Build a Cyber-Smart Workforce to Eliminate Security Risk

It's time to transform your employees into trusted guardians of your organization's data and infrastructure. SecurityIQ can help. By integrating comprehensive security education, learner risk detection and corrective data-driven actions into a single platform, SecurityIQ empowers your workforce and strengthens your human line of defense against phishing attacks, malware,social engineering, ransomware and other cyber threats.

*REDUCE PHISHING SUSCEPTIBILITY TO LESS THAN 1%*

PROTECT
Your Data

It's proven. The most effective foundation to data protection is a comprehensive security awareness and education program that combines:

- » Real-world phishing simulations
- » Engaging role-based training
- » One-button suspicious email notifier for employees
- » Offline awareness reinforcement

Data from over 1 million learners across industries shows SecurityIQ measurably reduces phishing susceptibility rates. At InfoSec Institute, we see most teams' initial phish rates around 29%. Using SecurityIQ's immersive phishing simulator, PhishSim™, drops your phish rate to 7%. Add AwareEd™ educational modules and see your phish rates drop as low as 1%.

Phish Rate vs. Months chart:
- 29% at month 0
- 16% at month 3 (Phishing Simulations Only)
- 6% at month 3 (Phishing Simulations & Security Awareness Training)
- 7% at month 12 (Phishing Simulations Only)
- 1% at month 12 (Phishing Simulations & Security Awareness Training)

● Phishing Simulations & Security Awareness Training
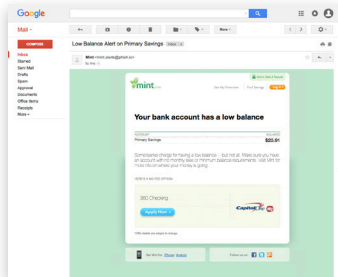● Phishing Simulations Only

DETECT
Human Endpoint Risks

Cutting susceptibility rates to 1% is significant, but does not completely mitigate cyber threats. Tackling the final 1%, requires an understanding of employee and departmental risk profiles. Through Security Posture Scorecarding, SecurityIQ continually monitors and reports all learning behaviors and outcomes. This holistic view of risk profiles and potential vulnerabilities across your entire organization gives you valuable insight into which departments, learner groups or individuals may require additional training or corrective reinforcement.
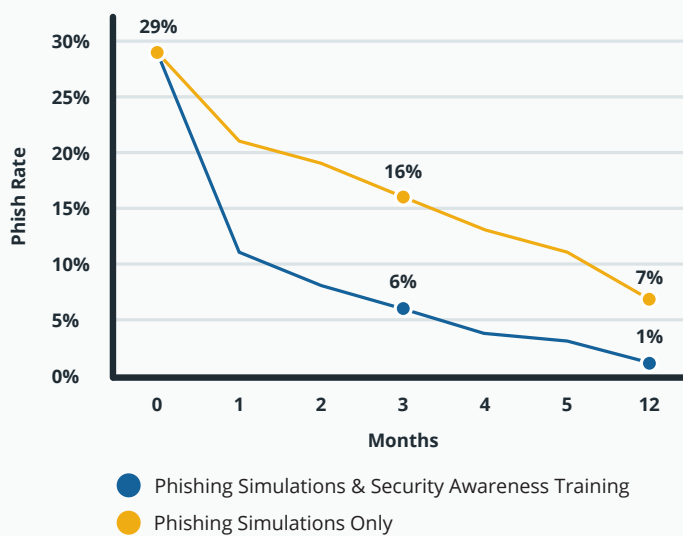
CORRECT
Learner Behavior

Driven by Scorecarding metrics, SecurityIQ dynamically builds and maintains learner groups based on employees' risk profiles and criteria you establish. PhishDefender™, leverages these groups to increase (or decrease) an individual's security controls. For example, a learner with a scorecard grade of C- or lower may see hyperlinks stripped and disabled from email body text. If after additional security awareness training, this learner's grade improves to an acceptable level, SecurityIQ restores email link functionality.

PROTECT

PhishSim

» 200+ frequently updated, real-world phishing simulation templates

» Programmed for progressive difficulty (automated or manual configuration)

» Phishing attack simulations (drive-by, data entry, attachment), spear-phishing, USB campaigns, Vishing, SMiShing and more

» PhishNotify one-button reporting and quarantine of suspicious emails

» Multi-language support
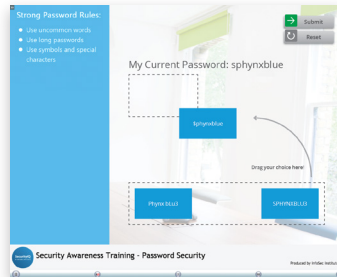
AwareEd

» Secure LMS with interactive, gamified learning & quizzes

» 130+ frequently updated AwareEd training modules

» All based in science-backed educational methods

» Customizable role- and industry-based modules

» Multi-language support

Security Excellence Resource Kit

» 12-month reinforcement program and project plan (posters, newsletters, handbooks, employee communication templates and more)

» Dedicated Client Success Manager from deployment to data-to-day management

» Resources to build executive and departmental buy-in

» Actionable performance analytics for program evaluation

» "Boardroom-ready" performance reports for public filings and risk evaluations

DETECT

» Analytics and reports to track start/completion rates and learners' training progress

» Learner grades and security posture scorecarding for individuals and departments

» Leaderboards to boost participation and engagement

» PhishSim analytics and reports to track open, phish and avoid rates

» PhishNotify-submitted phishing threat reports

CORRECT

» Learner grade analysis to auto-enroll at-risk users in additional training

» PhishDefender to dynamically increase/decrease security controls on risk-prone learners or groups

» Custom rule-based learner group creation

» At-a-glance management views of team progress and outcomes

» Internal program administrator reports

INFOSEC INSTITUTE