



자신을 안전하게 지키십시오. 사기와 속임수를 조심하십시오.

COVID-19 를 주제로 한 사기와 속임수가 앞으로 몇 달 동안 증가할 가능성이 있습니다.

사기꾼들은 가짜 이메일, 전화나 문자 메시지를 이용하여 개인 정보를 수집하려고 시도합니다. 그들은 귀하의 은행, 세계 보건 기구(WHO), 정부, 자선 단체나 여행사와 같은 합법적인 사업체, 전기, 전화나 인터넷 공급자 혹은 지역 슈퍼마켓인 것처럼 가장을 합니다.



자신을 보호하십시오.

귀하의 은행은 어떠한 은행 계좌나 금융 정보를 요구하는 이메일이나 문자 메시지를 절대로 보내지 않습니다. 여기에는 전화, 모바일 혹은 인터넷 뱅킹을 위해서 주소나 로그인 정보를 갱신하는 것을 포함합니다.

정부와 그 외의 합법 기관에서는 링크를 클릭하여 세부 정보를 갱신하라고 절대로 요구하지 않습니다. 의심이 가는 경우에는, 친구나 가족의 일원과 이야기 하거나 해당 기관에 직접 연락하여 문의하시기 바랍니다.

모르는 사람으로부터 개인 정보를 요구하는 전화를 받으시면, 끊어버리십시오. 해당 회사에 직접 전화하셔서 전화한 것이 맞는지 확인하시기 바랍니다.

본인이 모르는 사람이나 기관으로부터 온 첨부 파일은 절대로 열지 마십시오. 사실이라고 믿기에는 너무 좋게 들리거나 너무 많은 정보를 요구하는 제안은 항상 조심하십시오.



귀하의 은행이 도와줄 수 있으니, 다음의 경우에는 즉시 연락하십시오.

- 사기 전화, 이메일이나 문자에 대한 응답으로 여러분의 은행 정보를 공유한 경우
- 실수로 어떤 링크를 클릭하거나 어떤 첨부 파일을 다운로드 한 경우
- 귀하의 계좌에서 어떤 비정상적인 거래를 발견한 경우



사기를 발견하는 방법

- 주소, 생년월일, 은행 계좌 정보, 세금 파일 번호나 PIN 혹은 비밀 번호를 포함한 개인 정보를 업데이트 하거나 확인하기를 요구하는 경우
- 의심스럽게 보이는 링크가 포함된 이메일이나 문자 메시지 확실하지 않은 경우에는 친구나 가족 일원의 도움을 청하십시오.
- 즉시 입금이나 선불 보증금을 요구하는 경우
- 사실이기에는 너무 좋게 들리는 제안의 경우에도 가능성이 있습니다.
- 이메일 주소가 해당 회사와 일치하지 않는 경우
- 발신자가 컴퓨터를 원격으로 접속하도록 요청한 경우



사기와 속임수로부터 귀하의 재정 정보를 보호하기 위한 최고의 조언



· 의심스러운 전화는 끊고 대신에 그 회사의 웹사이트를 찾아보시거나 전화 번호를 찾아서 바로 연락해보십시오.



· 비밀번호나 PIN은 절대 공유하지 마십시오. 비밀번호로 기기를 보호하십시오. 컴퓨터를 공유하여 사용하는 경우에는 비밀번호를 절대로 저장하지 마시고 항상 귀하의 계정에서 로그아웃을 하십시오.



· 은행 계좌를 정기적으로 확인하여야 의심스러운 거래를 재빨리 찾아냅니다.



· 구매를 하기 위해 카드를 판독기에 넣지 마십시오. 카드를 대거나 끼워 넣는 것이 흔히는 더 안전합니다.



· 신용 카드의 현금 서비스를 차단하십시오.



· 귀하의 계정을 보호할 수 있는 최선책에 대해서 은행에 문의하십시오.



· 사기를 당했다고 생각하시면, 은행에 즉시 보고하십시오.



사기꾼이 여러분에게서 훔칠 수 있는 방법은 많으며, 여기에 주요한 방법들이 있습니다.

피싱 - 은행, 자선 단체나 정부와 같은 신뢰할 수 있는 출처에서 온 것처럼 속여서 개인 정보를 얻기 위해서 이메일이나 문자를 사용하는 방법 메시지는 실제인 것처럼 보이며 가짜 웹사이트에 개인 정보를 입력하라고 흔히 요구하거나 귀하에게 링크를 클릭하라고 할 것입니다. 그러면 사기꾼이 귀하의 컴퓨터와 개인 정보에 접속하게 됩니다.

온라인 쇼핑 사기 - 사기꾼들은 가짜 웹사이트나 순수한 소매 사이트에서 가짜 광고로 실제적인 온라인 스텝인 척 합니다. 가짜 온라인 쇼핑 사이트는 머니 오더, 전신 송금, 국제 자금 이체나 기프트 카드 같은 특이한 지불 방법을 종종 요구할 것입니다.

투자 사기 - 사기꾼은 증권 중개인 혹은 재정이나 투자 조언을 하는 포트폴리오 관리자라고 주장합니다. 실제일 수 있거나 아닐 수도 있는 투자 기회에 돈을 넘기라고 요구할 것이며 그 후에 그들은 귀하의 돈을 보관할 것입니다.

원격 접속 사기 - 사기꾼은 귀하의 컴퓨터나 인터넷 접속에 문제가 있다고 하거나 악성 코드에 감염되었다고 할 것입니다. 그들은 귀하에게 애플리케이션을 설치하도록 설득하거나 귀하의 컴퓨터에 접속하려고 노력할 것입니다. 이를 이용하여 귀하의 개인 정보에 접속하거나 문제를 해결하기 위해 '수수료'를 요구할 것입니다.

관계 및 데이트 사기-사기꾼은 돈이나 선물을 빼내기 위해서 귀하와 관계를 맺습니다. 그들은 시간이 가면 관계를 발전시키고 귀하에게 자산을 그들 이름으로 전환하거나 귀하의 유산의 수혜자가 되도록 하라고 요구합니다. 흔히는 건강, 여행이나 가족 문제를 해결하기 위해 돈을 요구할 것입니다.

유용한 링크:

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

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

www.scamwatch.gov.au/