Abnormal's Email Protection

Kyle Oliveira - 2024-11-01 - Comments (0) - Security

Abnormal's email protection is an advanced email security platform, integrated with Brown's Gmail service, that automatically detects and removes email-based threats, such as phishing, malware attachments, and business email compromises. It helps ensure a safer and more efficient email experience.

Below are frequently asked questions regarding the use of Abnormal. For any additional questions, please contact the OIT Service Center for assistance.

What is Abnormal?
Abnormal's email protection platform leverages artificial intelligence (AI) and machine learning to detect and prevent a wide range of email-based threats, including phishing and account takeover.

Abnormal's approach is based on understanding normal user behavior patterns and identifying anomalies that could indicate a security threat. This allows it to detect and block malicious emails before they reach users, protecting organizations from potential data breaches and financial losses.

Why are we using Abnormal's email protection?
On average, Brown receives 170 phishing attacks per day, impacting many community members. These attacks clutter our inboxes and force us to spend extra time verifying the legitimacy of messages, diverting attention from our work and studies. Moreover, they are very sophisticated now, convincing even the most threat-aware people to react by providing their credentials. When this happens, the damage comes swiftly, with people losing control of their university data, their personal information, and even sometimes their pay. The resulting cleanup takes a lot of time and is often an emotional ordeal.

This tool provides an automated method of putting attack messages out of harm's way. It works by evaluating attachments and links to assess potential threats, and keep them out of Inboxes.

Abnormal's email protection also enables us to detect unusual login activity, mail rule filter changes, shifts in email content and tone, and unusual recipients - key indicators of account compromise. This allows for a faster response to protect both you and the University from damage and data breaches.

How does Abnormal's email protection impact me?
Abnormal Email Security automatically detects dangerous and suspicious messages and removes them from your inbox.

You still need to be mindful of email-borne threats, but the number of malicious messages you receive will be dramatically reduced.

An email message appeared and disappeared from my inbox without me doing anything — should I be concerned?
Abnormal Email Security processes messages in a secure 'sandbox' after they arrive in our email environment. This can lead to messages being delivered and then remediated if deemed a threat. While this happens in milliseconds, you might notice a message appear and then disappear if actively monitoring your inbox. This is normal, however, if you have any concerns, please contact the OIT Service Center so we can confirm that the removal was part of the security tool's operation.

An email message I was expected to receive has not arrived and I do not see it in my spam folder — what should I do?
Abnormal may rarely inadvertently flag legitimate internal correspondence as malicious. In the unlikely chance this may have occurred, open a OIT Service Center ticket and OIT will confirm if the message arrived and if there were any security concerns with its contents.

Please include:

- Sender Email
- Subject
- Approximate timeframe email was sent

If the message was incorrectly flagged, OIT will recover the message, and Abnormal will dynamically learn from the situation, lowering the possibility of 'false positives' in the future.

What should I do if I find a suspicious email in my inbox?
Please report the email using the Phish Alert button so we can assess and help improve the tool.

Is Abnormal reading all my emails?
Abnormal processes and stores only the minimum amount of data, including personal data, necessary to enable it to perform its functions. It does not store, persist, or retain the contents of or attachments to email that the Abnormal identifies as non-malicious using its machine learning models; rather, only email content and attachments (if any) that it identifies as malicious are transferred to its cloud-based servers for further processing and analysis.

How does it appear in Gmail's recent activity list?
Abnormal will appear on Brown Gmail accounts' recent activity window as the Authorized application **116920771689407251245**, with a Virginia (VA) location/IP address. Rest assured, this is normal behavior.

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	**Location (IP address) [?]**	**Date/Time** (Displayed in your time zone)
Authorized Application (116920771689407251245) Show details	United States (VA) (100.28.21.230)	1:46 pm (0 minutes ago)

If you see other unrecognized account activity, or have reason to believe your account may otherwise be compromised, open an OIT Service Center ticket.