RESOLUTION IT
A zenzero COMPANY

Awareness to Action

Building a Cyber-Safe Workplace

Guernsey | Jersey | Dubai
resolutionit.com
hello@resolutionit.com

With 95% of data breaches caused by human error, the most effective defence is a well-informed, vigilant workforce.

This guide will help you understand why cyber awareness matters, how to embed it into your company culture and what practical steps you can take to protect your organisation.

Contents

Why Cyber Security Culture Matters

Cyber security is like a chain, its strength depends on every link. When employees are aware and engaged, the organisation becomes resilient. But when awareness is low, vulnerabilities emerge.

- Human error is the leading cause of breaches: Clicking phishing links, ignoring updates, or using weak passwords can open the door to attackers.
- Culture is a strategic asset: A cyber-aware culture reduces risk, improves compliance, and builds trust with clients and regulators.

95%
of data breaches are due to human error

84%
of UK cyber attacks are phishing attacks

7.8m
cyber attacks on UK businesses in 2024

Leadership Sets the Tone

A strong cyber culture starts at the top. When leaders champion cyber awareness, it sends a powerful message.

- Lead by example: Executives should participate in training and promote cyber hygiene.
- Make it visible: Start meetings with cyber updates or stories to keep awareness front of mind.
- Integrate into KPIs: Include cyber awareness goals in performance reviews and strategic planning.

For organisations without a dedicated security team, a virtual Chief Information Security Officer (vCISO) offers strategic leadership. This is a great way to foster a culture of cyber awareness from the top down. Leading by example is a great way to get employees engaged in cyber security practices.

Training as a Journey

Training should be a continuous journey to keep knowledge current and front of mind.

Security is everyone's business. Empower your employees to take ownership.

- Cyber Security Champions: Appoint advocates across departments to answer questions and promote best practices.
- Clear Reporting Channels: Make it easy to report suspicious activity without fear of blame.

In-Person Training

Led by cyber security experts, in-person sessions build trust and engagement.

- Customisable: These sessions can be tailored to different industries, roles or regulatory requirements.
- Interactive: In-person training is an interactive, collaborative environment, where attendees can ask questions to aid their learning.

Bite-Size Virtual Learning

Microlearning modules on phishing, password hygiene, and secure remote working.

- Fun and engaging: Gamified content to make learning memorable.
- Regular refreshers: Virtual learning sessions can be sent out regularly to help keep knowledge front of mind.

Simulated Phishing Campaigns

Test employee awareness in a safe environment and use results to educate and reinforce best practices.

- Measure training effectiveness: Test how well your user training is translating to practival knowledge and safe behaviours.
- Identify vulnerabilities: Identify which employees or departments are more susceptible to phishing attacks, allowing for targeted training and resources.

Building for the Future

Building a strong and sustainable cyber security culture is an ongoing journey.

- Stay updated: Monitor emerging threats and update training accordingly.
- Review policies regularly: Ensure they reflect current risks and technologies.
- Celebrate success: Recognise teams and individuals who demonstrate strong cyber hygiene.
- Cyber Security Champions: Appoint advocates across departments to answer questions and promote best practices.
- Clear Reporting Channels: Make it easy to report suspicious activity without fear of blame.

Measure Success

Consistently tracking performance will help you make improvements.

- Track training participation and phishing simulation results
- Use feedback to refine content and delivery
- Monitor incident reporting trends and response times

Resolution IT

Cyber Security Awareness Training

Creating a good security culture isn't a one-off initiative – it's an ongoing journey. By combining strategic leadership, engaging security training, and continuous learning, organisations can build a resilient, security-conscious workforce that protects both data and reputation.

At Resolution IT, we work with organisations across Guernsey, Jersey, and Dubai to deliver tailored cyber security solutions that drive measurable results.

Let's strengthen your cyber security culture together.

hello@resolutionit.com
resolutionit.com

GUERNSEY | JERSEY | DUBAI

RESOLUTION IT
A zenzero COMPANY