CASE STUDY

proofpoint.

UNIVERSITY STOPS EMAIL THREATS BEFORE THEY ARRIVE ON CAMPUS

PROTECTING USERS AND DATA, BOTH COMING AND GOING

CHALLENGE

- Stop phishing attacks to prevent credential theft
- Prevent university communications from being blocked
- Respond faster to potential incidents
- Protect sensitive patient and financial data from loss

SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection with URL Defense
- Proofpoint Email Encryption
- Proofpoint Email DLP

RESULTS

- Reduced phishing and unauthorized mass mailings to nearly zero, stopping advanced threats from reaching users' mailboxes
- Automated data loss prevention and encryption and gained detailed reporting without affecting the user experience
- Saved hours and days of time dealing with phishing attempts and remediation
- Respond up to 60 percent faster to stop or remediate a potential incident

Lincoln Memorial University was founded in 1897 as a memorial to America's 16th president, Abraham Lincoln. Today, it's a private four-year coeducational liberal arts college with almost 4,000 students working toward undergraduate, graduate, and professional degrees. With students and faculty members increasingly targeted by phishing attacks, the university chose Proofpoint for greater protection and peace of mind.

"Phishing was our biggest problem," said Clandis Smith, Network Administrator at Lincoln Memorial University. "Phishing emails got through our Barracuda filtering solution and tempted students, faculty, and staff to click on malicious links."

Phishers blatantly threatened users through impostor emails that supposedly came from the university's IT department. Emails would tell users that they had exceeded their email limits or that their mailboxes would be shut down unless they clicked a link. When they clicked, the link took them to an outside web page asking for their logins and passwords. From there, phishers used the credentials to send spam emails, which put Lincoln Memorial University on numerous "blocked" lists.

Smith's team would have to disable the user's account, change passwords, and sometimes remediate the machine, which could take up to a day. Even more time-consuming was having to contact each block list to be removed, and some of the lists required payment—adding insult to injury. During this process, the university was hampered from delivering email to alumni and the broader community.

PROTECTING USERS AND ACCELERATING RESPONSE

The IT team began looking for a spam filter replacement to deliver better email protection. After considering Proofpoint, Mimecast, and McAfee solutions, Lincoln Memorial University chose Proofpoint to help protect users and data.

"Attacks increasingly target individuals," said Smith. "We chose Proofpoint because the company and its solutions are mature, and it's an acknowledged leader in the Gartner Magic Quadrant for secure email gateways."

The university built its new defenses on Proofpoint Email Protection to protect the university from unwanted and malicious email. Email Protection gives the IT team detailed visibility and email continuity in the event of an outage. Proofpoint Targeted Attack Protection (TAP) adds strong protection against advanced email threats that use malicious URLs. TAP detects and blocks known and unknown threats, giving the team confidence with a broad view of the email threat landscape and human-assisted threat intelligence from Proofpoint. To complete its email defenses and protect sensitive data, the university deployed Proofpoint Email DLP and Email Encryption. Email DLP automatically enforces email communication policies from a central location, so neither users nor the IT team have to worry about sensitive information accidentally leaking. Email Encryption automatically secures outbound email messages and attachments based on configured policies without interfering with the way users work.

“All email now runs through the Proofpoint cloud,” said Smith. “We can stop advanced threats in email before they even arrive in our users’ mailboxes. At the same time, we can protect data being sent out to further reduce our attack surface. We’re protected coming and going.”

CONSISTENT DATA PROTECTION AND BETTER REPORTING

Before Proofpoint, the university’s two medical clinics and financial aid teams used a third-party DLP and encryption solution that ran in their Outlook. Now, if email senders know that a message includes data that needs encrypting, they simply type “encrypt” in the subject line, and Proofpoint automatically encrypts it. If a message contains sensitive data and hasn’t been encrypted, Proofpoint notifies Smith to review and approve it before it’s sent.

“We feel much more secure knowing that information isn’t accidentally leaked or compromised,” said Smith. “We also have better control and insight because Proofpoint reports which emails were encrypted and what was sent.”

BLOCKING AND TACKLING

Smith says that TAP has been a tremendous help. When it detects a suspicious email with a malicious URL, it blocks the entire email. If a phishing email does get through and the user tries to click the link, TAP blocks him from going to the site and notifies Smith’s team that the user’s machine might be affected.

“Phishing and mass emails have stopped,” said Smith. “It’s rare to see a phishing email, but if we do, we know who clicked, when they clicked, and if there is a problem. It’s a huge headache that’s gone.”

TIMING IS EVERYTHING

Responding to a possible incident is now up to 60 percent faster. Before, the team never knew if someone clicked on a malicious link until there was a problem. Today if a user receives a suspicious email, the IT team knows right away. They contact the user and tell them not to click on anything, but if they already did click, the IT team can perform a remote scan to check the machine. This returns hours and days of productivity to the IT team. They no longer have to unblock the university from blacklists, discover who received suspicious emails, remediate machines, investigate potential compromises, write firewall rules to block servers trying to phish users, or manually block malicious URLs in the content filter.

“Proofpoint delivers one of the best email protection solutions that I’ve used,” said Smith. “It covers our bases completely, and we don’t worry about email defenses anymore.”

For more information, visit www.proofpoint.com.

“Proofpoint delivers one of the best email protection solutions that I’ve used. It covers our bases completely, and we don’t worry about email defenses anymore.”

Clandis Smith,
Network Administrator,
Lincoln Memorial University