Abnormal
Customer Case Study

Pima Community College Protects Faculty, Students, and Staff with Abnormal AI

Multi-campus institution stops advanced phishing threats, neutralizes account takeovers, and automates user-reported messages.

PimaCommunityCollege

Industry
Higher Education

Headquarters
Tucson, AZ

Protected Mailboxes
34,000

Pima Community College (PCC) is a two-year institution of higher education in Pima County, Arizona serving the Tucson metropolitan area. The community college consists of five campuses, multiple education centers, and an online global presence. It provides traditional and online instruction for over 144 programs. PCC is one of the largest multi-campus community colleges in the United States.

The Pima Community College Email Security Challenge

Pima Community College protects 34,000 staff and student accounts across Google Workspace, creating a large, data-rich environment for attackers. In higher education, students are frequent targets because they can be easier victims for financial fraud, especially through fake job scams and credential harvesting. Before Abnormal, Pima's lean team was stuck in constant firefighting as phishing and internal email abuse demanded manual review. The team also needed better visibility into real account compromise risk and clearer ways to communicate security impact to leadership.

Customer Key Challenges

- Advanced phishing and employment scams bypassed native controls of Google Workspace.
- Manual review of user-reported messages slowed a lean security team.
- Limited visibility into true account compromise and fraud risk.

Abnormal Solution

- Inbound Email Security autonomously detects and remediates advanced email threats.
- Account Takeover Protection automatically detects account compromises, kills active sessions, and resets access.
- AI Security Mailbox automates the triage of user-reported messages.

"We want a partner that's going to constantly push the envelope and continue to innovate because the bad guys are doing the same thing... Abnormal's definitely pushing the envelope. We like to see it. And more importantly, when we give feedback, we feel like it's being heard."

Lorenso Trevino
CISO

Customer Case Study

15.98K
attacks remediated by Abnormal per month

$2.4M
total risk avoidance per month with Abnormal

7.81M
emails analyzed per month by Abnormal

The Abnormal AI Solution

Pima deployed Abnormal's Inbound Email Security, Account Takeover Protection, and AI Security Mailbox across its Google Workspace environment through direct API integration, without changing mail flow. Abnormal uses behavioral AI to stop advanced phishing, employment scams, impersonation, and internal email abuse before messages reach inboxes. AI Security Mailbox autonomously reviews user-reported emails and engages employees with informative, responsive follow up. Meanwhile, Account Takeover Protection surfaces high-confidence compromise activity so the team can respond faster and focus on higher-value work.

Why Pima Chose Abnormal

Abnormal has delivered measurable protection for PCC where it matters most. Abnormal stops advanced phishing and student employment scams before they reach users, detects compromised accounts quickly enough to prevent fraud and lateral attacks, and reduces the burden of triaging user reports manually. With Abnormal, Lorenso's team no longer manually reviews "hundreds" of emails daily, instead handling an average of three to four while freeing up capacity for other high-value priorities.

Just as important, PCC views Abnormal as a true partner and "an extension of the team." Lorenso values the evening or weekend emails he receives from Abnormal's customer success team, surfacing insights or responding to needs. That combination of strong protection, fast response, and hands-on partnership is why Pima continues to value Abnormal.

Stronger Protection with Less Manual Work

With Abnormal, PCC has moved from reactive, manual defenses to proactive, automated protection across both staff and student Google tenants. Behavioral AI now detects the subtle email attacks that once slipped past native controls, while AI Security Mailbox and Account Takeover Protection keep analyst workload low and focus attention on true risk. Backed by quarterly metrics and clear ROI framing, the security team can confidently explain value to leadership and continue investing in the platform as threats evolve.

> "[Abnormal] acts as another defender, but one that is faster than my team, one that can see things that my team wouldn't generally be able to see from the human perspective. Abnormal allows my team to concentrate on higher order alerts, higher order issues..."
>
> Lorenso Trevino
> CISO

Abnormal Products in use:

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

abnormal.ai ›

Abnormal