SSS – IT Security Specialists

Information Security Awareness Training

Exclusive pricing for ALGIM Members

ALGIM

0800 777 001

sales@sss.co.nz

NZ registration: 286883

IT SECURITY SPECIALISTS

Comprehensive security awareness options suitable for all staff

Security awareness training is not just for technical staff. Attackers constantly look for an easy way in and will often target your staff, regardless of their position in your organisation.

We have partnered with ALGIM to bring comprehensive training options to your staff, providing them with a strong foundation and ongoing learning opportunities.

More information

Sebastian Kramer
SSS – IT Security Specialists
Key Account and Vendor Manager
Sebastian.Kramer@sss.co.nz
04 917 6683

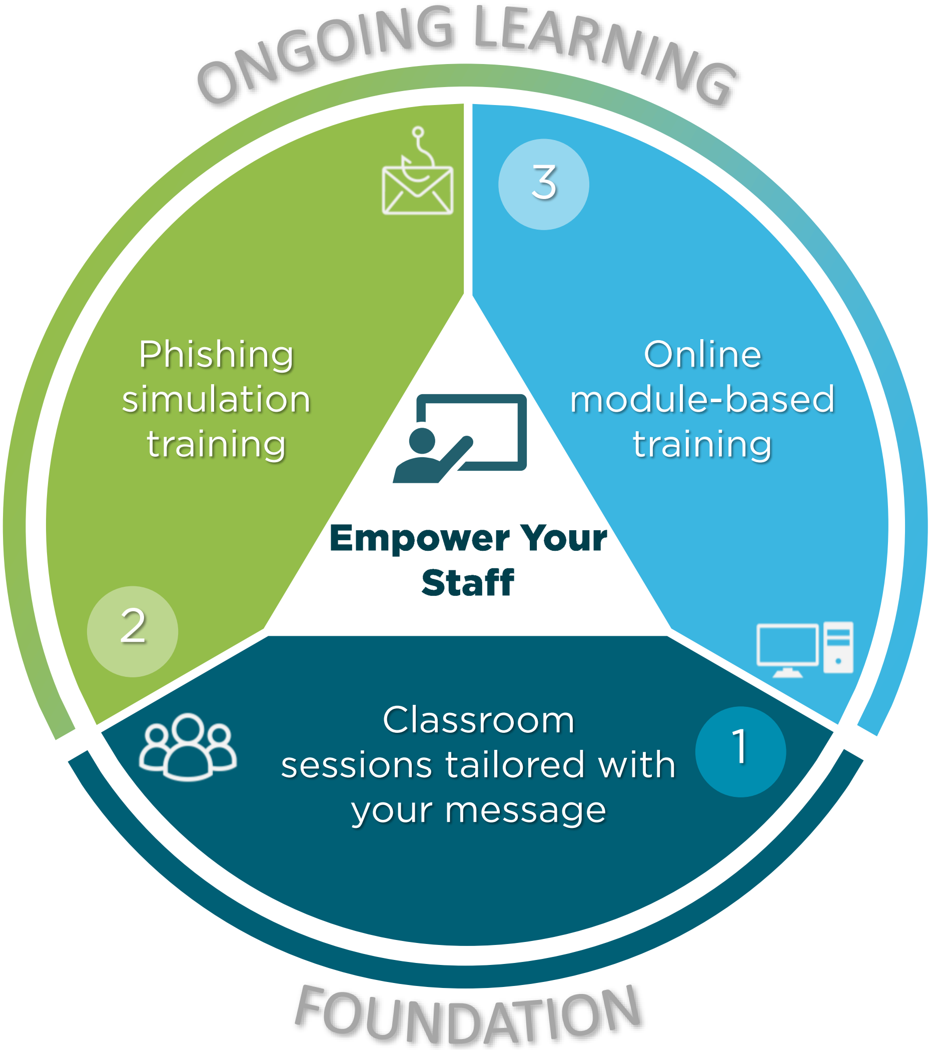
Training is one of the most important things you can do

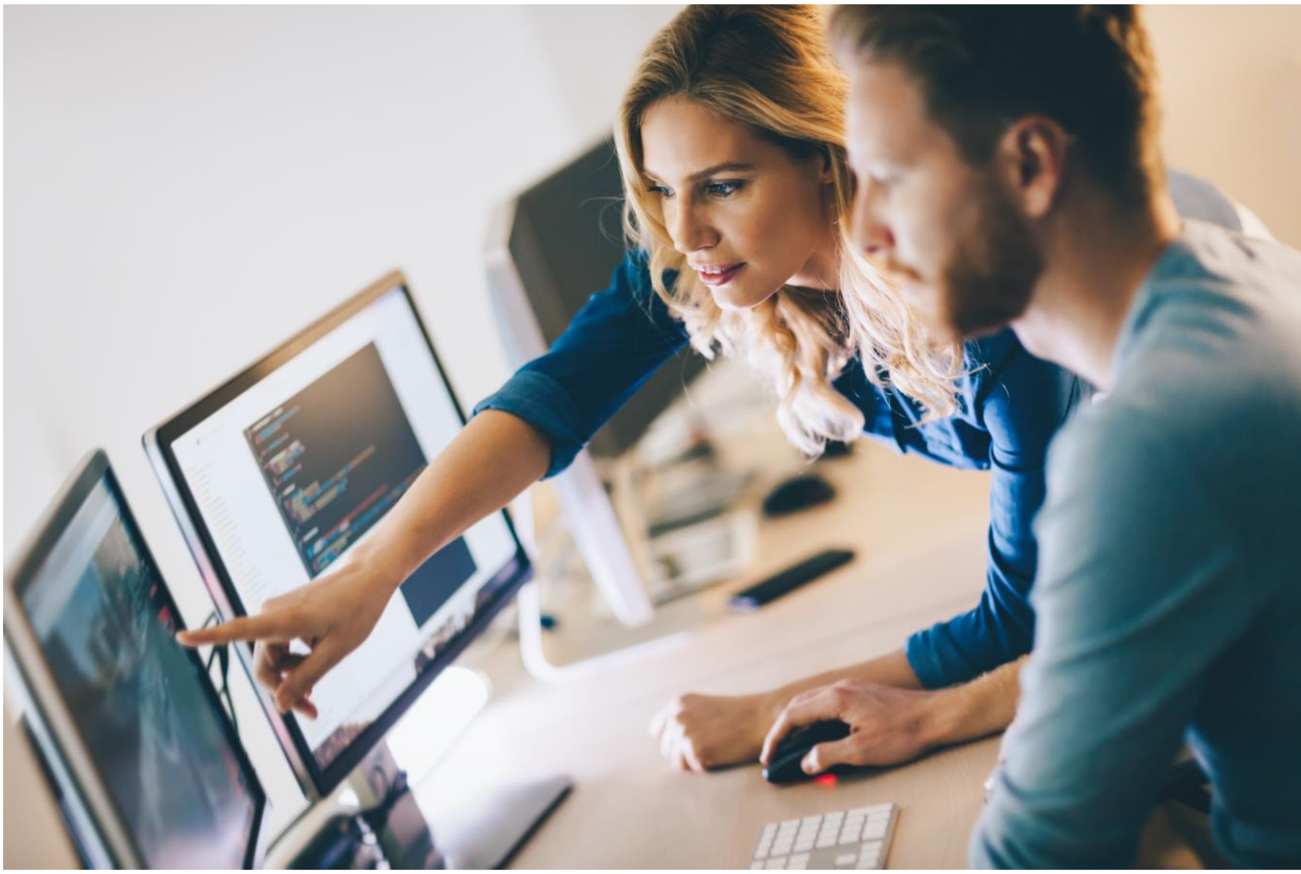
CERT NZ reported that in 2019 phishing and credential harvesting, and unauthorised access were two of the top reported incidents. Not all users understand what information security is, and that it extends to many different areas within your organisation.

Our training options will provide all your staff with important knowledge and awareness to empower them so they can help protect your organisation by detecting potential threats.

People learn in different ways

We offer three proven methods suitable for a diverse audience. Training can be taken as stand-alone options, or as a comprehensive, multi-faceted approach.


ONGOING LEARNING
3
Online module-based training
2
Phishing simulation training
Empower Your Staff
1
Classroom sessions tailored with your message
FOUNDATION



A multifaceted approach

Training can be taken as stand-alone options, or as a comprehensive, multi-faceted approach to help your staff with continued learning and development.

It takes time for user behaviour to change.

With our comprehensive training offering, staff will be able to develop and increase their knowledge in a way that will help them better retain the information they have learned and build a strong foundation.

Training that is:

- User-friendly
- Delivered in plain English
- Suitable for all staff
- Designed to empower your users

General user group	Technical group
General classroom-based sessions tailored with your specific message.*	Tailored classroom-based sessions to include more technical information*
Enrol all staff with Phriendly Phishing 101	
Targeted phishing campaigns for the general user group	Targeted phishing campaigns to suit the technical group
Enrol all staff in Shearwater Keep Secure 5 (KSec5)	

*Sessions can also be delivered via Zoom

Awareness Training sessions

Tailored messages to suit your audience and your organisation

What you get:

- Comprehensive in-person information security training.
- Provides a consistent message.
- Can be delivered to different groups customised to suit different technical and functional levels.
- Interactive; staff can get immediate feedback to their questions.
- Includes real-life examples to make the training more relevant to your environment.
- We can work with you to align our training with your objectives and customised to your business.
- Using non-technical language, we discuss easy to understand concepts making this informative for all participants.

How it works:

This training is facilitated as a 2-hour session and is suitable for all group sizes. For a general non-technical audience, this will include the following:

- The consequence of a cyber-related incident to you and your staff.
- What the internet is.
- How data remains on the internet even when you try to remove it.
- Who the bad guys are... and why they want to compromise you.
- How the bad guys trick your staff into helping them enter your systems.
- Some simple tips staff can use to protect you at work, and themselves at home.
- The facilitator will also share some fool-proof ways of selecting and remembering stronger and more complex passwords.

> *"The cybersecurity sessions were well attended, and the staff got a lot out of Gavin's non-technical approach and real-world examples. Many were taking a lot of notes and forming good strategies on how to protect themselves online. I received many thank-you's from staff for taking the time to organise these sessions."*
>
> *Peter Darlington, IS Manager, Tasman District Council*

PHRIENDLY PHISHING.com
by Shearwater Solutions

Simulation Training

Measure ❯❯❯ Educate ❯❯❯ Nurture ❯❯❯ Report

What you get:

- Empowers staff to recognise phishing attempts without making them feel like they have been tricked.
- Enables you to set a benchmark and measure the ongoing success of the training by sending phishing email campaigns.
- Reinforces the training in a safe environment without putting your organisation at risk. You can control the timing and difficulty of each campaign.
- Enrol your staff automatically through AD sync and schedule the frequency of training and phishing campaigns so they run automatically.
- Allow staff to build good habits through submitting suspect emails via the Outlook addon.

Scalable

User-friendly

Works on any device

How it works:

Training consists of two web-based modules teaching users what spam and phishing emails are and how to recognise these:

- Phriendly Phishing 101
- Phriendly Phishing 201

All users start with 101 before moving on with 201.
Following the base training, learning is reinforced with targeted safe phishing campaigns.

> *"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. 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"*
>
> Liz Schoff, Security Consultant at healthAlliance.

SHEARWATER™
securing your information

Keep Secure 5 (KSec5)

What you get:

- Comprehensive computer-based information security training.
- Web-based training that staff can complete in their own time.
- Structured in online modules with each following on from, and building on the previous module.
- Details psychological and historical events to build a holistic understanding of current security threats.
- Equips participants with foundational rules to guide security decision-making.
- Empowers employees to protect both their workplace and home from cyber attacks.

How it works:

Training is structured into the following modules:

- Security foundations
- Cyber-attack evolution
- Social engineering
- Online and remote threats
- Internal threats
- KSec5 framework

The modules will cover topics such as:

- How cyber criminals think differently
- Social media dangers
- How hacking really works
- Identity theft
- Perfect passphrases
- Phishing emails
- Opportunistic vs targeted attacks
- Download risks
- How hackers obtain and use your information
- Data leakage

A strong security culture is essential for minimising your organisation's risk profile. As the threat landscape evolves every employee needs to understand current security threats and their implications.