co-IT.eu GmbH • Kriegsstraße 39 • 76133 Karlsruhe
info@co-IT.eu • +49-721-935163-054

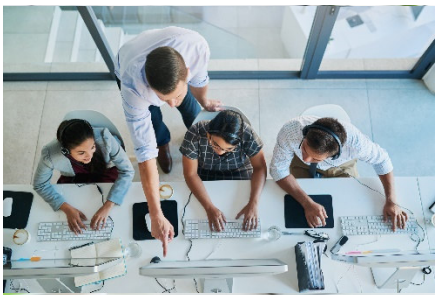
Cyber Lounge

Leistungsumfang

Letzte Aktualisierung: 23.02.2024

co-IT.eu GmbH • Kriegsstraße 39 • 76133 Karlsruhe
info@co-IT.eu • +49-721-935163-054

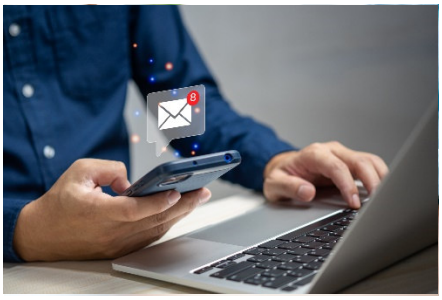
6 Kurse mit 4 Examen



Effektives Basiswissen

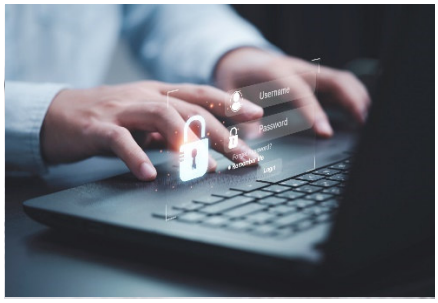
In diesem Kurs sind wertvolle Tipps und Tricks für das tägliche Arbeiten gebündelt. Angefangen beim Basiswissen über Dateiformate und Webseitenadressen, über Datenschutz mit Alexa bis hin zur sauberen Trennung zw. geschäftlichen und privaten Aspekten.

✓ Mit Examen und Anwenderzertifikat



Sicher per E-Mail kommunizieren

In diesem Kurs werden zunächst die theoretischen Grundlagen zur sicheren Kommunikation erläutert, bevor in einem Praxisvideo das Gelernte angewendet wird.

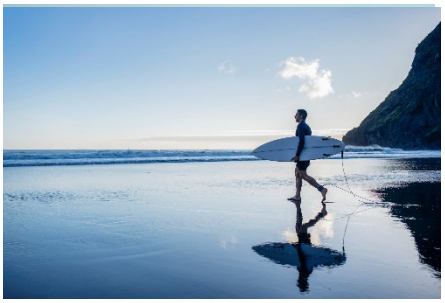


Endlich sichere Passwörter

Komplexe Passwörter ganz einfach merken: Mit den in diesem Kurs vermittelten Merktechniken ist das kein Problem. Außerdem zeigen wir Fortgeschrittenen moderne Softwarelösungen.

✓ Mit Examen und Anwenderzertifikat

co-IT.eu GmbH • Kriegsstraße 39 • 76133 Karlsruhe
info@co-IT.eu • +49-721-935163-054



Jederzeit sicher surfen

In diesem Kurs lernen Sie, woran Sie seriöse, sichere Webseiten erkennen und wie Sie beim Surfen keine Spuren hinterlassen.

✓ Mit Examen und Anwenderzertifikat

Augen auf beim Onlinebanking

Nach Durchführung dieses Kurses haben Sie das Wissen über die Auswahl geeigneter Produkte und Legitimierungsverfahren und Sie sind für Sicherheitsrisiken sensibilisiert, die auf technischer oder prozessualer Ebene bestehen.

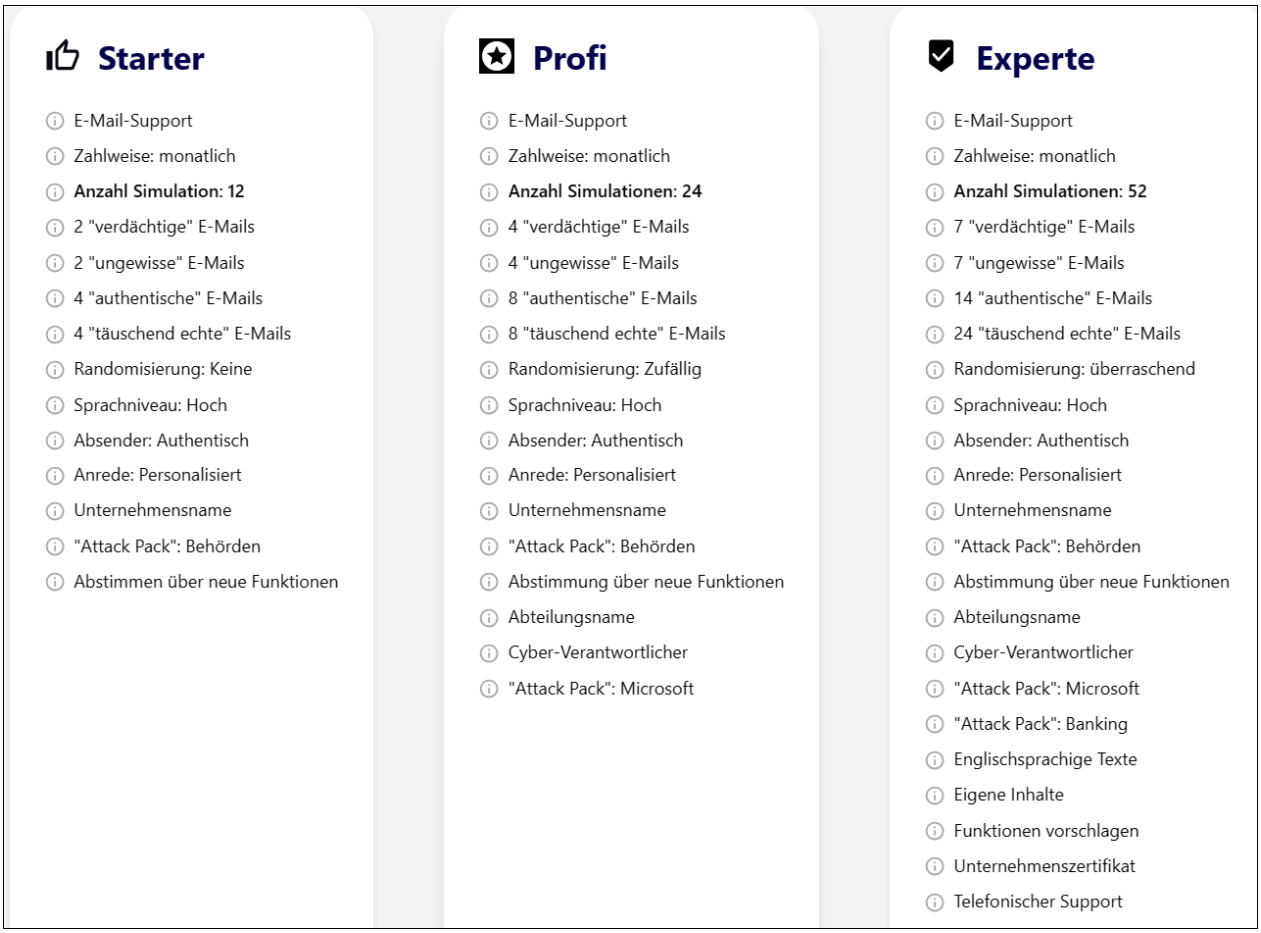
Schnelleinstieg Datenschutz

Mit diesem Kurs erhalten Sie einen schnellen Einstieg in die Datenschutzgrundverordnung, über Recht von Betroffen und Pflichten von Datenverarbeitern.

✓ Mit Examen und Anwenderzertifikat

co-IT.eu GmbH • Kriegsstraße 39 • 76133 Karlsruhe
info@co-IT.eu • +49-721-935163-054

Phishing-Simulationen



Starter

- E-Mail-Support
- Zahlweise: monatlich
- **Anzahl Simulation: 12**
- 2 "verdächtige" E-Mails
- 2 "ungewisse" E-Mails
- 4 "authentische" E-Mails
- 4 "täuschend echte" E-Mails
- Randomisierung: Keine
- Sprachniveau: Hoch
- Absender: Authentisch
- Anrede: Personalisiert
- Unternehmensname
- "Attack Pack": Behörden
- Abstimmen über neue Funktionen

Profi

- E-Mail-Support
- Zahlweise: monatlich
- **Anzahl Simulationen: 24**
- 4 "verdächtige" E-Mails
- 4 "ungewisse" E-Mails
- 8 "authentische" E-Mails
- 8 "täuschend echte" E-Mails
- Randomisierung: Zufällig
- Sprachniveau: Hoch
- Absender: Authentisch
- Anrede: Personalisiert
- Unternehmensname
- "Attack Pack": Behörden
- Abstimmung über neue Funktionen
- Abteilungsname
- Cyber-Verantwortlicher
- "Attack Pack": Microsoft

Experte

- E-Mail-Support
- Zahlweise: monatlich
- **Anzahl Simulationen: 52**
- 7 "verdächtige" E-Mails
- 7 "ungewisse" E-Mails
- 14 "authentische" E-Mails
- 24 "täuschend echte" E-Mails
- Randomisierung: überraschend
- Sprachniveau: Hoch
- Absender: Authentisch
- Anrede: Personalisiert
- Unternehmensname
- "Attack Pack": Behörden
- Abstimmung über neue Funktionen
- Abteilungsname
- Cyber-Verantwortlicher
- "Attack Pack": Microsoft
- "Attack Pack": Banking
- Englischsprachige Texte
- Eigene Inhalte
- Funktionen vorschlagen
- Unternehmenszertifikat
- Telefonischer Support

Funktionen	Erläuterungen
Schwierigkeitsstufen (Klickquoten): „verdächtige“ „ungewisse“ „authentische“ „täuschend echte“	Unsere Phishing-Simulationen werden vorab in einer Testgruppe aus mehreren Unternehmen mit über 300 Anwendern einem Praxischeck unterzogen. Anhand der Ergebnisse in unserer Testgruppe unterscheiden wir "verdächtige" (>20%), "ungewisse" (>40%), "authentische" (>60%) und "täuschend echte" (>80) Klickquoten. Alles unter 20% erhalten Sie gar nicht erst.

co-IT.eu GmbH • Kriegsstraße 39 • 76133 Karlsruhe
info@co-IT.eu • +49-721-935163-054

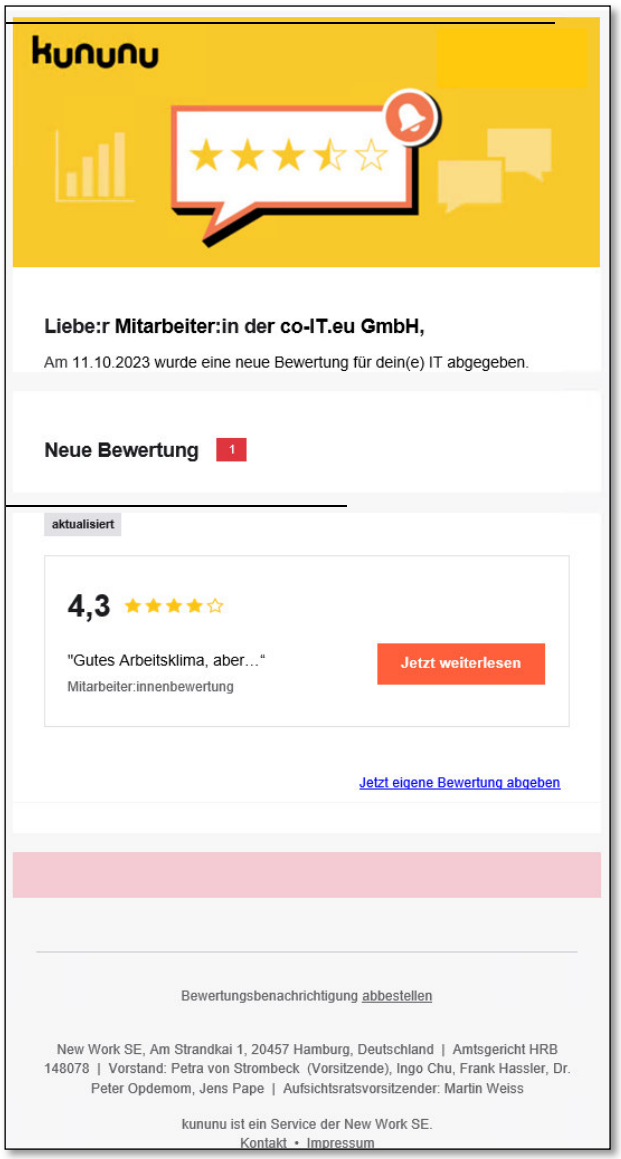
Randomisierung: Keine	Alle Anwender erhalten zur gleichen Zeit die gleiche Simulation - die gleiche Simulation, aber zu zufälligen Zeiten über Tage verteilt - unterschiedliche Simulationen zu unterschiedlichen Zeiten
Randomisierung: Zufällig	Alle Anwender erhalten die gleiche Simulation, aber zu zufälligen Zeiten über Tage verteilt
Randomisierung: Überraschend	Alle Anwender erhalten unterschiedliche Simulationen zu unterschiedlichen Zeiten
Sprachniveau: Hoch	Das Sprachniveau variiert zw. niedrig und hoch. Bei mittlerem Niveau wird korrekte Rechtschreibung und Grammatik benutzt. Auf hohem Sprachniveau wird zusätzlich auf eine klare Semantik und Plausibilität geachtet.
Absender: Authentisch	Authentische Absenderadressen sind z.B. Domains wie "bundesgerichtshof-karlsruhe.de" oder "bund-und-laender.online", wohingegen eine Domäne wie "why-how-what.info" weniger echt wirkt.
Anrede: Personalisiert	In den Phishing Simulationen wird der Name des Empfängers in der Anrede verwendet, also z.B. "Sehr geehrter Herr Tim Kater".
Unternehmensname	In den Phishing Simulationen wird Ihr Unternehmen referenziert, z.B. indem in einer Simulation eine "Kununu"-Bewertung zu Ihrer Firma nachgestellt wird.
„Attack Pack“: Behörden	Arbeitsrecht, Elternzeit, Unfallversicherung: Diese Inhalte interessieren praktisch jeden und haben eine hohe Klickquote.
„Attack Pack“: Microsoft	Microsoft verschickt regelmäßig Nachrichten zu Produkten wie Teams und Outlook. In diesen Simulationen versenden wir entsprechende Kopien.
„Attack Pack“: Banking	Speziell bei betrügerischen Zahlungsaufforderungen kann es schnell zu finanziellen Schäden kommen. Mit diesen

co-IT.eu GmbH • Kriegsstraße 39 • 76133 Karlsruhe
info@co-IT.eu • +49-721-935163-054

	Simulationen sollen Rechnungswesen und Einkauf gesondert sensibilisert werden.
Abstimmung über neue Funktionen	Ihre Stimme zählt: Sie können regelmäßig über die Priorisierung von neuen Funktionen mit abstimmen.
Abteilungsname	In den Phishing Simulationen wird die Abteilung des Empfängers referenziert, z.B. indem eine "Datenschutzbefragung" im "Einkauf" simuliert wird.
Cyber-Verantwortlicher	In den Phishing Simulationen wird der Name des Cyber-Verantwortlichen angedruckt, z.B. dass "Reinhold Müller" via OneDrive eine Datei mit dem Empfänger geteilt hat.
Englischsprachige Texte	Einige Phishing Simulationen werden in englischer Sprache verfasst. Das hilft Unternehmen, die regelmäßig mit dem Ausland korrespondieren.
Eigene Inhalte	Bei einer entsprechend großen Zahl an Empfänger können wir für Sie gezielt Inhalte einsteuern. Sprechen Sie uns darauf an.
Funktionen vorschlagen	Teilen Sie Ihre Ideen unserem Entwicklungsteam mit.
Unternehmenszertifikat	Nach 12 Monaten erhalten Sie ein auf Ihr Unternehmen ausgestelltes Zertifikat, das die kontinuierliche Sensibilisierung durch unsere Phishing Simulationen nachweist.

co-IT.eu GmbH • Kriegsstraße 39 • 76133 Karlsruhe
info@co-IT.eu • +49-721-935163-054

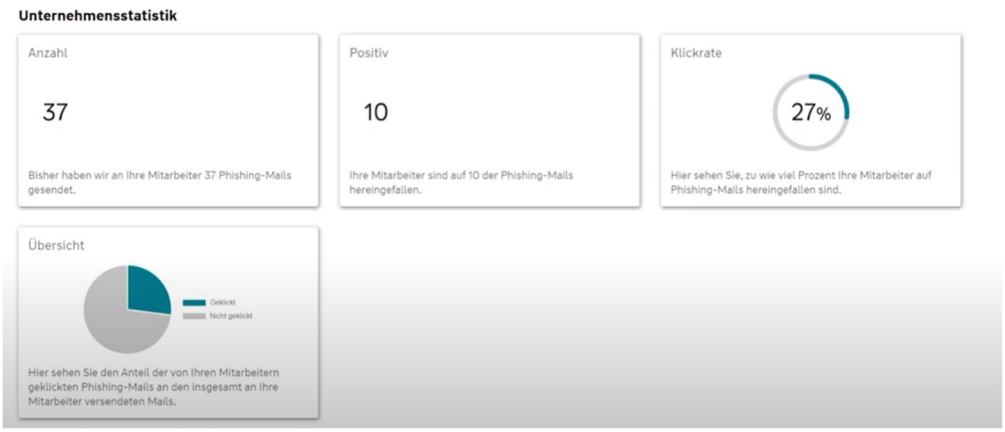
Gemäß gebuchtem Paket werden den Anwendern Ihres Unternehmens Phishing E-Mails als Sensibilisierungs-Training versandt. Hier werden unter anderem der Firmenname und der Name Ihres Cyber-Verantwortlichen dynamisch verarbeitet, sodass die Phishing E-Mails einem echten Angriff gleichen, der öffentlich zugängliche Daten verwenden würde.



co-IT.eu GmbH • Kriegsstraße 39 • 76133 Karlsruhe
info@co-IT.eu • +49-721-935163-054

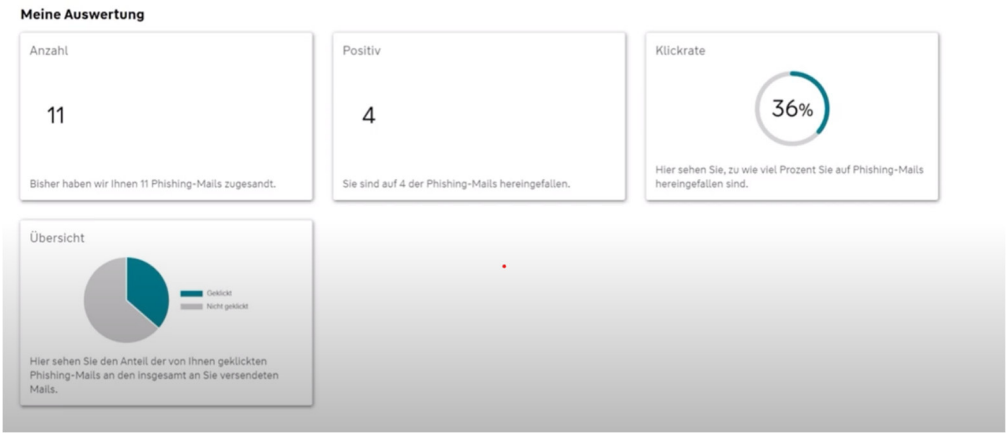
Statistiken

Unternehmensstatistik für Cyber-Verantwortlichen



Unter dem Menüpunkt Phishing-Simulationen gibt es für die Cyber-Verantwortlichen einsehbare Statistiken auf Unternehmensebene, um Risiken zu erkennen - unter anderem das Verhältnis von empfangenen Phishing-Simulationen zu geklickten.

Anwenderstatistik



Unter dem Menüpunkt Phishing-Simulationen sehen Anwender eine Auswertung zu den von uns an sie versendeten Phishing-Simulationen. Sie haben unter anderem Einsicht über die Anzahl der verschickten Phishing E-Mails und den davon erfolgreichen Angriffen. Außerdem haben Sie

co-IT.eu GmbH • Kriegsstraße 39 • 76133 Karlsruhe
info@co-IT.eu • +49-721-935163-054

beispielsweise eine Klickrate in Prozent sowie eine komplette Übersicht in Form eines Kreisdiagramms.

Der Datenschutz aller Anwender wird gewahrt und die Ergebnisse einzelner Personen können nicht nachvollzogen werden.

Werkzeugkasten

In dem integrierten Werkzeugkasten finden Sie beispielsweise ein Passwort-Check-Tool, mit dem Sie auf sichere Weise prüfen können, ob Ihr Passwort in Hackerdatenbanken gespeichert ist.

Unternehmenszertifikat

Nach Durchführung der Sensibilisierungs-Trainings erhalten Sie ein Unternehmenszertifikat, welches bestätigt, dass Sie unsere eLearning Plattform sowie Phishing-Simulationen nutzen, um die eigene Cybersicherheit und -hygiene zu verbessern und Ihre Anwender kontinuierlich im Umgang mit Cyber-Bedrohungen zu sensibilisieren.

co-IT.eu GmbH • Kriegsstraße 39 • 76133 Karlsruhe
info@co-IT.eu • +49-721-935163-054

Nutzerverwaltung für Cyber-Verantwortliche

In der Nutzerverwaltung haben Sie beispielsweise die Möglichkeit, sowohl manuell Nutzer über die Eingabe der E-Mail-Adressen als auch über einen Massenimport per CSV-Datei einzuladen.