proofpoint.

BUSINESS COMPROMISED

HOW BEC ATTACKS ARE ESCALATING AND WHO'S BEING TARGETED

Business email compromise (BEC) is a $3.1 billion[1] 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

1. FBI, "Business Email Compromise: The 3.1 Billion Dollar Scam," June 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

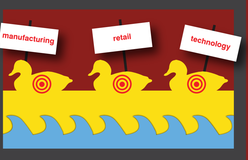
so that fraudulent emails displayed the same domain as that of the company targeted in the attack. The recipient sees a familiar name and assumes it is safe to open.

Companies of all sizes are prone to BEC attacks

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

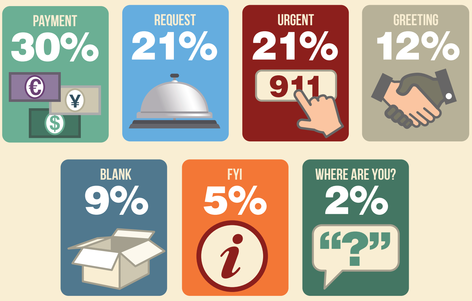
Manufacturing, retail and technology firms are targeted more often

Cyber criminals take advantage of these industries' complex supply chains and SaaS infrastructures.



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