Abnormal

Abnormal for K-12 School Systems

Discover the AI-based email security platform that protects educational organizations from the full spectrum of attacks.

$300M in losses prevented by stopping account takeovers.

95% reduction in investigations and response times.

15+ hours saved for security teams each week through AI automation.

Abnormal Overview

- Cloud-native email security platform that protects against the full spectrum of attacks and unwanted mail.
- API-based solution integrates with Microsoft 365 and Google Workspace in minutes.
- Behavioral AI baselines normal behavior to block deviations from known good.

What Sets Abnormal Apart

- No disruption to mail flow and no changes to MX records required.
- Protection against internal and external account compromise.
- AI-driven triage, investigation, and auto-remediation for more efficient SOC workflows.

Abnormal Integrates Quickly With

- Secure email gateways and existing security layers for advanced protection.
- SIEM, SOAR, and other SOC solutions for fully automated workflows.
- Email security solution dashboards for single-source visibility into email threats, investigations, and trends.

Sophisticated Email Attacks Put Schools at Risk

K-12 schools are home to student information, intellectual property, and sensitive research data. They also have large email attack surfaces, including staff, faculty, students, board members, vendors, partner institutions, and more. That's why schools are increasingly popular targets for advanced email attacks that can cost millions to remediate.

Advanced Attackers Know How to Evade Defenses

Modern credential phishing, ransomware, business email compromise, and account takeover attacks get past legacy defenses. Every threat that reaches the inbox puts school systems at risk for data breaches, FERPA violations, IP theft, financial losses, reputational damage, and loss of public trust. And while security awareness training is beneficial, ensuring that thousands of students, staff, board members, and others know how to spot an attack can be exceedingly difficult.

Modern Email Security for Educational Organizations

Abnormal's cloud-native solution integrates with Microsoft 365 and Google Workspace in minutes and uses thousands of signals across identity, behavior, and content to separate legitimate messages from dangerous threats. Abnormal quickly learns to recognize anomalies in messages to immediately detect and remediate threats that are targeting your faculty, staff, students, and others.

Criminals Target K-12 School Systems

82%

of K-12 schools experienced a recent cyber incident.

$3.5M

average cost of a data breach in the education sector.

45%

of attacks on K-12 schools target human behavior.

Source: K-12 Dive

Source: IBM Cost of a Data Breach Report 2024

Source: 2025 CIS MS-ISAC K-12 Cybersecurity Report

Abnormal for K-12 School Systems

Stop the most dangerous attacks that bypass your existing defenses.

Supply Chain Compromise

When your vendors are compromised, you can be compromised too. Attackers who breach trusted vendor email accounts can send fraudulent invoices and credential phishing attacks that bypass your security systems.

How Abnormal Stops Supply Chain Compromise:

Automatically knows your vendors

VendorBase™ auto-identifies suppliers, vendors, and partners via past email conversations and other signals gathered across the entire ecosystem.

Continuously monitors vendor risk and reputation

Assigns each vendor a risk score based on domains spoofed, accounts compromised, and suspicious messages.

Examines message content, tone, and attachments

Uses AI and ML to inspect emails and attachments for suspicious signals that can indicate vendor fraud and block the threat from reaching inboxes.

Credential Phishing

Attackers can spoof the internal email addresses of instructors or administrators to steal login IDs and passwords from students or staff, which they can then leverage to launch more damaging attacks.

How Abnormal Stops Credential Phishing:

Inspects email headers to expose impersonations

Determines when an email domain has been spoofed by analyzing header information.

Detects suspicious language, tone, and style

Recognizes the language that indicates phishing attacks, even in messages with no malicious links or attachments.

Understands communication patterns

Applies natural language processing (NLP) to learn people's typical tone, behavior, and communication patterns to detect changes that may indicate phishing.

Ransomware

Ransomware can disrupt classes, expose student data, and even cause schools to permanently close. Socially-engineered emails can trick students or staffers into giving credentials to attackers, who then access and encrypt critical systems.

How Abnormal Stops Ransomware:

Analyzes message content and other signals for credential phishing

Utilizes identity detection and NLP to spot first-stage attacks like phishing, even when messages come from trusted senders.

Blocks malicious attachments and links

Reviews all attachments and links for safety, including links that redirect upon clicking.

Gives security teams explainable insights and malware forensics

Automatically prepares detailed analyses of ransomware attempts, enabling teams to preview attachment content and link targets.

Account Takeover

The FBI has consistently warned education systems about a growing number of stolen academic credentials for sale online. Similar to this, criminals can use these credentials to access internal systems and steal or ransom sensitive data.

How Abnormal Stops Account Takeover:

Determines good sender behavior with multichannel analysis

Leverages API integration with Microsoft 365 and Google Workspace to analyze end-user behavior across devices, browsers, and apps.

Actively monitors user behavior and identity

Detects changes in content and tone, attempts to bypass multi-factor authentication, and shifts in normal login signals and then auto-remediates suspect accounts.

Includes unique VendorBase™ analysis and monitoring

Baselines known-good interactions with your vendors and evaluates vendor risk scores across the federated database of all customers to understand when a vendor may be compromised and block suspicious emails.

Abnormal

Request Your Abnormal Demo Now: abnormal.ai/demo ›