Customer Case Study

Savannah-Chatham County Public School System Protects Teacher Inboxes and Saves Employee Time

The school system reduced the number of phishing attacks in teachers' inboxes and hours spent on remediation by deploying Abnormal.

The Savannah-Chatham County Public School System (SCCPSS) serves more than 35,000 students and 55 schools with the mission to "ignite a passion for learning and teaching at high levels". The system is known for its innovative use of technology and its focus on each child and their future, and it strives to prepare all students to be successful and productive citizens. Teachers constantly work to cultivate a curriculum in which children can maximize their limitless potential in school and in life.

The SCCPSS Security Challenge

The struggles of SCCPSS are no different from any other public school system: there are finite resources, but they must continue to do it all. "Like many public schools, we're challenged with financial resources – both human and technical – to keep the data of our staff and students safe," said Carl Eller, Senior Director of Information Security and Technology Management, who oversees the organization's cybersecurity initiatives in addition to his other responsibilities. "We strive to protect data so it can't be used against parents or students."

SCCPSS

Industry
Education

Headquarters
Savannah, GA, USA

Employees
5,000+

Protected Mailboxes
5,000+

Customer Key Challenges

- Stop display name spoofing and bad actors targeting employees that resulted in personal financial losses.
- Prevent business email compromise (BEC) attacks and detect compromised vendor accounts.
- Increase employee efficiency by filtering away time-wasting phishing attacks.

Abnormal Products

- Inbound Email Security
- Email Account Takeover Protection
- Abuse Mailbox Automation

"One of the great advantages of Abnormal has been that it really runs itself; we don't run it. We're not in the Abnormal Portal every day, but I can see that it's stopping the things that we need it to block."

Carl Eller
Senior Director of Information Security and Technology Management

Customer Case Study

75+
Employee hours saved weekly on remediation.

1,228
Credential phishing attacks detected and remediated in 90 days.

48K
Attacks detected in 90 days.

The Abnormal Security Solution

Eller found Abnormal at a time in which there had been a few successful phishing attempts in the district. “We were doing a lot of work to stop emails that looked like they were coming from the principals, asking teachers to buy gift cards and other suspicious actions.” The cybersecurity division realized these vulnerable groups needed an added layer of protection.

The team explored multiple solutions to remedy this issue; some blocked too many emails, others were unable to conduct the behavioral analysis necessary to detect sophisticated spoofing emails. In contrast, the Abnormal proof of value process yielded the desired results. Said Eller, “As soon as we flipped that over to Abnormal, the attacks went away.”

Why SCCPSS Chose Abnormal

Display name spoofing was one of the biggest challenges SCCPSS faced. Human resources and payroll were constantly targeted with requests to change banking account details and contact information. Employees often detected these and did not make the changes, but the increasing number of attacks was overwhelming. Eller knew these emails were an issue. “It was wasting time because they were getting between 10 to upwards of 500 a day, then they'd have to follow up with each person. Adding Abnormal blocks these emails and saves them time.”

Abnormal also helped employees in the cybersecurity department, which Eller oversees. Prior to Abnormal, security employees would have to manually review all potential phishing emails and manually respond to them. “We had to go in and investigate, only getting through 20-30 each day, but we probably had 100 come in,” said John Middleton, Defense Engineer. Previously, the team had four individuals spending four hours a day moderating and looking into potential phishing. Since implementing Abnormal, they have saved roughly 75 hours a week—time they can now dedicate to other tasks.

Finding Time Savings and Making Happy Users

Eller knows he has helped his faculty and staff by implementing Abnormal. “If we were getting a hundred spoofing emails a day before, we're getting one a week now.”

With implementing Abnormal and the resulting massive time savings, the cybersecurity team is now able to concentrate on other threats. “We get thousands of malware or malicious alerts a day through avenues other than email and we have to investigate them. There's plenty we can now focus on, because we don’t have to determine whether an email is spam or not.”

> "We have to make an annual report to the board each year. The metrics from Abnormal help us to show that there is a true threat out there; we’re not making this up. The data shows how many people are trying to attack us, how many business email compromise threats we receive, and how many vendor attacks it’s stopping. The dashboard provides all the data we need."
>
> Carl Eller
> Senior Director of Information Security and Technology Management

abnormalsecurity.com →

Abnormal