Case Study

mimecast

Not-for-Profit Organization Sees Much-Needed Improvement in User Behavior and Security

over 60%

of inbound emails were phishing or spam

2-3 months

Within months, user risk scores started to improve

50 to 500

Malicious email reports jumped per quarter following training

Business Case

A not-for-profit organization in South Australia, dedicated to supporting older people in living well as they age, has seen significant improvements in cybersecurity and user behavior. With over 70 years of experience, the organization provides a wide range of services, including health and wellbeing programs, home assistance, residential care, retirement living, and specialized dementia support. Their mission is to promote independence, social connection, and quality of life for older individuals.

Employing around 1,800 trained staff and offering 24/7 customer service, the organization focuses on integrated care, ensuring that as needs change, individuals can access appropriate support. Their services also extend to carers, offering respite and advisory support. As an award-winning and accredited provider, they emphasize customer feedback and continuous improvement to deliver high-quality care.

For the past 12 months, the organization's cybersecurity has been managed by their Cybersecurity Specialist. As a non-profit with limited resources, the specialist has made it their mission to ensure the organization stays secure using automation and the best tools available within budget. Largely working solo, this specialist sought a trusted partner to help instill a culture of cybersecurity throughout the organization. He turned to Mimecast for support.

The Problem

Like many organizations, this not-for-profit was facing a variety of email security issues, ranging from business email compromise (BEC) to their email addresses being added to spam lists, which greatly increased the volume of spam emails received. This amplified the need to rethink their cybersecurity awareness strategies.

The organization was looking to move away from their current email security provider to a solution that offered better protection and more effective behavioral training options. Despite years of annual cybersecurity awareness training sessions, leadership found that there was no real behavioral change among team members.

They needed an email security partner that could deliver a secure email gateway to better protect against BEC attacks and provide a training solution

> We needed to find a security training solution that succeeded in modifying the behavior of our team members when it came to email security. We wanted to better understand how human risk was impacting our very diverse workforce. We needed a datadriven, adaptive solution that automated training interactions and could also be tailored to our team's actual behavior.
>
> **- Cybersecurity Specialist**

that would result in meaningful behavior change. "We needed to find a security training solution that succeeded in modifying the behavior of our team members when it came to email security," said the Cybersecurity Specialist. "We wanted to better understand how human risk was impacting our very diverse workforce. We needed a data-driven, adaptive solution that automated training interactions and could also be tailored to our team's actual behavior."

The Solution

Working with the Mimecast team, the organization implemented Mimecast Email Security for targeted threat protection, including features like URL protection, attachment sandboxing, and impersonation protection, as well as Mimecast Engage security awareness training. "Mimecast training is targeted and meaningful," said the Cybersecurity Specialist. They were hopeful that Mimecast Engage training reminders and phishing nudges would deliver actual results. Additionally, the short, informative, and entertaining training videos were expected to help change the culture around security.

"I knew Mimecast tools worked well," the specialist continued, "because I had worked with them in the past. I always felt supported by Mimecast and their team. They made sure we got the most out of the solutions we had implemented, stayed in touch through quarterly catchups, and even advised us on policy. The tool and the team were both intuitive, and the Mimecast helpdesk was always there. There was not much of a learning curve. Mimecast just worked. It was simple to understand and did its job."

The specialist was eager to see how Mimecast could help. Previous solutions had failed to properly secure email and had little impact on changing the organization's cybersecurity culture. "I knew that Mimecast Email Security was going to work because of my history with using Mimecast tools in the past," he added, "but what I didn't know for sure was if Mimecast security awareness training was going to actually have a positive impact on user behavior, which had been a long-term problem."

The Results

"Our transition away from our existing provider to Mimecast was very smooth," the specialist reported. "Transitioning with no impact was very important. We have a hybrid exchange environment with 15 email domains. We needed a solution that could accommodate moving our organization's email into a more secure environment without user experience impact or significant downtime. The transition to Mimecast was simple and straightforward with no impact on our users."

In addition, the specialist noticed that the new approach to training was working. "With the stats we were seeing from Mimecast Engage, about four to five months in, we noticed a real cultural shift. We saw the team's risk scores dropping as they completed more and more of the training modules, which helped change risky behaviors. Mimecast training was definitely solving one of our longest-standing cybersecurity issues."

When asked about addressing training for the riskiest users, the specialist said, "For those riskier users who try to actively avoid training, we have put them together in a training group that has tighter controls. Instead of just one in five clicks being prompted with a security awareness message, we can go as deep as prompting every email click with an 'Is this link safe?' message. It has had a real positive impact on these users. It might seem harsh to target every email click, but it has resulted in much better security awareness."

He added, "Twelve months ago, we were receiving only 50 suspicious email reports per quarter from our team. For a staff of 2,000 people, that is very little. Today, that number has jumped up to over 500 per quarter. This is a great indicator that the security awareness training is working well." Additionally, the specialist was pleased to discover that from day one, Mimecast immediately led to much less hands-on follow-up to incidents. This freed up time previously spent reacting to incidents, allowing for a greater focus on prevention and other important IT projects.

The Future

As the organization continues to see results from Mimecast Email Security and their new adaptive training regimen, they plan to monitor and modify their policies as necessary. Managing human risk and ensuring the riskiest users receive the right amount of security awareness training to adjust their behavior will remain a focus moving forward.

"Human Risk Management is about recognizing that technology alone isn't enough," the specialist said. "It's about empowering staff to be active defenders, not passive liabilities. It means using data to understand behavior, delivering relevant education, and creating a culture where security is part of everyday thinking. Mimecast Engage helps us do exactly that."

"If you're serious about reducing human risk, I believe Mimecast Engage is one of the most effective solutions available today," he added. "It's practical, scalable, and genuinely drives behavioral change, without overwhelming staff or causing training fatigue. I'd also recommend exploring the product roadmap; the upcoming capabilities and integrations are innovative and demonstrate Mimecast's clear commitment to evolving human risk management. In sectors like aged care, where protecting people goes far beyond just ticking compliance boxes, Mimecast Engage has proven to be an invaluable addition to our security strategy."

ROI is very important to the organization and its board because resources are limited. While Mimecast is already improving behavior and efficiency, the specialist looks forward to continuing to demonstrate the shift in engagement and culture, further solidifying to the board that Mimecast was a great investment.

> "Human Risk Management is about recognizing that technology alone isn't enough," the specialist said. "It's about empowering staff to be active defenders, not passive liabilities. It means using data to understand behavior, delivering relevant education, and creating a culture where security is part of everyday thinking. Mimecast Engage helps us do exactly that."
>
> **- Cybersecurity Specialist**