

# 사기를 당한 경우 해야 할 일



Korean



사기꾼이라고 생각되는 사람에게 돈을 지불했거나, 개인정보를 알려주었거나, 상대방에게 컴퓨터나 전화에 액세스할 수 있는 권한이 있는 경우, 어떻게 해야 하는지 알아보십시오.

사기꾼은 그럴듯하게 포장을 합니다. 사기꾼은 돈이나 사회 보장 번호 또는 계좌 번호 같은 민감한 개인정보를 얻어내기 위해 전화, 이메일, 문자 메시지를 보냅니다. 그리고 사기꾼은 사기에 능숙합니다. 사기꾼이라고 생각되는 사람에게 돈을 지불했거나, 개인정보를 알려주었거나, 상대방에게 컴퓨터나 전화에 액세스할 수 있는 권한이 있는 경우에는 다음과 같이 하십시오. 사기꾼에게 돈을 지불했다면 이미 돈이 없어졌을 수 있습니다. 지불 방법에 관계없이 항상 송금할 때 이용한 회사에 돈을 돌려받을 수 있는 방법이 있는지 물어보는 게 좋습니다.

## 사기꾼에게 돈을 지불한 경우

<p>신용 카드나 직불 카드로 결제를 하셨습니까?</p>	<p><a href="#">신용카드</a> 또는 <a href="#">직불카드</a>를 발급한 회사나 은행에 문의하십시오. 부정 사용된 사기 청구라고 말하십시오. 송금을 취소하고 돈을 돌려달라고 요청하십시오.</p>
<p>사기꾼이 은행 계좌에서 무단으로 자금을 이체했습니까?</p>	<p>은행에 연락하여 <a href="#">무단 대출</a> 또는 <a href="#">인출</a>이라고 말하십시오. 송금을 취소하고 돈을 돌려달라고 요청하십시오.</p>
<p>기프트카드로 결제하셨습니까?</p>	<p><a href="#">기프트 카드</a>를 발행한 회사에 문의하십시오. 사기에 사용되었다고 말하고, 돈을 돌려달라고 요청하십시오. 기프트카드와 기프트카드 영수증을 보관하십시오.</p>
<p>Western Union 또는 MoneyGram 같은 회사를 통해 전신 송금을 보내셨습니까?</p>	<p><a href="#">전신송금 회사</a>에 문의하십시오. 사기 송금이라고 말하십시오. 전신 송금을 취소하고 돈을 돌려달라고 요청하십시오.</p> <ul style="list-style-type: none"> <li>• MoneyGram, 1-800-926-9400</li> <li>• Western Union, 1-800-448-1492</li> <li>• Ria(Walmart 이외 송금), 1-877-443-1399</li> <li>• Ria(Walmart2Walmart 및 Walmart2World 송금), 1-855-355-2144</li> </ul>
<p>은행을 통해 전신 송금으로 돈을 보내셨습니까?</p>	<p>은행에 연락하여 사기 이체를 신고하십시오. 전신 송금을 취소하고 돈을 돌려달라고 요청하십시오.</p>
<p>송금 앱을 사용해 돈을 송금하셨습니까?</p>	<p>사기 거래를 <a href="#">송금 앱 회사</a>에 신고하고 결제를 취소해달라고 요청하십시오. 앱을 신용 카드 또는 직불 카드와 연결해 놓은 경우, 신용 카드 회사 또는 은행에 사기를 신고하십시오. 청구를 취소해달라고 요청하십시오.</p>

<p>가상화폐로 지불하셨습니까?</p>	<p>암호화폐 지불은 일반적으로 되돌릴 수 없습니다. 암호화폐로 지불하면 해당 지불액을 받은 사람이 돌려줘야만 돈을 돌려받을 수 있습니다. 그러나 돈을 보낼 때 사용한 송금 회사에 연락하여 사기 거래라고 밝히십시오. 가능하면 해당 거래를 취소해달라고 요청하십시오.</p>
<p>현금으로 지불하셨습니까?</p>	<p>미국 우편을 통해 현금을 보낸 경우 미국 우편검열국에 877-876-2455으로 연락하여 소포를 막도록 요청하십시오. 이 절차에 관한 자세한 내용은 <a href="#">USPS Package Intercept: The Basics</a>를 참조하십시오.</p> <p>다른 배송 서비스를 사용했을 때는, 최대한 빨리 연락을 취하십시오.</p>

### 사기꾼에게 개인정보를 알려준 경우

<p>사기꾼에게 사회 보장 번호를 알려주셨습니까?</p>	<p><a href="#">IdentityTheft.gov</a> 로 이동하여 신용 모니터링 방법을 포함해 어떤 조치를 취해야 하는지 확인하십시오.</p>
<p>사기꾼에게 사용자명과 비밀번호를 알려주셨습니까?</p>	<p><b>강력한 새 비밀번호</b>를 만드십시오. 다른 곳에서 같은 비밀번호를 사용하는 경우, 그곳의 비밀번호도 변경하십시오.</p>

### 사기꾼이 컴퓨터 또는 전화기에 액세스할 수 있는 경우

<p>사기꾼에게 컴퓨터에 원격으로 액세스할 수 있는 권한이 있습니까?</p>	<p><b>컴퓨터 보안 소프트웨어</b>를 업데이트하고 검사를 실행한 후 문제로 식별되는 모든 것을 삭제하십시오. 그런 다음 <b>개인정보를 보호</b>하기 위한 다른 조치를 취하십시오.</p>
<p>사기꾼이 휴대폰 번호와 계좌를 관리했습니까?</p>	<p>서비스 제공업체에 연락하여 휴대폰 번호에 대한 관리 권한을 되찾으십시오. 그렇게 한 다음, 계정 비밀번호를 변경하십시오.</p> <p>또한 신용 카드, 은행, 기타 금융 계좌에서 승인되지 않은 청구가 이루어졌는지 혹은 변경된 사항이 있는지 확인하십시오. 그런 일이 발생한 경우, 해당 회사 또는 기관에 신고하십시오. 그런 다음 <a href="#">IdentityTheft.gov</a> 에 접속하여 취해야 할 다른 조치를 확인하십시오.</p>

### FTC(연방거래위원회)에 사기 신고하기

사기를 신고하면, FTC(연방거래위원회)는 해당 정보를 사용하여 사기꾼에 대한 사례를 구축하고, 동향을 파악하고, 대중을 교육하고, 커뮤니티에서 일어나는 일에 대한 자료를 공유할 수 있습니다. 사기를 당했거나 사기를 발견한 경우, FTC에 [ReportFraud.ftc.gov](#) 를 통해 신고하십시오.



**FEDERAL TRADE COMMISSION**

십월 2022

[ftc.gov/exploredata](#) 를 방문하여 귀하의 주 또는 도시 지역에 무슨 일이 일어나고 있는지 확인할 수 있습니다.