**Is This Email Really From ‘The CEO’?**

A BBB Study Examines “Business Email Compromise” Scams

****

An in-depth investigative [study](https://www.bbb.org/becstudy) led by Better Business Bureau ([BBB](https://www.bbb.org/)) finds ‘business email compromise’ scams are skyrocketing in frequency and have cost businesses and other organizations more than $3 billion since 2016. Business email compromise (BEC) is an email phishing scam that typically targets people who remit payment for a business, government or nonprofit organization.

The FBI recognizes six types of fraudulent activity as BEC or email account compromise (EAC) fraud, which differ based on who appears to be sending the email, e.g., a chief executive officer (CEO) asking the CFO to wire money to someone, a vendor or supplier requesting a change in invoice payment, executives requesting copies of employee tax information, senior employees seeking to have their pay deposited into a new bank account, an employer or clergyman asking the recipient to buy gift cards on their behalf and even a realtor or title company redirecting proceeds from a real estate sale into a new account.

In 2018, 80 percent of businesses received at least one of these emails. This serious and growing scam has tripled over the last three years, jumping 50 percent in the first three months of 2019 compared to the same period of time in 2018. From January 2016 through May 2019, the Internet Crime Complaint Center received 58,571 complaints about BEC fraud, with reported losses in the US totaling $3.1 billion. BBB’s report found the average BEC loss involving wire transfers was $35,000, while the average loss involving gift cards ranges between $1,000 to $2,000. However, the cost to businesses can be much higher: Google and Facebook lost more than $100 million to BEC fraud before the perpetrator was arrested in 2017.

BBB urges businesses and other organizations to take technical precautions such as multi-factor authentication for email logins and other changes in email settings. The report also urges businesses and organizations to verify information changes about customers, employees or vendors, provide and require internet security training and consider implementing a confirmation policy, prior to an employee remitting payment of any kind.

**What to do if an organization has lost money to a BEC fraud:**

* If a business or organization has been a victim of a BEC fraud, they need to immediately call their bank to stop payment and report it to the FBI’s Internet Crime Complaint Center. If a report is filed within 48 hours, there is a chance the money can be recovered.
* Report fraud to [BBB Scam Tracker](http://www.bbb.org/scamtracker), even if the scam was unsuccessful. Information from attempts may help establish patterns and identify “mule” bank accounts.