Case Study

mimecast

UNIVERSITY OF CHICHESTER

Mimecast Earns Top Grades for Email Security from the University of Chichester

3 weeks

A one-month implementation schedule accelerated into a smooth three-week onboarding.

couple clicks

Email remediation that used to take 20 to 30 minutes and several steps is now possible in a couple of clicks.

10 fold

The volume of suspect emails spotted grew tenfold overnight after deploying Mimecast.

> "I know that there will be some apprehension about deploying security controls whilst balancing good customer service, but with Mimecast, we didn't hold back, and we're really pleased that we didn't."
>
> **Haydn Tarr, IT Service Development Manager at the University of Chichester**

Business case

The U.K.'s University of Chichester needed to establish stronger cybersecurity defenses that could keep up with evolving threats and scale as its student body and staff grew – but without adding to its administrative workload. IT administrators also felt a duty to prepare students for the cyberthreats they could face in their future careers.

Results

Choosing a suite of Mimecast email protection tools, the university was able to fortify its network from attacks and ensure outgoing mail was safer and less likely to end up in spam folders. The ease of implementation and user-friendly interface have made the work of IT less onerous while increasing security.

> “I found the interface a lot friendlier than the Microsoft interface. It’s easier to find everything, work out what’s a threat and then get rid of it.”

Andrew Thompson, Senior Technical Specialist at the University of Chichester

Overview

Institutions of higher education – and the public sector overall – have been a prime target for fraudsters, especially when learning went remote during the COVID-19 pandemic. Fortunately, the University of Chichester had managed to remain relatively safe from harm. Just a couple of relatively minor cyberattacks over a two-year period had succeeded in affecting a small number of users at the 183-year-old U.K. institution, though the university had not experienced any major breaches or ransomware attacks.

Still, the IT staff didn’t want to rely on luck to secure the university’s 5,500 full-time students and 1,000-member staff, located across two campuses. Even those small incidents required the university’s full-time IT staff – IT Service Development Manager Haydn Tarr and Senior Technical Specialist Andrew Thompson – to spend roughly 30 hours on mitigation and remediation, which was time that could have been put to better use, Tarr said.

Learn more about Mimecast’s complete suite of security solutions.

For more about the University of Chichester, visit its website **here**.

Knowledge Is Power

The only university in the county of West Sussex, Chichester continues to grow. Recent additions include a new nursing school and more business degrees, all of which has expanded the student body and staff, as well as the digital workload volume in the university's servers. At the same time, groups such as JISC, the U.K. membership organization advocating for technology upgrades in higher education, have been increasingly emphasizing the need to improve cybersecurity in the sector.

As the pandemic progressed and new technologies were adopted, the university's IT team noticed an increase in impersonation attempts against senior staff members who steer the university's strategic direction. In 2021, the team began looking for a stronger, more scalable email security solution that could address the university's needs, including improved URL and attachment protection.

"We also get a lot of students who are very technically [savvy] and really do make the best use of the university services that we provide," Tarr explained. "We're prepared for the fact that these students might be curious, and they might start exploring our network in ways that students haven't done before – which from a security perspective is something that we need to be prepared for, whilst also providing a flexible and accessible service."

Previously, the University of Chichester had been depending on the email security protections included in Microsoft 365 Office, which provided the email infrastructure for students and staff.

"But due to the proliferation of attacks and the sheer quantity of threats observable in the Internet, Exchange Online Protection wasn't enough," Tarr said.

Many other higher education providers had also implemented additional protections running alongside Exchange Online Protection, "so we knew we were heading in the right direction," he added.

Doing Their Homework

The university looked at four different technologies before choosing Mimecast's Perimeter Defense plan for email security, along with Internal Email Protect and Sync & Recover. Finding a solution that didn't require significant administrative overhead was an important consideration, one that ruled out a solution used by many financial organizations because it required too much coding to filter out potentially offensive emails.

"Immediately that was a nonstarter for us because it was not in our best interests to dedicate the human resources to do that," said Tarr. Added Thompson, who had worked with Mimecast in three previous organizations, "It's always been a very smooth process to implement and work with Mimecast."

Integrating Mimecast's threat remediation capabilities providing by Internal Email Protect into the Office 365 environment has streamlined the process to identify and get rid of a single malicious message from 20 to 30 minutes of running traces and writing scripts into a couple of clicks, Thompson noted. The interface is also a lot friendlier, he said.

"It's just made life 10 times easier," Thompson said. "It's easier to find everything, work out what's a threat and then get rid of it."

Additionally, IT wanted a solution that made transparent to users the protections brought to bear on their email accounts.

"We have a duty of care to our students when they go off to employment," Tarr said. Protection against phishing and malware without prompts to explain to users why it was necessary could send students into the work world without being prepared of email threats, he said.

"Mimecast does strike that balance of great security controls whilst also raising the awareness of our students and staff," he added.

Mimecast's products also were easy to integrate with an existing firewall from Palo Alto Networks and other Microsoft Office 365 products in use, without the need for wholesale customizations. The Palo Alto Wildfire firewall communicates with Mimecast's email protection tools and vice versa, so email attachments are double-checked by both.

Ahead of Schedule

The onboarding process itself moved smoothly over a period of three weeks, one week earlier than Tarr had expected. Everything went as expected with no service impact at all, he said.

Tarr also had praise for Mimecast's implementation manager, Ian Stobie, and the team. Having a sole point of contact for questions was a plus, he added.

"The questions I asked were welcomed and treated promptly, which made us feel more at ease," Tarr said. "We never had a security product that looked after email like Mimecast. So that was good."

Mimecast's protections showed their worth immediately after deployment. Suspect emails tagged by the filters increased nearly tenfold from the volume seen under Exchange Online Protection, which rejected less than 3% of emails received.

"In terms of noticeable changes, there is a lot less spam being delivered to people's inboxes, a huge reduction in harmful emails, including phishing and malware … and malicious attachments that have a delayed payload," Tarr said. "We're seeing a wholesale reduction in offensive emails and fewer impersonation attempts happening across our email estate."

Additionally, Thompson noted that fewer outgoing messages are now landing in their intended recipients' spam folders. "I think we've had some people very happy that the emails they're sending out to customers aren't getting chucked into the junk folder," he said.

After an initial year-and-a-half run with Mimecast, the university recently implemented Mimecast's DMARC Analyzer to better protect against domain spoofing.