Abnormal

Protect Grant Funding

Secure your federal funding from the full spectrum of cyberattacks with a robust cloud-native solution.

Federal financial assistance, primarily administered as grants, is one of the most significant sources of funding for state, local, and tribal governments, as well as educational institutions across K-12 school districts, colleges, and universities. Most often, federal grants are awarded as direct cash assistance, but federal grants can also include in-kind assistance.

There is an estimated **$1 trillion** in outlays for aid to state, local, tribal, and territorial governments in 2023. Unfortunately, these funds are prime targets for bad actors to attempt to steal. The ever-changing landscape of business email compromise (BEC) accounts for more financial loss than any other cyberthreat—and the media attention resulting from these grants enables threat actors to obtain all the information they need to target employees with socially-engineered attacks.

There is little denying that government employees and grantees play a key role in preventing fraud related to taxpayer-funded programs.

Email-Like Attacks Targeting Your Funding

Cybersecurity risks in grant funding pose a significant threat to organizations and individuals alike. Cybercriminals often target grant funding as a source of money, knowing that grant administrators may not have the same level of security in place as traditional banking institutions.

Cyberattackers may use a variety of methods to gain access to grant funds, such as phishing, malware, or social engineering techniques. These attacks can lead to a loss of funds, disruption of services, increased risk of data breaches, and reputation damage to the grant recipient. It is crucial that grant administrators take the necessary steps to protect their funds from cyber threats.

Recently there have been numerous accounts of Local Governments suffering attacks targeting Federal Funds for such things as Housing and Rental Assistance, COVID funding, ARPA funding, and others.

In light of these threats, many organizations are turning to Abnormal Security to safeguard their federal financial funds. Abnormal offers a robust cloud-native security solution so you can prevent email and email-like attacks that target your grant funding, while automating your security operations.

$1.2 trillion
Issued in federal financial assistance to state, local, tribal, and territorial governments in 2022.
**Grants.gov*

175%
Increase in BEC attack volume between over the last years.
**Abnormal Research*

$2.7 billion
Lost to BEC attacks in 2022 alone.
**FBI Internet Crime Center (IC3)*

Abnormal Keeps Your Grant Funding Secure from Email Threats Aiming to Steal It

- Baselines known good behavior across employees, vendors, and partners by analyzing every email from every identity across thousands of contextual signals, to build risk-aware detection models and stop all types of inbound email attacks
- Automatically builds searchable knowledge engines with detailed profiles of your organization's employees and vendors and monitors their risk levels.
- Remediates malicious emails to a hidden folder within milliseconds, removing the possibility of end user engagement.
- Fully automates email triage, remediation, and reporting, bringing together all auto-detected and user-reported threats into a single interface.
- Helps employees and executives be more productive by automatically moving unwanted mail out of the inbox..

See Abnormal in Action. **Request a Demo.**

abnormalsecurity.com →

Abnormal for Grant Funding

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.

Account Takeover

The FBI notified colleges and universities in May 2022 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 the 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 suspicious 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.

Credential Phishing

Attackers can spoof the internal email addresses of government officials or educational institutions to steal login IDs and passwords which they can leverage to access grant funding.

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

Socially-engineered emails can trick government officials or staffers into giving credentials to attackers, who can then access and encrypt critical information.

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.

See Abnormal in Action. **Request a Demo.**

abnormalsecurity.com →