Minidoka County School District

IT Department

Board Report - June 2025

- **Forms and Processes being worked on:**
  - **Onboarding/Exiting Employee & Student Processes and Procedures – Working with HR and appropriate stakeholder on this – This will continue into the Summer to make sure everything is in order**
  - **Student Fines and Fees**
    - **This has been updated**
    - **New model of devices ordered and will be getting ready soon**
- **New devices:**
  - **Working on old device decommission**
  - **New student devices ordered**
- **Adobe Pro Licenses:**
  - **The state is loading the licensing into our portal for any and all staff, students, or users in the district.**
- **Ticket Status 6/12-7/11:**
  - **31/47 Closed/Open (Analytics Attached)**
- **Abnormal Email Security:**
  - **Phishing Software for the district due to how bad it got for phishing emails.**
  - **Implemented July 1st**
  - **In the last 45 days of it being in view mode there were 17,318 email attacks**
  - **In the last 30 days (Analytics Attached), 7,947 attacks which is an overall decrease of 3,358 attacks from the previous 30 days. Which is probably lower due to having no students and most of the staff off not utilizing their emails as much.**

Source: All

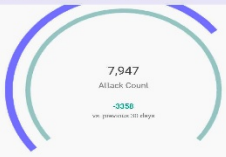
Last 30 days | Download

Attack Trends | AI Security Mailbox | Attack Highlights

Attack Overview

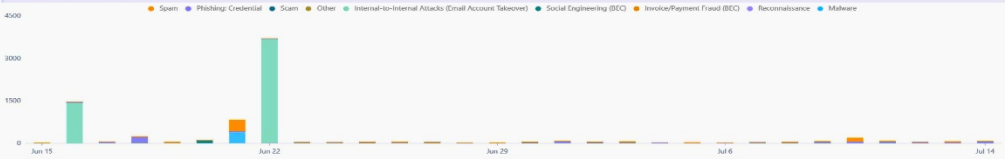
Attacks Stopped

Abnormal has detected 7947 attacks that reached your organization in the selected 30 days, down 3358 from the previous 30-day period.



Attack Frequency

Over the selected 30 days, Abnormal detected an average of 264 attacks per day, with a low of 22 attacks on Jun 15 and a high of 3720 attacks on Jun 22. The most common attack type daily was Internal-to-Internal Attacks (Email Account Takeover) (an average of 170 per day), while the least common was Invoice/Payment Fraud (BEC) (an average of 0.7 per day).



Attack Deepdive

Trending Attacks

Over the entire 30 day period, Abnormal detected Internal-to-Internal Attacks (Email Account Takeover) as the most common attack type for your organization. For reference, the most common attack type in the previous 30 day period was Internal-to-Internal Attacks (Email Account Takeover).

Attack Types	Attack Count	vs. Previous Period
Internal-to-Internal Attacks (Email Account Takeover) Attacker compromises an employee's account and delivers other internal employees fake invoices, credential phishing, and other malicious content	5110 (64%)	-1837 -19%
Phishing: Credential Attacker tricks victim into giving away their online credentials to unauthorized parties	718 (9%)	+402 +127%
Malware Attacker attempts to deliver malicious payload	410 (5%)	+389 +1852%
Scam Advance fee fraud and similar scams	240 (3%)	+59 +33%
Social Engineering (BEC) Attacker impersonates employee to establish rapport with victim recipient and convince victim to engage in actions such as changing direct deposit information, paying fake invoice, buying gift cards, or performing another task	167 (2%)	+136 +439%
Other Non-categorized attacks	127 (2%)	+17 +15%
Reconnaissance Unusual characters/Lack of subject or message content. Common signal of when attackers attempt to verify deliverable recipient email address in order to follow up with future phishing messages.	36 (0%)	+15 +71%
Invoice/Payment Fraud (BEC) Attacker impersonates a vendor, partner or well known brand and asks recipient for fake invoice/payment	21 (0%)	+2 +11%
Spam Unsolicited and unsolicited communications	1116 (14%)	+459 +70%

Attack Vector Breakdown

Over the selected 30 days, Abnormal found that Links were the most prominent means of attack against your organization.

Attacker Details

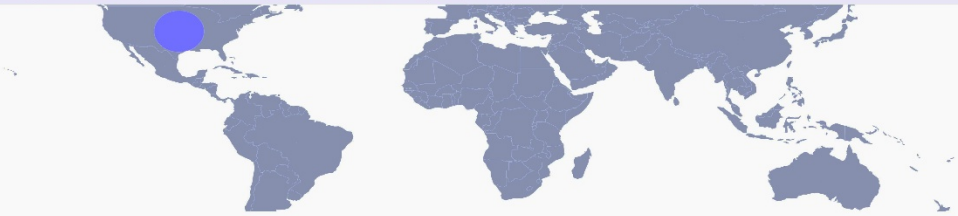
Attacker Strategy Breakdown

Abnormal found that, in the selected 30 days, attackers tried to commit fraud most often via Internal Compromised Email Account, Unknown Sender, and Name Impersonation. Click on each strategy to see example emails stopped by Abnormal.

Attack Strategies	Attack Count
Internal Compromised Email Account Sent from another employee's account of the same organization, without triggering alerts and with no unusual authentication.	5110 (64%)
Unknown Sender Sent from a never before seen sender, including fake employees/partners or real emails from unknown organizations.	2015 (25%)
Name Impersonation Uses sender name and/or email address to impersonate a party.	766 (10%)
Spoofed Email Sender address uses a forged domain; this usually results in unusual or failing authentication statuses.	41 (1%)
Covid 19 Related Attack Employs the context of Covid 19 as an attack strategy.	15 (0%)

Attacker Origin

For attacks detected by Abnormal in the selected 30 days, the highest number (7375 attacks) originated in United States of America, Ukraine (77 attacks), and Ireland (48 attacks).



Americas	7413
Europe	218
Unknown	209
Asia	95
Africa	16
Oceania	2

Sender Impersonation Breakdown

The top three entities most impersonated over the last 30 days are Employee (other), None / Others, and Brand.
This information can be helpful in training your employees about attacks they're most likely to receive.

Employee (other)	5299
None / Others	2230
Brand	249
VIP	104
Unknown Partner	50
Known Partners	4

Most Impersonated Entities

All Employees

Over the selected 30 days, the employees most commonly impersonated in email attacks are Heather Hepworth, Barbara Gallegos, and John Kontos. Click on each name to see example emails stopped by Abnormal.

Entity Name	Attack Count	vs. Previous Period
Heather Hepworth	95	+95 -
Barbara Gallegos	9	+6 +200%
John Kontos	8	+7 +700%
Gary Mittelsteadt	8	+5 +167%
Donna Cameron	5	+3 +150%
Reckea Stoker	5	+2 +67%
Scott Heins	4	+1 +33%
Lara Barfuss	4	+1 +33%
Krysta Haugeberg	4	+4 -
Gregory Durrant	4	+1 +33%
Ellen Austin	4	+1 +33%

Affected Employees

Recipient Employees Breakdown

VIP

The VIPs who received the most email attacks over the selected 30 days are Angela Davidson, Sean Boyer, and Dyann Blood. Click their names to view specific attacks received by these individuals to help you determine whether extra training and monitoring efforts may be needed.

Name	Job Title	Attack Count	vs. Previous Period	Attack Types
Angela Davidson		69	+37 +116%	
Sean Boyer	Director of Information Technology	66	+38 +141%	
Dyann Blood		63	+34 +117%	
Danelle Stutzman		30	+20 +200%	
Ellen Austin		28	+20 +250%	
Veronica Granillo		19	+17 +850%	
Katie Rogers		16	+9 +129%	
Heather Hepworth		15	+8 +114%	
Ashley Johnson		13	+9 +225%	
Jeannie Coulson		11	+8 +267%	
Gregory Durrant		11	+5 +83%	

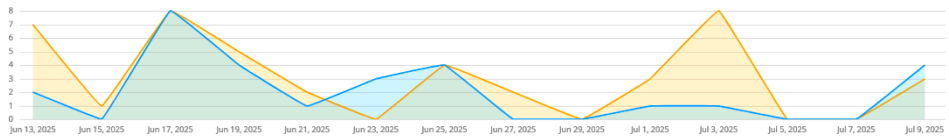
All Activity

Please wait - Exporting image ..

06/12/2025 › 07/11/2025

Explore ticket analytics filtered only by your permission level

Ticket Resolution Over Time (closed tickets vs. newly submitted)



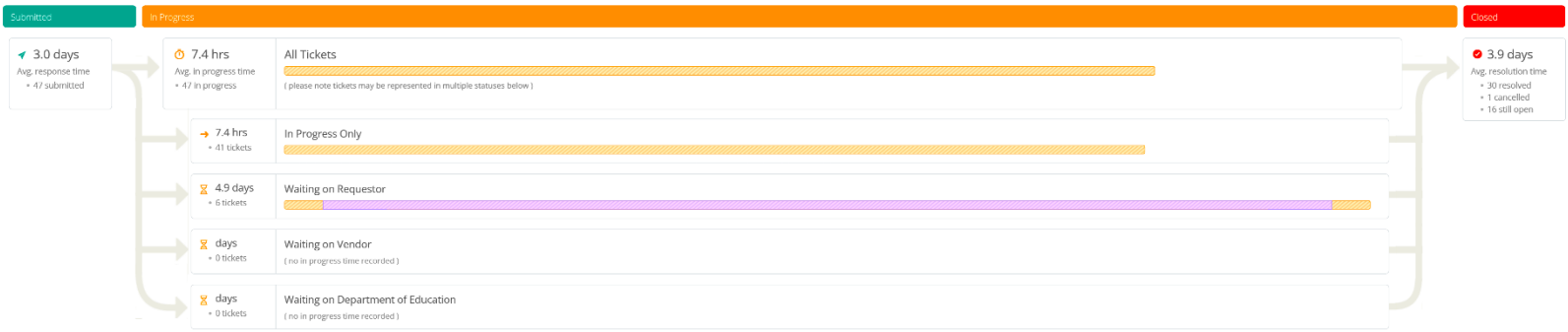
1.9 days
Response time (avg)
for all ticket statuses

31
Tickets now closed
out of 47 submitted

2.1 days
Resolution time (avg)

16
Tickets still open
3 waiting on requestor

Ticket Pipeline Analysis (shows time spent in each status, along with ticket routing for all workflows)



Top Models (sorted by total tickets)

0 minutes
Avg. time logged per ticket

SLA Response Time

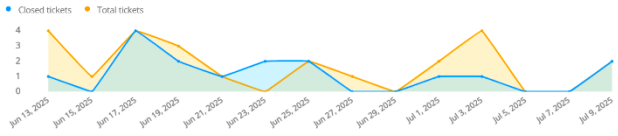
No data available

SLA Resolution Time

No data available

Tickets by Priority

Total Tickets Over Time



Tickets Submitted For

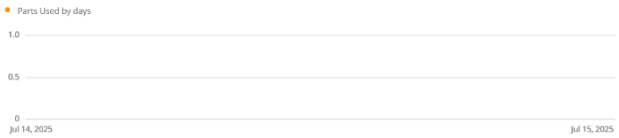
Response Time

Total tickets

% Parts Used

No data available

Quantity Parts Used



Resolution Time

Top 10 Parts Used

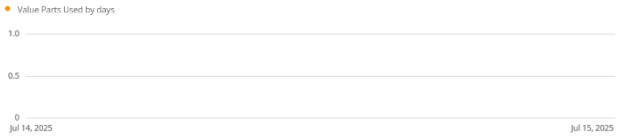
No data available

Top 10 Parts Used

% Value Parts Used

No data available

Value Parts Used



Top Issue Categories (sorted by total tickets)