



Security Awareness messbar steigern

„Dos and Don'ts“ bei Phishing-Simulationen

Dr. Niklas Hellemann
Managing Director

SoSafe: Die führende Awareness-Plattform in Deutschland.

CECONOMY

VATTENFALL 

vitra.

Netto
Marken-Discount

STADTWERKE
BOCHUM 

RÖSSMANN



 Avira

Coroplast


Köln Bonn Airport



dormakaba 

120+ Mitarbeitende

Cyber Security, Lernpsychologie,
Software-Entwicklung,
Grafikdesign, Gamification

500+ Kunden

In verschiedenen Sektoren wie
Logistik, Öffentlicher Sektor,
Automotive, KRITIS u.v.m

1.000.000+ Endnutzer

30+ Lernmodule und Videos,
500+ Phishing-Templates,
5.000+ E-Mails pro Tag

„Die spannende und moderne Aufbereitung von IT-Sicherheitsthemen hilft uns dabei, das Awareness-Level unserer Mitarbeiter zu steigern. Und durch umfangreiche und differenzierte KPIs können wir dies im Live-Betrieb überprüfen.“

Christian Schneider, CIO Vitra AG

SoSafe: Security Training, das hängen bleibt. Unsere Methode: Lernpsychologie und Spaß.



Cyber-Angriffe gefährden eine nachhaltige Digitalisierung – gerade auch im öffentlichen Sektor.

CYBERATTACKEN AUF MINISTERIEN

Umfassende Angriffe auf US-Sicherheitsapparat: Hacker haben wohl auch Atomwaffenbehörde attackiert

Datenschutz

Cyberangriff auf das Berliner Kammergericht

Malware-Befall: IT-Systeme der Stadt Frankfurt am Main offline

Security-Awareness rückt in den Fokus im Public Sector: bitkom Smart Country Convention.

bitkom



smart country

Startup Award

Winner 2020

Smart Country Startup Award: SoSafe ist das innovativste E-Government-Startup

Hacker greifen Systeme an?



Selten –
9 von 10
Cyberangriffen
Starten bei den
Mitarbeitenden.

Corona: Auch E-Mail-„Phisher“ sind sofort aufgesprungen.

Handelsblatt

IT-Sicherheit: Der perfekte Köder: Cyberkriminelle nutzen die Corona-Panik

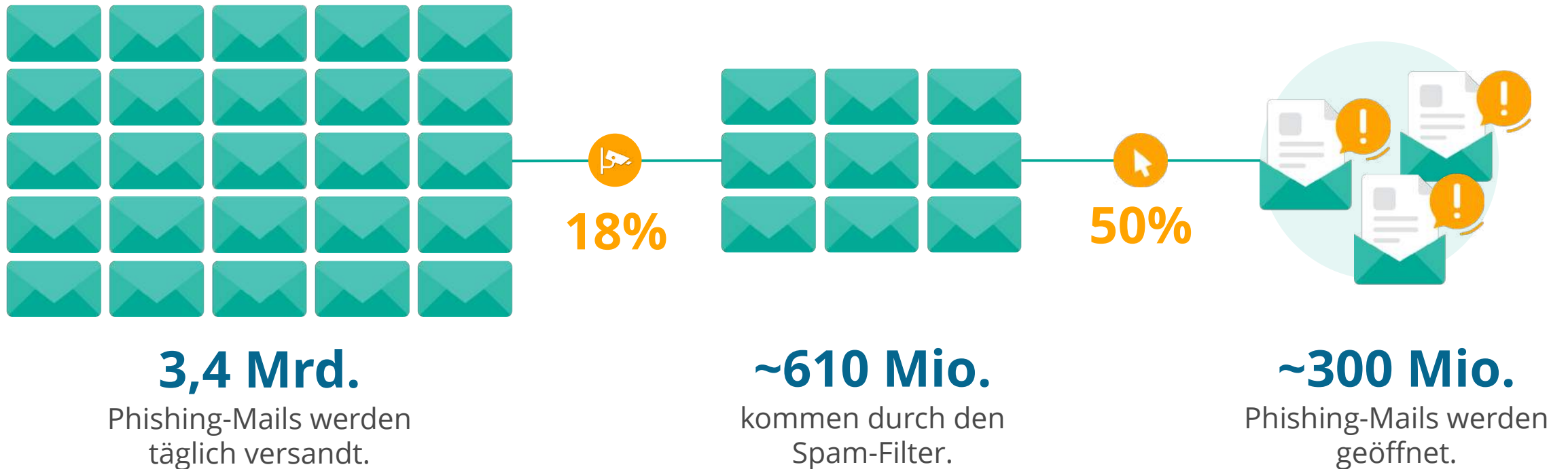
IT-Sicherheit Der perfekte Köder: Cyberkriminelle nutzen die Corona-Panik.
Die Coronavirus-Krise ist für die Angreifer besonders geeignet.



Coronavirus: How hackers are preying on fears of Covid-19



Herausforderung: Mitarbeitende sind häufig die letzte Verteidigungslinie.



Klassische Awareness-Formate sind ein guter Anfang...



Kommunikations-Kampagnen

- Gehen in der Nachrichtenflut unter
- Teilweise schwer übertragbar
- Nutzen sich schnell ab



Klassische Offline-Formate (z.B. Präsenzkurse)

- Kosten- und zeitintensiv
- Wenig flexibel
- Schwer auf alle Mitarbeiter übertragbar



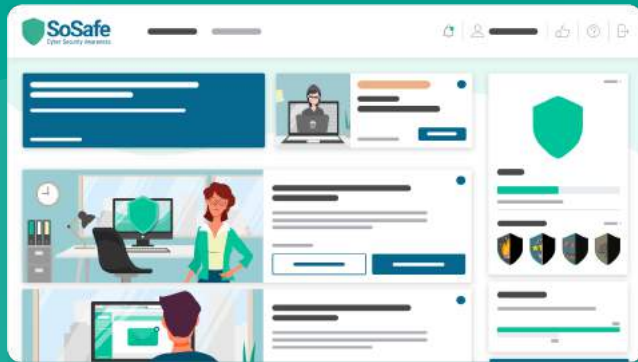
Web-Seminare

- Schlecht nachweisbar
- Teilweise sehr technisch
- Langfristiger Lerneffekt gering



Die **tagtägliche Umsetzung** von Wissen in Handeln bleibt ein Problem

Wir müssen uns aber etwas mehr ausdenken, um Verhalten nachhaltig zu verändern.



E-Learning-Plattform



Phishing-Simulation

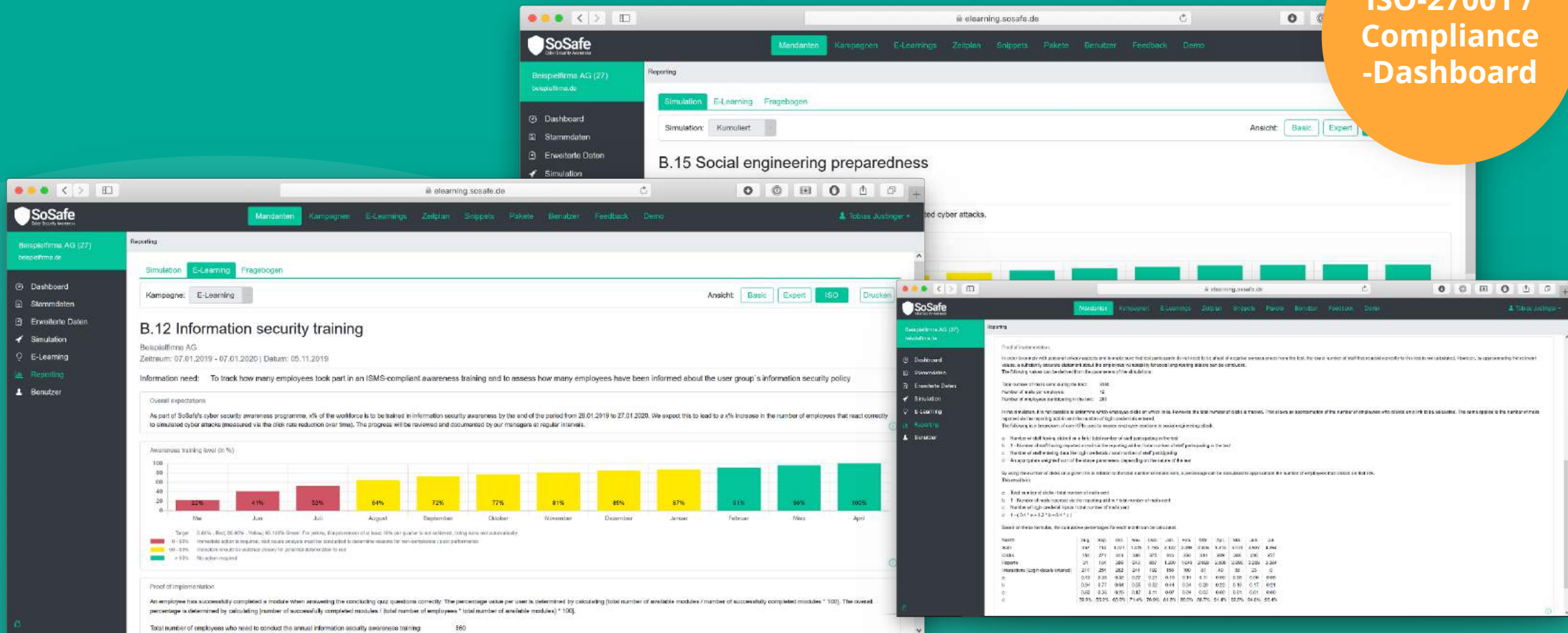


Strategisches Monitoring



Social-Engineering-Simulationen werden von verschiedenen Regulierungs-Frameworks vorgeschrieben.

ISO-27001 /
Compliance
-Dashboard



Phishing-Simulationen: „Dos and Don'ts“ – Aus unserer Erfahrung.



Mitarbeitende mitnehmen

- Vorankündigung Simulation an Mitarbeitende
- Einbindung aller Stakeholder (Mgmt., BR, IT, DSB)
- Ziel & Mehrwert Kampagne hervorheben



Überwachung im „Stealth-Modus“

- Reiner Test führt zu Widerstand
- Mehrwerte werden nicht klar
- Keine Wissensvermittlung



Dauerhafte Sensibilisierung

- Awareness muss laufend „aufgefrischt“ werden
- Vermittlung verschiedener Taktiken notwendig
- Wiederholung stärkt Lerneffekt



Einmalaktion

- Ausreichendes Wissen wird nicht vermittelt
- Geringer Awareness-Effekt: Klickraten steigen wieder an nach einiger Zeit



Sauberes Tracking

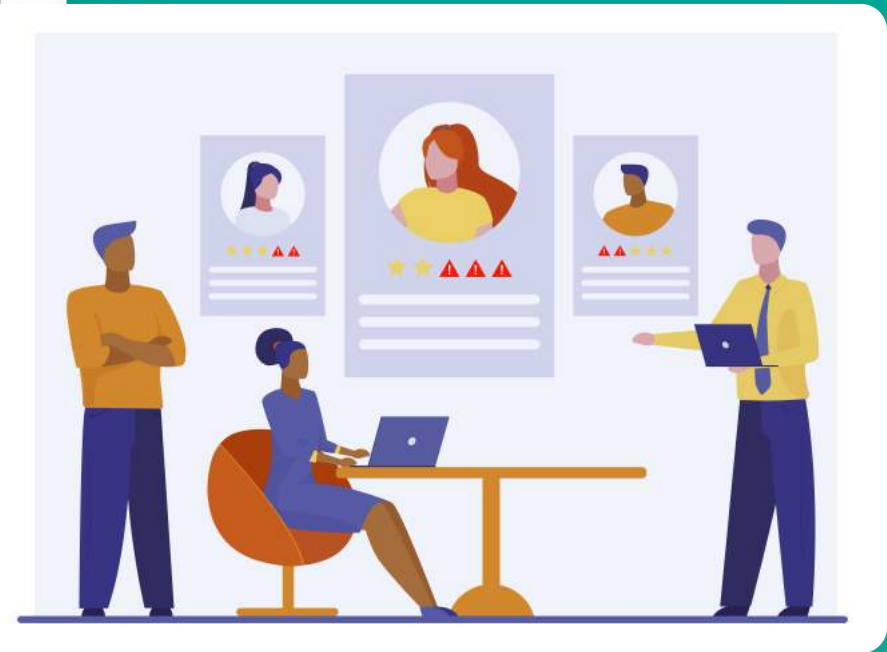
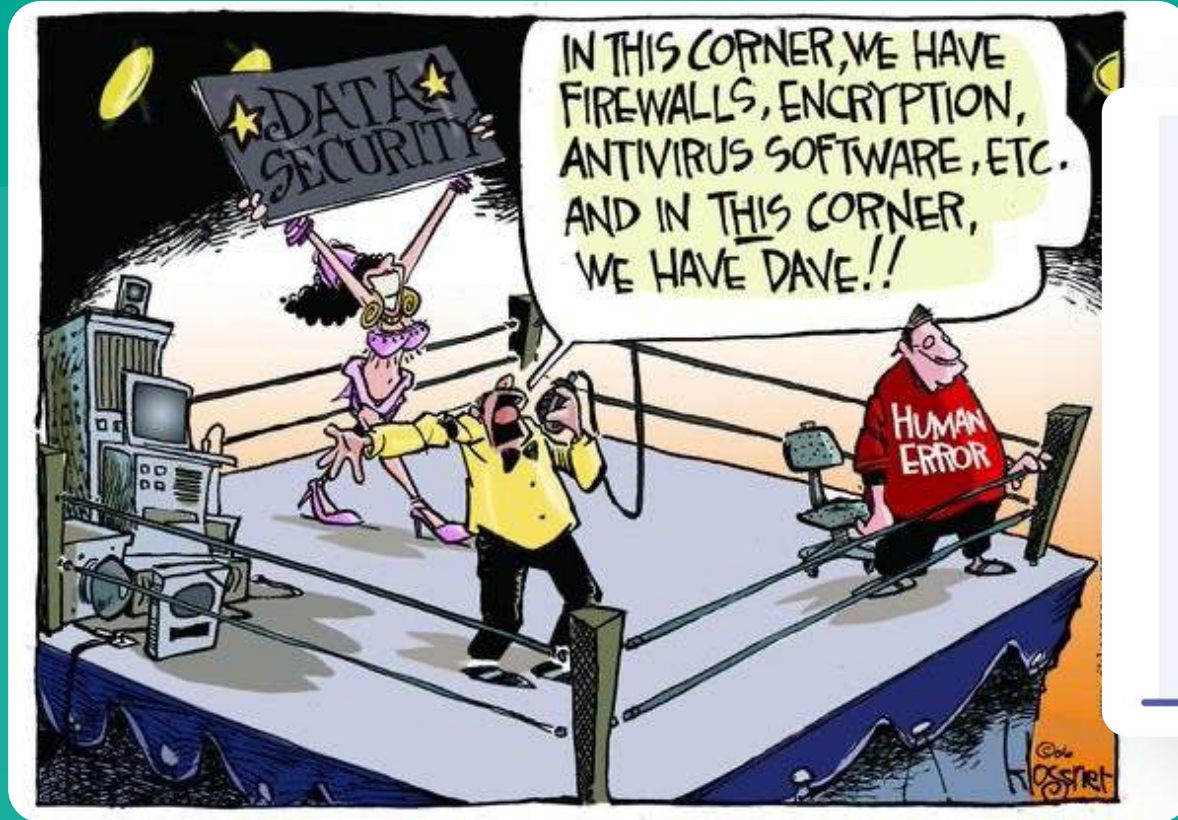
- DSGVO-Konformität beachten (US-Server/Cloud Act)
- Keine Erhebung individuellen Klickverhaltens
- Saubere Datenauswertung (inkl. relevanter KPIs)



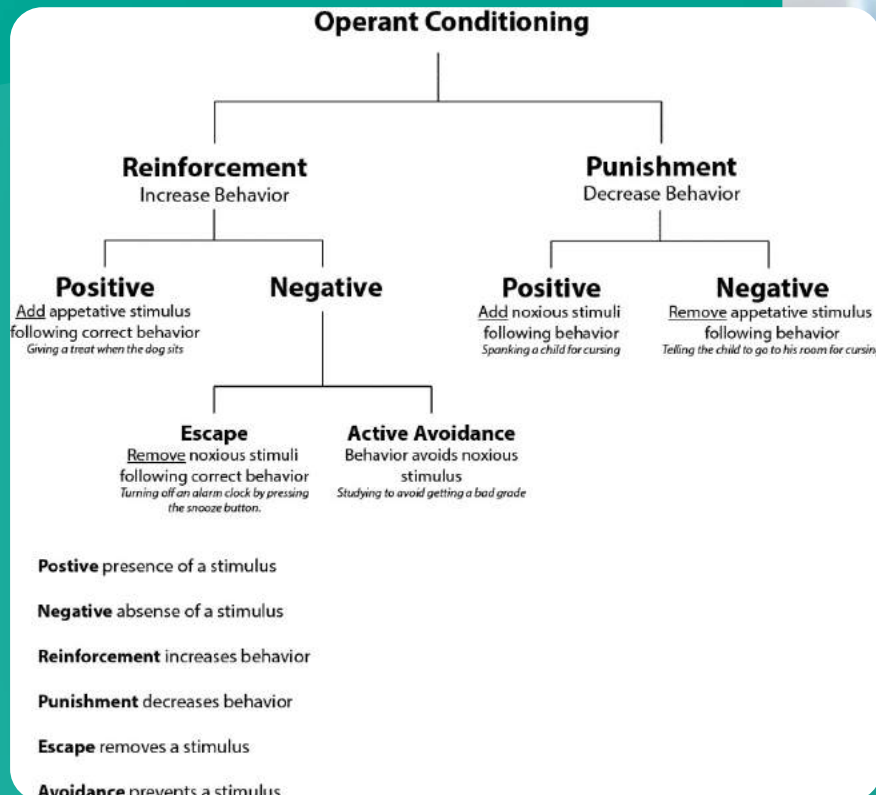
Fokus auf Mitarbeitendengruppen

- Punktuelle Tests der Organisation zeigen nicht das vollständige Bild
- Echte Hacker greifen meist an der schwächsten Stelle an – kann vom Manager bis Pförtner überall sein

Traditionell zielen Simulationen auf Mitarbeitendenbewertung – inklusive Konsequenzen.



Lernpsychologie: Bestrafung ist kein gutes Instrument.



Mit offenen Karten spielen: Vorab-Kommunikation hat zahlreiche Vorteile.

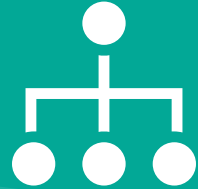
Höhere Akzeptanz /
besseres Feedback



Kein signifikanter
Effekt auf die Klickrate



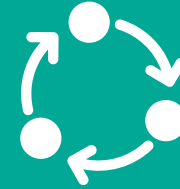
Ablauf: Dauerhafter Modus mit zahlreichen Vorteilen.



Einzelne Kampagnen

Die gleiche E-Mail wird an mehrere Mitarbeitergruppen gleichzeitig ausgespielt

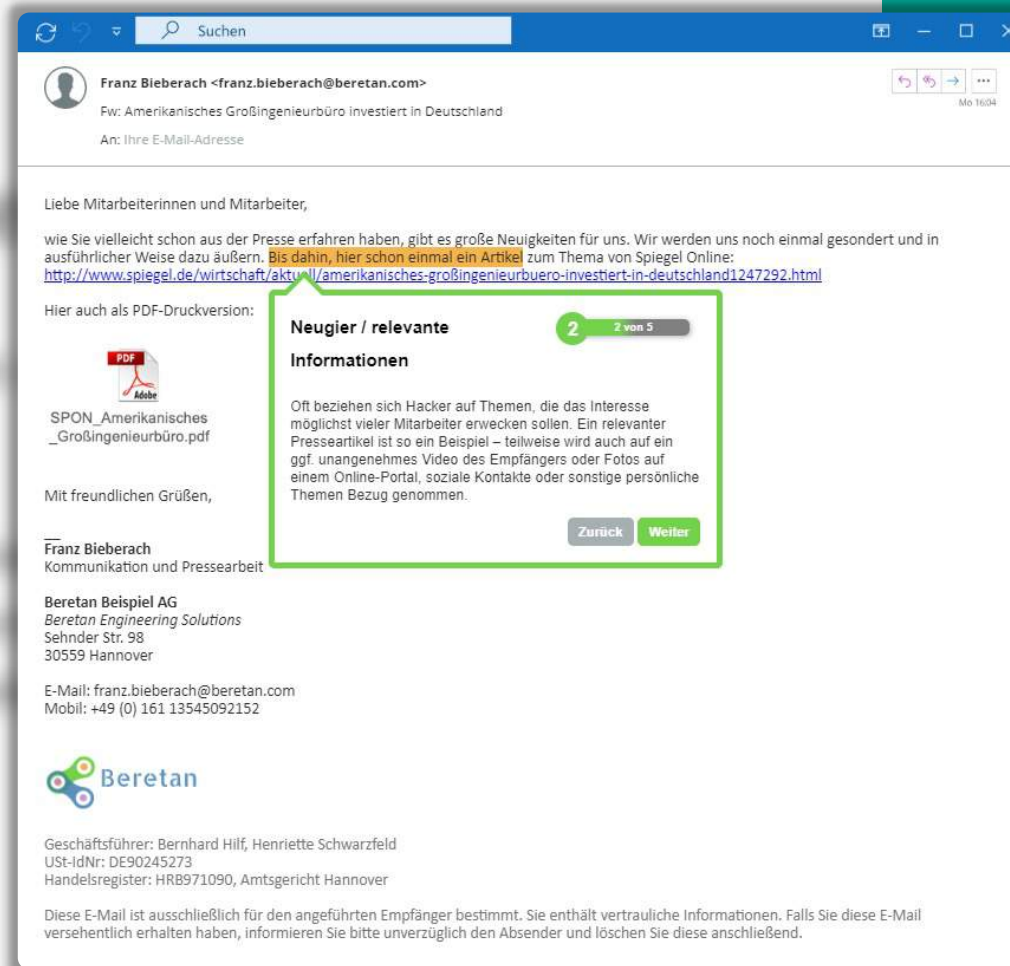
- Korrelation der Klickrate mit der Schwierigkeit der Templates
- Geballte Belastung der Organisation
- Templates sprechen sich sehr schnell herum



Dauerhafte Simulation

Verschiedene E-Mails werden laufend und randomisiert an alle Mitarbeiter ausgespielt

- + KPIs sind jederzeit live aussagekräftig
- + Optimale Verteilung der Ticketlast über die Zeit
- + Geringerer Sättigungseffekt




Suchen

Franz Bieberach <franz.bieberach@beretan.com>
Mo 16:04
Fw: Amerikanisches Großingenieurbüro investiert in Deutschland
An: Ihre E-Mail-Adresse

Liebe Mitarbeiterinnen und Mitarbeiter,

wie Sie vielleicht schon aus der Presse erfahren haben, gibt es große Neuigkeiten für uns. Wir werden uns noch einmal gesondert und in ausführlicher Weise dazu äußern. **Bis dahin, hier schon einmal ein Artikel** zum Thema von Spiegel Online: <http://www.spiegel.de/wirtschaft/aktuell/amerikanisches-großingenieurbüro-investiert-in-deutschland1247292.html>

Hier auch als PDF-Druckversion:


 SPON_Amerikanisches_Großingenieurbüro.pdf

Mit freundlichen Grüßen,

Franz Bieberach
Kommunikation und Pressearbeit

Beretan Beispiel AG
Beretan Engineering Solutions
Sehnder Str. 98
30559 Hannover

E-Mail: franz.bieberach@beretan.com
Mobil: +49 (0) 161 13545092152



Geschäftsführer: Bernhard Hilf, Henriette Schwarzfeld
USt-IdNr: DE90245273
Handelsregister: HRB971090, Amtsgericht Hannover

Diese E-Mail ist ausschließlich für den angeführten Empfänger bestimmt. Sie enthält vertrauliche Informationen. Falls Sie diese E-Mail versehentlich erhalten haben, informieren Sie bitte unverzüglich den Absender und löschen Sie diese anschließend.

Neugier / relevante Informationen 2 von 5

Oft beziehen sich Hacker auf Themen, die das Interesse möglichst vieler Mitarbeiter erwecken sollen. Ein relevanter Presseartikel ist so ein Beispiel – teilweise wird auch auf ein ggf. unangenehmes Video des Empfängers oder Fotos auf einem Online-Portal, soziale Kontakte oder sonstige persönliche Themen Bezug genommen.

Zurück Weiter

Simulationen sollten nicht überwachen, sondern schulen!

Next-Generation Teachable Moments

- Differenzierter Walkthrough
- Kurzvideos
- E-Learning-Modul

Tracking: DSGVO und Arbeitsrecht geben Rahmen vor.



DSGVO

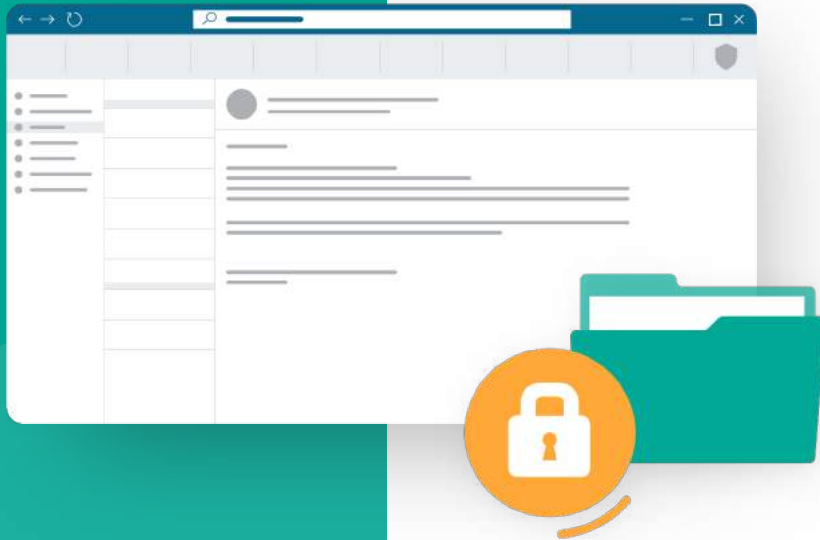


Arbeitsrecht



Betriebsrat

SoSafe gewährleistet 100% Datensicherheit und DSGVO-Konformität.



Made in Germany

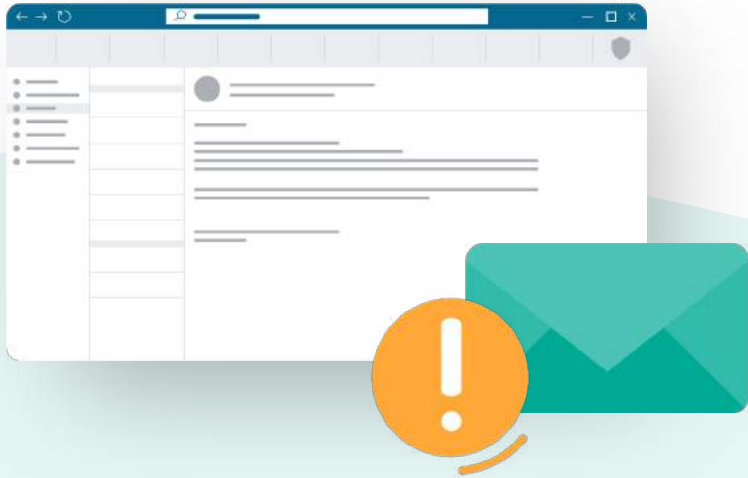
SoSafe speichert und verarbeitet Daten ausschließlich auf EU-Servern.



ISO-zertifizierte Partner

Alle Dienstleister, mit denen SoSafe zusammenarbeitet, sind DSGVO-konform und nach ISO 27001 zertifiziert.

Variation: Mail-Templates sollten systematisch erstellt...



Zusätzliche Differenzierung nach:

- Funktion der Empfänger
- Schwierigkeitsgrad
- Sprache

1

Psychologische Mechanismen

Druck, Gier, Vertrauen, Anerkennung, Angst, Lob/Schmeicheln, Flirt, Neugier

2

Technische Vektoren

Verschiedene Login-Masken, Anhänge, Malware

3

Identitätsdiebstahl

Adress-Spoofing, echte Absender-Domain

4

Motive

Geld, Datensätze, Geschäftsgeheimnisse, persönliche Motive

5

Kontexte

Beruflich, Hobby, Privat, Öffentlich

...und ausgewertet werden.

Klickrate nach psychologischer Taktik (in %)



SoSafe
Cyber Security Awareness

Beispielfirma AG
beispielfirma.de

Reporting

Simulation E-Learning

Simulation: Kumuliert

Simulation: Kumuliert

Beispielfirma AG
Zeitraum: 19.11.2018 - 19.11.2019 | Datum

Versandrate (3.360 / 3.360)
100%

Interaktionsrate (78 / 99)
78,8%

Antwortrate (161 / 3.360)
4,8%

Melderate (1.315 / 3.360)
39,1%

Generell können die Ergebnisse zu Beginn alarmierend sein.



~29 %

Durchschnittliche
Klickrate

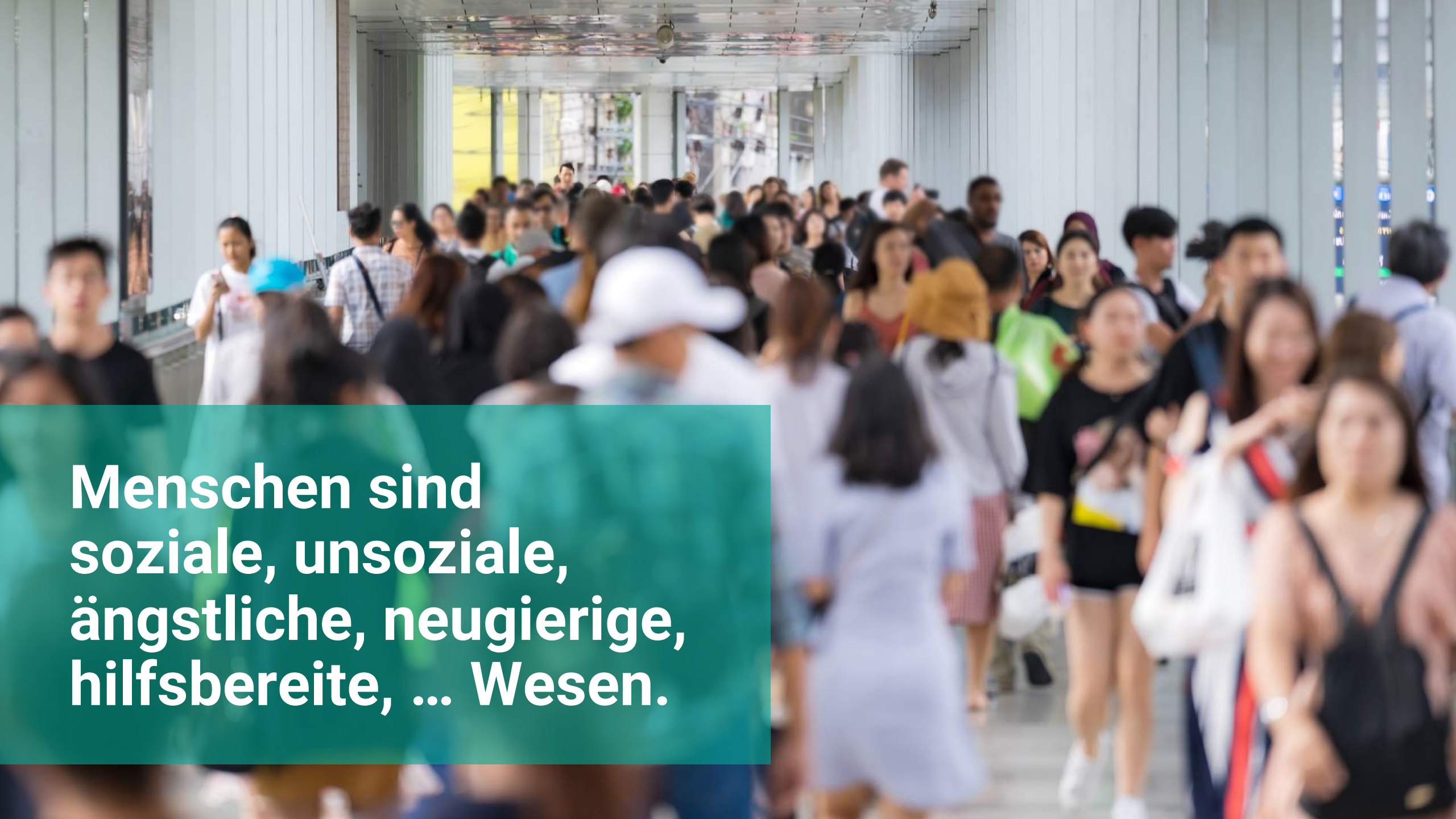


74 %

Eingaben auf
Fake-Login-
Seiten

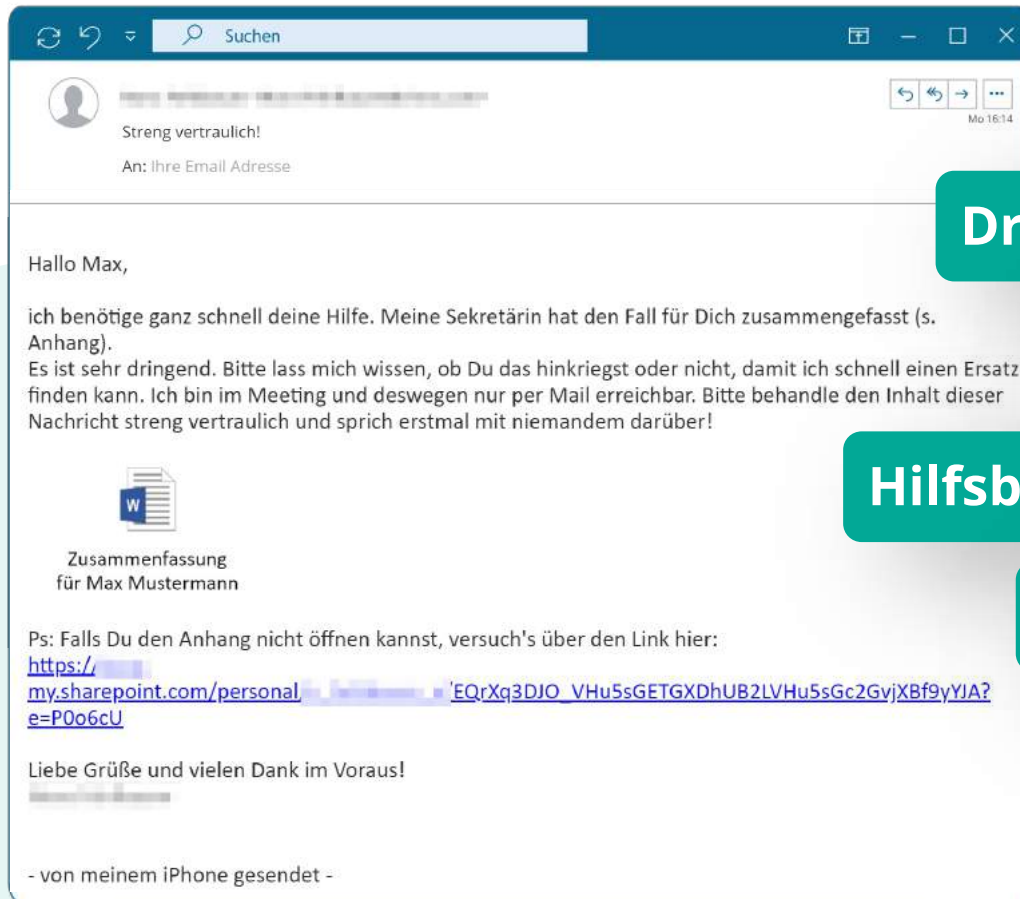


Warum ist das so einfach?



**Menschen sind
soziale, unsoziale,
ängstliche, neugierige,
hilfsbereite, ... Wesen.**

CEO-Fraud wird uns auch aktuell begleiten.



Druck / Angst

Autorität

Hilfsbereitschaft

Vertrauen

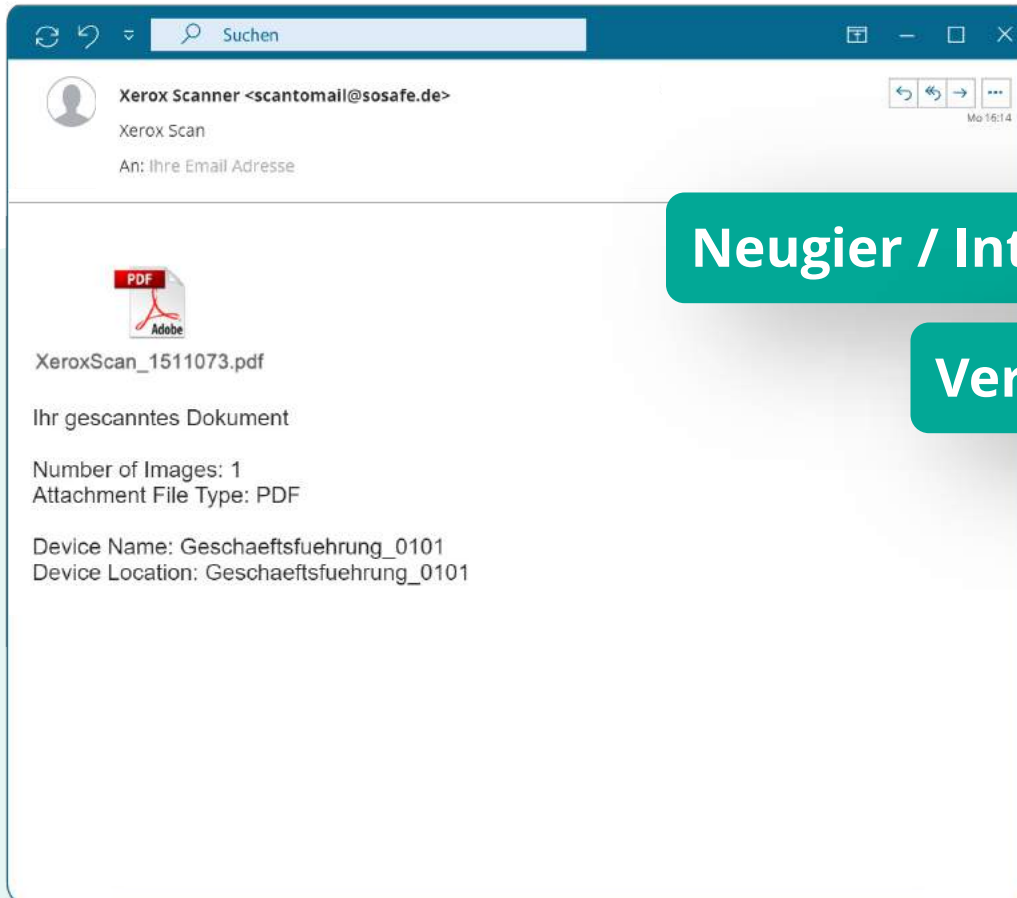


83 %

Klickrate

- Top 1 in unseren Simulationen
- Hoher Erfolg trotz zahlreicher Phishing-Anzeichen
- Zahlreiche weitergehende Angriffswinkel:
 - Emotet-Anhang
 - Password-Phishing
 - Social-Engineering

Auf die menschliche Neugierde ist Verlass.



Neugier / Interesse

Vertrauen



50 %

Klickrate

- Top 7 in unseren Simulationen
- Extrem simpler Aufbau
- Aufwand für den Phisher:

3 Minuten

„Loose lips save ships!“ – Oder: Flurfunk schützt.

Prä-
Corona



Klickrate Phishing-Mails nach Organisationsform



Systematische Awareness zeigt Wirkung – und macht auch noch Spaß!

28,6 %

durchschnittliche
Klickrate unserer Kunden



66%

Reduktion
der Klickrate¹



4,8 ★ ★ ★ ★ ☆

Durchschnittliche Bewertung durch
die Mitarbeitenden unserer Kunden

¹ Unsere Top Performer erreichen im ersten Jahr durchschnittlich eine Reduktion der Klickrate um 66 %.

Bestmögliche Klickratenreduktion durch Kombination unserer Produkte.

Phishing-Simulation & E-Learning



Phishing-Simulation



Phishing-Simulation & E-Learning



40%
zusätzliche
Klickratenreduktion

Interaktive Lernmodule schulen Mitarbeitende, um das Unternehmen umfassend vor Cyber-Angriffen zu schützen.



Kompakttraining IT-Sicherheit



**Grundlagen
Cyber-Sicherheit**



**Internet
& Webtools**



**E-Mails
sicher nutzen**



**Sicher am
Arbeitsplatz**



**Mobilgeräte
sicher nutzen**



Schadsoftware

Die E-Learning Module können an Ihre Corporate Identity angepasst werden.

neulipa

DATENSCHUTZ

WILLKOMMEN ZUM MODUL

Datenschutz

Start

Welche Daten müssen besonders geschützt werden?
Warum sind Datenschutz und IT-Sicherheit zwei Seiten einer Medaille?
Was bedeutet die Datenschutzgrundverordnung EU-DSGVO für Unternehmen und Mitarbeiter?

Bei Rückfragen kontaktieren Sie Ihren IT-Sicherheitsbeauftragten Herrn Meier per Mail an: meier@neulipa.de

An Ihre Firmenfarben (Corporate Design) anpassbar

Auf Ihre interne Kommunikation abgestimmt. Beispiel:
Bei Rückfragen kontaktieren Sie Ihren IT-Sicherheitsbeauftragten Herrn Meier per Mail an: meier@neulipa.de

Ihre Vorteile im Überblick.



Plug 'n Play

Keine internen Ressourcen und keine Integration in bestehende Systeme.



Effiziente Schulung

Deutliche Kosten- und Arbeitszeiterparnis ggü. klassischen Schulungsangeboten.



Individuelle Anpassbarkeit

Anpassbarer Content über intelligente Platzhalter und individuelle Phishing-Mails.



ISO-Schulungsnachweis

Auf DSGVO und ISO 27001 abgestimmte Reportings zum Nachweis auf Knopfdruck.



Sofortige Messbarkeit

Reduzierte Klickraten und erhöhte Wachsamkeit innerhalb weniger Wochen.



Made in Germany

SoSafe wird komplett in Deutschland entwickelt und gehostet – damit volle DSGVO-Konformität.

**100% Datensicherheit
durch europäische Server**

Kostenloses White Paper: Best Practices Phishing-Simulationen.

- 1 Aufbau und Erfolgsmethoden
- 2 Rechtliche Rahmenbedingungen
- 3 Konkrete Empfehlungen inkl. Checkliste

www.sosafe.de/whitepaper



“Amateure hacken Systeme, Profis hacken Menschen.”

Bruce Schneier

Experte für Kryptographie
und Computersicherheit,
Harvard University



SoSafe GmbH
Ehrenfeldgürtel 76, 50823 Köln
www.sosafe.de | info@sosafe.de

