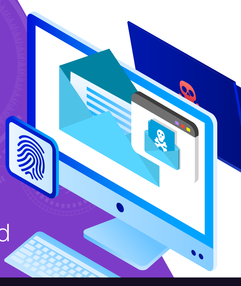
NICE · ACTIMIZE

Define, Detect, Defend:

The Path to Defeating Business Email Compromise Fraud



A rapidly growing financial threat to U.S. Businesses

A recent industry survey found business email compromise (BEC) was responsible for six in 10 frauds investigated, making it the most common fraud type among members.

In 2019, the FBI's Internet Crime Complaint Center recorded nearly 24,000 BEC complaints, totaling losses of **$1.7 billion** | an average of **$71,500** per event [1]

- At most companies, email is the main communication for employees
- The FBI estimates worldwide losses due to BEC at more than $26 billion over the past three years
- Research indicates 135 million phishing attacks are attempted every day

Define

BEC targets employees with access to company finances, using methods such as social engineering and computer intrusions.

BEC solutions:

- Focus on understanding specific challenges
- Identify fraud typologies
- Deploy targeted analytic and profiling strategies
- Enable development of targeted analytics and profiling strategies

Fraudsters trick employees into making a wire transfer to bank accounts controlled by perpetrators instead of trusted partners.

Detect

Review expected customer payment patterns, corresponding vendor relationships, and customer payment history to understand normal transactions.

Fraudsters continually shift their pattern of attack to:

- Identify targets who are the weakest links
- Gather information on internal processes
- Exploit vulnerabilities and execute fraud

Deploy real-time analytics, behavioral profiling, and user-defined rules to identify risky transactions with acceptable false positives.

Defend

- Engage operations team in the mitigation strategy
- Ensure that clients understand BEC risks and new mitigating procedures
- Develop series of predictive features for model development
- Implement effective detection strategies based on advanced analytics

Join the Fight >

1. 2019 Internet Crime Report. (2019, June 1). Retrieved June 1, 2020, from https://pdf.ic3.gov/2019_IC3Report.pdf

info@niceactimize.com | www.niceactimize.com/blog | @nice_actimize | linkedin.com/company/actimize | facebook.com/NICEActimize