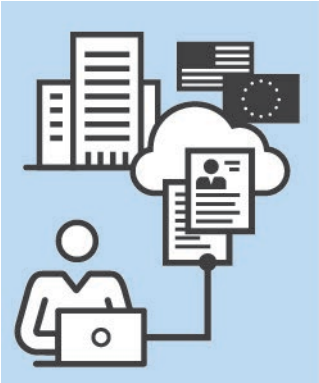
Business Email Compromise

FBICYBER

Business email compromise (BEC), also known as email account compromise (EAC) and/or CEO impersonation, is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests. Organized crime groups and cyber criminals have targeted large and small companies and organizations in every U.S. state and more than 100 countries around the world—from non-profits and well-known corporations to churches and school systems.

The scam occurs when a subject compromises or impersonates legitimate business or personal email accounts to conduct unauthorized transfers of funds through social engineering, spear-phishing, identity theft, email spoofing, or computer intrusion methods through the use of malware. In almost every case, the scammers target employees with access to company finances and deceive them into making wire transfers to bank accounts belonging to nefarious actors.

HOW IT OCCURS



Step 1

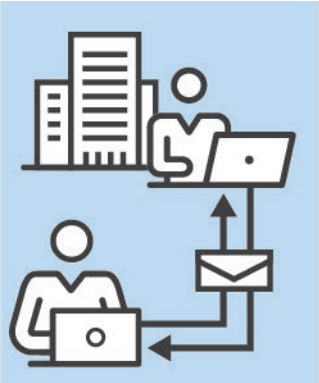
Identify Target

BEC actors target businesses and organizations, exploiting online information to develop a profile on the victim company and its executives.

Step 2

Grooming

Typically, somone in the finance department is targeted by spearphishing emails and/or phone calls. Criminal actors manipulate and exploit human nature through persuasion and pressure.



Step 3

Exchange of Information

With the victim convinced they are conducting a legitimate business transaction, they are provided with fradulent wiring instructions.

Step 4

Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the BEC actors.

DON'T BE A VICTIM

Implement the following practices to reduce your organization's likelihood of falling victim to a BEC/EAC scam:

Implement awareness and training programs.
All employees should go through regular training detailing the threat of BEC and how it is delivered, as well as best practices to prevent BEC by learning how to identify phishing emails and how to respond to suspected compromises.

Confirm payments via telephone prior to disbursing funds.
Require that the finance department contact vendors via the original phone numbers on file prior to transferring funds. Any phone numbers listed in a fund transfer request could be associated with the malicious actor.

Hold third-party suppliers accountable.
Require any payroll, financial service, and IT service contracting companies to outline all protective steps taken to protect the integrity of company data and networks.

Keep operating systems, software, and firmware up to date.
Regularly update and patch the operating system (OS), software, and firmware on company devices to mitigate vulnerabilities that could be exploited by adversaries to gain access to company networks.

Automate anti-virus and antimalware scans.
These scans can help organizations identify a breach more quickly.

Create strong intrusion detection system rules.
Ensure the intrusion detection system (IDS) rules monitor for emails with spoofed domains created to appear as a legitimate email account. For example, legitimate email of abc_company.com would flag fraudulent email of abc-company.com.

Flag suspicious emails.
Create an email rule to flag email communications where the "reply" email address is different from the "from" email address shown.

Clearly distinguish between internal and external email senders.
Establish a warning notification that clearly distinguishes emails that originated from an external sender.

REPORTING BEC/EAC INCIDENTS

If you discover you are the victim of a fraudulent incident, immediately contact your financial institution to request a recall of funds. Immediately request that your financial institution contact the financial institution where the fraudulent transfer was sent. Contact your local FBI field office and file a complaint—regardless of dollar loss—with the FBI's Internet Crime Complaint Center (IC3) at https://bec.ic3.gov.

WHAT ARE THE BENEFITS OF REPORTING BEC INCIDENTS TO THE FBI?

In response to a reported cyber incident, the FBI may be able to identify and stop the fraudulent activity through:

Recovery Asset Team (RAT).
The FBI's RAT was established in February 2018 by the FBI's IC3 to streamline communication with financial institutions and assist victim companies who made transfers to domestic accounts under fraudulent pretenses.

Apprehend or impose costs on cyber actors.
The DOJ and FBI can bring forth indictments and other deterring actions to degrade cyber actors' capabilities.

Information sharing.
FBI agents familiar with patterns of malicious cyber activity can work with your security and technical teams to help you quickly identify and understand the context of the incident.

International partnerships.
FBI Cyber Assistant Legal Attachés around the world can leverage the assistance of international law enforcement partners to locate stolen funds or data, or identify the perpetrator.

HOW DO I CONTACT THE FBI TO REPORT A CYBER INCIDENT?

- Local FBI Field Office: https://www.fbi.gov/contact-us/field-offices
- The FBI's Internet Crime Complaint Center (IC3): www.ic3.gov
- International FBI offices: https://www.fbi.gov/contact-us/legal-attache-offices