Business email compromise (BEC) is a $3.1 billion problem that shows no signs of slowing. Typically, a BEC email purports to be from an executive, tricking the recipient into sending money or sensitive data.

Proofpoint recently conducted extensive research into BEC attack attempts across more than 5,000 enterprise customers between July 2016 and December 2016, including U.S., Canadian, German, French, Australian, and UK organizations. These attacks don’t involve malware, making them hard to detect with conventional security tools.

Here’s what we found.

**BEC attacks jumped 45% between Q3 and Q4 of 2016.**

75% of our customers around the world experienced at least one BEC attack attempt in the last quarter of 2016.

2/3 of all BEC attacks spoofed an email address so that fraudulent emails displayed the same domain as that of the company targeted in the attack. The recipient sees a familiar name and assumes it is safe to open.

Companies of all sizes are prone to BEC attacks. We saw no correlation between the size of the company and BEC attack volume. A larger percentage of attacks on larger companies succeed due to stronger security, but those that do net a bigger payday. Smaller companies may be less lucrative, but they’re easier targets.

Cyber criminals are targeting victims deeper within organizations. Instead of sticking to traditional CEO-to-CFO attacks, they now also target accounts payable, human resources, and engineering.

CEO impersonation continues in BEC attacks. Cyber criminals are targeting victims deeper within organizations. Instead of sticking to traditional CEO-to-CFO attacks, they now also target accounts payable, human resources, and engineering.

To learn more about BEC attacks and how to stop them, visit proofpoint.com/bec