Stop Email-Based Financial Fraud

Attacks know the easiest way to the bank is through email

The most advanced email attacks today target humans and workflows rather than any security system or architecture. By compromising client accounts, using impersonation, and exploiting existing email workflows, these attacks cause billions of dollars of losses every year.

The FBI reported that Business Email Compromise (BEC) and Email Account Compromise (EAC) attacks accounted for $1.86 billion in losses in 2020 alone.

Any email workflow that can lead to the transfer of money is a workflow that needs checks and balances.

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

66%
Percent of advised investors who would switch financial advisors in case of a breach, according to a Fidelity study

36%
Percent of breaches in 2020 that involved phishing as a tactic according to the Verizon DBIR

Financial services’ unique email security challenges

Lean IT and Security Teams
Financial services security teams have a lot on their plate, often lacking the time and resources to triage and respond to high-volume email threats.

Client Email Compromise
Wire fraud is often carried out from legitimate (but compromised) client email accounts, which bypass eye tests as well as traditional security controls.

Financial Workflows Over Email
Whether it’s invoices, notifications from banks, or communicating with financial advisors, a lot of money travels over email. Attackers know this.

Credentials are King
Many credential phishing attacks try to extract victims’ banking or wealth management login details through brand impersonation.

Why Armorblox

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

Fidelity Institutional has a strategic relationship with Armorblox to protect their over registered investment advisors and end clients from targeted email attacks.

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

Identify when your end clients’ accounts have been compromised and are being used for payment/wire fraud.

Safeguard your personal, banking, and other sensitive data from cybercriminals without hampering your daily work.

Save time for strained IT/security teams with prebuilt detection policies and automatable response workflows.

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

Reassign your security team to higher-value activities by reducing phishing triage and response times by 75–97%.
How Armorblox Stops Email-Based Financial Fraud

Armorblox helps financial services firms 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. Financial services firms use Armorblox to stop BEC, wire fraud, and targeted email attacks, protect sensitive PII and PCI, and save time by automating the remediation of user-reported email 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 across affected mailboxes

Capabilities

**Inbound Email Protection**
- Stop a wide range of targeted email attacks - whether they have malicious links, 0-day links, or no links at all.

**Email Account Compromise Detection**
- Stop cybercriminals from taking over email accounts to launch attacks and exfiltrate sensitive data.

**Outbound Email Protection**
- Safeguard sensitive PII, PCI, and unencrypted passwords against accidental or deliberate exposure over email.

**Abuse Mailbox Remediation**
- Save time for the security team by automating triage and remediation of user reported email threats.

```
Hear From Others Like You

"Within two weeks of implementing Armorblox, it caught a client email compromise. We were able to quickly reach out to the client and head off any damage that could have occurred. Armorblox was the immediate identification tool that helped us take these preventive actions."

- Greg Fulk
  COO, Valeo Financial Advisors
```

**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.

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

Vendor / Invoice Fraud
Armorblox analyzes customers’ vendor communication history to flag compromised or spoof vendor email accounts being used as vehicles to steal money or data.

Armorblox detects:
- Identity: Impersonation attempt, vendor risk score.
- Behavior: Low communication history, vendor communication patterns.
- Language: Unusual request, changed banking details.

Payment Fraud
Armorblox stops cybercriminals from requesting fraudulent payments by pretending to be trusted entities.

Armorblox detects:
- Identity: Impersonation attempt, low reputation domain.
- Behavior: Low communication history.
- Language: Deadline, urgency, unusual payment request, financial topics.

Credential Phishing
Armorblox prevents attackers from stealing data by spoofing emails and landing pages from trusted service providers e.g. O365 login portals, banking portals.

Armorblox detects:
- Computer vision & image analysis: Fake login portal.
- Behavior: Low communication history.
- Language: Urgency, bad link.

Payroll Fraud
Armorblox identifies when attackers impersonate employees and email the payroll team with false direct deposit information.

Armorblox detects:
- Identity: Impersonation attempt.
- Behavior: Low communication history.
- Language: Urgency, unusual request, financial topics.

56,000 ORGANIZATIONS PROTECTED
5 MINUTES TO DEPLOY OVER API
75-97% REDUCTION IN PHISHING RESPONSE TIMES
Armorblox Benefits and Value

**For IT and Security Teams**
- Secure the organization against targeted email attacks like BEC, spear phishing, wire fraud, and other threats that steal money and data.
- Prevent internal 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 contextual email warning banners for your end users.

**For Financial Investment Advisors**
- Position your firm as one that prioritizes securing their end clients’ money and data.
- Provide peace of mind to your end clients that your firm has measures in place to stop email-based financial fraud.
- Safeguard your company’s sensitive data and end client data from targeted attacks and human error.
- Learn about suspicious email threats within the context of your regular email workflows with informative warning banners.

ARMORBLOX IS PROUD TO WORK WITH:

**Fidelity Institutional**

Learn More ⇢

Why Armorblox for Financial Services?

**Algorithms That Understand Hidden Threats**
Armorblox algorithms understand the content and context of communications to stop targeted phishing attacks and payloadless threats.

**Detection & Response That Saves Time**
Armorblox has out-of-the-box detection policies and automatable 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.