DollarBank

Business INSIGHTS BRIEF

INSIDE

Business Email Compromise

Dollar Bank
Business INSIGHTS BRIEF

Every day, you are faced with decisions to help keep your business on track. Business Insights Brief provides quick hitting resources and knowledge from our banking team to help you achieve your goals.

Overview

Business Email Compromise

How Business Email Compromise Works

Examples of Business Email Compromise Scams

Tips for Protecting Your Business

Fight business email compromise with powerful financial tools.

As business email compromise scams continue to grow in both sophistication and number, Dollar Bank's treasury management experts are dedicated to providing you with the best tools to help protect your business from fraud. Our fraud mitigation offering combines a variety of treasury management solutions designed to protect your accounts from unauthorized transactions and provide you with transparency, agility and peace of mind.

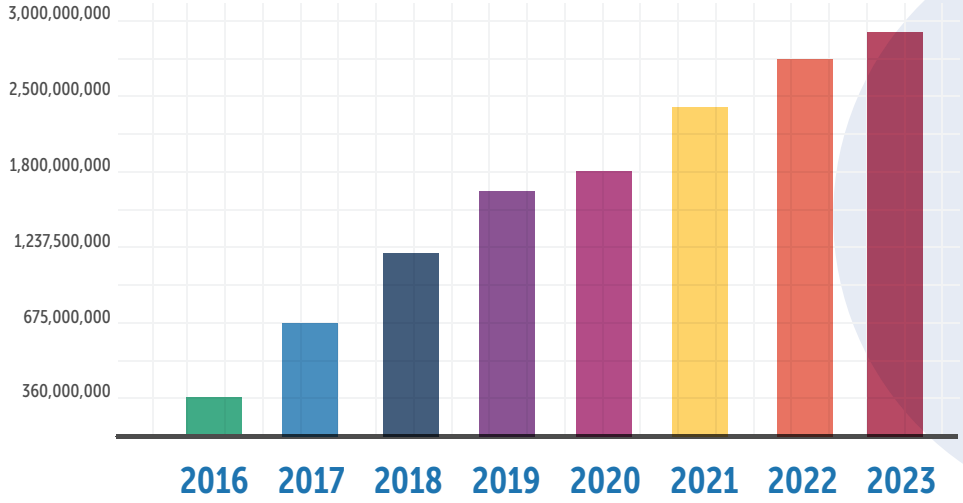
Let's talk @ 1-855-282-3888.

DollarBank®

One Click is all it May Take to Compromise Your Business

Business email compromise (BEC) is a type of cybercrime that targets companies' email communications through social engineering and/or computer intrusion techniques.

BEC losses approach $3 billion/year



Year	Losses	Year-Over-Year Change
2016	$360 million	
2017	$675 million	+88%
2018	$1.2 billion	+78%
2019	$1.7 billion	+42%
2020	$1.8 billion	+6%
2021	$2.4 billion	+33%
2022	$2.7 billion	+12%
2023	$2.9 billion	+7%

Source: FBI 2016-2023 Internet Crime Reports [2016 is the first year FBI began tracking business email compromise (BEC) and email account compromise (EAC) as a singular crime.]

BEC can result in financial losses, reputational damage and exposure of sensitive information for targeted firms. The relative ease of carrying out a BEC scam is perhaps what makes it so daunting: In many cases, all it takes is for one employee to click one illegitimate link to give a BEC scammer access to company systems and data.

In 2023, BEC cost businesses a combined $2.9 billion, as documented by incidents filed with the FBI's Internet Crime Complaint Center (IC3), making it second only to investment scams, with a reported $4.6 billion in losses. What's more, the 2024 Payments Fraud and Control Survey Report of the Association for Financial Professionals (AFP) revealed that 63% of organizations experienced some form of BEC in 2023. Businesses of all sizes and in all industries may be victimized.

How BEC Scams Work

Although business leaders are becoming more aware of BEC scams, cybercriminals continue to keep a step ahead by continually devising new schemes to catch potential victims off guard. Their methods typically include one or more of the following:

Spoofing

Spoofing. After collecting and analyzing publicly available (usually online) information about a particular company (names, titles, email addresses, etc.), the cybercriminal can "spoof" an email account or website by making a slight variation to the legitimate account — for example, rachael.smith@abcinc.com versus rachel.smith@abcinc.com — to trick recipients into believing a fake account is authentic.

Spear phishing

Spear phishing. Spear phishing is the practice of sending emails from spoofed accounts to targeted individuals or groups within a business with the goal of accessing the company's sensitive information or computer system. These emails often include a link or attachment that, when clicked, either takes the employee to an illegitimate site that asks them to enter a password or other credentials, or triggers a malicious software — called malware — download.

Malware downloads

Malware downloads. Malware downloads can be particularly harmful, as this software can be designed to steal sensitive data, disrupt network operations or surreptitiously monitor and record business activity on an ongoing basis. One type of malware — ransomware — locks users out of their computers until a specified payment is made to the cybercriminal.

Examples of BEC Scams

Learning to recognize BEC is the first step in protecting your business from its harmful effects. Here are a few examples of how cybercriminals may compromise your business through email:

- An invoice appearing to be emailed from one of your established vendors includes a change in payment instructions or mailing address, as well as a statement invoking a sense of urgency, such as "payment past due" or "account closure." If the recipient makes that change without confirming the instructions with a trusted vendor representative, your payment will be directed to an illegitimate account.
- An employee may receive an email, supposedly from one of the company's leaders, requesting them to purchase gift cards to be sent out as employee rewards. The email may state that the leader is unavailable for a call but that the employee should email them the serial numbers from the cards ASAP so the rewards can be distributed right away. With those numbers, the cybercriminal is free to use the gift cards as they choose.
- An email that looks to be from internal tech support asks employees to click a link that takes them to a website disguised to be part of the company's intranet. When the employees provide IDs, passwords or other requested data, the scammer can access their payroll records and redirect their pay into a fraudulent account.

Tips for Protecting Your Business

Keep your team well-informed. Cybersecurity awareness training sessions should be held regularly as BEC scams continue to evolve. Make sure employees understand the risks of phishing emails, the reality that a BEC attack could target them specifically, the clues that an email may be illegitimate and the importance of verifying the sender's identity.

The National Cybersecurity Alliance found, through its 2023 Oh Behave survey that cybersecurity training can be a strong motivator: 94% of respondents said they had changed their behaviors in some way following training — developing better skills for identifying scam emails or using multi-factor authentication (MFA), for example.

Ensure that employees use strong passwords and MFA. By adding an extra layer of security to the login process, MFA can reduce the risk of unauthorized access even if login credentials (usernames and passwords) are compromised. Time-based one-time passcodes (often six-digit numbers texted to the user for them to enter as a second password of sorts), hard tokens (key fobs, smart cards or USB devices), soft tokens (apps that generate one-time passcodes on demand) and biometric authentication (facial recognition, fingerprint or iris scans, etc.) are all examples of MFA solutions.

Put email security technology into place. Explore and adopt email security protocols designed to protect your domain from unauthorized access and usage. A good place to start is dmarc.org, which explains the capabilities and implementation of Domain-based Message Authentication Reporting and Conformance (DMARC).

Establish policies for verifying and reporting suspicious emails. Require employees to verify the sender of any email requesting money or sensitive information, either face-to-face or through a phone call to the purported sender's known, published number — not a phone number provided in the email. Put an incident response plan into place, too, so employees automatically alert relevant authorities and share their experiences internally to protect other potential victims.

Keep software up to date. Running the latest versions of software and keeping email servers and antivirus software updated help reduce cybersecurity risks by ensuring that the most current security measures, addressing the latest threats, are in place.

Consider email encryption for confidential information. Email encryption encodes email content so that only the legitimate recipient can read it. If an encrypted message were somehow intercepted by a bad actor, they would see scrambled, unreadable text.

Monitor and audit your systems. It's important to not only monitor your email system to detect suspicious activity but also conduct regular technology audits to uncover any vulnerabilities where hackers may be able to access your data and systems.

Do what it takes to keep your assets safe.

Dollar Bank's fraud mitigation solutions combine a variety of treasury management solutions designed to protect your accounts from unauthorized transactions, including fraudulent checks and bogus electronic transactions. Together, these solutions provide you with transparency, agility and peace of mind to stay ahead of the scams and schemes that continue to grow more sophisticated every day.

DollarBank®

Let's talk @ 1-855-282-3888.