FIRST BANK

What is business email compromise?

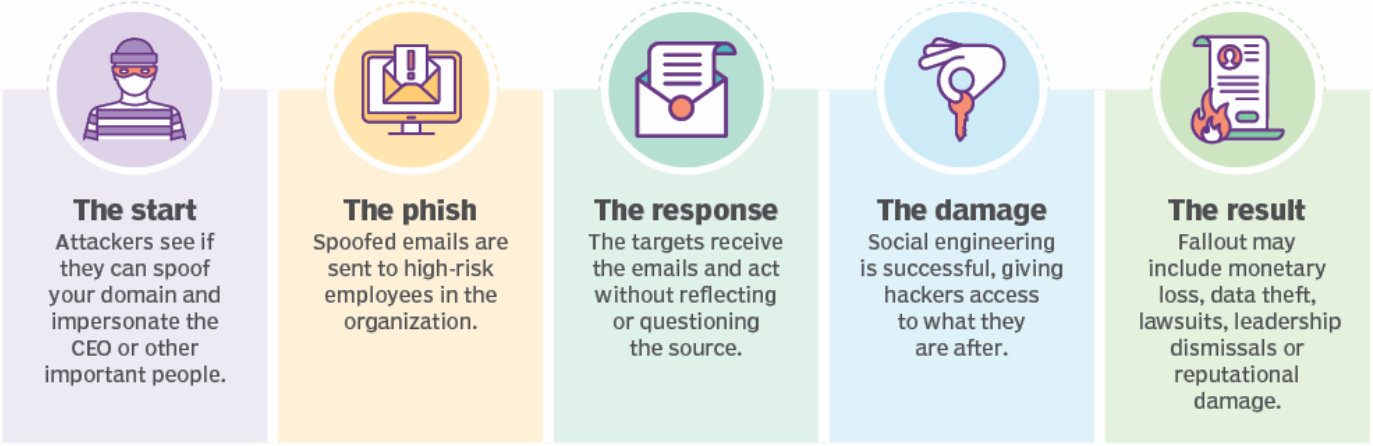
Business email compromise (BEC) — also known as **email account compromise (EAC)** — is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business — both personal and professional.

In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request, like:

- 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 have happened numerous times to real victims. All the messages were fake. And in each case, thousands — or even hundreds of thousands — of dollars were sent to criminals instead.

How BEC works



FIRST BANK

How criminals carry out BEC scams

A scammer might:

- **Spoof an email account or website**. Slight variations on legitimate addresses fool victims into thinking fake accounts are authentic (john.kelly@examplecompany.com vs john.kelley@examplecompany.com).

- **Send spear phishing 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.

How to 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.

How to mitigate BEC for your business

Here are some precautionary measures and mitigation strategies for BEC threats:

- Frequently monitor your email server for changes in configuration and custom rules for specific accounts

- Consider adding an email banner stating when an email comes from outside your organization, so they are easily noticed

- Conduct End User education and training on the BEC threat and how to identify a spear phishing email.

- Ensure company policies provide for verification of any changes to existing invoices, bank deposit information and contact information.

- Contact requestors by phone before complying with e-mail requests for payments or personnel records.

- Consider requiring two-party sign-off on payment transfers, like ACH and wire transactions.

FIRST BANK

Other suggestions for protection

Employees should be educated about and alert to schemes like these. Training should include preventative strategies and reactive measures in case they are victimized. Among other steps, employees should be told to:

- Use secondary channels or two-factor authentication to verify requests for changes in account information.
- Ensure the URL in emails is associated with the business it claims to be from.
- Be alert to hyperlinks that may contain misspellings of the actual domain name.
- Refrain from supplying login credentials or PII in response to any emails.
- Monitor their personal financial accounts on a regular basis for irregularities, such as missing deposits.
- Keep all software patches on and all systems updated.
- Verify the email address used to send emails, especially when using a mobile or handheld device by ensuring the senders address email address appears to match who it is coming from.
- Ensure the settings on the employees' computer are enabled to allow full email extensions to be viewed.

More resources

The Federal Trade Commission's website houses cybersecurity resources developed in partnership with the National Institute of Standards and Technology, the U.S. Small Business Administration and the Department of Homeland Security.

www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

Member FDIC EQUAL HOUSING LENDER