AUSTRALIAN COMPETITION & CONSUMER COMMISSION

घोटालों की छोटी काली पुस्तिका
(The Little Black Book of Scams)

पॉकेट-आकार की एक मार्गदर्शिका, जिससे आप घोटालों की पहचान कर सकें, उनसे वर्जन कर सकें, और खुद को सुरक्षित रख सकें

AUSTRALIAN COMPETITION & CONSUMER COMMISSION

घोटालों की छोटी काली पुस्तिका
(The Little Black Book of Scams)

पॉकेट-आकार की एक मार्गदर्शिका, जिससे आप घोटालों की पहचान कर सकें, उनसे वर्जन कर सकें, और खुद को सुरक्षित रख सकें

ISBN 978 1 920702 00 7

ऑस्ट्रेलियाई प्रतिस्पर्धा और उपभोक्ता आयोग (Australian Competition and Consumer Commission)
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 12/16_1129

www.accc.gov.au

सामग्री

परिचय

हरेक साल घोटालों के कारण ऑस्ट्रेलियावासियों, व्यवसायों और अर्थव्यवस्था को करोड़ों डॉलरों की क्षति होती है और पीड़ितों और उनके परिवारों को भावनात्मक नुकसान पहुँचता है।

स्वयं को सुरक्षित रखने का सबसे अच्छा तरीका जागरुकता और जानकारी रखना है। *घोटालों की छोटी काली पुस्तिका* के इस नए संस्करण को आपके लिए ऑस्ट्रेलियाई प्रतिस्पर्धा और उपभोक्ता आयोग (एसीसीसी) द्वारा प्रस्तुत किया गया है, जो उपभोक्ताओं की सुरक्षा के लिए राष्ट्रीय एजेंसी हैं। घोटालों की छोटी काली पुस्तिका को उपभोक्ताओं और छोटे व्यवसायों के लिए घोटालों के बारे में अवगत होने के लिए एक महत्वपूर्ण उपकरण के रूप में अंतरराष्ट्रीय स्तर पर मान्यता दी गई है, जिनमें निम्नलिखित शामिल हैं:

- सबसे आम घोटाले, जिनके प्रति सचेत रहना चाहिए
- विभिन्न तरीके, जिनके माध्यम से घोटालेबाज आपसे संपर्क कर सकते हैं
- आपके साथ चालाकी करने के लिए घोटालेबाजों द्वारा प्रयोग किए जाने वाले उपकरण
- चेतावनी के संकेत
- अपने आप को सुरक्षित रखने के तरीके, और
- आपको सहायता कहाँ से प्राप्त हो सकती है।

घोटालों की छोटी काली पुस्तिका इस वेबसाइट पर उपलब्ध है:
www.accc.gov.au/littleblackbookofscams।

अपनी सुरक्षा करें—स्कैमवॉच के लिए साइन अप करें

घोटालेबाजों से एक कदम आगे रहने के लिए एसीसीसी की स्कैमवॉच वेबसाइट —www.scamwatch.gov.au पर जाएँ तथा और अधिक जानकारी प्राप्त करें, जहाँ आप उपभोक्ताओं और छोटे व्यवसायों को निशाना बनाने वाले नए घोटालों के लिए निःशुल्क ईमेल चेतावनियों के लिए साइन अप कर सकते/सकती हैं। आप Twitter पर @scamwatch_gov या http://twitter.com/scamwatch_gov पर स्कैमवॉच को फॉलो भी कर सकते/सकती हैं।

सबसे आम घोटाले, जिनसे बचकर रहना चाहिए

कोई भी व्यक्ति घोटालों की चपेट में आ सकता है, इसलिए सभी को घोटालों की पहचान करने और उनसे बचकर रहने के बारे में जानकारी रखनी चाहिए। कुछ लोग सोचते हैं कि केवल लालची लोग ही घोटालों के शिकार होते हैं। सच्चाई यह है कि घोटालेबाज चालाक होते हैं और यदि आप यह नहीं जानते/जानती हैं कि किन बातों के प्रति सचेत रहना चाहिए, तो कोई भी व्यक्ति घोटाले का शिकार हो सकता है।

क्या आपको कोई ऐसा प्रस्ताव मिला है जो बहुत ही अच्छा लगता है, जैसे शायद आपको अपना कंप्यूटर ठीक करने में मदद दे के लिए फोन कॉल की गई हो या आपको ऐसी धनराशि का भुगतान करने के लिए धमकी मिली हो जो आपने उधार ही न ली हो, आपके बैंक या दूरसंचार प्रदाता की ओर से आपको अपने खाते में किसी समस्या के बारे में चेतावनी मिली हो या ऑनलाइन 'दोस्ती' या कनेक्ट करने के लिए निमंत्रण मिला हो? घोटालेबाज जानते हैं कि वे जो हासिल करना चाहते हैं उसके लिए आपकी नब्ज़ कैसे पकड़नी है।

वे समय के साथ आगे बढ़ते हुए नई तकनीकी, नए उत्पादों या सेवाओं से लाभ उठाकर और प्रमुख घटनाओं से आपको भरोसे में लेने वाली कहानियाँ गढ़कर और भी चालाक बनते जा रहे हैं, ताकि वे आपसे आपके पैसे ऐंठ सकें या आपका व्यक्तिगत विवरण हासिल कर सकें।

परंतु हरेक साल प्राप्त होने वाली हज़ारों घोटालों की रिपोर्टों के आधार पर एसीसीसी ने घोटालेबाजों की चालों और चालाकियों को उजागर करने के लिए सामान्य घोटालों की एक सूची तैयार की है, जिनके बारे में घोटालेबाज आपको अंधेरे में रखना चाहते हैं।

डेटिंग और प्रेम के नाटक वाले घोटाले

हरेक साल डेटिंग और प्रेम के नाटक वाले घोटालों से ऑस्ट्रेलियावासियों को करोड़ों डॉलर का नुकसान होता है और ऐसे घोटाले लोगों और परिवारों को बर्बाद कर सकते हैं।

घोटाला कैसे किया जाता है

डेटिंग और प्रेम का नाटक करने वाले घोटालेबाज वैध डेटिंग वेबसाइटों, मोबाइल ऐप्स या फेसबुक जैसे सोशल मीडिया प्लेटफॉर्मों पर अक्सर दूसरे लोगों की चोरी की गई तस्वीरें और पहचान का इस्तेमाल करके फर्जी प्रोफाइलें बनाते हैं। वे इन प्रोफाइलों का प्रयोग करके आपके साथ प्रेम संबंध बनाने की कोशिश करते हैं, जो आपके पैसे हड़पने का मौका मिलने तक महीनों या वर्षों तक चल सकते हैं। घोटालेबाज बीमार होने, चोट लगने, यात्रा के खर्चे या परिवार के संकट में मदद के लिए पैसे माँगेंगे। वे निर्दयी होते हैं और वे आपके अच्छे स्वभाव से लाभ उठाने के लिए आपसे झूठ बोलेंगे।

घोटालेबाज सामान्यतः विदेश में रह रहे होंगे और उनके पास इस बात का बहाना होगा कि वे वहाँ क्यों हैं, जैसे सेना में सेवा देना, इंजीनियर के रूप में काम करना या किसी दोस्त या रिश्तेदार की देखभाल करना। घोटालेबाज जो व्यक्ति होने का दावा करते हैं, वे कभी भी नहीं होते हैं और कुछ चालाक घोटालेबाज छोटे-मोटे उपहार भी भेज सकते हैं। यह बाद में आपसे और भी अधिक पैसे ऐंठने की एक बड़ी योजना का हिस्सा होता है।

अपनी सुरक्षा करें

- कभी भी ऐसे किसी व्यक्ति को पैसे न भेजें या अपना व्यक्तिगत विवरण न दें, जिससे आपने केवल ऑनलाइन मुलाकात की है।
- यदि कोई ऑनलाइन प्रशंसक केवल कुछ बार 'संपर्क' करने या बातचीत करने के बाद डेटिंग वेबसाइट या सोशल मीडिया प्लेटफॉर्म से बाहर संवाद करने के लिए कहता है, तो सावधान रहें - वह एक घोटालेबाज हो सकता है।
- अपने प्रशंसक की इमेज सर्च करके यह निर्धारित करने में सहायता प्राप्त करें कि वह जो व्यक्ति होने का दावा करता है, क्या वह वास्तव में वही व्यक्ति है। आप Google या TinEye जैसी इमेज सर्च सेवाओं का उपयोग कर सकते/सकती हैं।
- अंतरंग तस्वीरों या वीडियो को ऑनलाइन साझा करते समय सतर्क रहें। घोटालेबाजों को ऐसी तस्वीरों या वीडियो का प्रयोग करके अपने लक्ष्यों को ब्लैकमेल करने के लिए जाना जाता है, जिन्हें आप किसी अन्य व्यक्ति द्वारा नहीं देखा जाना चाहते/चाहती हैं।

निवेश केघोटाले

'खतरा मुक्त निवेश' या दुर्भाग्य को न्यौता?

घोटाला कैसे किया जाता है

निवेश के घोटाले कई रूपों में सामने आते हैं, जिनमें क्रिप्टोकरेंसी खरीद, बाइनरी विकल्प ट्रेडिंग, व्यापार उद्यम, सेवा-निवृत्ति योजनाएँ, प्रबंधित फंड और शेयरों या संपत्ति की बिक्री या खरीद शामिल हैं। घोटालेबाज अपने फर्जी कार्यों को पूरा करने के लिए पेशेवर दिखने वाले ब्रोशर और वेबसाइटों के साथ 'अवसर' तैयार करते हैं। ऐसे घोटाले अक्सर फोन कॉल या घोटालेबाज की ओर से मिली अनपेक्षित ईमेल से शुरू होते हैं, जिसमें एक 'नॉट-टु-बी-मिस्ड', 'हाई रिटर्न' या 'गारंटीड' अवसर प्रस्तुत किया जाता है। घोटालेबाज सामान्यतः विदेश से काम करता है, और उसके पास ऑस्ट्रेलियाई वित्तीय सेवाओं (Australian Financial Services) का लाइसेंस नहीं होगा।

भविष्यवाणी करने वाले कंप्यूटर सॉफ्टवेयर के घोटाले शेयर बाज़ार के उतार-चढ़ावों, घुड़दौड़ों के परिणामों, खेल आयोजनों या लॉटरी के परिणामों की सटीक भविष्यवाणी करने का वादा करते हैं। वास्तव में वे निवेश के रूप में जुए का एक प्रारूप होते हैं। अधिकाँश योजनाएँ या कार्यक्रम काम नहीं करते हैं और खरीदारों को अपना पैसा वापस नहीं मिलता है। कई बार तो सप्लायर रातों-रात गायब हो जाता है।

सेवा-निवृत्ति के घोटाले अक्सर एक स्व-प्रबंधित सुपर फंड के माध्यम से या एक शुल्क अदा करके सुपर फंड को आपके लिए समय से पूर्व सुलभ कराने का दावा करते हैं। घोटालेबाज आपको अपना पैसा समय से पूर्व प्राप्त करने के लिए एक कहानी पर भरोसा करने के लिए कह सकता है, और फिर आपके वित्तीय सलाहकार के रूप में कार्य करते हुए वह आपके सुपर लाभों का भुगतान सीधे खुद प्राप्त करने के लिए आपकी सेवा-निवृत्ति लाभ कंपनी को सीधे धोखा देता है। जब घोटालेबाज को आपका पैसा मिल जाता है, तो वह एक बड़ी 'फीस' ले सकता है या हो सकता है सब-कुछ खुद हड़पकर आपके लिए कुछ भी न छोड़े।

अपनी सुरक्षा करें

- अपने पैसे या निवेश के बारे में निर्णय लेने के लिए किसी को भी अपने ऊपर दबाव न डालने दें - विशेषकर यदि प्रस्ताव अनपेक्षित रूप से मिला हो।
- अपना पैसा देने से पहले निवेश कंपनी के बारे में स्वयं जाँच-पड़ताल करें और इस बात का पता लगाने के लिए वेबसाइट www.moneysmart.gov.au देखें कि उनके पास ऑस्ट्रेलियाई वित्तीय सेवाओं का लाइसेंस है या नहीं। अपने आप से पूछें: यदि कोई अजनबी पैसे कमाने का रहस्य जानता है, तो वह इसे साझा क्यों करेगा?

यदि आपकी उम्र सेवा-निवृत्ति की आयु से कम हैं, तो अपने संरक्षित सेवा-निवृत्ति लाभों को समय से पूर्व सुलभ कनाने वाले प्रस्तावों के प्रति सचेत रहें। अवैध रूप से अपने सुपर से समयपूर्व पैसा निकालने पर आपको कराधान कानून के तहत दंड दिया जा सकता है।

धमकी और जुर्माने के घोटाले

अगर कोई सरकारी प्राधिकरण या विश्वसनीय कंपनी आपको भुगतान करने के लिए कह रही है, तो रुकें, विचार करें और दोबारा जाँच करें।

घोटाला कैसे किया जाता है

ऐसे घोटाले इनाम, पैसे या छूट का प्रस्ताव देने के बजाए आपसे पैसे हड़पने के लिए भयभीत करने वाली धमकियों का प्रयोग करते हैं। घोटालेबाज आपको कॉल कर सकता है और आपको **गिरफ्तार** किए जाने की धमकी दे सकता है या फिर आपके ऊपर **तेज गति से वाहन चलाने, कर कार्यालय के ऋण** या **भुगतान न किए गए बिल** की बकाया राशि का दावा करने वाली ईमेल भेज सकता है।

फोन कॉल के दौरान घोटालेबाज आपके ऊपर तुरंत भुगतान करने के लिए दबाव डालेंगे और आपसे कहेंगे कि यदि आप मना करते/करती हैं, तो आपके घर पुलिस भेज दी जाएगी। घोटालेबाज हमारे समुदाय के कमजोर लोगों को लक्षित करने के लिए जाने जाते हैं, जैसे नए आए आप्रवासी। वे आव्रजन विभाग के अधिकारी होने का दिखावा करते हैं और अपने शिकार लोगों को वीज़ा में हुई गलतियों को सुधारने के लिए फीस का भुगतान न करने पर उन्हें **निर्वासन** की धमकी देते हैं। इसी तरह के एक अन्य घोटाले में घोटालेबाज स्वयं को ऑस्ट्रेलियाई कर कार्यालय (Australian Tax Office) का अधिकारी बताकर अपने शिकार को बकाया कर के बारे में बताते हैं।

घोटालेबाज आपकी बैंक, गैस, बिजली, पानी या फोन प्रदाता जैसी **भरोसेमंद कंपनियों** की ओर से होने का भी दिखावा करते हैं। यदि आप तुरंत बिल का भुगतान नहीं करते/करती हैं, तो वे आपकी सेवा को रद्द करने या आपसे अत्यधिक जुर्माना शुल्क वसूल करने की धमकी देंगे। कभी-कभी वे ऑस्ट्रेलिया पोस्ट (Australia Post) जैसे व्यवसाय की ओर से होने का दावा करके कह सकते हैं कि आपके लिए कोई वस्तु प्राप्त हुई है जिसे पिक-अप करना ज़रूरी है और यदि आप भुगतान नहीं करते/करती हैं तो आपसे हरेक दिन के लिए एक होल्डिंग शुल्क लिया जाएगा। चाहे जो भी हो, वे आपको चिंता में डालकर और कहानी

की सच्चाई के बारे में विचार और जाँच करने का समय दिए बिना अपना काम निकलवाने की कोशिश करते हैं।

यदि यह घोटाला ईमेल से भेजा जाता है, तो इसमें कोई एटैचमेंट या किसी फर्जी वेबसाइट का लिंक होने की संभावना होती है, जहाँ आपसे 'बिल', 'जुर्माने' या 'डिलीवरी विवरण' के प्रमाण को डाउनलोड करने के लिए कहा जाएगा। एटैचमेंट खोलने या फाइल डाउनलोड करने पर आपका कंप्यूटर मैलवेयर से संक्रमित हो जाएगा (पृष्ठ 16 देखें)।

अपनी सुरक्षा करें

- फोन पर धमकी देने वाले व्यक्ति के दबाव में न आएँ। रुकें, सोचें और उसकी कहानी की सच्चाई की जाँच करें।
- कोई सरकारी एजेंसी या भरोसेमंद कंपनी आपको गिफ्ट कार्ड, वायर ट्रांसफर या बिटकॉइन जैसे असामान्य तरीकों से भुगतान करने के लिए कभी नहीं कहेगी।
- संबंधित संगठन को सीधे कॉल करके उस संपर्क व्यक्ति की पहचान सत्यापित करें - फोन बुक, पुराने बिल या ऑनलाइन सर्च जैसे किसी निष्पक्ष स्रोत के माध्यम से उसके बारे में खोज करें।
- फोन कॉल या ईमेल में आपको दिए गए संपर्क विवरण का उपयोग न करें। किसी निष्पक्ष स्रोत के माध्यम से फिर से उसके बारे में खोज करें।

अनपेक्षित पैसे के घोटाले

यदि आपको सामान या पैसे प्राप्त करने से पहले कुछ भुगतान करने के लिए कहा जाता है, तो दो बार सोचें।

घोटाला कैसे किया जाता है

घोटालेबाज आपको अनपेक्षित तरीके से बताते हैं कि आप पैसे, बहुमूल्य रत्न, सोने या मूल्यवान शेयरों के हकदार हैं लेकिन उन्हें प्राप्त करने के लिए आपको **अग्रिम भुगतान** करने होंगे। आपसे जिस चीज का वादा किया गया था, वह आपको कभी नहीं मिलेगी और हमेशा इस बात का बहाना बनाया जाएगा कि आपको और अधिक भुगतान करने की ज़रूरत क्यों है। यदि आप फीस का भुगतान करते/करती हैं, तो आपको अपना पैसा कभी वापस नहीं मिलेगा।

रिबेट या रिक्लेम के घोटालों में घोटालेबाज आपको बताता है कि आपको कर का अधिक भुगतान किए जाने, बैंक फीस या किसी प्रकार के मुआवज़े जैसे कारणों की वज़ह से पैसा दिया जाना है। परंतु अपना पैसा प्राप्त करने से पहले आपको एक छोटे से प्रशासन शुल्क का भुगतान करने के लिए कहा जाता है।

विरासत के घोटालों में स्वयं को वकीलों, बैंकरों या विदेशी अधिकारियों के रूप में प्रस्तुत करके घोटालेबाज आपको बताते हैं कि आप एक बड़ी-भारी विरासत के/की हकदार हैं या आपका नाम एक मृत व्यक्ति के समान होने के कारण वे आपको एक योजना में हिस्सा देने का प्रस्ताव देते हैं। वे अक्सर आधिकारिक दिखने वाले दस्तावेज़ों का प्रयोग करते हैं और आपको विरासत दिए जाने से पहले वे आपसे शुल्क और करों के लिए भुगतान करने के लिए कहते हैं। वे 'आधिकारिक दस्तावेज़' भरने के लिए आपके व्यक्तिगत विवरण भी माँग सकते हैं। इसका अर्थ है कि आपके पैसे के साथ-साथ आपकी पहचान की चोरी भी की जा सकती है।

सामान्य रूप से **नाइजीरियाई घोटाले** कहे जाने वाले घोटाले संभवतः पश्चिम अफ्रीका में शुरू हुए होंगे, लेकिन ये दुनिया में कहीं से भी आ सकते हैं। इन

घोटालों में घोटालेबाज आपको बताते हैं कि उन्हें एक बड़ी-भारी संपत्ति को सुरक्षित करने के लिए आपकी सहायता की ज़रूरत है, जिसे वे अपने देश से बाहर स्थानांतरित करने की कड़ी कोशिश कर रहे हैं। वे दावा कर सकते हैं कि यह संपत्ति गुप्त पैसा, स्वर्ण, या भ्रष्ट सरकार या अधिकारी द्वारा पीछे छोड़ी गई परिसंपत्ति है और यदि आप इसे प्राप्त करने के लिए सहमत हैं, तो वे सुरक्षित होने पर आपको इसका एक बड़ा-भारी हिस्सा देंगे। ऐसे सभी घोटालों के समान ही वे आपसे कहेंगे कि इन पैसों को आपको भेजने से पहले आतंकवाद-विरोधी गतिविधियों और मनी लॉन्डरिंग की जाँच किए जाने के लिए आपको कर, बैंक के शुल्क या फीस के लिए भुगतान करना होगा।

सामान्य रूप से ये घोटाले विदेशों से आते हैं और आपको वायर ट्रांसफर के माध्यम से भुगतान करने के लिए कहा जाता है, लेकिन बैंक ट्रांसफर या अन्य विधियों से भुगतान करने के लिए भी कहा जा सकता है।

यदि आप इन घोटालों के बहकावे में आ जाते/जाती हैं, तो आपको घोटालेबाज से कुछ भी हासिल नहीं होगा और आप अपने भेजे हुए पैसे भी खो देंगे/देंगी।

अपनी सुरक्षा करें

- यह बात याद रखें कि ऐसी कोई योजना नहीं होती है, जो तुरंत धनवान बना सके: यदि कोई चीज़ इतनी अच्छी है कि लगता है वह सच नहीं हो सकती है, तो शायद वह सच नहीं है।
- किसी अजनबी द्वारा मनी ऑर्डर, वायर ट्रांसफर, अंतर्राष्ट्रीय फंड्स ट्रांसफर, प्रि-लोडेड कार्ड या इलेक्ट्रॉनिक करेंसी के माध्यम से तुरंत भुगतान करने के लिए कहने वाली व्यवस्था से दूर रहें। इस तरह से भेजे गए पैसों को वापिस पाना बहुत ही कठिन होता है।
- यदि कोई अनपेक्षित ईमेल संदिग्ध लगती है, तो उसे बस डिलीट कर दें। किसी भी लिंक पर क्लिक न करें।
- सरकारी विभाग, बैंक या सेवाएँ किसी शुल्क या छूट के लिए दावा करने से पहले आपको पैसे का तुरंत भुगतान करने के लिए कभी संपर्क नहीं करेंगे।
- सुनिश्चित न होने पर संपर्क की पहचान के बारे में स्वतंत्र रूप से जाँच करें। आपको भेजे गए संदेश में दिए गए संपर्क विवरण का प्रयोग न करें-फोन बुक या ऑनलाइन सर्च जैसे स्वतंत्र स्रोत के माध्यम से सही संपर्क विवरण प्राप्त करें।
- प्रस्ताव में दिए गए शब्दों का अक्षरशः प्रयोग करके ऑनलाइन सर्च करें - इस तरह से कई घोटालों की पहचान की जा सकती है।

इनाम और लॉटरी के घोटाले

किसी अप्रत्याशित इनाम के लालच में न आएँ – केवल घोटालेबाज ही यह इनाम अपने घर ले जाता है।

घोटाला कैसे किया जाता है

इन घोटालों में आपको ऐसी लॉटरी, स्वीपस्टेक या प्रतियोगिता से इनाम प्राप्त करने के लिए पैसे या अपने व्यक्तिगत विवरण देने के लिए कहा जाता है, जिसमें आपने कभी भाग ही नहीं लिया था। घोटालेबाज दावा करते हैं कि आपकी 'जीत' या इनाम आपको भेजे जाने से पहले आपको शुल्क या करों के लिए भुगतान करना होगा। आपको अपने इनाम का दावा करने के लिए एक ऊँची दर वाले फोन नंबर पर कॉल या टेक्स्ट करना पड़ सकता है।

स्क्रैची घोटालों में डाक से कई आकर्षक ब्रोशर और स्क्रैची कार्ड प्राप्त होते हैं, जिनमें से एक विजेता होगा। इसे और अधिक विश्वसनीय बनाने के लिए यह अक्सर दूसरा या तीसरा इनाम होता है। जब आप अपने इनाम का दावा करने के लिए कॉल करते/करती हैं, तो घोटालेबाज आपको अपना इनाम प्राप्त करने से पहले शुल्क या करों का भुगतान करने के लिए कहेंगे।

लॉटरी के घोटालों में यह दावा करने के लिए वास्तविक विदेशी लॉटरियों के नामों का प्रयोग किया जा सकता है कि आपने एक नकद लॉटरी जीती है, भले ही आपने उसमें कभी हिस्सा न लिया हो। घोटालेबाज सामान्यतः पैसे भेजने के लिए फीस या कर भरने की माँग करते हैं। वे आपको यह भी बताएँगे कि आपको सही विजेता प्रमाणित करने के लिए उन्हें आपके व्यक्तिगत विवरण की आवश्यकता है, लेकिन फिर वे इस जानकारी का उपयोग आपके बैंक खाते से आपकी पहचान या धन की चोरी करने के लिए करते हैं।

नकली वाउचर और गिफ्ट कार्ड के घोटालों में आपको घोटालेबाज द्वारा एक ईमेल या टेक्स्ट संदेश या सोशल मीडिया संदेश भेजा जाता है, जिसमें यह दावा किया जाता है कि आपने एक प्रसिद्ध रिटेलर का गिफ्ट कार्ड जीता है, लेकिन इसे प्राप्त करने से पहले आपको कुछ विवरण देना ज़रूरी होगा। यह आपकी व्यक्तिगत जानकारी प्राप्त करने की एक कोशिश होती है, जिसका उपयोग आपकी पहचान की चोरी करने या किसी अन्य घोटाले के लिए आपको लक्ष्य बनाने के लिए किया जा सकता है। ऐसे प्रस्ताव आपके डिवाइस में रैंसमवेयर डालने के लिए भी जाने जाते हैं (पृष्ठ 17 देखें)।

यात्रा इनाम के घोटालों में घोटालेबाज दावा करते हैं कि आपने एक निःशुल्क अवकाश या हवाई यात्रा जीती है। वास्तव में आपने होटल में ठहरने या हवाई जहाज के किराए के लिए वाउचर खरीदने का मौका जीता है। इन यात्रा वाउचरों में अक्सर छिपी हुई फीसें और शर्तें होती हैं, या फिर ये वाउचर नकली और बेकार हो सकते हैं। इसी तरह से घोटालेबाज आपको बेहतरीन छूट वाले अवकाश के ऐसे पैकेज प्रस्तुत कर सकते हैं, जो मौजूद ही नहीं होते हैं।

अपनी सुरक्षा करें

- याद रखें: यदि आपने किसी लॉटरी या प्रतियोगिता में हिस्सा ही नहीं लिया है, तो आप उसमें पैसा नहीं जीत सकते/सकती हैं।
- प्रतियोगिताओं और लॉटरियों में अपनी जीत की राशि पाने के लिए आपको शुल्क का भुगतान करने की आवश्यकता नहीं होती है - प्रस्ताव के शब्दों का अक्षरशः प्रयोग करके ऑनलाइन सर्च करें। इससे इसके घोटाले होने की पुष्टि में मदद मिल सकती है।
- '19' से शुरू होने वाले फोन नंबर पर कॉल करने या टेक्स्ट मैसेज भेजने से पहले दो बार सोचें – इनके लिए ऊँची दरों पर पर शुल्क लागू होता है।

ऑनलाइन खरीदारी, विज्ञापन और नीलामी के घोटाले

घोटालेबाज ऑनलाइन शॉपिंग की आसानी को भी बहुत पसंद करते हैं।

घोटाला कैसे किया जाता है

उपभोक्ताओं और व्यवसायों द्वारा ऑनलाइन खरीदारी और बिक्री में वृद्धि हो रही है। दुर्भाग्य से घोटालेबाज अपने शिकार के लिए ऑनलाइन खरीदारी करना पसंद करते हैं।

घोटालेबाज वास्तविक दिखने वाली **नकली रिटेलर वेबसाइटें** बना सकते हैं, जिनमें सोशल मीडिया पर फेसबुक जैसी वेबसाइटें भी शामिल हैं। किसी खुदरा वेबसाइट पर इस्तेमाल की जाने वाली भुगतान विधि से उस वेबसाइट के एक घोटाला होने की सबसे बड़ी चेतावनी मिल जाती है - यदि आपको वायर ट्रांसफर या अन्य असामान्य तरीकों से भुगतान करने के लिए कहा जाए, तो सावधान रहें।

ऑनलाइन नीलामी के घोटाले में घोटालेबाज यह दावा करता है कि आपने जिस वस्तु पर बोली लगाई है, उसे खरीदने के लिए आपको एक दूसरा मौका मिला है क्योंकि पहले विजेता ने उसे न खरीदने का निर्णय लिया है। घोटालेबाज आपको नीलामी वेबसाइट की सुरक्षित भुगतान सुविधा से बाहर भुगतान करने के लिए कहेगा; यदि आप ऐसा करते/करती हैं, तो आप अपना पैसा खो देंगे/देंगी तथा आपको वह वस्तु भी नहीं मिलेगी जिसके लिए आपने भुगतान किया था, और नीलामी वेबसाइट आपकी सहायता नहीं कर पाएगी।

ऑनलाइन विज्ञापनों के घोटाले सामान्यतः खरीदारों और विक्रेताओं, दोनों को निशाना बनाते हैं। खरीदारों को ऐसे घोटालेबाजों के प्रति सचेत रहना चाहिए जो वैध विज्ञापन वेबसाइटों पर नकली विज्ञापन पोस्ट करते हैं। ये विज्ञापन किराए की संपत्तियों से लेकर पालतू जानवरों, इस्तेमाल की गई कारों या कैमरों जैसी किसी

भी वस्तु के लिए हो सकते हैं, और अक्सर इनकी कीमत काफी कम होगी। यदि आप इस वस्तु में अपनी रुचि प्रदर्शित करते/करती हैं, तो घोटालेबाज यह दावा कर सकता है कि वे यात्रा कर रहे हैं या विदेश चले गए हैं और आपसे भुगतान प्राप्त करने के बाद एक एजेंट आपको वह वस्तु भेजेगा। भुगतान करने के बाद आपको वस्तु प्राप्त नहीं होगी या आप विक्रेता से संपर्क नहीं कर पाएँगे/पाएँगी।

विक्रेताओं को शिकार बनाने के लिए घोटालेबाज एक उदार प्रस्ताव के साथ आपके विज्ञापन का उत्तर देगा। यदि आप इस प्रस्ताव को स्वीकार करते/करती हैं, तो घोटालेबाज चेक या मनी ऑर्डर से आपको भुगतान भेजेगा। परंतु आपको प्राप्त होने वाला चेक या मनी ऑर्डर तय राशि से अधिक होता है। इस **अतिरिक्त भुगतान के घोटाले** में 'खरीदार' आपको बता सकता है कि उससे गलती हो गई थी और आपको मनी ट्रांसफर के माध्यम से अतिरिक्त पैसा वापिस भेजने के लिए कहेगा। घोटालेबाज यह उम्मीद करता है कि उसके चेक के बाउंस होने या मनी ऑर्डर के नकली होने का पता चलने से पहले आप उसे पैसे ट्रांसफर कर देंगे/देंगी। आप अपने पैसे खो देंगे/देंगी, और यदि आपने बेची गई वस्तु भेज दी हो तो आप उसे भी खो देंगे/देंगी।

अपनी सुरक्षा करें

- यह पता लगाएँ कि आप किसके साथ काम कर रहे/रही हैं। यदि वह एक ऑस्ट्रेलियाई रिटेलर है, तो कुछ गड़बड़ होने पर आप समस्या को सुलझाने के लिए बेहतर स्थिति में होंगे/होंगी।
- इस बात की जाँच करें कि क्या वह एक प्रतिष्ठित विक्रेता है, क्या उसकी कोई वापसी-नीति है और क्या वह शिकायतों का समाधान करता है।
- मनी ऑर्डर, वायर ट्रांसफर, अंतर्राष्ट्रीय फंड्स ट्रांसफर, प्रि-लोडेड कार्ड या इलेक्ट्रॉनिक करेंसी के माध्यम से तुरंत भुगतान करने के लिए कहने वाली किसी भी व्यवस्था से वर्जन करें। इस तरह से भेजे गए पैसों को वापस प्राप्त करना बहुत ही कठिन होता है। यदि आप किसी व्यक्ति से परिचित नहीं हैं या उसपर विश्वास नहीं करते/करती हैं, तो कभी भी उसे पैसे न भेजें या अपने क्रेडिट कार्ड अथवा ऑनलाइन खाते का विवरण न दें, और ईमेल से तो ऐसा कभी भी न करें।
- केवल वेबसाइट की सुरक्षित् भुगतान पद्धति के माध्यम से ही भुगतान करें – 'https' से शुरू होने वाले और बंद ताले के चिह्न वाले वेब पते के लिए देखें।
- आपके द्वारा सहमत धनराशि से अधिक पैसे का भुगतान करने वाले चेक या मनी ऑर्डर को कभी भी स्वीकार न करें, या किसी अन्य व्यक्ति के लिए पैसे अग्रेषित न करें।

कंप्यूटरों और मोबाइल उपकरणों को निशाना बनाने वाले घोटाले

याद रखें: इंटरनेट से जुड़ने वाली सभी उपकरणों की सुरक्षा के लिए खतरा मौजूद होता है।

घोटाला कैसे किया जाता है

रिमोट एक्सेस घोटालेबाज आपको फ़ोन पर कॉल करके इस बात का दावा करते हैं कि आपका कंप्यूटर वायरस से संक्रमित हो गया है। यदि आप उनके निर्देशों का पालन करते/करती हैं, तो वे आपके कंप्यूटर को एक्सेस और नियंत्रित करने में सक्षम हो जाएँगे जिससे वे आपकी जानकारी की चोरी कर सकते हैं या मैलवेयर इंस्टॉल कर सकते हैं। वे आपको 'एंटी-वायरस' सॉफ्टवेयर खरीदने के लिए प्रभावित करने की कोशिश भी कर सकते हैं, जो सामान्यतः बहुत महँगा होता है फिर या इंटरनेट पर निःशुल्क उपलब्ध हो सकता है।

मैलवेयर शब्द का प्रयोग वायरसों, स्पाईवेयर, रैंसमवेयर, ट्रोजन हॉर्सेज और कीस्ट्रोक लॉगर्स जैसे हानिकारक सॉफ्टवेयर के लिए किया जाता है, जिन्हें आपके कंप्यूटर या अन्य उपकरणों में इंस्टॉल किया जा सकता है।

कीस्ट्रोक लॉगर्स और स्पाइवेयर के माध्यम से घोटालेबाज आपके द्वारा अपने कीबोर्ड पर टाइप किए जाने वाले अक्षरों/अंकों/चिह्नों को रिकॉर्ड कर सकते हैं, जिससे वे आपके पासवर्डों और बैंक विवरण का पता लगा सकते हैं या आपकी व्यक्तिगत जानकारी तक पहुँच प्राप्त करके उसे कहीं भी भेज सकते हैं। एक बार स्थापित कर देने पर घोटालेबाज आपके ईमेल और सोशल मीडिया एकाउंट को नियंत्रित कर सकते हैं और आपके उपकरण पर उपलब्ध सभी जानकारी हासिल कर सकते हैं, जिसमें आपके पासवर्ड भी शामिल हैं। वे आपके खातों का उपयोग आपके मित्रों और परिजनों को और भी अधिक घोटाले भेजने के लिए कर सकते हैं।

रैंसमवेयर एक अन्य प्रकार का मैलवेयर होता है जो आपके उपकरण को एन्क्रिप्ट या लॉक करके आपको तब तक उपकरण का प्रयोग करने से रोक देता है, जब तक आप उसे अनलॉक करने के लिए भुगतान न करें। भुगतान करने के बाद भी इस बात की कोई गारंटी नहीं होती है कि उपकरण अनलॉक हो जाएगा या छिपे हुए वायरसों से मुक्त हो जाएगा, जो आपके नेटवर्क पर अन्य कंप्यूटरों या उपकरणों में फैलकर उन्हें भी संक्रमित कर सकते हैं।

मैलवेयर सामान्यतः ईमेल से वितरित किया जाता है और ऐसा प्रतीत हो सकता है कि यह वैध स्रोतों से आया है, जैसे आपका कोई सेवा प्रदाता, सरकारी एजेंसी या यहाँ तक कि जुर्माना जारी करने वाली पुलिस भी। ऐसे किसी लिंक पर क्लिक न करें या एटैचमेंट न खोलें, जिसके बारे में आप पूरी तरह से सुनिश्चित नहीं हैं। आप अनजाने में हानिकारक सॉफ्टवेयर डाउनलोड कर सकते/सकती हैं। ऐसे घोटाले व्यक्तियों और व्यवसायों, दोनों को निशाना बनाते हैं।

अपनी सुरक्षा करें

- संगीत, खेलों, फिल्मों और वयस्क साइटों को एक्सेस करने वाले निःशुल्क डाउनलोडों से सावधान रहें। वे आपकी जानकारी के बिना हानिकारक प्रोग्राम इंस्टॉल कर सकते हैं।
- अपने कार्यालय के नेटवर्कों, कंप्यूटरों और मोबाइल उपकरणों को सुरक्षित रखें। अपने सुरक्षा सॉफ्टवेयर को अपडेट करें, पासवर्ड बदलें और नियमित रूप से अपने डेटा का बैकअप लें। अपने बैकअप को ऑफसाइट और ऑफलाइन स्टोर करें। वेबसाइट www.staysmartonline.gov.au पर आपको समझाया गया है कि आप अपने डेटा का बैकअप और अपने मोबाइल उपकरणों की सुरक्षा कैसे कर सकते/सकती हैं।
- अजनबियों से प्राप्त हुए एटैचमेंट न खोलें या ईमेल अथवा सोशल मीडिया संदेशों में दिए गए लिंक पर क्लिक न करें - बस डिलीट दबाएँ।

पहचान की चोरी

सभी घोटालों में पहचान की चोरी किए जाने की संभावना होती है। स्वयं को घोटालों से सुरक्षित रखने का अर्थ अपनी निजी जानकारी को सुरक्षित रखना भी होता है।

प्रत्येक घोटाले में पहचान की चोरी किए जाने का खतरा होता है

अधिकाँश लोग घोटालों को आपसे पैसे ऐंठने के प्रयासों के साथ जोड़ते हैं। परंतु घोटालेबाजों के लिए आपकी जानकारी भी मूल्यवान होती है। घोटालेबाज आपके क्रेडिट कार्ड से अनधिकृत खरीदारी करने अथवा बैंक या टेलीफोन खाते खोलने के लिए आपकी पहचान का प्रयोग करने जैसी धोखाधड़ी की गतिविधियों के लिए आपकी व्यक्तिगत जानकारी की चोरी करते हैं। वे आपके नाम से ऋण ले सकते हैं या कोई गैर-कानूनी व्यवसाय चालू कर सकते हैं। वे आपकी जानकारी को आगे के गैर-कानूनी प्रयोग के लिए दूसरे घोटालेबाजों को बेच भी सकते हैं।

अपनी पहचान की चोरी होना वित्तीय और भावनात्मक रूप से भयानक हो सकता है। अपनी पहचान को फिर से प्राप्त करने में महीनों लग सकते हैं और चोरी का प्रभाव वर्षों तक बना रह सकता है।

फिशिंग – बैंक, फोन या इंटरनेट सेवा प्रदाता जैसे किसी वैध व्यवसाय की ओर से होने का दिखावा करके घोटालेबाज आपके साथ अनपेक्षित रूप से ईमेल, फोन, फेसबुक या टेक्स्ट संदेश के माध्यम से संपर्क करता है। वह आपको तकनीकी गलती के कारण सेवार्थी के रिकॉर्ड को सत्यापित करने के लिए व्यवसाय की वेबसाइट के एक नकली सँस्करण पर जाने के लिए निर्देश देता है। वह किसी बेशकीमती वस्तु के खुदरा विक्रेता की नकल करते हुए इस बात का दावा कर सकता है कि कोई दूसरा व्यक्ति आपके क्रेडिट कार्ड का उपयोग करने की कोशिश कर रहा है। वह आपको अपनी बैंक से संपर्क करने की सलाह देता है, लेकिन अपनी ओर से फोन लाइन को काटता नहीं हैं और लाइन पर बना रहता है। जब आप बैंक को कॉल करने का प्रयास करते/करती हैं, तो आप अनजाने में अभी भी उसी घोटालेबाज के साथ बात कर रहे होते/रही होती हैं क्योंकि वह वास्तविक कॉल का अनुकरण करता है, बैंककर्मी होने की नकल करता

है और आपके खाते के बारे में व सुरक्षा विवरण पूछता है। चाहे जो भी हो, घोटालेबाज आपके द्वारा दी गई जानकारी प्राप्त कर लेता है और फिर वह आपके खाते को एक्सेस करने के लिए उसका उपयोग करता है।

नकली सर्वेक्षण - घोटालेबाज ऑनलाइन सर्वेक्षों पूरा करने के बदले में जाने-माने खुदरा विक्रेताओं को गिफ्ट कार्डों या इनामों का प्रस्ताव देते हैं। सर्वेक्षण में आपको अपनी महत्वपूर्ण पहचान या बैंकिंग विवरण प्रकट करने के साकोथ-साथ कई प्रश्नों के उत्तर देने की आवश्यकता होती है।

किसी अन्य घोटाले के हिस्से के रूप में - घोटालेबाज अक्सर अन्य घोटालों में व्यक्तिगत जानकारी माँगते हैं। लॉटरी के घोटाले में घोटालेबाज अक्सर ड्राइवर्स लाइसेंस या पासपोर्ट के विवरण पूछते हैं, ताकि वे 'इनाम की धनराशि भेजने से पहले आपकी पहचान प्रमाणित कर सकें'। डेटिंग और प्रेम के नाटक वाले घोटालों में वे आपसे 'ऑस्ट्रेलिया आने के लिए अपने वीज़ा आवेदन को प्रायोजित करने के लिए' जानकारी पूछ सकते हैं।

याद रखें: घोटालेबाज को व्यक्तिगत जानकारी उपलब्ध कराना पैसे देने के समान ही हानिकारक हो सकता है। अपने व्यक्तिगत विवरण बस अपने पास रखें और उन्हें सुरक्षित रखें।

अपनी सुरक्षा करें

- **आप ऑनलाइन वातावरण में जो कहते/कहती हैं और करते/करती हैं, उसके बारे में दो बार सोचें**
  सोशल मीडिया, ब्लॉगों और अन्य ऑनलाइन फोरमों में अपने बारे में ऑनलाइन जानकारी साझा करते समय सावधानी बरतें। सर्वेक्षणों को पूरा करने, प्रतियोगिताओं में प्रवेश करने, लिंक या एटैचमेंट पर क्लिक करने, या यहाँ तक कि ऑनलाइन 'मित्र बनने', 'लाइक करने' या 'शेयर' करने से पहले ठहरें और सोचें।
- **आपसे विवरण या पैसे माँगे जाने के प्रति सचेत रहें**
  घोटालेबाज जानी-मानी कंपनियों या सरकारी विभागों के नाम का इस्तेमाल करके आपके विवरण हासिल करने के लिए आपको धोखा देने की कोशिश करेंगे।
  यदि आपको लगता है कि यह एक घोटाला है, तो उत्तर न दें। संगठन के संपर्क विवरण की जाँच करने के लिए फोन बुक का उपयोग करें या ऑनलाइन सर्च करें। मूल निवेदन में दिए गए संपर्क विवरण का उपयोग कभी न करें।

यदि आपने घोटालेबाजों को अपनी व्यक्तिगत पहचान की जानकारी दे दी है, तो 1300 432 273 पर IDCARE से संपर्क करें।

नौकरी और रोजगार के घोटाले

अच्छी आय की गारंटी? इसकी संभावना नहीं होती है!

घोटाला कैसे किया जाता है

नौकरी और रोजगार के घोटालों में घर से काम करने या एक 'व्यावसायिक अवसर' स्थापित करने और इसमें निवेश करने के प्रस्ताव शामिल होते हैं। घोटालेबाज अग्रिम भुगतान करने के बाद नौकरी, ऊँची आय या बड़े निवेश का वादा करते हैं। ये भुगतान 'व्यवसाय योजना', प्रशिक्षण कोर्स, सॉफ्टवेयर, वर्दियों, सुरक्षा मंजूरी, करों या शुल्कों के लिए हो सकते हैं। यदि आप शुल्क का भुगतान करते/करती हैं, तो हो सकता है कि आपको कुछ भी प्राप्त न हो या वह सेवा या वस्तु प्राप्त न हो जिसकी आपको आशा थी या जिसे उपलब्ध कराए जाने का वादा किया गया था।

नौकरी के कुछ प्रस्ताव **अवैध मनी लॉन्डरिंग** गतिविधियों को छिपाने के प्रयास हो सकते हैं, जिनमें आपको एक 'खाता प्रबंधक' या 'व्यक्तिगत सहायक' के रूप में कार्य करने के लिए कहा जाता है, आपको कमीशन देकर आपके बैंक खाते में भुगतान किया जाता है, और फिर आपको किसी विदेशी कंपनी को ये पैसे अग्रेषित करने के कहा जाता है। नौकरी के घोटालों को अक्सर स्पैम ईमेलों या जाने-माने अखबारों में विज्ञापनों और नौकरी खोजक वेबसाइटों - यहाँ तक कि सरकारी नौकरी खोजक वेबसाइटों के माध्यम से भी प्रचारित किया जाता है।

नौकरी के इन घोटालों में एक बड़ा-भारी खतरा यह रहता है कि आपसे टैक्स फाइल नंबर और पासपोर्ट या ड्राइवर्स लाइसेंस की प्रतियों समेत बहुत से अन्य व्यक्तिगत विवरण की माँग की जा सकती है, जो आपको नहीं देना चाहिए। बाद में इस जानकारी का इस्तेमाल पहचान की चोरी करने के लिए किया जा सकता है।

अपनी सुरक्षा करें

- आय की गारंटी देने का दावा करने वाले या अग्रिम भुगतान करने की आवश्यकता वाले प्रस्तावों या योजनाओं के प्रति सावधान रहें।
- कभी भी किसी अन्य व्यक्ति की ओर से पैसे हस्ताँतरित करने के लिए स्वीकृति न दें - यह मनी लॉन्डरिंग होती है और यह गैर-कानूनी है।
- नौकरी के लिए आवेदन करते समय अपना टैक्स फाइल नंबर, ड्राइवर्स लाइसेंस या पासपोर्ट का विवरण न दें। आपको यह जानकारी देने की आवश्यकता हो सकती है, लेकिन केवल तभी जब आपने काम शुरू कर दिया हो।

मनी लॉन्डरिंग एक अपराध है: किसी अजनबी के लिए पैसे हस्ताँतरित करने के लिए स्वीकृति न दें।

परोपकारी अनुदान और चिकित्सा के घोटाले

घोटालेबाज निर्दयी होते हैं और आपकी अत्यधिक आवश्यकता के समय आपको निशाना बना सकते हैं।

घोटाला कैसे किया जाता है

घोटालेबाज किसी कल्याकारी कारण या स्वास्थ्य समस्या का हल ढूँढने के लिए चंदा देने के इच्छुक लोगों से लाभ उठाते हैं ।

परोपकारी अनुदानों के घोटालों में घोटालेबाज किसी वैध अथवा काल्पनिक रूप से निर्मित जनहित या परोपकारी कार्य करने का ढोंग करके पैसे हासिल करते हैं। घोटालेबाज अक्सर समाचार में दिखाई गई हाल की किसी प्राकृतिक आपदा या संकट से लाभ उठाते हैं।

ऐसे घोटाले वैध परोपकारी कार्यों को मिल सकने वाले अत्यधिक आवश्यक चंदे छीन लेते हैं। परोपकारी सँस्थाओं को सरकार के साथ पँजीकृत होना चाहिए - उनके पंजीकरण की पहले जाँच करके आत्मविश्वास के साथ चंदा दें।

चमत्कारी उपचार वाले घोटालों में वैध वैकल्पिक औषधियाँ प्रतीत होने वाले कई प्रकार के उत्पाद और सेवाएँ उपलब्ध कराई जाती हैं, जो सामान्यतः साधारण चिकित्सीय रोगों के लिए जल्दी और प्रभावी उपचार का वादा करती हैं। 'ठीक' कर दिए गए रोगियों के झूठे प्रमाणों का प्रयोग करके इन उपचारों को अक्सर प्रचारित किया जाता है।

वजन घटाने के घोटाले बहुत कम या बिना किसी प्रयास के नाटकीय रूप से वजन घटाने का वादा करते हैं। इस प्रकार के घोटाले में असाधारण या प्रतिबंधित आहार, नई व्यायाम पद्धति, 'वसा-घटाने' वाला उपकरण, नवाचारी गोलियाँ और क्रीमें शामिल हो सकती हैं। लगातार रूप से आपूर्तियाँ प्राप्त करने के लिए आपको काफी बड़ा अग्रिम भुगतान करने या एक लंबे समय तक चलने वाले अनुबंध में प्रवेश करने की आवश्यकता हो सकती है।

नकली ऑनलाइन फार्मेसियाँ बहुत सस्ते दामों पर नकली दवाइयों और औषधियों का प्रस्ताव देती हैं, और वे कभी-कभी डॉक्टर के नुस्खे के बिना भी इन्हें उपलब्ध कराती हैं। इन दवाइयों में सक्रिय तत्व संभवतः सीमित मात्रा में या बिल्कुल भी नहीं होते हैं, जिसके कारण इनसे उपयोगकर्ताओं के लिए घातक परिणाम हो सकते हैं।

अपनी सुरक्षा करें

- यदि आपके पास सड़क पर कोई चंदा माँगने वाला व्यक्ति आता है, तो उसे अपना पहचान-पत्र दिखाने के लिए कहें। यदि आपको संदेह हो कि वह कौन है, तो उसे पैसे न दें।
- ऑस्ट्रेलियाई अनुदान और गैर-लाभ आयोग (Australian Charities and Not-for-profits Commission) के पास पँजीकृत सँस्थाओं की सूची की जाँच करें।
- यदि आप दवाइयों, संपूरक आहारों या अन्य उपचारों के बारे में 'चमत्कारी' या 'तत्काल-उपचार' के दावों के बारे में विचार कर रहे/रही हैं, तो अपने स्वास्थ्य देखभाल व्यावसायिक से परामर्श करें।
- स्वयं से पूछें: यदि यह वास्तव में एक चमत्कारी उपचार है, तो आपके स्वास्थ्य देखभाल व्यावसायिक ने आपको इसके बारे में क्यों नहीं बताया?

व्यवसायों को निशाना बनाने वाले घोटाले

घोटालेबाज व्यवसायों की व्यस्त प्रकृति का लाभ उठाकर उन्हें धोखा देते हैं।

घोटाला कैसे किया जाता है

व्यवसायों को निशाना बनाने वाले घोटाले सभी प्रारूपों में आते हैं और संभवतः वित्तीय वर्ष के अंत जैसे सबसे अधिक व्यस्त समय में उन्हें निशाना बनाते हैं।

गलत बिलिंग का घोटाला व्यवसायों को धोखा देने के लिए घोटालेबाजों की सबसे सामान्य चाल है। घोटालेबाज अवांछित या अनधिकृत लिस्टिंग्स, विज्ञापनों, उत्पादों या सेवाओं के लिए नकली बिल जारी करते हैं। एक जाना-माना उदाहरण **व्यवसाय निर्देशिका का घोटाला** है, जिसमें आपको एक तथाकथित रूप से प्रसिद्ध निर्देशिका में लिस्टिंग करने के लिए बिल प्राप्त होता है। घोटालेबाज इस प्रस्ताव को बकाया इनवॉइस या निःशुल्क लिस्टिंग के रूप में आपके सामने रखकर साइन अप करवाने के लिए धोखा देते हैं, जबकि उसमें महीन प्रिंट में छिपा हुए एक सदस्यता समझौता होता है।

डोमेन नेम का घोटाला घोटालेबाजों द्वारा की जाने वाली एक और चाल है, जिसमें आपको अपने डोमेन नेम के बिल्कुल समान एक अन्य अनचाहे इंटरनेट डोमेन के लिए पँजीकरण कराने के लिए धोखा दिया जाता है। आपको अपने वास्तविक डोमेन के नाम पर एक नकली नवीकरण नोटिस भी मिल सकता है और आप अनजाने में इसका भुगतान कर सकते/सकती हैं।

कार्यालय आपूर्ति के घोटाले में आपको ऐसे उत्पाद प्राप्त होते हैं और उनके लिए आपसे शुल्क लिया जाता है, जिनका आपने कभी आदेश ही नहीं दिया था। इन घोटालों में अक्सर स्टेशनरी और सफाई के साजो-सामान की आपूर्तियों जैसे उत्पाद या सेवाएँ शामिल होती हैं जिनके लिए आप नियमित रूप से आदेश दिया

करते/करती हैं। घोटालेबाज सामान्यतः आपके व्यवसाय को कॉल करके बताते हैं कि सेवा या उत्पाद के लिए पहले ही आदेश दिया जा चुका है।

भुगतान पुनर्निर्देशन के घोटालों में घोटालेबाज आपके कंप्यूटर सिस्टम को हैक करके प्राप्त की गई जानकारी का उपयोग करता है। फिर वह आपका एक नियमित आपूर्तिकर्ता होने का दिखावा करके आपको बताता है कि उनका बैंकिंग विवरण बदल गया है। वह आपको बता सकता है कि उन्होंने हाल ही में अपनी बैंक बदल दी है, और वह आपको विश्वास दिलाने के लिए कॉपी किए गए लेटरहेड और ब्रांडिंग का उपयोग कर सकता है। वह आपको एक नई बैंक खाता संख्या देकर भविष्य में सभी भुगतानों को नए खाते में भेजने के लिए कहेगा। इस घोटाले का पता अक्सर तब चलता है, जब आपके नियमित आपूर्तिकर्ता आपसे पूछते हैं कि उन्हें भुगतान क्यों नहीं किया गया है।

रैंसमवेयर किसी भी व्यवसाय के लिए बहुत हानिकारक हो सकता है। सबसे अच्छी सुरक्षा के लिए आपको अपने डेटा को नियमित रूप से बैकअप करना चाहिए और अपने बैकअप को ऑफसाइट और ऑफलाइन स्टोर करना चाहिए। पृष्ठ 17 पर और अधिक विवरण देखें।

अपनी सुरक्षा करें

- प्रस्तावों या सौदों के लिए तुरंत अपनी स्वीकृति न दें - प्रस्ताव को हमेशा लिखित में दिए जाने के लिए कहें और सौदे में पैसे, समय या लंबी अवधि की प्रतिबद्धता शामिल होने की स्थिति में स्वतंत्र सलाह लें।
- अपने व्यवसाय का बैंकिंग, वित्तीय और लेखा-जोखा विवरण कभी किसी ऐसे व्यक्ति को न दें, जो आपसे अनपेक्षित रूप से संपर्क करता है और आप उससे परिचित नहीं हैं तथा उसपर विश्वास नहीं करते/करती हैं।
- प्रभावी प्रबंधन प्रक्रियाएँ घोटालों को रोकने की दिशा में काफी दूर का रास्ता तय कर सकती हैं - खातों और चालानों को सत्यापित करने और भुगतान करने के लिए स्पष्ट रूप से परिभाषित प्रक्रियाएँ बनाएँ और बैंकिंग विवरण बदलने के निवेदनों को बहुत ध्यान से देखें।
- अपने कर्मचारियों को घोटालों की पहचान करने के लिए प्रशिक्षित करें।
- अपने व्यवसाय के डेटा को ऑफसाइट और ऑफलाइन बैकअप करें।
- भुगतान विवरण में परिवर्तनों का निवेदन करने वाली ईमेलों के प्रति सचेत रहें। हमेशा संबंधित व्यवसाय या व्यक्ति-विशेष के साथ भुगतान विवरण में परिवर्तनों की पुष्टि करें।

घोटाले कैसे काम करते हैं - घोटालों की संरचना

अधिकाँश घोटाले एक ही पैटर्न के अनुरूप होते हैं और एक बार जब आप इसे समझ लें, तो घोटालेबाज की चालों को आसानी से पहचाना जा सकता है।

इस पुस्तक में दिए गए अलग-अलग तरह के घोटालों पर ध्यान देने से आपको जल्दी ही यह दिखाई देगा कि अधिकाँश घोटालों के तीन चरण होते हैं: (1) संपर्क; (2) संचार; और (3) भुगतान।

घोटालों के मूल हिस्सों को समझने से आपको वर्तमान के घोटालों से सुरक्षित रहने और भविष्य में उभरने वाले नए घोटालों के प्रति सचेत रहने में सहायता मिलेगी।

1. तरीका: संपर्क करने का तरीका

जब घोटालेबाज आपसे संपर्क करते हैं, तो इसमें हमेशा एक कहानी शामिल होगी जिसका निर्माण आपको एक झूठ पर विश्वास करने के लिए किया गया होगा। घोटालेबाज एक सरकारी अधिकारी, विशेषज्ञ निवेशक, लॉटरी अधिकारी या यहाँ तक कि एक प्रेमपूर्ण प्रशंसक होने का दिखावा भी करेगा, जो वह वास्तव में है ही नहीं।

इस झूठ को आप तक पहुँचाने के लिए घोटालेबाज कई प्रकार की संचार विधियों का प्रयोग करेंगे।

ऑनलाइन

घोटालेबाज़ इंटरनेट के गुमनाम वातावरण में घात लगाकर ढूँढते रहते हैं।

घोटाले शुरू करने की एक पसंदीदा विधि **ईमेल** है, जो बड़े पैमाने पर संवाद करने का सस्ता और सरल तरीका प्रदान करती है। आपकी व्यक्तिगत जानकारी के लिए 'फिश' करने वाली फिशिंग ईमेल सबसे सामान्य प्रकार की ईमेल घोटाला होती है।

सोशल नेटवर्किंग प्लेटफॉर्म, डेटिंग साइटें और ऑनलाइन फोरम
घोटालेबाजों को आपसे 'दोस्ती करने' और आपके व्यक्तिगत विवरण का उपयोग करने के लिए आपके निजी जीवन में प्रवेश करने की अनुमति देते हैं, जिनका उपयोग बाद में आपके या आपके परिवार और दोस्तों के विरुद्ध किया जा सकता है।

घोटालेबाजों द्वारा ऑनलाइन खरीदारी, विज्ञापनों और नीलामी साइटों का उपयोग खरीदारों और विक्रेताओं को निशाना बनाने के लिए किया जाता है, जिसमें शुरुआती संपर्क अक्सर जानी-मानी और विश्वसनीय साइटों या वास्तविक साइटों की तरह दिखने वाली जाली वेबसाइटों के माध्यम से किया जाता है। सुरक्षित भुगतान विकल्पों के लिए देखें और वायरलेस ट्रांसफर, बिटकॉइन या प्रिलोडेड मनी कार्ड जैसी असामान्य भुगतान विधियों के प्रति सचेत रहें। क्रेडिट कार्ड सामान्यतः कुछ हद तक सुरक्षा प्रदान करते हैं।

फोन से

घोटालेबाज कॉल करते हैं और एसएमएस भी भेजते हैं।

कई प्रकार के घोटालों के लिए घोटालेबाज घरों और व्यवसायों में **फोन कॉल** करते हैं, जिसमें धमकियाँ देने वाले कर से संबंधित घोटालों से लेकर इनामों के प्रस्ताव और कंप्यूटर वायरसों के बारे में 'सहायता' शामिल होती है। वॉइस ओवर इंटरनेट प्रोटोकॉल (वीओआइपी) [Voice Over Internet Protocol (VOIP)] के माध्यम से सस्ती फोन कॉलों की उपलब्धता का अर्थ है कि कॉल सेंटर स्थानीय नंबरों जैसे दिखने वाले टेलीफोन नंबरों के साथ विदेश में रहते हुए काम कर सकते हैं। टेलीफोन कॉल करने वाले व्यक्ति की पहचान आसानी से छिपाई जा सकती है और घोटालेबाज इसके जैसी अनेकों चालों का उपयोग करके आपको यह विश्वास दिलाने की कोशिश करते हैं कि वे कोई अन्य व्यक्ति हैं।

घोटालेबाजों द्वारा **एसएमएस टेक्स्ट संदेशों** का प्रयोग प्रतियोगिता या इनाम के घोटालों समेत कई अन्य तरह के घोटालों के लिए किया जाता है। यदि आप उत्तर देते/देती हैं, तो आपसे ऊँची दरों पर शुल्क लिया जा सकता है या आपको स्वतः किसी सदस्यता सेवा में शामिल किया जा सकता है। जब तक आपको यह न पता हो कि ये टेक्स्ट संदेश किसने भेजे हैं, तब तक इनका उत्तर न देना या लिंक पर क्लिक न करना अधिक सुरक्षित रहता है। इनमें तस्वीरों, गानों, गेम्स या ऐप्स के रूप में हानिकारक एटैचमेंट भी शामिल हो सकते हैं या सॉफ्टवेयर के लिए लिंक दिए गए हो सकते हैं।

आपके घर के द्वार पर

सावधान रहें - कुछ घोटालेबाज सीधे आपके घर के द्वार पर आकर आपको धोखा देने का प्रयास करेंगे।

डोर-टु-डोर घोटालों में सामान्य रूप से घोटालेबाज ऐसे सामान या सेवाओं का प्रचार करते हैं, जो आपको कभी भी प्राप्त नहीं होते हैं या बहुत खराब गुणवत्ता के होते हैं। आपको ऐसे काम के लिए बिल भी मिल सकता है, जो आप नहीं करवाना चाहते थे/चाहती थीं या जिसके लिए आपने कभी स्वीकृति दी ही नहीं थी। धोखेबाज कारीगरों द्वारा सामान्य रूप से किए जाने वाले एक डोर-टु-डोर घोटाले में कारीगर एक स्थान से दूसरे स्थान पर जाते रहते हैं और घर की घटिया मरम्मतें करते हैं या बस आपका पैसा लेकर भाग जाते हैं।

वैध व्यवसाय डोर-टु-डोर बिक्री कर सकते हैं लेकिन उन्हें अपनी और अपनी कंपनी की पहचान स्पष्ट रूप से प्रकट करनी चाहिए और अन्य नियमों का पालन करना चाहिए। डोर-टु-डोर बिक्री प्रथाओं के संबंध में आपके पास विशिष्ट अधिकार होते हैं, जिनमें आपके पास अपना मन बदलने का अवसर मिलना भी शामिल है – वेबसाइट www.accc.gov.au/doortodoor पर और अधिक जानकारी प्राप्त करें।

घोटालेबाज चंदा इकट्ठा करने के लिए खुद को **परोपकारी सँस्थाओं के नकली कर्मियों** के रूप में भी प्रस्तुत कर सकते हैं। वे बाढ़ और बुशफायरों जैसी हाल की घटनाओं का लाभ उठाएँगे। चंदा देने से पहले उनसे पहचान-पत्र माँगें और उनकी आधिकारिक रसीद बुक देखें।

बल्क मेलिंग का प्रयोग अभी भी **लॉटरी और स्वीपस्टेक घोटालों के, निवेश के अवसरों, नाइजीरियाई घोटालों** और **जाली विरासत-पत्र** भेजने के लिए किया जाता है। आकर्षक दिखने वाला ब्रोशर किसी प्रस्ताव की वैधता की गारंटी नहीं होता है।

चाहे घोटालेबाज कोई भी संपर्क विधि अपनाए, उसकी कहानी हमेशा आपको चारे का लालच देती है और यदि आप इसके झाँसे में आ जाते/जाती हैं, तो वह आपको अगले चरण में ले जाने की कोशिश करेगा।

2. संचार और प्रोत्साहन

यदि आप घोटालेबाजों को आपसे बात करने का अवसर देते/देती हैं, तो वे आपके पैसे लेने के लिए अपने घोटालेबाज टूलबॉक्स में मौजूद दाँव-पेचों का प्रयोग करना शुरू कर देंगे।

घोटालेबाजों के उपकरणों में निम्नलिखित शामिल हो सकते हैं:

- घोटालेबाज जो चाहते हैं, उसे पाने के लिए विस्तृत और **भरोसेमंद कहानियों** गढ़ते हैं।
- वे आपके **व्यक्तिगत विवरण** का प्रयोग करके आपको यह विश्वास दिलाने की कोशिश करते हैं कि आपने पहले उनके साथ व्यवहार किया है और उनका घोटाला वैध है।
- घोटालेबाज़ विश्वास का निर्माण करने और स्वयं को आपके दोस्त, सहभागी या प्रेम-अभिरुचि के रूप में प्रदर्शित करने के लिए आपके साथ **नियमित रूप से संपर्क** कर सकते हैं।
- वे जीत के रोमाँच, आजीवन प्रेम के वादे, दुर्भाग्यपूर्ण घटना में सहानुभूति, सहायता न करने की ग्लानि या गिरफ्तारी और जुर्माने की चिंता और भय का प्रयोग करके **आपकी भावनाओं के साथ खिलवाड़** करते हैं।
- घोटालेबाज **तात्कालिकता की भावना** पैदा करना बहुत पसंद करते हैं, इसलिए आपके पास स्थिति के बारे में अच्छी तरह से सोचने का समय नहीं होता है और आप तर्क-वितर्क के बजाए भावुक होकर प्रतिक्रिया करते/करती हैं।
- इसी प्रकार वे **बिक्री के लिए अत्यधिक दबाव डालने वाली चालबाज़ी** का प्रयोग करते हुए कहते हैं कि यह प्रस्ताव सीमित है, मूल्य में वृद्धि होने वाली है, या बाज़ार आगे बढ़ने वाला है और अवसर खो जाएगा।
- घोटाले में एक वास्तविक व्यवसाय जैसा प्रतीत होने के सभी संकेत हो सकते हैं, जिनमें उद्योग का तकनीकी शब्दजाल प्रयुक्त करने वाले **आकर्षक ब्रोशर**, कार्यालय-कक्ष, कॉल सेंटर और पेशेवर वेबसाइटें शामिल हैं।
- इंटरनेट और सशक्त सॉफ्टवेयर की उपलब्धता के कारण घोटालेबाज आसानी से जाली और **आधिकारिक दिखने वाले दस्तावेज़** बना सकते हैं। सरकार द्वारा स्वीकृत प्रतीत होने वाला या कानूनी शब्दजाल से भरा दस्तावेज़ घोटाले को आधिकारिक प्रभाव दे सकता है।

घोटालेबाज के उपकरण इस उद्देश्य से बनाए गए होते हैं कि आप अपनी प्रतिरक्षा कम कर दें, उसकी कहानी पर विश्वास करें और जल्दी या तर्कहीन तरीके से काम करें तथा अंतिम चरण, यानि पैसे भेजने, की ओर आगे बढ़ें।

3. पैसे भेजना

कभी-कभी आपके पास घोटाले की पहचान करने का सबसे बड़ा सुराग यह होगा कि घोटालेबाज आपको किस तरह से पैसे भेजने के लिए कहता है।

पैसों की माँग घोटाले के शुरू होने के कुछ ही मिनटों के अंदर या फिर महीनों तक सावधानीपूर्वक आपको तैयार किए जाने के बाद सामने आ सकती है। घोटालेबाजों की इस बारे में अपनी प्राथमिकताएँ होती हैं कि आप उन्हें अपना पैसा कैसे भेजते/भेजती हैं।

घोटालेबाजों को पैसे भेजने के लिए लक्षित व्यक्तियों को अपने सबसे नज़दीकी **धन प्रेषण स्थान** (डाक घर, वायर ट्रांसफर सेवा या यहाँ तक कि बैंक) के लिए निर्देशित करने के लिए जाना जाता है। इस दौरान उन्हें फोन पर बने रहने, विशेष निर्देश देने और इसमें सहायता के लिए टैक्सी भेजने के लिए भी जाना जाता है। घोटालेबाज किसी भी तरीके से पैसे स्वीकार करने के लिए तैयार रहते हैं, और इसमें **डायरेक्ट बैंक ट्रांसफर, प्रिलोडेड डेबिट कार्ड, गिफ्ट कार्ड, गूगल प्ले, स्टीम या आईट्यून कार्ड** अथवा **बिटकॉइन** जैसी आभासी मुद्रा भी शामिल हो सकती है। असाधारण तरीके से पैसे भेजने का कोई भी निवेदन इस बात का स्पष्ट संकेत होता है कि यह एक घोटाले का हिस्सा है।

क्रेडिट कार्ड सामान्यतः कुछ हद तक सुरक्षा प्रदान करते हैं और आपको सुरक्षित भुगतान विकल्पों के लिए खोज भी करनी चाहिए, जहाँ वेब पते में 'https' दिखाई दे और साइट पर बंद ताले का चिह्न हो।

ऐसे किसी व्यक्ति को पैसे न भेजें जिससे आपने केवल ऑनलाइन या फोन के माध्यम से मुलाकात की है – विशेषकर यदि वह विदेश में रहता हो।

इस बात से अवगत रहें कि घोटालेबाज गहनों या इलेक्ट्रॉनिक्स जैसी कीमती वस्तुओं और महंगे उपहारों के रूप में भुगतान करने के लिए भी कह सकते हैं। आपको केवल घोटालेबाज को पैसे भेजने के बारे में ही चिंता नहीं करनी चाहिए - यदि आप किसी अजनबी के लिए पैसे हस्ताँतरित करने में मदद करते/करती हैं, तो आप अनजाने में **अवैध मनी लॉन्डरिंग** गतिविधियों में शामिल हो सकते/सकती हैं।

अपनी सुरक्षा करने के लिए सुनहरे नियम

इस तथ्य के प्रति सचेत रहें कि घोटाले उपस्थित होते हैं। यदि कोई अजनबी या व्यवसाय आपसे अनपेक्षित रूप से संपर्क करता है, चाहे यह फोन, डाक, ईमेल, व्यक्तिगत या सोशल नेटवर्किंग साइट पर हो, तो हमेशा इस बात की संभावना पर विचार करें कि यह संपर्क एक घोटाला हो सकता है। याद रखें, अगर कोई चीज इतनी अच्छी है कि लगता है वह सच नहीं हो सकती है, तो शायद वह सच नहीं है।

आप जिसके साथ लेन-देन कर रहे/रही हैं, उसके बारे में जानकारी रखें। यदि आपने किसी के साथ बस ऑनलाइन मुलाकात की है या आप किसी व्यवसाय की वैधता के बारे में अनिश्चित हैं, तो थोड़ी और अधिक खोजबीन करने के लिए समय निकालें। तस्वीरों के लिए गूगल इमेज सर्च करें या इंटरनेट पर उन लोगों के लिए खोज करें जिन्होंने संभवतः पहले उनके साथ लेन-देन किया हो।

संदिग्ध टेक्स्ट संदेशों, पॉप-अप विंडो या ईमेल न खोलें - उन्हें डिलीट कर दें। यदि आप अनिश्चित हैं, तो फोन बुक या ऑनलाइन खोज जैसे स्वतंत्र स्रोत के माध्यम से संपर्क की पहचान सत्यापित करें। आपको भेजे गए संदेश में दिए गए संपर्क विवरण का प्रयोग न करें।

अपना व्यक्तिगत विवरण सुरक्षित रखें। अपने मेलबॉक्स को तालाबंद रखें और अपने बिलों और अन्य महत्वपूर्ण दस्तावेज़ों को फेंकने से पहले उन्हें मशीन का प्रयोग करके काट-फाड़ दें। अपने पासवर्ड और पिन नंबरों को सुरक्षित स्थान पर रखें। सोशल मीडिया साइटों पर अपने बारे में व्यक्तिगत जानकारी साझा करने की सीमा के बारे में बहुत सावधान रहें। घोटालेबाज आपकी पहचान और तस्वीरों का उपयोग एक जाली पहचान बनाने या आपको घोटाले का निशाना बनाने के लिए कर सकते हैं।

भुगतान करने के असामान्य तरीकों के प्रति सचेत रहें। घोटालेबाज अक्सर वायर ट्रांसफर, प्रिलोडेड कार्ड और यहाँ तक कि गूगल प्ले, स्टीम या आईट्यून्स कार्ड और बिटकॉइन के माध्यम से पैसों की माँग करते हैं। यह लगभग हमेशा इस बात का संकेत होता है कि यह माँग एक घोटाले का हिस्सा है।

अपने मोबाइल उपकरण और कंप्यूटर सुरक्षित रखें। हमेशा पासवर्ड सुरक्षा का प्रयोग करें, दूसरों के साथ एक्सेस साझा न करें (दूरस्थ रूप से भी नहीं), सुरक्षा सॉफ्टवेयर को अपडेट करें और सामग्री का बैकअप लें। पासवर्ड का प्रयोग करके अपने वाईफाई नेटवर्क को सुरक्षित रखें और ऑनलाइन बैंकिंग एक्सेस करने या व्यक्तिगत जानकारी प्रदान करने के लिए सार्वजनिक कंप्यूटर या वाईफाई हॉटस्पॉट के प्रयोग से वर्जन करें।

अपने पासवर्ड सावधानीपूर्वक चुनें। ऐसे पासवर्ड चुनें जिनका अनुमान लगाना अन्य लोगों के लिए कठिन हो और उन्हें नियमित रूप से अपडेट करें। सशक्त पासवर्ड में बड़े और छोटे अक्षरों, सँख्याओं और चिह्नों का मिश्रण शामिल होना चाहिए। हरेक खाते/प्रोफाइल के लिए एक ही पासवर्ड का उपयोग न करें, और किसी के साथ भी अपना पासवर्ड साझा न करें।

अपने विवरण देने या पैसे भेजने के किसी भी निवेदन के प्रति सचेत रहें। ऐसे किसी व्यक्ति को कभी पैसे न भेजें और अपने क्रेडिट कार्ड नंबर, ऑनलाइन खाते का विवरण या व्यक्तिगत दस्तावेज़ों की प्रतियाँ न दें जिससे आप परिचित नहीं हैं या जिसपर आप भरोसा नहीं करते/करती हैं। किसी दूसरे व्यक्ति के लिए पैसे या सामान स्थानांतरित करने के लिए सहमति न दें: मनी लॉन्डरिंग एक अपराध है।

ऑनलाइन खरीदारी करते समय सावधान रहें। बहुत ही अच्छे प्रतीत होने वाले प्रस्तावों के प्रति सचेत रहें, और हमेशा ऐसी ऑनलाइन खरीदारी सेवा का उपयोग करें जिससे आप परिचित हैं और जिसपर आप विश्वास करते/करती हैं। आभासी मुद्राओं (जैसे बिटकॉइन) का उपयोग करने से पहले दो बार सोचें - ये अन्य लेनदेन विधियों की तरह सुरक्षित नहीं होती हैं, जिसका अर्थ है कि एक बार भेज देने के बाद आपको अपना पैसा वापिस नहीं मिल सकता है।

सहायता या समर्थन कहाँ से प्राप्त किया जा सकता है

यदि आपने किसी घोटाले में पैसे खो दिए हैं या किसी घोटालेबाज को अपनी व्यक्तिगत जानकारी दे दी है, तो आपको अपना पैसा वापिस मिलने की संभावना नहीं होती है। परंतु आप तुरंत कुछ कदम उठा सकते/सकती हैं जिससे आप अपने नुकसान को सीमित कर सकें और आगे के नुकसान से खुद को सुरक्षित रख पाएँ।

अपने बैंक या क्रेडिट यूनियन से संपर्क करें

यदि आपने किसी घोटालेबाज को पैसे या व्यक्तिगत बैंकिंग जानकारी भेजी है, तो तुरंत अपने बैंक या क्रेडिट यूनियन से संपर्क करें। वे संभावित रूप से आपके पैसे के हस्ताँतरण या चेक को रोक सकते हैं या घोटालेबाज के पास आपके खाते का विवरण होने की स्थिति में आपका खाता बंद कर सकते हैं। यदि आपका क्रेडिट कार्ड धोखे से चार्ज किया गया था, तो आपका क्रेडिट कार्ड प्रदाता संभावित रूप से 'चार्ज बैक' (लेनदेन पलटने) में सक्षम हो सकता है।

चोरी की गई अपनी पहचान को फिर से प्राप्त करें

यदि आपको अपनी पहचान की चोरी किए जाने का संदेह है, तो यह महत्वपूर्ण है कि आप वित्तीय नुकसान या अन्य प्रकार की हानि के खतरे को कम करने के लिए तुरंत कदम उठाएँ।

आईडीकेयर (IDCARE) से संपर्क करें – यह सरकार द्वारा वित्त-पोषित एक निःशुल्क सेवा है जो पहचान अपराध के पीड़ितों को सहायता प्रदान करती है। आईडीकेयर आपकी प्रतिष्ठा, क्रेडिट इतिहास और पहचान के नुकसान की बहाली में समुचित कदम उठाने के लिए एक प्रतिक्रिया योजना विकसित करने में आपकी मदद कर सकती है। आईडीकेयर की वेबसाइट www.idcare.org पर जाएँ या 1300 432 273 पर कॉल करें।

राष्ट्रमंडल पीड़ित प्रमाण-पत्र (Commonwealth Victims' Certificate) के लिए आवेदन करें – यह प्रमाण-पत्र पहचान अपराध का शिकार होने के आपके दावे का समर्थन करने में मदद करता है और इसका उपयोग सरकार या वित्तीय संस्थानों के साथ आपके परिचय को फिर से स्थापित करने में सहायता के लिए किया जा सकता है। अपनी पहचान की सुरक्षा और पुनर्प्राप्ति करने के बारे में और

अधिक जानकारी के लिए वेबसाइट www.ag.gov.au पर एटॉर्नी-जनरल विभाग (Attorney-General's Department) पर जाएँ (या 02 6141 6666 पर कॉल करें)।

एक परामर्श या सहायता सेवा से संपर्क करें

यदि आप या आपका कोई परिचित घोटाले का शिकार हुआ है और संभावित रूप से भावनात्मक तनाव या अवसाद से पीड़ित है, तो कृपया अपने जीपी, स्थानीय स्वास्थ्य व्यावसायिक या किसी अन्य भरोसेमंद व्यक्ति के साथ बात करें। आप परामर्श या समर्थन सेवाओं से संपर्क करने के बारे में भी सोच सकते/सकती हैं, जैसे:

लाइफलाइन (Lifeline) — जब आपको संकट के समय समर्थन की आवश्यकता हो, तो 13 1114 (24/7) पर लाइफलाइन से संपर्क करें या वेबसाइट www.lifeline.org.au पर जाएँ।

बियॉन्डब्लू (Beyondblue) — अवसाद या चिंता के बारे में जानकारी के लिए 1300 224 636 पर बियॉन्डब्लू से संपर्क करें या वेबसाइट www.beyondblue.org.au पर जाएँ।

किड्स हेल्पलाइन (Kids helpline) — पाँच से 25 वर्ष की आयु के युवाओं के लिए टेलीफोन और ऑनलाइन परामर्श और समर्थन सेवा। 1800 551 800 पर किड्स हेल्पलाइन से संपर्क करें या वेबसाइट www.kidshelpline.com.au पर जाएँ।

वित्तीय परामर्श ऑस्ट्रेलिया (Financial Counselling Australia) — यदि आप किसी वित्तीय संकट में हैं, तो एक निःशुल्क वित्तीय परामर्शदाता से बात करने के लिए 1800 007 007 पर कॉल करें या वेबसाइट www.financialcounsellingaustralia.org.au पर जाएँ।

घोटाले की रिपोर्ट कहाँ की जा सकती है

आप उपयुक्त अधिकारियों के पास घोटाले की रिपोर्ट करके दूसरों की सहायता कर सकते/सकती हैं। आपकी जानकारी इन संगठनों को सबसे हाल के घोटालों की एक बेहतर तस्वीर बनाने में सहायता करेगी और दूसरे लोगों को इस बारे में चेतावनी देगी कि उन्हें किन बातों के प्रति सचेत रहना चाहिए।

निम्नलिखित संगठन विशेष प्रकार के घोटालों के बारे में रिपोर्टिंग स्वीकार करते हैं।

स्कैमवॉच (Scamwatch)

स्कैमवॉच के माध्यम से एसीसीसी के पास घोटालों की रिपोर्ट करें - वेबसाइट www.scamwatch.gov.au पर जाएँ

घोटालेबाजों से एक कदम आगे रहें

घोटालेबाजों से एक कदम आगे रहें - स्कैमवॉच वेबसाइट पर जाकर ऑस्ट्रेलियाई व्यापारियों और छोटे व्यवसायों को निशाना बनाने वाले घोटालों के बारे में अवगत रहें। इस बारे में और अधिक जानकारी प्राप्त करें कि घोटाले कैसे काम करते हैं, आप स्वयं को सुरक्षित कैसे रख सकते/सकती हैं और यदि आप घोटाले का शिकार हुए/हुई हैं, तो क्या करना चाहिए।

समुदाय में चल रहे घोटालों के बारे में निःशुल्क ईमेल चेतावनियाँ प्राप्त करने के लिए स्कैमवॉच सदस्यता सेवा के लिए रजिस्टर करें।

www.scamwatch.gov.au

ट्विटर पर स्कैमवॉच को @scamwatch_gov या http://twitter.com/Scamwatch_gov पर फॉलो करें।

यदि आपको किसी वेबसाइट या सोशल मीडिया प्लेटफॉर्म पर कोई घोटाला दिखाई देता है, तो उस साइट पर इसकी रिपोर्ट करें ताकि इसकी जाँच की जा सके और इसे हटाया जा सके। यदि घोटालेबाज़ किसी सरकारी विभाग या बैंक जैसे वैध संगठन के नाम का उपयोग कर रहे हैं, तो उन्हें इसके बारे में जानकारी दें ताकि वे दूसरों को सचेत कर सकें।

अन्य एजेंसियाँ

आपको अपने घोटाले के बारे में अन्य एजेंसियों के पास रिपोर्ट करने के बारे में भी विचार करना चाहिए, जो विशेष प्रकार के घोटालों से व्यवहार करती हैं।

घोटाले का प्रकार	एजेंसी
साइबर अपराध	ऑस्ट्रेलियाई साइबर अपराध ऑनलाइन रिपोर्टिंग नेटवर्क (एकॉर्न) [Australian Cybercrime Online Reporting Network (ACORN)] - वेबसाइट www.acorn.gov.au पर जाएँ।
वित्तीय और निवेश के घोटाले	ऑस्ट्रेलियाई प्रतिभूति और निवेश आयोग (एसिक) [Australian Securities and Investments Commission (ASIC)] - वेबसाइट www.moneysmart.gov.au पर जाएँ या 1300 300 630 पर एसिक इन्फोलाइन को कॉल करें।
धोखाधड़ी और चोरी	आपकी स्थानीय पुलिस - 13 1444 पर कॉल करें।
स्पैम ईमेल और एसएमएस	ऑस्ट्रेलियाई संचार और मीडिया प्राधिकरण (एक्मा) [Australian Communications and Media Authority (ACMA)] - वेबसाइट www.acma.gov.au पर जाएँ या 1300 1200 115 पर एक्मा ग्राहक सेवा केंद्र को कॉल करें।
कर से संबंधित घोटाले	ऑस्ट्रेलियाई कराधान कार्यालय (एटीओ) [Australian Taxation Office (ATO)] – कर से संबंधित घोटाले की रिपोर्ट करने के लिए या एटीओ की ओर से आपके साथ संपर्क करने वाले व्यक्ति की वैधता को सत्यापित करने के लिए: • 1800 008 540 पर कॉल करें या अपनी कर से संबंधित घोटाले वाली ईमेल को ReportEmailFraud@ato.gov.au पर भेजें।
बैंकिंग	आपकी बैंक या वित्तीय सँस्थान

अपनी स्थानीय उपभोक्ता संरक्षण एजेंसी से संपर्क करें

एसीसीसी सामान्य उपभोक्ता संरक्षण मामलों से व्यवहार करने वाली राष्ट्रीय एजेंसी है, परंतु राज्यों और राज्य-क्षेत्रों की एजेंसियाँ भी आपकी सहायता करने में सक्षम हो सकती हैं।

ऑस्ट्रेलियाई राजधानी क्षेत्र नियामक सेवाएँ कार्यालय (Australian Capital Territory Office of Regulatory Services)	www.accesscanberra.act.gov.au 13 2281
उपभोक्ता मामले विक्टोरिया (Consumer Affairs Victoria)	www.consumer.vic.gov.au 1300 558 181
न्यू साउथ वेल्स निष्पक्ष व्यापार (New South Wales Fair Trading)	www.fairtrading.nsw.gov.au 13 3220
उत्तरी राज्य-क्षेत्र उपभोक्ता मामले (Northern Territory Consumer Affairs)	www.consumeraffairs.nt.gov.au 1800 019 319
क्वींसलैंड निष्पक्ष व्यापार कार्यालय (Queensland Office of Fair Trading)	www.fairtrading.qld.gov.au 13 7468
दक्षिण ऑस्ट्रेलिया उपभोक्ता और व्यवसाय सेवाएँ (South Australia Consumer and Business Services)	www.cbs.sa.gov.au/ 13 1882
तस्मानिया उपभोक्ता, भवन और व्यावसायिक सेवाएँ (Tasmania Consumer, Building and Occupational Services)	www.cbos.tas.gov.au/ 1300 654 499
पश्चिमी ऑस्ट्रेलिया खनन, उद्योग विनियमन और सुरक्षा विभाग (Western Australia Department of Mines, Industry Regulation and Safety)	www.consumerprotection.wa.gov.au/ 1300 304 054

और अधिक जानकारी

ऑस्ट्रेलियाई सरकार के पास ऑनलाइन सुरक्षित और सकुशल बने रहने के लिए कुछ बेहतरीन सँसाधन हैं।

- स्टे स्मार्ट ऑनलाइन सेवा (Stay Smart Online Service) — www.staysmartonline.gov.au
- साइबरस्मार्ट (CyberSmart) वेबसाइट — www.cybersmart.gov.au
- स्टे स्मार्ट ऑनलाइन (Stay Smart Online) मार्गदर्शिकाएँ - वेबसाइट www.staysmartonline.gov.au/get-involved/guides पर उपलब्ध

www.scamwatch.gov.au