SECURITY PARCOURS

WIR BRINGEN SIE INS SPIEL. MIT SICHERHEIT.

Mit IT-Sicherheit spielt man nicht – oder doch?
Stärken Sie Ihre Unternehmenssicherheit.
Sensibilisieren Sie Ihre Mitarbeiter. Spielen Sie mit!

ERLEBEN, WAS VERBINDET.

DATENDIEBSTAHL, WIRTSCHAFTSSPIONAGE, SABOTAGE – ES KANN JEDEN TREFFEN
TREFFEN SIE GENÜGEND VORKEHRUNGEN?

Angriffe auf die Informationsinfrastrukturen im Cyber-Raum nehmen zahlenmäßig stark zu und werden zunehmend komplexer und professioneller. Gleichzeitig nimmt die IT-Abhängigkeit von Unternehmen und damit auch das Schadenspotenzial drastisch zu. Grundlage zur Prävention und Reaktion auf diese Angriffe ist ein verlässlicher Schutz auf allen Ebenen.

VIER MILLIARDEN GESTOHLENE DATENSÄTZE 2017 – TENDENZ STEIGEND.

Damit stieg die Zahl der gestohlenen Datensätze um rekordverdächtige 566 Prozent weltweit an. Der finanzielle Schaden beläuft sich auf 111 Mrd. Euro.[1)] Und das ist erst der Anfang.

Cyber-Angriffe mit Erpressungs-Software (Ransomware) und gezielte Angriffe auf den Angestellten, bis in die Geschäftsetagen, (CEO-Fraud) zeigen, welche Konsequenzen diese Entwicklungen haben und wie verwundbar und angreifbar eine digitale Gesellschaft sein kann. Mit immer neuen Cybercrime-Methoden attackieren Hacker die Unternehmens-IT und deren schützenswerte Assets.

Neue und komplexe Angriffsformen erhöhen das Gefährdungspotenzial für Unternehmen beträchtlich. Gerade Ransomware ist ein sehr lukratives Geschäft für kriminelle Hacker.

Rund 70 Prozent aller betroffenen Unternehmen haben beachtliche Summen an Lösegeld gezahlt, um wieder Zugang zu ihren Geschäftsdaten und -systemen zu bekommen.[2)] Oft ohne Erfolg.

EIN KLICK GENÜGT UND IHR UNTERNEHMEN IST GEHACKT.

Eine funktionierende IT-Sicherheit ist ein wichtiger Schutzfaktor, Unternehmen gegen Angriffe zu schützen. Aber – Unternehmen sollten sich nicht nur vor Attacken auf Infrastrukturen schützen, sondern müssen gleichzeitig die Resistenz ihrer eigenen Mitarbeiter gegen Angriffe stärken. Potenzielle Bedrohungen müssen rechtzeitig erkannt werden. Richtiges Handeln ist erfolgskritisch. Nachlässigkeit und Unwissenheit stellen die größten Risiken im Business-Umfeld dar. Die beste technische Firewall schützt nicht, wenn von den eigenen Mitarbeitern unbewusst Zugang, beispielsweise zu sensiblen Firmeninformationen gewährt wird.

SIND SICH IHRE MITARBEITER DIESER VERANTWORTUNG BEWUSST ?

1) Quelle: Norton Cyber Security Insights Report 2017 – SCHÄDEN BEI KUNDEN DURCH CYBER-ATTACKEN IN 2017
2) Quelle: IBM X-Force Threat Intelligence Index 2017

FÜR IHRE ABWEHRBEREITSCHAFT
VON UNSEREN SICHERHEITSPROFIS

Mitarbeiter über die Methoden und Abwehr von Datendiebstahl und Informationsangriffen aufzuklären, ist das A und O eines jeden Sicherheitskonzepts.

Großer wirtschaftlicher Schaden für das Unternehmen kann entstehen, wenn unüberlegt gehandelt wird:

- Diebstahl und unbefugte Weitergabe vertraulicher Daten
- Diebstahl von ungeschützter Hardware und hierüber Zugang zu Daten und Netzwerk
- Verbreitung von Viren, Malware oder Ransomware im Firmennetzwerk
- Systemausfälle und Beschädigung von Daten

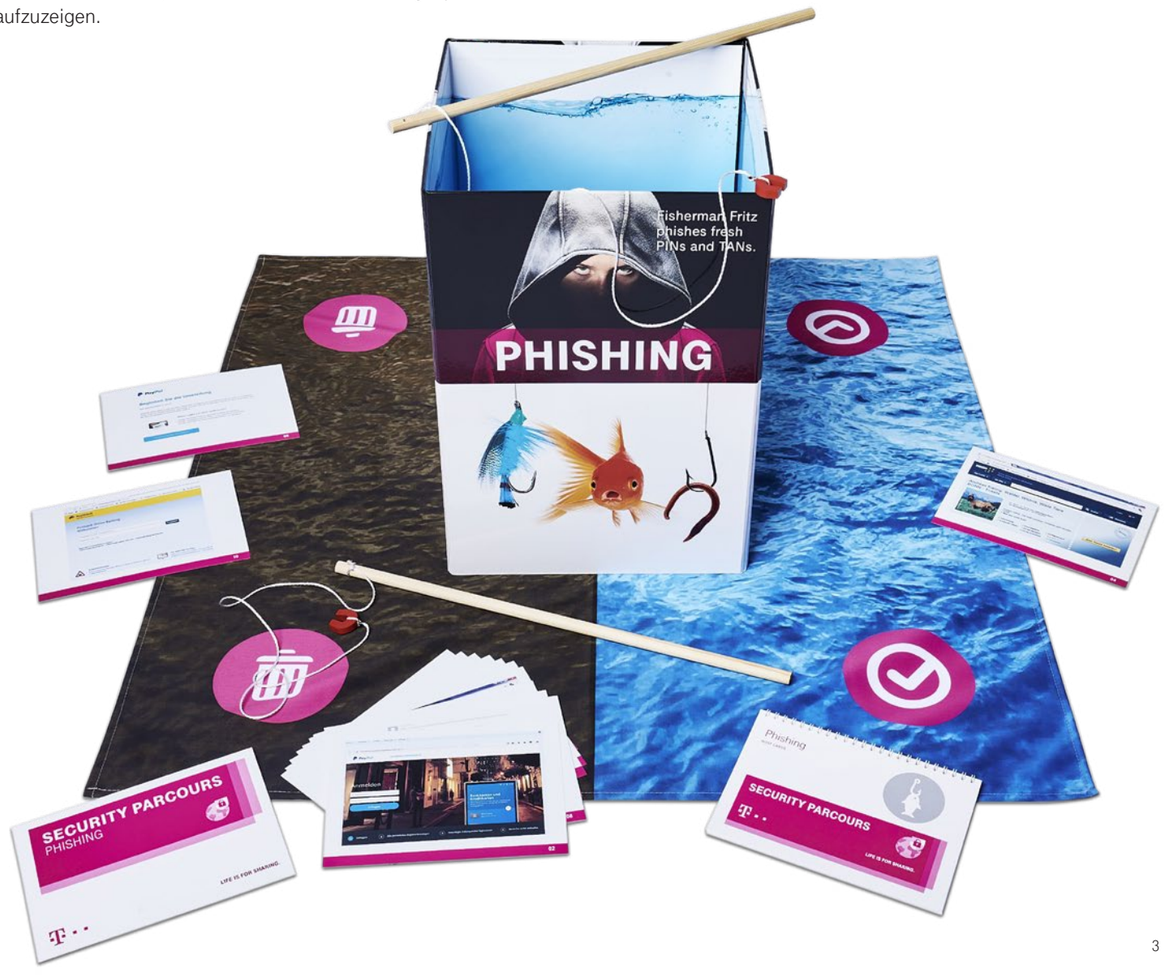
Damit Angriffe abgewehrt werden können, ist es wichtig, das Sicherheitsempfinden eines jeden einzelnen Mitarbeiters zu aktivieren und klare, einfach umsetzbare Handlungsoptionen aufzuzeigen.

LANGWEILIG WAR GESTERN.

Mit dem Security Parcours bieten wir genau das an. Spielerisch informieren und sensibilisieren ist ein attraktiver und erfolgreicher Weg, Sicherheitsbewusstsein in Unternehmen hineinzubringen.

Security Parcours bedeutet: Echte Mitarbeiterbeteiligung, hohe Motivation, gelebter Teamgeist, nachhaltige Aufklärung und Sensibilisierung.

Informieren und sensibilisieren Sie Ihre Kolleginnen und Kollegen mit dem Security Parcours ebenso spielerisch wie nachhaltig.



MEHR SICHERHEIT
IN WENIGER ALS ZWEI STUNDEN

Der Security Parcours ist ein spielerisches Training, das anhand konkreter Gefahren angemessene Verhaltensregeln vermittelt, wie sich jeder schützen kann. Ob im beruflichen oder auch privaten Umfeld, nicht erkannte Bedrohungen aus der realen und Cyber-Welt können fatale Folgen für Unternehmen und Familie haben.

Der Security Parcours bietet eine gezielte Auswahl von sicherheitsrelevanten Themen an und sorgt dafür, dass inhaltlich keine Flanke offenbleibt.

- Pro Sicherheitsthema gibt es eine Station; ein Parcours umfasst in der Durchführung in der Regel 5 Stationen
- Die Spieldauer beträgt pro Station ca. 15 Minuten
- In Teams von bis zu 10 Personen wird im Wettbewerb gegeneinander gespielt
- Es wird von Station zu Station gewechselt

Sie wollen ein bestimmtes Sicherheitsthema gezielt angehen? Manche Themen sind für sich von besonderer Wichtigkeit? Der Security Parcours lässt sich individuell nach Ihren Anforderungen zusammensetzen und durchführen.

MIT DEM SECURITY PARCOURS KÖNNEN AN NUR EINEM TAG GANZE ABTEILUNGEN SPIELERISCH TRAINIERT UND AKTIVIERT WERDEN.

WENIG AUFWAND
ÜBERALL SPIELBAR

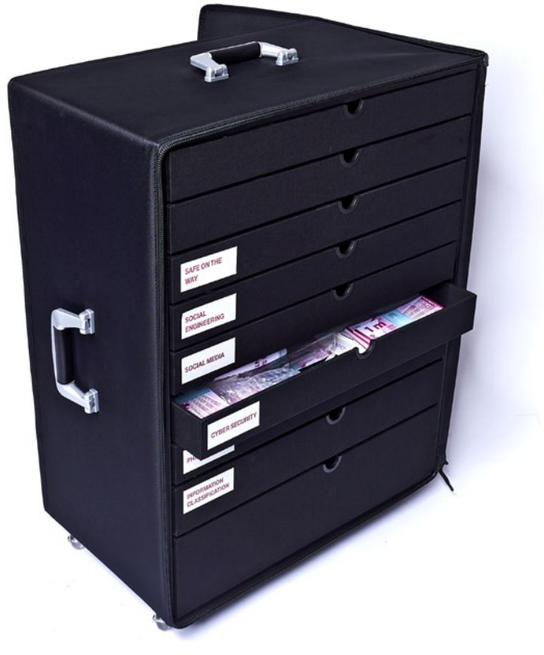
Der Security Parcours lässt sich flexibel und ortsunabhängig mit geringem Organisationsaufwand einsetzen.

ALLES EINFACH UND VERSTÄNDLICH.

Der Ablauf des Security Parcours wird von einem Moderator begleitet. Er sorgt für die Einführung in die Thematik und geht gezielt dabei auf Ihre Sicherheitsziele ein. Ein Spielleiter pro Station involviert auf unterhaltsame Art und Weise die Teilnehmer in Gespräche zu dem jeweiligen Sicherheitsthema, in dem Aufgaben gestellt werden, die es im Team zu lösen gilt.

ALLES IN EINEM KOFFER.

Der Security Parcours besteht aus einem hochwertigen Koffer. Darin enthalten sind sämtliche Materialien und Unterlagen, die nach Sicherheitsthemen sortiert sind. So lässt sich der Security Parcours bequem transportieren. Alles ist immer gut geordnet und praktisch einsetzbar.



IN EIGENER REGIE
ODER ZUSAMMEN MIT UNS

Option 1: Security Parcours buchen

SIE KÖNNEN DEN SECURITY PARCOURS GANZ EINFACH ÜBER UNS BUCHEN.

In diesem Fall übernehmen wir die Durchführung Ihres Security Parcours. Wir stimmen mit Ihnen die Auswahl der Themen und damit der Stationen ab. Ebenso können wir flexibel auf Zeiten, Räumlichkeiten und Organisationsvorstellungen eingehen. Ein erfahrenes Team aus Moderatoren übernimmt die komplette Durchführung für Sie vor Ort. Sie bestimmen die Inhalte – wir übernehmen den Rest.

Ein Security Parcours kann auch im Kontext von Security Days, Sommerfesten oder auch als Teambuilding-Maßnahme eingesetzt werden. Sprechen Sie uns an. Wir setzen den Parcours dann in den richtigen Kontext.

Option 2: Security Parcours erwerben

SIE HABEN DIE MÖGLICHKEIT, DEN SECURITY PARCOURS KOMPLETT IN EIGENER REGIE DURCHZUFÜHREN.

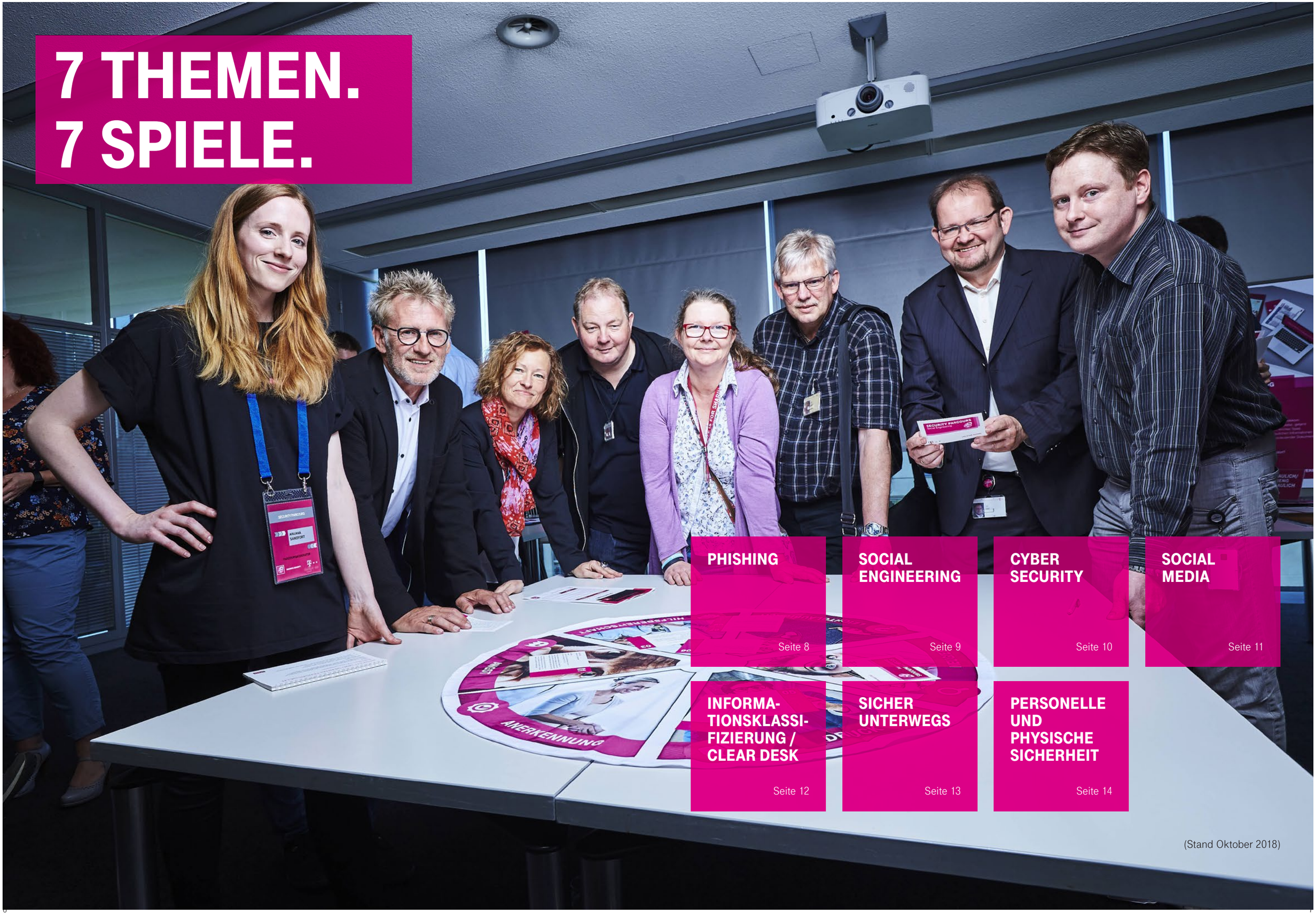
Hierzu erhalten Sie auf Lizenzbasis den Security Parcours-Koffer mit den von Ihnen gewählten Spielstationen.

Auf Wunsch können wir den Security Parcours auch nach Ihrem individuellen Firmen-Corporate Design branden. Einzelne Inhalte des Security Parcours lassen sich selbstverständlich auch auf die Bedürfnisse Ihres Unternehmens individualisieren.

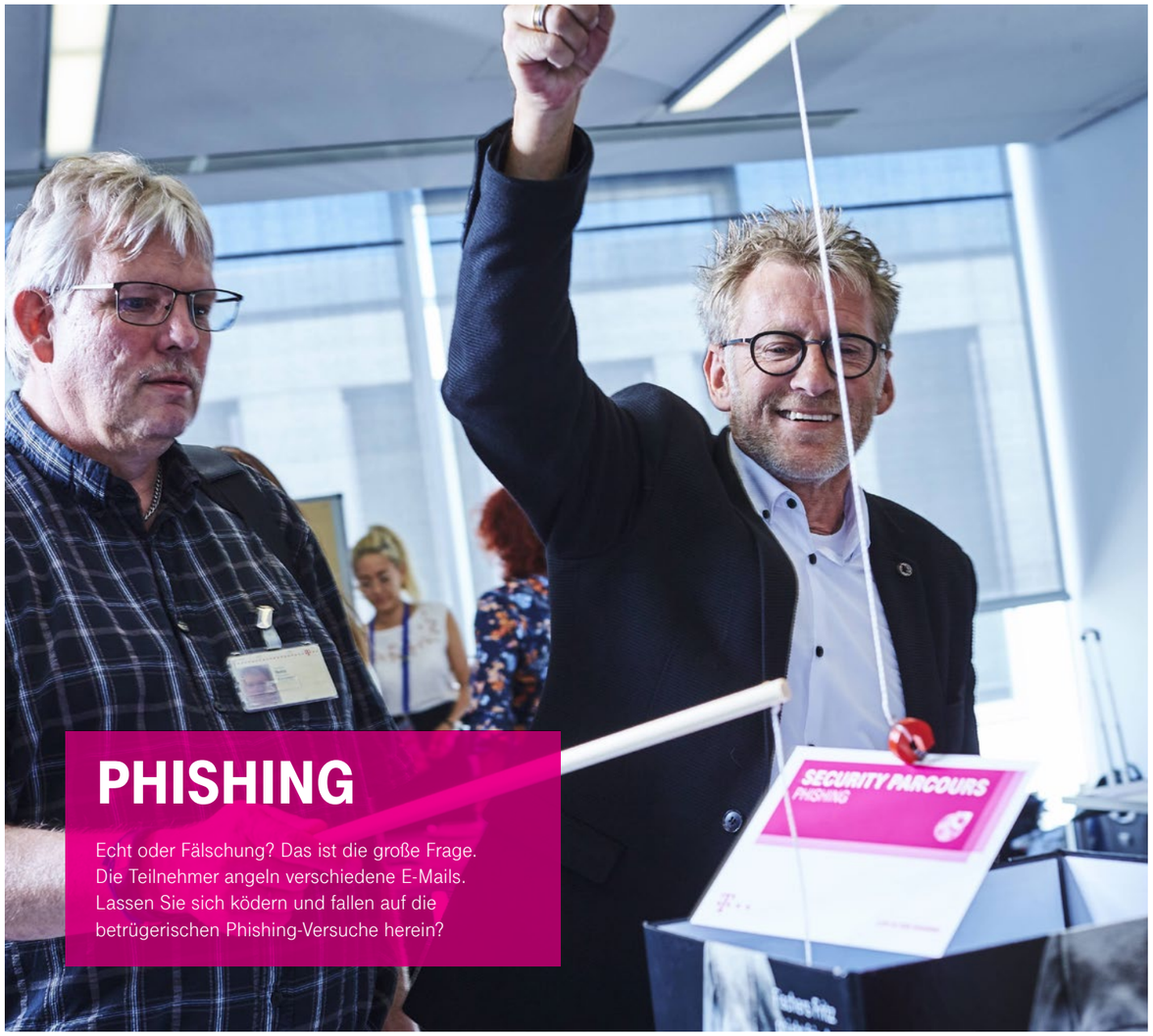
Vor dem ersten Einsatz sorgen wir mit einem ausführlichen Briefing und intensiven Training dafür, dass Ihre Moderatoren und Spielleiter sicher durch den Security Parcours führen können.

Der Security Parcours wird auch in der Zukunft um weitere Sicherheitsthemen ergänzt. Diese können Sie flexibel hinzufügen, um so immer auf dem Laufenden zu sein. Sollten Sie ein für Sie wichtiges Thema vermissen, so können wir dieses gerne individuell für Sie entwickeln und umsetzen.

7 THEMEN.
7 SPIELE.

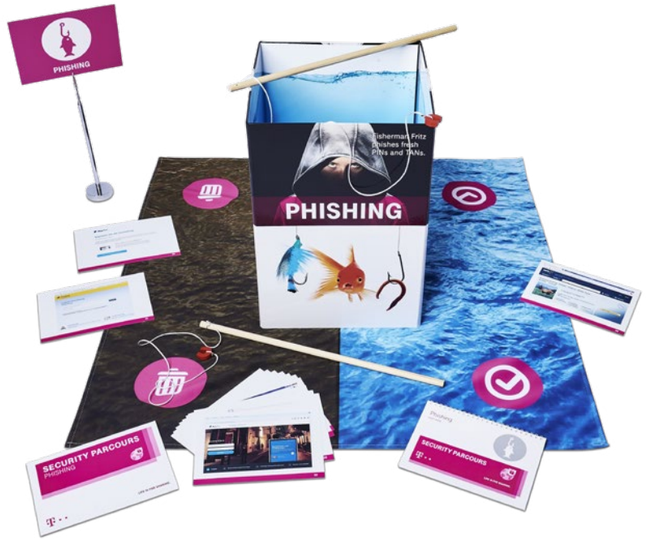


(Stand Oktober 2018)



PHISHING

Echt oder Fälschung? Das ist die große Frage. Die Teilnehmer angeln verschiedene E-Mails. Lassen Sie sich ködern und fallen auf die betrügerischen Phishing-Versuche herein?

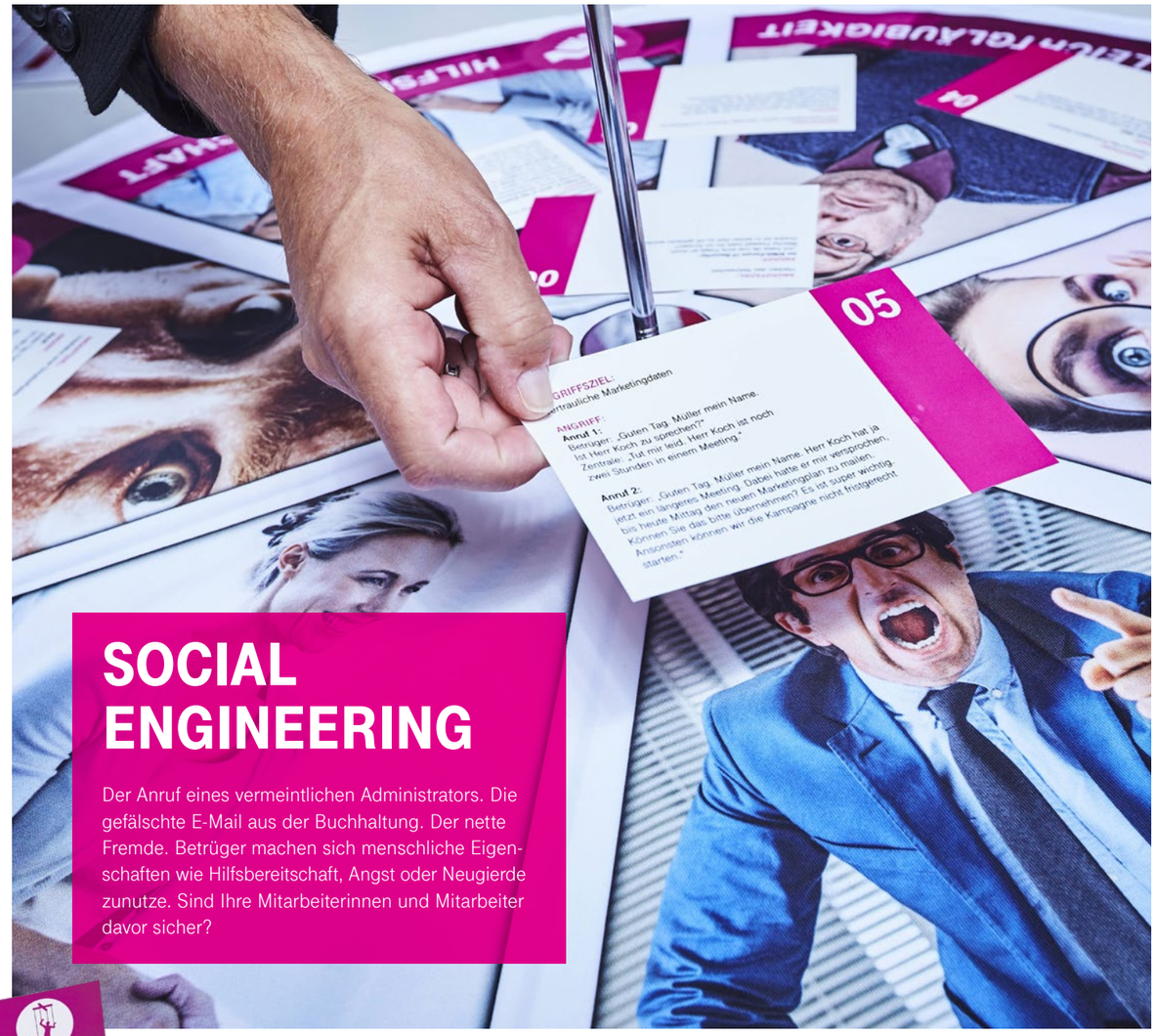


ZIEL DES SPIELS:

Die Teilnehmer lernen wichtige Merkmale zur Erkennung von Phishing-Mails kennen.

MATERIALIEN:

- 1 Spielfeld
- 1 Aufsteller aus Karton
- 2 Spielzeugangeln
- 15 Spielkarten: Phishing-Mails oder Phishing-Websites und sichere Mails bzw. Websites
- 1 Moderations-Booklet, inklusive Lösungen und Empfehlungen
- Stoppuhrapp auf dem Handy des Moderators erforderlich



SOCIAL ENGINEERING

Der Anruf eines vermeintlichen Administrators. Die gefälschte E-Mail aus der Buchhaltung. Der nette Fremde. Betrüger machen sich menschliche Eigenschaften wie Hilfsbereitschaft, Angst oder Neugierde zunutze. Sind Ihre Mitarbeiterinnen und Mitarbeiter davor sicher?

ZIEL DES SPIELS:

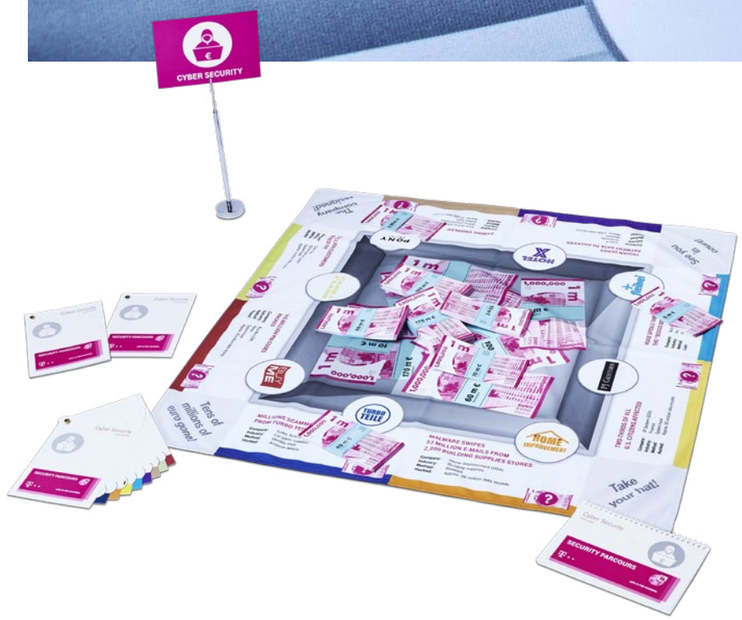
Die Teilnehmer erlangen die Erkenntnis, dass Kriminelle durch soziale Manipulation wichtige Informationen erbeuten.

MATERIALIEN:

- 1 Spielfeld
- 1 MP3-Lautsprecher (optional)
- 10 Spielkarten
- 1 Moderations-Booklet, inklusive Lösungen
- Stoppuhrapp auf dem Handy des Moderators erforderlich

CYBER SECURITY

Über 50 Milliarden Euro pro Jahr – Cybercrime kommt die deutsche Wirtschaft teuer zu stehen. Auf Basis realer Cyber-Incidents gilt es, den finanziellen Schaden von Hackerangriffen zu schätzen. Wie teuer kann ein falscher Klick für mich und mein Unternehmen werden? Das Spiel wird's zeigen.

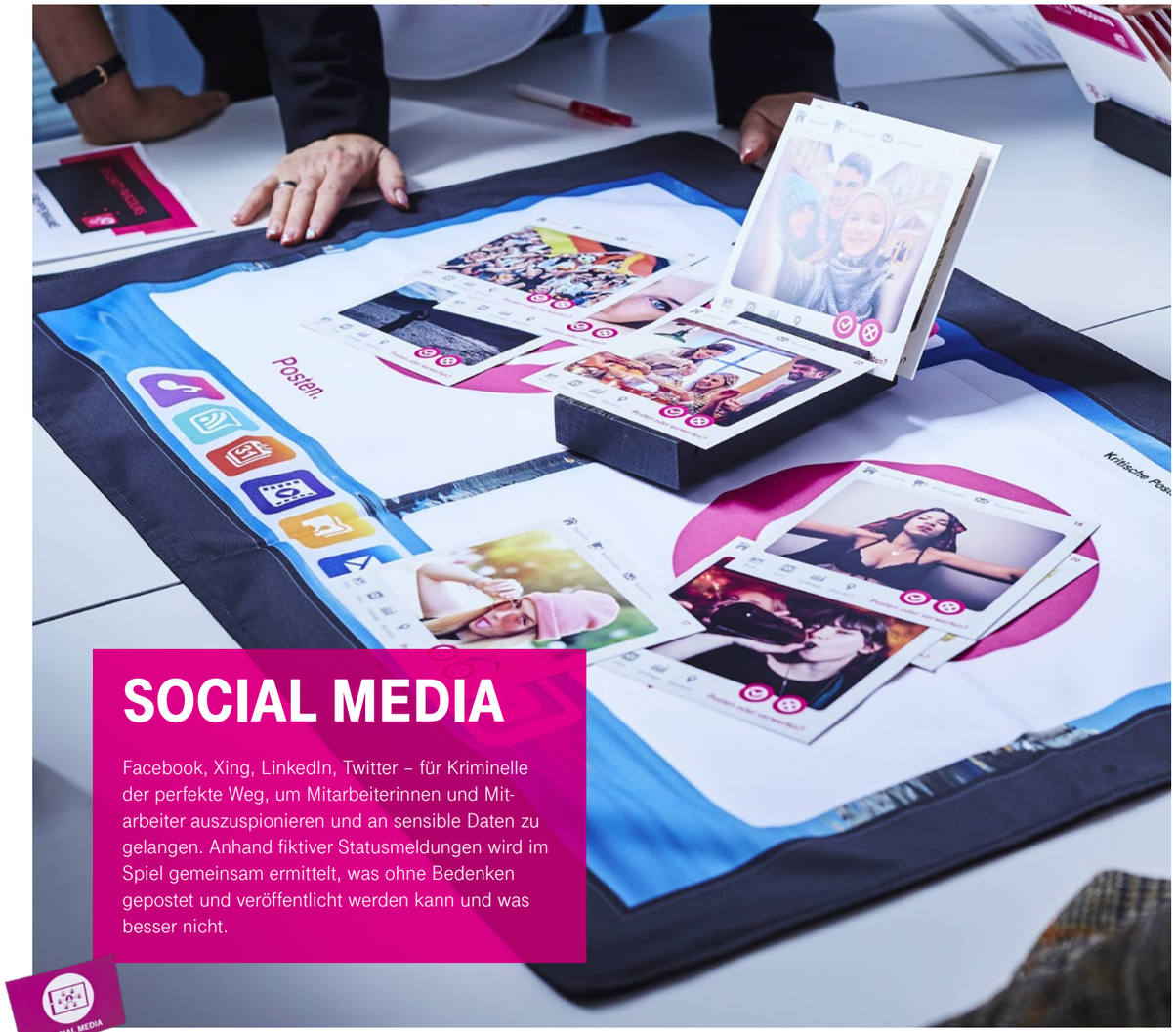


ZIEL DES SPIELS:

Den Teilnehmern wird bewusst, welche Schäden durch vermeintlich kleine Sicherheitsvorfälle entstehen können.

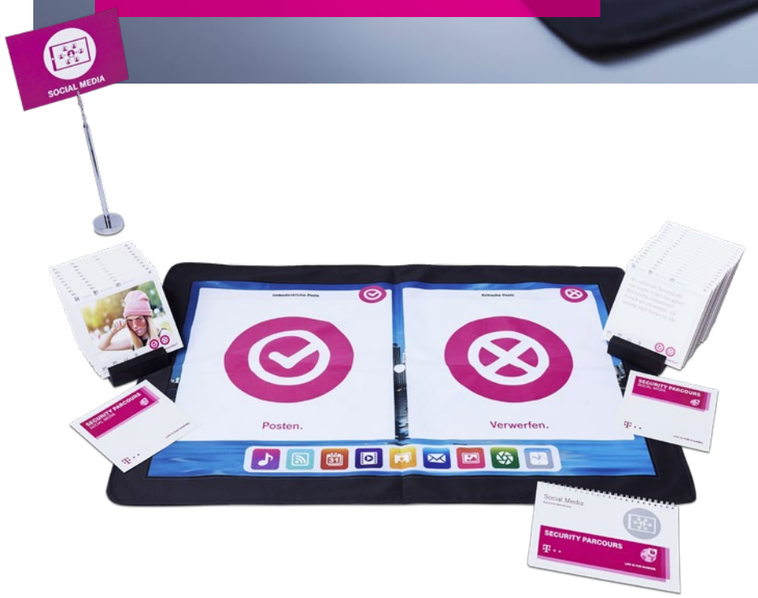
MATERIALIEN:

- 1 Spielfeld
- 10 gebundene achtseitige Booklets mit Fallbeispielen
- 8 gebundene Bündel Spielgeld
- 1 Moderations-Booklet, inklusive Lösungen und Empfehlungen
- Stoppuhrapp auf dem Handy des Moderators erforderlich



SOCIAL MEDIA

Facebook, Xing, LinkedIn, Twitter – für Kriminelle der perfekte Weg, um Mitarbeiterinnen und Mitarbeiter auszuspionieren und an sensible Daten zu gelangen. Anhand fiktiver Statusmeldungen wird im Spiel gemeinsam ermittelt, was ohne Bedenken gepostet und veröffentlicht werden kann und was besser nicht.



ZIEL DES SPIELS:

Sensibilisierung der Teilnehmer im Umgang mit sozialen Medien.

MATERIALIEN:

- 1 Spielfeld
- 2 Holzträger
- 24 Social Media-Karten
- 1 Moderations-Booklet, inklusive Lösungen und Empfehlungen
- Stoppuhrapp auf dem Handy des Moderators erforderlich

INFORMATIONS-KLASSIFIZIERUNG/ CLEAR DESK

Kundendaten, Strategiepläne, unveröffentlichte Bilanzen – das Risiko von Datendiebstahl ist allgegenwärtig. Umso wichtiger ist die Klassifizierung von Informationen (öffentlich, intern, vertraulich) und eine von sensiblen Inhalten befreite Schreibtischplatte. In diesem Spiel heißt es daher: Das Durcheinander sortieren, aufräumen und wegschließen. Gar nicht so leicht.

ZIEL DES SPIELS:

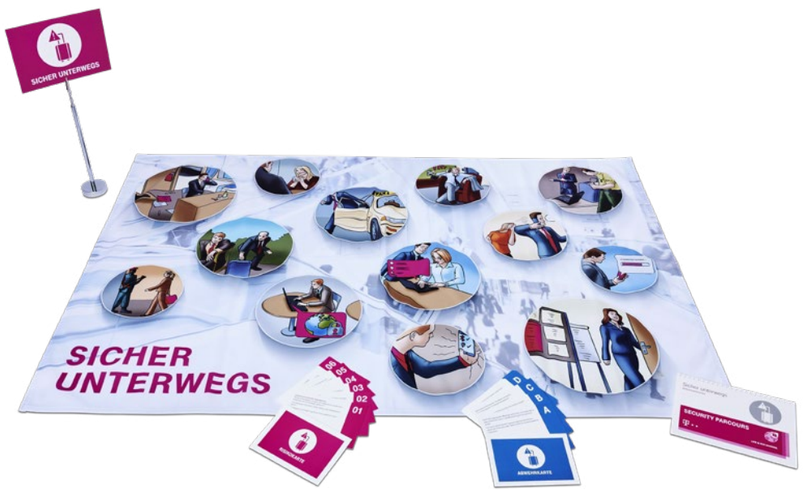
Die Teilnehmer lernen, sensible Informationen zu identifizieren und richtig damit umzugehen.

MATERIALIEN:

- 1 Spielfläche
- 3 Aufsteller für die Schutzklassen
- Zum Sortieren: 20 Dokumente, 1 Handy, 1 USB-Stick, 1 Stift, 1 Schlüsselbund
- 1 Moderations-Booklet, inklusive Lösungen und Empfehlungen
- Stoppuhrapp auf dem Handy des Moderators erforderlich

SICHER UNTERWEGS

Ausspionierte Laptops, manipulierte Smartphones, gestohlene USB-Sticks: Ein großer Teil der Angriffe erfolgt außerhalb des Firmenareals, beispielsweise am Flughafen, beim Zoll, im Hotelzimmer und vielerorts mehr. Wo lauern Risiken? Wie schütze ich meine Daten? Das Spiel lässt nichts aus.

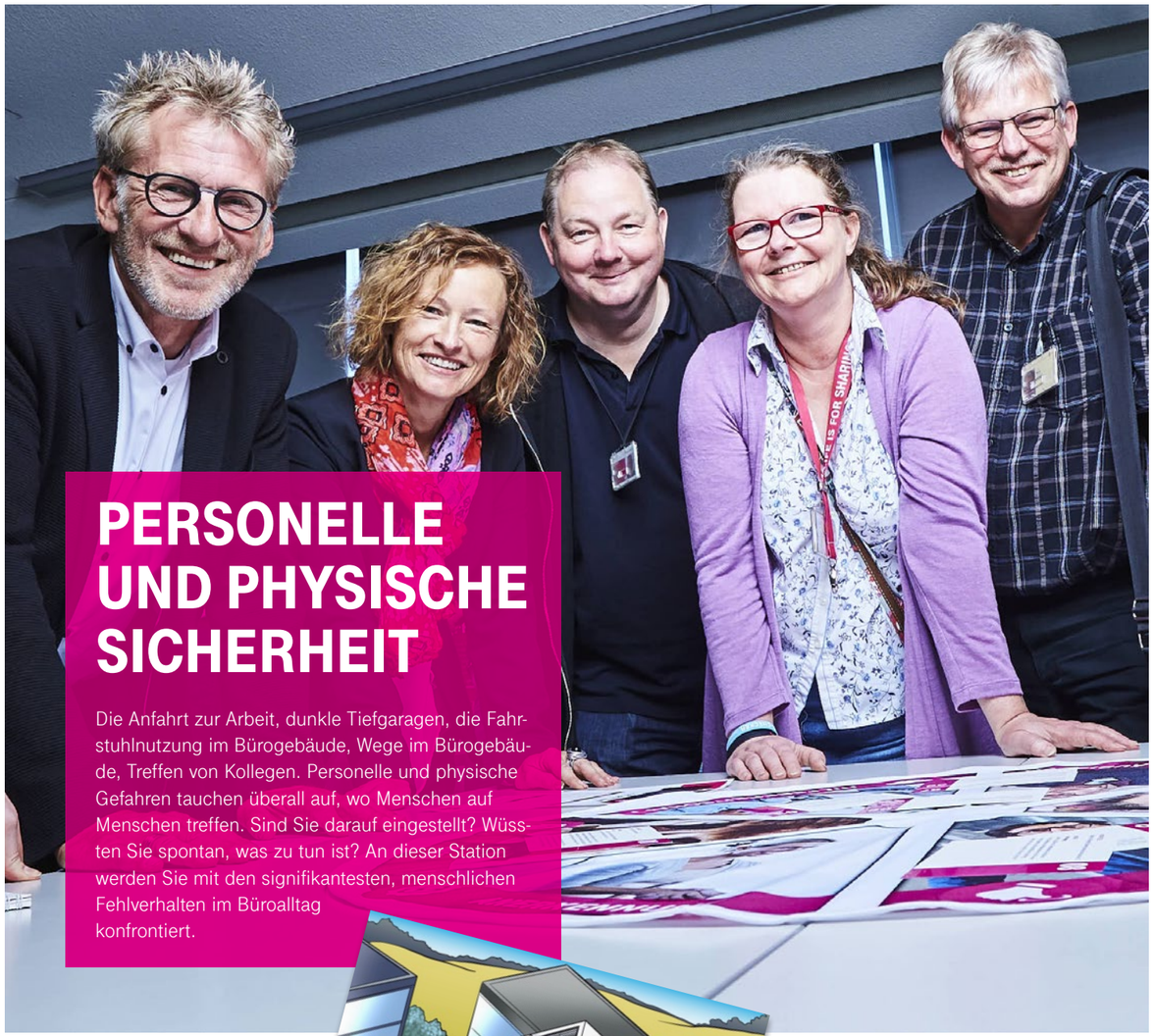


ZIEL DES SPIELS:

Nach dem Spiel wissen die Teilnehmer, warum unachtsames Arbeiten unterwegs so riskant sein kann.

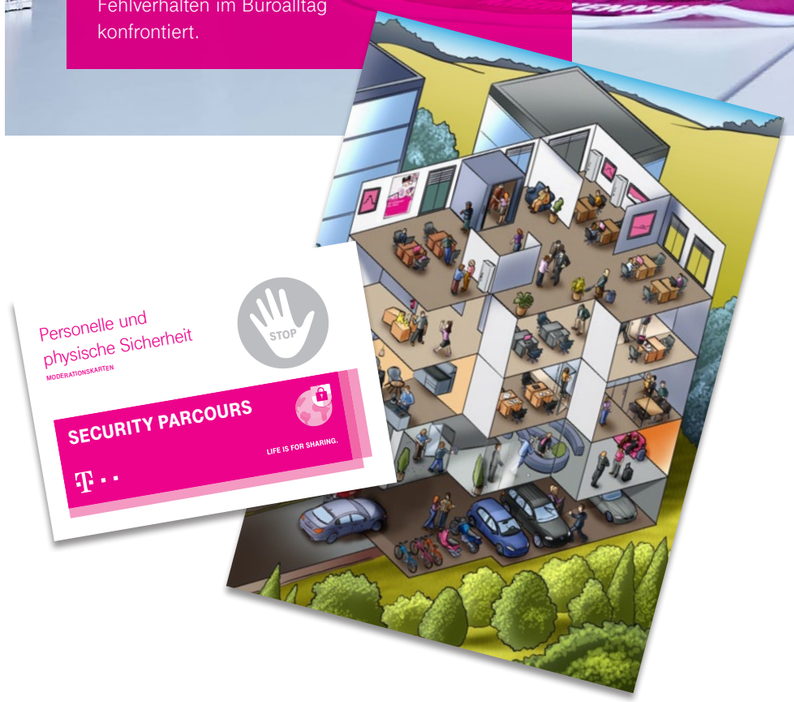
MATERIALIEN:

- 1 Spielfeld
- 13 Risikokarten
- 13 Abwehrkarten
- 1 Moderations-Booklet, inklusive Lösungen und Empfehlungen
- Stoppuhrapp auf dem Handy des Moderators erforderlich



PERSONELLE UND PHYSISCHE SICHERHEIT

Die Anfahrt zur Arbeit, dunkle Tiefgaragen, die Fahrstuhlnutzung im Bürogebäude, Wege im Bürogebäude, Treffen von Kollegen. Personelle und physische Gefahren tauchen überall auf, wo Menschen auf Menschen treffen. Sind Sie darauf eingestellt? Wüssten Sie spontan, was zu tun ist? An dieser Station werden Sie mit den signifikantesten, menschlichen Fehlverhalten im Büroalltag konfrontiert.



ZIEL DES SPIELS:

Durch aufgezeigte Fallbeispiele wird die Handlungssicherheit der Teilnehmer in Konfliktsituationen gestärkt.

MATERIALIEN:

- 1 Spielfeld
- 11 Moderationskarten
- 1 Bonuskarte
- 12 Coins
- 1 abwischbare Tafel mit passendem Stift
- 1 Moderations-Booklet, inklusive Lösungen und Empfehlungen

COMING SOON

TATORT BÜRO als Virtual Reality
PASSWORTSICHERHEIT
RISIKOMANAGEMENT

Wir arbeiten konstant an einer Ausweitung und Aktualisierung des Security Parcours.

Verpassen Sie nicht die Chance, sich und Ihre Mitarbeiter beim Thema Sicherheit immer auf den topaktuellen Stand zu bringen.

Schaffen auch Sie Sicherheit mit Nachhaltigkeit.
Und sichern Sie so den Erfolg Ihres Unternehmens.

SECURITY PARCOURS
WIR BRINGEN SIE INS SPIEL.
MIT SICHERHEIT.

Erspielen Sie sich in Ihrem Unternehmen nachhaltiges Sicherheitsdenken und -handeln.

NOCH FRAGEN?

Melden Sie sich!

Security-Parcours@t-systems.com
Telefon: +49 (0)228 181-88590

HERAUSGEBER

T-Systems International GmbH
Hahnstraße 43d
D-60528 Frankfurt am Main
www.t-systems.com

Stand: Oktober 2018

ERLEBEN, WAS VERBINDET.