SLASHNEXT

CASE STUDY

C&S COMPANIES

Over 55% More BEC Threats Stopped Using Generative AI

The Company

The C&S Companies, at its core, is a 54-year-old engineering and construction firm with about 600 employees located across the United States. The firm serves government, airports, higher education, healthcare, industrial, private development, and other clients with infrastructure planning, design, and construction projects.

The Challenge

C&S realized BEC, spear-phishing, and malicious attachment attacks were increasingly bypassing their Mimecast Secure Email Gateway (SEG). They could see that their current security stack was not keeping up with email phishing attacks. Also, phishing email threats were escalating rapidly and C-Level employees were frequently targeted.

C&S knew there were other communication channels like mobile and collaboration apps that had little to no protection and they were also experiencing attacks. There was an increase in SMS phishing attacks including Business Text Compromise (BTC) and the threat actors were starting to penetrate their Teams app with new zero-day attacks occurring every day.

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

- Supplements Mimecast SEG to protect from sophisticated targeted threats
- 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 threat in all web messaging apps including email, ads, social, search, collaboration platforms

The Challenge

- Mimecast SEG failed to stop sophisticated BEC, spear phishing, and malicious attachment attacks
- Mobile and collaboration apps like Teams had little to no protection

The Solution

- SlashNext multi-channel email, mobile, and browser phishing protection
- Generative AI security protects against spear phishing, BEC, smishing, social engineering attacks, and others
- Supplements Mimecast SEG to close security gaps

The Results

- Caught 55% more multi-stage BEC attacks with 30% of those targeting C-Level employees
- Uncovered thousands of malicious links from email, mobile messages, Teams, Facebook feeds, and other channels

The Results

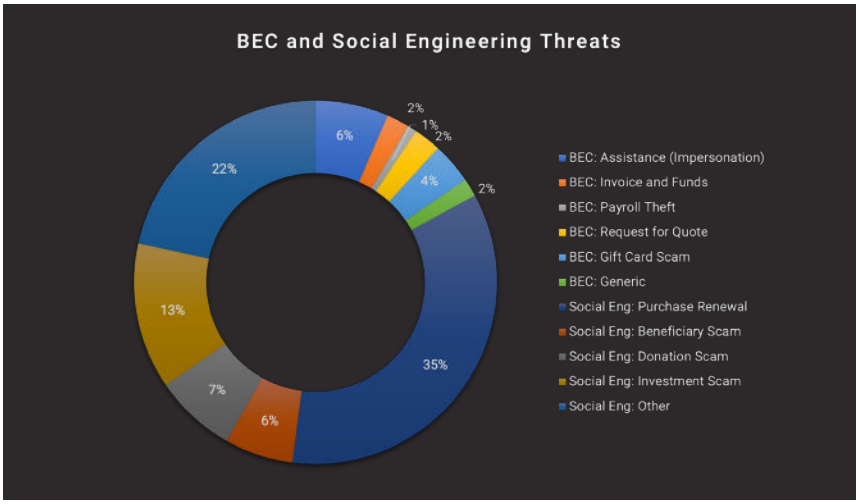
SlashNext Complete™ uncovered thousands of malicious links coming from email, mobile text messages, Teams, Facebook feeds, and other channels. In four weeks after deployment, SlashNext caught 55% more multi-stage BEC attacks with 30% of those directly targeting C-Level employees, including:

- Executive impersonation
- Payroll diversion
- 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 saved the C&S security analyst an estimated six hours per week to perform other critical security job functions.

"SlashNext and its machine learning is staying ahead of the game. It protects against links even beyond email, and provides the most serious layers of defense."

— Eric Quinn, CIO, C&S Companies



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

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 signficant boost from the public availability of generatve AI bots.

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

6701 Koll Center Parkway, Suite 250, Pleasanton CA 94566 | slashnext.com | info@slashnext.com | 800.930.8643
REV 231115