CYBER CRIME TIME

THE LEARNING JOURNEY

imc
part of Scheer

Verbessern Sie das Bewusstsein für Cyberkriminalität in Ihrer Organisation und schützen Sie sich vor Angriffen.

Ihre Mitarbeiter*innen lernen, Bedrohungen zu erkennen und praktische Maßnahmen zu ergreifen, um Ihre Organisation weniger angreifbar zu machen.

Bieten Sie eine Schulung an, die im Gedächtnis bleibt - nicht nur eine weitere langweilige Schulung, die ein paar Stunden später wieder vergessen ist.

Warum ein Training über Cyberkriminalität?

Die Gefahr von Cyberangriffen nimmt zu. Da die Welt in praktisch allen Bereichen digital wird - Arbeit, Schule, Meetings, Familientreffen - ergeben sich für Angreifer neue Möglichkeiten.

Angreifer können aus einer Vielzahl von Techniken wählen: Von einfachen Social Engineering-Betrügereien wie Phishing bis hin zu ausgefeilten Cybersecurity-Angriffen wie Ransomware-Angriffen oder anderer Malware, die darauf abzielt, geistiges Eigentum oder persönliche Daten zu stehlen. Und diese Angriffstechniken werden jeden Tag raffinierter.

Cyber Crime Time schafft ein Bewusstsein für die Gefahren von Cyber-Bedrohungen, indem es Lerner*innen in die Rolle eines Hackers versetzt. Sie lernen die gängigsten Angriffstechniken kennen, wie sie funktionieren und wie man sich vor ihnen schützen kann. Sie werden sehen, dass der beste Weg, sich vor Hackern zu schützen, darin besteht, vorübergehend selbst einer zu werden.

> ***“Cyberkriminalität ist die größte Bedrohung für jedes Unternehmen auf der Welt”.***
>
> **Virginia Rometty**
> IBMs Vorstandsvorsitzende

DAS SPIEL EPISODE #1

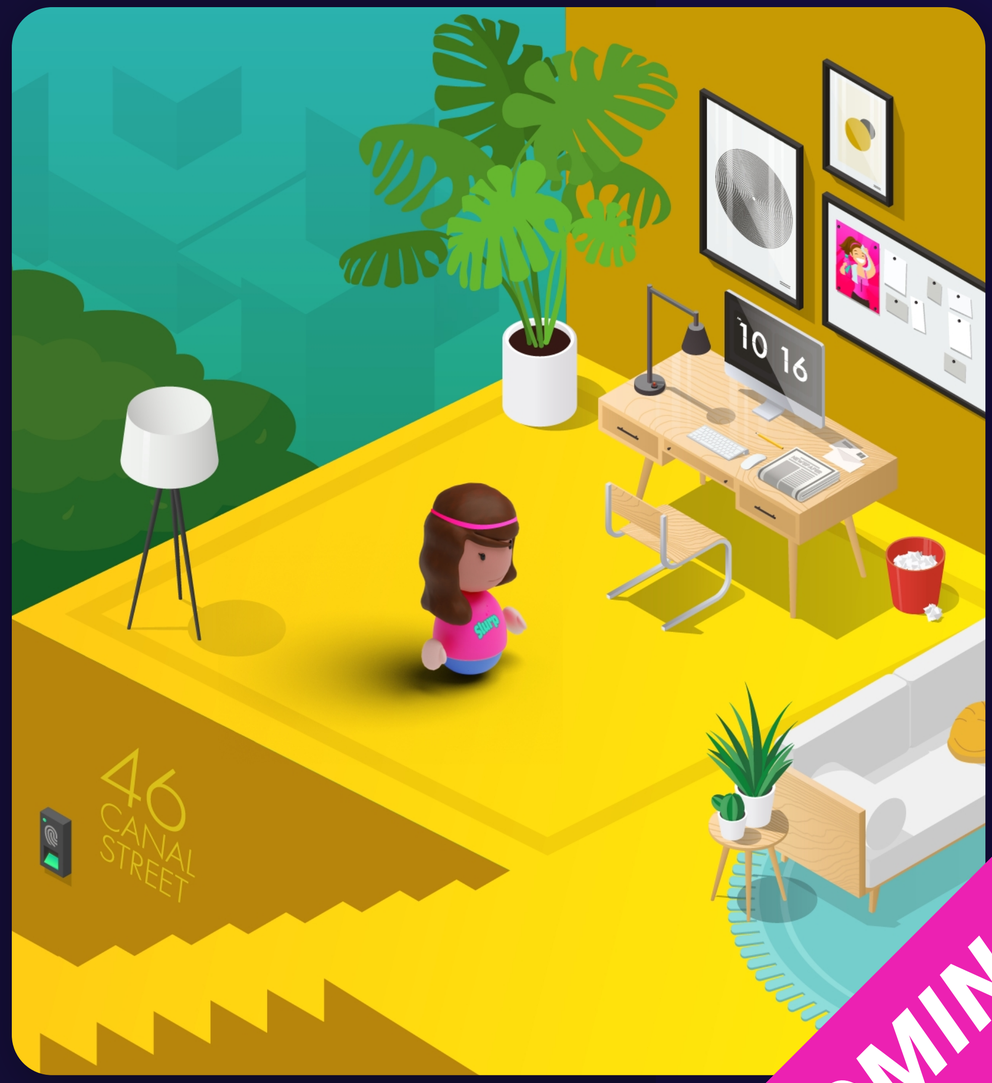
Im Spiel werden die Lerner*innen als Hacker engagiert, um Firmengeheimnisse zu stehlen. Ziel des Angriffs ist Slurp Corp, bekannt für ihren beliebten Energy Drink SLURP. Den Spieler*innen stehen verschiedene Angriffstechniken zur Verfügung, um das Rezept für SLURP zu stehlen. Im Zuge des Spiels wird erklärt, welche Arten von Cyberattacken es gibt und wie man sich davor schützen kann.

PHISHING DETECTION BOOSTER

Können Ihre Mitarbeiter*innen erkennen, ob sie Opfer eines Phishings sind? In unserem Phishing Detection Booster müssen sie für jede Nachricht entscheiden, ob sie gefälscht oder legitim ist.

WORKING FROM HOME

Der durchschnittliche Heimarbeitsplatz ist nicht so sicher wie ein Firmenbüro. „Working from home” sensibilisiert die Lernenden für die spezifischen Bedrohungen der Cybersicherheit und wie man sie vermeiden kann.



COMING SOON

READINESS CHECK

Ermitteln Sie das Wissen Ihrer Mitarbeiter*innen zur Cyberkriminalität, finden Sie Wissenslücken und geben Sie ihnen individuelles Feedback.

COMING SOON

THE MYSTERIOUS CYBERCRIME CASE

Einige Sicherheitsverstöße sind leicht aufzuspüren, aber es sind die, die unentdeckt bleiben, die am interessantesten sind. In diesem Teil der Learning Journey müssen die Lernenden einen mysteriösen Fall lösen.

COMING SOON

HOT TOPICS

Die Cybersicherheit ist ein schnelllebiger Sektor, in dem jeden Tag neue Bedrohungen auftreten. In der Reihe “Hot Topics” werden diese Trends in kurzen Videos und Content Nuggets untersucht.

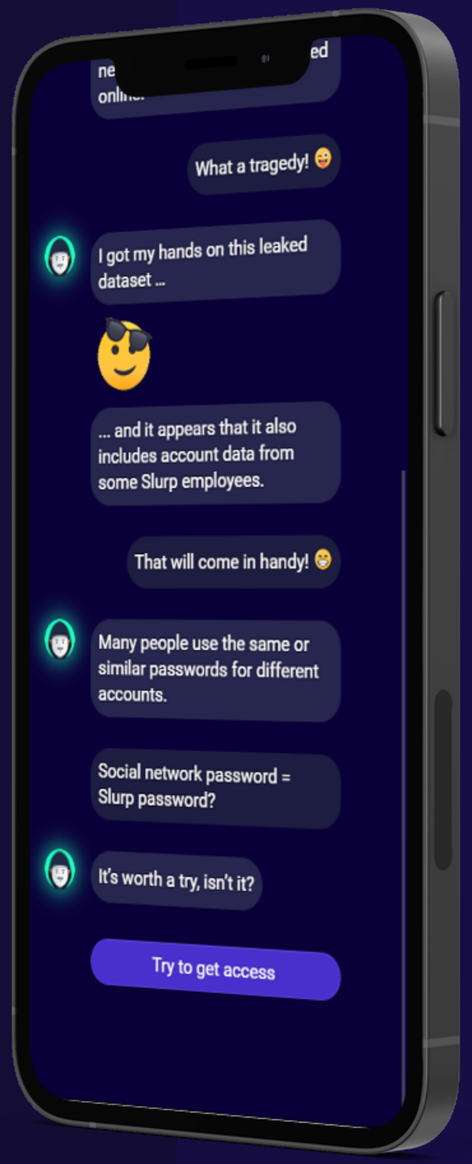
COMING SOON

Ein E-Learning, das im Gedächtnis bleibt

Cyber Crime Time ist ein unterhaltsames und spannendes Cybersecurity-Sensibilisierungstraining, das nicht wie ein Training aussieht oder sich anfühlt.

Sie wollen, dass Ihre Mitarbeiter*innen die grundlegenden Prinzipien verstehen und wissen, wie diese sich auf ihr tägliches Leben anwenden lassen? Das richtige Format ist bei der Vermittlung der Inhalte ausschlaggebend.

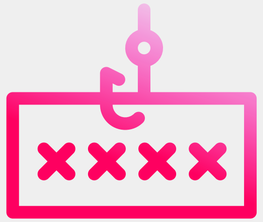
Niemand will ein Buch über Cybersicherheit lesen. Spannende Lerninhalte, die die Nutzer aktiv einbeziehen, steigern den Lernerfolg und bleiben länger im Gedächtnis. Deshalb haben wir ein E-Learning entwickelt, dass Spaß macht – nicht nur eine weitere langweilige Schulungssitzung, die man nach ein paar Stunden wieder vergessen hat. Cyber Crime Time nutzt Techniken des Spieldesigns wie Storytelling und eine spielerische Umgebung, um in das Thema einzuführen.



Die Themen

Social Engineering
Amateure hacken Systeme. Profis hacken Menschen.

Sichere Passwörter
Wie Sie mit sicheren Passwörtern Daten schützen.



Phishing
Eine gängige und wirksame Technik, um Daten zu stehlen.

Home Office
Das durchschnittliche Home Office ist nicht so sicherwie ein Firmenbüro. Wie ist das bei Ihnen?

Malware & Ransomware
Software, die Computer, mobile Geräte, Diensteoder Netzwerke schädigt oder ausnutzt.

Identity fraud
Verwendung der persönlichen Daten einer anderen Personfür einen Angriff.

Öffentliches W-LAN
Die Menschen lieben kostenloses W-LAN. Hacker auch.

Media dropping
Was würden Sie tun, wenn Sie einen fremden USB-Stick finden?

In Ihr LMS integrierbar

Cyber Crime Time kann in alle Lernmanagementsysteme (LMS) integriert werden, die SCORM 2004 oder SCORM 1.2 unterstützen. Sie haben kein LMS? Das ist kein Problem. Sie erhalten ein persönliches Konto für alle Lerner*innen, um über unser Cloud-basiertes Lernportal auf Cyber Crime Time zuzugreifen, einschließlich Zertifizierung und Reporting.

imc
part of Scheer

Rewrite the way we learn

About imc

Mehr als 20 Jahre Erfahrung, 12 internationale Standorte, 300 Mitarbeiter und über 1200 Kunden weltweit: imc ist der führende Full-Service Anbieter für digitale Trainings- und E-Learning Lösungen.

Wir machen Lernen besser – indem wir die Art und Weise, wie wir lernen, neu definieren.

Experten auf den Gebieten Technologie, E-Learning Content und Strategie arbeiten Hand in Hand, um ganzheitliche sowie maßgeschneiderte E-Learning Lösungen zu bieten, und das weltweit.

im-c.com

imc information multimedia communication AG

Hauptsitz Saarbrücken
Scheer Tower,
Uni-Campus Nord
66123 Saarbrücken
T +49 681 9476-0
info@im-c.com

imc Standorte
Deutschland (Saarbrücken, Essen, Freiburg, München)
Australien (Melbourne)
Großbritannien (London)
Niederlande (Vianen)
Österreich (Graz)
Rumänien (Sibiu)
Schweiz (Zürich)
Singapur
USA (Dover)