February 11, 2020
SHARE POST

Author

Michael W. Kahn

Nacha

Business Email Compromise shows no signs of abating, as the number of complaints—and losses—soared last year, a new federal report shows.

"In 2019, the IC3 received 23,775 Business Email Compromise (BEC) / Email Account Compromise (EAC) complaints with adjusted losses of over $1.7 billion," according to the "2019 Internet Crime Report" by the FBI's Internet Crime Complaint Center (IC3).

The number of complaints rose almost 17% from 2018, while the amount lost jumped nearly 42%.

"BEC/EAC is constantly evolving as scammers become more sophisticated," noted the report released Feb. 11. Last year brought an increase in complaints about the diversion of payroll funds.

"In this type of scheme, a company's human resources or payroll department receives an email appearing to be from an employee requesting to update their direct deposit information for the current pay period. The new direct deposit information generally routes to a pre-paid card account," the report said.

While the traditional BEC methods of spoofing or hacking CEO and CFO email accounts remain popular, the bad guys are branching out.

"You may get a text message that appears to be your bank asking you to verify information on your account," said Donna Gregory, chief of IC3. That's a tactic known as "smishing."

"Or you may even search a service online and inadvertently end up on a fraudulent site that gathers your bank or credit card information," Gregory said, describing what's known as "pharming."

What can you do to avoid becoming a victim? Gregory encourages a healthy amount of skepticism, along with lots of double-checking.

"In the same way your bank and online accounts have started to require two-factor authentication—apply that to your life," said Gregory. "Verify requests in person or by phone, double-check web and email addresses, and don't follow the links provided in any messages."