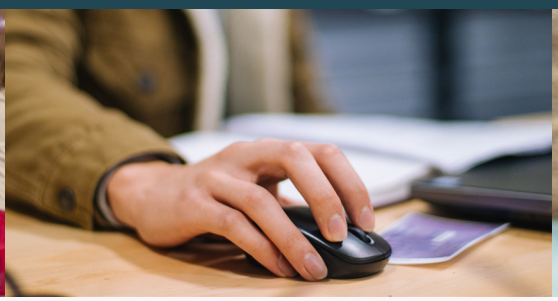
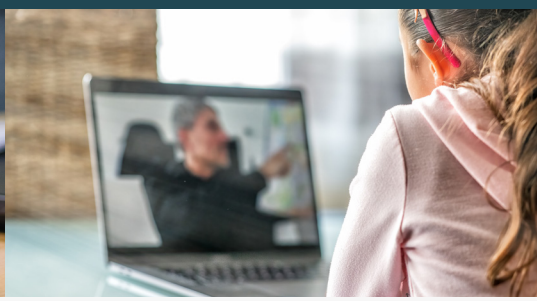
Customer Case Study

Virginia Beach City Public Schools Charts Course for Student Success, Staff Productivity, and Community Trust

Virginia Beach City Public Schools (VBCPS) is one of Virginia's top-performing school divisions, educating approximately 65,000 K-12 students—all of whom have division-issued Chromebooks and Gmail accounts. Because VBCPS uses Microsoft 365 for faculty and staff email, the division's small IT team must protect two large email ecosystems in compliance with federal COPPA, CIPA, and FERPA regulations governing students' data privacy.

There are wider concerns, too. "Approximately 20% of our student population has military ties," said CIO David Din. "We're always concerned about the potential for a data leak that would allow threat actors to connect student information with military information. Generally, K-12 is a high-value soft target because of the student data and a traditional lack of resources to stop attacks."

"It's getting harder to distinguish between a malicious email and a legitimate email, and it's not possible to mandate security training for K-12 teachers because of contract stipulations and because teachers have too much on their plates already." Among the issues affecting teachers were impersonation emails that scammed some of them into making gift card purchases.

With a small team, complex challenges, and limited resources, Din needed better security tools. "We made a strategic decision to look for an AI-based solution to understand and learn from the tactics that attackers are using to get emails into end-users' mailboxes, and to stop them from reaching our users."

VIRGINIA BEACH CITY PUBLIC SCHOOLS
CHARTING THE COURSE

Industry
Primary and Secondary Education

Headquarters
Virginia Beach, VA

Employees
14,160+

Protected Mailboxes
192,000+

Employees
19,950+
(Microsoft 365)

Students
172,000+
(Google Workspace)

Schools Targeted by Impersonation Emails

Attackers evade schools' secure email gateways by posing as administrators or trusted brands. During the first half of 2022, education and religious organizations received more than twice as many brand-impersonation emails as the next-most-targeted sector. Since activation, Abnormal has detected and blocked BEC attacks that impersonated cybersecurity brands, universities, VBCPS employees, and the superintendent.

"Abnormal is a set-it-and-forget-it solution, taking the worry out of cloud email security. The combination of behavioral AI to find malicious emails and automation to remediate them allows my team to focus on other things."

David Din
CIO

Customer Case Study

187,000+

all-time attacks found by Abnormal over the past 9 months.

16,000+

credential phishing attacks stopped.

59

high-risk compromised/ impersonated vendor email accounts detected by VendorBase™

A Single Security Solution for Multiple Email Ecosystems

Abnormal complemented the VBCPS existing security stack, which includes Microsoft and Google Workspace. “Managing a large number of mailboxes across two systems, we needed comprehensive threat protection that would work with Gmail to protect student inboxes and Microsoft 365 to keep threats out of staff and faculty inboxes,” said Shane Snedecor, Information Security Manager.

Abnormal’s API-based solution was simple to use from the start. “With a couple of clicks and in less than an hour, we were up and running—first in read-only mode. It was eye-opening to see all the emails that Abnormal could catch and remediate,” Snedecor said.

“Prior to turning on Abnormal, attackers would create one Gmail address after another to impersonate familiar people—our superintendent, principals, and teachers. We couldn't do much about those attacks before. We have a Google Workspace instance that we use for students, so we couldn't block Gmail addresses. With Abnormal, it catches those impersonation emails automatically, so we don’t have to spend time responding to those threats manually.”

Stopping Account Takeover, Preserving the School Division’s Reputation

With Abnormal stopping the impersonation attacks, VBCPS senior leadership has fewer worries about email attacks putting their reputation and community trust at risk. Staffers and teachers also have more confidence that the messages they receive are safe to open and act on.

Abnormal also simplifies management of two complex email ecosystems. Because Abnormal integrates easily with Office 365 and Google Workspace, the VBCPS security team was able to apply the same advanced solution to both platforms, increasing security and visibility into threats.

“Abnormal’s dashboard gives us good information,” Snedecor said. “The weekly reports show what kind of threats we’ve been remediating.” Better visibility also helps the team answer questions from individual users about specific email messages. “Maybe it’s in their junk folder or it got caught by a rule the user set up without realizing it. With Abnormal I can search for a specific message and see what’s going on with it right away.”

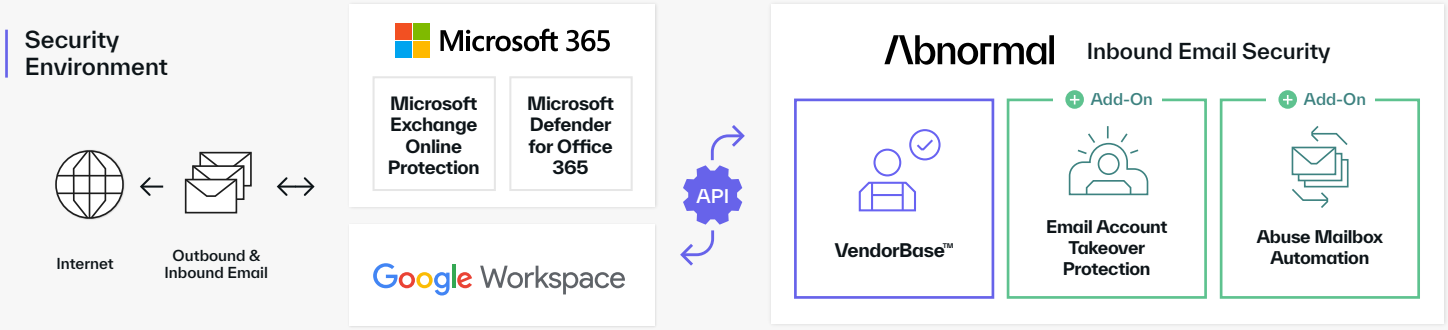
Email Account Takeover Protection

Credential phishing attacks can give attackers access to victims’ email accounts so they can steal data, launch ransomware, and commit financial fraud. Recently, 63% of the attacks on VBCPS were credential phishing emails, and 83% used name impersonation to deceive recipients. Now, Abnormal baselines normal VBCPS email user behavior to detect and instantly block credential phishing and name impersonation messages.

888

internal email account takeovers detected by Abnormal in the past 9 months.

Customer Case Study



AI-driven Automation Saves Security Team Time

Abnormal has also freed Snedecor and his team from time-intensive manual investigation and remediation tasks. “Before Abnormal, we'd have to look up reported emails in the Office365 portal and engage another team that’s more experienced with Microsoft Exchange products to find the suspicious emails quickly. Often, by the time they could run a script to remediate bad emails out of mailboxes, users might have already opened them,” Snedecor said. The process required many hours each time.

Now, remediation is instant. That’s critical for Snedecor’s small team. “I’ve got two people on security and our email team has a couple more. The automation from Abnormal is amazing, and not just with the emails that it catches and auto-remediates. Our users can easily report emails they’re concerned about to Abnormal, and it automatically assesses them as good or post-remediates them—not that we see many false positives now.”

A Partnership That Builds Trust and Creates Value

Din said working with Abnormal helps the whole organization. “When an email goes out impersonating the superintendent, that creates a trust issue that can be difficult to recover from. By stopping these kinds of emails, Abnormal helps us maintain our reputation in the community. Imagine all of the time and stress that we've saved our teachers, staff, and administrators because they don't have to worry about malicious emails. That’s a huge value.”

> “When we started O365 and Google Workspace in full enforcement with Abnormal, there was a back-end issue, and the support team was very easy to work with to resolve it. They’re always available when I reach out for anything,”

Shane Snedecor,
Information Security Manager

abnormalsecurity.com →