DIE EUROPÄISCHE AWARENESS-PLATTFORM

Sicherheit beginnt mit Ihren Mitarbeitenden.

Security Awareness.
Realistische Simulationen.
Lernen, das im Arbeitsalltag ankommt.

Mappe entdecken →

Kontakt aufnehmen →



Eine Plattform für Ihre Sicherheitskultur.

01
Angriffe erleben

02
Risiken verstehen

03
Sicher handeln

INHALT / DIREKT ZUM THEMA

Alles auf einen Blick.

Die Plattform verstehen, Simulationen kennenlernen oder gezielt im Kursangebot stöbern: Wählen Sie Ihren Schwerpunkt.

01 03-04 →

Plattform & Ansatz

Überblick und Zusammenspiel der drei Komponenten

02 05-07 →

Simulationen & Analysen

Angriffsformen, Kampagnen und Auswertungen

03 08-13 →

Trainings & Kurskatalog

2D, Microlearnings, 3D und Terminalkurse

04 14-15 →

Lernmanagement & Funktionen

Zentrale Verwaltung, eigene Inhalte und Lernfortschritt

05 16-18 →

Vorteile & Einsatzgebiete

Organisationen, Hosting und Zusammenarbeit

06 19 →

Kontakt

Protectly kennenlernen und Kontakt aufnehmen

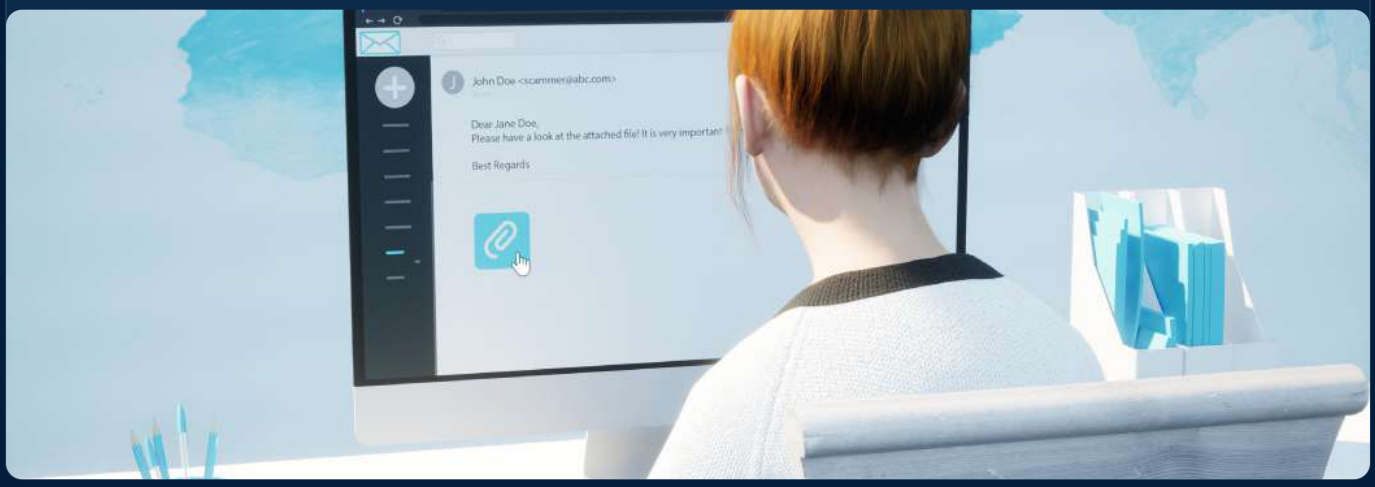
Über die Navigation am Seitenkopf wechseln Sie jederzeit das Kapitel.

01 / PLATTFORM & ANSATZ

Was ist Protectly?

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

PLATTFORMEINBLICK



Protectly unterstützt Sie dabei, Ihre Mitarbeitenden wirksam vor modernen Cyberangriffen zu schützen. Realistische Simulationen, klare Analysen und interaktive Trainings machen Ihre Sicherheitskultur messbar und stärken sie nachhaltig.

DIE PLATTFORM VERBINDET

- Multi-Channel-Phishing: E-Mail, SMS, WhatsApp, QR-Code sowie Voice- und KI-Anrufe
- Deepfake-Simulationen und automatisch zugewiesene Awareness-Trainings
- LMS für E-Learning, Seminare, Phishing-Kampagnen und Simulationsanalysen
- Autorentool und über 30 Awareness-Kurse in 2D/3D, barrierefrei und DSGVO-konform

DER PROTECTLY-ANSATZ

Awareness entsteht durch Erfahrung.

Drei Komponenten greifen ineinander und stärken den IT-Schutz Ihrer Organisation: simulieren, analysieren und gezielt trainieren.

01 Social-Engineering-Simulationen



Realistische Alltagssituationen zeigen, wie Ihre Mitarbeitenden auf moderne Angriffe reagieren.

E-Mail · QR-Code · Deepfake-Meetings · Voice-Agenten · Videobotschaften & Sprachnachrichten

02 Simulationsanalysen



Erkennen Sie, wo Risiken bestehen und welche Teams zusätzliche Unterstützung benötigen.

Klick-, Öffnungs-, Dateneingabe- und Melderaten

03 Awareness-Trainings



Passende Lernmodule übersetzen die Ergebnisse in sichere Entscheidungen im Arbeitsalltag.

2D- & 3D-E-Learnings · Datenschutz & Informationssicherheit · Lern-Badges · Bestenlisten · Zertifikate

02 / SOCIAL ENGINEERING

Moderne Angriffe. Realistisch simuliert.

Täuschend echte Nachrichten, Videoanrufe und Sprachnachrichten: Protectly simuliert moderne Angriffsformen unter realistischen Bedingungen - sicher, DSGVO-konform und vollständig automatisiert.

E-Mail-Simulationen

Realistisch gestaltete Phishing-Mails prüfen das Verhalten im Arbeitsalltag. Öffnungs-, Klick-, Eingabe- und Downloadraten machen Risikobereiche sichtbar.

QR-Code-Simulationen

Prüfen Sie den Umgang mit QR-Codes im Büro und unterwegs: in Meetingräumen, auf Dokumenten oder in E-Mails.

Live-Deepfake-Meetings

Gefälschte Videocalls zeigen, wie visuelles Vertrauen missbraucht wird. Mitarbeitende erleben Deepfake-Führungskräfte oder Kolleginnen und Kollegen, die Anweisungen erteilen.

Voice-Agent-Simulationen

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

Video- & Sprachnachrichten

Täuschend echt erzeugte Video- oder Audio-Nachrichten schaffen Druck- und Stresssituationen. So wird sichtbar, wie souverän Mitarbeitende mit KI-basierten Täuschungen umgehen.

PHISHING-SIMULATIONEN

Von der Vorlage zum Lernmoment.

Erstellen Sie in wenigen Schritten täuschend echt wirkende Phishing-Simulationen und Landingpages. Der Versand an Ihre Mitarbeitenden erfolgt automatisiert.

01 Templates auswählen oder selbst gestalten

Nutzen Sie zahlreiche vorgefertigte Templates. Falls kein passendes dabei ist, erstellen Sie in wenigen Sekunden Ihre eigene Simulation - in Ihrem gewünschten Look.

02 Zielgruppen und Versand festlegen

Legen Sie flexibel fest, welche Abteilung wann und wie oft eine Simulation erhält. Auch unterschiedliche Phishing-E-Mails lassen sich gleichzeitig und automatisiert versenden.

03 Direkt aufklären

Nach einem Linkklick oder einer Dateneingabe auf der simulierten Landingpage erscheint eine individuell gestaltete Informationsseite. Sie erklärt die vermeintliche Cyberattacke und zeigt typische Merkmale einer Phishing-Mail.

04 Passende Trainings zuweisen

Bei einem Fehlklick oder einer Dateneingabe können automatisch passende Awareness-Trainings folgen. Die Simulation wird zum konkreten Lernanlass.

SIMULATIONSANALYSEN & REPORTS

Risiken erkennen. Fortschritte sichtbar machen.

Alle Phishing-Simulationen werden automatisch ausgewertet. Übersichtliche Berichte zeigen Risiken und Lernfortschritte über wiederholte Kampagnen hinweg.

KENNZAHL	WELCHE REAKTION WIRD SICHTBAR?
Öffnungsrate	Wurde die Nachricht geöffnet?
Klickrate	Wurde ein Link angeklickt?
Dateneingaberate	Wurden auf der simulierten Landingpage Daten eingegeben?
Downloadrate	Wurde ein Download ausgelöst?
Melderate	Wurde der verdächtige Inhalt gemeldet?

Teams gezielt unterstützen

Betriebsrat-konforme Auswertungen zeigen, welche Teams oder Abteilungen bei Phishing-Angriffen noch sensibilisiert werden müssen und zusätzliche Unterstützung benötigen.

Den nächsten Lernimpuls auslösen

Klicks auf gefälschte Links oder Dateneingaben können automatisch passende Trainings auslösen. Der unmittelbare Lernimpuls unterstützt nachhaltige Verhaltensänderungen.

Von der Risikoerkennung bis zur Lernerfahrung: Jede Simulation wird Teil Ihrer Sicherheitsstrategie. Sensibilisierte Mitarbeitende helfen, Schäden durch Cybercrime zu verhindern.

03 / AWARENESS-TRAININGS

Wissen, das bleibt.

Gamification, interaktive Übungen und praxisnahe Szenarien vermitteln Sicherheitswissen abwechslungsreich und fördern die Anwendung im Arbeitsalltag. Die Inhalte decken die relevanten Bereiche der Informationssicherheit ab.

Ergänzende KI-Trainings unterstützen eine verantwortungsvolle, kompetente und rechtssichere Nutzung von KI-Tools. 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.

Kurse ansehen →

2D Microlearnings

Kompakte Lerneinheiten, die direkt nach einer Simulation in wenigen Minuten gezielt schulen.

Kurse ansehen →

3D Awareness-Trainings

Gamifizierte Lernszenarien machen Sicherheitsentscheidungen realistisch und komplexe Themen spielerisch erfahrbar.

Kurse ansehen →

Terminalkurse

Kompakte Kurse zu zentralen Sicherheitsregeln. Direkt im LMS verfügbar und individuell anpassbar.

Kurse ansehen →

Die geprüften Kurse sind auf die Unterstützung nachweisbarer Schulungsanforderungen ausgerichtet:

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

KURSANGEBOT / 2D

2D E-Learnings

Unterhaltsame Clips und interaktive Übungen: kurzweilig lernen und Sicherheitswissen gezielt vertiefen.

23 Kurse / 4 Themenfelder / SCORM verfügbar

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

Informationssicherheit / Forts.

- 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 Ihr firmeninternes LMS verfügbar.

KURSANGEBOT / 2D MICROLEARNINGS

Kleine Lerneinheiten. Direkter Lernimpuls.

Kurz, prägnant und direkt im Arbeitsalltag einsetzbar: 2D Microlearnings vermitteln in wenigen Minuten genaues Wissen für sichere Entscheidungen.

4 Lerneinheiten	Direkt nach einer Simulation zuweisbar

INFORMATIONSSICHERHEIT

01 Was ist Phishing?

02 Was ist Ransomware?

03 Wie erkenne ich Phishing- und Spam-Mails?

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

Direkt nach einer Simulation zuweisbar. Alle Awareness-Trainings sind auch als SCORM-Datei für Ihr eigenes LMS verfügbar.

KURSANGEBOT / 3D / TEIL 1

3D E-Learnings

Spielerisch lernen: 3D-animierte Kurse nutzen Gamification und machen Wissen rund um Cybersecurity und weitere Arbeitsalltagsthemen erlebbar.

47 Kurse / 8 Themenfelder / SCORM verfügbar

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

Compliance / Fortsetzung

- Kartellrecht
- Prävention von Mobbing am Arbeitsplatz
- Finanzmarkt-Compliance
- 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

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

KURSANGEBOT / 3D / TEIL 2

3D E-Learnings

47 Kurse / 8 Themenfelder / SCORM verfügbar

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
- 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

Diversität und Inklusion

- Diskriminierung und Belästigung am Arbeitsplatz

Nachhaltigkeit im Unternehmen

- Nachhaltigkeit im Arbeitsalltag

Persönliche Weiterbildung

- Konzentriert arbeiten
- Effektive E-Mails schreiben
- Das 80/20-Prinzip für Produktivität und Zeitmanagement

Alle Trainingsformate →

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

KURSANGEBOT / ÖFFENTLICHER DIENST

Terminalkurse

Kompakt, barrierefrei und klar verständlich: grundlegende Sicherheitsregeln speziell für den öffentlichen Dienst.

18 Kurse / Informationssicherheit und KI

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
- Informationssicherheit vertiefend für öffentliche Bedienstete

Künstliche Intelligenz

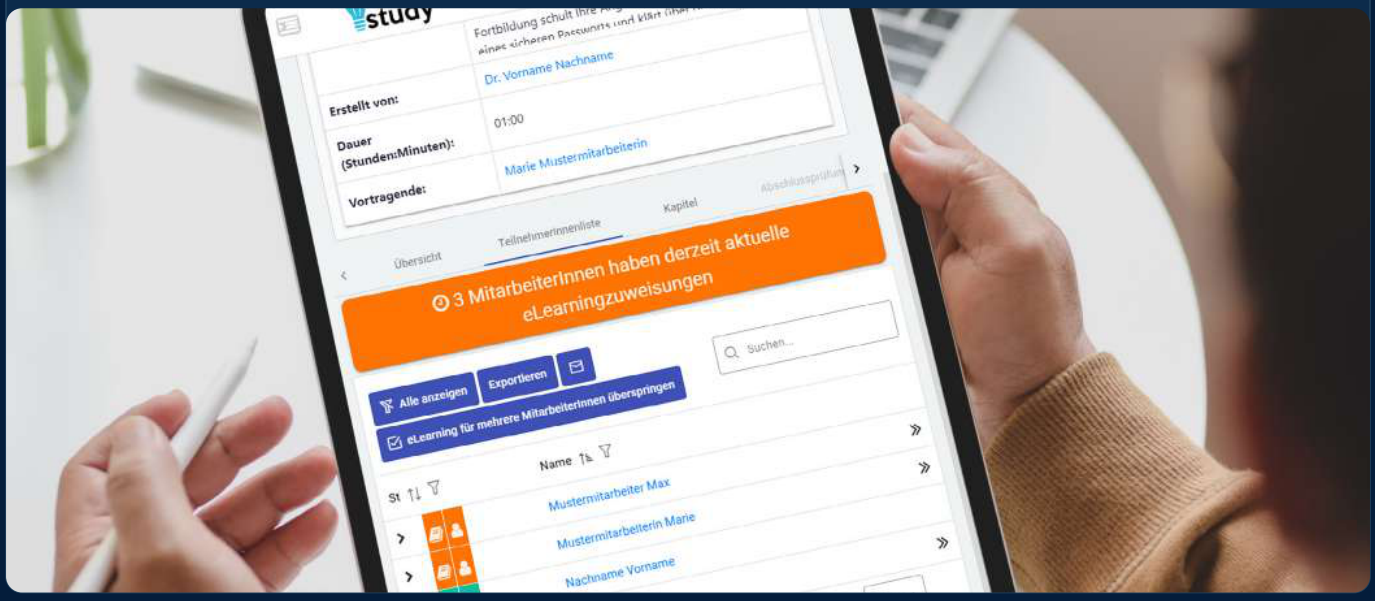
- KI verstehen - Grundlagen, Einsatz und rechtliche Rahmenbedingungen im öffentlichen Dienst
- KI nutzen - Chancen, Risiken und richtige Anwendung in der Praxis

Direkt im Protectly-LMS verfügbar. Die Terminalkurse können individuell angepasst werden.

04 / INTEGRIERTES LERNMANAGEMENTSYSTEM

Alles an einem Ort.

EINBLICK IN DAS LERNMANAGEMENT



Steuern Sie Trainings und Phishing-Kampagnen zentral. Das Protectly-LMS gibt Ihnen einen klaren Überblick über den Lernfortschritt Ihres Teams und das Sicherheitsniveau Ihrer Organisation.

Lernen begleiten und dokumentieren

Zertifikate nach abgeschlossenen Trainings, Lernbadges, individuelle Lernpfade und Umfragen fördern Motivation und eine nachhaltige Lernkultur. Dashboards zeigen absolvierte Trainings, offene Aufgaben und Bereiche mit weiterem Unterstützungsbedarf.

Eigenen Content einfach erstellen

Mit dem integrierten Authoring Tool erstellen Sie eigene Kurse, Phishing-Kampagnen und Landingpages ohne zusätzliche Software. Inhalte lassen sich sofort zuweisen, verwalten und dokumentieren.

FUNKTIONEN / VERWALTUNG BIS INTERAKTION

Die Plattform im Detail.

Verwaltung & Steuerung

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

Lernen & Motivation

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

Kursentwicklung & Inhalte

- Authoring Tool für eigene Trainings
- Eigenes Kursmaterial selbst erstellen
- 2D-Kurse, 3D-Kurse & interaktive Übungen
- Phishing-Kampagnen mit Templates

Analysen & Überblick

- Klare Fortschritts- & Risikoeinschätzungen
- Talentmanagement

Seminare & Präsenzformate

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

Kommunikation & Interaktion

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

05 / WARUM PROTECTLY?

Eine Plattform. Viele Vorteile.

50.000+

aktive Nutzende

Entwickelt in Österreich

Simulationen, Analysen und Trainings in einer Plattform.



Datenschutz & Hosting

DSGVO-konform und auf der Open Telekom Cloud gehostet.

Einfach starten

Erst-Set-up inklusive. Unterstützung durch den Support-Service.

Überall nutzbar

Web, PC und Mobile. Mehrsprachig und barrierefrei.

Individuell anpassbar

Kursanpassungen und Erstellung von Inhalten nach Ihren Vorgaben.

Simulationen und Trainings in einer Plattform: Risiken erkennen, Lernimpulse auslösen und Fortschritte zentral verfolgen.

EINSATZGEBIETE

Für Ihren Arbeitsalltag.

Ob Verwaltung, kritische Infrastruktur oder verteilte Teams: Protectly verbindet passende Lerninhalte mit realistischen Angriffsszenarien.

01

Öffentlicher Dienst & Verwaltung

Land, Bund und Gemeinden: sichere Schulungen gemäß BSI und Datenschutz.

02

Gesundheit & KRITIS

Sensibilisierung gegen Social Engineering und Deepfake-Risiken.

03

Industrie & Produktion

Spezielle 3D-Kurse für Produktionsumgebungen.

04

Bildungseinrichtungen

Große Mandanten, viele Nutzende und eine einfache Ausrollung.

05

Unternehmen mit verteilten Teams

Trainings für mobile und hybride Arbeitsformen.

06

Hoher Informationsschutzbedarf

Für Rechtsanwaltskanzleien, Finanzdienstleistende und Energieanbietende.

PROTECTLY & DEUTSCHE TELEKOM

Starke Zusammenarbeit. Europäisches Hosting.

TECHBOOST

Teil des Startup-Förderprogramms der Deutschen Telekom seit März 2021.

TechBoost unterstützt ausgewählte Technologie-Startups mit Vertriebs- und Marketingsupport und bringt etablierte Unternehmen mit innovativen Lösungen zusammen.

60.000

gemeinsam neu gewonnene Userinnen und User

Die Zusammenarbeit zeigt, wie essenziell sensibilisierte Mitarbeitende für die IT-Sicherheitsstrategie eines Unternehmens sind.

Gehostet auf der Open Telekom Cloud

DSGVO-konformes Hosting mit modernen Technologien zum Schutz vor Systemausfällen. Die Rechenzentren werden ausschließlich mit erneuerbaren Energien betrieben und benötigen 30 % weniger Energie als herkömmliche Zentren.

PROTECTLY KENNENLERNEN

Machen Sie Ihr Team bereit für den Ernstfall.

Kontaktieren Sie uns und testen Sie alle Vorteile von Protectly.

E-Mail schreiben →

Website besuchen →

IHR KONTAKT

Protectly

by Smart-Study GmbH
Villefortgasse 11
8010 Graz

+43 316 438 017

info@smartstudy.at

www.smartstudy.at

www.protectly.eu

Produkt- und Kursstand: Februar 2026