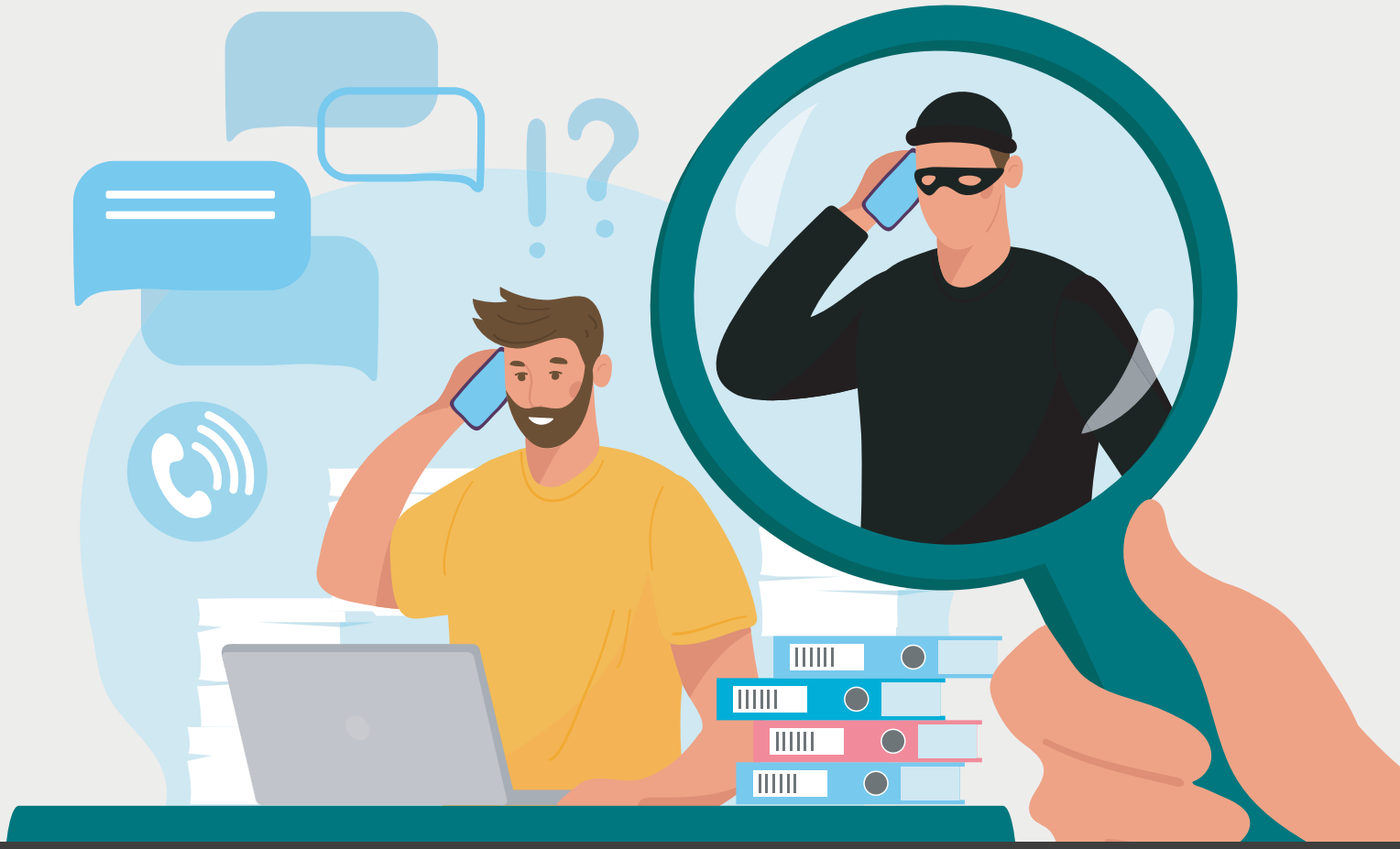
SCHÜTZEN SIE IHR UNTERNEHMEN

GEGEN SOCIAL ENGINEERING



Stärken Sie die Security Awareness Ihrer Beschäftigten

Neben Ihrer IT-Infrastruktur, stellen auch Ihre Beschäftigten ein Angriffsziel für Cyberkriminelle dar. Durch Social Engineering-Angriffe wie Phishing-E-Mails versuchen Cyberkriminelle menschliche Eigenschaften Ihrer Beschäftigten auszunutzen, um diese zu schädlichen Aktionen zu verleiten.

Das Serious Game **HATCH** ermöglicht ein unterhaltsames, interaktives Gruppentraining, bei dem Ihre Beschäftigten lernen, Social Engineering-Angriffe zu erkennen und erfolgreich abzuwehren.

HATCH

6. Deutscher IT-Sicherheitspreis 3. Preis 2016

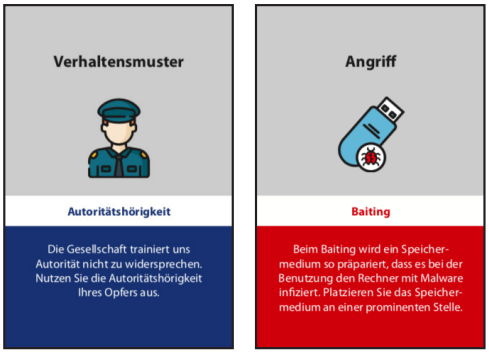
SOCIAL ENGINEERING ACADEMY

Mit Hilfe von Serious Games können Ihre Beschäftigten auf eine unterhaltsame und nachhaltige Weise in Sicherheitsaktivitäten eingebunden werden.
Nutzen Sie ein Training mit unserem physischen Kartenspiel **HATCH**, um das Bewusstsein für und das Abwehrverhalten gegen Social Engineering-Bedrohungen zu stärken.

Unsere Trainings werden ausschließlich von Cybersecurity-Experten durchgeführt.

Szenariobasiertes Training

- Simulation aktueller Angriffe
- Interaktives Training der Teilnehmenden
- Erfüllt ISO 27001 Control A.7.2.2



Unternehmensspezifische Lerninhalte

- Unternehmensspezifische Anpassung (z. B. Industriezweig) des Spielszenarios ist möglich

Bedrohungsanalyse

- Einsatz zur Bedrohungsanalyse möglich
- Identifikation und Bewertung von relevanten Social Engineering-Bedrohungen

Kontaktieren Sie uns für weitere Informationen

Telefon: +49 (0) 69 9451952 40
E-Mail: info@social-engineering.academy

Besuchen Sie auch unsere Webseite
https://www.social-engineering.academy

HATCH

6. Deutscher IT-Sicherheitspreis 3. Preis 2016

SOCIAL ENGINEERING ACADEMY