



# Sicherheitskultur stärken:

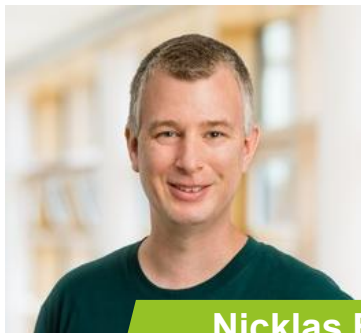
Von Richtlinien zu gelebter Informationssicherheit

Nicklas Baier, Kommunale Versorgungskassen Westfalen-Lippe

Don Diephaus, viadee Unternehmensberatung AG



## // Wer sind wir?



**Nicklas Baier | kww**

### **IT-Sicherheitsbeauftragter**

- IT-Sicherheitsbeauftragter für kww & Mandanten
- UNIX/Linux, Netzwerk & regulatorische IT-Sicherheit (DORA, NIS2)
- Awareness- & Phishingkampagnen, Förderung der IT-Sicherheitskultur

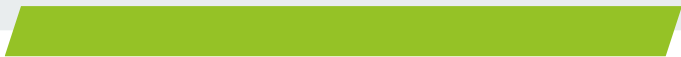


**Don Diephaus | viadee**

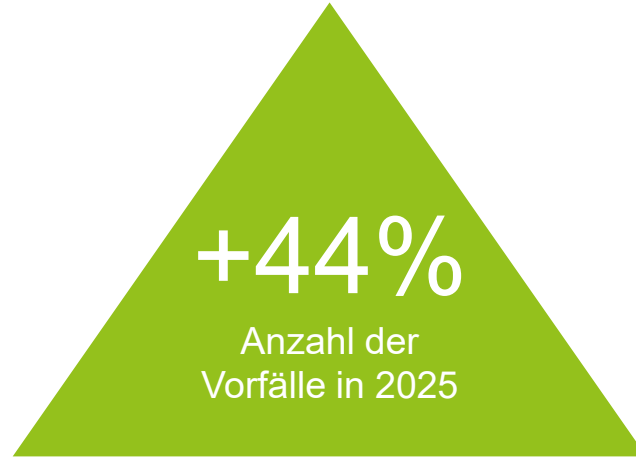
### **IT-Berater**

- IT-Security Management & Awareness
- Web-Security Testing
- Software Entwicklung

# // Motivation






## // Cyberangriffe nehmen rasant zu



<https://www.orangecyberdefense.com/global/white-papers/security-navigator-2025>  
<https://www.security-insider.de/alarmierender-anstieg-cyberkriminalitaet-europa-a-9c06fd96fb6c74ff31b921608618eee9/>

# // Öffentlicher Dienst zunehmend im Fokus

## Angriffsmotive

-  Finanzieller Anreiz
-  Hochsensible Daten
-  Politische Instabilität

## Fallbeispiel:

Südwestfalen IT: Ransomware-Angriff

-  2,8 Mio EUR Schaden
-  22.000 Arbeitsplätze lahmgelegt
-  70+ Kommunen
-  1,6 Mio. Bürger:innen betroffen

<https://www1.wdr.de/nachrichten/westfalen-lippe/ein-jahr-nach-cyberangriff-suedwestfalen-it-100.html>

<https://www.zeit.de/news/2025-11/11/oeffentliche-verwaltung-im-visier-von-cyberspionen>

<https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimsschutz/cyberspionage/cyberspionage-artikel.html>

# // Faktor Mensch – das größte Einfallstor

Schwache Passwörter 

Unachtsamkeit 

Phishing 

Fehlkonfigurationen 


Social Engineering 

## 74 %

Alle Sicherheitsvorfälle sind  
auf menschliches  
Fehlverhalten zurückzuführen

 Vishing



 Deepfakes

# // Das Vorgehen im Überblick





# Grundlagen

# // Drei Säulen der Informationssicherheit



# // Was ist Sicherheitskultur?

„Geteilte Werte, Normen und Verhaltensweisen aller Mitarbeitenden zum Schutz von Informationen – **Sicherheit als gelebter Alltag nicht als Pflicht.**“



## Organisation

- ✓ Führung lebt Sicherheit vor
- ✓ Klare Verantwortlichkeiten
- ✓ Offene Fehlerkultur



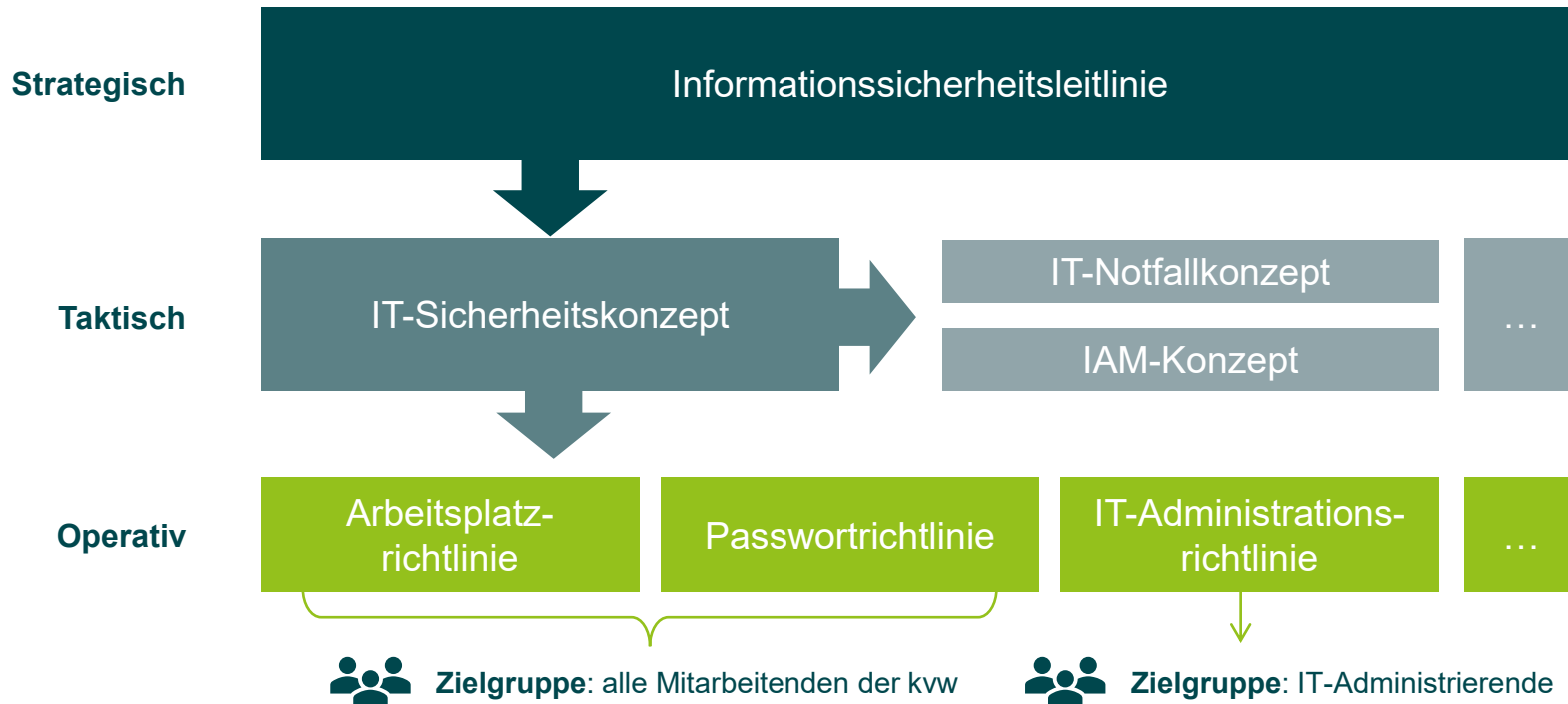
## Mitarbeitende

- ✓ Fühlen sich mitverantwortlich
- ✓ Kennen aktuelle Bedrohungen
- ✓ Melden Vorfälle proaktiv



# Sicherheitsdokumentation @ kvw-IT

# // Struktur der Sicherheitsdokumentation



# // Wie alles zusammenhängt



# // Einblick in die IT-Arbeitsplatzrichtlinie

## Inhaltsverzeichnis

Glossar .....	5
Verbindlichkeiten und Festlegungen .....	6
1. Dokumentinformationen .....	7
1.1 Einleitung .....	7
1.2 Zielsetzung .....	7
1.3 Geltungsbereich .....	8
1.4 Ansprechpersonen für das tägliche Arbeiten .....	8
1.4.1 IT-Koordination (ITK) .....	8
1.4.2 IT-Service-Desk .....	8
2. Nutzung der dienstlichen Geräte der kww .....	10
2.1 Umgang mit der kww-Hardware .....	10
2.2 Anschluss externer Geräte .....	11
2.3 WLAN und andere Netzwerke .....	11
2.4 Installation von Programmen .....	11
2.5 Reparatur und Wartung .....	11
2.6 Verhalten bei veränderten Arbeitsweisen von Arbeitsgeräten .....	11
2.7 Datensicherung und -speicherung (Backup) .....	12
2.8 Einsatz eines Virenschutzprogramms .....	12
2.9 Außerbetriebnahme von dienstlicher Hardware .....	12
3. Zugriff auf Daten und Anwendungen der kww .....	13
3.1 Schutz vor unbefugtem Zugriff – Passwortrichtlinie der kww .....	13
3.2 Verlassen des Arbeitsplatzes .....	13
3.3 Berechtigter Zugriff anderer Benutzer:innen auf ihre Arbeitsgeräte .....	13
3.3.1 Zugriff von kww-Mitarbeitenden .....	13
3.3.2 Zugriff der IT (Remote, Inventory, Softwareverteilung) .....	13
4. Datenschutz .....	14
4.1 Allgemeines .....	14
4.2 Weitergabe von personenbezogenen Daten .....	14
4.3 Vorbeugung gegen „Social Engineering“ .....	15

4.4 Beaufsichtigung und Begleitung von unberechtigten Personen .....	15
4.5 Temporäre Laufwerke „tmp/“ .....	15
4.6 Hinweise zum Datenschutz .....	16
4.7 Dienstvereinbarung zu Videokonferenzen .....	16
5. Datenaustausch .....	17
5.1 Datenaustausch über das interne Netz der kww .....	17
5.2 Datenaustausch über das Internet .....	17
5.3 Datenaustausch über Public Cloud-Services .....	17
5.4 Weitergabe von Daten an Externe .....	17
6. Datenträgeraustausch .....	18
7. E-Mail-Nutzung .....	19
8. Internet-Nutzung .....	21
9. Speziellere Regelungen für Mobiles Arbeiten .....	22
9.1 Allgemeines .....	22
9.2 Authentifizierung .....	22
9.3 Spezielle Regeln zur Nutzung dienstlicher Smartphones und Tablets .....	23
9.3.1 Allgemeines .....	23
9.3.2 Anwendungskontrolle .....	23
10. Grundlagen zur Nutzung von Suchmaschinen .....	24
11. Grundlagen zur Nutzung künstlicher Intelligenz .....	25
12. Aushändigung der IT-Arbeitsplatz-Richtlinie .....	26
13. Schlussbestimmung .....	27
14. Anhang .....	28

# // Unsere Inspiration: IT-Grundschutz-Kompendium



SYS.2: Desktop-Systeme

## SYS.2.1: Allgemeiner Client

### SYS.2.1.A1 Sichere Benutzerauthentisierung (B)

Um den Client zu nutzen, MÜSSEN sich die Benutzer gegenüber dem IT-System authentisieren. **Benutzer MÜSSEN eine Bildschirmsperre verwenden, wenn sie den Client unbeaufsichtigt betreiben.** Die Bildschirmsperre SOLLTE automatisch aktiviert werden, wenn für eine festgelegte Zeitspanne keine Aktion durch den Benutzer durchgeführt wurde. Die Bildschirmsperre DARF NUR durch eine erfolgreiche Benutzerauthentisierung deaktiviert werden können. Die Benutzer SOLLTEN verpflichtet werden, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden.

Richtlinie



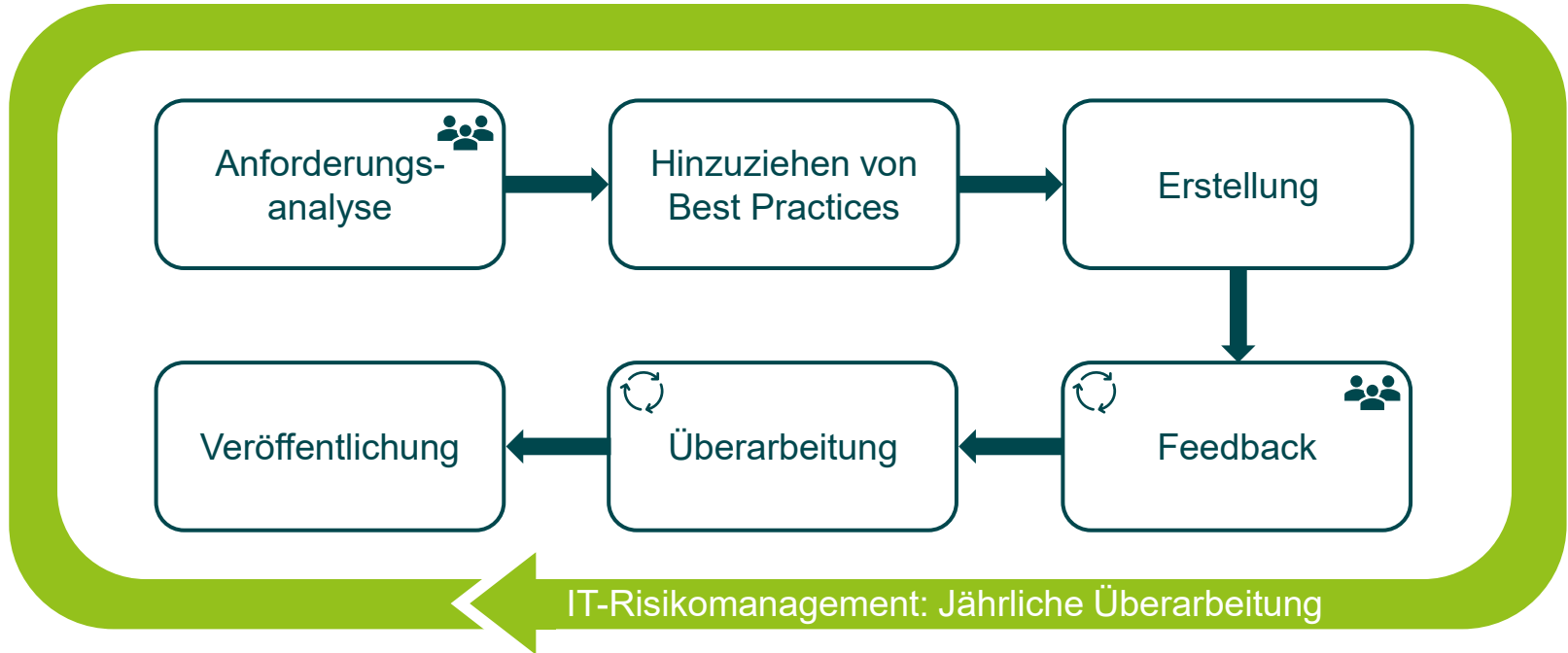
## IT-Arbeitsplatzrichtlinie der Kommunalen Versorgungskassen Westfalen-Lippe


Verantwortung: Informationssicherheit, Nicklas Baier

### 3.2 Verlassen des Arbeitsplatzes

Die **Benutzer:innen MÜSSEN** dafür Sorge zu tragen, **dass beim Verlassen des Arbeitsplatzes das Notebook manuell gesperrt wird** (Windowstaste + L oder Strg + Alt + Entf und dann Sperren).

## // Der Erstellungsprozess im Überblick



A woman with a distressed expression is buried up to her chest in a chaotic mountain of black ring-bound folders and stacks of papers. She is looking upwards with a worried look, her hands resting on the papers. The office environment is cluttered, with a window in the background showing a view of mountains. The overall mood is one of frustration and being overwhelmed by a large volume of work.

Und jetzt?



# Von Richtlinien zu gelebter Praxis



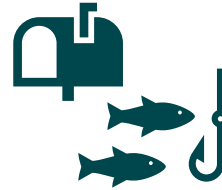
## // Unsere Werkzeuge



Richtlinien



Awareness  
Schulungen



Phishing-  
Kampagnen



Offene  
Kommunikation



**Förderung der Sicherheitskultur**

## // Awareness Schulung



Kurs

+



Prüfung

1x  
jährlich

30  
min

# // Awareness Schulung: Kurse

## ➤ Klar und in aller Kürze: Anforderungen der Richtlinien

Folie 7 / 14  
Arbeitsplatz

### Arbeitsplatz

Die Wahrung von Geschäfts- und Betriebsgeheimnissen ist für ein Unternehmen unabdingbar. Deshalb ist es wichtig, vertrauliche Dokumente sorgfältig, und nicht für andere einsehbar, aufzubewahren.

---

#### ! REGELN

- Lassen Sie keine vertraulichen Dokumente unbeaufsichtigt auf Ihrem Schreibtisch liegen. Verfolgen Sie möglichst eine Clean Desk-Politik.
- Vertrauliche Dokumente sind gesichert aufzubewahren bzw. sachgerecht in die dafür vorgesehenen Papierbehälter zu entsorgen.
- Nicht mehr benötigte elektronische Datenträger sind zur fachgerechten Entsorgung an den IT-Service Desk zu geben.

Folie 8 / 14  
Gebäudesicherheit

### Gebäudesicherheit

Die Unternehmensräume sind besonders schützenswert, da sich dort sensible und wertvolle Informationen, Gegenstände und Infrastrukturen befinden. In den Büroräumen dürfen sich deshalb nur berechnigte Personen aufhalten. Das Verhalten der Mitarbeiter:innen ist für diesen Schutz entscheidend.

---

#### ! REGELN

- Lassen Sie keine unberechnigten Personen in die Büroräume.
- Sprechen Sie verdächtige, unbekannte Personen an und informieren Sie das Vorzimmer/ die Gebäudesicherheit.
- Achten Sie darauf, Türen und Fenster bei Abwesenheit zu schließen.
- Melden Sie den Verlust von KABA-Zugangsmedien unverzüglich an den IT-Service Desk sowie das Vorzimmer.

# // Awareness Schulung: Kurse

## ➤ Für Gefahren sensibilisieren und auf den Ernstfall vorbereiten

☰ ⚙️ **KVV** Folie 11 / 14  
Social Engineering

## Social Engineering

Beim Social Engineering geht es um die zwischenmenschliche Beeinflussung einer Person. Dabei versucht der Angreifer das Vertrauen des Opfers zu gewinnen und ihn so zum Beispiel in einem Telefonat zur Preisgabe von vertraulichen Informationen oder zur Freigabe von Passwörtern zu bewegen.

---

### ! REGELN

- Verfügen Sie über ein gesundes Misstrauen gegenüber fremden Personen.
- Stellen Sie durch Rückruf sicher, dass es sich bei Ihrer Gesprächspartnerin oder Ihrem Gesprächspartner wirklich um die vorgegebene Person handelt.
- Seien Sie insbesondere bei E-Mails skeptisch, da sich Absenderdaten leicht fälschen lassen.
- Achten Sie darauf, auf öffentlichen Plattformen und sozialen Netzwerken nicht zu viele Informationen über sich preiszugeben, um möglichem Identitätsdiebstahl vorzubeugen.

☰ ⚙️ **KVV** Folie 13 / 14  
IT-Sicherheitsvorfälle

## IT-Sicherheitsvorfälle

Sobald Anzeichen zu erkennen sind, dass es sich um einen IT-Sicherheitsvorfall handelt, sollte man die Ruhe bewahren und umgehend den IT Service Desk kontaktieren. Damit gewährleisten alle Mitarbeiter:innen, dass mögliche Risiken minimiert oder eliminiert werden können.

Beispiele für IT-Sicherheitsvorfälle sind verlorene KABA-Zugangsmedien, kompromittierte Accounts, seltsames Verhalten des Computers oder verdächtige E-Mails und Anrufe.

---

### ! REGELN

- Wenn Sie das Gefühl haben, es liegt ein IT-Sicherheitsvorfall vor, melden Sie dies unverzüglich.
- Wurde während eines IT-Sicherheitsvorfalles eine Eingabe der Zugangsdaten getätigt, muss das aktuelle Passwort sofort geändert werden und der IT Service Desk informiert werden.

# // Awareness Schulung: Kurse

## ➤ Tipps und praktisches Wissen vermitteln

☰ ⚙️ **KWV** Folie 3 / 14  
Passwort-Sicherheit: Hinweise

### Passwort-Sicherheit: Hinweise

**Änderungszyklus**  
Zum Schutz der Datensicherheit müssen alle Anwender:innen insbesondere ihr zentrales Passwort mindestens **einmal jährlich** ändern.  
Wird das Passwort nicht innerhalb eines Jahres eigenständig geändert, wird die Aktualisierung des Passwortes beim nächsten Anmeldeversuch systemseitig erzwungen.

**Überprüfung**  
Zur eigenen Überprüfung der Passwortstärke kann der Service "Have I been pwned" verwendet werden. Hierbei handelt es sich um einen sicheren Service, welcher überprüft, ob das eigene Passwort bereits durch einen Datenleck veröffentlicht wurde.

**Tipps für ein starkes Passwort**  
Zur Erstellung eines starken Passworts ist die Bildung eines Satzes hilfreich, bei welchem nur Anfangs- oder Endbuchstaben der jeweiligen Wörter kombiniert werden und wiederum einzelne Wörter durch Zahlen oder Sonderzeichen ersetzt werden.

**Was hat Ihr Passwort mit Pizza zu tun?**

Denken Sie sich einen Satz aus, der mindestens eine Zahl enthält, zum Beispiel:



## Was hat Ihr Passwort mit Pizza zu tun?

Denken Sie sich einen Satz aus, der mindestens eine Zahl enthält, zum Beispiel:

**„Am liebsten esse ich Pizza mit vier Zutaten und extra Käse!“**

Merken Sie sich nun den ersten Buchstaben eines jeden Wortes und Sie erhalten ein starkes und sicheres Passwort.

**AleIPm4Z+eK!**

**i**  *Tipp: Nutzen Sie Passwort-Manager! Das sind Apps oder Software-Programme, die alle Ihre Passwörter und die zugehörigen Benutzernamen sicher verwalten. Sie brauchen sich dann nur ein sicheres Masterpasswort für den Passwort-Manager merken.*

© Bundesamt für Sicherheit in der Informationstechnik (BSI) [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)

# // Awareness Schulung: Prüfung

## ➤ Erlerntes festigen

**Sie benötigen ein neues Passwort. Wie gehen Sie bei der Erstellung vor?**

Ich kombiniere Sonderzeichen, Groß- und Kleinbuchstaben zu einem möglichst komplexen Passwort (z.B.: „W@SSerStNaSS!“).

Ich bilde einen Merksatz, leite aus diesem Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen ab, um ein möglichst komplexes und langes Passwort zu erstellen.

Ich verwende ein möglichst komplexes und langes Passwort, das ich mir merken kann, da ich es für etliche private und geschäftliche Dienste verwende.

Als Standardbenutzer wähle ich ein komplexes Passwort mit einer Mindestlänge von 10 Zeichen.

Ich entscheide mich für das Passwort "Schalke04!!!", da es alle Kriterien der Passwortrichtlinie erfüllt.

Die Passwortrichtlinie schreibt eine mind. 12 Zeichen lange Kombination aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen vor.

Es bietet sich an einen Merksatz zu bilden, aus dem Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen abgeleitet werden können.

Beispiel: „Am Aasee kann ich im Sommer fünf Stunden lang sitzen, während es im Winter eher 20 Minuten sind!“ -->  
„AAkii55Sl,weiWe20Ms!“.

Verwenden Sie Passwörter einmalig je Dienst und vermeiden Sie triviale Passwörter bzw. solche die in bekannten Datenlecks veröffentlicht wurden, etwa „Schalke04!!!“. Eine Prüfung, ob ein Passwort kompromittiert wurde, kann über folgende Plattform erfolgen:  
<https://haveibeenpwned.com/Passwords>

# // Awareness Schulung: Prüfung

## ➤ Teilnehmende in alltagsnahe Szenarien versetzen

**Sie erhalten eine verdächtige E-Mail mit der Bitte, Ihre Bank-Zugangsdaten zu überprüfen. Was sollten Sie tun, um Phishing zu vermeiden?**

Wählen Sie **alle** richtigen Antworten (Mehrfachauswahl möglich).

Auf den Link in der E-Mail klicken, um zu prüfen, ob die Website echt aussieht.

Die Echtheit der Nachricht durch direkte Kontaktaufnahme mit der Bank über bekannte, offizielle Kanäle überprüfen.

Die E-Mail ignorieren oder löschen, wenn sie verdächtig wirkt oder viele Rechtschreibfehler enthält.

Niemals persönliche Daten oder Passwörter über Links in E-Mails eingeben.

Den Mauszeiger über den Link in der E-Mail bewegen, um die tatsächliche Webadresse zu überprüfen.

**Nach Feierabend treffen Sie sich mit Freunden am Aasee. Sie haben Ihr dienstliches Notebook dabei und möchten kurz zum Kiosk gehen, um ein Getränk zu kaufen. Wie sollten Sie sich in dieser Situation verhalten?**

Wählen Sie **alle** richtigen Antworten (Mehrfachauswahl möglich).

Sie nehmen Ihr dienstliches Notebook mit, damit es nicht unbeaufsichtigt bleibt.

Sie lassen das Notebook kurz bei Ihren Freunden liegen - es ist ja nur ein Moment.

Falls das Gerät verloren geht oder gestohlen wird, melden Sie den Vorfall umgehend beim IT-Service Desk.

Sie lassen das Gerät offen auf einer Parkbank liegen, um einen Platz zu sichern.

# // Awareness Schulung: Prüfung

## ➤ Für Gefahren sensibilisieren

Welche der folgenden Informationen könnten Social Engineers versuchen von Ihnen zu erlangen?

Wählen Sie **alle** richtigen Antworten (Mehrfachauswahl möglich).

Persönliche Informationen über Mitarbeitende, etwa Geburtstage oder Hobbys.

Intern verwendete Begriffe, Abkürzungen oder Prozesse.

Das Wetter am Unternehmensstandort.

Öffentliche Pressemitteilungen der kww.

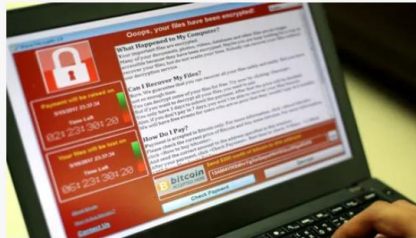
System- und Netzwerkkonfigurationen der kww.

Zugangsdaten wie Benutzername und Passwort.

Informationen über aktuelle Sicherheitslücken der kww.

Sie arbeiten an Ihrem Laptop, als plötzlich folgende unbekannte Meldung angezeigt wird. Was sollten Sie jetzt tun?

Wählen Sie **alle** richtigen Antworten (Mehrfachauswahl möglich).



Erst mal einen Kaffee holen.

Welche IT-Sicherheitsverstöße können Sie im folgenden mobilen Arbeitsszenario identifizieren?



Private Hardware ist am Dienstgerät angeschlossen.

Mobiles Arbeiten in der Öffentlichkeit ist grundsätzlich nicht erlaubt.

Unberechtigte Personen haben Einsicht auf potenziell geschäftliche Daten auf dem Bildschirm.

Es sind keine IT-Sicherheitsverstöße zu erkennen.

Getränke stehen offen direkt neben elektronischen Geräten.

# // Frage an das Publikum!

- Welche IT-Sicherheitsverstöße identifizieren Sie?

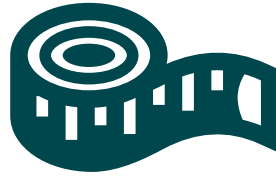


## // Phishing Kampagnen



Sensibilisierung

+



Messinstrument

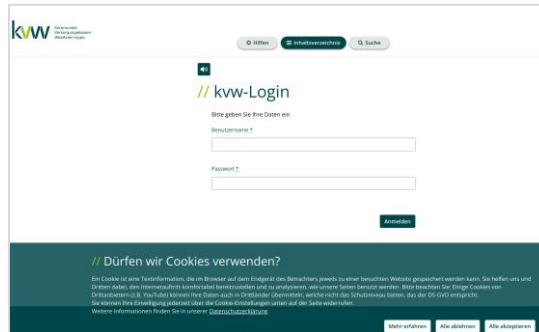


# // Klassisches Format

Phishing-Mail



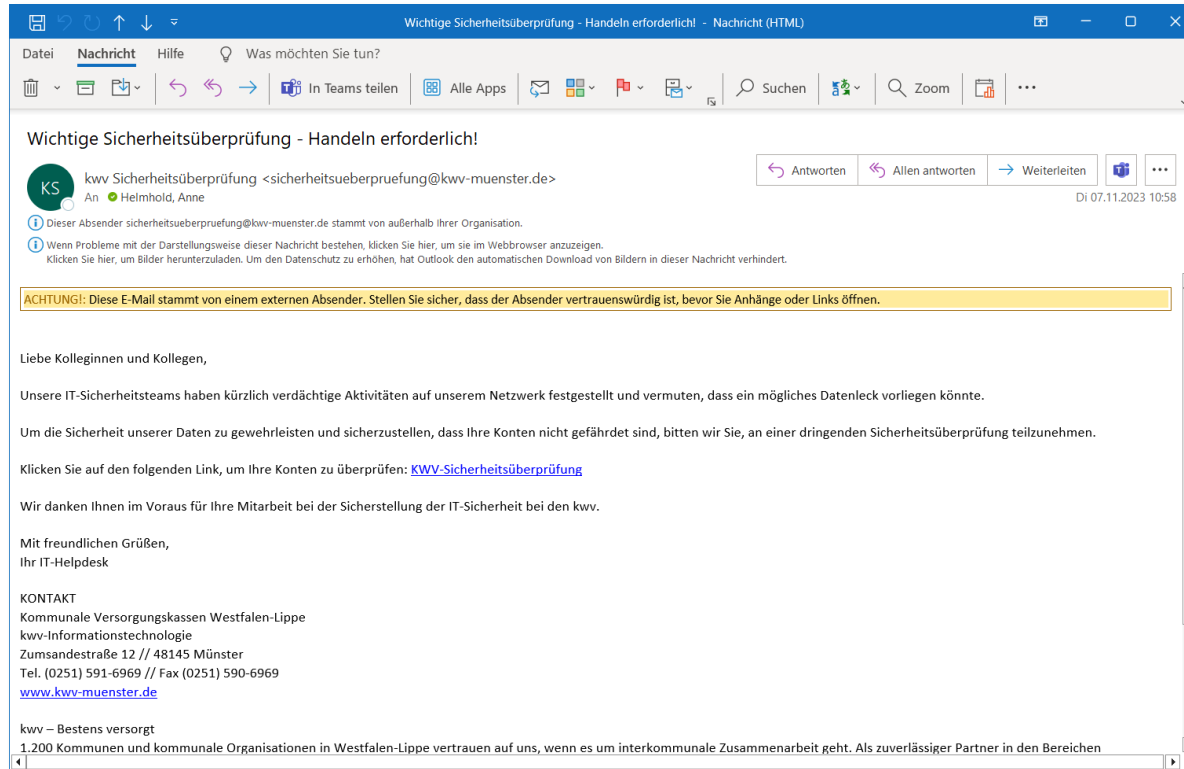
Landing-Page



Learning-Page



# // Phishing-Mail



# // Landing-Page

**kvv** Kommunale Versorgungskassen Westfalen-Lippe

Hilfen Inhaltsverzeichnis Suche

Startseite > Sicherheitsüberprüfung > KVV-Login

// KVV-Login

Bitte geben Sie hier ihre Daten zur Überprüfung ein

Benutzername \*

Passwort \*

// Dürfen wir Cookies verwenden? [Anmelden](#)

Ein Cookie ist eine Textinformation, die im Browser auf dem Endgerät des Betrachters jeweils zu einer besuchten Website gespeichert werden kann. Sie helfen uns und Dritten dabei, den Internetauftritt komfortabel bereitzustellen und zu analysieren, wie unsere Seiten benutzt werden. Bitte beachten Sie: Einige Cookies von Drittanbietern (z.B. YouTube) können Ihre Daten auch in Drittländer übermitteln, welche nicht das Schutzniveau bieten, das der DS-GVO entspricht. Sie können Ihre Einwilligung jederzeit über die Cookie-Einstellungen unten auf der Seite widerrufen. Weitere Informationen finden Sie in unserer [Datenschutzerklärung](#).

Mehr erfahren Alle ablehnen Alle akzeptieren

# // Learning-Page

**viadee**  
PRAKTIKUMSCHAFT

## GLÜCK GEHABT!


Dieser Phishing-Angriff ist Teil der IT-Security Kampagne der kww.  
Wichtig: Wir haben keine Daten von Ihnen abgegriffen.

Ansprechpartner für diese Aktion bei den kww: Nicklas Baier (n.baier@kww-muenster.de), Olaf Werning (o.werning@kww-muenster.de)

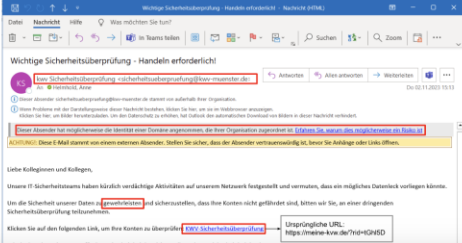
### Wie hätten Sie den Betrug entdecken können?

**Als kleiner Merksatz gilt der Phishing-WALD:**

- W**ortwahl
- A**bsender
- L**inks und Anhänge
- D**ateneingabe



Mit einem Klick auf die rot markierten Umrandungen erhalten Sie Hinweise zu den Erkennungsmerkmalen der empfangenen Phishing-Mail.



# // Alternative Formate

The screenshot shows an Outlook window titled "Bitte um Bestätigung des neuen Rechnungseingangs - Nachricht (HTML)". The ribbon includes "Datei", "Nachricht", and "Hilfe". The "Nachricht" ribbon is active, showing options like "Löschen", "Archivieren", "Antworten", "Allen antworten", "Weiterleiten", "In Teams teilen", "Alle Apps", "QuickSteps", "Verschieben", "Markierungen", "Bearbeiten", "Plastisch", "Übersetzen", "Zoom", "Mit Terminabfrage antworten", and "Nachricht melden".

The email content is as follows:

**Bitte um Bestätigung des neuen Rechnungseingangs**

Rechnungseingang <eRechnung@kvw-muenster.de>  
An Helmhold, Anne  
Mo 24.06.2024 15:23

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.  
Wir konnten die Identität des Absenders nicht verifizieren. Klicken Sie hier, um weitere Informationen zu erhalten.  
Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Rechnung\_06\_2024\_037221805.pdf  
99 KB

Hallo Anne Helmhold,

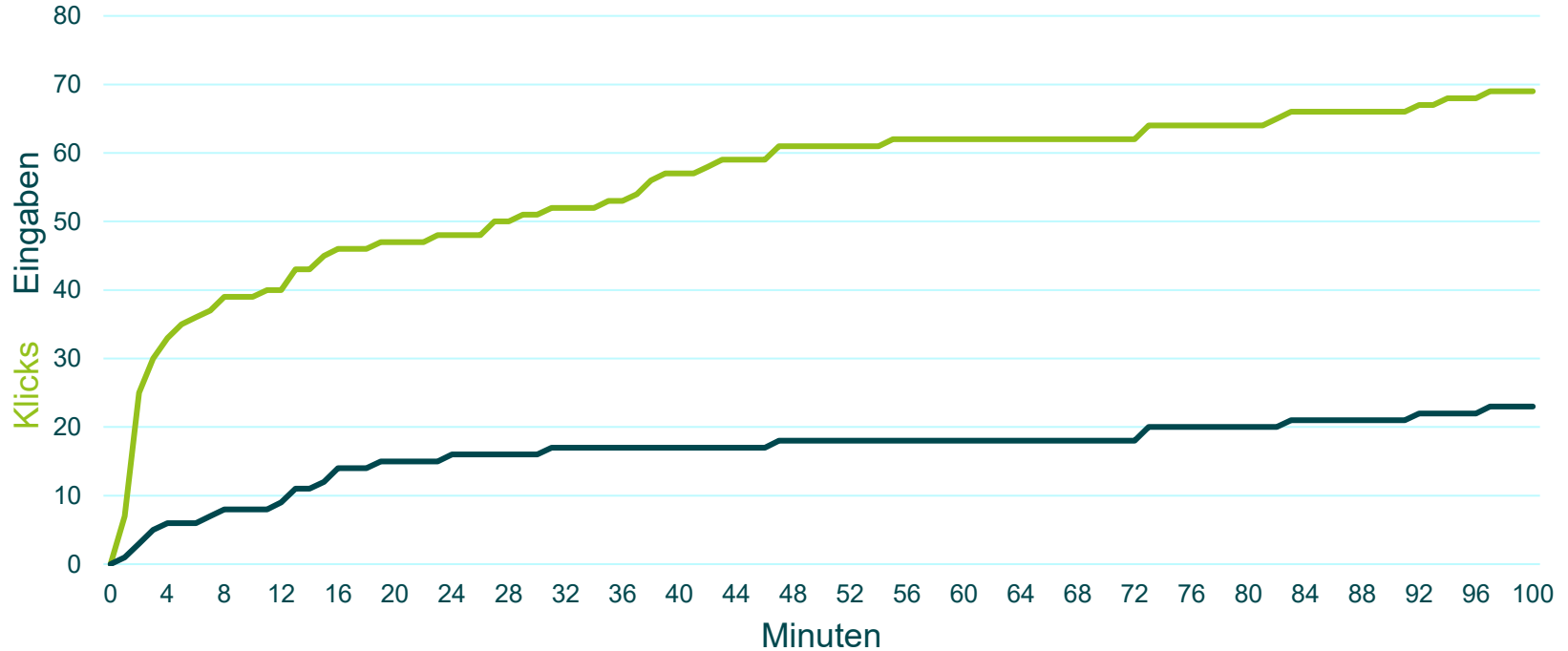
bitte überprüfen Sie, ob die im Anhang befindliche Rechnung korrekt ist und senden Sie zur Freigabe eine Bestätigungsmail.

Vielen Dank!

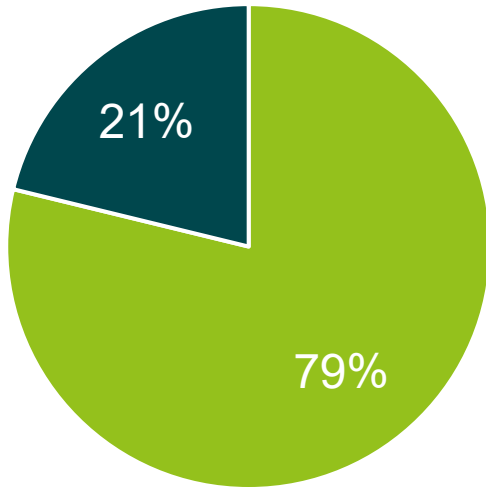
Mit freundlichen Grüßen  
Im Auftrag  
kvw-Controlling

**KONTAKT**  
Kommunale Versorgungskassen Westfalen-Lippe  
kvw-Controlling  
Zumsandstraße 12 // 48145 Münster  
Tel. [0251 591-6749](tel:02515916749) // Fax [0251 591-5915](tel:02515915915)  
[eRechnung@kvw-muenster.de](mailto:eRechnung@kvw-muenster.de)  
[www.kvw-muenster.de](http://www.kvw-muenster.de)  
[karriere.kvw-muenster.de](http://karriere.kvw-muenster.de) // [kvw-muenster.de/youtube](http://kvw-muenster.de/youtube) // [kvw-muenster.de/beihilfe-app](http://kvw-muenster.de/beihilfe-app)

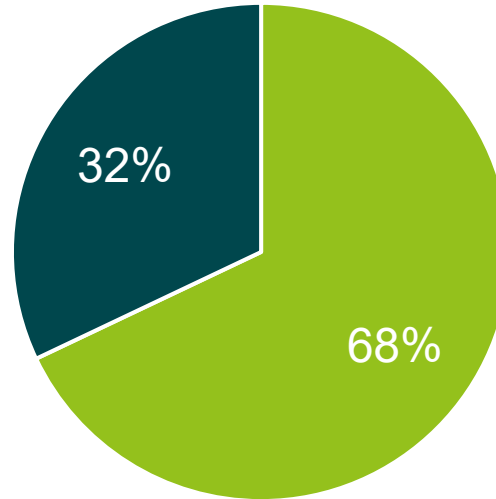
## // Messinstrument: Klickzahlen



## // Messinstrument: Datenangaben & Reports



■ Link nicht angeklickt   ■ Link angeklickt



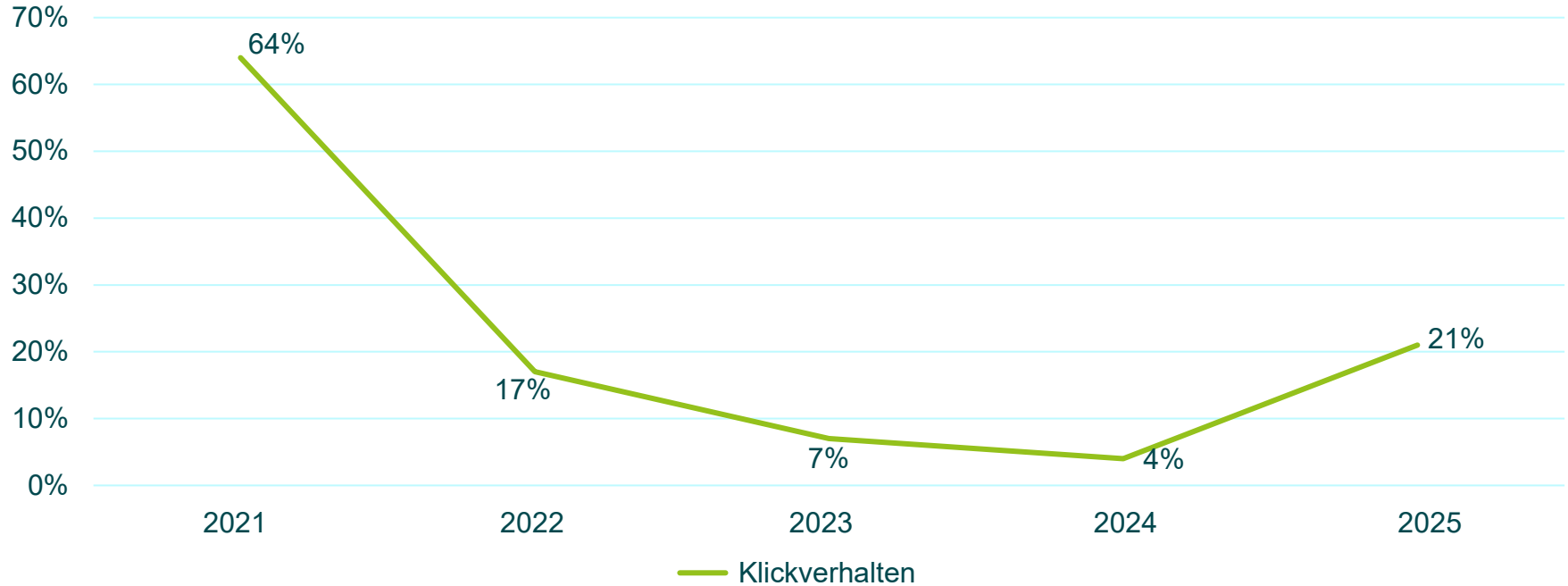
■ Zugangsdaten nicht eingegeben   ■ Zugangsdaten eingegeben

47

Reports in Outlook

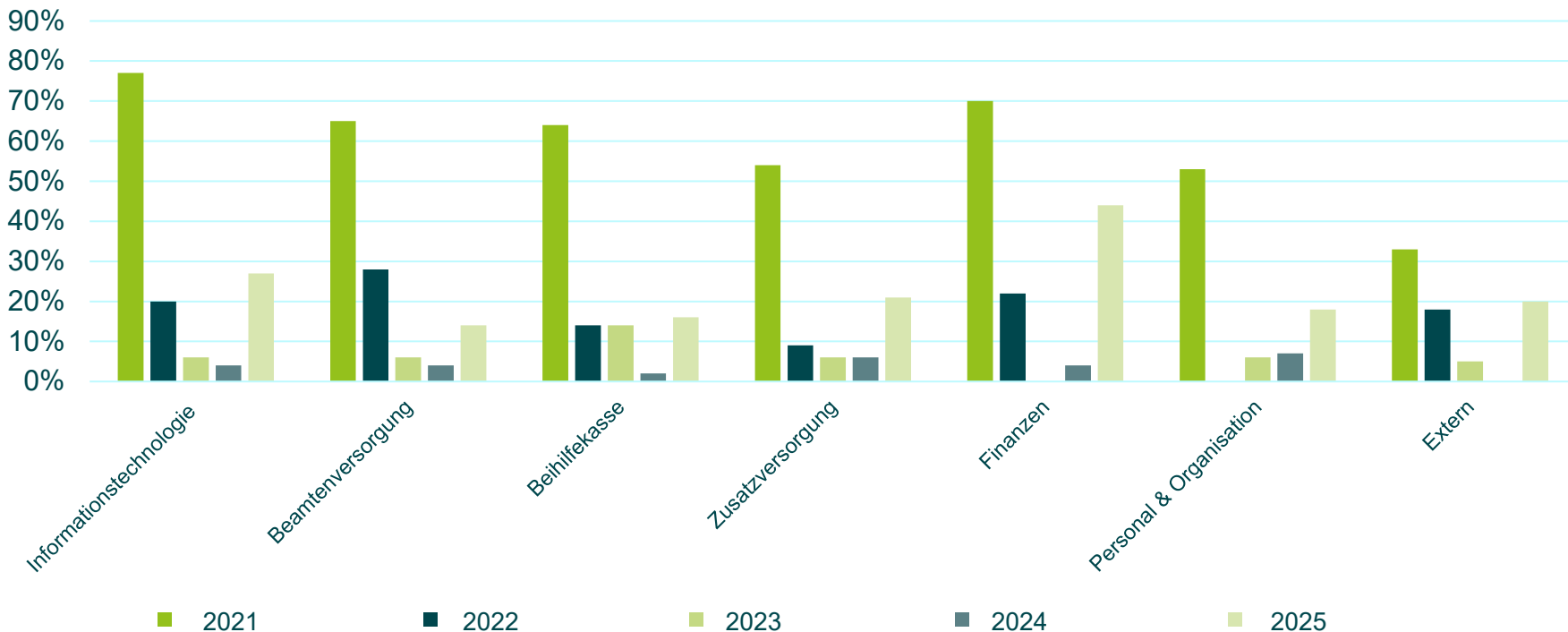
// 🔍 Und was hat's gebracht?

## // Klickraten im zeitlichen Verlauf



# // Klickraten je Unternehmensbereich

ca. 450 Mitarbeitende



## // Auf der Tonspur:

*„Klar strukturierte und umsetzbare Richtlinien.“*

*„Hilft mir auch privat, mich und meine Familie besser zu schützen!“*

*„Überraschend praxisnahe Schulung – einiges konnte ich direkt im Job anwenden!“*

*„Ich schaue mir E-Mail deutlich kritischer an!“*



*„Ich weiß jetzt, wie ich mich im Ernstfall richtig verhalte!“*

*„Ich weiß an wen ich mich wenden kann, wenn etwas verdächtig ist.“*

*„Habe ein besseres Gefühl für aktuelle Bedrohungen“*

*„Wir sprechen im Team offener über Sicherheit.“*

## // Ein kleiner Ausblick

### Trends und Regulatorik im Blick behalten



Künstliche Intelligenz & neue Technologien



Wandelnde regulatorische Anforderungen

### Wir haben noch einige Ideen!



USB-Drop-Kampagnen



Physische Security Awareness



Neue Phishing-Varianten

Voice-Phishing / QR-Code-Phishing / Deepfakes



Aufbau einer Community of Practice



*Kein Projekt, sondern ein fortlaufender Prozess!*

## // Auflösung des Ratespiels



- ✓ Vertrauliche Dokumente offen sichtbar
- ✓ Zugangsdaten einsehbar
- ✓ Computer nicht gesperrt