City of Launceston

Phriendly Phishing helps City of Launceston boost cyber resilience

The Challenge

As Australia's local government sector finds itself on the front line in the fight against cyber attacks, councils need to embrace security measures to protect themselves and their residents from costly breaches.

Numerous recent attacks against local governments show that hackers are increasingly turning their attention to the public sector. Under-resourced local governments are particularly vulnerable as they often lack the expertise or systems to prevent attacks. Furthermore, if they do find themselves being targeted, they may experience widespread and long-term disruptions to their operations which negatively impact local communities who are reliant on the provision of essential council services.

The City of Launceston in Tasmania was determined not face the same fate as numerous other local government areas in Australia. To prevent costly disruptions to their operations, City officials committed to taking steps that would strengthen the council's cyber resilience.

In determining what specific strategies should be embraced, City officials carefully undertook risk assessments to consider the range of potential threats. Based in part on the experiences of other local government areas, it was determined that email systems needed to be secured so the City would be able to prevent the growing threat of ransomware.

Under the guidance of David Kamphuis, IT Security and Infrastructure Administrator and Kieran Ollier, Senior IT Support Officer, it was recognised that the City faced a particular risk due to the range of public-facing communication channels it utilised. City staff regularly used these channels to communicate with members of the local community, as well as different organisations across Tasmania.

City officials had noticed that they were receiving targeted phishing attempts following third-party vendors being compromised. On several occasions, these phishing attempts were being specifically directed towards the City's CFO, who was receiving numerous suspicious emails.

Given that many attackers view local government as an easy target, the City resolved that strengthening its cyber resilience required training staff so they would have the necessary skills to identify and block potentially malicious emails.

The Solution

City officials turned to Phriendly Phishing as the ideal training platform that would equip all council staff with the skills they needed to prevent email-based attacks.

A key priority for the City's IT team was having a centralised management portal which would integrate with their Azure cloud infrastructure. This would facilitate onboarding staff easily, which was critical given the City employs over 500 staff, across 11 separate locations.

Equally important was the need for the training modules to be engaging and interactive. The skills acquired through the Phriendly Phishing modules enable multilevel threat awareness. Users begin with the basics of cyber resilience, such as learning the importance of strong passphrases and multi-factor authentication. They then start learning many of the tactics cyber-attackers use to trick people into executing malware. Over time, and with ongoing testing, staff develop a strong awareness of the potential threats and how to appropriately respond to them.

For Kamphuis and Ollier, it was essential to engage staff and have them think about cyber security in a holistic way. Phriendly Phishing's unique approach enables ongoing education, rather than the one-off training of other providers.

The Phriendly Phishing admin portal also allowed them to monitor the efficacy of the training with ongoing statistics that helped them identify areas for improvement among specific staff members. The platform gave them a strong sense of how the training was progressing at any point in time.

Phriendly Phishing

The Results

Following the introduction of Phriendly Phishing, the City has significantly reduced its risk of phishing attacks. At the commencement of the training initiative, 15.6% of test phishing emails that were sent to City staff were being clicked. Since undergoing Phriendly Phishing training modules, that click-through-rate has dropped to 2.59% – a very significant improvement!

This clearly demonstrates that City staff are developing strong skills that allow them to quickly identify potentially dangerous emails.

Encouragingly, the feedback from City staff has been positive, with many also reflecting on the fact that they had received phishing emails in their personal email accounts. Thanks to the Phriendly Phishing training they had been able to protect personal devices from malware as well.

For City officials, the best part about Phriendly Phishing is the fun way it seeks to educate users about cyber security. By being really engaging and interactive, it helps motivate staff to engage with the content in ways that other training programs don't.

15.6%
Original click-through-rate

↓2.59%
Click-through-rate after Phriendly Phishing training

Future Steps

The City of Launceston plans to introduce additional training programs developed by the Phriendly Phishing team. These include S.C.A.M. 201 and Keep Secure general security awareness courses.

To see how Phriendly Phishing can work for you, request a **free demonstration** of the product at **PhriendlyPhishing.com**