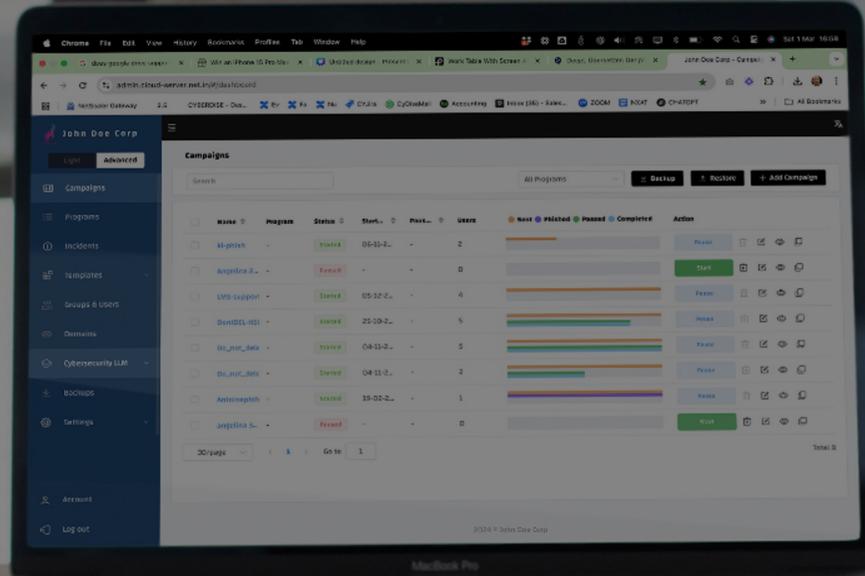


CYBERDISE

Palo Stacho, Managing Director
palo.stacho@cyberdise.io
+41793017810

**Pioneering Cybersecurity
Awareness in the Age of AI**

Was hat Awareness mit Schweizer Eishockey gemein?



Supported by:
Start-up innovation project supported by

- Schweizerische Eidgenossenschaft
- Confédération suisse
- Confederazione Svizzera
- Confederaziun svizra
- Swiss Confederation
- Innosuisse – Swiss Innovation Agency

Die Schweiz hatte schon immer ausgezeichnete Eishockey Trainer

Ralph Krueger

Trainer Schweizer Nationalmannschaft 1991—1997, 2000-2004

CYBERDISE

Doch kamen die Eidgenossen vor 2004 im weltweiten Vergleich nicht über das Mittelfeld hinaus...

1985-2004:

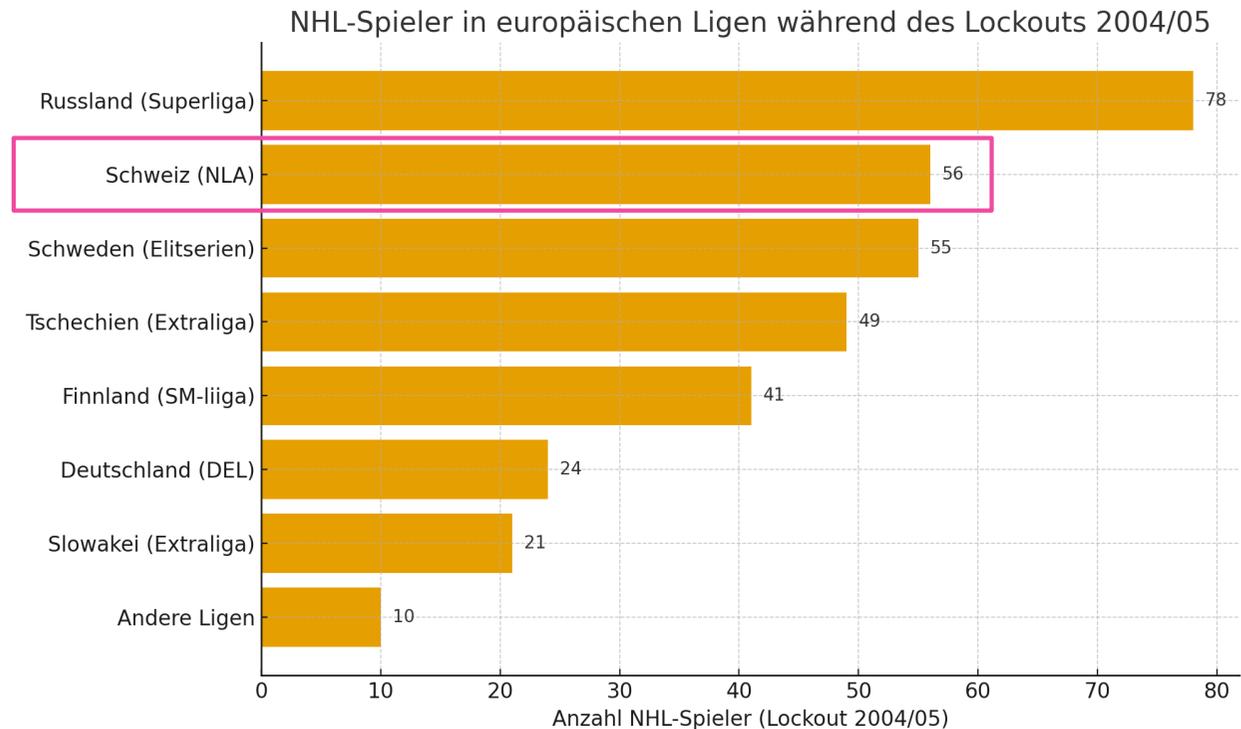
2 x in Top 5

1985: 10. Platz	1995: 12. Platz
1986: 9. Platz	1996: 14. Platz
1987: 8. Platz	1997: 15. Platz
1988: keine WM	1998: 4. Platz
1989: 12. Platz	1999: 8. Platz
1990: 9. Platz	2000: 6. Platz
1991: 7. Platz	2001: 9. Platz
1992: 4. Platz	2002: 10. Platz
1993: 10. Platz	2003: 8. Platz
1994: 13. Platz	2004: 8. Platz

WM-Rankings

CYBERDISE

Erst der NHL Lockout 2004/05 brachte den entscheidenden Schritt!



Die Kombi von Spitze-Trainern und world-class Gastspielern änderte alles!

CYBERDISE

Die Parallelen zu Cybersecurity Awareness

Die Studie: Leveraging AI-enabled spearphishing to enhance Cybersecurity

Innocheck (73275.1 INNO-ICT), [AISP](#) (AI enabled Spear Phishes)

Studienpartner

- Lucerne University of Applied Sciences and Arts
- CYBERDISE Awareness
- GLB (A Swiss medium-sized construction company)

Studienperiode November 2024 bis Juni 2025

CYBERDISE

Start-up innovation project
supported by



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation

Innosuisse – Swiss Innovation Agency

HSLU Hochschule
Luzern

AISP - Research Questions

Wird KI effektivere Cyberangriffe ermöglichen und wie sollen wir darauf reagieren? Konkret:

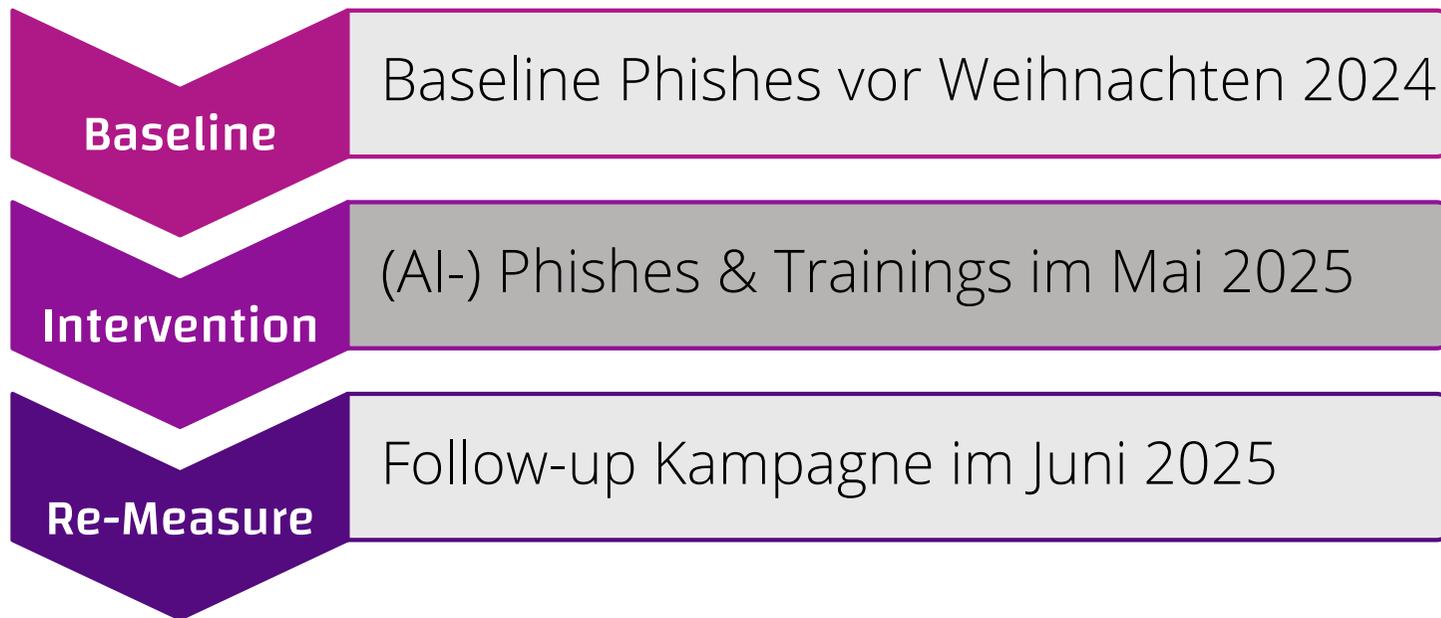
- Sind KI-gestützte Spearphishing-Angriffe im europäischen OSINT-Kontext gefährlicher als herkömmliches Phishing?
- Wie effektiv ist Risiko-Exposition im Vergleich zu normativem Training? (Sprich: angegriffen zu werden und zu wissen, dass man angegriffen wird vs. Standardausbildung zum richtigen Verhalten)?

Will AI enable more effective cyber attacks and how do we respond? Specifically:

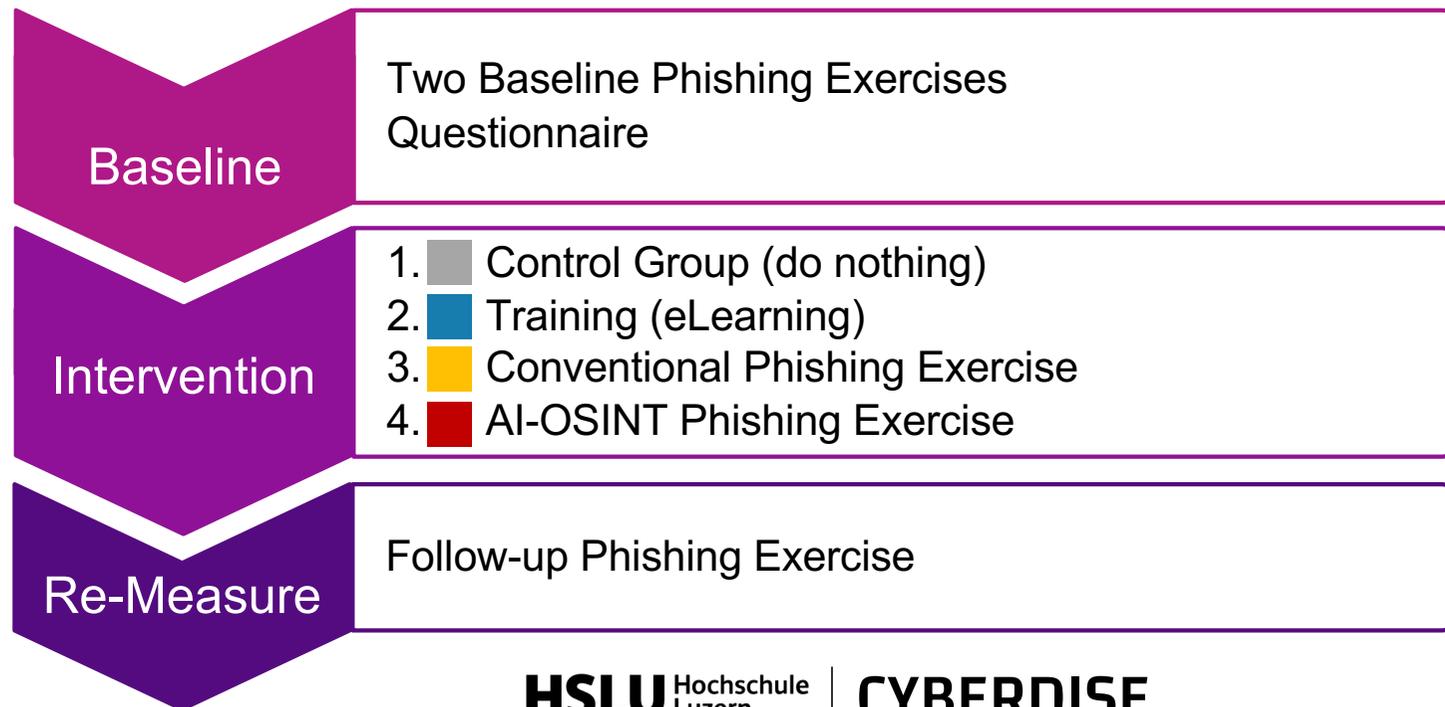
Are AI-enabled spearphishing attacks more dangerous than conventional phishing in a European OSINT context?

How effective is risk exposure (being attacked and knowing you are being attacked) vs. normative training (standard education on how to behave)?

AISP – Studienstruktur und Ablauf



AISP – Vier Kohorten in der Interventionsphase



Resultate und Erkenntnisse aus der Studie

AISP - Leveraging AI-enabled spearphishing to enhance cybersecurity

AISP – Studienresultate: Attitüde vs Verhalten

"This project allowed us to investigate the effect of different interventions to impact risk behavior and risk attitude in cybersecurity." - Dr. Carlo Pugnetti, Scientific Study Director, HSLU

Risk Behavior = actions

Beobachtbare Handlungen der Mitarbeiter im Bereich Cybersicherheit (z. B. Meldung von Phishing-E-Mails, Befolgung von Richtlinien).

Risk Attitude = mindset

Grundlegende Einstellungen gegenüber Sicherheitsrisiken (z. B. Risikobereitschaft, Bedrohungswahrnehmung, Vertrauen vs. Skepsis).

AISP – Studienresultate

Wirksamkeit von Interventionen	Wirksamkeit von ‚Attacken‘^[1]
<ul style="list-style-type: none">• Normative Schulungen reduzierten die Anfälligkeit für Phishing um ~40 %.• Die Risikoexposition (Phishing-Simulation) war besser:<ul style="list-style-type: none">• Herkömmliche Phish-Sims reduzierten riskantes Verhalten um ~45 %.• KI-/OSINT-Phish-Sims reduzierten es sogar noch stärker (≈60 %). <p>In allen Gruppen gab es Verbesserungen.</p>	<ul style="list-style-type: none">• Weniger OSINT-Daten in Europa verringern den Realismus von KI-Phishing.• Herkömmliches Phishing kann ebenso gefährlich sein, ist jedoch kostspieliger.• KI-Spearphishing ist günstiger sobald die Tools vorhanden sind, ist jedoch weniger effektiv, als US-Studien vermuten lassen.

[1] Simulated Phishing Attacks is one subtype of an intervention.

AISP – Studienresultate

Risk
Behavior

Ergebnisse zu Risikoverhalten

Gemessen durch Phishingergebnisse:

- Baseline Daten-Eingaberate 8–10%.
- Nach der Interventionsphase, Eingaberaten:
 1.  Control Gruppe 11%, keine Änderung[1].
 2.  Training Gruppe 6%.
 3.  Konventionelle Phishing Exposition 7%.
 AI/OSINT Phishing Exposition 4%.
- **Direkte Konfrontation mit Angriffen veränderte das Verhalten am stärksten,** insbesondere bei KI/OSINT-Phish-Übungen

[1] Das bedeutet, dass der Sensibilisierungseffekt nach 5 Monaten verschwunden ist.

Risk
Attitude

Ergebnisse zur Attitüde

Gemessen mit Fragebögen[2].

- **Schulungsmaßnahme:** führte zu einer signifikanten positiven Veränderung der Einstellung gegenüber dem Risikobewusstsein.
- **Phishing-Maßnahmen:** führten trotz einer Verringerung des Verhaltens zu keiner wirklichen Verbesserung der Risiko-Einstellung (Attitüde).
- **Kontrollgruppe:** leichte Besserung, statistisch nicht signifikant

[2] Fragen wie z. B. „Wir sind ein Ziel für Hacker“, „Cybersicherheit ist jedermanns Verantwortung“ usw.

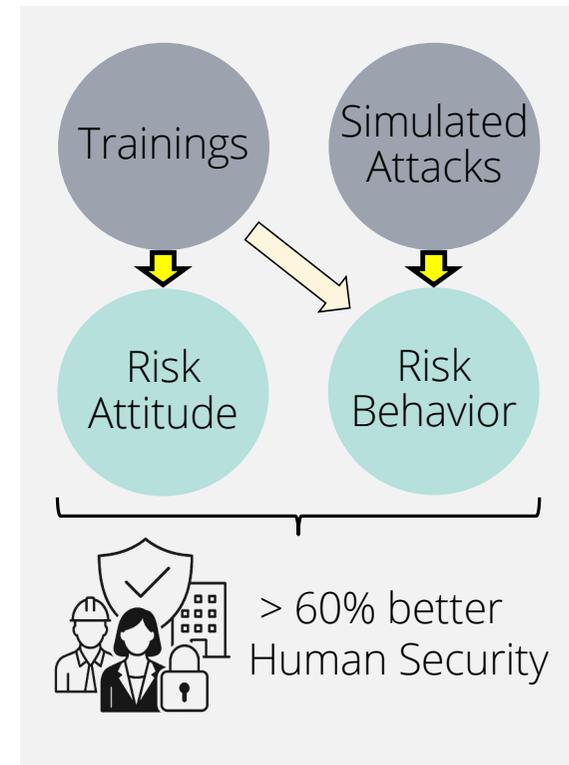
Konklusionen

aus der Studie «*AISP - Leveraging AI-enabled spearphishing to enhance cybersecurity*»

AISP-Studienresultate: AI-enabled Spear Phishing Exercises

Hauptkenntnisse

- E-Learning/CBTs eignen sich hervorragend, um die Einstellung der Menschen zum Thema Cybersicherheit zu beeinflussen.
- Exposure (Phishing-Übungen, insbesondere auf Basis von KI/OSINT) eignet sich toll, um das tatsächliche Verhalten der Menschen zu beeinflussen.
- KI-Phishing-Übungen sind am Besten, sie verbessern das Risikoverhalten um bis zu 60 %
- **Aktion & Attitüde** - Du brauchst beides: Phish-Sims und Infosec Schulungen.



Aktion & Attitüde während Lockout 2004

Trainer stärkten das Mindset, NHL-Profis das Verhalten

1985-2004:

2 x in Top 5

2005-2025:

8 x in Top 5

4 x Silber

2005 – 8. Platz	2015 – 8. Platz
2006 – 9. Platz	2016 – 11. Platz
2007 – 8. Platz	2017 – 6. Platz
2008 – 7. Platz	2018 – Silber
2009 – 9. Platz	2019 – 8. Platz
2010 – 5. Platz	2020 – kein Turnier
2011 – 9. Platz	2021 – 6. Platz
2012 – 11. Platz	2022 – 5. Platz
2013 – Silber	2023 – 5. Platz
2014 – 10. Platz	2024 – Silber
	2025 – Silber

WM-Rankings

2005-2025

CYBERDISE

Was haben wir daraus gemacht?

Produkt-Implikationen der Studie «AISP -
*Leveraging AI-enabled spearphishing to enhance
cybersecurity»*

Wir haben KI-Features gebaut

- OSINT Reconnaissance
- Educational Vulnerability Profiles
- AI Phish Generator
- Custom InfoSec-Chatbot

Sender Name: Ardian Berisha
Sender Email: aberisha@g1b.ch
Language: German
Subject: Stellenausschreibung: Fragen zu Bewerber
Source Code: WYSIWYG

Wichtige Mitteilung: Aktualisieren Sie Ihre Kontodaten dringend!
<html> <body> <p>Sehr geehrter Herr Münster,</p> <p> Aufgrund einer kürzlichen Aktua...</p> </body> </html>

Wichtige Aktualisierung Ihres Zugangskontos erforderlich
<html> <body> <p>Sehr geehrter Herr Sandhas,</p> <p>Wir haben kürzlich verdächtige Aktivit...</p> </body> </html>

Wichtige Sicherheitsüberprüfung Ihres Kontos erforderlich
<html> <body> <div style="font-family: Arial, sans-serif; line-height: 1.6;"> <p>Sehr ge...</p> </div> </html>

Wichtige Sicherheitsbenachrichtigung: Ihr Konto ist in Gefahr
<html> <body> <p>Sehr geehrter Herr Citrix,</p> <p>Wir haben verdächtige Aktivitäten in Ih...</p> </body> </html>

Wichtige Mitteilung: Überprüfung Ihrer Kontoinformationen erforderlich
<html> <body> <p>Sehr geehrte Frau Anjesa,</p> <p> Wir hoffen, dass Sie einen angene...</p> </body> </html>

Aktualisieren Sie Ihr Benutzerkonto sofort
<html> <body> <p>Sehr geehrter Herr Aemisegger,</p> <p> wir haben verdächtige Aktivitäten in Ihre...</p> </body> </html>

John Doe Corp
Light | Advanced
Campaigns
Programs
Incidents
Templates
Groups & Users
Domains
Cybersecurity LLM
Backups
Settings
Account
Log out

Osint Data
Edit Osint Data
Links
Names
Skills
Skills include Risk Analysis
Skills include Cyber Risk M
Skills include Insurance Se
Add Fact

AISP Core Team German
Overview | Users | + Collect OSINT Data
Dynamically Adding Users
Users: 5 | Modules: 1 | Rating: 1
OSINT Data Collection Status: Finished
100% Progress: 4/4
2024 © John Doe Corp

Hobbies
Hobbies include Swimming [Delete]
Hobbies include Skiing [Delete]
Hobbies include Playing strategy games [Delete]
Add Fact

Projects
Project: AI-Enabled Spearphishing Project (June 14, 2024 - December 31, 2024) [Delete]
Project: Research on Cyber Risk Behavior and Expectations towards Insurers [Delete]

CYBERDISE AWARENESS

Wo KI-Forschung auf
menschliches Verhalten
trifft

CYBERDISE



450'000+
licensed Users

6 Countries
served

220+
Templates

First
AI-native
Solution

Besuchen Sie uns am Stand
6-342 und erhalten Sie **20%**
Rabatt auf Ihren nächsten
Einkauf.



CYBERDISE

palo.stacho@cyberdise.io

+4179 301 78 10



Hier geht's zur Studie



Supported by:
Start-up innovation project
supported by

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Innosuisse – Swiss Innovation Agency