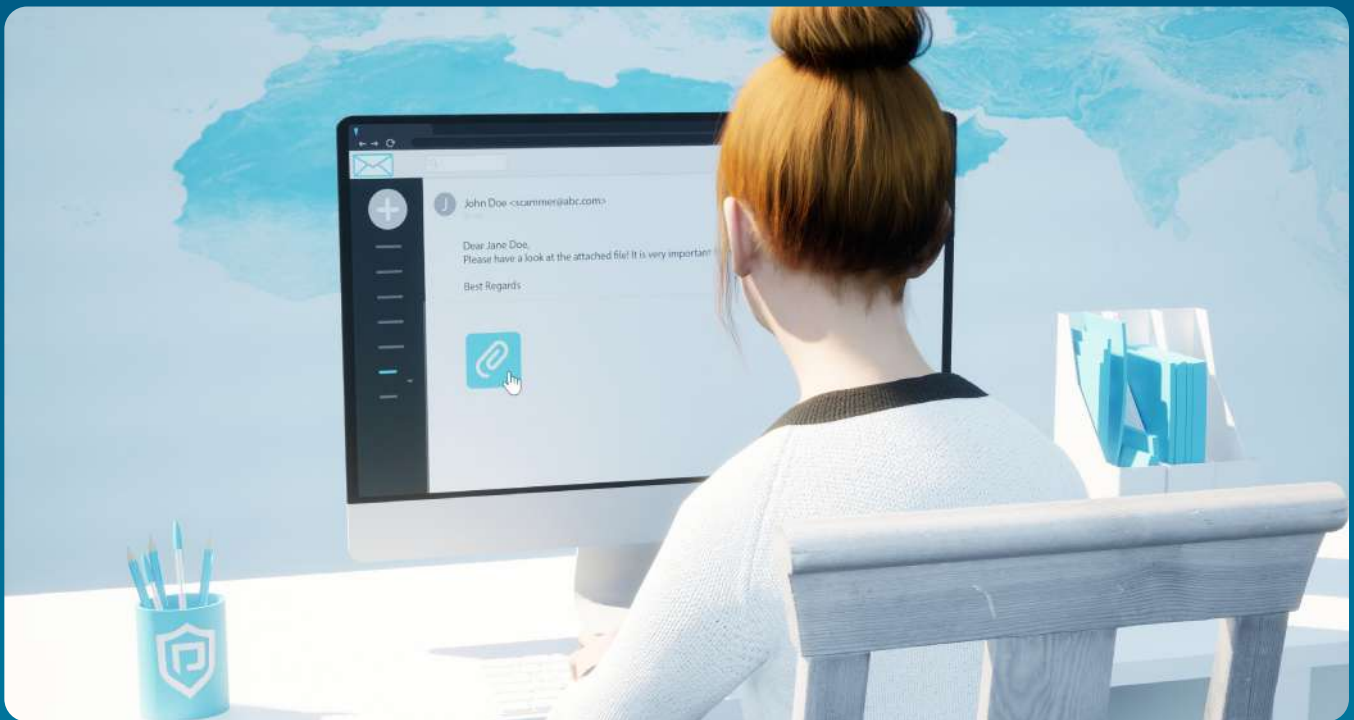




Protectly
BY SMART STUDY

Was ist Protectly?



Protectly – Die europäische Plattform für Security Awareness, Phishing-Simulationen und KI-gestützte Social-Engineering-Prävention

Protectly unterstützt Sie dabei, Ihre Mitarbeitenden wirksam vor modernen Cyberangriffen zu schützen. Die Kombination aus realistischen Simulationen, klaren Analysen und interaktiven Trainings macht die Sicherheitskultur Ihrer Organisation messbar und stärkt sie nachhaltig.

Unsere Plattform kombiniert:

- Multi-Channel-Phishing-Simulationen (E-Mail, SMS, WhatsApp, QR-Code, Voice/AI-Calls)
- Deepfake-Simulationen
- Automatisierte Zuweisung von Awareness-Trainings
- Ein Lernmanagementsystem für E-Learning, Seminare, Phishingkampagnen & Simulationsanalysen
- Ein Autorentool zur Erstellung von eigenen Trainingsinhalten
- Über 30 Awareness-Kurse in 2D/3D, barrierefrei und DSGVO-konform

Wie entsteht Awareness?

Damit Ihre Mitarbeitenden Cyber-Awareness entwickeln und somit den IT-Schutz Ihres Unternehmens stärken, kombiniert Protectly drei Komponenten:

Social-Engineering-Simulationen

Führen Sie realistische Simulationen durch, um zu erkennen, wie Ihre Mitarbeitenden in Alltagssituationen reagieren.

- E-Mail-Simulationen
- QR-Code-Simulationen
- Deepfake-Meetings
- Voice-Agent-Simulationen
- Videobotschaften & Sprachnachrichten



Simulationsanalysen

Analysieren Sie, wo Risiken für Ihr Unternehmen bestehen.

- Klickraten
- Öffnungsraten
- Dateneingaberaten
- Melderaten



Awareness-Trainings

Trainieren Sie Ihre Mitarbeitenden mit den passenden Lernmodulen.

- 2D & 3D E-Learnings
-  Datenschutz- & Informationssicherheitskurse
- Lern-Badges & Bestenlisten
- Lernzertifikate



Social-Engineering-Simulationen

Realistische Angriffe. Messbare Ergebnisse. Höchste Wirksamkeit.

Cyberangriffe sind heute so gut gemacht, dass sie kaum noch von echten Nachrichten, Videoanrufen oder Sprachnachrichten zu unterscheiden sind. PROTECTLY simuliert diese modernen Angriffsformen unter realistischen Bedingungen – sicher, DSGVO-konform und vollständig automatisiert.

E-Mail-Simulationen

Realistisch gestaltete Phishing-Mails prüfen das Verhalten im Arbeitsalltag und zeigen, wie Mitarbeitende auf täuschend echte Nachrichten reagieren. Die Analyse umfasst Öffnungs-, Klick-, Eingabe- und Downloadraten und macht Risikobereiche klar sichtbar.

QR-Code-Simulationen

Simulieren alltägliche Situationen im Büro oder unterwegs und prüfen, wie Mitarbeitende mit QR-Codes umgehen. Ideal, um Sicherheitsrisiken in Meetingräumen, auf Dokumenten oder in E-Mails aufzudecken.

Live-Deepfake-Meetings

Gefälschte Videocalls zeigen, wie leicht sich visuelles Vertrauen missbrauchen lässt. Mitarbeitende erleben realistisch, wie Deepfake-Führungskräfte oder Kolleg*innen Anweisungen erteilen.

Social-Engineering-Simulationen

Voice-Agent-Simulationen

KI-generierte Stimmen wirken vertraut und überzeugend. Diese Simulationen testen, wie gut Mitarbeitende in scheinbar echten Telefonanrufen auf verdächtige Anfragen reagieren

Videobotschaften & Sprachnachrichten

Täuschend echt erzeugte Video- oder Audio-Nachrichten schaffen Druck- oder Stresssituationen. Sie eignen sich ideal, um zu prüfen, wie souverän Mitarbeitende mit KI-basierten Täuschungen umgehen.

Phishing-Simulationen

Mit Protectly erstellen Sie in nur wenigen Schritten täuschend echt wirkende Phishing-Simulationen und Landingpages!

Diese Simulationen werden dann automatisiert an Ihre Mitarbeitenden versendet.



Templates für Simulationen

Protectly bietet zahlreiche vorgefertigte Templates für Phishing-Simulationen an. Falls kein passendes Template dabei ist, kreieren Sie einfach in wenigen Sekunden Ihre eigene Phishing-Simulation, ganz in Ihrem gewünschten Look!

Automatisierte Versendung

Welche Abteilung wann und wie oft einen vorgetäuschten Phishing-Angriff erhält und erkennen muss, ist flexibel einstellbar. Sie möchten unterschiedliche Phishing-E-Mails gleichzeitig aussenden? Mit Protectly ist auch das kein Problem. Und das Beste: **Alles funktioniert automatisiert!**

Information

Wird auf den Link in der simulierten Phishing E-Mail geklickt oder werden auf der vorgetäuschten Landingpage die geforderten Daten eingegeben, landet man auf einer individuell gestalteten Informationsseite. Die betroffene Person wird somit über die vermeintliche Cyber-Attacke aufgeklärt und über die Merkmale einer Phishing E-Mail informiert.

Bei einem Fehlklick oder einer Dateneingabe können auch automatisch passende Awareness-Trainings zugewiesen werden.

Simulationsanalysen & Reports

Alle Phishing-Simulationen werden automatisch ausgewertet und übersichtlich dargestellt. Die Berichte zeigen sowohl Risiken, die sich aus den Reaktionen Ihrer Mitarbeitenden ergeben, als auch deren Lernfortschritte bei wiederholten Kampagnen.



Die Plattform zeigt auf einen Blick, wie Mitarbeitende auf realistische Angriffe reagieren. Klick-, Öffnungs-, Eingabe-, Download- und Melderaten werden automatisch erfasst und klar visualisiert.

Alle Daten sind Betriebsrat-konform und auf einen Blick einsehbar.

So erkennen Sie schnell, welche Teams oder Abteilungen noch auf Phishing-Attacken sensibilisiert werden müssen und zusätzliche Unterstützung benötigen.

Die Analyse bildet die Grundlage für gezielte Weiterbildungsmaßnahmen:

Bei Klicks auf gefälschte Phishing-Links oder einer Dateneingabe werden automatisch passende Awareness-Trainings zugewiesen, damit Lernimpulse unmittelbar folgen und Verhaltensänderungen nachhaltig entstehen.

So wird aus jeder Simulation nicht nur ein Test, sondern ein kontinuierlicher Teil Ihrer Sicherheitsstrategie – von der Risikoerkennung bis zur Lernerfahrung. Denn nur mit sensibilisierten Mitarbeitenden können Schäden durch Cybercrime verhindert werden.

Awareness-Trainings

Mit den Protectly Cybersecurity Awareness-Trainings sensibilisieren Sie Ihre Mitarbeitenden effizient und nachhaltig für Cyber-Gefahren und IT-Sicherheit.

Unsere E-Learning-Kurse kombinieren Gamification, interaktive Übungen und praxisnahe Szenarien, damit das Gelernte abwechslungsreich vermittelt und sicher im Arbeitsalltag angewendet wird. Die Inhalte decken alle relevanten Bereiche der Informationssicherheit ab. So stellen Sie sicher, dass Ihr Team in allen entscheidenden Themenfeldern geschult wird.

Ergänzend dazu bieten wir Trainings zur sicheren Nutzung von Künstlicher Intelligenz. Diese zeigen, wie KI-Tools verantwortungsvoll, kompetent und rechtssicher eingesetzt werden können. Die Inhalte orientieren sich am EU AI Act und helfen, rechtliche Risiken zu minimieren.



2D Awareness-Trainings

Kurze, animierte Kurse mit klaren Beispielen und interaktiven Übungen, die Sicherheitswissen verständlich und alltagsnah vermitteln.



2D Microlearnings

Ultra-kompakte Lerneinheiten, die direkt nach einer Simulation zugewiesen werden und Mitarbeitende in wenigen Minuten zielgerichtet schulen.



3D Awareness Trainings

Gamifizierte 3D-Lernszenarien, die Sicherheitsentscheidungen realistisch simulieren und komplexe Themen spielerisch erfahrbar machen.

Awareness-Trainings



Terminalkurse

Kompakte Kurse, die zentrale Sicherheitsregeln klar und verständlich vermitteln, direkt im LMS verfügbar sind und individuell angepasst werden können.

Unsere Protectly Security-Awareness-Kurse wurden umfassend geprüft und erfüllen die höchsten Standards der Informationssicherheit. Sie sind optimal geeignet, um die Anforderungen der wichtigsten Normen und Richtlinien nachweisbar zu erfüllen:

- BSI IT-Grundschutz
- NIS2-Richtlinie
- ISO 27001
- EU AI Act

2D E-Learning Awareness-Trainings

Unterhaltsame Clips gemischt mit interaktiven Übungen:

Die 2D E-Learning Cyber-Security-Awareness-Trainings sensibilisieren Ihre MitarbeiterInnen kurzweilig und effizient.



Kursangebot

Arbeitssicherheit

Arbeitssicherheit

Brandschutz

Datenschutz

Datenschutz Deutschland

Datenschutz Österreich

Datenschutz & IT-Sicherheit

Informationssicherheit

Advanced Persistent Threat

CEO Fraud

Dumpster Diving & Clear Desk Policy

Informationssicherheit

Informationssicherheit auf Reisen

Informationssicherheit im Homeoffice

2D E-Learning Awareness-Trainings

Informationssicherheit zu ChatGPT und Chatbots

IT-Compliance

Mobiles Arbeiten

Öffentliches WLAN

Passwortsicherheit

Phishing, Spear-Phishing & mehr

Sichere Nutzung mobiler IT-Geräte

Social Engineering

Was ist Clone Phishing?

Was ist ein QR-Code Scam?

Künstliche Intelligenz

KI verstehen – Grundlagen, Einsatz und rechtliche Rahmenbedingungen im öffentlichen Dienst

KI nutzen – Chancen, Risiken und richtige Anwendung in der Praxis

Alle Awareness-Trainings sind auch als SCORM-Datei für den Import in das firmeninterne LMS verfügbar.

2D Microlearnings

Kurz, prägnant und direkt im Arbeitsalltag einsetzbar:

2D Microlearnings vermitteln in wenigen Minuten genaues Wissen für sichere Entscheidungen im Arbeitsalltag.



Kursangebot

Informationssicherheit

Was ist Phishing?

Was ist Ransomware?

Wie erkenne ich Phishing- und Spam-Mails?

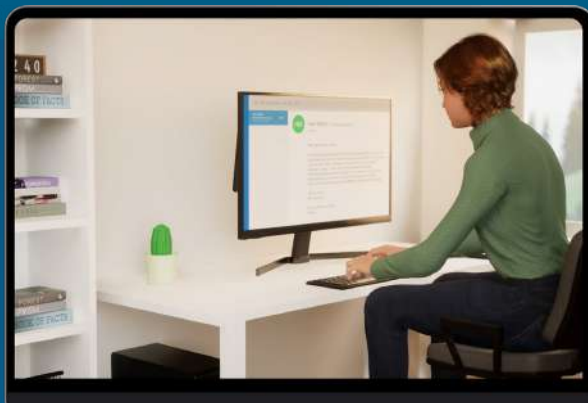
Wie verhalte ich mich richtig, wenn eine Phishing-Mail eingeht?

Alle Awareness-Trainings sind auch als SCORM-Datei für den Import in das firmeninterne LMS verfügbar.

3D E-Learning Awareness-Trainings

Die 3D animierten E-Learning Kurse basieren auf dem Gamification-Prinzip:

Ihre Mitarbeitenden lernen spielerisch die wichtigsten Dinge rund um Cyber Security.



Kursangebot

Arbeitssicherheit

Ergonomie am Arbeitsplatz

Gesundheit und Sicherheit am Arbeitsplatz

Brandschutz

Erste Hilfe

Compliance

Diskriminierung und Belästigung am Arbeitsplatz

Code of Conduct

Whistleblowing – Hinweisgeberschutz

NIS2 – Management Training

Das Allgemeine Gleichbehandlungsgesetz (AGG)

Compliance

Kartellrecht

Prävention von Mobbing am Arbeitsplatz

Finanzmarkt-Compliance

3D E-Learning Awareness-Trainings

Prävention von Geldwäsche und Terrorismusfinanzierung

Korruptionsprävention

Hygiene im Umgang mit Lebensmitteln

PSD 2 – Zahlungsdiensterichtlinie

Datenschutz

Datenschutz in Deutschland

Datenschutz in Österreich

Datenschutz in der Schweiz

Die EU-Datenschutz-Grundverordnung

Datenschutz und IT-Sicherheit

Diversität und Inklusion

Diskriminierung und Belästigung am Arbeitsplatz

Informationssicherheit

Sichere Nutzung von Cloud-Software

Verhalten bei Sicherheitsvorfällen

Sicheres Arbeiten im Homeoffice

Cybersecurity

Sicheres Arbeiten in der Öffentlichkeit

Phishing

Social Engineering

Informationssicherheit für Produktionsmitarbeiter

Sicheres Surfen im Internet

Phishing-Training

Klassifizierung von Informationen

Sichere Nutzung mobiler IT-Geräte

3D E-Learning Awareness Trainings

Passwortsicherheit

CEO-Fraud

Informationssicherheit vertiefend

Informationssicherheit auf Reisen

Sichere Nutzung sozialer Netzwerke

Künstliche Intelligenz

IT-Sicherheit, Datenschutz und KI

Sichere Nutzung von KI

KI-generierte Werke: Rechtliche Grauzonen

Nachhaltigkeit im Unternehmen

Nachhaltigkeit im Arbeitsalltag

Persönliche Weiterbildung

Konzentriert arbeiten

Effektive E-Mails schreiben

Das 80/20-Prinzip für Produktivität und Zeitmanagement

Alle Awareness-Trainings sind auch als SCORM-Datei für den Import in das firmeninterne LMS verfügbar.

Terminalkurse

Kompakt, barrierefrei und klar verständlich:

Unsere Terminalkurse vermitteln grundlegende Sicherheitsregeln speziell für den öffentlichen Dienst.



Kursangebot

Informationssicherheit für öffentliche Bedienstete

Merkmale gefährlicher Internet-Links

Merkmale gefährlicher E-Mail-Anhänge

Physische Sicherheit

Sicheres Surfen für Beamt:innen

Sicherer Umgang mit E-Mails

Social Engineering für öffentliche Bedienstete

Phishing, Spear-Phishing und Ransomware für öffentliche Bedienstete

CEO-Fraud

Sicheres Arbeiten in der Öffentlichkeit für öffentliche Bedienstete

Informationssicherheit auf Reisen

Ransomware

Sicheres Arbeiten im Homeoffice für öffentliche Bedienstete

Passwortsicherheit im öffentlichen Dienst

Mobiles Arbeiten für öffentliche Bedienstete

Klassifizierung von Informationen für öffentliche Bedienstete

Terminalkurse

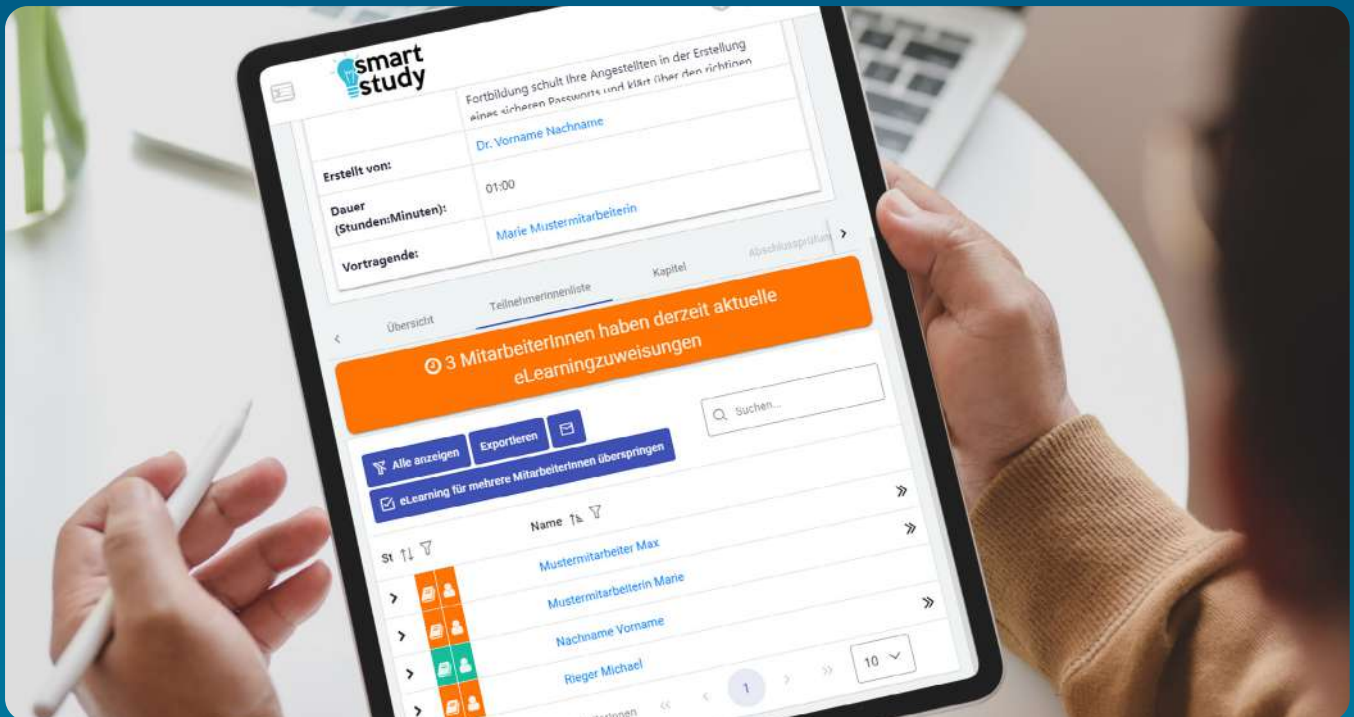
Informationssicherheit vertiefend für öffentliche Bedienstete

Künstliche Intelligenz

KI verstehen – Grundlagen, Einsatz und rechtliche Rahmenbedingungen im öffentlichen Dienst

KI nutzen – Chancen, Risiken und richtige Anwendung in der Praxis

Integriertes Lernmanagementsystem



Das **Protectly Lernmanagementsystem (LMS)** bietet Ihnen einen klaren Überblick über den Lernfortschritt Ihres gesamten Teams und über das Sicherheitsniveau Ihrer Organisation. Alle Trainings und Phishing-Kampagnen werden zentral gesteuert und einfach nachvollziehbar dargestellt.

Nach jedem abgeschlossenen Awareness-Training können Mitarbeitende ein Zertifikat erhalten. Gamification-Elemente wie Lernbadges, individuelle Lernpfade und Umfragen sorgen für Motivation und eine nachhaltige Lernkultur.

Dank übersichtlicher Dashboards sehen Sie jederzeit, welche Trainings bereits absolviert wurden, wo noch Aufgaben offen sind und welche Bereiche weitere Unterstützung benötigen.

Eigenen Content erstellen – einfach & schnell:

Mit dem integrierten Authoring Tool erstellen Sie mühelos eigene Kurse, Phishingkampagnen und Landingpages – ohne zusätzliche Software. Inhalte können sofort zugewiesen, verwaltet und dokumentiert werden.

Funktionen der Protectly Plattform



Verwaltung & Steuerung

- Zentrale Steuerung aller Lernaktivitäten
- Abbildung der Unternehmensstruktur
- Individuelles Branding nach Corporate Design
- Manuelle & automatisierte Kurszuweisungen
- Multimandanten-Fähigkeit
- Dateimanager
- SCORM-Kompatibilität



Kursentwicklung & Inhalte

- Authoring Tool zur Erstellung eigener Trainings
- Eigenes Kursmaterial schnell & einfach selbst erstellen
- 2D-Kurse, 3D-Kurse & interaktive Übungen
- Phishing-Kampagnen mit vorgefertigten Templates



Lernen & Motivation

- Lernbadges & Bestenlisten
- Zertifikate
- Lernpfade
- Kurs-Kalender
- Automatisierte Erinnerungsmails
- Push-Benachrichtigungen

Funktionen der Protectly Plattform



Analysen & Überblick

- Klare Fortschritts- & Risikoeinschätzungen
- Talentmanagement



Seminare & Präsenzformate

- Seminar-Management
- Anwesenheitsbestätigung bei Vor-Ort-Schulungen



Kommunikation & Interaktion

- Online-Umfragen & Feedback-Tool
- Newsfeed & Chat

Warum Protectly?

Eine Plattform. Viele Vorteile.

- DSGVO-konform
- Gehostet auf Open Telekom Cloud
- Inklusive Erst-Set-up
- Web, PC & Mobile
- Simulations- & Trainingsplattform in einem
- Individuelle Kursanpassungen & Erstellung nach Ihren Vorgaben
- Support-Service
- Mehrsprachig
- Barrierefrei
- Über 50.000 aktive Nutzende
- Entwickelt in Österreich

Einsatzgebiete

- **Öffentlicher Dienst & Verwaltung (Land/Bund/Gemeinden):**
Sichere Schulungen gemäß BSI & Datenschutz
- **Gesundheit & kritische Infrastruktur (KRITIS):**
Sensibilisierung gegen Social Engineering & Deepfake-Risiken
- **Industrie & Produktion:**
Spezielle 3D-Kurse für Produktionsumgebungen
- **Bildungseinrichtungen:**
Große Mandanten, viele Nutzende, einfache Ausrollung
- **Unternehmen mit verteilten Teams:**
Mobile und hybride Arbeitsformen
- **Unternehmen mit hohem Informationsschutzbedarf:**
Rechtsanwaltskanzleien, Finanzdienstleistende, Energieanbieter

TECH BOOST

Protectly ist seit März 2021 Teil von **TechBoost – einem Startup-Förderprogramm der Deutschen Telekom.**

Die Deutsche Telekom unterstützt mit TechBoost ausgewählte Technologie-Startups mit wertvollem Vertriebs- & Marketingsupport und bringt etablierte Unternehmen mit den innovativen Lösungen der Start-ups zusammen.

60.000 gemeinsam neu gewonnene User:innen sprechen Bände über den Erfolg dieser Zusammenarbeit.

Und sie zeigen, wie essenziell sensibilisierte Mitarbeitende für die IT-Sicherheitsstrategie eines jeden Unternehmens sind.

Protectly wird auf der **Open Telekom Cloud** gehostet, die nicht nur DSGVO-konform ist, sondern dank modernster Technologien vor Systemausfällen sicher ist.

Außerdem werden die Rechenzentren ausschließlich mit erneuerbaren Energien betrieben und benötigen 30 % weniger Energie als herkömmliche Zentren.



Protectly

BY SMART STUDY

**Kontaktieren Sie uns jetzt gleich
und testen Sie alle Vorteile
von Protectly!**

Protectly
by
Smart-Study GmbH
Villefortgasse 11
8010 Graz
Tel.: +43 316 438 017
E-Mail: info@smartstudy.at
Web: www.smartstudy.at

www.protectly.eu