

Southeastern University Secures a Global Community with Abnormal AI

Global university uses Abnormal AI to stop advanced email threats, prevent account compromise, and automate security operations.

Southeastern University (SEU) is a Christ-centered institution of higher learning. Founded in 1935 and located in the Central Florida community of Lakeland, SEU offers more than 80 degree programs including bachelor's, master's, and doctoral degrees. Its reach expands beyond the Lakeland campus, with a comprehensive online learning program and more than 100 extension site programs nationwide. SEU is accredited by the Southern Association of Colleges and Schools Commission on Colleges.

The Southeastern University Email Security Challenge: Securing a Global University

Southeastern University operates a complex global environment spanning students, faculty, and staff, with learners traveling internationally and studying through partner sites overseas. As a result, the university couldn't rely on location-based controls alone to secure access. Email represented its top attack vector, with students frequently targeted by fake job offers, phishing, and other advanced threats. Before Abnormal, SEU's lean security team relied on Google Workspace's native protections and investigated incidents manually, often spending an entire day responding to a single campaign after accounts had already been compromised.



Industry
Education

Headquarters
Lakeland, FL

Protected Mailboxes
23,700+

Customer Key Challenges

- Protect a global community of students, faculty, and staff.
- Stop advanced email threats targeting students and contain account compromise.
- Reduce manual investigation and time-consuming workflows for a lean security team.

Abnormal Solution

- Inbound Email Security blocks student-targeted scams, phishing, and other advanced email attacks before they reach inboxes.
- AI Security Mailbox accelerates triage of user-reported messages, while Account Takeover Protection secures compromised accounts.
- Email Productivity reduces graymail so faculty and staff can focus on the messages that matter most.

"Having dealt with all the incidents that led us to Abnormal, I can say it's one of the best investments we've made to strengthen our cybersecurity posture."

Joshua Rhoden
Executive Director, IT Operations and Security



Customer Case Study

140K+

email threats remediated by Abnormal in 2025

7.5M+

graymail messages filtered in 2025

21

active account takeovers remediated in 2025

The Abnormal AI Solution

SEU relies on the Abnormal to protect students, faculty, and staff from advanced email threats. Abnormal's Inbound Email Security blocks socially-engineered attacks and student-targeted scams before they reach inboxes. Account Takeover Protection automatically detects compromised accounts and resets access, preventing lateral attacks. AI Security Mailbox automates the triage of user-reported messages and the response to submissions. Meanwhile, Email Productivity autonomously filters graymail based on learned user preferences to reduce distractions in the inbox.

Why Southeastern University Chose Abnormal

SEU chose Abnormal after an extended proof of value demonstrated that Abnormal would have stopped the threats targeting students and staff. Paired with transparent pricing that differentiated student mailboxes, it made advanced protection affordable at scale and the decision easy for leadership.

Since deployment, SEU has significantly reduced email incidents, stopped the chain of account compromises that once followed successful attacks, and reclaimed hours each week previously spent investigating threats in Google Workspace. Graymail filtering from Email Productivity keeps leaders' inboxes focused on what matters most, while Abnormal's low-maintenance design and responsive support have made it one of SEU's most valuable security investments.

Supporting the Next Stage of Cybersecurity Maturity

As SEU continues to mature its cybersecurity program, Abnormal remains a key part of that progress. The university is focused on strengthening policy, compliance, and third-party risk management, and it relies on Abnormal to keep email threats contained without adding operational burden. That gives the team more time to invest in the broader initiatives that will shape SEU's long-term security posture.

"It's a set-it-and-forget-it kind of technology. We don't have a robust team to spend a lot of time in a platform. We don't have that luxury. So it's nice having a system that works and that we can trust."

Neal Dyer
Chief Technology Officer

Abnormal Products in use:

- Inbound Email Security
- Account Takeover Protection
- AI Security Mailbox
- Email Productivity

abnormal.ai >