EMPLOYEE SECURITY TRAINING

ACE Technology Group

SECURITY AWARENESS TRAINING

Reduce human vulnerabilities through a robust security awareness program. With continuous training and informative quizzes, employees will be up to date on the latest threats.

SENSITIVE COMPANY DATA

Employees will learn what PII (Personally Identifiable Information) and sensitive company data are, where they are located, and how they can do their part in helping protect it.

BREACH RESPONSE

It's important to prepare business owners and employees for how to respond to a breach, similar to how they'd prepare for a potential fire in the building. Repetition is often the key to preparation, and can make the difference between getting an insurance payout and having to foot the bill yourself. Cyber-Liability claims can get rejected if you haven't taken proper precautions and training.

THREATS

The training courses educate staff on the different tactics cyber criminals use to trick their victims. Some topics include phishing, password reuse, and more.

CYBERCRIME TARGET

Whether or not you are running a multi-million dollar business, or a small mom and pop store, your data is a target for cybercrime. If a bad actor gains access to your customer data, they can easily monetize and sell it on the dark web.

PHISHING SIMULATIONS

1. SEND PHISHING TESTS

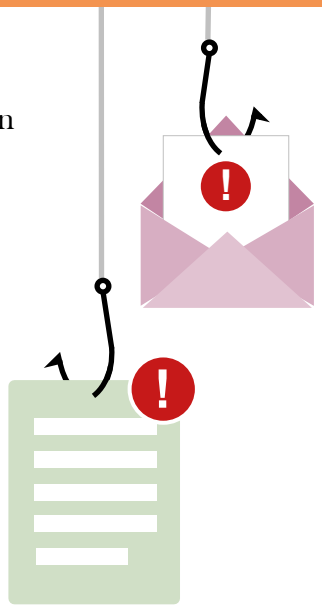
Our security awareness & training platform automatically sends phishing tests on your specified schedule that mimic real world phishing scams.

2. IDENTIFY & ADDRESS

Identify which employees are clicking phishing links so they may be addressed through supplemental training, likely preventing them from clicking a link in an actual phishing email.

3. IMPROVE RESILIENCE

Phishing simulations provide a valuable metric for the management team. Over time, the results of phishing simulations have a tendency to show gradual improvement in employee decision making around phishing emails. Harness the power of built-in reporting tools to generate educational and data-driven reports that offer insight on employee performance.



95% of breaches are caused by **human error.**

43% of employees are not aware that clicking a suspicious link or opening an unknown attachment in an email is **likely to lead to a malware infection.**