Phriendly Phishing

Case Study

Top professional services organisation slashes cyberthreats with Phriendly Phishing

The Challenge

With more than 1700 employees, operating across multiple sites, the professional services organisation recognised that a proactive approach was required to better manage the risks arising from the increasing number of malicious phishing and spam emails employees were receiving and the threat this posed to sensitive data.

The technical controls were already in place, but the Chief Information Officer (CIO) recognised that, while prior cybersecurity education had achieved a small improvement, cybersecure behaviour was not sustained and employees lacked confidence in their abilities to recognise and respond to malicious emails.

This was impacting regular work duties, as instead of employees confidently deleting malicious emails, they were sending increasing volumes to the IT department. Knowing that real change takes more than a single educational session, the organisation began researching more creative ways to teach cybersecure behaviours.

“We were looking for something to make this a lot more real and less theoretical...” Company CIO

The organisation sought a solution that would engage, educate and reinforce cybersecure behaviours, over a sustained period of time.

They concluded that the opportunity to test, revisit areas requiring improvement and support and develop employees’ cybersecurity knowledge, long term, was a key requirement and outweighed the ‘quick fix’ promises some training suppliers were offering.

The Solution

The company's CIO was impressed with how well Phriendly Phishing's mission to support Australian businesses, while also speaking directly to employees in a relevant, accessible and engaging way, aligned with their key requirements.

The organisation ran a pilot campaign, involving 500 employees at one of their sites. It proved to be an overwhelming success, with marked employee improvement across the board.

Delighted with the results, the organisation chose to roll out Phriendly Phishing to all 1700 employees across the country.

As a cloud-based solution, Phriendly Phishing's material did not consume additional company resources and, with continual updates (to meet ever changing phishing threats and techniques), offered employees the most up-to-date information at any one time.

"The monthly tracking and reporting was fantastic. You could see who was receiving what emails, what staff clicked on and how we were tracking against our baseline," said the CIO.

The organisation was able to track the significant change in how their employees responded to the simulated malicious phishing emails and this consistent monitoring, referral and re-education was instrumental in the organisation successfully slashing its phishing risk.

Phriendly Phishing

The Results

Today, only 1.6% of this organisation's employees click on the Phriendly Phishing simulated phishing emails, compared to 20% at the start of the program.

Phriendly Phishing has been a catalyst in bringing about employee engagement in developing an organisation-wide information security mindset and cybersecure behaviours, to effectively defend against phishing threats, and is now a valued component of this organisation's cybersecurity program.

20%

Before Phriendly Phishing Training 20% of employees clicked on simulated phishing emails

↓1.6%

After Phriendly Phishing Training 1.6% of employees clicked on simulated phishing emails

1.48%

Increased employee engagement in developing an organisation-wide information security mindset & cybersecurity behaviours

> "We were looking for an ongoing, effective solution because we've seen a lot of phishing activities coming to our business, due to the nature of the services we provide," said the CIO. "[Phriendly Phishing's] monthly tracking and reporting was fantastic. You could see who was receiving what emails, what staff clicked on and how we were tracking against our baseline."