# 신용사기를 피하는 방법

CommBank는 신뢰와 보안을 최우선 사항으로 다룹니다. 요즘 당사 고객들이 사기꾼의 압박이나 속임수에 넘어가 그들에게 돈을 송금하는 사례가 증가하고 있습니다. 이러한 사기 행각은 교묘하고 다양한 형태로 나타날 수 있습니다. 의심스러운 점이 발견되면 계속 주시하면서 저희에게 알려주시는 것이 중요합니다. 스스로를 보호하고 신용 사기를 신고하는 방법에 대해 자세히 알아보시려면 **commbank.com.au/safe**를 참조하십시오.

## 인증 및 확인

- CommBank 앱에서 보안 점검을 완료하세요.
- 신원 증명 시 추가 확인이 요구되는 다단계 인증절차를 사용하도록 설정하세요.
- **CallerCheck**을 사용하여 은행에서 거는 전화라고 주장하는 발신자의 신원을 확인하세요.
- 지점에서는 **CustomerCheck**을 사용하여 은행 직원에게 본인임을 인증해주세요.
- 첫 결제의 계좌 정보가 올바르게 보이지 않은 경우, **NameCheck**가 확인을 요구할 것입니다.

## 기기 및 결제 보안

- 바이러스 백신 소프트웨어를 최신 상태로 유지하고 일반적인 위험으로부터 여러분의 컴퓨터를 보호하세요.
- 카드를 탭하거나 삽입하는 등의 안전한 결제 방법을 사용하세요.
- 여러분의 디지털 지갑 사용이 가능한 기기는 공유하지 마세요.

## 비밀번호 및 개인 정보

- 비밀번호나 핀을 공유하지 마시고, 개인정보를 공유할 경우 주의를 기울이세요.
- CommBank 직원을 포함하여 누구에게도 NetCode를 알려주지 마세요.
- 여러분의 비밀번호는 NetBank 및 CommBank 앱에서 언제든지 변경할 수 있습니다.
- 강력한 비밀번호를 만들고 정기적으로 변경하세요. 비밀번호 생성에 대한 조언은 commbank.com.au/password-security를 참조하세요.

## 이메일, SMS 및 온라인

- 의심스러운 이메일이나 SMS에 포함되어 있는 링크는 누르지 마세요.
- 메시지 내용이 의심스럽다면 신뢰할 수 있는 사람과 상의하거나 공식적인 연락처를 통해 해당 기관에 직접 문의하세요.
- 제3자가 보낸 자동 전화, 의심스러운 전화, 협박성 전화는 바로 끊으세요.
- 소셜 미디어 및 온라인 플랫폼 이용시 모르는 연락처에 주의하세요.

## 멈추세요. 확인하세요. 거부하세요.

**멈추세요.** 뭔가 이상하다고 생각되십니까? 의심스럽다면 멈추는 것이 가장 좋습니다. 심호흡을 하세요.
**확인하세요.** 신뢰할 수 있는 사람과 상의하거나 공식 연락처를 통해 해당 기관에 직접 문의하세요.
**거부하세요.** 전화를 끊고, 이메일을 삭제하고, 해당 전화번호를 차단하세요. 여러분의 비밀번호를 변경하세요.

신용 사기의 피해를 당했다는 생각이 들 경우, 즉시 CommBank에 **13 22 21**번으로 전화하시거나, 해외의 경우 **+61 2 9999 3283**번으로 전화하세요.

영어가 모국어가 아닌 경우, 호주 정부의 무료 통번역 서비스를 통해 당사와 소통하실 수 있습니다. 이 서비스는 150개 이상의 언어로 제공됩니다. 당사에 전화하시거나 지점을 방문하시면 이 서비스를 주선해드릴 수 있습니다.





Commonwealth Bank

발행일 01/06/2024

# 일반 신용 사기에 대한 중요 정보

## 투자 (암호화폐 포함)

사기범들은 종종 암호화폐 또는 기타 투자 기회에 대한 고수익을 약속하며 사람들을 유혹합니다. 사기범은 전화, 이메일 또는 소셜 미디어 플랫폼을 통해 연락을 시도할 수도 있습니다.

### 자신을 보호하기 위한 팁:

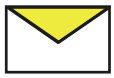
- 진짜라고 믿을 수 없을만큼 좋게 들린다면, 가짜일 가능성이 높습니다.
- 원하지 않은 제안을 하거나, 투자를 하라거나 서두르라는 압박을 준다면 주의하세요.
- 우선 ASIC 웹사이트에서 해당 회사나 브로커가 합법성을 갖추고 있는지 확인하세요.

## 원격 접근

사기범이 신뢰할 수 있는 회사나 기관을 사칭하며 전화를 걸어 여러분의 계좌나 기기에 대해 접근 권한을 얻으려고 시도하는 경우.

### 자신을 보호하기 위한 팁:

- 전화를 통한 제3자의 요청이나 압박에 따라 원격 접근 소프트웨어를 다운로드 하지 마세요.
- 여러분은 언제든지 해당 기관의 공식 웹사이트에 기재된 공식 연락처로 확인 전화를 하실 수 있습니다.
- CommBank 직원이라고 주장하는 사람으로부터 전화를 받는 경우, 여러분은 언제든지 앱 안에 있는 CallerCheck 기능을 통해 해당 전화의 진위성 확인을 요청하실 수 있습니다.



## 비즈니스 이메일 침해

사기범은 침해된 주소에서 보낸 이메일 또는 비서, 고객, 변호사, 관리자, 공급업체 등 여러분이 신뢰할 수 있는 대상이 보낸 것처럼 꾸민 이메일을 사용하여 사업체를 겨냥할 수 있습니다.

### 자신을 보호하기 위한 팁:

- 첫 결제를 하거나 결제 세부 정보를 변경하기 전에 먼저 해당 기관의 공식 연락처로 전화하여 세부 사항을 확인하세요.
- 결제 시 NameCheck 기능을 사용하여 계좌 이름이 제공된 BSB 및 계좌번호와 일치하는지 확인하세요.
- 직원들이 피싱 시도를 알아차리고 신고하도록 교육하세요.

## 피싱 및 스미싱

사기범들은 가짜 웹사이트로 연결되는 링크를 포함하거나 민감한 개인 정보를 요구하는 사기성 이메일이나 문자를 사용합니다.

### 자신을 보호하기 위한 팁:

- 의심스러운 이메일이나 SMS에 포함된 링크는 누르지 마세요.
- 메시지의 진위 여부는 해당 기관의 공식적인 연락 방법을 통해 직접 연락하여 확인하실 수 있습니다.
- CommBank로부터 받은 의심스러운 메시지는 hoax@cba.com.au로 신고하세요.

# 일반 신용 사기에 대한 중요 정보

## 관계

사기범들은 가짜 프로필을 만들어 관계를 형성한 다음 피해자가 돈이나 개인 정보를 보내도록 유도합니다.

### 자신을 보호하기 위한 팁:

- 신뢰할 수 없는 사람에게 돈을 보내거나 비밀번호, 신용카드 또는 계좌 정보를 그들과 공유하지 마세요.
- 구글이나 소셜 미디어 앱을 통해 여러분의 잠재적 파트너에 대해 온라인으로 검색해보세요. 이미지 역방향 검색을 통해 여러분에게 발송된 사진을 다른 사람이 소유하고 있는지 확인하세요.
- 가족이나 친구에게 여러분이 온라인으로 형성한 관계에 대해 이야기하세요. 가족이나 친구는 자신들의 관점을 제시하여 여러분이 미처 알아차리지 못한 경고 징후들을 파악할 수도 있습니다.

## 온라인 쇼핑

사기범은 온라인 상점이나 광고를 제작하여 존재하지 않거나 가짜 제품을 구매하도록 유도합니다.

### 자신을 보호하기 위한 팁:

- 평판이 좋고 안전한 웹사이트에서만 쇼핑을 하고, 너무 좋아보이는 제안에 주의하세요.
- 안전한 결제 수단을 사용하고 판매자에게 직접 송금하는 것을 피하세요.
- 서두르지 마시고, '한정 세일' 또는 세일 종료 ' 임박' 등에 압박을 받지 마세요.

## 채용 기회

거의 또는 전혀 노력하지 않고도 높은 금전적 이득을 얻을 수 있거나 빠르게 돈을 벌 수 있다고 약속하는 일자리 제안.

### 자신을 보호하기 위한 팁:

- 공식 채널을 통해 해당 회사 및 제안을 확인하고, 해당 회사에 대한 조사를 통해 그 회사가 합법적이고 현재 거래 활동을 하는지 여부를 확인하세요.
- 전혀 모르는 사람이나 회사로부터 소셜 미디어, 암호화된 채팅, 이메일, 전화, 편지 등을 통해 오는 일자리 제안에 주의하세요.
- 합법적인 회사는 선불을 요구하거나 회사 자금이나 거래를 위해 여러분의 개인 은행 정보를 사용하지 않습니다.

## 협박 및 처벌

사기범은 당국이나 신뢰할 수 있는 기관을 사칭하여 벌금이나 법적 조치 등의 협박을 통해 돈을 갈취합니다.

### 자신을 보호하기 위한 팁:

- 협박전화를 받으면 전화를 끊고 해당 기관에 직접 문의하세요.
- 합법적인 기관은 기프트 카드나 스토어 카드, iTunes 바우처, 전신 송금 또는 비트코인과 같은 비정상적인 방법으로 결제를 요청하지 않습니다.
- 안전이 염려된다면 경찰 지원 서비스에 연락하세요.