Healthcare Products and Services (B2B)

Proof of Concept: Anti-Phishing Assessments and Education

Scope

A global B2B healthcare product and service provider evaluated components of the Wombat Anti-Phishing Training Suite. A test group of 50 employees took part in the three-stage Proof of Concept, which included two simulated phishing assessments and our *Email Security* interactive training module.

Process

1. All participants were sent an initial simulated 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 on avoiding future traps.
2. Individuals who fell for the initial mock attack were automatically scheduled for follow-up training via our Auto-Enrollment feature. Those who did not fall for the attack received a training assignment via email. Users had one month to complete the voluntary education. (*Note: Though completion was not mandatory, our experience has shown that linking assessments and training markedly raises participation rates.)*
3. Following the one-month training period, users were sent a second simulated phishing attack in order to measure the level of improvement.

Results

1. **Initial phishing assessment** – 25 users fell for the simulated attack, an email from "Voicemail System" that indicated users had a voicemail waiting from an unknown caller. This represents a 50% failure rate.
2. **Follow-up education** – 33 of the 50 total users accessed the *Email Security* interactive module, for a training penetration rate of 61%.
3. **Phishing reassessment** – Only seven users fell for the second simulated attack, a message from "Help Desk" that asked employees to change their passwords as part of a standard 90-day update process. This represents a failure rate of 14%. Four of the seven in this group were repeat offenders (i.e., they had also clicked on the initial message).

Overall Risk Reduction

The company saw a **72% reduction** in vulnerability between the first and second simulated phishing assessments, with 18 fewer users falling for the follow-up mock attack.

Healthcare Cyber Risks

63%
of detected healthcare-related security incidents affected availability of email and applications; unintentionally exposed private or sensitive data; and/or compromised customer records[1]

12%
of identified security incidents targeted the Retail/Wholesale and Health and Social Services industries[2]

More than **95%**
of identified security incidents recognized "human error" as a contributing factor[2]

76%
less is spent on security events when employees are trained[1]

[1] Source: *2014 US State of Cybercrime Survey*

[2] Source: *IBM Security Services 2014 Cyber Security Intelligence*