35% OF DATA BREACHES ARE ATTRIBUTED TO HUMAN ERROR*

Too many incidents are due to staff negligence or ignorance;

▶ It's time to upskill your team.

16% OF DATA BREACHES ARE CAUSED BY PHISHING ATTACKS*

Phishing and social engineering is becoming more sophisticated;

▶ Give your staff the upper hand, so they know what to look for.

KNOWLEDGE IS POWER

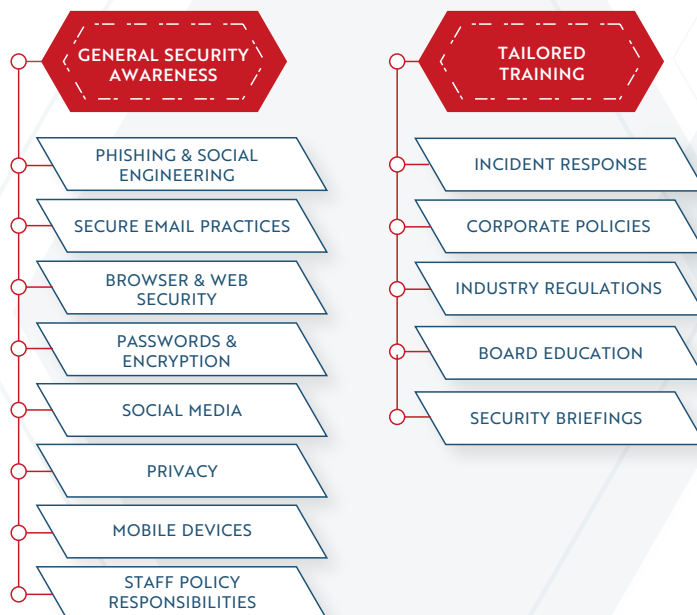Staff don't know what they don't know and can easily make costly mistakes;

▶ Educate staff with your expectations on security.

Security Training

Cyberattacks don't differentiate between organisation industry, type or size. Everyone is a target and vulnerable to attacks like phishing, social engineering and ransomware, and we're all only as strong as our weakest link. How would your organisation be impacted if your sensitive data was lost or stolen or your systems shut down, and you were unable to conduct business?

Cybersecurity Awareness Training is no longer optional. Helping your team protect themselves and your business from potentially massive financial losses and reputational damage is essential. Regardless of the framework, standard or best practice; keeping staff informed of security threats is a win–win scenario.

We offer general security awareness training and tailored programs to suit your needs:

GENERAL SECURITY AWARENESS

- PHISHING & SOCIAL ENGINEERING
- SECURE EMAIL PRACTICES
- BROWSER & WEB SECURITY
- PASSWORDS & ENCRYPTION
- SOCIAL MEDIA
- PRIVACY
- MOBILE DEVICES
- STAFF POLICY RESPONSIBILITIES

TAILORED TRAINING

- INCIDENT RESPONSE
- CORPORATE POLICIES
- INDUSTRY REGULATIONS
- BOARD EDUCATION
- SECURITY BRIEFINGS

Red Piranha offers standard and tailored online cybersecurity training programs to help your staff understand risks as well as policies and procedures to better protect your organisation.

BENEFITS

Upskill your staff
—
Reduce risk
—
Ensure compliance

Red Piranha
Automated Cybersecurity

We're helping protect the world from cybersecurity threats by providing automated security solutions for every business; large and small.

ISO 27001 — Information Security Management System Certified

Certificate No. 781489
Crystal Eye Security operations

---

* Australian Government's Office of the Australian Information Commissioner, Notifiable Data Breaches Scheme 12 month Insights Report, July 2019

SECURITY TRAINING

Compliance

Businesses are under increasing pressure to meet a range of compliance requirements such as ISO 27001. Almost every standard and industry best practice now mandates a form of security awareness training. Cybersecurity is no longer just a technology issue; it is a business issue, too.

Why Security Training?

If your staff are unable to recognise a security threat, taking the necessary steps to avoid it and report it is not possible. Even with the right security controls in place, the human element can render these systems useless, exposing organisations to many forms of cyberattacks. People, not technology, are the most common entry points for many cyberattacks. When employees are aware of security threats, what they look like, and what procedures to follow once identified, you're strengthening one of the weakest links in your security chain.

Security Policies

Significant time and resources are spent developing corporate policies; however, too often, they're not implemented or communicated to staff correctly. Red Piranha can develop a tailored training module to ensure your staff understand your corporate policies and aren't posing a risk to your business. Most employees aren't aware of what applications and programs they aren't allowed to run on the corporate network. Knowing what to do and what not to do, as well as the possible impacts of not following policies and procedures is vital.

The Right Training Program

Security awareness training is not a one-off event. A comprehensive training program must be developed to ensure all staff understand and apply the necessary behaviours and skills to keep your organisation secure. An effective program includes staff induction training as well as continuous and engaging communications, with staff reminded of their responsibilities and updated with new developments.

Training programs need to accurately track employees' completion of various training modules to ensure compliance and effectiveness. Monitoring training activity allows you to see which team members need extra training to strengthen your weakest links. Security is everyone's responsibility. Awareness training makes everyone accountable for their actions, creating a shared sense of responsibility company-wide.

Staff are Critical

People are your most valuable assets and the highest operating expense for most organisations. With such a significant investment in your team, it's critical to ensure they're doing their job in an effective, safe and compliant manner. Staff are on the front line not only to your customers, suppliers and partners but also the first point of call for cybercriminals looking to exploit weaknesses and gain access to sensitive information.

Conclusion

Cyberattacks are no longer a case of "if I get attacked" but a matter of "when I get attacked". Give your organisation the chance to avoid an incident. A single employee who knows how to recognise a threat could be the difference between staying secure and a crippling breach. Ultimately, when it comes to cybersecurity training for employees, the only question to be asked is "Are you doing enough?"

PRICING

Standard pricing is available for general security awareness training and our custom programs are priced for your specific requirements.

—

NEXT STEPS

1. Get in touch

2. Get a proposal

3. Get started

—

+61 8 6365 0450
redpiranha.net
sales@redpiranha.net

Red Piranha Services

- Assessment
- Resourcing
- Compliance
- Training
- Testing
- Management
- Investigation

AUTOMATED PROTECTION ▶ **AUTOMATED DETECTION** ▶ **AUTOMATED RESPONSE**