



moffatt & nichol

Over 90% More BEC Threats Stopped Using Generative AI, Saved Millions of Dollars

Company

As a global infrastructure advisory firm, Moffatt & Nichol provides engineering and consulting services to clients in the marine terminal, transportation, energy, environmental, federal, and urban development markets around the world.

Challenge

At Moffatt & Nichol, threat actors were using Business Email Compromise (BEC) to initiate vendor impersonation and invoice fraud against the company through a multi-stage attack. Lookalike domains were used and emails were coming from Google Workspace accounts to evade IP reputation detection. The company was vulnerable to attacks launched using Google, Adobe, Dropbox, and other widely used trusted domains. The bad actors first "instructed" a company user to provide a mobile number for the next stage of attack. Then, the bad actors requested wire payments to the attacker's account.

Solution - Generative AI Powered Email, Mobile, and Browser Protection

- Stops credential stealing, BEC, spear-phishing, legitimate link compromise, social engineering scams, ransomware and malware in real time with fast 99.9% detection rates and a one in 1 million false positive rate
- Five-minute set-up and deployment immediately demonstrates ROI by revealing compromised devices in the organization
- Prevents smishing and BTC with zero-hour protection against the broadest range of link based and natural language threats in any mobile application
- Integrated browser extension stops zero-hour link and exploit threats in all web messaging apps including email, ads, social, search, and collaboration
- Educates employees at the point of click to reinforce training programs



BUSINESS CHALLENGE

Security didn't stop sophisticated multi-stage spear phishing, malicious attachments, and BEC vendor impersonation, invoice fraud, and others; attacks evaded IP reputation detection



SOLUTION

SlashNext multi-channel Email+ mobile and browser phishing protection; generative AI security protects against spear phishing, BEC, smishing, social engineering attacks, and others



RESULTS

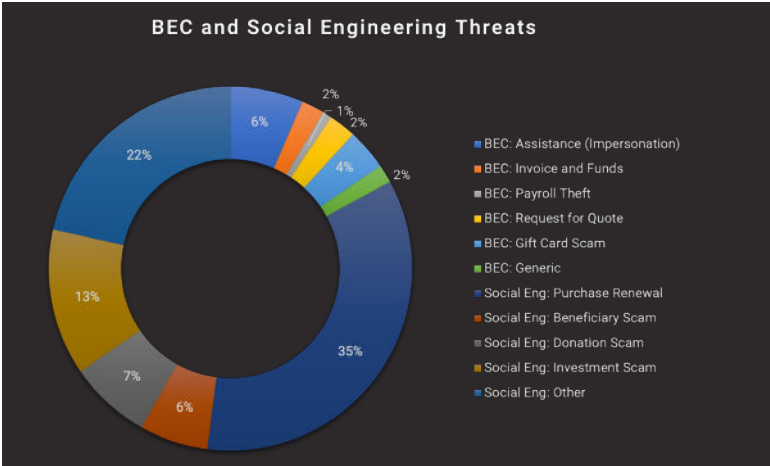
Caught 92% more BEC attacks in first month, many of which targeted C-Level employees; saved company millions of dollars from losses

SlashNext Email+ Security immediately detected 92% more multi-stage BEC and natural language attacks in the first 30 days after deployment. The types of attacks included BEC impersonation, invoice fraud, payroll theft, and others in addition to social engineering threats that were associated with purchase renewals, beneficiary information, donations, investments, and loans. SlashNext found a significantly high number of users targeted with threats that included executive impersonation, payroll theft, and invoice fraud.

According to the 2022 FBI IC3 report, the average cost of each successful BEC attack is \$124K per attack. The number of attacks caught by SlashNext saved millions of dollars in annual losses. SlashNext’s intuitive and easy-to-use console not only thwarted zero-hour phishing attacks, it also saves security analysts an estimated six hours per week to perform other critical security job functions.

“We found a lot of value in their (phishing) protection. Overall, a great addition to our cybersecurity protection suite.”

– Jason Jewitt, CIO, Moffatt & Nichols



The results align with our 2023 State of Phishing Report, which captured 12 months of customer data. In a SlashNext survey of cybersecurity professionals, 46% reported that they received a BEC attack.

The diversity and sophistication of BEC types (shown in the image on the left) have received a significant boost from the public availability of generative AI bots.

BEC Threat Types by Percentage – from SlashNext 2023 State of Phishing Report

About SlashNext

SlashNext protects the modern workforce from malicious messages across all messaging channels. SlashNext Complete™ integrated cloud messaging security platform uses patented generative AI technology with 99.9% accuracy to detect threats in real-time to stop zero-hour threats in email, mobile, and web messaging apps across M365, Gmail, LinkedIn, WhatsApp, Telegram, Slack, Teams, and many others messaging channels. Take advantage of SlashNext’s Integrated Cloud Messaging Security for email, browser, and mobile to protect your organization from data theft and financial fraud breaches today.

For more information, visit www.SlashNext.com

Schedule a customized email risk assessment at <https://slashnext.com/risk-assessment>