करने के लिए भरोसेमंद कहानियाँ बनाते हैं।

घोटालेबाज और भी अधिक चालाक बनते जा रहे हैं और नई तकनीकी, उत्पादों, सेवाओं और मुख्य घटनाओं का फायदा उठा रहे हैं, ताकि आपको भरोसा दिलाया जा सके कि उनके घोटाले वास्तविक हैं।

घोटाले का पता लगाना बहुत कठिन हो सकता है। यहाँ कुछ परिस्थितियाँ दी गई हैं, जिनका ध्यान रखा जाना चाहिए। कभी-कभी घोटालेबाज इनमें से कई चालबाजियों का साथ में इस्तेमाल करते हैं।

1. **पैसे कमाने या बचाने के अवसर:** घोटालेबाज आपको यह भरोसा देने के लिए धोखा देंगे कि आपको एक बेहतरीन सौदा या प्रस्ताव मिल रहा है। वे आपके ऊपर जल्दी से कदम उठाने का दबाव डालेंगे, ताकि आप चूक न जाएँ। याद रखें कि जो सौदे इतने अच्छे प्रतीत हों कि उनपर यकीन करना कठिन हो, वे आमतौर पर सच नहीं होते हैं।
2. **दु:खद कहानियाँ और समर्थन के लिए रोना-धोना:** घोटालेबाज आपकी शराफत का इस्तेमाल आपके खिलाफ करने की कोशिश करेंगे। वे आपके साथ दिल टूटने और त्रासदी की कहानियाँ साझा करेंगे और समझाएँगे कि उन्हें आपकी सहायता और आपका पैसा क्यों चाहिए।
3. **लिंक्स और एटैचमेंट्स:** घोटालेबाज आपकी जानकारी और पैसे चुराने के लिए निर्मित स्कैम वेबसाइट्स पर आपको भेजने के लिए लिंक्स का उपयोग करते हैं। घोटालेबाज आपको एटैचमेंट्स खोलने के लिए भी कह सकते/ती हैं। ये आपकी जानकारी चुराने वाले वायरस इंस्टॉल कर सकते हैं।



4. **जल्दी कदम उठाने के लिए दबाव:** घोटालेबाज यह नहीं चाहते हैं कि आप परिस्थितियों के बारे में सोचने के लिए अपना समय निकालें। वे आपके ऊपर जल्दी कदम उठाने के लिए दबाव डालना चाहते हैं। इसमें इस बात की धमकी देना शामिल हो सकता है कि यदि आप जल्दी कदम नहीं उठाते/ती हैं, तो कुछ बुरा होगा।
5. **असामान्य या विशिष्ट तरीकों से भुगतान करने के निवेदन:** घोटालेबाज अक्सर प्रीलोडेड डेबिट कार्ड, iTunes कार्ड्स या Bitcoin जैसी वर्चुअल करेंसी जैसे असामान्य तरीकों का उपयोग करके आपसे भुगतान करने के लिए कहते हैं। एक बार यह पैसा खर्च हो जाने के बाद आपको यह वापिस नहीं मिल सकता है।
6. **नए खाते या PayIDs सेटअप करने का निवेदन:** घोटालेबाज उन्हें भुगतान करने (या उनके द्वारा भुगतान किए जाने) के लिए आपसे एक नया बैंक खाता या PayID सेटअप करने के लिए कह सकते हैं। वे आपकी बैंक होने का दिखावा कर सकते हैं और आपसे अपने पैसे सुरक्षित रखने के लिए नए खातों में स्थानांतरित करने के लिए कह सकते/ती हैं।

यदि घोटालेबाज आपके पैसे लेने में सफल हो जाते हैं, तो वे आपसे और अधिक पैसे हथियाने की कोशिश करेंगे। दुर्भाग्यवश घोटाले का शिकार हुए तीन लोगों में से एक व्यक्ति एक से अधिक बार घोटाले का शिकार बनता है। यदि आपने किसी घोटाले में पैसे खो दिए हैं, तो अपने पैसों को वापिस पाने में सहायता के प्रस्ताव देने वाले घोटालेबाजों से सचेत रहें। यह एक अन्य प्रकार का फॉलो-अप घोटाला होता है।

टेक्स्ट या एसएमएस घोटाले

घोटालेबाज सरकार, कानून प्रवर्तन, विश्वसनीय व्यवसायों, या यहाँ तक कि आपके अपने परिवार या दोस्तों की ओर से होने का दिखावा करने वाले मैसेजेस भेजते हैं।

ये मैसेजेस अति आवश्यक प्रतीत होंगे और आपको जल्दी से कदम उठाने के लिए कहने की कोशिश करेंगे। अक्सर इनमें एक लिंक शामिल होगा, जो आपको एक स्कैम वेबसाइट पर ले जाएगा। घोटालेबाज इन स्कैम वेबसाइट्स पर एंटर की गई किसी भी व्यक्तिगत जानकारी को चुरा सकते हैं और इसका उपयोग आपके पैसे हथियाने या आपके नाम पर धोखाधड़ी करने के लिए कर सकते हैं।

घोटालेबाज इन मैसेजेस का वास्तविक होना दिखाने के लिए वैध व्यवसायों या आपके परिचित लोगों के फोन नंबर और कॉलर आईडी के पीछे अपना फोन नंबर कॉपी करके या छिपाकर रखते हैं।

यहाँ तक कि संगठन की ओर से वास्तविक मैसेजेस की समान चेन में ही स्कैम मैसेजेस भी दिखाई दे सकते हैं, जिससे इनकी पहचान करना और भी कठिन हो जाता है।

मैसेज के घोटाला होने के संकेत

मैसेज में:

आपसे तुरंत कदम उठाने, भुगतान करने या पैसे ट्रांस्फर करने के लिए कहा जाता है।

आपसे किसी लिंक पर क्लिक करने या मैसेज में दिए गए नंबर पर कॉल करने के लिए कहा जाता है।

आपसे अपने यूज़रनेम और पासवर्ड के साथ ऑनलाइन खाते में लॉग ऑन करने या अन्य व्यक्तिगत जानकारी प्रदान करने के लिए कहा जाता है।

परिवार के किसी सदस्य या दोस्त की ओर से कहा जाता है कि उनका संपर्क विवरण बदल गया है।

आपको कदम न उठाने पर किसी सेवा को रोकने या आपसे शुल्क वसूलने की धमकी दी जाती है।

आपको या आपके खातों को हैक किए जाने अथवा धोखाधड़ी में शामिल होने का सुझाव दिया जाता है।

आपके भुगतान या आपके पैकेज वितरण में कोई समस्या होने का सुझाव दिया जाता है।

मैसेजिंग घोटालों से स्वयं को सुरक्षित रखने के लिए कदम

1. यदि आपका कोई परिचित व्यक्ति यह बताने के लिए मैसेज भेजता है कि उनके पास एक नया फोन नंबर है, तो:
   a. अपने पास उपलब्ध उनके वर्तमान नंबर पर उन्हें कॉल करने की कोशिश करें, और
   b. उन्हें नए नंबर पर एक प्रश्न के साथ मैसेज भेजें जिसका उत्तर केवल उन्हें ही पता होगा, ताकि यह जाँच की जा सके कि वे वही व्यक्ति हैं जो वे होने का दावा करते हैं।

2. मैसेजेस में दिए गए लिंक्स पर कभी क्लिक न करें।

3. यदि कोई मैसेज किसी वेबसाइट से लिंक करता है, तो लिंक पर क्लिक न करें। इसके बजाय वेबसाइट को स्वयं ऑनलाइन खोजें, या किसी आधिकारिक ऐप का उपयोग करें।

4. उपलब्ध कराए गए फोन नंबर का उपयोग करके टेक्स्ट मैसेज का उत्तर न दें।

5. उस फोन नंबर पर संगठन या व्यक्ति को वापिस कॉल करें जिसकी खोज आपने स्वयं की है, जैसे कि संगठन की वेबसाइट से।

ईमेल घोटाले

घोटालेबाज सरकार, कानून प्रवर्तन और व्यवसायों की ओर से होने का दिखावा करने वाली ईमेलें भेजते हैं। वे आपके द्वारा जल्दी कदम उठाने के लिए अत्यावश्यकता का आभास पैदा करते हैं।

घोटालेबाज वास्तविक संगठन के समान लोगो और समान ईमेल पते का उपयोग करते हैं। घोटालेबाज किसी संगठन या व्यवसाय के ईमेल पते के पीछे अपने ईमेल पते को कॉपी करके या छिपा करके रख सकते हैं, ताकि घोटाले वाली ईमेल को और भी अधिक वास्तविक दर्शाया जा सके।

ईमेल के घोटाला होने के संकेत

ईमेल में:

भुगतान का निवेदन किया जाता है, लेकिन खाते के विवरण नए हैं या आपके द्वारा किए गए अंतिम भुगतान के बाद बदल गए हैं।

आपसे अपने यूज़रनेम और पासवर्ड के साथ ऑनलाइन खाते में लॉग ऑन करने या अन्य व्यक्तिगत जानकारी प्रदान करने के लिए कहा जाता है।

आपको एक ऐसी ईमेल भेजी जाती है जिसकी आप उम्मीद नहीं कर रहे थे/थी, और उसमें एक एटैचमेंट खोलने का निमंत्रण शामिल है।

आपको रिफंड या ऐसे पैसे प्राप्त करने के लिए अपने बैंकिंग विवरण की पुष्टि करने के लिए कहा जाता है, जिसकी आप उम्मीद नहीं कर रहे/ही हैं।

आपके या आपकी इमेजेस के बारे में जानकारी होने का दावा किया जाता है और इन्हें प्रकट करने की धमकी दी जाती है।

आपको पैसे की वसूली अथवा डेटा उल्लंघन या पहचान की चोरी के लिए मुआवज़ा मिलने में सहायता का प्रस्ताव दिया जाता है।

ईमेल घोटालों से स्वयं को सुरक्षित रखने के लिए कदम, जो आप उठा सकते/ती हैं

1. ईमेल के वास्तविक होने की जाँच करने के लिए:
   a. व्यक्ति या संगठन से सीधे उन संपर्क विवरणों का प्रयोग करके संपर्क करें जिनका पता आपने स्वयं लगाया है, जैसे संगठन की वेबसाइट से या,
   b. संगठन की आधिकारिक ऐप के माध्यम से उन्हें एक्सेस करें (कभी भी किसी लिंक के माध्यम से नहीं)।

2. आपको धमकी देने या डराने की कोशिश करने वाले किसी भी व्यक्ति के साथ तुरंत संपर्क बंद कर दें।

3. आपको इन बातों का प्रस्ताव देने वाले किसी भी व्यक्ति को कभी व्यक्तिगत विवरण न दें या कोई भुगतान न करें:
   a. पूर्व में किसी घोटाले या डेटा उल्लंघन से उबरने के लिए मुआवज़ा या सहायता, अथवा
   b. जीत, पुरस्कार या विरासत।

4. यथासंभव multi-factor authentication का उपयोग करें। यह एक अतिरिक्त सुरक्षा पर्त प्रदान करता है और इसका अर्थ है कि घोटालेबाज को आपके ईमेल खाते में एक्सेस प्राप्त करने के लिए आपका ईमेल पासवर्ड और आपके फोन पर भेजा गया एक पिन नंबर जानना होगा।

फोन घोटाले

घोटालेबाज जाने-माने संगठनों की ओर से होने का दावा करते हुए कॉल करते हैं। इसमें सरकारी संगठन, कानून प्रवर्तन, निवेश और कानून फर्म, बैंक और दूरसंचार प्रदाता शामिल हैं।

वे आपके द्वारा जल्दी कदम उठाने के लिए अत्यावश्यकता का आभास पैदा करते हैं। वे आपको अपने व्यक्तिगत या बैंक खाते के विवरण, या अपने कंप्यूटर की एक्सेस देने के लिए आश्वस्त करने की कोशिश कर सकते हैं।

कॉलर के पास आपके बारे में पहले से ही कुछ विवरण उपलब्ध हो सकते हैं, जैसे आपका नाम या पता, जिससे कॉल वास्तविक प्रतीत होती है।

फोन कॉल के घोटाला होने के संकेत

फोन करने वाला व्यक्ति:

भुगतान करने के लिए कहता है या आपको एक नए खाते में पैसे स्थानांतरित करने के लिए कहता है।

आपसे आपका पासवर्ड, पिन, वन-टाइम कोड या कुछ अन्य सुरक्षा जानकारी मांगता है।

आपसे आपके वित्तीय विवरण मांगता है, जैसे क्रेडिट कार्ड या बैंकिंग विवरण।

आपसे आपके मोबाइल फोन या कंप्यूटर पर कोई कार्रवाई करने के लिए कहता है, जैसे सॉफ्टवेयर इंस्टॉल करना या एक संरक्षित खाता एक्सेस करना।

कानून प्रवर्तन की ओर से होने का दावा करता है और आपको तुरंत गिरफ्तारी या देश से निकाले जाने की धमकी देता है।

यह कहता है कि आपके बैंक या अन्य ऑनलाइन खातों को हैक कर लिया गया है या धोखाधड़ी में शामिल किया गया है।

फोन घोटालों से स्वयं को सुरक्षित रखने के लिए कदम, जो आप उठा सकते/ती हैं

1. कॉल के वास्तविक होने की जाँच करने के लिए:
   a. व्यक्ति या संगठन से सीधे उन संपर्क विवरणों का प्रयोग करके संपर्क करें जिनका पता आपने स्वयं लगाया है, जैसे संगठन की वेबसाइट से या,
   b. संगठन की आधिकारिक ऐप के माध्यम से उन्हें एक्सेस करें (कभी भी किसी लिंक के माध्यम से नहीं)।

2. यदि आप सुनिश्चित नहीं हैं कि कॉलर कौन है अथवा यदि वे आपको धमकाते या भयभीत करते हैं, तो तुरंत हैंग अप कर दें।

3. कभी भी ऐसा सॉफ्टवेयर इंस्टॉल न करें, जो किसी अन्य को आपके कंप्यूटर या डिवाइस को एक्सेस करने की अनुमति दे।

4. आप अपरिचित नंबरों से आने वाली कॉलों को अनदेखा कर सकते/ती हैं या ऐसी कॉलों को वॉइसमेल में जाने दे सकते/ती हैं।

जानकर अच्छा लगा!

यदि आपके पास एक निजी नंबर हो या आप Do Not Call रजिस्टर में शामिल हों, तो भी आपको स्कैम कॉलें मिल सकती हैं।

वेबसाइट घोटाले

घोटालेबाज ऑनलाइन रूप से कोई भी होने का दिखावा कर सकते हैं, जिसमें सरकार, कोई वास्तविक व्यवसाय, प्रसिद्ध हस्तियाँ अथवा आपके मित्र या परिवार भी शामिल हैं।

वे प्रसिद्ध ब्रांडों की तरह दिखने के लिए नकली वेबसाइट्स बना सकते हैं। वे प्रसिद्ध लोगों का प्रतिरूपण कर सकते हैं और उन्हें वस्तुओं या सेवाओं को स्वीकृति देते हुए दिखा सकते हैं। आपको भरोसा दिलाने के लिए इन वेबसाइट्स पर नकली समीक्षाएँ शामिल हो सकती हैं।

ऑनलाइन होने पर आपको नकली विज्ञापन बैनर्स या पॉप-अप विंडोज़ दिखाई दे सकती हैं, जिनमें नकली चेतावनियाँ या एरर मैसेजेस शामिल हो सकते हैं।

वेबसाइट के घोटाला होने के संकेत

वेबसाइट में:

सामान्य रूप से या अन्य साइट्स की तुलना में काफी कम कीमतों पर बिक्री के लिए आइटम प्रस्तावित किए जाते है।

आपको कम खतरे या प्रयास के साथ जल्दी, आसानी से पैसे कमाने के तरीके के बारे में बताया जाता है।

अत्यावश्यक चेतावनी या एरर मैसेज होता है, जिसमें आपसे किसी लिंक पर क्लिक करने के लिए कहा जाता है।

असामान्य या विशिष्ट तरीकों से भुगतान करने के लिए कहा जाता है, जैसे गिफ्ट कार्ड्स या Bitcoin जैसी क्रिप्टोकरेंसी के माध्यम से।

केवल सकारात्मक समीक्षाएँ ही शामिल होती हैं।

वेबसाइट घोटालों से सुरक्षित रहने के लिए कदम, जो आप उठा सकते/ती हैं

1. कीमतों की तुलना करें। यदि कोई प्रस्ताव इतना अच्छा प्रतीत हो कि उसपर यकीन करना कठिन हो, तो आमतौर पर यह सच नहीं होता है।

2. आप जिस संगठन या व्यक्ति के साथ व्यवहार कर रहे/ही हैं, उन्हें अपने पैसे या व्यक्तिगत जानकारी देने से पहले उनके बारे में जाँच-पड़ताल करें।

3. वेबसाइट पर ही लिखी गई समीक्षाओं पर भरोसा न करें। वेबसाइट या व्यवसाय का नाम और 'scam' या 'reviews' शब्दों की सर्च करें।

4. यदि आपकी स्क्रीन पर कोई चेतावनी या एरर मैसेज पॉप-अप होता है, तो उसपर क्लिक न करें। इसके बजाय सीधे उस एप्लिकेशन पर जाएँ जिसे यह रेफर करता है, ताकि इसके वास्तविक होने या न होने की की जाँच की जा सके।

5. ऑनलाइन शॉपिंग के लिए आपके द्वारा उपयोग किए जाने वाले डिवाइस में अपने ऑपरेटिंग सिस्टम और ऐप्स के लिए 'automatic updates' को एनेबल करके इसे अप-टु-डेट रखें।

जानकर अच्छा लगा!

स्वयं को ऑनलाइन सुरक्षित रखने के व्यावहारिक तरीके www.cyber.gov.au पर उपलब्ध हैं।

सोशल मीडिया, ऐप-आधारित और ऑनलाइन मैसेजिंग घोटाले

यदि कोई अपरिचित व्यक्ति आपसे सोशल मीडिया, WhatsApp या WeChat जैसे मैसेजिंग प्लेटफॉर्म या ऐप के माध्यम से संपर्क करता है, तो यह एक घोटाला हो सकता है।

कोई अन्य होने का दिखावा करने वाले घोटालेबाज अक्सर उस व्यक्ति की वास्तविक फोटो या उस संगठन के आधिकारिक लोगो का उपयोग करते हैं जिसका वे दिखावा कर रहे हैं, ताकि घोटाले का पता लगाना अधिक कठिन हो जाए।

घोटालेबाज सोशल मीडिया पर नकली प्रोफाइलें सेट-अप करेंगे और सरकार, वास्तविक व्यवसाय, कार्य-नियोक्ता, निवेश फर्म, या यहाँ तक कि कोई दोस्त, परिवार के सदस्य या प्रेमपूर्ण रुचि होने का दिखावा भी करेंगे।

वे प्रसिद्ध लोगों का प्रतिरूपण कर सकते हैं और ऐसा दिखा सकते हैं कि वे वस्तुओं या सेवाओं का प्रचार कर रहे हैं।

घोटालेबाज आपके सोशल मीडिया खातों पर आपके द्वारा प्रकट किए गए विवरणों के माध्यम से भी आपके बारे में बहुत कुछ सीख सकते हैं। वे आपके खाते के पासवर्ड्स का अनुमान लगाने या अन्य घोटालों के माध्यम से आपको लक्षित करने के लिए इस जानकारी का उपयोग कर सकते हैं।

सोशल मीडिया या ऐप घोटाले के संकेत

सोशल मीडिया प्रोफाइल या ऐप में:

आपको कम खतरे या प्रयास के साथ जल्दी, आसानी से पैसे कमाने के तरीके के बारे में बताया जाता है।

आपको किसी प्रतिस्पर्धा या सीमित अवधि के प्रस्ताव में प्रवेश करने के लिए आमंत्रित किया जाता है।

डेटिंग ऐप जैसी किसी ऐप से बातचीत को अन्य निजी चैट या ईमेल पर ले जाने का निवेदन किया जाता है।

किसी प्रसिद्ध व्यक्ति द्वारा किसी उत्पाद या सेवा के अनुमोदन या समर्थन का सुझाव दिया जाता है।

ऐसा कहा जाता है कि आपके द्वारा बेची जाने वाली किसी चीज को कोई अन्य व्यक्ति पहले देखे बिना और ऊँची कीमत पर आपसे खरीदेगा।

आपकी निजी तस्वीर को साझा करने की धमकी दी जाती है, जब तक आप उन्हें पैसे न दें।

आपको नौकरी देने के लिए आपसे संपर्क किया जाता है।

जानकर अच्छा लगा!

अनेकानेक सोशल मीडिया प्लेटफॉर्म्स पर सुरक्षित कैसे रहें, इस बारे में जानकारी www.esafety.gov.au पर उपलब्ध है।

सोशल मीडिया और ऐप-आधारित घोटालों से सुरक्षित रहने के लिए कदम, जो आप उठा सकते/ती हैं

1. इस बात की जाँच करें कि क्या प्रोफाइल नकली हो सकती है। क्या खाता सक्रिय है? उनके कितने फ्रेंड्स/फॉलोवर्स हैं और वे ऑनलाइन कितना पोस्ट करते हैं?

2. 'Scam' शब्द के साथ प्रोफाइल के नाम की ऑनलाइन खोज करें।

3. साक्षात्कार, या आपके अनुभव, उपयुक्तता और संदर्भों के बारे में चर्चा किए बिना आपको प्रस्तावित की गई नौकरी को कभी न स्वीकार करें। भर्तीकर्ता और पद का प्रस्ताव देने वाले व्यवसाय या व्यक्ति-विशेष के बारे में जाँच-पड़ताल करें। भर्ती एजेंसी से असंबद्ध इंटरनेट खोज से प्राप्त फोन नंबरों के माध्यम से उनसे संपर्क करें। केवल नौकरी का पद बचाकर रखने के लिए ही पैसों का भुगतान न करें।

4. निवेश के बारे में केवल Australian Financial Services लाइसेंसधारी व्यक्ति से ही सलाह लें और यह जाँच करें कि कंपनी या वेबसाइट का नाम International Organization of Securities Commission's (IOSCO) इन्वेस्टर एलर्ट पोर्टल पर तो नहीं है।

5. कभी भी किसी ऐसे व्यक्ति को पैसे न दें, जिससे आप केवल ऑनलाइन मिले हों। घोटालेबाज अक्सर कहते हैं कि वे विदेश में रहते हैं और आपसे व्यक्तिगत रूप से नहीं मिल सकते/ती हैं।

6. किसी ऐसे व्यक्ति को कभी भी अपनी अंतरंग तस्वीरें न भेजें, जिससे आप केवल ऑनलाइन मिले हों।

घोटालों के बारे में और अधिक जानकारी के लिए Scamwatch पर जाएँ, जहाँ ऐसे अन्य तरीके भी शामिल हैं जिनके माध्यम से घोटालेबाज आपसे संपर्क कर सकते हैं, जैसे व्यक्तिगत रूप से और डाक से।

प्रमुख घोटाले, जिनके बारे में आपको पता होना चाहिए

यहाँ कुछ सबसे सामान्य प्रकार के घोटाले दिए गए हैं, जिनके बारे में आपको अवगत होना चाहिए। आप Scamwatch वेबसाइट पर इनमें से प्रत्येक प्रकार के घोटालों के बारे में और अधिक जानकारी प्राप्त कर सकते/ती हैं, जिसमें चेतावनी के संकेत और आपकी सुरक्षा के लिए कदम भी शामिल हैं।

प्रतिरूपण घोटाले

घोटालेबाज आपको यह मानने के लिए धोखा देते हैं कि वे विश्वसनीय संगठनों की ओर से हैं, जैसे पुलिस, सरकार, बैंकें और प्रसिद्ध व्यवसाय। वे आपके दोस्त या परिवार के सदस्य होने का नाटक भी कर सकते हैं। घोटालेबाज फ़िशिंग ईमेल्स या मैसेजेस भेजकर आपके बारे में जानकारी की खोज करते हैं। इन्हें आपकी जानकारी की चोरी करने के लिए निर्मित किया जाता है। वे किसी आधिकारिक संगठन या आपके किसी परिचित या भरोसेमंद व्यक्ति की ओर से होने का दिखावा करके आपको अपनी व्यक्तिगत जानकारी देने के लिए आश्वस्त करने की कोशिश करते हैं।

घोटालेबाज अपनी कॉल्स या मैसेजेस को वैध फोन नंबरों की ओर से होने का दिखावा करने के लिए तकनीकी का उपयोग करते हैं। वे किसी संगठन के वास्तविक मैसेजेस की चर्चा श्रृंखला में ही टेक्स्ट मेसेजेस को प्रदर्शित कर सकते हैं।

निवेश घोटाले

घोटालेबाज विश्वसनीय मार्केटिंग और नई तकनीकी का उपयोग करके अपने निवेश प्रस्ताव को इतना अच्छा दिखाते हैं कि आपको लगता है कि आप इनसे चूक न जाएँ। वे आपसे कम या खतरे से मुक्त बड़े डिविडेंड्स का वादा करते हैं। वे अक्सर आपके द्वारा जल्दी कदम उठाए जाने के लिए दबावपूर्ण कार्यनीति का उपयोग करते हैं, ताकि वे आपके पैसे चुरा सकें।

नौकरी और रोजगार घोटाले

घोटालेबाज ऐसी नौकरियाँ प्रस्तावित करते हैं, जो कम प्रयास के साथ अच्छा वेतन देती हैं। वे हाई-प्रोफाइल कंपनियों और ऑनलाइन शॉपिंग प्लेटफॉर्म्स की ओर से भर्ती करने का दिखावा करते हैं। कभी-कभी उनके द्वारा सूचीबद्ध की गई नौकरी वास्तविक होती ही नहीं है। घोटालेबाज प्रसिद्ध भर्ती एजेंसियों का प्रतिरूपण भी करते हैं। उनका लक्ष्य आपके पैसे और व्यक्तिगत जानकारी चुराना होता है। वे आपसे पैसों का पूर्वभुगतान करने के लिए कह सकते हैं, ताकि आप उनके लिए काम करने में सक्षम हो सकें।

उत्पाद और सेवाएँ घोटाले

घोटालेबाज आपके पैसे चुराने के लिए एक खरीदार या विक्रेता होने का प्रतिरूपण करते हैं। वे वैध रिटेलर साइट्स पर नकली वेबसाइट्स या प्रोफाइलें बनाकर उत्पादों या सेवाओं के लिए इतनी अच्छी कीमतों का प्रस्ताव देते हैं कि उनपर यकीन करना कठिन होता है। वे नकली विज्ञापन और नकली समीक्षाएँ पोस्ट करते हैं। वे चोरी किए गए लोगो, किसी .com.au डोमेन नेम और चोरी किए गए Australian Business Number (ABN) का उपयोग कर सकते हैं। इन घोटालों का पता लगाना कठिन होता है।

घोटालेबाज आपको नकली बिल भेजने के लिए आपके परिचित और भरोसेमंद व्यवसाय होने का प्रतिरूपण भी करते हैं। वे वास्तविक इन्वॉइसों में विवरण भी बदल सकते हैं, ताकि ग्राहक आपके बजाय घोटालेबाज को भुगतान करे।

प्रेम (रोमांस) के घोटाले

घोटालेबाज आपके पैसे चुराने के लिए प्रेम, डेटिंग या दोस्ती के वादे का इस्तेमाल करते हैं। वे यह जताने के लिए काफी गहराई तक जाते हैं कि संबंध वास्तविक है और उन्हें पैसे देने के लिए आपके साथ चालाकी करते हैं।

घोटालेबाज सोशल मीडिया, डेटिंग या गेमिंग ऐप्स और वेबसाइट्स पर आपको ढूंढते हैं। वे आपको टेक्स्ट या ईमेल भी भेज सकते हैं। वे कभी-कभी प्रसिद्ध लोगों समेत अन्य लोगों की नकली प्रोफाइलों और पहचानों के पीछे छिपे रहते हैं। एक बार जब आप उनपर भरोसा कर लेते/ती हैं, तो वे ऐसा दिखावा करेंगे कि वे एक 'आपातस्थिति' में हैं और आपसे सहायता मांगेंगे। यह अक्सर पैसे या अन्य उत्पादों के लिए अनुरोध होगा।

धमकी और ज़बरन वसूली घोटाले

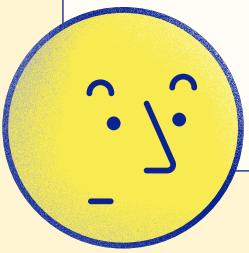
घोटालेबाज किसी विश्वसनीय संगठन की ओर से होने का दिखावा करते हैं और यह दावा करते हैं कि आपको पैसे देने की आवश्यकता है, अन्यथा कुछ बुरा होगा। यदि आप उन्हें तुरंत भुगतान करने के लिए सहमत नहीं होते/ती हैं, तो वे आपको गिरफ्तारी, देश से निकाले जाने, अथवा यहाँ तक कि शारीरिक नुकसान होने की धमकी भी दे सकते हैं।

वे आपके द्वारा भेजी गई नग्न तस्वीरों या वीडियो को साझा करने की धमकी देकर आपको ब्लैकमेल भी कर सकते/ती हैं, जबतक कि आप उन्हें पैसे न भेजें।

अप्रत्याशित पैसों के घोटाले

घोटालेबाज आपको यह समझाने की कोशिश करते हैं कि आपके ऊपर पैसे बकाया हैं अथवा आप पैसों या जीत के/की हकदार हैं, जिसे मिलने की आपको उम्मीद ही नहीं थी।

आपके द्वारा पैसे या जीत एकत्र कर पाने से पहले घोटालेबाज आपको शुल्क का भुगतान करने अथवा अपनी बैंकिंग या पहचान के विवरण देने के लिए कहता है। दुर्भाग्यवश कोई भी पैसे मुफ़्त में नहीं होते हैं।



घोटालों की रिपोर्ट कहाँ करें

हम घोटालों की पहचान करने, इनसे सुरक्षित रहने और इनकी रिपोर्ट करने के तरीके के बारे में जागरुकता बढ़ाकर ऑस्ट्रेलिया को घोटालेबाजों के लिए एक अधिक कठिन लक्ष्य बनाने की दिशा में काम कर रहे हैं।

हम घोटालों की रिपोर्टों से जानकारी साझा करते हैं और घोटालों को बाधित करने व इन्हें रोकने के लिए सरकार, कानून प्रवर्तन और निजी क्षेत्र के साथ काम करते हैं।

Scamwatch पर रिपोर्ट करके दूसरों की सहायता करें। Scamwatch की वेबसाइट www.scamwatch.gov.au पर उपलब्ध रिपोर्ट फॉर्म भरके घोटाले के अपने अनुभव के बारे में सूचना दें।

याद रखें, यदि आप किसी घोटाले का शिकार हुए/ई हैं, तो आपके लिए जल्दी कदम उठाना महत्वपूर्ण है।

- यदि किसी घोटालेबाज के कारण आपका पैसा डूब गया है, तो अपनी बैंक या कार्ड प्रदाता से संपर्क करें।
- IDCARE से संपर्क करें: 1800 595 160 | idcare.org

और अधिक सहायता एवं समर्थन

किसी घोटाले का शिकार बनने से असुरक्षित महसूस हो सकता है। यह याद रखना महत्वपूर्ण है कि ऐसा किसी के साथ भी हो सकता है, और समर्थन उपलब्ध है।

यदि आपके या आपके किसी परिचित के साथ घोटाला हुआ है, तो इस बारे में किसी से बात करें। आप परिवार, दोस्तों, अपने जीपी या निम्नलिखित में से किसी समर्थन सेवा से समर्थन प्राप्त कर सकते/ती हैं।

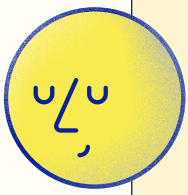
Lifeline: 13 11 14 | lifeline.org.au
या ऑनलाइन संकट समर्थन चैट (दिन में 24 घंटे, सप्ताह में 7 दिन)

Beyond Blue: 1300 22 4636 | beyondblue.org.au
या ऑनलाइन चैट (दिन में 24 घंटे, सप्ताह में 7 दिन)

Kids Helpline: 1800 55 1800 | kidshelpline.com.au
(दिन में 24 घंटे, सप्ताह में 7 दिन)

घोटालों के आर्थिक प्रभाव विनाशकारी और जीवनपरिवर्तक हो सकते हैं।

यदि आपको आर्थिक कठिनाई का सामना करना पड़ रहा है, तो आप National Debt Helpline: 1800 007 007 पर सोमवार से शुक्रवार सुबह 9:30बजे से दोपहर 4:30बजे तक किसी वित्तीय सलाहकार से बात कर सकते/ती हैं या फिर सोमवार से शुक्रवार सुबह 9:00बजे से रात 8:00बजे तक लाइव चैट का उपयोग करें।



scamwatch.gov.au