

Cyber Security Awareness Training



SOCIAL ENGINEERING

Lernen Sie in einem eindrücklichen und spielerischen Ansatz die Gefahren von Social Engineering Angriffen kennen. Lernen Sie diese zu erkennen und abzuwehren – mit unserem Cyber Risk Awareness Training.

Wir schützen das, was uns wichtig ist. Dies gilt gleichermassen für die analoge und die digitale Welt. Aber für Cyberbedrohungen haben wir noch kein ausreichendes «Gespür» entwickelt. Das Thema Social Engineering zeigt eindrücklich, dass Schutz von Informationen kein reines IT-Thema ist. Cyber-Kriminelle entwickeln dazu Angriffstechniken die mehr auf Menschen, als auf Infrastrukturen abzielen. Sie bedienen sich dabei psychologischen Manipulationstechniken, um an Informationen zu gelangen, Systeme zu kompromittieren oder Vermögenswerte zu erschleichen.

«Ich doch nicht», werden Sie nun sagen. Sind Sie sicher? Nach einer fesselnden Einführung, die zeigt wie ein hochrangiger General der Schweizer Armee gehackt wurde, werden Sie im Rahmen eines Serious-Game Angriffe auf eine Organisation durchführen und analysieren. Dabei lernen Sie, Social-Engineering zu erkennen, Angriffe zu identifizieren und abzuwehren. Denn Sicherheit in einer vernetzten Welt braucht beides: Sichere Technologien und aufmerksame Anwender.

Teil 1: Einführung Social Engineering

In der Einführung werden Sie in die Welt des Social Engineering eintauchen und Vorgehensweisen, Methoden und Werkzeuge kennen und verstehen lernen.

Teil 2: Serious Game – (k)eine Spielerei!

In dieser geführten und interaktiven Simulation schlüpfen Sie selbst in die Rolle eines Angreifers, lernen die Anfälligkeit eines Unternehmens einzuschätzen und gewinnen ein «Gespür» für Cyberbedrohungen.

Ihr Nutzen

Durch den erfahrungsbasierten und spielerischen Ansatz des Trainings wird Ihr kritisches Denken aktiviert, Sie werden sensibilisiert sowie zur Selbstreflexion angeregt. Die praxisorientierte Grundlagenvermittlung stärkt Ihr Risikobewusstsein, was zu einem besseren Verständnis von Cyber-Risiken beiträgt.

Unser Team

Philipp Leo ist Berater zahlreicher Behörden und Organisationen im In- und Ausland und ausgewiesener Experte für Cyber-Risiken und Digitalisierung.

Fabian Muhly ist Doktorand in Kriminologie und beschäftigt sich mit dem Faktor Mensch von Cyber Risiken sowie mit innovativen Methoden zur Wissensvermittlung.

Olivier Laube weiss, was Kommunikation bedeutet. Er war Kommunikationschef von McDonald's Schweiz während der BSE-Krise und stand viele Jahre selbst vor der Kamera.

Kontaktieren Sie uns jetzt!

Kontaktieren Sie uns für weitere Informationen oder gleich besser für ein unverbindliches Gespräch.

Olivier Laube

+41.79.577.78.05, laube@zwygartleadership.ch

Zwygart Leadership GmbH, 8852 Altendorf, Schweiz
www.zwygartleadership.ch