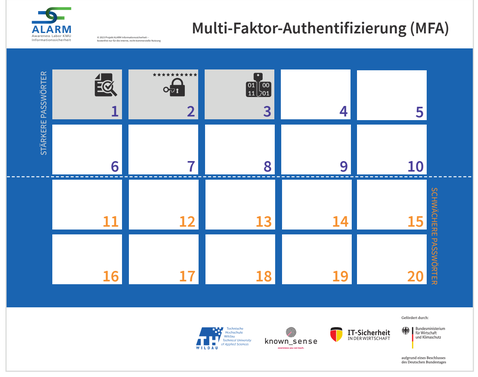
ALARM
Awareness Labor KMU
Informationssicherheit

Analoge & digitale Serious Games

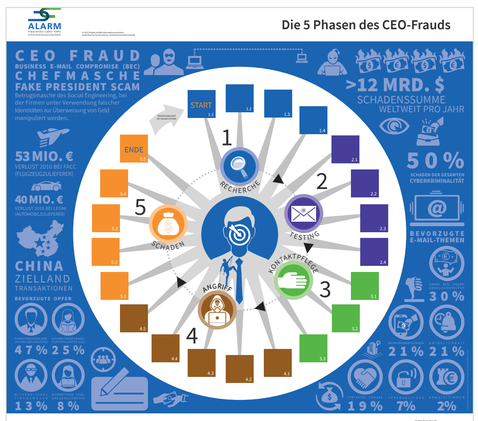
Sicher zuhause wohnen & arbeiten

Dieses Serious Game gibt einen Überblick über die wichtigsten betrieblichen und privaten Informationssicherheits- und Datenschutzrisiken in der eigenen Wohnung bzw. im eigenen Haus sowie über zugehörige Präventionsmaßnahmen, um Risiken zu minimieren.



Multi-Faktor-Authentifizierung (MFA)

Dieses Serious Game vereint Aspekte von Passwortschutz und der Multi-Faktor-Authentifizierung (MFA) und demonstriert, dass der Schutz von Informationen in einem großen Maße von einer sicheren Authentifizierung abhängt. Es zeigt, wie ein „starkes“, weil sicheres, Passwort gebildet wird und dass ein (1!) Faktor zum Schutz sehr sensibler Informationen nicht ausreichend ist.

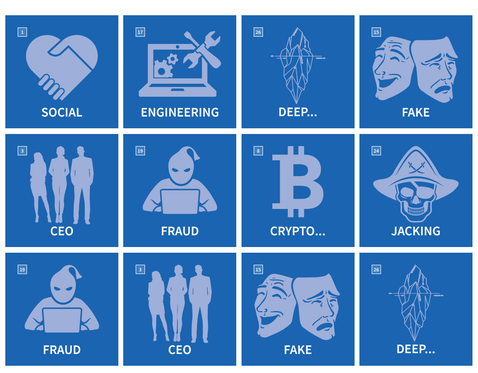


Die fünf Phasen des CEO Frauds

Dieses Serious Game gibt einen Überblick über den Gesamtprozess von CEO Fraud und über Präventionsmaßnahmen – insbesondere auch für das oft übersehene „Vorspiel“ der Vorbereitungen.

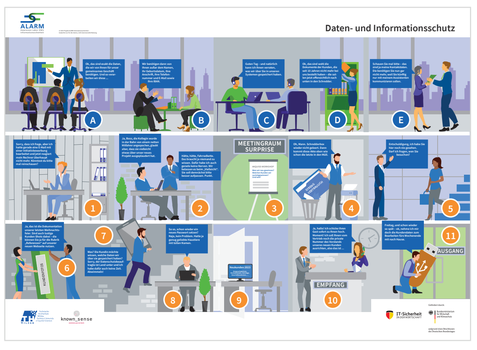
Mobile Kommunikation, Apps & Co.

Dieses Serious Game sensibilisiert in Bezug auf Risiken und Präventionsmaßnahmen, die die potenziellen Gefahren mobiler Kommunikation bzw. bei Nutzung von Apps verringern.



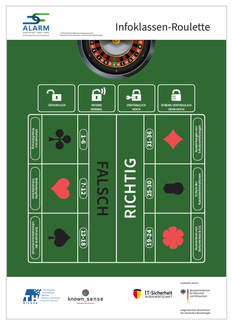
Cyber Pairs

Dieses Serious Game bricht mögliche Barrieren auf und führt zu mehr Sicherheit im Umgang mit Begriffen bzw. Bezeichnungen von gängigen bzw. neuartigen Cybercrime-Angriffen. Es unterstützt dabei, diese auch im Detail zu verstehen und in Bezug auf mögliche Präventionsmaßnahmen unterscheiden zu können – stets verbunden mit der Fragestellung, was jede/r Einzelne von uns tun kann, um Risiken zu minimieren.



Daten- und Informationsschutz

Der Schutz von Informationen und Daten von Kund/innen, Mitarbeitenden und anderen Parteien ist Teil des Geschäftes jedes Unternehmen. Dieses Serious Game unterstützt dabei, Daten- und Informationsschutz zu gewährleisten, indem der Umgang mit den wichtigsten Schutzstrategien rekapituliert und eingeübt wird.



Infoklassen-Roulette

Der Zweck von Informationsklassifizierung ist der Schutz von wertvollen Informationen jeder Organisation. Die „richtigen“ Klassen hängen von den potenziellen Auswirkungen auf Verfügbarkeit, Beschädigung oder Verlust von Informationen ab. Dieses Serious Game unterstützt beim Verständnis von Informationsklassifizierung und deren Notwendigkeit.

Der erste Tag

Social Engineering & Passwortschutz

Ziel des Spiels ist eine Einführung in das Thema Informationssicherheit anhand klassischer Situationen rund um Social Engineering und Passwortschutz, die eine hohen Identifikation für alle Spielenden bieten. Bewertet werden dabei Sicherheitsverständnis und Sozialkompetenz.

Der Hackerangriff

Social-Engineering-Methoden & -Werkzeuge

Ziel des Spiels ist es, die gängigen von Hackenden benutzten Strategien in einer reellen Situation und aus der Perspektive der Hackenden kennenzulernen und dabei spielerisch zu erleben, wie schon kleinste Sicherheitslücken ausreichen, um Hackenden den Zugriff zu erlauben. Bewertet werden dabei Effizienz und die Variabilität an Angriffswegen, die die Spielenden ausprobieren.

Die Spurensuche

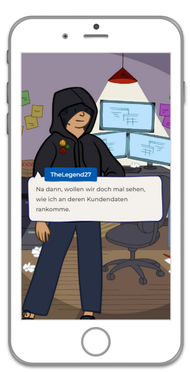
CEO-Fraud-Methoden & -Schutzmaßnahmen

Ziel des Spiels ist es, gängige Praktiken von CEO Fraud aufzudecken und wirksame Schutzmaßnahmen zu ergreifen. Eine besondere Rolle spielt bei diesem Thema die Zeit – nur wenn die Spielenden die Attacke rechtzeitig auflösen, können sie größeren Schaden verhindern. Bewertet werden dabei Effizienz, entdeckte Lerninhalte und Sozialkompetenz.

KI im Homeoffice

Schutzmaßnahmen im Homeoffice & Smarthome

Ziel des Spiels ist es, nicht einen großen Aktionserfolg zu erzielen, sondern durch kleinere Aufgaben die beliebtesten Fehler im Homeoffice zu finden. Dabei wird in praktischen und witzigen Beispielen auf die Tücken des Homeoffice aufmerksam gemacht. Bewertet werden dabei Sicherheitsbewusstsein und Machine Learning.



Alles nur geCLOUD

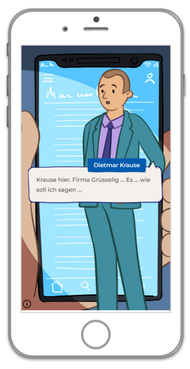
Password-Hacking-Methoden & Passwortschutz

Ziel des Spiels ist es, das Thema Datenspeicherung in der Cloud und Passwortsicherheit aus zwei verschiedenen Perspektiven zu beleuchten: des Angreifenden und des Aufklärenden. Dabei stehen jeweils unterschiedliche Aspekte der Gefährdung im Mittelpunkt und erlauben ein ganzheitliches Erleben des Themas. Bewertet werden dabei Effizienz und Gründlichkeit.

Eine Klassifizierung für sich

Info-Klassen und Verwendungszweck

Ziel des Spiels ist es, ein System zu entwickeln, wie Informationen richtig klassifiziert werden können. Dabei gibt es drei Informationskategorien, denen bestimmte Eigenschaften zugeordnet werden. Bewertet werden dabei die Fähigkeit, Kategorien zu definieren, Informationen einzuordnen, Termine zu verwalten und Fehler zu identifizieren.



Der Ransomware-Angriff

Verschlüsselung und Messenger-Dienste

Ziel des Spiels ist es, die Sicherheitslücke im Messenger zu identifizieren und unter Zeitdruck ein verschlüsseltes Passwort zu entschlüsseln, um die gefährdeten Daten zu sichern. Bewertet werden dabei Codeknacker Kompetenz und Aufmerksamkeit.