Hospital and Medical Center

Results Snapshot: Anti-Phishing Awareness and Training

Scope

A regional hospital and medical center based in the southeastern U.S. evaluated components of the Wombat Anti-Phishing Training Suite. A test group of 501 employees took part in the three-stage Results Snapshot, which included two simulated phishing assessments and one interactive training module, *Email Security*.

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 to avoid future traps.
2. Individuals who fell for the initial 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.
3. Following the three-week training period, a second simulated phishing assessment was sent in order to measure the level of improvement.

Results

1. **Initial phishing assessment** – 243 users fell for the simulated attack, an email that posed as blocked email notification. This represents a 48.50% failure rate.
2. **Follow-up education** – Of the users who were auto-enrolled in the *Email Security* module, 75% completed the training. This is a marked increase over the 53% completion rate of users who were not auto-enrolled. This reflects a trend we often see with our customers: Users who fall for a simulated attack and receive an immediate training assignment are very motivated to complete follow-up education, even when it's voluntary.
3. **Phishing reassessment** – Only 34 users fell for the second simulated attack, a message that claimed a user's online healthcare account had been suspended due to unauthorized access. This represents a failure rate of 6.79%. Of those who clicked, 22 were repeat offenders (i.e., they had also clicked the initial message).

Overall Risk Reduction

The company saw an **86% improvement** between the first and second simulated phishing assessments, with 209 fewer users falling for the follow-up mock attack.