즉시 배포용: 2022년 3월 22일 KATHY HOCHUL 주지사

HOCHUL 주지사, 러시아의 우크라이나 침공으로 인한 사기 및 사이버 보안 위협에 대해 소비자 경고

도움을 필요로 하는 우크라이나인을 돕기 위해 기부금을 사용하는 검증되고 평판 좋은 단체에 기부

뉴욕주 당국에서는 민감한 정보를 보호하고 보안을 강화하고 사이버 위협이 강화될 때 주의를 기울이기 위한 권고 사항을 발표

오늘 Kathy Hochul 주지사는 뉴욕 시민들에게 블라디미르 푸틴의 우크라이나 침공과 관련하여 자선 사기 및 사이버 보안 위협 증가에 대한 소식을 전했습니다. 뉴욕주 소비자 보호국(New York State Division of Consumer Protection)은 전쟁 희생자를 지원하기 위해 자선 구제 자금을 사기로 요청한 사실을 알게 되었습니다. 소비자들은 돈이나 물품을 기부하기 전에 모든 금전 요청을 신중하게 평가하고 자선 단체를 확인하는 것이 좋습니다. Hochul 주지사는 뉴욕주민들이 세무 재무부의 보안 권고를 활용해 사이버 보안 위협이 증가하는 가운데 민감한 정보를 온라인에 공개할 경우 한치의 경계도 늦추지 말 것을 권고하고 있습니다. 주지사는 합동 보안 운영 센터(Joint Security Operations Center, JSOC), 창설을 발표했습니다. 이 기관은 지역, 주 및 연방의 사이버 능력을 통합하는 본부입니다.

"뉴욕은 미국에서 가장 많은 우크라이나 인구가 거주하고 있으며, 뉴욕주민들은 항상 도움이 필요한 사람들을 돌보는 데 도움의 손길을 내밀고 있다"고 **Governor Hochul는 말했습니다.** "그러나 다른 사람의 친절을 이용하여 사기를 치려는 자들을 조심해야 합니다. 우크라이나 친구와 가족을 돕기 위해 기부자의 관대한 마음을 이용하려는 의심스러운 점이 보인다면, 그럴 수 있다는 사실을 기억하십시오. 친구와 가족, 특히 연로한 가족이 온라인에서 경계를 늦추지 않게 하십시오."

재해가 발생할 때마다 사기꾼들은 도움을 청하는 자들의 마음을 노립니다. 우크라이나 침공은 사기꾼들이 가짜 자선 단체를 설립하거나 강력한 전쟁 희생자로 가장할 수 있는 기회를 보입니다. 어떤 이들은 순진한 기부자의 돈 및/또는 개인 정보를 훔치기 위해 합법적 자선 단체의 공식 사이트를 모방하도록 웹사이트를 설계합니다.

Robert J. Rodriguez 국무장관은 다음과 같이 말했습니다. "뉴욕주민들은 도움을 필요로 하는 사람들을 지지하고 호의를 베풀기로 유명합니다. 우크라이나 전쟁이 계속되면서 사기꾼들이 계속해서 소비자를 속이기 위해 감정적인 책략과 가짜 권유를 사용하여 나타날 것입니다. 저는 뉴욕주민들이 자신들의 착한 의도를 보호하고 힘들게 번 돈이 여러분의 지원을 절실히 필요로 하는 이들에게 전달될 수 있도록 기부 전에 항상 해당 자선 단체가 정식 단체인지 조사할 것을 권장합니다."

Amanda Hiller 조세재무국장 대행은 다음과 같이 말했습니다. "우크라이나의 글로벌 위기로 인해 사이버 공격에 대한 우려가 높아졌습니다. 따라서 우리는 기밀 정보가 잘못된 손에 넘어가거나 서비스 거부 공격 및 기타 부정적인 결과가 발생하지 않도록 주의해야 합니다."

정보 기술 서비스 사무국(Office of Information Technology Services) CIO Angelo 'Tony' Riddick은 다음과 같이 말했습니다, "가장 선한 의도를 품은 수많은 뉴욕주민들이 우크라이나 국민을 지원하기 위해 자선 단체에 기부했고, 그들은 변화를 이뤄내고 있습니다. 안타깝게도, 이러한 관대함은 사이버 범죄자들이 악용할 수 있는 새로운 기회를 낳습니다. 자신을 보호하고 관대한 기부가 항상 도움이 진정으로 필요한 사람들에게 전달되도록 하기 위해 ITS는 뉴욕주민들에게 이러한 모범 사례를 따르고 최근의 온라인 위협 및 사이버 사기에 대해 경계할 것을 촉구합니다."

국토안보 비상 서비스부(Division of Homeland Security and Emergency Services) 장관 Jackie Bray는 이렇게 말했습니다. "모든 뉴욕주민들은 개인 정보를 보호하고 사이버 위협으로부터 자신을 보호할 경우 해야 할 역할이 있습니다. 우리는 도움이 필요할 때 악한 가해자가 도움을 주려는 사람들을 이용하려고 한다는 것을 알고 있습니다. 온라인 또는 디지털 기부를 통해 우크라이나 국민을 지원하려는 경우 경계를 늦추지 않고 다음 모범 사례를 따라 기부가 확실하고 정보가 안전하게 유지되도록 하십시오."

Kevin Thomas 주 상원의원은 다음과 같이 말했습니다. "많은 뉴욕주민들이 우크라이나 국민을 돕기 위해 행동을 취했다는 것은 우리 이웃의 이야기입니다. 안타깝게도, 이런 선행은 사기꾼들에게 이 위기를 자신들의 사적 이득을 위해 악용할 수 있는 절호의 기회를 낳았습니다. 저는 뉴욕주민들이 경계를 늦추지 않고 그들의 관대한 기부가 합법적인 대의에 사용되도록 추가 예방 조치를 취할 것을 촉구합니다."

Nily Rozic 하원의원은 이렇게 말했습니다. "사기꾼들은 국제 위기 속에서도 항상 새로운 방법을 시도하여 여러분을 속이려고 합니다. 뉴욕주민들이 도움이 필요한 시기에 우크라이나를 지원하기 위해 모일 때, 소비자들이 귀하의 관대함이 이용되지 않도록 기술과 지식으로 무장하는 것이 중요합니다. 뉴욕주민들이 친절로 인해 사기를 당하지 않도록 해준 Hochul 주지사에게 감사드립니다."

사기꾼들은 종종 소셜 미디어, 광고성 이메일, 전화 통화 또는 문자 메시지를 통해 연락합니다. 사기꾼들은 Cash App, Venmo 또는 Zelle과 같은 결제 앱을 통해 송금하거나 해외 은행 계좌로 송금하거나 선불 기프트 카드를 보내도록 요청할 수 있습니다. 최근의 많은 사기에는 비트코인 또는 이더리움과 같은 암호화폐 기부 요청이 포함됩니다. 사기꾼은 교묘하고 사람들을 속이는 새로운 방법을 계속 강구할 것이기 때문에 소비자는 항상 경계해야 합니다.

기부금이 잘못된 이들의 손에 들어가지 못하도록 하기 위해 뉴욕주 소비자 보호과(New York State Division of Consumer Protection)에서는 다음 예방 조치를 취할 것을 권장합니다.

- **요청을 인증하십시오.** 사기꾼들은 소셜 미디어에서 친구, 가족 또는 연인으로 가장하고 기부를 요청하는 경우가 더 많습니다. 온라인에서 다른 사람의 사진 및 약력을 복사하고 가짜 계정을 만들기는 쉽습니다. 온라인에서 광고성 기부금 구호 요청을 받으면 아는 사람처럼 보여도 다른 통신 연결망을 통해 직접 전화를 걸어 해당 요청이 진짜인지 확인하십시오. 출처를 확인하기 전에 링크를 클릭하거나 양식을 작성하지 마십시오. 최근에 온라인에서 만난 사람에게서 요청이 온 경우 사기일 가능성이 높으므로 특히 주의해야 합니다.
- **자선 단체를 조사하십시오.** 자선단체 웹사이트에만 의존하지 마십시오. 그룹 이름과 "리뷰" 및 "사기"와 같은 검색어를 사용하여 자선 단체에 기부하기 전에 온라인으로 검색하십시오. 연방 거래 위원회(Federal Trade Commission)는 자선 단체에 대한 보고서와 등급을 보려면 give.org, charitynavigator.org,charitywatch.org 또는 candid.org에서 확인할 것을 권장합니다. 국세청(IRS)에서도 자선단체 등록 여부를 확인할 수 있습니다. 법무장관실(Office of the Attorney General)은 자선단체가 재정적으로 건전한지 확인하기 위해 기부 전에 재정 보고서에 대한 자선단체 등록부도 검토할 것을 권고하고 있습니다.
- **고압적인 전술에 넘어가지 마십시오.** 상황이 시급하지만 소비자는 즉시 기부하라는 압력을 받아서는 안 됩니다. 사기꾼들은 종종 즉시 기부하도록 압력을 가하여 위험 신호를 간과하도록 시선을 분산시킵니다. 가슴 아픈 이야기를 이용해 즉시 기부를 요구하는 피해자와 변호사의 다이렉트 이메일을 조심하십시오. 홍보 텔레마케터에게 전화로 돈을 기부하지 마십시오. 대신 전화를 건 사람에게 자선 단체와 기부처에 대한 서면 자료를 보내달라고 요청하십시오.
- **개인 정보를 비공개로 유지하십시오.** 원치 않는 자선 요청에 응하려고 사회 보장 번호, 신용카드 또는 직불카드 번호 또는 기타 개인 신원 정보를 제공하지 마십시오. 온라인으로 기부할 경우, 기부 요청을 따르기 전에 인터넷 연결이 안전한지 확인하십시오.

- **돈을 어떻게 쓸 것인지 물어보십시오.** 소비자들은 자신의 돈이 피해자에게 직접 전달된다는 사실을 알고 싶어합니다. 진정한 자선단체는 관리 수수료가 아닌 프로그램에 직접 기부할 금액을 알려줄 수 있어야 합니다.

- **수표 또는 신용카드로 기부하십시오.** 현금, 기프트 카드, 암호화 통화 또는 추적하기 어려운 입찰을 사용하여 돈을 주지 마십시오. 기부 기록이 있는지 확인할 수 있도록 수표나 신용카드로 기부하십시오. 수표는 개인이 아닌 자선 단체에 보내십시오. 자선단체 웹사이트를 통해 기부하기로 선택한 경우 웹사이트가 안전한지, 컴퓨터에 최신 안티바이러스 보호 기능이 설치되었는지 확인하십시오.

기부금 모금 사기를 당했다고 의심될 경우, 다음 연락처로 뉴욕주 소비자 보호국(New York State Division of Consumer Protection)에 불만을 제기할 수 있습니다: https://dos.ny.gov/file-consumer-complaint.

이 부서의 소비자 지원 상담 전화는 월요일부터 금요일, 오전 8:30부터 오후 4:30까지 1-800-697-1220번으로 연락 가능합니다. 소비자 보호 알림과 최신정보는 소비자 보호국의 소셜 미디어인 트위터(@NYSConsumer) 및 페이스북(www.facebook.com/nysconsumer)에서 팔로우하십시오.

사이버 보안에 대한 국제적 우려가 고조되는 가운데, 뉴욕주 세무 재무부는 납세자들이 세금 시즌 및 연중 내내 개인 정보를 보호하는 데 도움이 되는 일련의 중요한 팁을 공유합니다.

개인 정보를 요구하는 광고성 이메일과 전화에 주의하십시오. 광고성 이메일이나 전화에 응하고자 사회 보장 번호와 같은 개인 정보를 공유하지 마십시오. 이메일이나 전화가 소속 회사에서 발송한 것이라고 명시된 경우 직접 회사에 전화해 해당 연락처가 확실한지 보십시오. 사기꾼들은 종종 세금 부채와 관련된 위협 전술과 위협을 사용하여 개인 및 금융 정보를 공유하도록 합니다.

휴대 기기를 보호하십시오. 알려진 취약점을 패치하는 소프트웨어 업데이트가 제공되는 즉시 적용하십시오. 암호구문 등 기기에 내장된 보안 기능을 사용하고 기기를 분실했거나 도난당했을 경우 데이터를 암호화하고 원격으로 콘텐츠를 제거하는 프로그램을 사용하십시오.

Wi-Fi 핫스팟에 주의하십시오. 공용 무선 핫스팟은 안전하지 않습니다. 즉, 사이버 도둑이 사용자가 연결되어 있는 동안 휴대 기기에서 수행 중인 작업을 쉽게 볼 수 있습니다. 공용 Wi-Fi에서 하는 일을 제한하고 민감한 계정에 로그인하지 마십시오.

본인의 앱 알기. 앱을 다운로드하기 전에 앱의 세부정보와 사양을 철저히 검토하십시오. 각 모바일 앱의 개인 정보 보호 정책을 검토 및 숙지하십시오. 앱에서 사용자의 위치 및 개인 정보에 대한 액세스를 요청할 수 있습니다.

소셜 미디어에서 공유하는 정보에 주의하십시오. 생년월일, 전화번호, 집 주소 또는 직업이나 취미를 나타내는 이미지를 게시하지 마십시오. 한 가지 이유: 이러한 유형의 정보는 비밀번호 재설정에 사용되는 보안 질문에 대한 답변을 결정하는 데 사용될 수 있으며 귀하는 귀하의 계정 및 개인 정보에 액세스하려는 사기꾼의 표적이 됩니다.

강력한 비밀번호 사용. 매 계정마다 다른 비밀번호를 만드십시오. 비밀번호는 현재 업계 표준인 14자 이상의 비밀번호를 사용하십시오. 문자(대소문자), 숫자, 기호를 조합하여 사용하십시오. 기억하기 어려운 문구의 첫 글자를 사용하여 추측하기 어려운 복잡한 비밀번호를 만드는 비밀번호 문구를 고려하십시오. 비밀번호/암호구문을 정기적으로 변경하십시오.

보안 질문을 변경하십시오. 여러 계정에서 동일한 보안 질문을 사용하지 마십시오. 소셜 미디어 또는 인터넷 검색으로 답을 추측하거나 찾을 수 없는 보안 질문을 선택하십시오.

2단계 인증을 사용하여 계정에 액세스하십시오. 온라인 계정의 보안을 강화하기 위해 가능하면 로그인할 때 신원을 확인하기 위해 비밀번호와 추가 보안 코드를 요구합니다.

피싱을 경계하십시오. 링크를 클릭하거나 파일을 다운로드하거나 알 수 없는 발신자가 보낸 이메일의 첨부 파일을 열지 마십시오. 보낸 사람을 알고 있더라도 첨부 파일을 예상하고 포함된 내용을 알고 있을 때만 첨부 파일을 여십시오.

민감한 정보를 보호하는 데 필요한 단계를 정기적으로 검토하는 것이 중요합니다.

신고하십시오. 귀하가 세금 관련 신분 도용의 피해자이거나 피해자일 수 있다고 생각되면 즉시 저희에게 알리십시오. 귀하의 정보를 추적하여 개인 정보를 보호해 드리겠습니다. 조세 부서의 사기, 스캠 및 신원 도용 신고 웹페이지를 방문해서 신고 방법을 확인하세요.

세무 부서는 고급 암호화, 방화벽, 침입 감지 시스템 및 기타 보안 조치를 사용하여 시스템과 민감한 데이터를 보호하지만 납세자는 온라인에서 스스로를 보호하기 위해 사전 예방적 접근 방식을 취해야 합니다.

###

구독 취소