# Was Cybersecurity Awareness mit Schweizer Eishockey gemein hat

**Eine aktuelle Studie der HSLU zeigt: KI-Phishing-Simulationen verbessern das Risikoverhalten von Mitarbeitenden deutlich. Effektives Awareness hat zwei Ströme: Trainings prägen die Einstellung, praktische Übungen das Verhalten. Beides ist notwendig – wie auch im Eishockey.**

Was Cybersecurity Awareness und Schweizer Eishockey gemeinsam haben? Mehr, als man auf den ersten Blick vermuten würde – denn in beiden Fällen macht die richtige Kombination aus Training und praktischer Erfahrung den Unterschied.

## Eishockey als Analogie

Die Schweiz verfügte schon lange über hervorragende Trainer. Der Aufstieg des Schweizer Eishockeys in die Weltspitze nach 2004 war jedoch nicht allein ihr Verdienst. Trainer vermittelten Know-how und arbeiteten an der Einstellung der Spieler. Den entscheidenden Qualitätssprung brachten jedoch die NHL-Stars, die während des Lockouts 2004/05 quasi die ganze Saison in der Schweiz spielten. Ihre Präsenz führte dazu, dass einheimische Spieler ihr Verhalten nachhaltig verbesserten – das Niveau stieg dauerhaft.

## Parallelen zu Cybersecurity Awareness

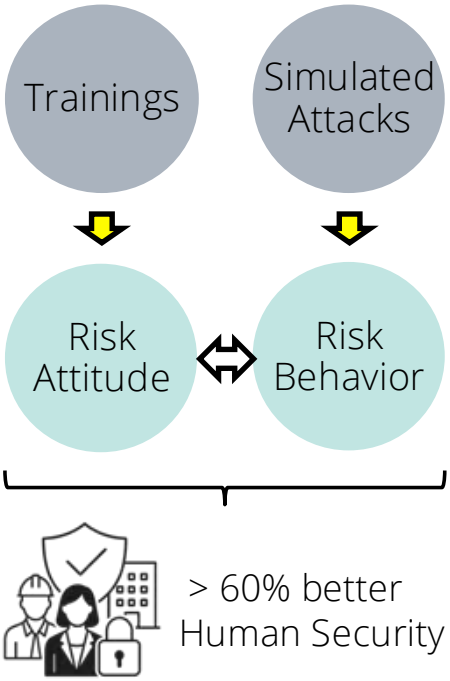
Ein ähnliches Bild zeigt die HSLU-Studie «Leveraging AI-enabled spearphishing to enhance cybersecurity»[1]. Untersucht wurde die Wirksamkeit von KI-/OSINT-gestützten Spearphishing-Simulationen im Vergleich zu klassischen Awareness-Massnahmen, herkömmlichen Phishing-Übungen und normativem Training. Hintergrund: Phishing bleibt auch 2025 das grösste Einfallstor für Cyberangriffe, während Kriminelle längst routinemässig KI einsetzen[2, 3].

## Zentrale Ergebnisse

- Personalisierte KI-Phishing-Übungen sind am wirksamsten für das Verhalten und zugleich am kostengünstigsten.
- KI/OSINT-Simulationen verbessern gemäss der Studie das Risikoverhalten um 60 Prozent gegenüber herkömmlichen Phishing-Übungen.
- Normatives Training beeinflusst vor allem Wahrnehmung und Verantwortungsbewusstsein – also die Einstellung.
- Kombination beider Ansätze (Verhalten & Einstellung) ist notwendig, um nachhaltige Awareness zu erzielen.
- Zeitfaktor: Bereits nach fünf Monaten verlieren einmalige Kampagnen ihre Wirkung. Wer lediglich zwei Kampagnen pro Jahr durchführt, muss jedes Mal von Grund auf neu beginnen und verschenkt den kontinuierlichen Lerneffekt.

## Nachhaltiger Effekt wie im Sport

Der Vergleich zum Schweizer Eishockey macht es greifbar: Trainer stärkten das Mindset, die NHL-Profis verbesserten das Verhalten. Das Ergebnis: In den 20 Jahren vor 2004 erreichte die Schweiz nur zweimal die Top Fünf bei Weltmeisterschaften. In den 20 Jahren danach gelang dies achtmal, darunter vier Silbermedaillen[4].




**Die HSLU-Studie beweist: Nachhaltige Awareness entsteht nur durch die Kombination von Trainings und simulierten Angriffen.**

## Fazit

Die HSLU-Studie zeigt klar auf: Für Unternehmen gilt dasselbe Prinzip. Nur die laufende Wiederholung und Kombination aus normativem Training (Attitüde/Mindset) und Simulation (Verhalten) schaffen eine nachhaltige Sicherheitskultur. Wer Awareness-Kampagnen regelmässig und kombiniert durchführt, kann ähnlich beeindruckende Fortschritte erzielen wie das Schweizer Eishockey nach 2004. ■

Cyberdise Awareness AG, CH-6300 Zug
✆ +41 (0)41 511 78 10
palo.stacho@cyberdise.io
www.cyberdise-awareness.com

[1] https://www.hslu.ch/en/lucerne-university-of-applied-sciences-and-arts/research/projects/detail/?pid=6700
[2] IBM Cost of Data Breach Study 2024
[3] IBM Cost of Data Breach Study 2025
[4] https://internationalhockey.fandom.com/wiki/Swiss_National_Team