proofpoint.

Princeton University Keeps Communications and Reputation Safe With Proofpoint Email Security

The Challenge
- Help secure interaction with students, faculty and vendors
- Safeguard domain reputation
- Support cloud migration strategy

The Solution
- Proofpoint Secure Email Relay

The Results
- Secures transactional email from internal applications and SaaS providers
- Scalable, flexible solution accommodates emerging cloud strategy
- Safer outgoing email protects email domain and reputation

The Organization

How does a world-renowned institution like Princeton University maintain its sterling reputation in the academic world? Assuring trust and integrity in every interaction is essential. And protecting its email and domain with Proofpoint solutions is a critical first step.

The Challenge

Securing academic collaboration
More than 200 years old, Princeton University is one of the highest-ranked universities in the world. Serving 8,500 students, the private Ivy League institution provides undergraduate and graduate instruction in the social sciences, humanities, natural sciences and engineering.

Like all research universities, Princeton depends on its communications infrastructure to support an open exchange of ideas—and its day-to-day operations. Keeping critical services, such as email, operating safely and securely is the responsibility of the central IT office.

"I have six people in my group, two of whom are focused on email services, infrastructure and routing," said Mark Ratliff, director of cloud infrastructure, office of information technology at Princeton University. "We have mailboxes in Google, which are mainly student accounts, as well as mailboxes in Microsoft Exchange Online. We have no mailboxes on premises any longer, but we do have our own SMTP server on-prem, and we have a Listserv on-prem."

Ratliff and his team strive to work strategically. They have a long-term focus on moving more of the university's infrastructure to the cloud, strengthening security, and ensuring safe, reliable email delivery. When the university updated its email system, the team realized that it needed a dependable solution to protect its outgoing email.

"We needed an outbound mail server, and since we're looking to move our infrastructure to the cloud, we didn't want to stand up any infrastructure on our own network," said Ratliff. "As we looked at several options, we needed to know that the service that any vendor provided us would be reliable. We needed a solution that would allow our Listserv system to occasionally send high volumes of outbound email, which is something that Exchange Online and GMail will not allow. We also wanted spam and malware detection and filtering capabilities for outbound email."

"We wanted some protection in the event one of our on-prem systems was compromised, as well as the ability to detect whether someone inadvertently sent spam outbound. We wanted to protect our email and domain reputation. Proofpoint gave us the control over outbound email that we needed."

Mark Ratliff, director of cloud infrastructure, office of information technology, Princeton University

The Solution

Maintaining the integrity of outbound email
Princeton was familiar with Proofpoint solutions, and chose Proofpoint Secure Email Relay to support its updated email system. This hosted solution meets all of the university's requirements, and it prevents compromised third-party senders from sending malicious email using the organization's domains.

"We wanted some protection in case one of our on-prem systems was compromised, as well as the ability to detect whether someone inadvertently sent spam outbound," said Ratliff. "We wanted to protect our email and domain reputation. Proofpoint gave us the control over outbound email that we needed. We had a longstanding relationship, and knew that they were more than capable of providing reliable service."

Proofpoint Secure Email Relay helps the university better manage third-party senders that are sending email on its behalf. This gives Ratliff and his team better visibility and control.

"We have departments on campus that use third-party services for various functions, such as organizing conferences and communicating with alumni groups," explained Ratliff. "The vendors of these services will often send email on behalf of the university from their own mail servers without properly configuring email authentication. If those vendors instead make use of our instance of Proofpoint Secure Email Relay, email authentication will automatically be in place."

The Results

Protecting the university's users and reputation
Proofpoint Secure Email Relay enables Princeton to regain control of its third-party senders by enabling consolidation and centralized management. It provides improved visibility by validating third-party senders who are sending emails using its domains.

"The Proofpoint Secure Email Relay service addresses our need for monitoring and control of outbound mail," said Ratliff. "Other email relaying services assume that the email being sent is authorized and safe. They perform no security analysis on the messages being sent. We needed a solution that would monitor outbound email for malicious content. We were pleased to get that capability with Proofpoint."

The Proofpoint solution is both flexible and scalable. This gives the university a future-ready platform that will continue to support its evolving infrastructure strategy.

"We plan to shift usage away from our on-prem SMTP servers with the goal of ultimately eliminating that infrastructure. We will need to modify some of our email routing from Microsoft Exchange Online and from our Listserv service. Devices and applications on campus will be reconfigured to make use of Proofpoint Secure Email Relay."

With its Proofpoint solution in place, Princeton can continue to develop its cloud and communications strategy. And it can be confident that its domain and reputation remain protected.

LEARN MORE

For more information, visit **proofpoint.com**.

proofpoint.