Security Awareness Training

Designed to Protect Against Human Error

CYBER ATTACKS ARE ON THE RISE

Employees are the core of any business and for this reason they are often the main target during a cyber attack. Making sure your employees stay up-to-date with cybersecurity 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.

Cybercriminals are always on the hunt for vulnerabilities and they often can be found in your own employees. Though automated campaigns and often targeted socially engineered attacks, hackers will attempt to get users to grant them access to a credentials, data and even large sums of money.

TRAINING AND PHISHING SIMULATIONS

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.

Security awareness training and phishing simulations go hand in hand.

Email Phishing is when a hacker fraudulently attempts to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity. Phishing has become harder to detect as criminals have found ways to make their emails as realistic as possible.

These emails can be designed to come from coworkers, banks, email providers,

90%
of Breaches Are Caused By Human Error.*

Phishing simulations test employees on how they would respond to a real-life phishing attack. We can send these mock attacks at staggered times which helps avoid the "prairie dog effect" where employees warn one another of the email. We'll track which employee behaviors and report on which employees ignored, click or completed the objected of the simulated attack.

*Willis Towers Watson

V19.1

844.638.7328 | SALES@SECNAP.COM | SECNAP.COM

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.

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.

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.

Benefits of an Ongoing Security Awareness 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 keep your data safeguarded.