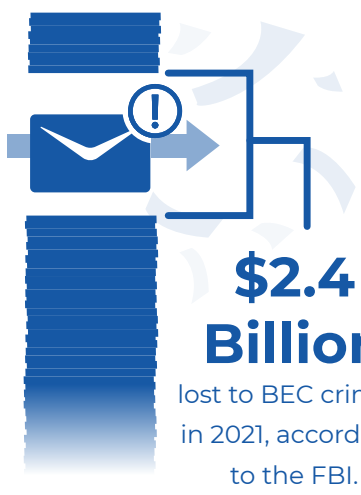
Nationwide® is on your side

Business Email Compromise Explained

Business email compromise (BEC)—sometimes referred to as email account compromise—is a type of social engineering that is one of the most financially damaging forms of cybercrime. In a BEC scam, cybercriminals impersonate a seemingly legitimate party, such as a senior executive, vendor, financial institution, professional service or another type of organization a business interacts with on a regular basis.

The cybercriminal will send a legitimate-looking email to an employee. The details of the email are often crafted to look authentic. Once trust is established, attackers trick the email recipient into wiring money, providing confidential information or performing similar compromising actions, all meant to defraud a business.



$2.4 Billion
lost to BEC crimes in 2021, according to the FBI.

Read on to learn about **common BEC scams** and **how to protect against them**.

Common BEC scams

False invoice scheme
Cybercriminals send a spoof email pretending to be one of the company's vendors. Then they request fund transfers to pay a fake invoice.

$43.3 Billion lost due to BEC between 2016 and 2021, according to the FBI.

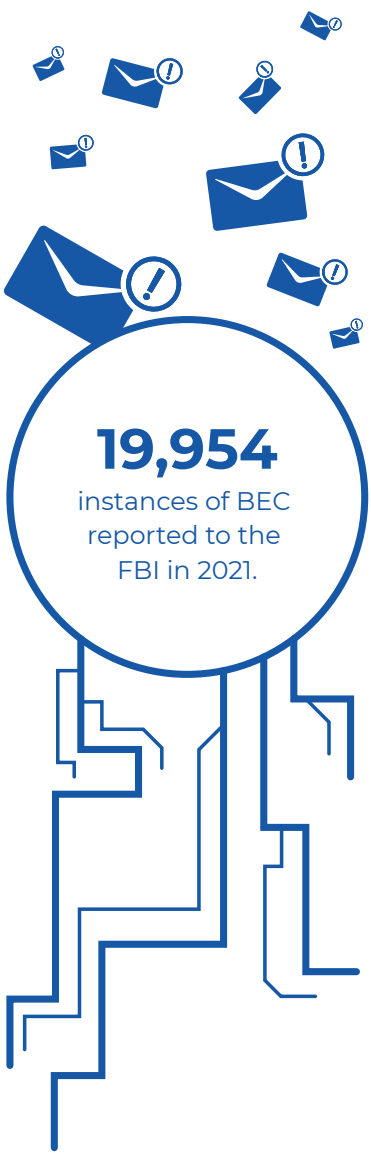
CEO fraud
Scammers pose as high-level executives and request a wire transfer. The email will often urge immediate action, preying on the recipient's fear of losing their job or other consequence if the funds are not transferred quickly enough.

Account compromise
This type of scam is difficult to identify. Cybercriminals hack directly into the email account of an executive or employee and use that account to request invoice payments to vendors listed in the email contacts. Those payments are then directed to the criminals' bank accounts.

Attorney impersonation
Attackers will impersonate a corporate lawyer or law firm. They will claim they are handling confidential, time-sensitive matters that require the immediate transfer of funds. To make the emails sound more convincing, the attackers will often reference publicly available information, such as recent news regarding mergers and acquisitions.

Data theft
In these scams, attackers aren't after money but rather sensitive information such as names, addresses, birthdays, Social Security numbers or tax documents. They might pose as HR professionals or other employees who work in functional areas of the company. Once they obtain the sensitive data, cybercriminals can use it to carry out future attacks.

Signs of BEC



19,954
instances of BEC reported to the FBI in 2021.

Unusual requests from high-level executives
If a high-ranking executive asks for information about an individual employee, that's a red flag. Executives aren't usually interested in items like W2 forms or tax information. Employees should always think about whether the request in the email makes sense.

Look-alike emails
Attackers will set up spoof email addresses and websites designed to mimic the real thing. The address might only be off by a single character. So, for example, "honestemail.com" might appear as "h0nestemail.com."

Requests for secrecy
Cybercriminals often request that their emails be kept confidential or that the recipient only communicates with them via one email account.

Urgent or threatening language
Emails that ask the recipient to bypass standard procedures to execute a task as soon as possible or include threatening language should be viewed as suspicious.

Unusual grammar or formats
Often, the word choice or sentence structure of a scam email will sound slightly off, as if written by a non-native speaker.

Flaws in logos or graphics
Scammers spend a lot of time and effort trying to make their emails look official by recreating company logos and graphics. However, careful viewers can often spot tiny flaws or poor quality in these imitations on closer inspection.

Protecting against BEC

Set clear policies
Businesses should create policies that limit or eliminate the amount of sensitive information made available to employees, customers and the general public. As a rule, avoid emailing personal or financial information when unnecessary.

Prohibit work information on social media
Employees should be instructed not to post sensitive work-related information on social media websites. Even a simple post about being out of the office for a short period of time could be all the information an attacker needs to pull off a scam.

Train employees
Include BEC training as part of larger cybersecurity education initiatives. This training should include training on how to spot BEC scams and other phishing attempts.

Enable email security features
Utilizing anti-spoofing and email authentication techniques, such as Sender Policy Framework, DomainKeys Identified Mail and Domain-based Message Authentication, Reporting & Conformance, can help block BEC attempts from reaching employees.

Verify payment and purchase requests
Instruct employees to verify wire requests in person. Additionally, those in charge of transferring funds or making payments should confirm any change in account numbers or payment procedures with the person making the request. This confirmation should be done with contact information already on file—not the contact information in the email making the requested change.

Report potential instances of BEC
If it's suspected an organization has been targeted by a BEC email, the incident should be reported immediately to law enforcement or file a complaint with the IC3.