Business Email Compromise – What is it and how to protect yourself

Business email compromise (BEC) is one of the most financially damaging online crimes. It exploits the fact that most of us rely on email to conduct both our personal and professional business.

In a BEC scam—also known as email account compromise (EAC)—criminals send an email message that appears to come from a known source making a legitimate request, like in these examples:

- A vendor your company regularly deals with sends an invoice with an updated mailing address.
- A company CEO asks her assistant to purchase dozens of gift cards to send out as employee rewards. She asks for the serial numbers so she can email them out right away.
- A homebuyer receives a message from his title company with instructions on how to wire his down payment.

Versions of these scenarios happened to real victims … but all the messages were fake.

And in each case, thousands—or even hundreds of thousands—of dollars were sent to criminals instead.

How BEC Scams Work

- **Spoof an email account or website.** Slight variations on legitimate addresses (john.kelly@examplecompany.com vs. john.kelley@examplecompany.com) fool victims into thinking fake accounts are authentic.
- **Send spearphishing emails.** These messages look like they're from a trusted sender to trick victims into revealing confidential information. That information lets criminals access company accounts, calendars, and data that gives them the details they need to carry out the BEC schemes.
- **Use malware.** Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages so accountants or financial officers don't question payment requests. Malware also lets criminals gain undetected access to a victim's data, including passwords and financial account information.

Protect Yourself

- Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.
- **Don't click on anything in an unsolicited email or text message asking you to update or verify account information.** Look up the company's phone number on your own (don't use the one a potential scammer is providing) and call the company to ask if the request is legitimate.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.
- Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate**. You should verify any change in account number or payment procedures with the person making the request.**
- Be especially wary if the requestor is pressing you to act quickly.

If you believe you have been affected by a Business Email Compromise (BEC), please contact the bank immediately at (213) 892-9999 or email us at support@myopenbank.com.

Rev. 12/31/2025

비즈니스 이메일 사기(BEC) – 어떻게 해야 피할 수 있을까요?

비즈니스 이메일 사기(BEC)는 온라인 범죄 중에서 재정적으로 큰 피해를 주는 범죄유형 중 하나입니다. 우리는 개인 및 업무상 이메일을 많이 의존하기 때문에 범죄에범죄자들은 이를 악용하고 있습니다. 일반 피싱 이메일과는 다르게 BEC 사기(EAC 라고 부르는 경우도 있습니다)는 여러분이 아는 이메일 주소-즉 신뢰하는 이메일 주소로부터로 정상적인 거래를 가장한 피싱이메일을 보내온 다는 점이 가장 큰 특징입니다. 예를 들면 다음과 같습니다:

- 여러분이 거래하는 공급업체가 송금 주소가 변경되었다며 인보이스를 보냅니다.
- 회사대표가 직원에게 직원들에게 선물할 기프트 카드를 여러 장 구매해달라고 요청한뒤 해당 기프트카드의 Redeem code 이메일로 바로 보내달라고 합니다.
- 주택을 구매한 분이 타이틀 회사로부터 계약금 송금 방법에 대한 이메일을 받습니다.

이러한 시나리오들은 모두 가짜 메세지이지만 미국내에서 유사한 사례들로 부터 피해자들이 속출 하고 있고 각각 사건마다 수천 달러, 심지어 수십만 달러가 범죄자에게 송금되어지고 있습니다.

BEC 사기는 어떻게 진행되나요?

- **신뢰할 수 있는 이메일 계정나 웹사이트 이름을 가장합니다.** 예를 들어, john.kelly@examplecompany.com 이 사용자가 신뢰하는 이메일 주소라면 이와 아주 비슷한 주소(예, john.kelley@examplecompany.com)를 만들어 피해자가 자신이 알고 있는 신뢰하는 계정에서 온 메세지라고 믿게 만듭니다.
- **스피어피싱 이메일을 보냅니다.** 이러한 이메일들은 신뢰할 수 있는 발신자에게서 온 것처럼 가장하여 피해자가 민감한 정보를 보내도록 유도합니다. 이렇게 탈취한 정보로 범죄자는 회사 계정, 일정, 데이터에 접근해 BEC 사기를 실행하는 데 필요한 세부 정보를 얻습니다.
- **컴퓨터 바이러스를 사용합니다.** 악성소프트웨어같은 바이러스를 통해 여러분의 회사 컴퓨터나 이메일 정보에 접근한 후 탈취된 정보를 통해 상대방에게 결제 요청을 시기적절하게 보내거나 회계 담당자가 결제 요청을 의심하지 않도록 합니다. 이렇게 설치된 악성소프트웨어는 컴퓨터에 남아 피해자의 데이터(비밀번호, 금융 계좌 정보 등)에 추가로 몰래 접근할 수 있게 합니다.

어떻게 해야 BEC 사기를 피할 수 있나요?

- 온라인이나 소셜 미디어에 공유하는 정보에 주의하세요. 반려동물 이름, 졸업한 학교, 가족 구성원, 생일 등은 범죄자들이 비밀번호나 보안 질문의 답을 추측하는 데 사용되어지고 있습니다..
- **계정 정보를 업데이트하거나 확인하라는 요청이 담긴 의심스러운 이메일이나 문자 메시지에 있는 링크를 클릭하지 마세요.** 혹시 이런 메세지를 받으면 해당 회사/서비스의 공식 전화번호를 직접 검색하여 이러한 요청이 실제로 해당 회사/서비스로부터 온 것인지를 문의하세요. 문의하실땐 의심스러운 메세지에 적힌 전화번호를 사용하시면 절대로 안됩니다.

- 이메일 주소, 웹사이트 주소, 철자 등을 꼼꼼히 확인하세요. 사기 범죄자들은 우리가 쉽게 놓칠 수 있는 아주 작은 차이를 이용해 신뢰할 수 있는 이메일인 것처럼 가장 한다는 것을 잊지마세요.
    - 다운로드를 할땐 늘 주의하세요. 모르는 사람에게서 온 이메일 첨부파일은 절대 열지 마세요. Forwarding 된 이메일에 첨부되있는 파일도 주의하세요.
    - 가능하다면 모든 계정에 2 단계 인증을 설정해두세요.
- 결제 및 구매 요청은 직접 대면하거나 전화하여 요청자가 실제로 보낸 것이 맞는지 확인해보세요. **기존에 거래하던 곳이라도 계좌번호나 결제 절차가 변경되었다면 송금전에 반드시 요청자에게 거듭 확인해보세요.**
- 또한 이러한 것들이 아주 짧은 시간내에 완료되야된다며 요청해오면 의심해보셔야 합니다.

만약 비즈니스 이메일 사기(BEC) 피해가 의심된다면 즉시 Open Bank 로 연락하세요 (213-892-9999, support@myopenbank.com).

감사합니다.