뉴욕 검찰총장 레티샤 제임스
(Letitia James)

친애하는 뉴욕 주민 여러분,

귀하의 신원이 위험합니다. 온라인, 전화, 심지어 대면에서도 사기꾼이 귀하의 개인 정보를 도용하여 사기를 저지르는 것이 그 어느 때보다 더 쉬워졌습니다.

신원 도용은 매년 수백만 명의 사람들에게 영향을 미칩니다. 사기꾼은 귀하의 이름으로 신용 카드를 신청하고, 의료 혜택을 받고, 심지어 소셜 시큐리티 번호를 세무 사기에 이용해 귀하의 신용을 떨어뜨리고 이를 회복하는 시간과 돈을 낭비하게 합니다.

약간의 주의만 기울인다면 귀하의 개인 정보를 보호하고 대부분의 신분 도용을 방지할 수 있습니다. 귀하가 그 방법을 습득할 수 있게 도와드리겠습니다.

신원을 안전하게 지키는 방법 또는 신원이 도난당했다고 생각될 경우 취해야 할 조치에 대한 상세 내용은 웹사이트 ag.ny.gov를 방문하십시오.

감사합니다.

Letitia James

리소스

뉴욕주 법무장관실 소비자 사기 방지국
사기를 신고하거나 불만을 제기합니다.
(800) 771-7755 / ag.ny.gov

미국 연방거래위원회
사기 또는 신원 도용을 신고합니다.
877- 382-4357 / ftc.gov

연례 신용 보고서
신용 보고서를 확인하거나 동결시킵니다.
877-322-8228 / annualcreditreport.com

주요 신용 보고 기관

Experian:
(888) 397-3742 / experian.com

TransUnion:
(800) 888-4213 / transunion.com

Equifax
(800) 685-1111 / equifax.com

Innovis
innovis.com

귀하의 신원을 보호하십시오

본인의 신원을 안전하게 지키는 요령

뉴욕 주 검찰총장 사무소 레티샤 제임스 ***(Letitia James)***

개인 정보 보안

일반적으로 이름이나 전화번호를 제공하는 것이 안전하지만 생년월일, 주민등록번호 또는 계좌 번호를 타인에게 알려주면 신분 도용에 노출될 수 있습니다. 비밀번호를 잊어버렸을 경우에도 웹사이트에 대한 “백업” 답변으로 사용하는 정보를 공개해서는 안 됩니다.

모르는 사람에게서 걸려 온 전화에 본인의 개인 정보를 제공하지 마십시오. 본인이 상대방에게 전화를 건 것이 아니라면 “피싱”을 당할 가능성이 있습니다.

피싱은 피해자가 사용자 이름, 비밀번호 또는 신용카드 번호 등 개인 정보를 발설하게 유도하려는 시도입니다. 사기꾼은 문자, 전화 또는 이메일로 연락할 수 있으며 종종 정부 기관, 은행 또는 유명 업체로 가장합니다. 사기꾼들은 어떤 문제나 긴급 상황을 해결하기 위해 귀하의 개인 정보를 요구하거나 귀하에게 무언가를 제공하기 전에 “정보 확인”만 하면 된다고 말합니다.

이러한 조직 중 어느 곳에서도 실제로 중요한 정보를 얻기 위해 이런 방식으로 귀하에게 연락을 취하지 않습니다. 확실히 잘 모를 경우, 게시된 번호를 사용해 회사에 전화를 걸어 그것이 실제 번호인지 확인하십시오. 일부 피싱 시도는 웹 사이트로 이동하거나 첨부 파일을 열라고 말합니다.**첨부 파일을 다운로드하거나 본인도 모르는 사람의 링크를 클릭하지 마십시오.** 여기에는 컴퓨터를 감염시키고 개인 정보를 훔치는 바이러스가 포함되었을 수 있습니다.

의심스러운 메시지

메시지가 친척이나 유명 업체 등 신뢰할 수 있는 출처에서 온 것처럼 보이더라도 여전히 피싱 시도일 수 있습니다. 사기꾼들은 계정을 도용하거나 비슷한 이름으로 새 계정을 만들 수 있습니다. 메시지 내용이 보낸 사람의 어조가 아닌 것 같거나, 메시지에 설명 없이 링크나 첨부 파일만 포함되었거나, 의심스러운 메시지처럼 보일 경우, “보낸 사람” 필드를 다시 확인하여 올바른 주소인지 확인하거나 보낸 사람에게 전화하여 실제 발신자인지 확인하십시오. 이것은 이메일이나 문자를 통해 소셜 미디어에서 쉽게 발생할 수 있으니 “친구”라는 자가 보낸 의심스러운 메시지를 믿지 마십시오.

사회보장번호

회사에서 귀하의 사회보장번호를 물어 보아야 될 필요는 거의 없습니다. 만일 물었을 경우, 특히 정부 기관, 고용주, 은행 또는 금융 기관이 아니라면 왜 필요한지 물어보십시오. **그리고 다시 강조하지만, 귀하에게 원치 않는 연락을 취하는 자에게 절대 사회보장번호를 알려주지 마십시오.**

방화벽 사용, 운영 체제 업데이트

인터넷을 검색하다 보면 컴퓨터가 바이러스에 노출될 수 있습니다. 운영 체제 및 바이러스 백신 프로그램을 최신 버전으로 유지하고 방화벽을 계속 실행하여 안전을 유지하십시오.

강력한 비밀번호 작성

인터넷을 사용할 경우 강력한 비밀번호가 필요하며 그 중 여러 개가 필요합니다. 강력한 비밀번호는 다음과 같습니다.

- 길이가 길어야 합니다. 최소 8자 이상이어야 하지만 길수록 좋습니다.
- 아무도 추측할 수 없어야 합니다. 생일이나 친척의 이름 등을 사용해서는 안 됩니다.
- 본인이 기억할 수 있어야 합니다. 길고 흔치 않은 단어(“배터리 스테이플러”)를 결합하는 방법이 유용할 수 있습니다.
- 한 번만 사용해야 합니다. 비밀번호를 반복 사용했는데 누군가가 그 비밀번호를 알게 되면 모든 계정에 접속할 수 있습니다.

비밀번호 관리자

최신 브라우저에는 비밀번호를 기억하는 “비밀번호 관리자”가 설치되어 있습니다. 관리자를 다운로드하기만 하면 다른 모든 작업이 자동으로 완료됩니다. 관리자의 비밀번호는 최대한 안전하게 유지하십시오. 사기꾼이 비밀번호에 접근하면 귀하의 모든 계정에 접속할 수 있습니다.

비밀번호로 보호되는 장치

휴대폰과 컴퓨터 계정을 웹사이트의 계정처럼 취급하십시오. 고유하고 강력한 비밀번호를 지정하십시오.

기본 비밀번호

라우터나 모뎀과 같은 일부 장치에는 기본 비밀번호가 있습니다. 기본 비밀번호는 거의 안전하지 않기 때문에 즉시 변경해야 합니다.

정기적인 비밀번호 변경

이 조언을 따르더라도 비밀번호를 오래 사용하면 해커가 비밀번호를 얻게 될 가능성이 높아집니다. 웹사이트의 보안이 뚫릴 수 있는 것입니다. 해당 웹사이트가 뚫렸을 경우에는 항상 비밀번호를 변경하고, 안전을 위해 정기적으로 비밀번호를 변경하십시오.

보안 연결

안전하지 않은 웹 사이트 또는 Wi-Fi 네트워크는 개인 정보를 노출시킬 수 있습니다. 공용 네트워크에서는 개인 또는 금융 거래 서비스를 이용하지 말고 웹사이트에 민감한 정보를 제공하기 전에 웹사이트가 “안전”한지 확인하십시오. 보안 웹사이트는 **“https://”** 로 시작합니다(**“http://”** 가 아님)

불필요한 데이터 삭제

더 이상 필요하지 않은 개인 정보 기록은 파기하십시오. 영수증, 세금 신고서, 재정 또는 의료 기록 등 물리적 문서는 파쇄 처리하십시오. 디지털 계정은 삭제 또는 비활성화하고 디지털 파일을 삭제하십시오. 삭제된 파일도 여전히 하드 드라이브에 있을 수 있으니 구형 컴퓨터를 처분할 경우 모든 개인 데이터를 지우려면 특수 보안 소프트웨어가 필요합니다.

재무 관련 내용 점검

본인이 승인하지 않은 모든 활동에 대해 신용카드 및 은행 거래 내역을 주의 깊게 확인하십시오.

의료비와 건강 보험을 주의 깊게 확인하여 설명된 치료를 실제로 받았는지 확인하십시오.

신용 보고서

누구나 주요 신용보고기관에서 매년 무료 신용 보고서를 한 부씩 수령할 수 있습니다. 귀하가 시작하지 않았거나 모르는데 계정이 보이거나 문의가 있다면, 타인이 귀하의 ID를 사용하고 있음을 나타낼 수 있습니다. 웹사이트 annualcreditreport.com에 접속하거나 전화 (877) 322-8228 번으로 연락하여 연중 다른 시기에 정기 보장을 받는 여러 기관의 보고서를 예약할 수 있습니다.

자녀 신원 도용

자녀의 신원은 가장 많이 도용당하며 때로는 신용 등급이 나쁜 가족 구성원이 도용합니다. 자녀의 개인 정보를 본인의 것처럼 보호하십시오. 타인이 자녀 명의로 청구서 징수 전화나 신용 제안을 받거나, 타인이 자녀의 번호를 사용하여 혜택을 거부당하거나, IRS로부터 납부해야 할 세금에 대한 통지를 받았을 경우 이에 대해 이의를 제기하고 조치를 취하십시오.