Wyntec
stress free IT

CUSTOMER SUCCESS STORY

Scientific research company discovers prevention better than cure with Cyber Security Awareness Program

Customer introduction

Social research is an important tool in company decision making. Off the back of a decade of successful research and innovation, our customer founded their organisation with a core focus and goal of improving the social performance of their customers around the world.

Their crucial work is underpinned by data and analytics and continues to expand through community engagement both on the ground and digitally. While they had worked to ensure their technical data security arrangements were sound, growth in the team led to other, unforeseen risks.

The situation

It has been documented that human errors and behaviours cause 95% of cyber attacks, and a prime example of this statistic can be seen in the incident experienced by this organisation.

A new hire in their first week received a seemingly innocuous email from the CEO asking them to undertake an errand for them. Nobody is more eager to please the boss than a new hire, and as such, this employee jumped at the opportunity and quickly responded.

This “CEO” then directed the staff member to go out and purchase iTunes vouchers to assist with a client. This new recruit then went and spent $1,500 of personal money to secure these vouchers, activated them, and sent them to the “CEO”.

Of course, this was not the CEO and instead was a relatively common form of Targeted Spear Phishing that targeted the most vulnerable entry-point into this organisation: the human element. The hackers had simply used a fake account that looked like it came from the CEO to persuade this over-eager employee to do their bidding.

For all technical purposes, the email was a legitimate and well-formed message. It was simply a display name that had been modified to make it feel like it came from the CEO. The user in the case was unaware of company policy around purchasing and was unaware of what to look for when it comes to these types of common scams.

Enter Wyntec's Security Team

As you can see, technology played a minimal role in this form of unsophisticated attack, and therefore simply upgrading cyber security software would not have protected this organisation from this successful phishing attack.

The organisation understood that the upgrade needed for this type of cyber attack was for its human element and they sought the specialised cyber services of Wyntec.

Wyntec are the Aussie experts in all things cyber. They have developed a comprehensive program to ensure your organisation does not end up a costly cyber crime statistic.

The Wyntec Security Team quickly proposed and actioned a comprehensive Cyber Awareness program for the staff. This focused on identifying and understanding the staff's behaviours and attitude towards security.

The Cyber Awareness Program includes:

- Compromised Account Reviews
- Spear Phishing Simulations
- User Knowledge & Risk Profile Assessment
- Corporate Threat Profile Assessment
- Cyber Vulnerabilities Analysis Reporting
- Team Training
- Reinforcement Tools & Resources
- Self Assessment Resources.

Outcomes & what's next?

After undertaking comprehensive risk assessments and utilising both targeted and general phishing testing across the organisation, Wyntec identified who was vulnerable throughout the business and measured the overall susceptibility of the organisation itself to various forms of cyber attacks including the likelihood of being targeted again.

These results highlighted previously unforeseen gaps throughout the organisation and its staff, and immediate training was provided through real-life scenarios and education on how these events happen.

Staff are now more confident in what to look out for and understand the changes they needed to make (and continue to make) with their online behaviours. Staff now act as a 'human firewall' across the organisation and the first line of defence as both cyber risk and threat detectors.

Ongoing Cyber Awareness training is being rolled out as an ongoing solution to reduce the risk for existing staff and ensure that new staff joining the business have a much-improved understanding of policy and security awareness from the outset and won't go rushing out to buy any more surprise iTunes vouchers!

Is it time you started taking cyber awareness seriously? Get in touch to explore the best path forward for your organisation.

Contact us