Business Email Compromise (BEC)

Archived: 2026-04-29 02:02:16 UTC

What is BEC?

Business email compromise (BEC) is a cyberattack technique whereby adversaries assume the digital identity of a trusted persona in an attempt to trick employees or customers into taking a desired action, such as making a payment or purchase, sharing data or divulging sensitive information.

According to the FBI's 2022 Congressional Report on BEC and Real Estate Wire Fraud, BEC is "one of the fastest growing, most financially damaging internet-enabled crimes." In 2021, claimed losses exceeded $2.4 billion, a 566% increase since 2016, according to the Internet Crime Complaint Center (IC3). Cases of BEC are expected to rise given the increase in remote work and, by extension, the ubiquity of digital communication channels like email.

Email account compromise (EAC) vs BEC

Email Account Compromise (EAC) is a cyberattack technique in which hackers leverage a variety of methods, including social engineering, malware or password cracking tools, to compromise a legitimate email account.

In many cases the objective of a BEC attacker and EAC attacker are the same: They want to steal money, data or other sensitive information. However, the key difference is that in a BEC attack, the hacker is merely posing as a trusted figure, such as a business executive, lawyer, or important vendor, usually via a spoofed email account. That person then attempts to direct an employee or other person to take a given action, such as wiring funds to the attacker's account.

In EAC attacks, however, the attacker breaches a legitimate email account and acts as the owner of that account. With access to real credentials, the actor is able to conduct fraudulent activity and bypass multi-factor authentication tools.

5 types of BEC scams

According to the FBI, there are five main types of BEC scams:

1. Account compromise

In an account compromise, an employee's email account is hacked and used as a vehicle for financial or data-related crimes. In most cases, the attacker will use the account to request payments on behalf of vendors; these funds are then transferred to accounts owned or controlled by the attackers.

2. Attorney impersonation

An attorney impersonation attack typically targets newly hired or junior employees. In this attack, the hacker will pose as a lawyer or legal team member and pressure or manipulate the employee into taking action, such as sending data or requesting a wire transfer. Because the request is typically framed as urgent, confidential or both, many new or relatively inexperienced employees do not know how to validate the request and simply comply in order to avoid negative consequences.

3. CEO fraud

CEO fraud is similar to an attorney impersonation attack except in this case the attacker poses as the CEO. In most instances, the attacker will target a member of the finance team, again claiming to need urgent support on a time-sensitive or confidential matter. In these events, the employee is goaded into transferring money into an account controlled by the attacker.

4. Data theft

BEC attackers can also target a company for data. In a data theft attack, the attacker will most commonly zero in on HR or finance team members and attempt to steal personal information about the company's employees or customers. This information can be sold on the dark web or used to inform and advance future attacks.

5. Fake invoice scams

In a fake invoice scam, the attacker poses as a vendor and requests payment from an employee for a service. In most cases, the attacker will present themselves as an actual vendor and edit an official vendor invoice template. However, the attacker will alter the account details so that funds will be transferred into an account owned by the hacker.

How does a BEC scam work?

Most BEC scams follow the same process, though the identity assumed by the attacker and their targets will vary.

Phase	Description
1. Identity Research	A skilled BEC attacker conducts thorough research of their desired target and determines what identity to assume relative to the action they want to inspire. For example, if the scammer is looking for a quick score, they may simply create an email account that is very similar to the company's CEO or other executive and request that employee purchase and send them several digital gift cards as a "bonus" for an internal team or sign of appreciation for a vendor. BEC scams can also be far more elaborate. For example, a hacker may pose as a new vendor, such as a payroll provider, and offer a free trial for payroll services — only to steal employees' personal information or even divert paychecks during a fictitious trial.
2. Employee Research	Once the hacker identifies their attack technique and assumed identity, they must conduct research on their targets. This may involve mining the company website for contact information or to determine the typical email address format; they may also leverage social networking sites like LinkedIn to research names and titles of various team members, as well

Phase	Description
	as their roles and responsibilities. With substantial research, it is possible that the attacker could zero in on a person who has handled similar, legitimate requests in the past, or employees who may not be familiar with company processes and procedures.
3. Attack Prep	With the identity and target set, the attacker will then prepare other components of the attack. This could include creating a spoofed email account, posting a fake company website, setting up bank accounts, creating invoices or any other asset the attacker will need to substantiate their identity or the request.
4. Attack Launch	In the final stage, the attacker will put their plan into action. BEC scammers will use their digital identity to manipulate or pressure the target to take a desired action, often inspiring a false sense of urgency to ensure the person acts on the request without discussing it with another employee or fully thinking through the scenario. If the attacker is successful, the attack will end with the transfer of money, data or other information to the hacker.

3 BEC techniques

BEC attackers leverage a variety of techniques to carry out their attacks. Three of the most common methods are:

- **Domain spoofing**: Domain spoofing is a form of phishing where an attacker impersonates a known business or person via a fake website or email domain to fool people into trusting them. Typically, the domain appears to be legitimate at first glance, but a closer look will reveal that a W is actually two Vs, or a lowercase L is actually a capital I. Users responding to the message or interacting with the site are tricked into revealing sensitive information, sending money or clicking on malicious links.
- **Social engineering**: Social engineering is the act of manipulating people to take a desired action, like giving up confidential information. Social engineering attacks work because humans can be compelled to act by powerful motivations, such as money, love and fear. Adversaries play on these characteristics by offering false opportunities to fulfill those desires.
- **Compromised accounts**: A compromised account is an email or system account that has been breached by an attacker. The hacker can leverage a variety of methods, including social engineering, malware, or password cracking tools, to compromise the account. Once they have control, the attacker can then masquerade as the user and carry out any activity the legitimate owner is able to do.

How to protect against BEC scams

BEC attacks rely on a human-to-human connection, as opposed to digital tools like malware or viruses. As a result, BEC are difficult to detect or prevent with traditional security tools, such as antivirus solutions or endpoint detection and response (EDR).

Since BEC attacks are generally human-centric, the methods of protection and prevention must also be human-centric. Below are some best practices to consider when defending against BEC attacks:

1. Implement a robust cybersecurity training program for all employees.

The organization's first line of defense in BEC attacks is their workforce. Therefore, it is essential that the organization creates a robust cybersecurity training program that includes specific modules about social engineering techniques. As part of the training program, the organization may wish to test the effectiveness of the course through a variety of simulations or drills.

Specific points to cover in the training may include:

- What constitutes an unusual, atypical or inappropriate executive request, such as requests for personal information about a specific employee
- Proper processes and procedures for financial transactions, including who is approved to conduct such activity and how to inform that person of a request made to another team member
- Proper processes and procedures for managing vendor invoices, even for urgent requests
- Examples of how the attacker may use fear, intimidation, confidentiality or urgency to manipulate an employee
- How to identify spoofed email addresses or domains, as well as mismatched "reply to" addresses

2. Implement a Zero Trust strategy.

Zero Trust is a security concept that requires all users to be authenticated and authorized before being granted access to applications and data. Execution of this framework combines advanced technologies such as risk based multi-factor authentication, identity protection, next-generation endpoint security, and robust cloud workload technology to verify a user or systems identity, consideration of access at that moment in time and the maintenance of system security. This is especially important in preventing EAC attacks, where the adversary assumes the identity of a legitimate system user and masquerades as that person.

3. Monitor the deep and dark web for signs of compromise.

The dark web is the part of the internet where users can access unindexed web content anonymously through special web browsers like TOR. Dark web monitoring tools are similar to a search engine (like Google) for the dark web. These tools help to find leaked or stolen information such as compromised passwords, breached credentials, intellectual property and other sensitive data that is being shared and sold among malicious actors operating on the dark web

4. Make an inventory of actors who leverage BEC as an attack technique.

For large organizations that face a high level of risk, it may also be wise to track and analyze the actors who apply BEC. This typically involves partnership with a trusted cybersecurity solution provider that can help the organization identify the adversary universe and zero in on those actors and techniques that are most likely to affect the organization.

5. Implement an incident response (IR) plan.

Incident response (IR) is the steps used to prepare for, detect, contain and recover from a data breach. The two most well-respected IR frameworks were developed by NIST and SANS to give IT teams a foundation to build their incident response plans on.

BEC and EAC solutions

As with so many cyberattacks, the organization's best and most important line of defense against BEC and EAC will be an engaged, knowledgeable and vigilant workforce.

However, even though BEC attacks target humans, there are still steps organizations can take to reduce risk and strengthen their defenses against such attacks.

CrowdStrike Falcon® Intelligence Recons is a security solution that enables security teams to track adversaries and their activities outside the network perimeter. With this tool, organizations can:

- Monitor the criminal underground
- Identify exposed confidential data
- Discover domain impersonations
- Assign, track and manage alerts
- Build adversary profiles
- Discover external attack vectors

CrowdStrike Falcon® Identity Threat Detection is a security solution that enables hyper-accurate detection of identity-based threats in real time, leveraging AI and behavioral analytics to provide deep actionable insights to stop modern attacks. With this tool, organizations can:

- Unlock insights and analytics for all credentials
- Detect lateral movement for authenticated accounts
- Enable AD security without using logs

Source: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/business-email-compromise-bec/