

몽고메리카운티 소비자 보호 사무소

명절은 즐거움 이상의 것을 불러옵니다.

바로... 사기꾼들입니다.

2020년 11월 2일

연말연시가 다가오고 있습니다. 판데믹으로 기존의 사기 행각이 변형된 형태로 기승을 부리고 있으며 명절이라고 예외는 아닙니다. 빈 기프트 카드, 자선 모금 사기, 사이버 공격 및 택배 짹쓸이 절도는 연말연시에만 일어나는 일은 아닙니다. 온라인 거래와 통신수단에 크게 의존한 2020년도는 불편한 한해였고 이로 인해 올해는 더 많은 소비자가 피해를 볼 것으로 기대합니다. 이번 명절을 안전하게 보내기 위해 따라야 할 몇 가지 조언을 알려 드립니다:

- **온라인 쇼핑**

연방거래위원회에 따르면 대부분의 온라인 구매에 대해 추가 보호를 제공하는 신용카드로 지급하는 것이 가장 안전하다고 합니다. 또한, 신용카드는 반품 또는 교환할 때 발생하는 분쟁 조치 및 혜택을 제공합니다. Visa 또는 Mastercard 로고가 있는 데빗카드는 신용카드와 동일한 보호 및 분쟁 조치를 제공하지 않습니다.



Craigslist, Facebook Marketplace, Letgo 또는 다른 온라인 직거래 장터에서 물건을 사는 경우 사기꾼도 당신을 속이려 이런 사이트를 이용하고 있다는 점에 유의하십시오. 범죄자들은 실제 상품 사진 및 같은 상품의 다른 거래 사진을 사용하여 존재하지 않는 상품을 판매하고 심지어는 대여까지 합니다. 믿을 수 없을 정도로 좋은 조건의 거래이거나 물건을 보기



공정 거래 확립

• • •

사기 범죄의 피해자이거나 판매자의 고객 서비스에 대한 분쟁이 있는 경우 소비자 보호 사무소에 문의하십시오.

100 Maryland Avenue
Suite 3600

Rockville, MD 20850

대표: 240.777.3636

한국어서비스: 240.777.3759

제보: 240.777.3681

Fax: 240.777.3768

이메일:

Consumer@MontgomeryCountyMD.gov

이곳을 클릭하여 온라인으로 불만을 제기하십시오.



전에 디지털 결제 또는 기프트 카드를 보내라고 하면 사기를 당하고 있다는 신호입니다. 귀하가 판매자일 때 사기꾼은 고의적으로 귀하가 원하는 가격보다 더 많은 금액을 부도수표로 냅니다. 그리고 금액의 차액을 당신의 수표로 그 사람한테 보내라고 합니다. 이것이 바로 수표 사기의 수법입니다.

마지막으로, 올해는 유난히 존재하지 않는 상품을 판매하는 [가짜 소매 웹 사이트가](#) 증가했습니다. 이들은 Shopify를 플랫폼으로 사용하고 소셜 미디어에 광고합니다. 이러한 사이트는 위조품 또는 존재하지 않는 상품을 판매합니다. 또한, 이들은 은행을 통한 지불 거절 또는 분쟁을 방지하기 위해 물품을 보내는 대신 배달 증명을 첨부한 빈 봉투를 보내기도 합니다. Forbes에 따르면, 사기의 한 가지 특징은 특이한 이름을 사용하는 수많은 다른 사이트를 찾아 다른 특이한 이름을 사용하여 동일한 광고, 사진 및 거래를 유도하는 것입니다. 예를 들면 Geoghost라는 사이트에서 할인가에 판매하는 운동기구를 똑같은 방식으로 Predictfuture라고 하는 사이트를 개설해 사기의 피해자를 유도하는 것입니다.

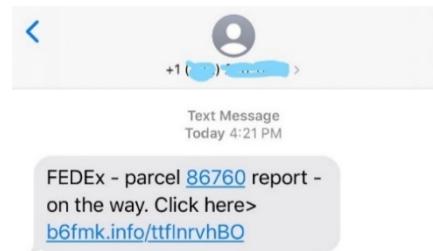
• 기프트 카드(Gift Card)

이러한 카드는 매우 유용하고 편리한 선물입니다. 하지만 기프트 카드가 사실상 추적이 불가능하다는 것을 알고 있는 범죄자에게는 가장 좋은 목표물입니다. 누군가 미납 청구서에 대해 연락하여 기프트 카드나 선불카드 또는 전신 송금을 통해 지급을 요구하는 경우 사기가 진행되고 있다는 위험 신호입니다. 기프트 카드를 구매할 때 포장이 훼손되지 않았는지 확인하세요. 카드 뒷면에 있는 바코드가 보이게 포장된 기프트 카드는 사지 마세요. [CNBC](#)가 보고한 AARP 설문 조사에 따르면 소비자 5명 중 1명은 기프트 카드가 비어 있다고 답했습니다. 범죄자는 빈 기프트 카드 정보를 저장 및 등록하고 카드가 활성화되었다는 알림을 기다린

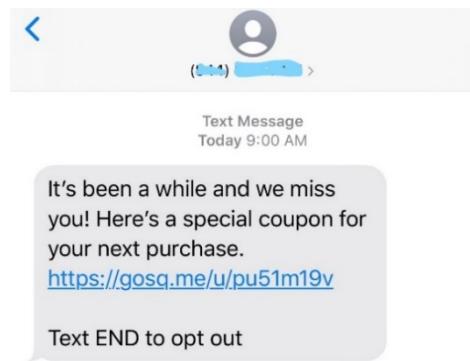
후 기프트 카드를 선물하기도 전에 카드에 충전된 금액을 빼냅니다. CNBC는 역시 온라인 경매 사이트를 통해 판매된 기프트 카드가 종종 도난당한 카드라고 보고합니다. [기프트 카드](#) 사용에 대한 자세한 내용은 저희 웹사이트를 참조하십시오.

• 사이버 보안

피싱(Phishing) 및 스미싱(Smishing)을 통한 사이버 공격은 초가을부터 시작된 배송 지역에 대한 거짓 문자 메시지를 보내는 방법입니다.



또는 귀하의 관심을 사려고 정체불명의 판매자 할인권을 보내기도 합니다.



이러한 메시지를 받았을 때 보낸 사람의 주소를 보면 이상하지는 않습니까? 우체국(USPS)에서 귀하에게 .biz 또는 .net 주소로 이메일을 보내나요? FedEx로 연결된 문장이 실제 FedEx의 웹사이트 같지 않은 이상한 웹 주소로 연결되어 있습니까? 소셜 미디어 또는 기타 통신 앱 플랫폼을 통해 받은 원치 않는 이메일, 문자, 채팅을 클릭하지 마세요. 이러한 것으로 귀하를 사기 치거나 언젠가

신분도용에 사용할 귀하의 계정과 이메일 액세스 정보를 훔치는 바이러스 또는 악성 코드를 설치합니다. [피싱, 스미싱 및 파밍에 대한 자세한 내용은 저희 웹사이트를 참조하십시오.](#) (참고 설명: 1. 피싱-전자우편 또는 메신저를 사용해서 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장함으로써 기밀 정보를 훔침, 2. 스미싱-문자메시지에 포함된 인터넷주소를 클릭하면 악성 코드를 설치해 기밀 정보를 훔침, 3. 파밍(Pharming)-사용자가 자신의 웹 브라우저에서 정확한 웹 페이지 주소를 입력해도 가짜 웹 페이지에 접속하게 하여 개인 기밀 정보를 훔침.)

- **택배 싹쓸이 절도**

택배 싹쓸이 절도는 [새로운 형태의 도둑질입니다.](#) 이 범죄는 상점에서 물건을 훔치는 대신 당신의 현관 앞에서 훔칩니다. 한 [보고서](#)에 따르면 2019년 소비자의 36%가 적어도 하나 이상의 배송을 도난당했다고 보고했습니다.



택배 싹쓸이 절도의 피해를 막는 방법으로는 빨리 회수할 수 있게 온라인에서 배달 현황을 추적하거나 직장 주소로 배달 또는 매장 내 픽업을 사용하는 방법이 있으며 현관에 도둑이 숨어하는 보안 카메라, 스팟라이트 또는 잠금 박스를 설치하십시오. 물건을 도난당한 경우 판매자 및 배송 업체에 즉시 배상을 청구하십시오.

- **우편물 약탈자**

연말연시에 많은 주민이 연하장과 함께 동봉한 수표나 기프트 카드를 보내려 집 앞 우편함을 사용하지만, 우편함의 깃발을 올리는 순간 훔칠 수 있는 우편물이 있다고 도둑에게 알려주는 격이 됩니다.



[훔친 우편물](#)로 “변조 수표” 즉 수취인을 본인으로 바꾸거나 동일 계좌번호를 사용하여 위조 수표를 인쇄합니다. 우편물을 우체국으로 직접 가져가거나 파란색 우체통에 넣으십시오.

- **기부**

자선 활동과 모금 활동은 연말연시에 증가합니다. 자선 단체에 기부하시기 전에 [사기성 자선단체](#)가 아니라 [메릴랜드주 사무국](#)에 등록된 올바른 자선 단체인지 확인하십시오.



그러고 나서, 받은 기부금이 업무의 용도인지 아니면 더 많은 기부를 받으려고 콜센터 인원을 고용하는 데 사용하고 있는지 조사해 보십시오. 조사에 도움이 되는 몇 군데 단체를 알려 드립니다.

[Charity Navigator](#), [Guidestar](#), [Charity Watch](#), [Give.org](#)

- **결론**

연말연시를 사고 없이 보내려면 끊임없는 고심이 필요합니다. 저희 웹 사이트를 참조하시면 [연말연시](#)

쇼핑에 대한 자세한 정보와 조언, 또는 반품 및 교환에 관한 메릴랜드 법률, 또는 신용 카드나 데빗카드 대신 디지털 결제 앱 사용과 같은 기타 관련 정보를 얻으실 수 있습니다.

