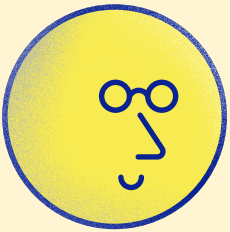
사기를 알아채고 피하는 방법



사기로부터 스스로를 보호하는 방법에 대한 지침

Australian Government

National Anti-Scam Centre

ScamWatch
Stop. Better safe than scammed.

원주민 존중 의례

ACCC는 호주 전역에 걸친 이 땅의 전통적인 소유주 및 관리인을 인정하며 그들의 토지, 바다 및 지역사회와의 지속적인 연계를 존중합니다. 당사는 그들과 그들의 문화, 그리고 그들의 과거, 현재, 미래의 장로들에게 존경심을 표합니다.

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

© 호주 연방 2023

본 문서는 저작권으로 보호됩니다. *1968 년 저작권법*에 따라 허용된 사용 외에도 본 저작물에 포함된 모든 자료는 Creative Commons Attribution 4.0 Australia 라이선스에 따라 제공되며 이에는 다음이 제외됩니다.

- 연방 문장
- ACCC 및 AER 로고
- ACCC가 저작권을 보유하지 않지만 본 출판물의 일부이거나 본 출판물에 포함될 수 있는 모든 그림, 도형, 사진 또는 그래픽

CC BY 4.0 AU 라이선스에 대한 전체 법적 코드와 마찬가지로 관련 라이선스 조건에 대한 세부 정보는 Creative Commons 웹사이트에서 확인할 수 있습니다.

복제 및 권리에 관한 요청 및 문의는 다음으로 문의하시기 바랍니다:
Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

주요 고지사항

본 출판물에 포함되는 정보는 일반적인 지침 목적으로만 제공됩니다. 이는 법적 또는 기타 전문적인 조언을 구성하지 않으며 모든 관할권의 법률로 해석 및 의존되어서는 안 됩니다. 일반적인 지침으로 작성되었으므로 일반화가 포함될 수 있습니다. 특정 우려사항이 있는 경우 전문적인 자문을 구하시길 바랍니다.

ACCC는 최신의 정확한 정보를 제공하기 위해 모든 합당한 노력을 기울였으나 해당 정보의 정확성, 최신성 또는 완전성에 관해 어떠한 보장도 하지 않습니다.

본 출판물의 정보를 재발행 또는 인용하고자 하는 당사자는 출판 전 정보의 최신성 및 정확성을 반드시 확인해야 합니다. ACCC 지침 및 관련 임시 법률이 자주 변경되므로 이는 각 출판 이전에 수행되어야 합니다. 문의사항이 있는 경우 다음으로 문의하시기 바랍니다:
Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 05/24_24-13

www.accc.gov.au

목차

도움을 받을 수 있습니다 1

사기는 무엇인가요? 3

사기를 알아채고 피하는 간단한 방법 4

문자 또는 SMS 사기 7

이메일 사기 11

전화 사기 15

웹사이트 사기 19

소셜미디어, 앱 기반 및 온라인 메시지 사기 23

여러분이 알아야 하는 흔한 사기 유형 27

사기를 신고하는 곳 31

더 많은 도움 및 지원 33

본 지침은 국가 사기방지센터(National Anti-Scam Centre, NASC)에서 작성했으며 이는 여러분이 사기를 구별하고 이로 인한 피해로부터 스스로를 보호하는 데 도움이 될 것입니다.

사기는 범죄이며 사기를 행하는 사람은 범죄자입니다. 호주의 많은 사람들이 사기를 당하고 돈을 잃고 있으며 때로는 평생 모은 돈을 잃기도 합니다. 사기는 사람들의 인생을 힘들게 합니다.

사기를 알아채기가 점점 어려워지고 있으므로 우리는 함께 힘을 모아 사기를 막아야 합니다.

NASC는 호주인들을 사기로부터 안전하게 보호하기 위해 존재합니다.

당사는 정부 및 관련 산업들과 협력해 사기꾼들이 호주인들의 돈과 개인정보를 훔치는 것을 막을 수 있는 새로운 방법을 모색합니다. 당사가 이를 달성하는 몇 가지 방법은 다음과 같습니다.

사람들이 사기를 알아채고 피할 수 있도록 지원합니다.

Scamwatch를 통해 사기 유형과 사기로부터 스스로를 보호하는 법에 대한 최신 정보를 공유합니다.

사기꾼들에게 혼선을 야기시킵니다.

정부와 업계 전반에 걸쳐 정보를 수집하고 이를 공유함으로써 사기꾼들이 계속해서 범죄를 저지르는 것을 더 어렵게 만들고 사람들이 사기를 더 쉽게 신고할 수 있도록 합니다.

도움을 받을 수 있습니다

본 지침을 읽고 계시다면 아마 여러분 또는 여러분이 아는 누군가는 사기의 피해자였을 것입니다. 안타깝게도 아마 여러분 뿐만이 아닐 것입니다. 사기 수법은 점점 진화하고 있으며, 이는 누구나 그 대상이 될 수 있음을 의미합니다.

만약 사기를 당하셨다면, 빠른 조치를 취하는 것이 중요합니다.

사기꾼에게 돈을 빼앗긴 경우, 거래은행 또는 카드 제공업체에 연락하세요.

IDCARE(1800 595 160번, www.idcare.org)에 연락하세요.

사기가 통하는 이유는 실제처럼 보이기 때문입니다. 사기꾼들은 급한 상황, 놓치고 싶지 않은 굉장한 거래 조건, 또는 여러분이 신뢰하는 사람에게서 온 것처럼 보이는 상황을 제시하면서 이에 가려져 여러분이 위험 신호를 발견하지 못하는 것을 이용합니다.

다음 세 단계를 따라 사기로부터 스스로를 보호하세요:

멈추세요

확실하지 않으면 그 누구에게도 돈 또는 개인정보를 제공하지 마세요.

사기꾼들은 여러분에게 도움을 주는 척을 하거나 여러분의 신원을 확인할 것입니다. 서비스 제공업체, 경찰, 여러분의 거래은행 또는 정부 서비스와 같이 여러분이 알고 신뢰하는 조직에서 연락하는 것처럼 연기할 것입니다.

확인하세요

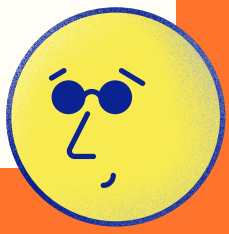
스스로에게 물어보세요 – 메시지 또는 전화 내용이 거짓일 수 있을까?

메시지 속 링크를 절대로 클릭하지 마세요. 사업체 또는 정부에 연락을 해야 하는 경우, 그들의 공식 웹사이트 또는 앱에서 여러분이 직접 찾은 연락처를 통해서만 연락하세요. 확실하지 않은 경우 '아니요'라고 답하거나, 끊거나 삭제하세요.

신고하세요

무언가가 잘못되었음을 느낄 경우 빠른 조치를 취하세요.

이상한 결제가 보이거나 사기꾼이 여러분의 돈 또는 정보를 확보한 경우 거래은행에 연락하세요. 지원을 요청하고 사기를 ReportCyber 및 Scamwatch에 신고하세요. 사기를 신고하면 사기에 대한 호주 방어 체계를 구축할 수 있으며 이는 모든 호주인을 돕는 것입니다.



사기는 무엇인가요?

사기는 누군가가 여러분을 속여 여러분의 돈 또는 개인정보를 도용하는 행위입니다.

사기는 경제 범죄이며 대개 매우 조직적이고 정교한 범죄자들에 의해 운영됩니다.

사기의 특징:

- 범죄자에 의해 운영됩니다
- 실제처럼 보입니다
- 믿을만한 이야기가 동반됩니다
- 어떠한 조치를 취하도록 압박을 가합니다

다음의 경우는 사기가 아닙니다:

- 컴퓨터 해킹
- 불합리한 계약 조건
- 집요한 마케팅 방식

불쾌한 경험이 꼭 사기가 아니라는 것을 기억하는 것이 중요합니다. 비용을 결제했으나 물품을 못 받은 경우, 혹은 무언가를 구매했으나 제품의 질이 좋지 않은 경우를 경험해 보셨을 수도 있습니다. 실망스러울 수는 있으나 이러한 경우들이 반드시 사기인 것은 아닙니다. 호주 소비자법은 호주 소비자들에게 이러한 문제에 대한 보호를 제공하고 있습니다.

더 자세한 정보를 원하시면 www.accc.gov.au/consumers를 방문하세요.

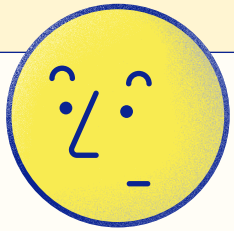
사기를 알아채고 피하는 간단한 방법

사기는 누구에게나 일어날 수 있습니다. 사기가 통하는 이유는 사기꾼들이 믿을만한 이야기를 제시하며 여러분의 돈 또는 개인정보를 훔치기 때문입니다.

사기꾼들은 점점 지능적으로 진화하고 있으며 그들은 새로운 기술, 제품, 서비스 및 대형 이벤트 등을 이용해 자신의 사기가 진짜인 마냥 여러분을 설득할 것입니다.

사기를 알아채는 것이 때론 굉장히 어려울 수 있습니다. 다음은 여러분이 주의를 기울여야 하는 몇 가지 예시 상황입니다. 사기꾼들은 때때로 이러한 전략을 조합해서 사용합니다.

1. **돈을 벌거나 모을 수 있는 기회:** 사기꾼들은 여러분이 굉장한 거래나 제안을 받고 있다고 믿도록 속일 것입니다. 그들은 여러분이 이러한 기회를 놓치지 않기 위해 빠르게 행동하도록 압박할 것입니다. 기억하세요, 말도 안되게 좋아 보이는 거래는 아마 문제가 있을 것입니다.
2. **슬픈 사연 및 도움을 요청하는 절박한 호소:** 사기꾼들은 여러분의 인심을 역으로 이용하려고 할 것입니다. 그들은 여러분에게 가슴 아프고 비극적인 이야기를 전달하며 왜 여러분의 도움과 돈이 필요한지 설명할 것입니다.
3. **링크 및 첨부파일:** 사기꾼들은 여러분의 정보와 돈을 훔치도록 설계된 사기 웹사이트로 접속되는 링크를 이용합니다. 또한 여러분이 첨부파일을 열람할 것을 요청할 수도 있습니다. 이들 링크 및 첨부파일은 여러분의 정보를 훔치는 바이러스를 설치할 수 있습니다.



4. **빠른 조치를 취하도록 압박하는 행위:** 사기꾼들은 여러분이 시간을 두고 여러 방면을 고려하는 것을 원하지 않습니다. 그들은 여러분이 빠른 조치를 취하도록 압박하고 싶어 합니다. 이에는 여러분이 빠른 조치를 취하지 않으면 안 좋은 일이 벌어질 거라는 협박을 하는 행위가 포함됩니다.
5. **특이하거나 특정한 방식의 결제 요청:** 사기꾼들은 종종 사전 충전된 직불 카드, 아이튠즈(iTunes) 카드 또는 비트코인 등 가상 통화와 같은 흔하지 않은 방법을 사용해 결제하도록 요청합니다. 이러한 결제 방법은 결제하는 순간 되돌릴 수 없습니다.
6. **새로운 계정 또는 페이아이디(PayID) 생성 요청:** 사기꾼들은 여러분이 그들에게 비용을 지급할 수 있도록(혹은 지급받을 수 있도록) 새로운 은행 계좌 또는 PayID를 생성할 것을 요청할 수도 있습니다. 그들은 여러분의 거래은행인 척 연기하며 여러분의 돈을 안전하게 보관하기 위해 이를 새 계좌로 이체하라고 지시할 수도 있습니다.

사기꾼들은 여러분의 돈을 훔치는 데 성공하면 더 많은 돈을 훔치려고 시도할 것입니다. 안타깝게도 사기 피해자 3명 중 1명은 한 번 이상 사기를 당합니다. 만약 사기로 돈을 잃었다면 돈을 돌려받을 수 있도록 도와주겠다고 제안하는 사기꾼들을 조심하세요. 이는 또 다른 형식의 후속 사기입니다.

문자 또는 SMS 사기

사기꾼들은 정부, 법 집행 기관, 신뢰할 수 있는 기업, 심지어는 여러분의 가족이나 친구로 가장해 메시지를 보냅니다.

이러한 메시지는 급박한 분위기를 조성해 여러분이 빠른 조치를 취하도록 유도할 것입니다. 이에는 사기 웹사이트로 연결되는 링크가 포함되는 경우가 많습니다. 사기꾼들은 이러한 사기 웹사이트에 입력되는 모든 개인정보를 훔칠 수 있으며 그들은 이를 사용해 여러분의 돈을 빼앗거나 귀하의 이름으로 사기를 저지를 수 있습니다.

이러한 메시지가 진짜처럼 보이도록 하기 위해 사기꾼들은 자신의 전화번호를 실제 회사나 아는 사람의 전화번호와 발신자 번호로 복제하거나 위장합니다.

사기 메시지는 어떠한 기관과 나눈 실제 메시지와 동일한 대화창에 나타날 수 있으며 이는 이러한 메시지를 구별하기 더욱 어렵게 만듭니다.

문자가 사기일 수 있다는 징후

문자 내용 특징:

즉각적인 조치를 취하거나, 결제를 하거나, 돈을 이체하라고 요청합니다.

링크를 클릭하거나 메시지에 제공된 번호로 전화하도록 요청합니다.

여러분의 사용자 아이디와 비밀번호로 특정 온라인 계정에 로그인하거나 기타 개인 정보를 제공하도록 요청합니다.

가족이나 친구가 자신의 연락처가 변경되었다고 합니다.

조치를 취하지 않으면 서비스를 중단하거나 비용을 청구하겠다고 위협합니다.

귀하 또는 귀하의 계정이 해킹되었거나 사기에 연루되었음을 시사합니다.

결제 또는 소포 배송에 문제가 있음을 시사합니다.

메시지 사기로부터 스스로를 보호하는 방법

1. 만약 여러분이 아는 누군가가 자신의 연락처가 변경되었다는 메시지를 보내올 경우:
   a. 여러분이 가지고 있는 기존의 번호로 연락을 시도한 후
   b. 상대방의 신원을 검증하기 위해 그 사람만이 답을 아는 질문과 함께 새 번호로 메시지를 보내세요.

2. 메시지 속 링크는 절대로 클릭하지 마세요.

3. 메시지가 웹사이트로 연결될 경우, 링크를 클릭하지 마세요. 대신, 웹사이트를 직접 찾아보거나 공식적인 앱을 이용하세요.

4. 제공된 번호를 사용해 문자 메시지에 답하지 마세요.

5. 해당 기관의 웹사이트 등에서 여러분이 직접 찾은 전화번호로 해당 기관이나 사람에게 다시 전화하세요.

이메일 사기

사기꾼들은 정부, 법 집행 기관 및 기업에서 보낸 것처럼 가장해 이메일을 보냅니다. 그들은 급박한 분위기를 조성해 여러분이 빠른 조치를 취하도록 유도합니다.

사기꾼들은 실제 기업과 동일한 로고와 유사한 이메일 주소를 사용합니다. 또한 그들은 사기 이메일이 더욱 신빙성 있게 보이도록 자신의 이메일 주소를 기관이나 기업의 이메일 주소로 복제하거나 위장할 수도 있습니다.

이메일이 사기일 수 있다는 징후

이메일 내용 특징:

결제를 요청했으나 새로운, 혹은 마지막 결제와는 다른 계좌 정보가 제공됩니다.

여러분의 사용자 아이디와 비밀번호로 특정 온라인 계정에 로그인하거나 기타 개인 정보를 제공하도록 요청합니다.

예상치 못한 이메일로 열람하라는 안내가 있는 첨부 파일이 포함되어 있습니다.

여러분이 모르는 미불 환불금 또는 자금이 있다고 말하며 이를 받으려면 여러분의 은행정보 확인이 필요하다고 말합니다.

여러분에 관한 정보 또는 여러분의 사진이 있다고 주장하고 이를 공개하겠다고 위협합니다.

데이터 침해 또는 신원 도용에 대해 돈을 회수하거나 보상을 받을 수 있도록 도와주겠다고 제안합니다.

이메일 사기로부터 스스로를 보호하기 위해 취할 수 있는 조치

1. 다음 방법 중 하나로 이메일의 신빙성을 확인하세요:
   a. 해당 기관의 웹사이트 등에서 여러분이 직접 찾은 전화번호로 해당 기관이나 사람에게 다시 전화하거나
   b. 공식 앱을 통해 기관 서비스를 이용합니다. (절대 링크를 통하지 않습니다.)

2. 여러분을 협박하거나 위협하려고 하는 모든 사람과는 연락을 그 즉시 끊으세요.

3. 다음을 제공한다는 사람에게는 개인정보 또는 돈을 절대로 제공하지 마세요.
   a. 이전에 발생한 사기 또는 데이터 침해 손실을 회복하기 위한 보상 또는 지원; 또는
   b. 상금, 상품 또는 상속.

4. 가능한 경우에는 다중인증(multi-factor authentication)을 사용하세요. 이는 추가 보호 단계로 사기꾼이 여러분의 이메일 계정에 접근하려면 여러분의 이메일 비밀번호와 휴대폰으로 전송된 핀 번호를 알아야 함을 의미합니다.

전화 사기

사기꾼들은 유명한 기관의 직원임을 주장하면서 전화를 겁니다. 이에는 정부 기관, 법 집행 기관, 투자 및 법률 회사, 은행, 통신 제공업체가 포함됩니다.

그들은 급박한 분위기를 조성해 여러분이 빠른 조치를 취하도록 유도합니다. 그들은 여러분이 개인정보나 은행계좌 정보, 또는 컴퓨터에 대한 접근 권한을 제공하도록 설득하려고 할 수 있습니다.

전화 발신자가 이름이나 주소 등 여러분에 대한 몇 가지 세부 정보를 이미 알고 있어 전화가 실제 통화인 것처럼 보일 수도 있습니다.

전화가 사기일 수 있다는 징후

통화 내용 특징:

비용 지급 또는 새 계좌로 돈을 이체하도록 요청합니다.

비밀번호, 핀 번호, 일회성 코드 또는 기타 보안 정보를 요청합니다.

신용카드나 거래은행 정보 등 금융 세부정보를 요청합니다.

소프트웨어 설치, 보안 계정 접근 등 휴대폰이나 컴퓨터에서 특정 작업을 수행하도록 요청합니다.

법 집행 기관 소속이라고 주장하며 즉시 체포하거나 추방하겠다고 위협합니다.v

귀하의 은행이나 기타 온라인 계좌가 해킹되었거나 사기에 연루되었다고 말합니다.

전화 사기로부터 스스로를 보호하기 위해 취할 수 있는 조치

1. 다음 방법 중 하나로 통화의 신빙성을 확인하세요:
   a. 해당 기관의 웹사이트 등에서 여러분이 직접 찾은 전화번호로 해당 기관이나 사람에게 다시 전화하거나
   b. 공식 앱을 통해 기관 서비스를 이용합니다. (절대 링크를 통하지 않습니다.)

2. 발신자가 누구인지 확실하지 않거나 그들이 여러분을 협박 또는 위협하는 경우 그 즉시 전화를 끊으세요.

3. 타인이 여러분의 컴퓨터나 기기에 접근하는 것을 허용하는 소프트웨어는 절대 설치하지 마세요.

4. 모르는 번호의 전화는 무시하거나 음성편지함으로 넘어가도록 하세요.

알아두면 좋은 정보!

발신번호 표시제한으로 설정되어 있거나 Do Not Call(전화 금지) 명단에 등록되어 있어도 사기 전화를 받을 수 있습니다.

웹사이트 사기

사기꾼들은 정부, 실제 기업, 연예인 또는 여러분의 친구나 가족 등을 비롯해 온라인에서 다른 사람인 것처럼 가장할 수 있습니다.

그들은 유명한 브랜드인 것처럼 보이도록 거짓 웹사이트를 만들 수 있습니다. 유명인들을 흉내내며 마치 그들이 해당 상품 또는 서비스를 보증하는 것처럼 비출 수 있습니다. 이러한 웹사이트는 여러분이 신뢰하도록 거짓 리뷰를 포함할 수 있습니다.

온라인에 접속하면 거짓 경고나 오류 메시지가 포함된 거짓 광고 배너나 팝업 창이 나타날 수 있습니다.

웹사이트가 사기일 수 있다는 징후

웹사이트 내용 특징:

일반적인 수준 혹은 다른 사이트에 비해 훨씬 저렴한 가격으로 판매 품목을 제공합니다.

위험이나 노력이 거의 요구되지 않는, 빠르고 쉽게 돈을 벌 수 있는 방법을 알려줍니다.

링크를 클릭하라는 긴급 경고 또는 오류 메시지가 포함되어 있습니다.

기프트 카드나 비트코인과 같은 암호화폐 등 비정상적이거나 특정한 방법으로 결제를 요청합니다.

호의적인 리뷰만을 포함합니다.

웹사이트 사기로부터 스스로를 보호하기 위해 취할 수 있는 조치

1. 가격을 비교하세요. 말도 안되게 좋아 보이는 거래는 아마 문제가 있을 것입니다.

2. 여러분의 돈이나 개인정보를 제공하기 전에 거래 기관 또는 상대방에 대해 조사하세요.

3. 해당 웹사이트에 기재된 리뷰에만 의존하지 마세요. 해당 웹사이트 또는 사업체명을 ‘scam’ 또는 ‘reviews’라는 단어와 함께 검색하세요.

4. 화면에 경고 또는 오류 메시지가 나타나면 이를 클릭하지 말고 해당 응용 프로그램으로 직접 이동해 진실 여부를 확인하세요.

5. 온라인 쇼핑에 사용하는 기기의 운영 체제 및 앱에 대한 '자동 업데이트'를 활성화해 최신 상태로 유지하세요.

알아두면 좋은 정보!

온라인상에서 스스로를 보호하는 실질적인 방법에 대한 정보는 www.cyber.gov.au에서 확인할 수 있습니다.

소셜미디어, 앱 기반 및 온라인 메시지 사기

만약 모르는 누군가가 소셜미디어, 메시지 플랫폼(예: WhatsApp, WeChat) 또는 앱을 통해 여러분에게 연락을 할 경우, 이는 사기일 수 있습니다.

다른 사람인 것처럼 가장하는 사기꾼들은 사기 여부 판단을 더욱 어렵도록 하기 위해 자신이 가장하는 조직의 공식 로고나 사람의 실제 사진을 사용하는 경우가 많습니다.

소셜 미디어상의 사기꾼들은 가짜 프로필을 설정하고 정부, 실제 사업체, 고용주, 투자 회사, 심지어 친구, 가족 또는 연인인 것처럼 가장합니다.

유명인들을 흉내내며 마치 그들이 해당 상품 또는 서비스를 보증하는 것처럼 비출 수 있습니다.

또한 사기꾼들은 여러분이 소셜미디어 계정에 공유하는 정보만으로도 여러분에 대해 많은 것을 파악할 수 있습니다. 그들은 이 정보를 이용해 여러분의 계정 비밀번호를 유추하거나 여러분을 다른 사기의 표적으로 삼을 수 있습니다.

소셜미디어 또는 앱이 사기일 수 있다는 징후

소셜미디어 프로필 또는 앱 내용의 특징:

위험이나 노력이 거의 요구되지 않는, 빠르고 쉽게 돈을 벌 수 있는 방법을 알려줍니다.

추첨 또는 기간 한정 기회에 참여하도록 초대합니다.

데이트 앱 등 앱에서 나눈 대화를 비공개 채팅이나 이메일로 이전할 것을 요청합니다.

유명인이 특정 상품 또는 서비스를 보증하거나 지지한다는 뉘앙스의 이야기를 전달합니다.

여러분이 판매하는 물건을 누군가가 보지도 않고 높은 가격에 살 것이라고 말합니다.

돈을 지불하지 않으면 여러분의 사적인 사진을 공유하겠다고 위협합니다.

여러분에게 일자리를 제안하기 위해 연락합니다.

알아두면 좋은 정보!

다양한 소셜 미디어 플랫폼에서 안전을 유지하는 방법에 대한 정보는 www.esafety.gov.au에서 확인할 수 있습니다.

소셜미디어 및 앱 기반 사기로부터 스스로를 보호하기 위해 취할 수 있는 조치

1. 프로필의 진위 여부를 확인하세요. 계정이 사용되고 있는지 확인하세요. 해당 사람의 친구/팔로워 및 게시물 수를 확인하세요.

2. 온라인에 해당 프로필의 이름을 'scam'이라는 단어와 함께 검색하세요.

3. 인터뷰나 경력, 적합성, 추천에 대한 논의 없이 제의받은 일자리는 절대 수락하지 마세요. 채용담당자 및 해당 일자리를 제공하는 기업 또는 개인에 대해 조사하세요. 별도의 인터넷 검색을 통해 알아낸 전화번호를 통해 채용 기관에 문의하세요. 일자리를 확보하기 위해 선급금을 지불하지 마세요.

4. 호주 금융서비스(Australian Financial Services) 라이선스를 가진 사람에게서만 투자 조언을 듣고 국제증권위원회(International Organization of Securities Commission, IOSCO) 투자자 알림 포털에 해당 회사나 웹사이트의 이름이 기재되어 있는지 여부를 확인하세요.

5. 온라인상에서만 만난 사람에게는 절대로 돈을 전달하지 마세요. 사기꾼들은 종종 자신이 해외에 거주하고 있고 실제로는 만날 수 없다고 말합니다.

6. 온라인상에서만 만난 사람에게는 절대로 본인의 사적인 사진을 전송하지 마세요.

사기꾼들이 여러분에게 접근하기 위해 사용하는 기타 접근법(대면, 메일 등)을 비롯해 사기에 대한 더 자세한 정보를 원하시면 Scamwatch를 방문하세요.

여러분이 알아야 하는 흔한 사기 유형

여러분이 알아야 하는 가장 일반적인 사기 유형 중 일부는 다음과 같습니다. 위험 신호와 자신을 보호하기 위해 취할 수 있는 조치를 포함해 각 사기 유형에 대한 더 자세한 정보는 Scamwatch 웹사이트에서 확인할 수 있습니다.

신원 도용 사기

사기꾼들은 경찰, 정부, 은행, 유명 기업 등 신뢰할 수 있는 조직에서 연락하는 것처럼 속입니다. 심지어는 여러분의 친구나 가족인 것처럼 가장할 수도 있습니다. 사기꾼들은 피싱 이메일이나 메시지를 보내 여러분에 관한 정보를 알아내려고 합니다. 이는 여러분의 정보를 훔치기 위해 설계됐습니다. 그들은 공식 기관이나 여러분이 알고 신뢰하는 사람인 것처럼 가장해 여러분이 개인정보를 제공하도록 설득하려고 합니다.

사기꾼들은 기술을 사용해 전화나 메시지가 실제 전화번호에서 온 것처럼 보이게 합니다. 문자 메시지가 어떠한 기관과 나눈 실제 메시지와 동일한 대화창에 나타나도록 할 수 있습니다.

투자 사기

사기꾼들은 설득력 있는 마케팅과 신기술을 사용해 놓칠 수 없을 정도로 좋아 보이는 투자를 제안합니다. 그들은 위험이 거의 또는 전혀 따르지 않는 큰 배당금을 약속합니다. 또한 종종 여러분의 돈을 훔치기 위해 여러분이 빠르게 조치를 취하도록 압박 전략을 사용합니다.

일자리 및 채용 사기

사기꾼들은 적은 노력으로도 높은 급여를 받을 수 있는 일자리를 제안합니다. 그들은 유명 기업과 온라인 쇼핑 플랫폼을 대리해 채용 절차를 수행하는 척합니다. 때로는 그들이 광고하는 일자리가 애초에 존재하지도 않습니다. 사기꾼들은 유명 채용 에이전시를 가장하기도 합니다. 그들의 목적은 여러분의 돈과 개인정보를 훔치는 것입니다. 그들은 여러분에게 일자리를 대가로 선급금을 지불하라고 요구할 수도 있습니다.

상품 및 서비스 사기

사기꾼들은 여러분의 돈을 훔치기 위해 구매자 또는 판매자인 척 위장합니다. 그들은 합법적인 소매업체 사이트에 가짜 웹사이트나 프로필을 설정하고 상품이나 서비스를 말도 안 되게 좋은 가격에 판매합니다. 또한 거짓 광고 및 리뷰를 게시합니다. 그들은 도용한 로고, '.com.au' 도메인 이름 및 도용한 호주사업자번호(ABN)를 사용할 수도 있습니다. 이러한 사기는 알아채기 어렵습니다.

사기꾼들은 또한 여러분이 알고 신뢰하는 업체인 것처럼 가장해 거짓 청구서를 보냅니다. 고객이 여러분이 아닌 사기꾼에게 비용을 지불하도록 실제 청구서의 세부 정보를 변경할 수도 있습니다.

로맨스 사기

사기꾼들은 여러분의 돈을 훔치기 위해 사랑, 연애 또는 우정에 대한 여러분의 기대를 이용합니다. 그들은 관계의 진실성을 증명하고 여러분이 돈을 제공하도록 설득하기 위해 많은 노력을 기울입니다.

사기꾼들은 여러분에 대한 정보를 소셜미디어, 데이트 앱, 또는 게임 앱 및 웹사이트에서 찾을 수 있습니다. 그들은 또한 여러분에게 문자 또는 이메일을 전송할 수 있습니다. 사기꾼들은 거짓 프로필과 신원 뒤에 숨으며 어떤 경우엔 유명인을 가장하기도 합니다. 여러분이 그들을 신뢰하는 순간 그들에게 어떠한 '비상 상황'이 발생할 것이며 그들은 여러분에게 도움을 요청할 것입니다. 이는 대개 돈 또는 기타 제품에 대한 요구일 것입니다.

협박 및 강탈 사기

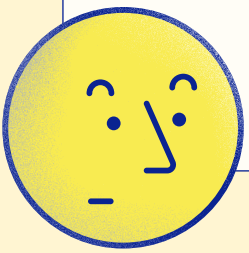
사기꾼들은 신뢰할 수 있는 조직의 직원인 것처럼 가장해 돈을 지불하지 않으면 안 좋은 일이 일어날 것이라고 주장합니다. 즉시 비용을 지불하는 데 동의하지 않으면 체포, 추방 또는 심지어 신체적 상해를 가하겠다고 위협할 수도 있습니다.

또한 여러분이 돈을 지급하지 않으면 여러분이 보낸 나체 사진이나 동영상을 공유하겠다고 협박할 수도 있습니다.

예상에 없는 돈에 대한 사기

사기꾼들은 여러분에게 예상 밖의 돈이나 상금을 받을 자격이 있다고 설득하려고 합니다.

사기꾼은 여러분이 돈이나 상금을 받기 전에 수수료를 지불하거나 은행 또는 신원 정보를 제공하도록 요구합니다. 안타깝게도 세상에는 대가없이 받는 돈은 존재하지 않습니다.



사기를 신고하는 곳

당사는 사기를 식별하고, 피하고, 신고하는 방법에 대한 인식을 높여 사기꾼에게 호주가 더 어려운 표적이 되도록 하기 위해 노력하고 있습니다.

당사는 사기 신고에서 얻은 정보를 공유하고 정부, 법 집행 기관 및 민간 부문과 협력해 사기를 저지하고 예방합니다.

Scamwatch 신고로 타인을 도우세요. Scamwatch 웹사이트 www.scamwatch.gov.au의 신고 양식을 통해 사기 험을 신고하세요.

기억하세요, 사기의 피해자라면 빠른 조치를 취하는 것이 중요합니다.

- 사기꾼에게 돈을 빼앗긴 경우, 거래은행 또는 카드 제공업체에 연락하세요.
- IDCARE에 연락하세요. 1800 595 160| idcare.org

더 많은 도움 및 지원

사기 피해자가 되면 모든 게 벅차게 느껴질 수도 있습니다. 사기는 누구에게나 일어날 수 있고 지원이 존재함을 기억하는 것이 중요합니다.

만약 여러분이나 여러분이 아는 누군가가 사기를 당했다면 이에 대해 타인과 이야기 나누세요. 가족, 친구, 여러분의 담당의 또는 다음 지원 서비스 중 하나에 지원을 요청할 수 있습니다:

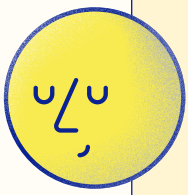
Lifeline: 13 11 14 | lifeline.org.au
또는 온라인 비상 지원 채팅(주 7일, 24시간)

Beyond Blue: 1300 22 4636 | beyondblue.org.au
또는 온라인 채팅(주 7일, 24시간)

Kids Helpline: 1800 55 1800 | kidshelpline.com.au
(주 7일, 24시간)

사기로 인한 재정적 피해는 파괴적이며 삶에 중대한 영향을 미칠 수 있습니다.

재정적 어려움을 겪고 계시다면 국가 부채상담서비스(National Debt Helpline)를 통해 재정 상담사와 상담하실 수 있습니다.
1800 007 007번(월요일 ~ 금요일, 오전 9:30 ~ 오후 4:30)
또는 실시간 채팅(월요일 ~ 금요일, 오전 9:00 ~ 오후 8:00)



scamwatch.gov.au