northjersey.com

# Business email scams hit New Jersey hard in 2023. What they are and how to avoid them

*Amanda Wallace*

5–6 minutes

---

Don't click on that random link in your inbox, avoid answering phone calls from numbers you don't recognize and err on the side of caution before giving out any personal information online, even if the destination seems legitimate.

In this day and age, these "rules" may feel like common knowledge, but with all of the scammers and online criminals out there, even the most cautious of internet users sometimes get caught up in a scam.

Online scams can come in various formats such as fake shopping websites, contest winnings and job offers. One common type of scam is called a BEC scam. New Jersey saw the second-highest average per capita financial loss to BEC scams in 2023, said HoustonTech, a Texas-based managed IT service provider.

Here is everything you need to know:

## What is a BEC scam?

Business email compromise scams, also called BEC scams, are

one of the most financially damaging online crimes, according to the FBI. They work by exploiting the fact that many people rely on email to conduct both personal and professional business.

The FBI's Internet Crime Complaint Center (IC3) defines a BEC scam as a "sophisticated scam targeting both businesses and individuals performing transfers of funds."

In conducting a BEC scam, criminals will send an email that appears to have come from a known source such as a vendor that a company regularly deals with. The email from the "vendor" might include an invoice with an updated mailing address.

Scammers will often spoof email accounts with slight variations, send spearphishing emails that look like they can be trusted, or use malware to gain access to company networks such as email threads so they can properly time requests that are less likely to be questioned, the FBI said.

Another example from the FBI is the CEO of a company asking their assistant to buy gift cards to send out to employees. The "CEO" may ask for the serial numbers so they can be sent out right away.

Both the CEO and vendor examples have happened, and the requests in the emails were fake, leading to hundreds or even thousands of dollars being sent directly to the scammers.

According to the IC3's 2023 Internet Crime Report, the center received 21,489 BEC complaints last year with adjusted losses of over $2.9 billion.

## BEC scams in New Jersey

To determine the rankings by state, HoustonTech analyzed 2023 data on BEC crimes reported across states from the FBI's IC3. They calculated per capita losses by incorporating state populations, "providing insights into the economic impact of BEC scams in each state."

New Jersey had a victim count of 628 people out of a population of 9,290,841, equating to 6.76 victims per every 100,000 residents. New Jersey's total victim loss to BEC scams in 2023 was $140,070,206 and the loss per capita came out to $15.08.

Alaska took the top spot, with 67 victims, victim loss of $12,236,756 and a per capita loss of $16.68.

The remainder of the top 10 states with the highest per capita loss due to BEC crime in 2023 are:

- Nevada: 235 victims, $46,004,149 victim loss, $14.40 loss per capita.
- Rhode Island: 62, $14,195,616, $12.95.
- Minnesota: 321, $69,732,152, $12.15.
- Utah: 224, $38,595,361, $11.29.
- New York: 1,324, $216,249,339, $11.05.
- California: 3,161, $412,112,798, $10.58.
- Connecticut: 276, $38,103,346, $10.53.
- Arizona: 545, $76,850,493, $10.34.

"The study's findings reveal the alarming prevalence of BEC scams and their detrimental effects on state economies," said Nuresh Momin of HoustonTech. "With states like Alaska and New Jersey experiencing disproportionately high losses, it's evident that

BEC scams pose a significant threat nationwide."

## How to protect yourself

According to the FBI, ways you can protect yourself from BEC scams include:

- Be careful with information you share online or on social media, such as pet names, schools, links to family members, birthdays, etc., as these things can give scammers information that they need to guess passwords or security questions.
- Don't click on unsolicited emails or text messages that ask you to update or verify account information. Look up the company's phone number on your own and call to make sure the request is real. Do not use the phone number provided by the potential scammer.
- Carefully examine email addresses, URLs and spelling in any correspondence.
- Download carefully, and never open email attachments from someone you do not know.
- Set up two-factor or multifactor authentication on accounts that allow it.
- Verify payment and purchase requests in person or by calling to make sure they are legitimate.
- Be especially wary if the requester seems to be rushing you.

If you or your company become the victims of a BEC scam, you should contact your financial institution immediately and request that they contact the institution where the financial transfer was

sent.

To report the crime, you can contact your local FBI field office and file a complaint with the IC3 at ic3.gov.