Restaurant and Retail Sales

Results Snapshot: Anti-Phishing Awareness and Training

Scope

A restaurant chain and food product retailer in the northeastern U.S. evaluated components of the Wombat Anti-Phishing Training Suite. A test group of 234 employees took part in the three-stage Results Snapshot, which included two simulated phishing assessments and two interactive training modules, *Email Security* and *URL Training*.

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 mock 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. A month after the 30-day training period, a second simulated phishing assessment was sent in order to measure the level of improvement.

Results

1. **Initial phishing assessment** – 72 users fell for the simulated attack, an email that posed as a password change request. This represents a 30.7% failure rate.
2. **Follow-up education** – 132 of the 234 total users attempted or completed the modules, for a training penetration rate of 56%. Of the users who were auto-enrolled, 85% participated in the training, a marked increase over the 66% 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. **Phishing reassessment** – Only 1 user fell for the second simulated attack, a message that claimed users needed to perform a security update. This represents a failure rate of just 0.4%. The lone clicker on the second email was a repeat offender (i.e., the user had also clicked the initial message).

Overall Risk Reduction

The company saw a **98.6% reduction** in vulnerability between the first and second simulated phishing assessments, with 71 fewer users falling for the follow-up mock attack.