Secure Your Campus Against Email Compromise

Email risk is a reality for every educational institution

Educational institutions - whether K-12 or universities - want their students to have an open, transparent, and secure learning experience. Cybercriminals exploit this transparency by using impersonation and social engineering to target the human layer of campuses - students, faculty, and staff.

The 2021 Verizon DBIR found that 50% of breaches in the Education sector involved social engineering. Around 80% of these social engineering breaches involved Pretexting as a tactic, which is heavily associated with BEC.

If an email workflow can be spoofed by scammers, that workflow needs checks and balances in place.

$1.86 B
Reported losses from BEC and EAC attacks in 2020 according to the FBI Internet Crime Report

50%
Percent of breaches in 2020 in the Education sector that involved social engineering according to the Verizon DBIR

36%
Percent of breaches in 2020 that involved phishing as a tactic, up from 25% last year according to the Verizon DBIR

Education’s unique email security challenges

Lean IT and security teams
Your teams have a lot on their plate and often lack the time and resources to triage and respond to high-volume email threats.

Device & application sprawl
Your students have multiple email IDs, bring their own devices, and work across many cloud applications for daily work. All those email IDs and apps are potential entry points for compromise.

Weaponized transparency
Your institution has open staff directories and contact details for transparency - but that opens up the door for a variety of email impersonation attacks.

Productive (but risky) behaviors
Your students and staff may think of security as a blocker, using personal VPNs and executing workarounds for ease of work. This fogs over visibility for security teams and can lead to email account compromise.

WHY ARMORBLOX

More than 56,000 organizations across industries and sizes trust Armorblox to secure their human layer against targeted attacks and data loss.

Stop BEC, impersonation, extortion, and other sophisticated email threats that get past Microsoft, Google, and SEG security controls.

Prevent your faculty and student email accounts from being compromised by cybercriminals and used to launch follow-on phishing attacks against stakeholders.

Safeguard your personal, banking, research, and intellectual property data from cybercriminals without hampering your daily work.

Reduce the burden on strained IT / security teams with prebuilt detection policies and automatable response workflows.

Improve investigation quality with detailed email threat insights that are built for human eyes.

Quick time to value with deployment over APIs that takes minutes and works with Office 365, Google Workspace, Exchange, and hybrid email environments.

Armorblox is a proud member of the Internet2 community.

Reassign your security team to higher-value activities by reducing phishing triage and response times by 75-97%.
How Armorblox Secures Campuses Against Email Compromise

Armorblox helps educational institutions communicate more securely over email using the power of Natural Language Understanding (NLU). Armorblox connects over APIs to understand the content and context of communications and secures the human layer from compromise. Educational institutions use Armorblox to stop BEC and targeted email attacks, protect sensitive PII and PCI, and reduce phishing response times for user-reported threats.

How It Works

- Connects over APIs in 5 minutes
- Builds communication baselines for your organization and users
- Automatically flags targeted email attacks - no custom policy creation needed
- Automated and configurable remediation actions (delete, quarantine, lock user account) across affected mailboxes

Capabilities

**Inbound Email Protection**
- Stop targeted attacks such as BEC, spear phishing, impersonation, and vendor fraud.
- Use detailed threat intelligence and IOCs that draw from 1000s of signals across identity, behavior, and language.
- Simplify email security operations with OOTB detection policies and automated remediation actions.

**Email Account Compromise Detection**
- Detect and block emails that try to phish for account credentials e.g. fake O365 login portals.
- Identify anomalous email behavioral patterns and remotely lock suspicious user accounts.
- Prevent data exfiltration by detecting anomalous mail forwarding rules, suspicious email forwards.

**Outbound Email Protection**
- Detect loss of sensitive PII/PCI over email e.g. SSNs, bank account details.
- Configure in compliance mode (only monitoring and detection) or block mode (applying enforcement actions to noncompliant emails).
- Increase accuracy with language-based models that identify PII/PCI within email context.

**Abuse Mailbox Remediation**
- Automatically monitor and analyze every user-reported email threat.
- Auto-remediate safe emails and known threats to focus on reported emails that need human review.
- Remove identical and similar suspicious emails across user mailboxes with one click.

Hear From Others Like You

"Wow! Here’s a technology that solves the problem for us. We’re tired of saying sorry to our clients and other stakeholders.
- CIO, Business School, University of California"
For IT and Security Teams

- Secure the campus against targeted email attacks like BEC, spear phishing, impersonation, and other threats that steal money and data.
- Prevent campus email accounts from getting compromised and being used to launch follow-on phishing attacks against external stakeholders.
- Save time on email security operations with quick deployment, rich threat insights, pre-built policies, and automatable remediation actions.
- Shift the perception of ‘security as a blocker’ to ‘security as an enabler’ with in-context email threat education for your end users.

For Faculty and Students

- Communicate over email and other cloud applications with confidence.
- Reduce the likelihood of your email account being compromised and used as a vehicle for phishing attacks against people you know.
- Safeguard your personal, banking, research, and intellectual property data from cybercriminals without hampering your daily work.
- Learn about suspicious email threats within the context of your regular email workflows with informative warning banners.

Why Armorblox for Education?

Algorithms That Understand Hidden Threats
Armorblox algorithms understand the content and context of email communications to stop today’s advanced threats.

Detection & Response That Saves Time
Armorblox has out-of-the-box detection policies and automated response actions that take email security busywork out of your hands.

Machine Learning Tailored to Your Business
We don’t have all the answers, but you do. Armorblox builds custom ML models for every customer and end user to keep learning and get better with time.