Hijacked inboxes and hijacked Money: The true cost of business email compromise

Executive Summary

- Business email compromise has become one of the most financially damaging forms of cybercrime, exploiting trust-based communication instead of technical vulnerabilities
- Attackers use tactics like account takeover, email spoofing, and social engineering to redirect payments, steal sensitive data, and manipulate business operations.
- Recent data shows BEC losses continuing to rise worldwide, with billions lost annually and recovery rates remaining extremely low once funds are transferred.
- Businesses, law enforcement agencies, and financial institutions all face major challenges, including slow cross border coordination, weak verification processes, and inconsistent security standards.
- Stronger authentication streamlined payment-verification procedures, and improved public-private information sharing are critical to reducing BEC's success rates.

Introduction

Business Email Compromise (BEC) is a target, financially motivated cybercrime that hijacks trust rather than infrastructure. “It exploits that most of us rely on email to conduct both our personal and professional business.” (FBI) BEC involves criminals manipulating legitimate business email channels to trick organizations into sending money or sensitive data to fraudulent destinations. Unlike other flashy attacks like ransomware, offenders slip into email threads, impersonate executives, suppliers, or trusted partners and redirect payments or sensitive information before anyone realizes they have been targeted and tricked. The crime is built around social engineering more than code, but its impact hits just as hard, often leaving companies with massive financial losses and no chance of recovery.

The process can begin in a few separate ways. Spoof an email account or website, such as a minor change to a legitimate address such as, changing, removing, or adding a character to fool victims into thinking the account is authentic. Send Spearphising emails which look like they are from trusted senders tricking their victims into sending sensitive information. That information lets criminals access company or personal accounts and data that gives them the details they need to carry out the attack. As well as using malware, malicious software that can infiltrate a company's networks and gain access to legitimate email threads about billing and invoices.

Facts and figures

Over the past decade, Business email compromise has emerged as one of the most financially destructive forms of cyber fraud world-wide. According to the FBI Internet Crime Complaint center (IC3), in 2022 the IC3 received 21,832 Business email compromise Complaints with adjusted losses nearly adding up to $2.7 billion (about $8.3 per person in the US). (FBI IC3, 2022). By 2023, reported BEC losses reached about 2.9 billion U.S. dollars

across 21,489 complaints. (FBI IC3, 2023). That same year BEC ranked as the second highest cyber-crime in terms of dollar losses, just below investment frauds. Between 2019 and 2023, BEC complaints have grown increasingly as shown in figure 1.

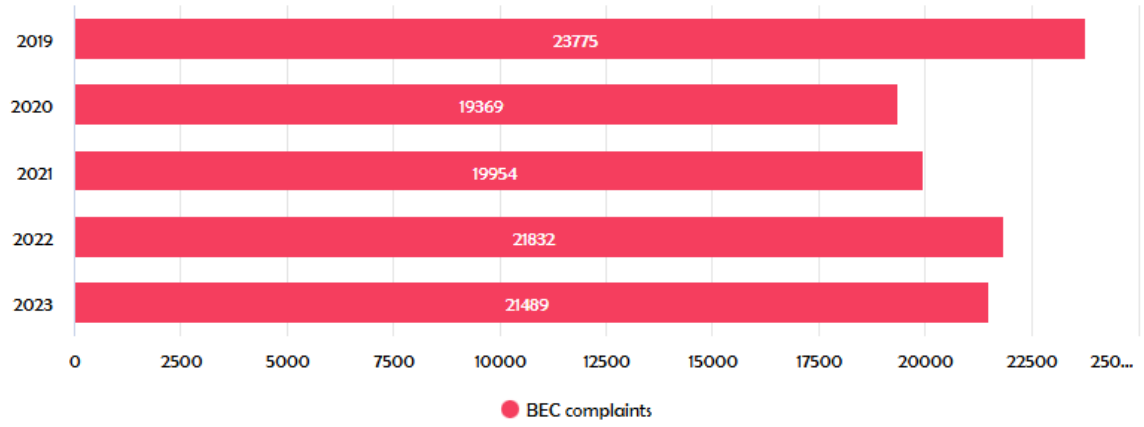

Figure 1 Increase in reported BEC complaints. (FBI IC3)

Average losses per incident have also climbed. Reports indicate that in 2019, the average loss per BEC complaint was around $74,700. By 2023, that figure had jumped to approximately $137,100 per incident, reflecting a trend toward fewer but higher value attacks. The nature and geography of BEC attacks have become more complex over time. The IC3 reports BEC frauds have been documented in all 50 U.S. states and in over 177 countries world-wide, with fraudulent transfers reaching at least 140 different nations. In recent years, funs stolen via BEC have increasingly been directed not just to conventional bank accounts but also to third party payment processors, custodial accounts, or cryptocurrency0exchange accounts. (IC3, 2023). Figure 2 shows the gradual loss of money by victims of BEC.

Figure 2 BEC losses by victims (FBI IC3)

Small and midsized businesses appear especially vulnerable. Data suggests that a sizable portion of BEC victim reports came from smaller firms, which often lack the robust financial controls and layered security infrastructure of larger enterprises. (Eser, 2025). At the same time, certain sectors including real estate and organizations processing large vendor or payroll transactions, have become frequent targets, reflecting how attackers adapt their methods to exploit business workflows and financial practices. (IC3, 2023). Despite growing awareness, the recovery rate remains low, and the financial damage is high. Many of the funds transferred through BEC frauds quickly disappear into international accounts, cryptocurrency exchanges, or shell transfers before victims realize what has happened. (IC3) The trend toward higher value incidents means that even a single successful BEC attack can cripple a small business or cause major damage for larger firms, making BEC not just a common nuisance, but a potentially existential threat to affected organizations.

Moving forward

The rising impact of Business Email Compromise makes one thing obvious. The current mix of fragmented laws, outdated verification practices, and weak user awareness is not enough

to slow crime that keeps evolving faster than institutions can respond. Moving forward, law enforcement

Agencies need stronger cross-border cooperation, faster information sharing channels and clearer legal authority to investigate BEC cases that cross multiple districts in a matter of minutes. International money movement is the backbone of most BEC frauds, and without synchronized rules for freezing suspicious transfers, investigators will continue to chase criminals who can launder funds across two or three countries before a single agency even opens a case file. The gap between how quickly money moves and how slowly agencies can act is the defining enforcement challenge of this crime and closing it demands modernization, not more reports explaining why the systems remain stuck.

For businesses, the next step of mitigation involves more than surface level cyber training. BEC thrives on routine processes, predictable workflows, and non-informed employees. That means the future of prevention depends on reshaping internal operations so that a single forged email cannot cause the fall of an organization. Stronger authentication for email logins, zero-trust verification for payments, and automated alerts for unexpected vendor changes are quickly becoming baseline necessities, not optional upgrades. Organizations also need to treat employee training as a continuous security control rather than a once-a-year compliance exercise. Attackers iterate constantly, so businesses need staff who can recognize a suspicious request even when it looks authentic and well timed to the victim's role.

Policymakers have their own responsibilities in this shift. Clearer national standards for email authentication, incident reporting, and financial transaction verification would give organizations a shared baseline instead of a patchwork of voluntary guidelines. Governments could also establish incentives or requirements for financial institutions to adopt real-time fraud

detection systems that match the speed at which BEC attack transfers occur. Because BEC relies on exploiting human predictability, policymakers need to craft rules that make it harder to weaponize everyday communication channels. Stronger email security should be treated as a public safety issue, not something left entirely to private companies to figure out on their own.

The last piece of the picture involves the users, both individual employees, and the public. Awareness alone will not eliminate BEC, a population that understands how impersonation frauds work is far harder to exploit. Training that focuses on real examples, real financial processes, and realistic attacker methods can shift user behavior in ways that directly reduce risk. When employees become conditioned to verify all unexpected financial requests, even the most convincing forged email has a much lower chance of succeeding. People are not the weakest link; they become the weakest link when no one gives them the tools to recognize when they are being targeted.

If these gaps are not addressed, the trajectory is predictable. BEC losses will keep climbing; attackers will continue refining their methods, and small businesses will face financial exposure they cannot absorb. But with coordinated enforcement reforms, stronger business controls, smarter policy and a focus on empowering users, the damage from BEC does not have to keep rising. The next decade will show whether institutions adapt fast enough, or whether criminals keep dictating the pace of change.

Figure 3 What to do in the case of an attack (IC3, 2024)

Glossary

Business email Compromise (BEC): A cyber-attack where criminals impersonate trusted individuals, such as executives or vendors, to trick employees into transferring money or sensitive information.

Web attack: A malicious attempt to exploit vulnerabilities in websites or web applications to gain unauthorized access, steal confidential information, introduce harmful content, or alter the website's content.

Email spoofing: The practice of sending email messages with a forged sender address, making the email appear to be from someone it is not.

Multi-factor authentication (MFA): A security method that requires users to provide two or more distinct forms of verification to access an account or system.

References

Axnmedia. (2024, March 21). A Look at U.S. Business Email Compromise Statistics (2024) - Axnhost.com. Axnhost.com. https://axnhost.com/2024/03/a-look-at-u-s-business-email-compromise-statistics-2024/?utm

Federal Bureau of Investigation. (n.d.). Business Email Compromise. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise

Internet Crime Complaint Center (IC3) | Business Email Compromise: The $50 Billion Scam. (2023, June 9). Ic3.Gov. https://www.ic3.gov/PSA/2023/PSA230609?utm_

jannik.lindner@globalcommercemedia.com. (2025, May 30). Business Email Compromise Statistics: ZipDo Education Reports 2025. ZipDo. https://zipdo.co/business-email-compromise-statistics/?utm_

Public Service Announcements and Industry Alerts. (n.d.). Retrieved December 4, 2025, from https://www.ipa.org/uploads/1/3/1/4/131403368/ic3_brochure_03-16-2023.pdf?utm_