Business Email Compromise

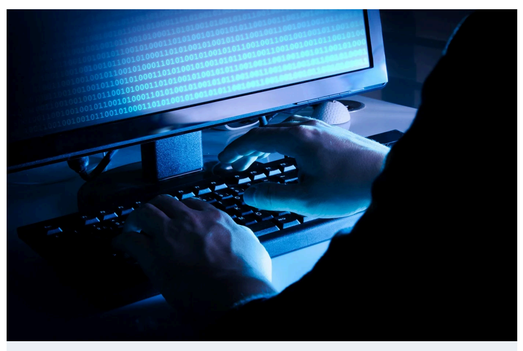
Business email compromise (BEC) is one of the most financially damaging online crimes. It exploits the fact that so most of us rely on email to conduct both our personal and professional business.

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.



Report BEC

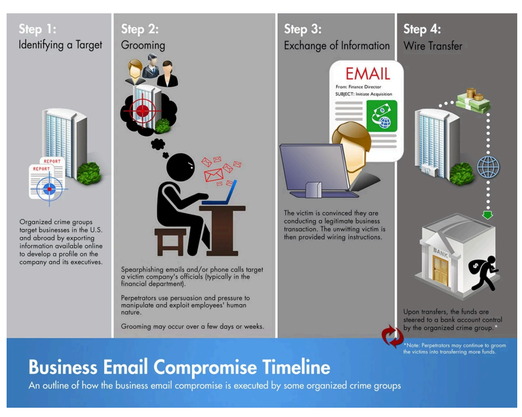
Visit ic3.gov, the FBI's Internet Crime Complaint Center (IC3), to business email compromise scams.

You should also contact your financial institution immediately and request that they contact the financial institution where any transfer was sent.

How BEC Scams Work

A scammer might:

- **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.



Full-size image

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.

News and Resources

IC3 Resources

- FBI's Internet Crime Complaint Center (IC3)
- Business Email Compromise: Virtual Meeting Platforms
- Cyber Criminals Conduct Business Email Compromise Through Exploitation of Cloud-Based Email Services, Costing U.S. Businesses More Than $2 Billion
- Business Email Compromise: The $26 Billion Scam
- FBI 2022 Congressional Report on BEC and Real Estate Wire Fraud

Press Releases

10.01.2024 Previously Extradited Nigerian National Sent to Prison for Role in Multimillion-Dollar Business Email Compromise Scheme

09.26.2024 Two Nigerian Nationals Charged in Connection with Business E-Mail Compromise Scheme

09.24.2024 Nigerian Man Pleads Guilty After Extradition to Participating in Romance Scams and Other Fraud Schemes Targeting Elderly Victims

09.03.2024 Two Foreign Nationals Sentenced for Victimizing U.S. Companies Through Business Email Compromise Scheme

08.30.2024 Nigerian National Extradited From Ghana to Face Charges for an Alleged $7.5 Million Business Email Compromise Scheme Involving Two Charitable Organizations

08.06.2024 Zimbabwe National Found Guilty of Laundering More Than $1.2 Million