MAKE YOUR EMPLOYEES THE FRONTLINE OF CYBER DEFENSE.

Let us provide you a full picture of your company's security posture and potential risk, so the employees who were the weakest link in your defense can become its strongest point of protection.

CYBER-ATTACKS ARE ON THE RISE

Because employees are the core of any business, they will be the main target for cyber criminals. Making sure your people stay up-to-date with cyber security knowledge, and teaching them to recognize threats, is imperative to the security of your business. The threat landscape is constantly evolving, and so should your approach to defense.

90%
of security breaches are inadvertent, unintentional, and caused by human error.

TRAIN AND PHISH!

Trained and aware employees are critical to securing an organization, and an effective, ongoing internal security awareness program can help reduce your company's vulnerability, turning the "weakest link" in your cyber defenses into its greatest strength.

92.4%
of malware is delivered via email

Security awareness training and phishing simulations go hand in hand. Phishing has become very sophisticated and almost undetectable, as criminals have found ways to make their emails as realistic as possible. Phishing simulations test employees on how they would respond to a real-life phishing attack. We can send these mock attacks at staggered times, avoiding the "prairie dog effect" where employees warn one another of the email, for the best measurement of all employees' awareness. We'll track which employees have clicked on a phishing email, who has given away their password and who has ignored the email.

Once a learning gap is detected, we'll deliver interactive educational videos to the most susceptible users. These easy-to-understand, short and visually engaging training videos include an online quiz to verify the employee's retention of the training content. Training can be delivered regularly, to reinforce the importance of every employee's role in protecting your business.

Designed to Protect Against Human Error.

01454 838490 | security@refresh-it.co.uk

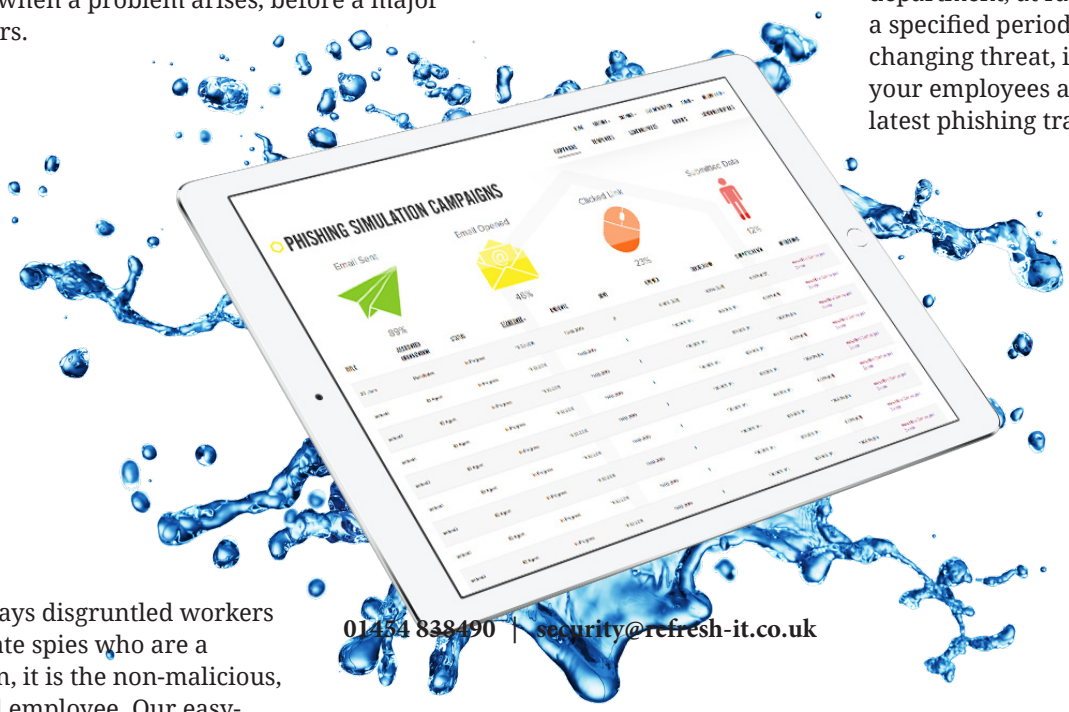
PHISHING SIMULATION & SECURITY AWARENESS TRAINING.

DETECT

Employees often use the same password for multiple services on the web, such as CRM, e-commerce sites, and social media. Proactive monitoring for stolen and compromised employee data on the dark web allows us to detect when a problem arises, before a major breach occurs.

PHISH

We can send scheduled phishing campaigns, including customized messages to fit each group or department, at random times during a specified period. With an ever-changing threat, it is important that your employees are exposed to all the latest phishing traps set by criminals.



TRAIN

It is not always disgruntled workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee. Our easy-to-understand, short and visually engaging training videos end with an online quiz to verify the employee's retention of the training content.

MEASURE AND TRACK

Your regular Security Threat Report will demonstrate the overall cybersecurity posture of your organization, to include dark web credential compromises combined with employee phishing and training campaign results.

WHY YOU NEED AN INTEGRATED, ONGOING PROGRAM

- Cyber-attacks are on the rise; particularly among small- and mid-sized businesses.
- You may have the most up-to-date and strongest security systems in place, but this will be a wasted investment if you don't also train and test your staff.
- Threats are ever-evolving and become more sophisticated and harder to detect. Regular training on the latest criminal tactics will help mitigate risk.

Your employees are your first and primary line of defense against online crime. Equip them with the knowledge and skills they need to protect themselves - and your business - from criminal elements.

01454 838490 | security@refresh-it.co.uk