Phishing Awareness Training & Simulation

Case Study

Top professional services organisation slashes cyberthreats with Phriendly Phishing

One of Australia's largest professional services organisations has slashed their phishing risk from 20 to 1.6 per cent by integrating the sustainable and extremely effective phishing awareness and simulation program Phriendly Phishing into their cybersecurity program.

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. Having recently combatted ransomware, the organisation wanted to prevent future, avoidable, situations that can lead to costly and time-consuming remediation.

The Chief Information Officer (CIO) already had technical controls in place, to protect employees, but 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 and instead of employees confidently deleting malicious emails, they were sending increasing volumes to the IT department.

"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.

Knowing that real change takes more than a single educational session, the organisation began researching more creative ways to teach cybersecure behaviours. Seeking a solution that would engage, educate and reinforce cybersecure behaviours, over a sustained period of time, the organisation took an innovative step towards social engineering and explored a number of providers who offered more than just a static training experience. 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.

"We were looking for something to make this a lot more real and less theoretical…" said the CIO.

The solution: A sustainable and effective way to teach cybersecure behaviours

Following the recommendations of a trusted Phriendly Phishing partner, the organisation approached Phriendly Phishing to find out more about the Australian cloud-based program. 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.

Summary

Customer: Professional services business
Industry: Professional services
Location: Australia

Challenge

- Train a large employee base of 1700, operating across multiple sites, against phishing threats
- Minimise phishing risks
- Establish sustainable cybersecure behaviours.

Solution

- Phriendly Phishing: A cloud-based phishing awareness and simulation program that tests, revisits areas requiring improvement and supports and develops employees' cybersecurity knowledge.

Result

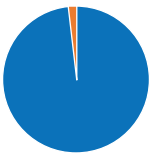
- The organisation slashed their phishing risk from 20 to 1.6 per cent

Before Phriendly PhishingTraining

20%

of employees click on the Phriendly Phishing simulated phishing emails

After Phriendly Phishing Training



1.6%

of employees click on the Phriendly Phishing simulated phishing emails

- The ability to track employee improvement and offer support where needed
- Employee engagement in developing an organisation-wide information security mindset and cybersecure behaviours.

Pilot Study

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

One of the core features that the organisation found attractive was the ability to roll out the same educational content to the pilot group concurrently. And being cloud-based, 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. They also liked that, unlike other products they had researched, Phriendly Phishing measures a user's existing knowledge before deploying the educational modules, tests improvements and supports re-education. This journey-based approach encourages users to reach milestones and gain practical experience by testing their skills on simulated phishing campaigns. It is these features that make Phriendly Phishing an engaging and extremely effective cybersecurity training program.

Multisite National rollout

Delighted with the results of the pilot study, the organisation chose to roll out Phriendly Phishing to all 1700 employees across the country and, to benchmark their knowledge, ran an anonymised simulation, also known as a baseline campaign.

In this instance, an engineered email, masked as a phishing email, was released to all employees and their behaviours were anonymously recorded. While the organisation was prepared for an initially higher number of poor responses, what they didn't expect was that one in five failed the security checks and clicked on the test email.

To expedite learning and retention, the organisation activated the Phriendly Phishing simulation option. This simulation supports the education modules by allowing an organisation to choose when a simulated phishing email is sent to their employees, and the level of difficulty, allowing employees to practice and receive real-time feedback. It also provides detailed reporting insights, down to an individual status, on how employees are learning to recognise and manage malicious emails.

"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.

The results

Today, only 1.6 per cent of this organisation's employees click on the Phriendly Phishing simulated phishing emails.

And finding their employees diligent against cyberthreats, the organisation notes that employees (across all demographics within the organisation) are now more confident when it comes to managing phishing emails and proactively and consistently refer unclear content to their service desk for review.

Phriendly Phishing has dramatically reduced the likelihood of an employee clicking on malicious content more than any other program or initiative the organisation has tried; actively demonstrating value and impact and creating sustainable behavioural changes that have seen the organisation's risk drop from 20 to 1.6 per cent. 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.

"*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.*"

"*We were looking for something to make this a lot more real and less theoretical…*"

"*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.*"

For more information on Phriendly Phishing, please visit www.phriendlyphishing.com

CASE STUDY

PHRIENDLY PHISHING AWARENESS TRAINING

PHRIENDLY PHISHING .com by Shearwater Solutions | SSS IT SECURITY SPECIALISTS

"We have absolutely no doubt that behaviour across the organisation has improved – it's measurable – and we believe this would neatly translate across to actual malicious emails."

BUSINESS CHALLENGE

healthAlliance NZ is the largest shared ICT services provider to the public health sector in New Zealand, with more than 26,000 customers across a network of more than 10 hospital sites. With healthcare now the most targeted sector for cyber-crime and ransomware attacks, healthAlliance is constantly looking for smart technologies and solutions to help mitigate its risk.

"Health is now the number one target for ransomware around the world – more so than Finance, Retail, Transportation and Manufacturing," says Liz Schoff, Security Consultant at healthAlliance. "The value of a health record on the dark web can be as much as USD $100, compared to just a few dollars for a black-market credit card number," she adds. "The reason is when a credit card number or bank account number is compromised it can pretty quickly be shut down and not used again, but health information sticks with people forever," she explains. "The value of stolen or ransomed health information remains the highest and that's why we continue to get targeted the most," she adds.

In today's world you cannot run a hospital without computers. Patient information is held online, and computers are used to run various essential operations every day. "There have been instances where hospitals have been forced to pay when a cyber-criminal has managed to encrypt a hospital network and demand a ransom," says Ms Schoff. "It is absolutely critical for us to make sure that all of our staff understand how to identify phishing emails and not have a behaviour that could lead to a compromise of our network," she adds.

These behaviours could be clicking on links, giving away one's credentials or downloading attachments that might have viruses. "Even though there are technologies to reduce risks by looking at attachments before they are downloaded, or by checking websites before you allow someone to visit them, cyber-criminals are always innovating and they're getting smarter," says Ms Schoff. "It's really hard to have technology that's 100% up to speed, so having an educated staff is absolutely the best defence a hospital can have," she adds.

ORGANISATION
healthAlliance NZ Ltd

CUSTOMERS
More than 26,000 DHB staff

LOCATION
10+ Hospital Sites across the North Island of New Zealand

SOLUTION
Shearwater Phriendly Phishing, provided in NZ by SSS - IT Security Specialists

healthAlliance
Right behind better healthcare

ABOUT HEALTHALLIANCE NEW ZEALAND LTD

healthAlliance is one of the most significant shared services organisations for the health sector in New Zealand.

healthAlliance is a not-for-profit organisation established in July 2000 as a joint venture between Waitemata District Health Board and Counties Manukau Health to provide key non-clinical business services for both DHBs.

In March 2011, Northland District Health Board and Auckland District Health Board joined, and collectively the four formed the Northern Region DHBs. We help our partner DHBs provide health services to 36% of New Zealanders from Pukekohe to Kaitaia.

healthAlliance FPSC Ltd., a wholly owned subsidiary of healthAlliance NZ Ltd., provides Procurement and Supply Chain services to generate savings and create efficiencies or the region's health sector. The organisation is jointly owned by the four Northern Region district health boards: Northland, Waitemata, Auckland, and Counties Manukau Health.

healthAlliance provides a range of shared services for the New Zealand health sector, support multiple DHBs, and also provide some services to Hutt Valley DHB, Taranaki DHB and the Northern Regional Alliance.

THE SOLUTION

In recognising its increased potential for phishing attacks, healthAlliance began looking for solutions that could help it better manage the risk by training its employees to identify phishing emails. "We had heard that another district health board in New Zealand had run with Shearwater's Phriendly Phishing software, so we touched base with them and asked about how it was working," says Ms Schoff. "When another organisation in our sector successfully uses a solution, word gets around, and that gives us an immediate level of comfort that the product should also work for us," she adds.

Phriendly Phishing is a Phishing Awareness and Simulation program designed to help organisations measure, track and improve their staff's ability to identify and manage phishing and spear-phishing threats. Typically, up to 70 out of 100 employees would open a spear-phishing email, and 35 would click on the embedded link. The resulting ransomware can cause significant business disruption and costly remediation, not to mention reputational damage. With Phriendly Phishing, organisations get a fully managed, comprehensive and measurable training solution, with easy-to-use tools that will help them to understand their organisation's overall phishing risk profile, educate their staff, nurture awareness and prove successful behavioural change across their organisation.

Phriendly Phishing works in three simple stages:

MEASUREMENT: Baseline Audit
Starts with a simulated phishing campaign to determine your organisation's overall phishing risk, and to establish a baseline for future improvement measurements.

IMPROVEMENT: Awareness Training
Delivered via the Internet; with tiers targeted at the beginner, intermediate and advanced levels, the training creates awareness of phishing threats and enables staff to develop phishing detection skills. Users start at the beginner level and work their way up.

REINFORCEMENT: Learning Reinforcement
To enhance the training concepts and incorporate them into the employee's day-to-day reality, staff members will receive simulated phishing emails, varying in sophistication, at random intervals. This is designed to help fine tune detection skills. If users open any of the simulated emails on a link, they will be redirected to the portal for a training recap.

IMPLEMENTATION - MADE EASY

With the decision made to run with Phriendly Phishing, healthAlliance needed to work out how to best use the solution across its organisation. "My role at healthAlliance was to put together a plan around how we would best use Phriendly Phishing, recognising that it needed to go beyond simple awareness and training, and needed to help us in supporting our team to shift from risky to safe behaviour," says Ms Schoff. "Shearwater Solutions provided us with an excellent portal with a lot of automated interfaces and reporting modules which we felt were fundamental to allowing us to continue to effectively manage awareness and positive behavioural change across the business," she adds.

With the help of the Shearwater team, healthAlliance was able to get an immediate base-line understanding of what kind of behaviour it had in its organisation at the time of implementation. It then conducted short online modules geared at training its people in the day-to-day identification of phishing emails, before then undertaking scheduled monthly campaigns using simulated phishing emails to continue team education, awareness and behaviour shaping.

"If someone clicks one of our simulated links then we are able to immediately give them feedback," says Ms Schoff. "We then direct them to the specific training area where they can learn how it was that they were caught – what particular phishing technique they succumbed to," she explains. Immediate feedback is achieved through the simple deployment of an easy-to-use button on the email interface or in the email window of all staff, allowing them with one press to record anything they think is phishing activity. "It's a clever little button. If they record one of our simulated emails, they get immediate positive feedback congratulating them for correctly identifying a Phriendly Phishing email," explains Ms Schoff. "If it's not a simulated email, their reporting alerts our IT Security team to investigate and make sure it is not an actual threat," she adds.

The size of, and daily demands on, the healthAlliance IT network sometimes adds complexity to the implementation of new software solutions. "The implementation went very smoothly and that reflects both the user-friendly nature of the product, and the excellent support of the Shearwater team," says Ms Schoff. "We required some minor vocabulary modifications to the training modules and some additional types of reporting, and the support we received was always really responsive," she adds.

OUTCOMES

healthAlliance has been sending its monthly simulated phishing emails for more than 6 months and they are delighted with the results they are seeing across the organisation. "The Phriendly Phishing portal is a great tool and allows us to see specifically who's recording scams, and more importantly identify the staff who continually click on the simulated links," says Ms Schoff.

Hospitals are vulnerable because doctors and nurses are very busy people. Cyber criminals are also getting smart about the times they send their phishing emails, on or around shift changes. "When you're busy it's easy to forget and quickly look at your emails, open messages and click links because you're rushed," says Ms Schoff. "Our training programmes, which send simulated phishing emails every month, provide the platform for our people to get a regular reminder to keep sharp and alert to threats," she adds.

When asked if healthAlliance believes it is a safer organisation because of the introduction of Phriendly Phishing by Shearwater Solutions, Ms Schoff is in no doubt. "We know that the behaviour across the organisation has improved because we can measure exactly how many people are recording our simulated links, and more importantly we have clear evidence our people are clicking less on dangerous links," concludes Ms Schoff.

LIZ SCHOFF
SECURITY CONSULTANT AT HEALTHALLIANCE

PHRIENDLY PHISHING.com
by Shearwater Solutions

ABOUT PHRIENDLY PHISHING

Phriendly Phishing is a Phishing Awareness and Simulation program developed to deliver easy-to-use tools that will help you understand your organisation's phishing risk, educate your staff, nurture awareness and prove success across your organisation.

Measure, improve, and track your staff's ability to detect phishing and spear-phishing threats.

Reduce employee clicks on malicious links.

Fight back against ransomware and executive fraud and reduce the risk of scams and malware proliferation.

Close the path of advanced malware to your systems.

For more information on Phriendly Phishing, please visit www.phriendlyphishing.com