



As our customer, you play a vital role in safeguarding your financial information, particularly as fraud schemes such as impersonation and Business Email Compromise (BEC) become increasingly sophisticated. Fraudsters are also leveraging artificial intelligence (AI) to create highly convincing phishing attempts, including realistic emails, text messages, and even voice or video impersonations that may appear to come from trusted sources or someone you know. These tactics often create a sense of urgency, prompting immediate action without proper verification.

Open Bank maintains robust security measures to protect your accounts, including transaction monitoring, fraud detection systems, and account alerts. If suspicious activity is identified, we may contact you to verify transactions or temporarily restrict account access as a precaution. Please note that we will never ask for your password, PIN, or one-time passcode, nor will we instruct you to transfer funds to a “safe” account.

To further protect yourself, you are encouraged to:

- Verify any unexpected requests for funds or sensitive information using official Bank contact channels
- Use strong, unique passwords and enable multi-factor authentication where available
- Regularly review your account activity and promptly report any unauthorized transactions
- Avoid clicking on suspicious links or sharing sensitive information via email, text, or phone
- Call and verbally verify the legitimacy of the request

Staying informed and exercising caution are essential to reducing fraud risk and ensuring the continued security of your accounts. If you receive any suspicious requests regarding your account, please contact us immediately at **(213) 892-9999** or **support@myopenbank.com**.

Thank you.



고객님께서서는 고객님의 금융 정보를 보호하는 데 중요한 역할을 하고 계십니다. 특히 요즘처럼 사칭 사기 및 비즈니스 이메일 사기(BEC)와 같은 사기 수법이 점점 더 정교해지고 있는 상황에서 더욱 그렇습니다. 사기범들은 인공지능(AI) 도구들을 활용하여 매우 정교한 피싱 이메일을 만들어 내고 있으며, 여기에는 진위 여부를 쉽게 구분하기 어려운 이메일, 문자 메시지, 심지어 신뢰할 수 있는 출처나 지인으로 가장한 음성 또는 영상 사칭까지 포함됩니다. 이러한 수법은 해당 내용이 긴급한 것 같은 어투나 상황을 조성하여 피해자 분들이 해당 내용을 확인할 겨를 없이 즉시 특정 행동을 하게끔 유도합니다.

Open Bank는 고객님의 계정을 보호하기 위해 거래 모니터링, 사기 탐지 시스템, 계정 알림 등 강력한 보안 조치를 유지하고 있습니다. 의심스러운 활동이 감지될 경우, 거래 확인을 위해 고객님의 연락드리거나 예방 차원에서 계정 접근을 일시적으로 제한할 수 있습니다. Open Bank는 고객님의 비밀번호, PIN 또는 일회용 인증번호를 절대 요청하지 않으며, 자금을 “안전한” 타 계좌로 이체하셔야 한다고 안내하지 않습니다.

고객님의 금융 정보와 계좌를 안전하게 보호하기 위해 다음 사항을 권장드립니다:

- 예정에 없던 자금 요청이나 민감한 정보 요청이 들어오면, 반드시 은행의 공식 연락 채널을 통해 확인하십시오
- 예측하기 어려운 고유한 비밀번호를 사용하고, 가능한 경우 다중 인증(MFA)을 활성화하십시오
- 계좌 내역을 주기적으로 확인하시고 승인하지 않은 거래가 발견되면 즉시 신고하십시오
- 의심스러운 링크를 클릭하거나 이메일, 문자, 전화로 민감한 정보를 공유하지 마십시오
- 의심스러운 요청을 받으시면 반드시 전화로 상대방과 직접 통화하여 진위 여부를 확인하십시오

관련 정보를 지속적으로 정보를 숙지하고 주의를 기울이는 것이 사기 피해 위험을 줄이고 고객님의 계정을 안전하게 유지하는 데 필수적입니다. 계좌와 관련하여 의심스러운 요청을 받으신 경우, 즉시 **(213) 892-9999** 또는 **support@myopenbank.com**으로 연락해 주시기 바랍니다.

감사합니다.