



Wie entfaltet sich ein Ransomware-Angriff?

Multimedia Lernvideo im Lernlabor Cybersicherheit – Faktor Mensch

Unser Video-Demonstrator zerstreut den Mythos, dass Cyberangriffe vom Basement-Hacker im Hoodie durchgeführt werden. Es werden sowohl der menschliche Faktor als auch das professionelle Vorgehen der Angreifenden beleuchtet, um komplexe Konzepte einem breiten Publikum zugänglich zu machen und zu zeigen, wie Angreifer Verhalten manipulieren.

Entdecken Sie die Phasen und Strukturen eines Ransomware-Angriffs auf ansprechende Weise

- **Klare, verständliche Sprache**
Technische Konzepte werden für Laien erläutert.
- **Interaktive Deep-Dives**
Optionale vertiefende Erkundung von Begriffen und Schritten.
- **Effektives Lernen**
Wissenschaftlich erwiesen: Optimale kognitive Belastung führt zu effektivem Lernen.

Was kann ich lernen?

Das Video zeigt ein realistisches Szenario, wie sich ein Ransomware-Angriff entwickelt: Vom Aufbau einer Verbindung zum Opfer über schrittweise Manipulation, dem ersten Systemzugriff bis zum Zugriff auf die ganze IT.

Wir helfen Ihnen, sich zu schützen!

Das Lernvideo bietet einen erlebnisorientierten Einstieg in unsere Schulungen zu Cybersicherheit mit dem Menschen im Fokus.



Schützen Sie sich!



<https://s.fhg.de/LernlaborCSFM>

Interaktion



Künstliche
Intelligenz



Spracheingabe
und Audio



Faktor Mensch



Physische
Interaktion



How does a ransomware attack unfold?

An Engaging Multimedia Learning Video from the Cybersecurity Training Lab – The Human Factor



Our video demonstrator dispels the myth of cyberattacks being carried out by a lone hoodie-wearing hacker in a basement. Instead, it highlights both the human factor and the highly professional methods used by attackers. By doing so, it makes complex cybersecurity concepts accessible to a broad audience and illustrates how attackers deliberately manipulate human behavior.

Discover the phases and steps of a ransomware attack in an engaging and compelling way

- **Clear, accessible language**
Technical concepts are explained in a way that is easy for non-experts to understand.
- **Interactive deep dives**
Optional in-depth explanations of key terms and particular attack steps.
- **Effective learning**
Scientifically proven: optimal cognitive load results in effective learning.

What will I learn?

The video presents a realistic scenario showing how a ransomware attack typically unfolds: from establishing initial contact with the victim, through step-by-step manipulation and gaining initial system access, all the way to full control of the entire IT infrastructure.

We empower you to protect yourself!

This learning video provides an experience-based introduction to our cybersecurity training programs, with a strong focus on people as the key factor.

Interaction



Artificial
Intelligence



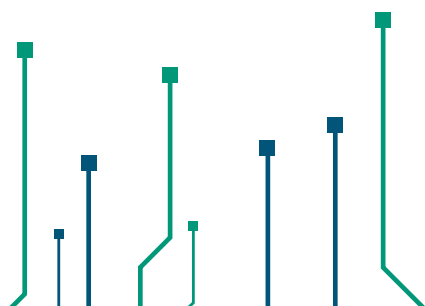
Voice input
and audio



Human Factor



Physical
Interaction





KI-gestütztes Spear-Phishing

Demonstrator im Lernlabor Cybersicherheit – Faktor Mensch



Lernlabor
Cybersicherheit
Faktor Mensch

Mit unserem Demonstrator zeigen wir, wie KI soziale Manipulationen präziser, schneller und glaubwürdiger macht und warum Unternehmen heute stärker denn je gefährdet sind. Es wird deutlich, wie Angreifer öffentlich verfügbare Informationen und KI automatisiert ausnutzen können und welche Schutzmaßnahmen tatsächlich wirken. So entsteht ein praxisnahes Verständnis für Risiken, Angriffsdynamiken und die Bedeutung robuster Sicherheitskultur.

In Sekunden von öffentlichen Daten zur perfekten Angriffsmail

- **Simulierter-Angriff**
Erleben Sie, wie KI aus öffentlichen Daten (OSINT) eine täuschend echte Spear-Phishing-Mail erstellt.
- **Konzern als Ziel**
Wir zeigen den Angriff am Beispiel bekannter Unternehmen.
- **Ihre Daten als Waffe**
Sehen Sie, wie einfach zugängliche Informationen aus Social Media und über Webseiten für Angriffe missbraucht werden.

Was kann ich lernen?

Unser Demonstrator macht verständlich, wie mit KI und OSINT der Mensch angegriffen werden kann.

Generative Modelle imitieren Sprache, Rollen und Kommunikationsstile so gut, dass selbst geschulte Mitarbeitende getäuscht werden können. Schon kleine, frei verfügbare Informationsfragmente reichen aus, um präzise Social-Engineering-Angriffe zu ermöglichen.

Wir helfen Ihnen, sich zu schützen!

Nutzen Sie das Erlebnis als Einstieg in unsere Schulungen zu Cybersicherheit mit dem Menschen im Fokus.

Schützen Sie sich!



[https://s.fhg.de/
LernlaborCSFM](https://s.fhg.de/LernlaborCSFM)

Interaktion



Künstliche
Intelligenz



Spracheingabe
und Audio



Faktor Mensch



Physische
Interaktion



AI-powered spear-phishing

Demonstrator in the Cybersecurity Training Lab – The Human Factor



Lernlabor
Cybersicherheit
Faktor Mensch

With our demonstrator, we show how Artificial Intelligence (AI) makes social engineering manipulation more precise, faster, and more convincing — and why organizations are more at risk than ever before. It exhibits how attackers can automatically exploit publicly available information using AI, and which protective measures truly make a difference. This creates a practical understanding of risks, attack dynamics, and the importance of a strong security culture.

From public data to the perfect phishing email – in seconds

■ Simulated attack

Experience how AI uses publicly available data and Open-Source Intelligence (OSINT) to generate a deceptively realistic spear phishing email.

■ Large enterprises as targets

We demonstrate the attack using well-known companies as examples.

■ Your data as a weapon

See how easily accessible information from social media and corporate websites can be misused for attacks.

What will I learn?

Our demonstrator clearly illustrates how AI and OSINT can be used to target people.

Generative models imitate language, roles, and communication styles so effectively that even well-trained employees can be deceived. Even small, freely available fragments of information are enough to enable highly targeted social engineering attacks.

We empower you to protect yourself!

Use this experience as an entry point into our cybersecurity training programs — with people at the center.

Interaction



Artificial
Intelligence



Voice input
and audio



Human Factor



Physical
Interaction



Realitätsnahe IT-Angriffe im geschützten Raum erleben

Demonstrator ELITE 2.0 im Lernlabor Cybersicherheit – Faktor Mensch

Mit ELITE 2.0 schaffen wir einen Cybersicherheits-Erlebnisort, in dem Beschäftigte in einem geschützten Raum realitätsnahe IT-Angriffe erfahren und verstehen, wie sie sich im Arbeitsalltag davor absichern können. Die Plattform richtet sich speziell an kleine und mittlere Unternehmen (KMU), für die menschliches Fehlverhalten zunehmend das größte Einfallstor für Cyberangriffe darstellt.

Im Zuge der digitalen Transformation wird die Relevanz der Informationssicherheit oft unterschätzt

- **Risikobewertung**
Risiken werden nicht erkannt oder falsch eingeschätzt.
- **Social Engineering**
Der Faktor Mensch ist heute der prominenteste Angriffsvektor (z. B. Social Engineering, Phishing).
- **Sicherheitsfaktor Mensch**
Ein starker Fokus auf rein technische Maßnahmen führt oft dazu, dass Mitarbeitende als Sicherheitsfaktor außen vor bleiben.

Was kann ich lernen?

ELITE 2.0 ist eine modular aufgebaute Demonstrator-Plattform, innerhalb derer IT-Angriffe und Schutzmaßnahmen praktisch erfahrbar gemacht werden. Dabei werden typische KMU-Arbeitsituationen simuliert. Anwenderinnen und Anwender erleben:

- Wie IT-Sicherheitsvorfälle ausgelöst werden,
- welche Folgen entstehen,
- welche Maßnahmen tatsächlich schützen,
- wie eigenes Verhalten zur Sicherheit beiträgt.

Wir helfen Ihnen, sich zu schützen!

Nutzen Sie das Erlebnis als Einstieg in unsere Schulungen zu Cybersicherheit mit dem Menschen im Fokus.



Lernlabor
Cybersicherheit
Faktor Mensch

Schützen Sie sich!



<https://s.fhg.de/LernlaborCSFM>

Interaktion



Künstliche
Intelligenz



Spracheingabe
und Audio



Faktor Mensch



Physische
Interaktion

Realistic cyberattacks, experienced safely

ELITE 2.0 Demonstrator in the Cybersecurity Training Lab – The Human Factor



With ELITE 2.0, we create an immersive cybersecurity experience space in which employees can encounter realistic IT attacks in a safe environment and learn how to protect themselves against them in their day-to-day work. The platform is specifically designed for small and medium-sized enterprises (SMEs), where human error is increasingly the largest entry point for cyberattacks.

In the course of digital transformation, the relevance of information security is often underestimated

- **Risk assessment**
Risks are not identified or are misjudged.
- **Social engineering**
The human factor is now the most prominent attack vector (e.g., social engineering, phishing).
- **People as a security factor**
A strong focus on purely technical measures often leads to employees being overlooked as a critical security factor.

What will I learn?

ELITE 2.0 is a modular demonstrator platform that makes IT attacks and protective measures tangible and experiential. Typical SME workplace scenarios are simulated. Participants experience:

- how IT security incidents are triggered,
- what consequences arise,
- which measures truly provide protection, and
- how personal behavior contributes to overall security.

We empower you to protect yourself!

Use this experience as an entry point into our cybersecurity training programs — with people at the center.

Interaction



Artificial
Intelligence



Voice input
and audio



Human Factor



Physical
Interaction



Hypebox

Interaktive Cybersicherheits-Storytelling-Plattform



Lernlabor
Cybersicherheit
Faktor Mensch

Unsere Hypebox-Demo ist eine interaktive Cybersicherheits-Storytelling-Plattform, die eine komplette Unternehmensumgebung mit allen Abteilungen nachbildet. Für jede Abteilung erleben die Teilnehmenden eine knappe, realistische Cybergeschichte, die dem typischen Arbeitskontext der Abteilung entspricht. Jede Geschichte endet mit einer klaren Erkenntnis und Hinweisen zur vertiefenden Erkundung, zum Beispiel zum Schutz vor KI-gestütztem Social Engineering oder zur empathischen Gestaltung und Kommunikation von Sicherheitsrichtlinien.

Warum es wichtig ist:

- **Zielgerichtetes Training**
Ein One-Size-Fits-All-Ansatz funktioniert nicht bei der Cybersicherheits-Bewusstseinsbildung; Bedrohungen variieren je nach Abteilung.
- **Interaktives Lernen**
Die Szenarien werden klar präsentiert, unterstützt durch Quizze und interaktive Elemente, um Engagement und Lernwirksamkeit sicherzustellen.

Was kann ich lernen?

Sie gewinnen ein Verständnis des gesamten Bedrohungsspektrums in einem Unternehmen, mit abteilungsspezifischen Implikationen vom Fertigungsbereich bis HR, Finanzen und Controlling sowie dem Vorstand. Die Hypebox zeigt, wie Cybersecurity durch nutzerorientiertes Sicherheitsdesign und effektive Sicherheitskommunikation unterstützen kann.

Wir helfen Ihnen, sich zu schützen!

Nutzen Sie das Erlebnis als Einstieg in unsere Schulungen zu Cybersicherheit mit dem Menschen im Fokus.

Schützen Sie sich!



<https://s.fhg.de/LernlaborCSFM>

Interaktion



Künstliche
Intelligenz



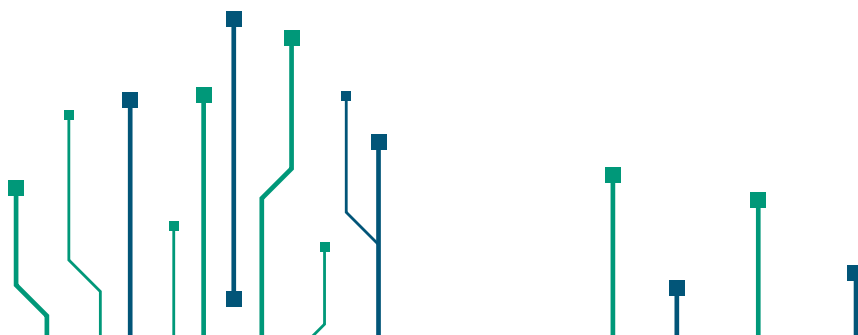
Spracheingabe
und Audio



Faktor Mensch



Physische
Interaktion





Hypebox

Interactive Cybersecurity Storytelling Platform



Lernlabor
Cybersicherheit
Faktor Mensch

Our Hypebox demonstrator is an interactive cybersecurity storytelling platform that recreates a complete corporate environment, including all departments. For each department, participants experience a concise, realistic cyber story tailored to the typical work context of that function. Each story concludes with a clear takeaway and provides guidance for deeper exploration, for example, on protecting against AI-powered social engineering or on designing and communicating security policies in an empathetic and an effective way.

Why it matters:

■ Targeted training

A one-size-fits-all approach does not work for cybersecurity awareness; threats vary significantly by department.

■ Interactive learning

Scenarios are presented clearly and supported by quizzes and interactive elements to ensure engagement and effective learning.

What will I learn?

You gain an understanding of the full spectrum of threats within an organization, with department-specific implications ranging from manufacturing to HR, finance and controlling, as well as executive management. Hypebox demonstrates how cybersecurity can be strengthened through user-centered security design and effective security communication.

We empower you to protect yourself!

Use this experience as an entry point into our cybersecurity training programs — with people at the center.

Interaction



Artificial
Intelligence



Voice input
and audio



Human Factor



Physical
Interaction

