In Zusammenarbeit mit HSLU Hochschule Luzern

STUDIENZUSAMMENFASSUNG

Verbesserung des Cyber-Risikoverhaltens durch KI-Spearphishing

✳ Zusammenfassung

Diese Studie untersuchte, wie man Mitarbeiter davon abhalten kann, auf gefährliche E-Mails zu klicken, indem drei Methoden getestet wurden: Normale Cybersicherheitsschulungen, reguläre Phishing-Simulationen und neues KI-Spearphishing. Sie zeigte, dass die Einstellung zu Cyberrisiken (Risikohaltung) sich vom tatsächlichen Handeln (Risikoverhalten) unterscheidet.

✳ Wie verschiedene Methoden das Klickverhalten beeinflussten

Schulungen (Normative Sensibilisierung)

Ausgangswert: 21,3%–25,5% besuchten schädliche Websites
Nach Schulung: 12,1% besuchten schädliche Websites

Konventionelle Phishing-Übungen

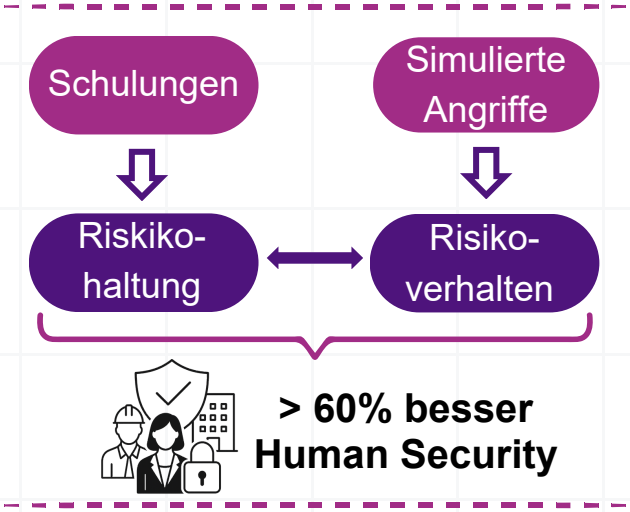
Ausgangswert: 19,0%–19,7% besuchten schädliche Websites
Nach konventionellem Phishing: 10,9% besuchten schädliche Websites

KI--gestütztes Spearphishing

Ausgangswert: 22,6%–23,4% besuchten schädliche Websites
Nach KI-Spearphishing: 8,9% besuchten schädliche Websites

Gemessene Verbesserung der Human Security

KI-gestütztes Spearphishing reduzierte riskantes Klickverhalten um bis zu ~60% im Vergleich zum Ausgangswert. Mitarbeiter, die personalisierten Angriffen ausgesetzt waren, zeigten die geringste Interaktion mit schädlichen Links (8,9%) im Vergleich zu ~23% beim Ausgangswert. Dies zeigt, dass gezielte Exposition zu stärkeren Verhaltensänderungen führt als Sensibilisierungsschulungen oder generische Simulationen.



Fazit

Unternehmen sollten eine Kombination aus Schulungen, Phishing-Simulationen und insbesondere KI-gestützten Spearphishing-Übungen einsetzen, um Mitarbeiter wirklich vorsichtig zu machen und die Organisation vor modernen Cyberangriffen zu schützen. CYBERDISE Awareness bietet alle drei Ansätze in einer universellen Lösung.

Lesen Sie die vollständige Studie „Improving Cyber Risk Behavior through AI-Enabled Spearphishing - A Comparative Analysis" auf **cyberdise-awareness.com**