Phishing and Malware Prevention
through Google Workspace for Education Plus

Statement

Threatened as the target of both phishing and malware campaigns, educational institutions are searching for a solution that fits seamlessly into their environment that can quickly identify and mitigate security threats.

Results

In combination with Google's Security Summit, Amplified IT worked with the leaders at Mid-Del to identify key security issues within the school districts ecosystem and assisted with the implementation of Google Workspace for Education Plus to alleviate the districts phishing and malware threats.

How does Google Workspace for Education Plus mitigate phishing and malware security threats?

The Mid-Del School District is based in the Oklahoma City metro area. The district serves more than 14,600 K-12 students and supports 22 public schools, a career technology school, and virtual academy. The district was an early Google trailblazer in Oklahoma with initial adoption beginning in 2011 with continual growth, which has been a critical contributor to their success in 2020 when classes went virtual. Their Google for Education technology expansion has been a critical contributor to their ability to easily move studies virtual with Google Classroom and 1:1 device allocation.

Email security has been a key topic in the Mid-Del School District. Prior to the district transitioning their email system to Google, they were the regular targets of phishing and malware campaigns. The Security Dashboard and advanced Gmail visibility were the two features that initially drew the IT team at Mid-Del to consider the upgrade to Education Plus.

15,000+ Students & Staff

1:1 Chrome Devices

Mitigated Attack within first 30 days

The Security Dashboard and advanced Gmail visibility provided the team with the ability to fully and easily see an email message, header, and attachments from the console. "This additional ease in investigation management is important because without it our ability to respond to a security incident would be delayed due to longer investigation times." With the standard version of Google Workspace for Education, viewing an email that could be "potentially malicious", requires the use of other tools such as Vault, Google Apps Manager (GAM), or other 3rd party tools, which can incur lag times for resolutions as well as the use of additional resources.

> "Google Workspace for Education Plus is a must for school districts wanting to increase security in their Google environments. This upgrade in services provides enterprise-level tools needed to address the everyday security challenges plaguing public education. This upgrade coupled with the expertise of Amplified IT will enhance and secure your district's Google environment and presence."
>
> **-Alison Hood -** System Administrator,
> Mid-Del Public School District

Furthermore, in the Spring of 2020, the State Board of Education shut down all public schools and instituted distance learning for the remainder of the school year as a response to COVID-19. Instantly the district had to operate with 90% of our staff at home. Thankfully, having Google Workspace for Education Plus already in place, the team was able to immediately use the Google Meet and Chat features to communicate with staff, students, and parents. Teachers were also able to pick up where they left off in Google Classroom if they were already utilizing that feature. These tools allowed Mid-Del to offer one-to-one communication while maintaining social distancing, which was crucial to their success.

Today, the daily processes at Mid-Del Public Schools have evolved from being reactive to proactive. With Education Plus security features, their IT team has the ability to see and stop almost all phishing scams before reaching the user. Learn how to optimize your domain with Google Workspace for Education Plus or other Amplified IT products and services by connecting our team of experts.