NOT FOR PROFIT ORGANISATION MIMECAST CASE STUDY

An Enablis Case Study

"I'm getting a lot of feedback that people actually look forward to the user awareness training. They find it amusing, interesting and educational. I can also see stats that show 76% of people have made changes to how they operate in order to be more security conscious. That's a very positive result for us." - **Head of IT**

BACKGROUND

As the head of IT at a not for profit community-focused organisation, my first day was spent dealing with a full-blown cyber incident.

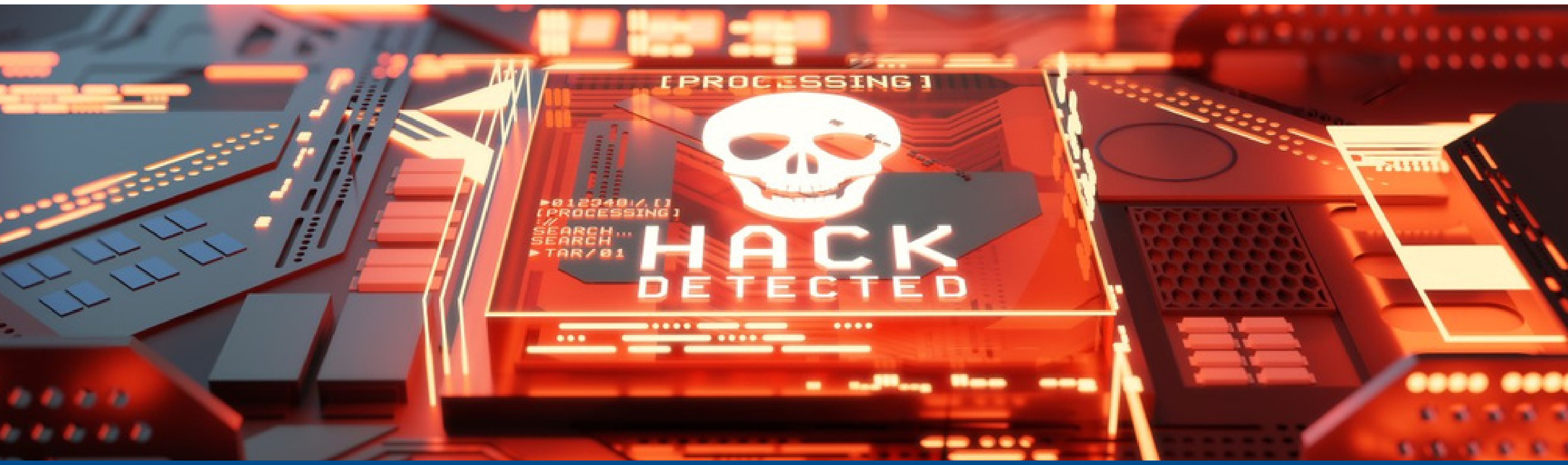
Most of us would recall our first day in a new job as a fairly relaxed affair. It's usually spent familiarising ourselves with our new employer's network and procedures, finding our way around the building, getting our desk set up, and introducing ourselves to our new colleagues.

The organisation had been hit by a ransomware attack. There was a major cyber breach activity happening at the time. Essentially, when I walked into the role there was no IT team, as they were in the grip of a ransomware attack, and the whole place was shut down.

SUMMARY

Mimecast and Enablis helped build a secure solution to free the IT support team from hours of having to respond to helpdesk requests by introducing a self-service portal where users can resolve email and other basic issues themselves.

The client also assessed the security awareness of all staff and pinpointed the areas that needed further attention. The goal was for each individual to achieve the security knowledge needed to keep the network as safe from human error as possible.



CHALLENGES - we had been hit by a ransomware attack

All of the our backups were infected and encrypted, as there were some fundamental issues with the way things were set up. I quickly realised that we had to change a few things around...and fast! Thankfully, we were able to get to the back up tapes. The incident had happened on the 2nd of the month, which fell on a Sunday, and we had access to the end of month backups from the Friday. It was still an arduous process to restore the data, virus check it, sanitise it, and move it to another platform, before eventually putting it back into production.

The issue we had was that we were unable to identify how the ransomware attack got through. While we suspected a staffer clicked on a bad link, there was no way of confirming if this was the case with our legacy set up

We weren't fully up and running until the end of the fourth week, and there were still a bunch of remediation activities that had to be done over the months following that period.At least one saving grace was that the attack started two weeks prior to me joining the role, rather than it being on my watch. But it still required my help to rapidly build a security solution.

There was a massive impact for us in terms of lost productivity as a consequence of the outage. Marketing campaigns had to be cancelled, just as we were going into our big spring marketing period; a particularly busy time for our organisation.

THE SECURITY SOLUTION

ENABLIS & MIMECAST EMAIL SECURITY SOLUTION AND AWARENESS TRAINING

Unsurprisingly, the board wasted no time in asking me how we should go about addressing the situation at hand and securing the environment. The solution that we had was out of date and unpatched, so I looked for one that was less hands-on, one which we could outsource to a large extent. That's where Mimecast came into the picture, because it didn't require us to engage in that hands-on type of maintenance that we were looking to avoid.

What I found was that the team were tweaking rules on a daily or weekly basis. If a user said they were not getting all of their email, they'd tweak a rule and relax something. Then people would start getting spam, so they'd do another tweak and roll that out again, so some people were receiving emails while others weren't getting the emails they needed. It was a nightmare.

Enablis and the Mimecast team has saved our team up to 20 hours a month, by doing away with constant hands-on policy tweaks. We can now spend that time on actually adding value to the business.

We looked at Proofpoint and Barracuda as potential solutions, as well as a few others that were discarded earlier in the process because they didn't meet our needs. Then we were recommended Mimecast, and once we'd shortlisted those three products, Mimecast came out on top, both in terms of the price point and its capabilities. Another important aspect for us is Mimecast's approach to user awareness training.

Mimecast Awareness Training uses humour to engage staff in its training, something which has proven to be very effective. Staff are now more aware of potential phishing and other malicious emails and flagging them, rather than clicking on them and potentially enabling the network to be compromised. We're feeling a lot safer and more secure with our IT than we were before Mimecast.

AT A GLANCE

- Security awareness training reporting through Mimecast now provides us with a clear view of our staff security knowledge, and the gaps in that knowledge that need to be filled.
- Enhanced security features mean that malicious threats can be identified and blocked by Mimecast before they reach their intended recipient, and other suspicious messages can be identified and flagged as requiring attention.
- The Enablis and Mimecast support teams provided fast and accurate responses to any issues raised by our IT team, whereas previously we were left to resolve our issues ourselves through time-consuming research.

LOOKING AHEAD

The helpdesk is no longer getting tickets saying ‘could you please unlock this email for me?’ Previously, something would get blocked or caught on the firewall, and IT support would have to fix it. Now, with Mimecast’s self-service portal, the user can go in and unlock it ourselves. That's saved hours of productivity for our IT helpdesk every week. We are now able to able to go and focus more on time on value adds, such as Office 365 rollouts, and improving the overall IT infrastructure, rather than unblocking people's emails.