CYBERSNAP
Cybersecurity Culture Creators

Segregating Phishing Tests and Cybersecurity Awareness Training Providers

Executive Summary

Phishing simulations and cybersecurity awareness training are essential pillars of an organization's defence against social engineering and cyberattacks. However, when the same provider delivers both activities—or when each provider is aware of the other's methods—their effectiveness is diminished. This white paper outlines the compelling reasons to engage separate, independent companies for phishing assessments and cybersecurity awareness training, ensuring neither is privy to the other's strategies or schedule.

Introduction

- **Phishing simulations** assess an organization's resilience to real-life email-based attacks by attempting to deceive employees in a controlled manner.
- **Cybersecurity awareness training** educates users on best practices, risks, and response strategies, typically following missed simulations or scheduled sessions.

Conducting both activities independently and without coordination prevents bias, creates realistic testing conditions, and provides more accurate metrics of employee readiness.

Key Arguments for Separation

1. Objectivity and Unbiased Metrics

- **Eliminates bias in performance results:** If the training company is aware of test scenarios, it may tailor content too closely to anticipated simulations, artificially boosting success rates.
- **Phishing assessments should be blind:** Mimicking real-world unpredictability simulates actual attacker tactics, yielding authentic behaviour instead of patterned responses.

2. True Measurement of Behavioural Change

- **Independent evaluation:** Only by acting independently can phishing tests genuinely reflect the transfer of knowledge from training to practical action.
- **Avoidance of "teach to the test":** Employees retain knowledge better when unaware of the exact nature or timing of simulations; this also reduces risk of information leaks or collusion.

3. Strengthened Security Posture

- **Defence-in-depth approach:** Using multiple vendors reduces the risk of a single point of failure or systemic oversight, comparable to having separate auditors and accountants.
- **Reduces insider threat risk:** Segregating sensitive knowledge between organizations mitigates the chance of intentional or unintentional leaks.

4. Regulatory and Audit Requirements

- **Improved audit trails:** Independent records and methodologies lend credibility and transparency during external audits.
- **Alignment with best practices:** Leading frameworks (e.g., NIST, ISO/IEC 27001) encourage independent testing and review to detect issues missed by internal teams.

Potential Risks of Combined Providers

Risk	Impact
Training tailored to test clues	Inflated success rates, false confidence
Shared scheduling reduces test surprise	Employees become alert only during test windows
Increased chance of operational shortcuts	Overlooked security gaps
Single-provider bias	Reduced diversity in tactics and approaches

Benefits of Independent, Disconnected Providers

- **Unannounced, unpredictable testing.**
- **Continuous improvement:** Training evolves to address emerging threats while tests adapt to exploit new vulnerabilities.
- **Clearer ROI measurement:** Leadership gains visibility into actual strengths and gaps, enabling more effective allocation of resources.

Practical Implementation Guidance

- Use different vendors for phishing simulation and cybersecurity training.
- Do not disclose the testing schedule or simulation themes to the training company (or vice versa).
- Rotate simulation vendors or training providers periodically to ensure ongoing integrity and diversity in approach.

Conclusion

Segregating phishing testing and cybersecurity awareness training ensures that neither provider has insight into the other's activities, generating authentic and actionable insights. This approach builds organizational resilience and a genuinely alert workforce, ready to counter modern cyber threats.

Elevate your organization's security posture—commit to truly independent phishing tests and cybersecurity awareness training.

Contact Cybersnap today! info@cybersnap.ca / Canada: 1-647-948-7769 / U.S.A.: 1-322-244-9225