Email Security Service – Frequently Asked Questions

Service Overview and Capabilities

What is the email security service offered?

A cloud-based email security solution that protects against phishing, malware, and account compromise using advanced monitoring and detection.

Who is the provider/What platform are you using?

University of Texas Regional Security Operations Center (UT-RSOC) is the provider, and Abnormal AI (formerly Abnormal Security) is the platform.

What does this service provide?

Abnormal AI provides artificial intelligence (AI)-driven security services that protect organizations from phishing, business email compromise, and account takeover attacks by analyzing behavioral anomalies rather than relying on traditional email filtering rules.

Will this replace Gmail or Microsoft 365?

No. Abnormal integrates with your existing platform and does not replace your email system.

Does it work with Google Workspace?

Yes, Abnormal supports both Google Workspace and Microsoft 365 environments.

Will it support student and staff email?

Yes.

Why Abnormal if we already have an email security solution?

Abnormal complements traditional secure email gateways and native Microsoft/Google protections by focusing on behavioral analysis and post-delivery detection of sophisticated attacks, such as business email compromise, account takeover, and vendor fraud.

How does this email security service compare to traditional email security platforms?

Abnormal differs from traditional email security platforms by focusing on post-delivery detection of social-engineering attacks using behavioral analysis, and it is often deployed alongside native or gateway-based email security solutions.

Technical Integration and Compatibility

What do I have to change on my system?

Abnormal integrates using secure API (application programming interface) connections rather than inline mail routing or installed agents. There are no agents to deploy and no changes required to MX (mail exchange) records or mail flow.

Will it disrupt email?

No. Abnormal AI does not disrupt email delivery or mail flow. It connects to your email environment (Microsoft 365 or Google Workspace) using API-based integration. There are no agents to install, no changes to MX records, and no downtime. Email continues to flow normally while Abnormal analyzes messages after delivery and takes action only when a threat is detected.

Can we keep current tools?

Yes, Abnormal can operate alongside existing tools or replace them later if desired.

Will Abnormal work with my other products and tools? (e.g., Darktrace, Checkpoint, Fortimail, Mimecast, etc.)

Yes. Abnormal AI is designed to work alongside existing security tools and should not interfere with or disrupt other products in your environment. Because Abnormal uses an API-based integration and does not sit in-line with email delivery, it can coexist with secure email gateways, network security tools, and other monitoring solutions.

For questions about specific tools or configurations, school systems should contact UT-RSOC to review compatibility and provide guidance based on your environment.

Does the product or service have a customer interface or dashboard?

Abnormal AI provides a unified portal for all core functionality. The centralized interface reduces operational complexity, accelerates response, and simplifies onboarding.

Implementation and Participation Requirements

What is required for implementation?

To implement email security services through UT-RSOC, a school system must:

- be a Texas school system (either charter or independent district)
- complete the TEA email security pre-registration survey form sent to the Cybersecurity Coordinator on 4/21/2026.
- execute an interlocal contract (ILC) with UT-RSOC

What if I cannot find the TEA email security pre-registration survey form?

Email TEA at k12cyber@tea.texas.gov and request your unique survey link.

What if my school already has an agreement with another RSOC?

This email security service is only being offered through UT-RSOC at this time. However, the RSOCs (regional security operation centers) coordinate closely with one another to ensure alignment and support.

During implementation, notify UT-RSOC that you receive services from another RSOC, and they can coordinate with your RSOC so that they have visibility into your dashboard and can provide additional guidance and support.

If I already signed an ILC with my RSOC, will I need to sign another one with UT-RSOC?

Yes.

Operations and Security Functionality

Can we evaluate the service before enabling remediation?

Yes. School systems can begin in a passive monitoring mode where threats are identified and reported without automatically removing messages. This allows school systems to review detections and build confidence before enabling active remediation.

What does active remediation look like with Abnormal?

Active remediation automatically removes confirmed malicious emails from user inboxes after delivery, reducing exposure to threats. The malicious emails are put into a quarantine folder.

What support is included?

When email security services are provided through UT-RSOC, participating organizations receive both the Abnormal email security platform and UT-RSOC support for onboarding, threat monitoring, incident awareness, and security operations coordination within Microsoft 365 or Google Workspace environments.

Who has access to data?

When a school system uses Abnormal AI through UT-RSOC, the school system retains ownership and primary access to its data. Abnormal accesses only what is necessary for email security via district approved APIs, and UT-RSOC has limited visibility for security operations support without assuming control or ownership of district systems or data.

What control do school systems have?

School systems that participate in Abnormal AI services through UT-RSOC retain full ownership and control of their data, systems, policies, and incident response decisions, while UT-RSOC provides optional security monitoring, threat analysis, and advisory support.

Does the solution have access to personal or institutional data?

Abnormal processes customer personal data as necessary to provide the service. This includes analysis of email metadata (e.g., headers and footers), email content, attachments, and related system data such as message IDs. You can review Abnormal's Privacy Notice https://abnormal.ai/service-privacy-notice or visit their Security Hub https://security.abnormal.ai to review security compliance.

Are you providing consulting services?

No.

Cost, Funding and Commitment

What does it cost?

This service is provided at no cost to the school system. TEA pays for the service through the K-12 Cybersecurity Initiative fund.

Will the funding continue?

This service is funded through this biennium (2026-2027) and is expected to be funded through the next biennium (2028-2029) with legislative support.

If I sign up, how long am I obligated for?

There is no long-term obligation. You may cancel the service at any time. Once the service is implemented, it will continue on an ongoing basis and does not require annual reenrollment. The service remains active unless you choose to cancel it.

Where can we learn more?

Additional information is available on the TEA K-12 Cybersecurity Initiative site