PHISHING-SIMULATOR

Phishing erkennen, bevor es teuer wird

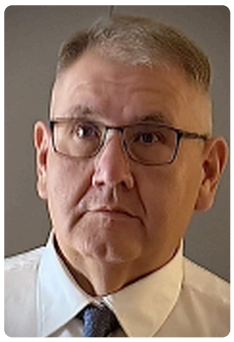
Wissen, Quiz und realistische Übung im simulierten Posteingang – vollständig simuliert, ohne echte Mails.

Angriffe über alle Kanäle – sicher geübt

- E-Mail
- SMS
- Chat
- QR-Code
- Social Engineering

Simulator
Wissen · Quiz
Übung

- CEO-Fraud
- Rechnungsbetrug
- MFA-Fatigue
- Quishing
- Paket-SMS



Heinrich Markus Schulte
IT-Auditor · Sachverständiger

Rund 500 Szenarien
E-Mail · SMS · Chat · QR-Code
Realistisch geübt. Keine echten Daten. Messbar.

Erst verstehen. Dann üben. Dann sicher entscheiden.

Der Lernweg im Phishing-Simulator

Wissen – Infografiken → **Quiz** – 75 % zum Bestehen → **Posteingang** – echt oder Phishing? → **Entscheidung** – melden · löschen · trauen → **Feedback** – Merkmale erklärt

Auswertung je Person und anonymisierter Management-Bericht

Häufigster Einstieg
Phishing und Social Engineering stehen am Anfang sehr vieler Sicherheitsvorfälle.

Sicher simuliert
Keine echten Mails, keine Zugangsdaten, fiktive Inhalte – datenschutzfreundlich.

Messbar
Serverseitige Auswertung und ein Bericht, den die Leitung versteht.

~500	4	3	75 %	0	PDF
Szenarien	Kanäle	Stufen	Bestehen	echte Mails	Management-Bericht

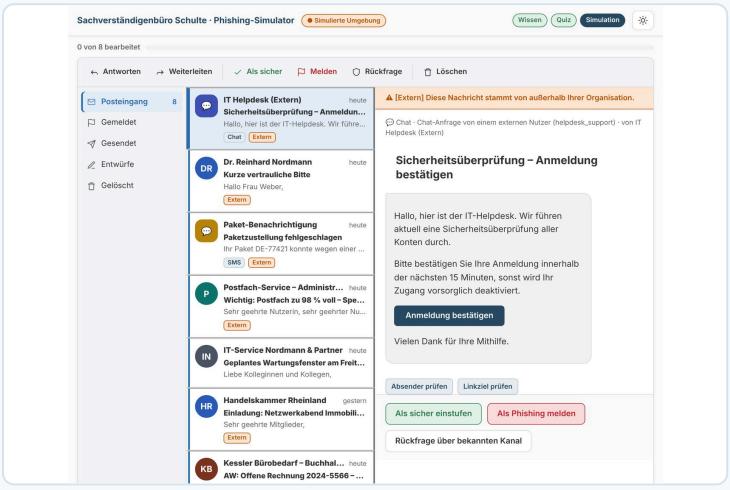
Testzugang oder Demo anfragen

Schulungsseite öffnen

12 Monate Zugang einschließlich Updates · vollständig simuliert, keine echten Mails · DSGVO-freundlich, ohne Werbe-Tracker

Phishing ist kein Pech, sondern Methode.

Warum Erkennen trainiert werden muss – nicht nur erklärt



Der simulierte Posteingang: Jede Nachricht wird geprüft und entschieden – mit sofortiger Erklärung der Merkmale.

Angreifer imitieren Vorgesetzte, Lieferanten, Paketdienste und Cloud-Anbieter – per E-Mail, SMS, Chat oder QR-Code. Wer die Merkmale nur einmal im Jahr auf einer Folie sieht, erkennt sie im Alltag selten. Erkennen ist eine Fertigkeit, und Fertigkeiten entstehen durch Übung.

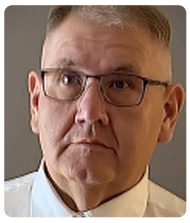
Der Phishing-Simulator führt in drei Stufen dorthin: Ein didaktischer Wissensteil mit Infografiken erklärt Anatomie, Kanäle und Maschen. Ein Quiz sichert das Verständnis. Danach entscheiden die Teilnehmenden in einem realistischen Posteingang, welche Nachrichten echt sind – und erhalten zu jeder Entscheidung eine Erklärung.

Alles ist vollständig simuliert: Es werden keine echten Mails versendet, keine Zugangsdaten abgefragt und keine Personen bloßgestellt. Die Landeseiten zeigen, was passiert wäre – ohne Datenabfrage.

RECHTSRAHMEN & BEZÜGE

§ 30 BSIG · **Art. 21 NIS-2-RL** · **DSGVO-freundlich** · **keine Bloßstellung**

Alle Szenarien sind fiktiv. Individualisierte Szenarien für Ihr Unternehmen sind als Add-on möglich.



PRÜFERBLICK

Heinrich Markus Schulte
IT-Auditor · Sachverständiger
CISA · CISM · CIPP/E · CEH · T.I.S.P.

> *Ein guter Phishing-Test beschämt niemanden. Er macht sichtbar, wo Wissen fehlt – und schließt die Lücke sofort.*

MASCHEN KENNEN

CEO-Fraud, Rechnungsbetrug, MFA-Fatigue, Quishing, gefälschte Paket- und Cloud-Nachrichten.

MERKMALE PRÜFEN

Absender, Domain, Links, Anhänge, Druck und Tonfall – im Detail erklärt.

RICHTIG REAGIEREN

Melden statt löschen, nicht antworten, nicht anrufen – und im Zweifel nachfragen.

WIRKUNG MESSEN

Ergebnis je Person, Bescheinigung und anonymisierter Bericht für die Leitung.

Fragen, die Aufsicht und Prüfer stellen

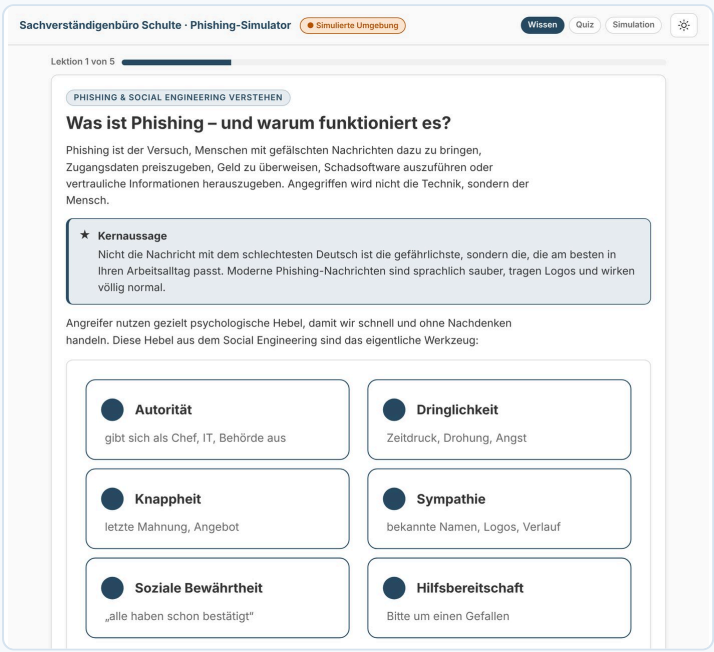
- Wie wird die Phishing-Resilienz der Beschäftigten gemessen?
- Werden alle Kanäle berücksichtigt – auch SMS, Chat und QR-Codes?
- Wie erfährt die Leitung, ob die Sensibilisierung wirkt?
- Wie werden die Persönlichkeitsrechte der Teilnehmenden gewahrt?

Verstehen · Üben · Entscheiden · Melden · Messen · Verbessern

PHISHING-SIMULATOR

Ablauf, Nutzen und Pakete

Wissen, Quiz und Übung – mit Auswertung für Teilnehmende und Leitung



Der Wissensteil: Phishing-Merkmale und Maschen mit Infografiken anschaulich erklärt.

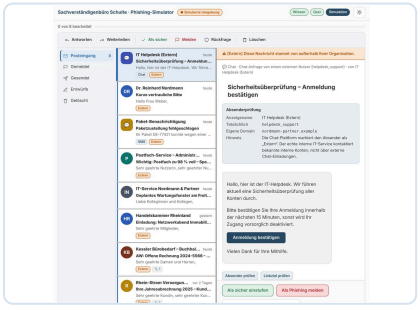
Was Sie lernen

1. **Anatomie einer Phishing-Nachricht**
   Absender, Betreff, Link, Anhang, Handlungsdruck
2. **Kanäle**
   E-Mail, SMS (Smishing), Chat, QR-Code (Quishing)
3. **Maschen**
   CEO-Fraud, Rechnungsbetrug, MFA-Fatigue, Paketdienst
4. **Links prüfen**
   die echte Domain erkennen, Subdomain-Tricks
5. **Übung im Posteingang**
   echte und gefälschte Nachrichten unterscheiden
6. **Melden & Feedback**
   richtig reagieren, Erklärung zu jeder Entscheidung

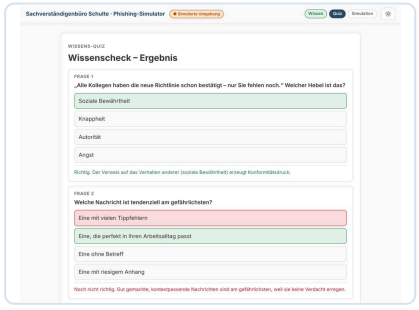
FÜR WEN **Alle Beschäftigten – besonders Buchhaltung, Einkauf, Assistenz, Personal und Leitung**

IHR MEHRWERT

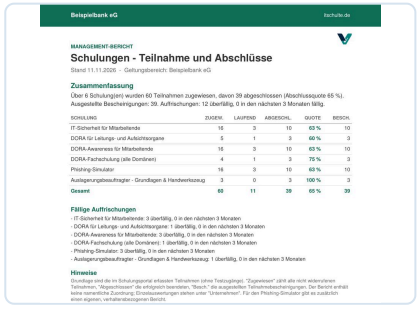
- **Realistisch**
  Rund 500 Szenarien über vier Kanäle.
- **Fair & sicher**
  Vollständig simuliert, keine echten Daten.
- **Lernwirksam**
  Sofortige Erklärung zu jeder Entscheidung.
- **Steuerbar**
  Management-Bericht für die Leitung als PDF.



Merkmale im Detail prüfen



Wissenscheck mit Auswertung



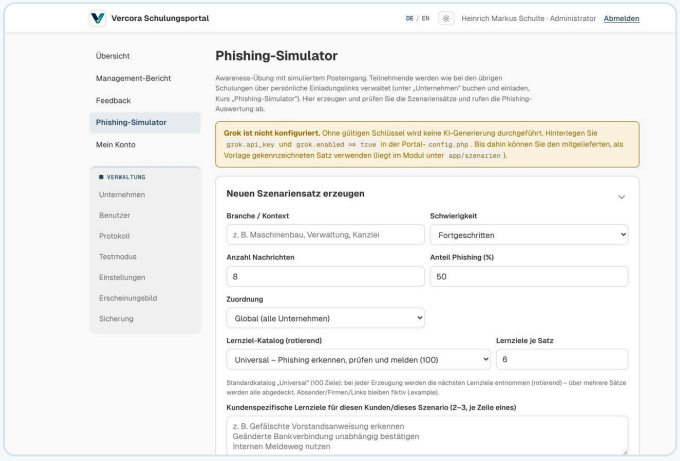
Management-Bericht im Kundendesign

PAKET & BUCHUNG Teil des Basispakets für alle Beschäftigten (mit IT-Sicherheit und Datenschutz für Mitarbeitende) · individualisierte Phishing-Szenarien als Add-on zum Abo.

So läuft es ab

Von der Einladung bis zum Management-Bericht

Im Vercora Schulungsportal inklusive



- **Teilnehmerverwaltung:** Plätze buchen, Personen anlegen, persönliche Einladungslinks ohne Passwort
- **Fortschritt & Management-Bericht:** Teilnahme, Abschlüsse und fällige Auffrischungen als PDF für die Leitung
- **Nummerierte Bescheinigung:** PDF mit Online-Echtheitsprüfung, Protokoll und eigenem Nummernkreis
- **Wiederholungsintervall:** je Schulung 6, 12, 24 oder 36 Monate – das Portal zeigt, wann nachgeschult wird
- **Ihr Erscheinungsbild:** auf Wunsch mit Ihrem Logo und Ihrer Farbe – auch auf Bescheinigung und Bericht
- **Sicher & datensparsam:** Anmeldung mit zweitem Faktor, Hash-Ketten-Protokoll, keine Werbe-Tracker

Der Schulungsprozess im Überblick

1 Buchen
Basispaket für alle Beschäftigten

2 Lernen
Wissen und Quiz mit 75 %-Grenze

3 Anwenden
Entscheidungen im Posteingang

4 Nachweisen
Bescheinigung je Person, Bericht

5 Auffrischen
Auffrischung mit neuen Szenarien

Was Sie erhalten

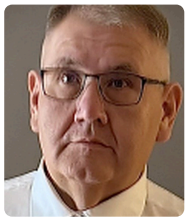
Rund 500 Szenarien
E-Mail, SMS, Chat und QR-Code mit realistischen Maschen

Wissensteil mit Infografiken
Anatomie, Kanäle, Maschen und Prüfschritte

Auswertung
serverseitig je Person, nummerierte Bescheinigung

Management-Bericht
anonymisiert, als PDF im Erscheinungsbild Ihres Unternehmens

PRÜFERBLICK



Heinrich Markus Schulte
IT-Auditor · Sachverständiger
CISA · CISM · CIPP/E · CEH · T.I.S.P.

Was die Leitung braucht, ist kein Pranger, sondern ein Lagebild: Wo stehen wir, und wo müssen wir nachschulen?

Demo oder Testzugang anfragen

itschulte.de/schulungen.html

Sachverständigenbüro Schulte
Grünberger Weg 9 · 40627 Düsseldorf · +49 211 93375777 · sachverstaendiger@itschulte.de