CautelaLabs

Social engineering attacks are widespread and growing. The human element is often the weakest component in a company's security. Attackers know this and exploit it.

- 78% of malicious software attacks used email attachments.[1]
- Spear-phishing attacks increased 91% in 2013 and an additional 8% in 2014.[2]
- Sales/Marketing, Finance, and Operations were targeted most often.[2]
- Over $5.9 billion is lost annually due to phishing.[3]
- Successful phishing attacks account for over 20% of reported breaches in 2014.[4]

Key Benefits

Phishing simulation exercises can provide a measurable increase in security. Clients can expect initial failure rates exceeding 30%. Targeted training can reduce that rate to around 5%. Ongoing training and testing addresses employee turnover and forgetfulness, maintaining failure rates at a low level.

Phishing simulations let employees to experience a phishing email, allowing them to associate the training with an actual event. After seeing the phishing email and receiving targeted training, employees better understand the risk and are more security-conscious.

Targeted training aimed specifically at employees who have been susceptible to a phishing email, as demonstrated by repeat failures, can address those employees without the cost and burden of training all employees, increasing security compliance with a lower impact on overall productivity.

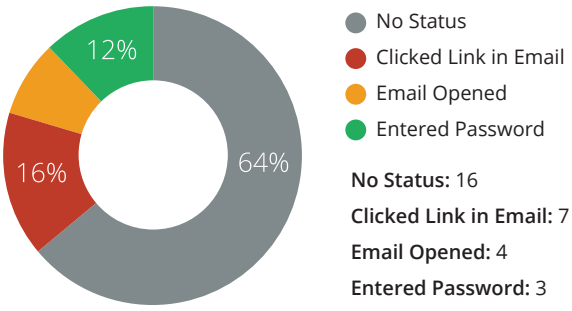
Comprehensive reporting helps key stakeholders understand the security weaknesses and provides evidence to obtain executive management buy-in for security initiatives.

Ongoing phishing simulations with targeted training demonstrates that the company understands the current threats and is taking steps to reduce risks to their customer data.

Features and Capabilities

- Choose one time or ongoing phishing tests
- Targeted or random selection of recipients
- Customized and default email templates
- Immediate training feedback for susceptible users
- Comprehensive reporting showing individual user actions
- Historical and trending reports to measure increases in compliance
- No software or hardware to implement

Summary graphics show increasing levels of response



(1) Verizon Data Breach Investigations Report, 2014
(2) Symantec Internet Security Threat Report, 2014
(3) 2013 A Year in Review – RSA Fraud Report
(4) Verizon Data Breach Investigations Report, 2015

sales@cautelalabs.com | 5080 N. 40th Street, Suite 300 | Phoenix, AZ 85018 | 800-997-8132