Security Education & Awareness Training

Cyber heists are costing millions of dollars, and 79% of small and medium-sized businesses have become the biggest targets. Educating employees with the knowledge they need to identify the techniques hackers use to target humans has become a critical, yet small investment to help prevent a business from falling prey.

Your employees will learn how to identify common threat tactics:

» Social engineering
» Phishing
» Spoofing
» Ransomware

Employees are the weakest link in your IT security

The bad guys go after them because all too often your employees are easy to trick. Your defense is to create a "human firewall" which relies both on technology and the ability of employees to recognize risky situations and act accordingly. Locknet's Security Education & Awareness Training will help keep your employees on their toes.

Protect yourself and your business

With Security Education & Awareness Training, Locknet uses the most state-of-the-art training and engages its security team to help you define your online training campaign, schedule simulated attacks, and provide the necessary reporting for compliance requirements. Locknet is there to answer questions every step of the way.

Our training arms your employees with the knowledge they need, including:

» Self-service enrollment—employees take the training when it fits their schedule
» Pre- and post-training audits assess the impact of the training
» Online training includes case studies, live demonstration videos, and short tests
» Tests conclude each module assuring employees have retained the information
» Monthly phishing security test
» Access to administrative portal
» Large selection of security awareness training courses
» Monthly email exposure check

Process (36-month program)

1. We send a pre-test simulated phishing attack to your employees and report how "phish-prone' your organization is
2. Training starts when your employees receive an email requiring them to complete the e-learning modules
3. A dashboard allows management to audit who has, and has not, completed the training
4. After training is complete, another simulated phish attack assesses your security training effectiveness, individual follow-up can occur for those who remain at risk
5. Monthly recurring phishing tests to keep employees aware and engaged

LOCKNET
AN EOJOHNSON COMPANY

locknetmanagedit.com » 844-365-4968