



# Föderale Digitalstrategie



**Digitale  
Transformation**



**Digitale  
Infrastruktur**



**Digitale  
Anwendungen**



**Datennutzung**

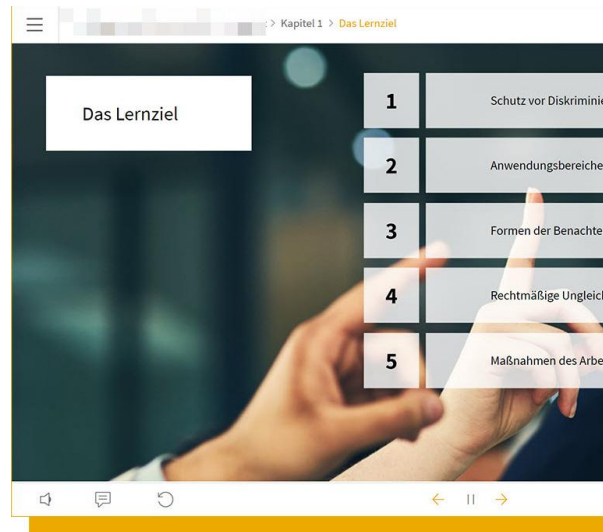


**Informations-  
sicherheit**

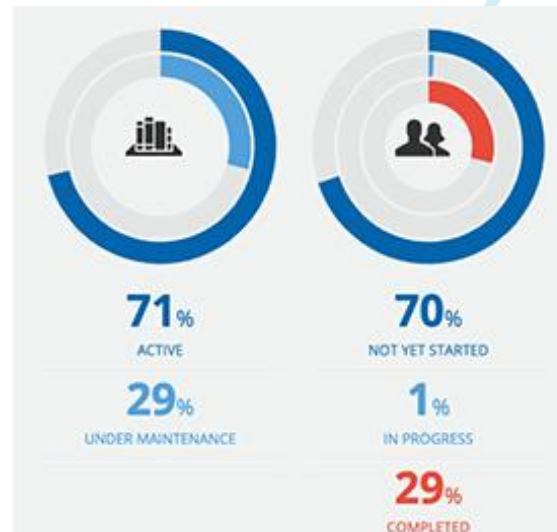
# Agenda

- Ausgangssituation 2024
- IT-Security-Awareness-Training
- Phishing-Simulation
- Fragen

# Ausgangssituation 2024



In die Jahre  
gekommenes  
Online-Training



Schlechte Werte bei  
Registrierung  
und Teilnahme

Sehr geehrte Damen und Herren,  
eine durchaus ernst gemeinte Frage:  
**Wollt Ihr mich verarschen?**  
Eindeutig eine Spam E-Mail, die wird von jedem funktionierenden Filter abgefangen.

**Und kommt mir nicht wieder mit eurem Standardsatz wegen Spam E-Mails. Ich erwarte endlich Ergebnisse bzw. ein Unterlassen der ständigen Prüfungen.**

Mit freundlichen Grüßen

Negatives Feedback zur  
Phishing-Simulation



# IT-Security-Awareness-Training

# Anforderungen – IT-Security-Awareness-Training

1. Praxisnahe & modulare Inhalte – individualisierbar und passend für Kommunen
2. Didaktisch wertvoll und fundiert – Ansätze aus der Verhaltenspsychologie
3. Interaktive & abwechslungsreiche Formate – Videos, Story-Elemente und Gamification
4. Personalisierte Auswertung & Feedback – Fortschritt und Zertifikat
5. Messbarkeit & Reporting für Führungskräfte – KPIs und Berichte
6. Regelmäßige Wiederholung & Anpassung – Trainings basierend auf Lernstand


# IT-Security-Awareness-Training von sosafe

FRIEDRICHSHAFEN Training Erfolge

### Willkommen Ralph!


Sie sind etwas hinter dem Zeitplan – aber keine Sorgen, das können Sie schnell und einfach aufholen!

### Ihre Erfolge




**Level 7**

320 von 1130



Zertifikat ausstellen


### Ihr Lernpfad



Verpflichtend ~5 Min.

#### Filesharing

0%



Verpflichtend ~3 Min.

#### Schadsoftware

0%

Neugierig auf mehr? Hier finden Sie alle Lektionen.

### Bibliothek

Kompakttraining IT-Sicherheit

Alle Lektionen Verpflichtend Überfällig

#### Bedeutung von Cyber-Sicherheit

1 Min.

Abgeschlossen

#### Richtiges Verhalten bei IT-Sicherheitsvorfällen

4 Min.

Abgeschlossen

#### Cyber-Attacken abwehren

1 Min.

Abgeschlossen

**FACHKONGRESS**  
DES IT-PLANUNGSRATS



## Richtige Nutzung

Clara kennt nun die Tools und weiß um ihren Nutzen. Kennt sie aber auch deren Risiken? Jan gibt ihr eine praktische Checkliste für die Zukunft.

Weiter

- 
- 1 Nutzung mit der zuständigen Abteilung (Benutzerservice IuK) abstimmen**  
Vermeiden Sie es, eine parallele „Schatten-IT“ aufzubauen.
  - 2 Dateien und Links überprüfen**  
Kontaktieren Sie den Absendenden einer Datei im Zweifel über ein **anderes Medium**, z. B. Telefon.
  - 3 Programm nach Nutzung schließen**  
Microsoft Remote Desktop z. B. lässt sich **deaktivieren**, solange Sie es nicht benötigen.
  - 4 Daten nicht leichtfertig weitergeben**  
Prüfen Sie immer genau, mit wem Sie Daten **austauschen**.
  - 5 Name der Organisation auslassen**  
Wählen Sie stattdessen ein Codewort als Namen aus.









# Phishing-Simulation

# Anforderungen – Phishing-Simulation

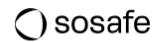
1. Realistische, maßgeschneiderte Phishing-Mails
2. Regelmäßige, aber nicht überfordernde Durchführung
3. Messbarkeit & aussagekräftige Metriken
4. Sofortiges Feedback & begleitendes Lernen
5. Rechtliche & organisatorische Compliance

# Phishing-Simulation von sosafe

The screenshot displays the sosafe Phishing-Simulation interface. On the left, a sidebar contains the 'sosafe' logo, a user profile placeholder, and a navigation menu with 'Phishing' selected and a 'Simulation' button. Below the menu is a 'Profilbasierte Simulation' section with tags for Finance, IT-Management, Leadership, Human Resources, Packaging, and Bio Chemicals. The main area is titled 'Phishing-Simulationstyp' and asks the user to 'Wählen Sie die Art der Simulation aus.' Three options are available: 'Einfach' (Einfache Simulation), 'Gezielt' (Umfassende Individualisierung), and 'Verhaltensbasiert' (Adaptives Lernen). The 'Gezielt' option is selected and highlighted with a blue border. Below this, a preview of a simulated phishing email is shown. The email has a subject line 'Kritisches Sicherheitsproblem' and is in German. The body text reads: 'Hallo [Vorname], wir haben am [seven Tage vor dem heutigen Datum] ein kritisches Sicherheitsproblem in unserem Netzwerk festgestellt, das umgehend Ihre Aufmerksamkeit erfordert. Bitte klicken Sie unten auf den Link, um den Update-Prozess auf Ihrem Gerät zu starten: [Hier klicken]'. There is a placeholder for a 'Gefälschter Anhang' (Faked Attachment) with a hand cursor over it. The email ends with 'Mit freundlichen Grüßen, Ihr IT-Support-Team'.



# Klick führt auf E-Learning Seite



## Glück gehabt! Dies hätte eine Phishing-Mail sein können...

Die E-Mail, auf die Sie soeben geklickt haben, ist Teil einer autorisierten **Simulation von Cyberangriffen im Auftrag der Stadt Friedrichshafen**. Ziel ist es, Ihnen zu zeigen, worauf Sie achten müssen, um derartige Attacken erkennen und verhindern zu können.

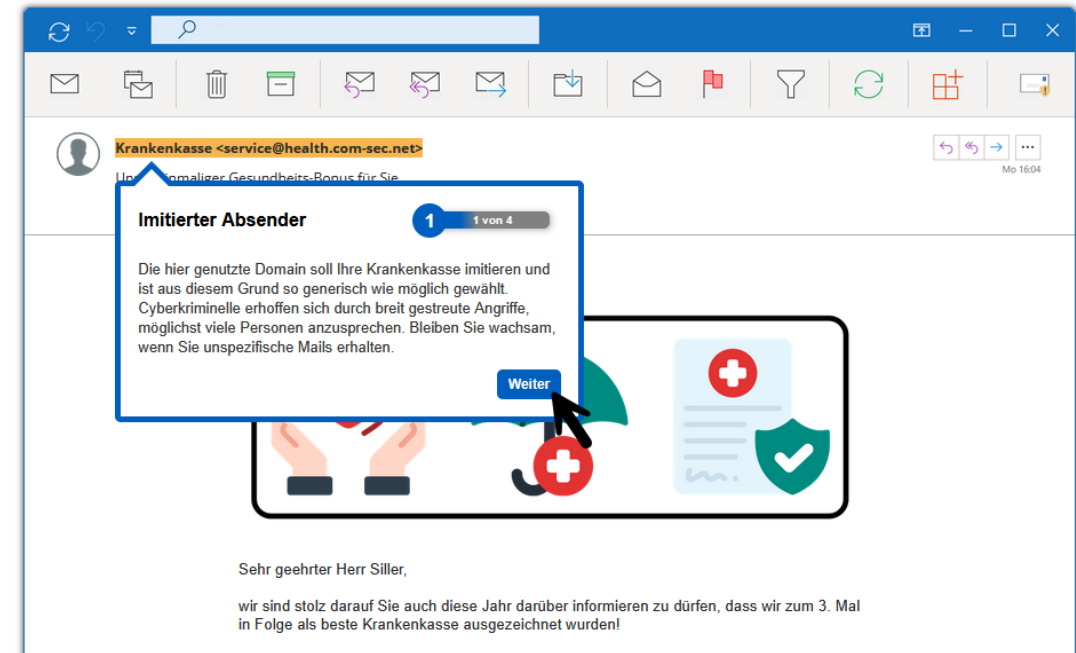
- Es besteht **keine Gefahr** für Sie, Ihre Daten oder Ihr Endgerät – die Simulation dient lediglich zu Schulungszwecken
- Es werden **keine individuellen Daten** (z. B. ob Sie auf einzelne Mails klicken) an Ihren Arbeitgeber zurückgemeldet
- Klicken Sie auf **Erklärung starten**, um konkrete Hinweise zu der von Ihnen geklickten Mail angezeigt zu bekommen

Wir empfehlen, Ihren Lernerfolg und den Inhalt der Phishing-Mails nicht mit Kolleginnen und Kollegen zu teilen. So haben alle Teilnehmenden die Chance, von der Phishing-Simulation zu profitieren.

... aber es hätte Sie Millionen kosten können.

### 1 von 5 Sicherheitsverletzungen beginnt mit Phishing

Ein einziger Klick kann ausreichen, um einen schwerwiegenden Sicherheitsvorfall auszulösen. Kontinuierliches Bewusstsein ist Ihre stärkste Verteidigung. Verpassen Sie nicht diesen kritischen Moment, während er noch frisch in Ihrem Gedächtnis ist - starten Sie jetzt Ihre E-Learning-Lektion, um sich gegen sich entwickelnde Bedrohungen zu wappnen.



# Detaillierte Auswertung und niedrige Klickraten

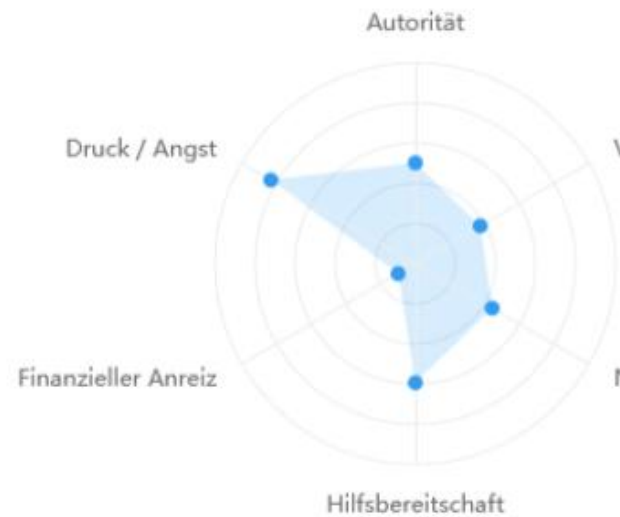
## Klickrate

10,6%

1.177 / 11.069

## Klickrate

nach psychologischer Taktik in %



## Klickrate

nach technologischem Vektor in %





# Fragen ?



## Ralph Erhardt

Amtsleitung/CDO

[r.erhardt@friedrichshafen.de](mailto:r.erhardt@friedrichshafen.de)

+49 7541 203-51500

[www.friedrichshafen.de](http://www.friedrichshafen.de)

# Danke!



## Noch Fragen ?