CUSTOMER SUCCESS STORY

Human error opens the door to financial firms cyber attack

Customer introduction

Our client, one of Australia's leading accounting and financial service providers with their core focus on helping their clients achieve their visions and goals. They represent dozens of partners and hundreds of staff across Australia. Even with such a broad reach and workforce, they proudly work as a family to drive value and growth to their clients.

The incident

One of their local team members received a call from 'Amazon' while at work. They were convinced by this caller to allow them to take control of their work computer for some routine maintenance. This opened the door for this hacker in disguise to gain control of the employee's personal bank account with its details saved in their computer for ease of use.

The user was unaware of the potential risks this placed them, and the organisation, in and they were then scammed for over $2,000 of their own money as a result.

Enter Wyntec's Security Team

Once the organisation became aware of this incident, the Wyntec team was contacted late on a Friday afternoon to assist with their cyber security and risk prevention expertise.

Additional technology solutions may have prevented the remote control attack from being initiated, but the attack had already been successfully deployed. Therefore, it was too late for this particular incident to be prevented and unfortunately, nothing could be done post-incident to recover the funds.

To eliminate the ongoing threat this breach presented to the organisation as a whole, Wyntec immediately isolated the user's computer, disconnected it from the network and performed a complete wipe to ensure no residual software could impact the business.

Outcomes & what's next?

While nothing short of a time machine could have reversed the damage and costs this attack inflicted, the quick action of Wyntec and its cyber expertise quickly mitigated any additional costs or damage to the organisation.

The organisation is now looking into additional technology-based solutions that may have prevented the attack from taking place, such as Application Whitelisting solutions deployed throughout the business. However, this attack primarily was able to occur due to the all too familiar human element. It is reported that 95% of all cyber attacks* occur due to human error, and only adequate cyber awareness training and education can genuinely prevent these common attacks. Had this particular user been at home, precisely the same outcomes would have occurred, if not worse, as there would have been no one to see the action taking place. The prevention is education, awareness and behaviour change.

A few weeks after the attack took place and was stopped from escalating due to the actions of Wyntec, the business is now reviewing how better to equip its staff with education and awareness training.

This is focused on real-world scenarios around what the impact is to the individual, just as much to the business. What individuals do at home significantly affects their personal risks, and addressing these flows into the business.

Is it time you started taking cyber awareness seriously?

Get in touch to explore the best path forward for your organisation.

Contact us