

Healthcare Research and Development

Results Snapshot: Security Awareness and Training Software, Managed Services

Scope

A healthcare research and development company evaluated Wombat's Managed Services offering along with components of the Wombat Anti-Phishing Training Suite. A test group of nearly 1,000 employees from the company's IT department took part in the three-stage Results Snapshot, which included two PhishGuru® assessments and two interactive training modules, *Email Security* and *URL Training*.

Process

1. All participants were sent an initial PhishGuru mock attack to assess employee recognition of phishing emails and establish a baseline vulnerability measurement. All employees who fell for (i.e., clicked) the email immediately received a Teachable Moment message explaining what happened and offering tips to avoid future traps.
2. Individuals who fell for the initial simulated attack were automatically scheduled for follow-up training via our Auto-Enrollment feature. Those who did not fall for the attack received training assignments via email. Training was voluntary for all users.
3. Following the 30-day training period, a second PhishGuru assessment was sent in order to measure the level of improvement.

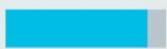
Results

1. **Initial PhishGuru assessment** – 334 users fell for the simulated attack, an email that posed as a social media connection request from the company's CIO. This represents a 34.7% failure rate.
2. **Follow-up education** – 535 of the 962 total users attempted or completed the modules, for a training penetration rate of 55%. Of the users who were auto-enrolled, 80% took the training, a significant increase over the 42% who weren't auto-enrolled. (*Note: Users who fall for a simulated attack are very motivated to complete follow-up training, even when it's voluntary.*)
3. **PhishGuru reassessment** – Only 104 users fell for the second mock attack, a message that claimed users needed to update their passwords following a security update to a popular social media site. This represents a failure rate of 10.8%. Of those who fell for the second attack, 45 were repeat offenders (i.e., they had also clicked on the initial message).

Overall Risk Reduction

The company saw a **69% reduction** in vulnerability between the first and second PhishGuru assessments, with 230 fewer users falling for the follow-up simulated attack.

Healthcare R&D Cyber Risks

91% 

The percentage of healthcare organizations that have suffered at least one data breach in the past two years

Source: Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute

£1.8B
(~\$2.8B*) per year

The impact of IP theft on UK pharmaceutical companies alone

Source: The Cost of Cyber Crime, the United Kingdom Office of Cyber Security and Information Assurance

* Conversion calculated on 5/20/15