International Manufacturer

Results Snapshot: Anti-Phishing Awareness and Training

Scope

A Fortune 1000 manufacturer of energy and power management products evaluated components of the Wombat Anti-Phishing Training Suite.
A test group of 200 employees took part in the three-stage Results Snapshot, which included a baseline simulated phishing assessment, a training assignment (our interactive *Email Security* module), and a follow-up phishing assessment.

Manufacturing Data Breach Statistics

73%

of breaches resulted from attacks that combined social engineering and malware (e.g., a phishing email with a malicious link or attachment)

94%

of breaches linked to cyber-espionage

90%

of data stolen was classified as corporate secrets/intellectual property

Source: *2017 Verizon Data Breach Investigations Report*

Process

1. The initial simulated attack was sent to all participants 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 training period, a second simulated phishing assessment was sent in order to measure the level of improvement.

Results

1. **Initial phishing assessment** – 52 users fell for the baseline attack, a simulated corporate eFax notification, a 26% failure rate.
2. **Follow-up education** – An overall training penetration rate of 29.5% was achieved, with 59 of 200 users completing training. However, there was a much higher assignment completion rate with the users who were auto-enrolled: 25 of 52 (48%) completed training compared to 34 of the 148 (23%) who received the voluntary training assignment via email.
3. **Phishing reassessment** – Just 28 users — a 14% failure rate — fell for the second simulated attack, a message intended to fool users into believing an outgoing email had been blocked by a spam filter. Of those who clicked, 22 were repeat offenders (i.e., they had also clicked the initial message).

Overall Risk Reduction

The 48% participation in auto-enrolled training likely contributed to the **46% improvement** between the two phishing assessments. A more knowledgeable user base is key to reducing risk over the long term.