In collaboration with HSLU Hochschule Luzern

STUDY SUMMARY

Improving Cyber Risk Behavior with AI-Spearphishing

Executive Summary

This study examined **how to stop employees from clicking** on dangerous emails by testing three methods: Normal cybersecurity training; Regular fake phishing; New AI-Spearphishing. It showed that how people think about cyber risks (**risk attitude**) is different from how they act (**risk behavior**).

How Different Methods Affected Clicking Behavior

Training (Normative Awareness)

Baseline: 21.3%–25.5% visited malicious sites
After training: 12.1% visited malicious sites

Conventional Phishing Exercises

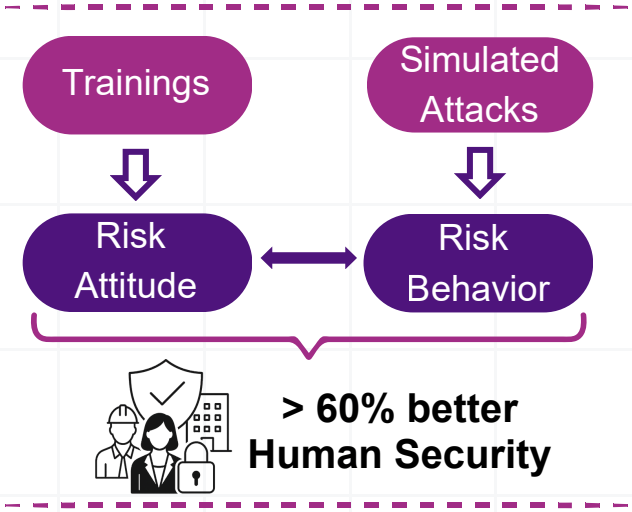
Baseline: 19.0%–19.7% visited malicious sites
After conventional phishing: 10.9% visited malicious sites

AI-Enabled Spearphishing

Baseline: 22.6%–23.4% visited malicious sites
After AI-spearphishing: 8.9% visited malicious sites

Measured Improvement in Human Security

AI-enabled spearphishing reduced risky clicking behavior by up to ~60% compared to baseline. Employees exposed to personalized attacks showed the lowest interaction with malicious links (8.9%), compared to ~23% at baseline. This demonstrates that targeted exposure drives stronger behavioral change than awareness training or generic simulations.



Conclusion

Companies should use a mix of training, phishing simulations, and especially AI-powered spearphishing exercises to make employees truly cautious and protect the organization from modern cyberattacks. CYBERDISE Awareness provides all three approaches in one universal solution.

Read the full study “Improving Cyber Risk Behavior through AI-Enabled Spearphishing - A Comparative Analysis” at cyberdise-awareness.com