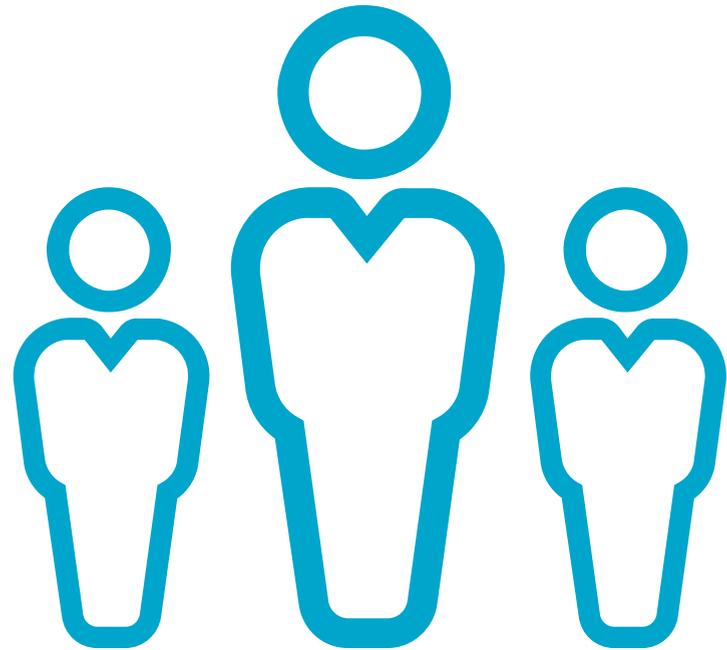


**D:BRFIN'**

SPIELEND BESSER LERNEN



# DEBRIEFING

steht für „Debriefing“ [Aussprache nach IPA: /di:'bri:fiŋ/] und meint damit das Nachbereiten, das Sammeln, Strukturieren sowie Sichern von Erfahrungen, gleich ob positiv oder negativ. Das „debriefing“ eignet sich also besonders gut zur Reflektion vergangener Situationen.

## **Der Nutzen:**

Das Bewußtsein wird geschärft und ist gewappnet für künftige Situationen mit ähnlichem Muster.

## **Unser Schlüssel für den Lernerfolg:**

Den Spieltrieb wecken! Wer spielt, entwickelt Sympathie für ein Thema, lernt leichter und handelt im entscheidenden Augenblick richtig.

## **Das Ergebnis:**

Sicherheitsvorfälle durch menschliches Fehlverhalten sinken in Unternehmen mit geschulten Mitarbeitern erheblich.

## LERNPRINZIP

### Systematischer Lernerfolg

Menschen vergessen Gelerntes mit der Zeit. Das Serious Game **D:BRFIN** setzt deshalb auf den natürlichen Spieltrieb um erlerntes aufzufrischen oder neues Wissen zu erarbeiten.

Mitarbeiter erleben kompakte Lerninhalte bequem online und in kurzen Abständen. Der Zeitaufwand bleibt gering, die Motivation durch den cleveren Gamification-Ansatz hoch.

### Der Lernerfolg überzeugt

Wichtiges bleibt dauerhaft präsent und Mitarbeiter handeln im entscheidenden Augenblick richtig.



### Registrieren

Pseudonym ausdenken, Opt-in bestätigen und direkt loslegen



### Spielen

Alltägliche Handlungen erfahren und Rätsel lösen



### Lernen

Inhalte erklären lassen und verstehen



### Motivieren

Mit anderen Spielern messen

## SPIELABLAUF

Die Spieler erleben in **D:BRFIN** den (Büro)-Alltag und müssen sich der täglichen Herausforderung stellen, kein leichtes Ziel für die Hacker abzugeben. Die Hacker versuchen Informationen abzugreifen und ihren Erfolg zu sichern.

Hierbei werden im Ansatz zentrale Themen der Informationssicherheit angesprochen.



### Spam & Phishing

Finde den Fehler: Gefälschte Emails erkennen und klassifizieren



### Sichere Passwörter

Methoden kennenlernen und anwenden



### Clean Desk & Screen

Sensible Informationen vor dem Zugriff Dritter schützen



### Malware

Typen und Wirkung kennenlernen



### Sichere Videokonferenzen

Informationen schützen und Fehlverhalten verhindern



### Social Engineering

Manipulationen identifizieren und Bewußtsein sensibilisieren

## WEB BASED TRAINING

### Zielgruppe

Personen, die in den relevanten Themen der Informationssicherheit und im Rahmen der digitalen Transformation und Kommunikation sensibilisiert werden sollen.

Personen, die im geschäftlichen Umfeld (im Büro, im Homeoffice) digitale Endgeräte und Kommunikationsmedien nutzen und sensibilisiert werden sollen.

### Schützen Sie Ihr Unternehmen

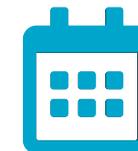
Schulen Sie Ihre Mitarbeiter proaktiv und spielerisch und stärken das Bewusstsein für den richtigen Umgang mit Informationen.



**E-Learning**



**Online durchführbar**



**Jederzeit verfügbar**



**1.5 Unterrichtseinheiten**

## IHRE VORTEILE



- ✓ **Gamification-Ansatz**  
Spielend alltägliche Bedrohungen kennenlernen und identifizieren
- ✓ **Gesteigerter Lerneffekt**  
Eigenes Erleben sorgt als emotionaler Anker für nachhaltiges Lernen

- ✓ **Teambuilding**  
Lernen in der Gruppe weckt das Interesse für Informationssicherheits-Themen
- ✓ **Mehr Sicherheit**  
Mit erhöhter Awareness sinkt die Gefahr für menschliches Fehlverhalten



**HIDDEN Awareness UG** (haftungsbeschränkt)  
0531 / 28 79 46-21  
[www.hidden-awareness.de](http://www.hidden-awareness.de)  
[kontakt@hidden-awareness.de](mailto:kontakt@hidden-awareness.de)

[www.hidden-awareness.de](http://www.hidden-awareness.de)