CASE STUDY

SLASHNEXT
NEXT GEN AI EMAIL+ SECURITY

Advanced Threats Blocked Using Gen AI, Over $1.2 Million Annual Savings and 5+ Hours/Wk in SOC Time

UNIVERSITY OF HEALTH SCIENCES & PHARMACY in St. Louis

Company

University of Health Sciences and Pharmacy (UHSP) in St. Louis is dedicated to educating the whole student with a challenging curriculum taught through the lens of healthcare. The school offers undergraduate, graduate, and professional degrees preparing students for a variety of health professions careers.

Challenge

The education sector is a highly targeted industry for cyber criminals and, as such, UHSP was experiencing a huge amount of malicious emails. They were using an enterprise Secure Email Gateway (SEG) and needed to stop attacks coming through. The existing approach and tooling created a highly time-consuming process, a stressful exerpience for the SOC team, and a suboptimal user experience.

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 99.99% 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

Company used an enterprise SEG but was experiencing a huge amount of malicious emails getting through; also SOC team was stretched

SOLUTION

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

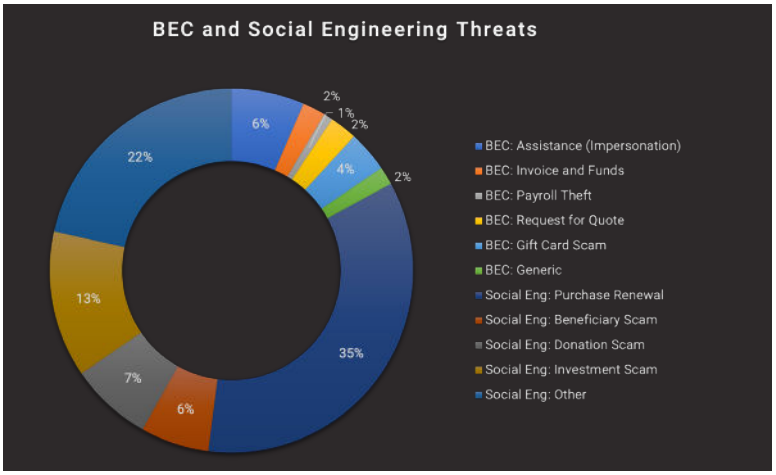
RESULTS

Saved company millions of dollars from losses and SOC team over 5 hours per week in Operating Expenses

SlashNext Email+ Security immediately increased the security footprint with a more robust next-gen solution and detected more multi-stage BEC and natural language attacks. The types of attacks included malicious emails, QR Code attacks, Smishing attacks, and other known attack vectors. SlashNext found a significantly high number of users targeted with threats at the school.

According to a recent FBI IC3 report, the average cost of each successful BEC attack is $124K per attack. At the University of Health Sciences & Pharmacy, the number of attacks caught by SlashNext saved over $1.2 million dollars in the first year. SlashNext's intuitive and easy-to-use console not only thwarted zero-hour phishing attacks, it also save security analysts over five hours per week to perform other critical security job functions.

> ***"We looked at Abnormal, Proofpoint, and Mimecast. SlashNext provided the highest detection and a solid price point."***
>
> — Zachary Lewis, Assistant VP of IT & CISO, University of Health Sciences & Pharmacy



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 99.99% 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

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

REV 240821-001