



# Awareness

Leistungsbeschreibung –  
Unser Portal für Cybersicherheit

Unsere Lösungen für Ihre Cybersicherheit

# Lösungen im Überblick

Das Online-Portal für Cybersicherheit von Perseus ist schnell installiert, einfach zu bedienen und jederzeit erreichbar. Herzstücke des Online-Portals sind unser Online-Training für Mitarbeitende sowie die Phishing-Simulationen. Erweitert wird unser Rundum-Ansatz für Cybersicherheit durch den Werkzeugkasten für Cybersicherheit und die Gefahrenwarnungen für Unternehmen.

Unser Online-Portal für Cybersicherheit lässt sich einfach und schnell in Unternehmen jeder Größe integrieren und mit wenig Aufwand von zentraler Stelle (z. B. vom CISO, von der IT etc.) steuern.

In dieser Leistungsbeschreibung stellen wir Ihnen die Leistungen\* des Online-Portals im Detail vor.

Online-Portal für  
Cybersicherheit

Jetzt Demo anfragen

|                                   |    |
|-----------------------------------|----|
| Online-Portal für Cybersicherheit | 03 |
| Sicherheitsassistent für Admins   | 04 |
| Mitarbeitendenverwaltung          | 05 |
| Online-Trainings                  | 06 |
| Zertifikate                       | 11 |
| Aktivierung von Mitarbeitenden    | 12 |
| Phishing-Simulation/Reporting     | 13 |
| Werkzeugkasten                    | 15 |
| Blog, Newsletter & Glossar        | 17 |
| Gefahrenwarnung                   | 18 |

\*Sollten Sie Kunde von einem unserer Kooperationspartner sein, dann können Ihre Leistungen evtl. abweichen. Bei Fragen wenden Sie sich bitte an unseren Kundenservice: 030/95 999 80 80. Wir freuen uns auf Sie!

# Online-Portal für Cybersicherheit

## Bestandteile des Online-Portals:

- **Sicherheitsassistent für Admins:**  
Sicherheitsübersicht über Ihr ganzes Unternehmen
- **Mitarbeitendenverwaltung:** Fortschritt der Mitarbeitenden bei den Trainings einsehen und Erinnerungen versenden
- **Online-Trainings:** Die Trainings vermitteln wichtiges Wissen zu Cybersicherheit, Datenschutz und Phishing
- **Zertifikate:** Unsere Zertifikate gelten als Schulungsnachweis der Mitarbeitenden im Sinne der DSGVO
- **Aktivierung von Mitarbeitenden:** Wir erinnern regelmäßig per E-Mail daran Trainings abzuschließen
- **Phishing-Simulation:** Perseus versendet vollautomatisierte, simulierte Phishing-E-Mails an Mitarbeitende, um sie auf Gefahren zu sensibilisieren
- **Werkzeugkasten:** Tools, die den Arbeitsalltag sicherer machen
- **Gefahrenwarnungen:** Wir warnen Mitarbeitende vor neuen Online-Bedrohungen

## Zwecke und Zielsetzung des Online-Portals

- Herstellung, Wahrung und Verbesserung der Cybersecurity- und Datenschutz-Compliance
- Datenschutz und Informationssicherheit zur Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und personenbezogener Daten
- Reporting von IT-Sicherheitsprozessen für Verantwortliche
- Durchführung und Nachhalten von Online-Trainings zu den Themen Cybersicherheit und Datenschutz
- Erteilung von persönlichen Zertifikaten als Nachweis für erworbenes Wissen zu Cybersicherheit und Datenschutz

# Sicherheitsassistent für Admins

Der Sicherheits-Assistent für Admins gibt einen Sicherheitsüberblick über Ihr ganzes Unternehmen. Neben dem aktuellen Sicherheitsstatus erhalten Sie hier Statistiken zu absolvierten Schulungen oder Phishing-Tests, bzw. Hinweise darüber, wie Sie Ihr Unternehmen noch sicherer machen können.

## Überblick auf Knopfdruck:

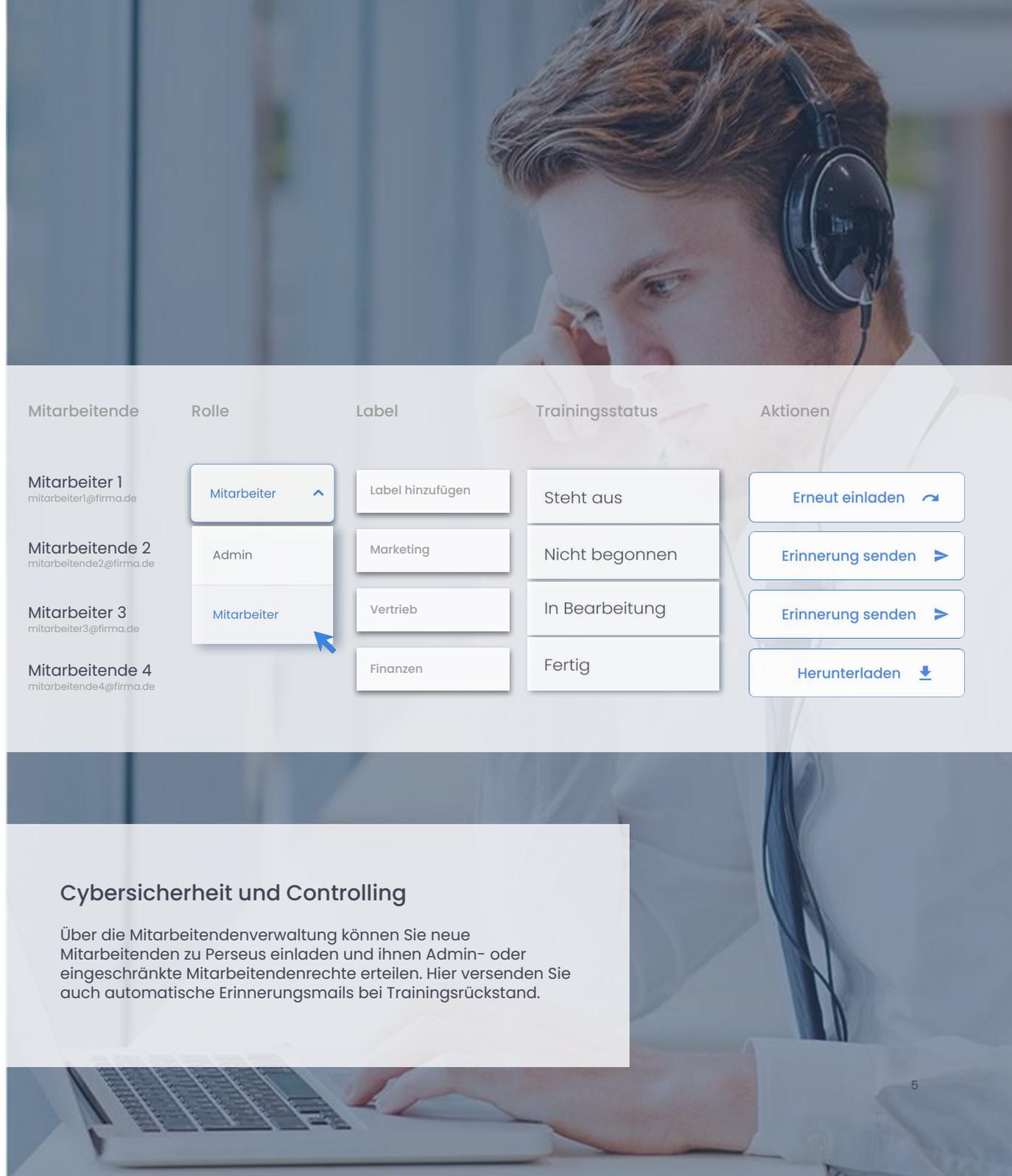
- **Phishing erkannt:** Wie erfolgreich waren Ihre Mitarbeitenden beim letzten Phishing-Test?
- **Training absolviert:** Erfahren Sie jederzeit den Trainingsstand des gesamten Unternehmens.
- **Browser aktuell:** Veralterte Software ist ein großes Sicherheitsrisiko. Haben alle Ihre Mitarbeitenden die neueste Browser-Version installiert?
- **Phishing-Status des Unternehmens:** Statistiken zu aktuellen Phishing-Kampagnen (kann als XLS-Datei heruntergeladen werden).



# Mitarbeitenden- verwaltung Rechte & Trainingsstatus

## Alles im Blick:

- **Mitarbeitende einladen:** Neue Mitarbeitende fügen Sie einfach und schnell über die Eingabe von E-Mail-Adressen hinzu.
- **Rollen-/Rechteverteilung:** Sie möchten mehreren Nutzern Admin-Rechte geben? Kein Problem. Auch die Rollenverteilung lässt sich mit einem Klick über die Mitarbeitendenverwaltung regeln.
- **Trainingsstatus:** Erfahren Sie als Admin jederzeit, wie weit Ihre Mitarbeitenden in den Online-Trainings fortgeschritten sind.
- **Erinnerungen senden:** Einzelne Mitarbeitenden haben das Training noch nicht begonnen oder noch nicht abgeschlossen? Erinnern Sie sie mit einem Klick per vorgefertigter E-Mail.
- **Erneut einladen:** Die Anmeldung einiger Mitarbeitenden steht noch aus? Versenden Sie von hier aus einfach eine erneute Einladung zur Registrierung bei Perseus.



| Mitarbeitende   | Rolle       | Label            | Trainingsstatus | Aktionen            |
|---|-------------|------------------|-----------------|---------------------|
| Mitarbeiter 1<br><small>mitarbeiter1@firma.de</small>     | Mitarbeiter | Label hinzufügen | Steht aus       | Erneut einladen ↻   |
| Mitarbeitende 2<br><small>mitarbeitende2@firma.de</small> | Admin       | Marketing        | Nicht begonnen  | Erinnerung senden ▶ |
| Mitarbeiter 3<br><small>mitarbeiter3@firma.de</small>     | Mitarbeiter | Vertrieb         | In Bearbeitung  | Erinnerung senden ▶ |
| Mitarbeitende 4<br><small>mitarbeitende4@firma.de</small> |             | Finanzen         | Fertig          | Herunterladen ↓     |

## Cybersicherheit und Controlling

Über die Mitarbeitendenverwaltung können Sie neue Mitarbeitenden zu Perseus einladen und ihnen Admin- oder eingeschränkte Mitarbeitendenrechte erteilen. Hier versenden Sie auch automatische Erinnerungsmails bei Trainingsrückstand.

# Online-Training für Cybersicherheit

## Grundlagen der Cybersicherheit:

1. Sicherheitsupdates
2. Antivirensoftware
3. Firewall
4. Öffentliche WLAN-Netze
5. Sicherheitskopien

## Cybersicherheit in der Praxis:

1. Sichere Passwörter
2. 2-Faktor-Authentifizierung
3. Sicher E-Mails versenden
4. Sicher online zusammenarbeiten

## Zielsetzung und Zweck

Durchführung und Nachhalten von Online-Trainings zu den Themen Cybersicherheit und Datenschutz zur Herstellung, Wahrung und Verbesserung der Cybersecurity- und Datenschutz-Compliance bei Kunden und Bezugsberechtigten

## Modernes E-Learning-Format

Die Kombination aus lehrendem Dozent und hilfreichen Animationen zum besseren Verständnis führen zu einem nachhaltigen Lernerfolg.



**Online-Videos:** Hintergründe zu Cybergefahren und Sicherheitsrisiken mit konkreten Handlungsempfehlungen.

**Grundlagen der Cybersicherheit**

5 Videos

5:52 min

Fortschritt 0%

[Beginnen](#)

**Cybersicherheit in der Praxis**

4 Videos

07:39 min

Fortschritt 0%

[Beginnen](#)

ZERTIFIKAT

[Herunterladen](#)



**Mehrsprachigkeit:** Die Leistungen des Online-Portals sind aktuell in den Sprachen Deutsch, Englisch und Spanisch verfügbar.

# Online-Training für Datenschutz

## DSGVO – Die Grundlagen:

1. DSGVO – Die Grundlagen (Intro)
2. Ziele & Bedeutung für Unternehmen
3. Personenbezogene Daten
4. Verarbeitung personenbezogener Daten
5. DSGVO im Privatleben & Zusammenfassung

## Personenbezogene Daten – Der richtige Umgang (Teil 1):

1. Grundsatz der Rechtmäßigkeit
2. Grundsatz der Zweckbindung
3. Grundsatz der Datenminimierung
4. Grundsatz der Speicherbegrenzung

## Personenbezogene Daten – Der richtige Umgang (Teil 2):

1. Grundsätze der Richtigkeit und der Transparenz
2. Grundsatz der Integrität und Vertraulichkeit
3. Grundsatz der Rechenschaftspflicht
4. Wissenswertes zur Weitergabe personenbezogener Daten

## Betroffenenrechte und Datenschutzverletzungen:

1. Allgemeines und das Recht auf Auskunft
2. Das Recht auf Löschung
3. Verletzung des Schutzes personenbezogener Daten
4. Meldung, Benachrichtigung und Dokumentation



**Online-Videos:** Einfach, verständlich und kompakt – Informationen zu Datenschutz und seinen gesetzlichen Anforderungen.

**DSGVO – Die Grundlagen**

5 Lektion(en)

10:00 min

Fortschritt 0%

[Beginnen](#)

**Personenbezogene Daten – der richtige Umgang Teil 1**

4 Lektion(en)

7:00 min

Fortschritt 0%

[Beginnen](#)

**Personenbezogene Daten – der richtige Umgang Teil 2**

4 Lektion(en)

8:30 min

Fortschritt 0%

[Beginnen](#)

**Betroffenenrechte und Datenschutzverletzungen**

4 Lektion(en)

6:30 min

Fortschritt 0%

[Beginnen](#)

ZERTIFIKAT

Herunterladen

ZERTIFIKAT

Herunterladen

# Online-Training gegen Phishing

Die neue E-Learning-Serie zum Thema Phishing ist die perfekte Ergänzung zu unserem Phishing-Training. So werden Lernen und Sensibilisierung zum ganzheitliches Awareness-Konzept.

## Phishing – die Methoden:

1. Interessante Links
2. Vertraute Links
3. Handeln aus Angst
4. Ist Ihr Passwort sicher?
5. Gehackte Freunde
6. Gefährliche Anhänge
7. Wie können Sie sich schützen?

## Phishing – die Auswirkungen:

1. Spyware
2. Ransomware
3. Computerviren und Würmer
4. Merkmale von Phishing-Nachrichten

## Phishing – Basiswissen:

1. Phishing – Definition
2. Wie können Sie sich schützen

## Phishing – Zusammenfassung:

1. Zusammenfassung
2. Gut zu wissen

**Phishing-Videos:** Phishing-Attacken sind die größte Cyberberbedrohung für kleine und mittelständische Unternehmen. Aus diesem Grund legen wir bei unseren Online-Trainings einen besonderen Fokus auf dieses Thema. Ihre Mitarbeitenden lernen Phishing-Attacken zu erkennen und abzuwehren.



**Phishing – Basiswissen**  
2 Lektion(en)  
5:00 min  
Fortschritt 100%

Fertig!



**Phishing – die Methoden**  
6 Videos  
7:47 min  
Fortschritt 0%

Beginnen



**Phishing – die Auswirkungen**  
4 Videos  
05:34 min  
Fortschritt 0%

Beginnen



**Phishing – Zusammenfassung**  
2 Lektion(en)  
2:00 min  
Fortschritt 50%

Weiter lernen

ZERTIFIKAT

Herunterladen

**Quizzes & Zertifikate:** Nach allen Lernvideos folgt ein kurzes Quiz als Lernkontrolle. Lernnachweise (Zertifikate) können nach erfolgreich absolviertenn Kursen heruntergeladen werden.

# Online-Training

## Vertiefende Lektionen zu Cybersicherheit & Datenschutz

### Social Media:

1. Online-Quiz
2. Berufliche Netzwerke
3. Beruflich und privat
4. Wie können Sie sich schützen

### Mobiles Arbeiten:

1. Öffentliches WLAN
2. Gefahren der Schatten-IT
3. Online Meetings & Kollaboratives Arbeiten
4. Spear Phishing und CEO-Fraud
5. Sicheres Homeoffice & DSGVO

### Umgang mit Informationen:

1. Lebenszyklus von Informationen
2. Vertrauliche vs. öffentliche Informationen
3. IT-, und Informationssicherheit
4. Clean Desk Policy

### Menschliche Firewall:

1. Menschliche Firewall
2. Gefahren im Netz

### Cyber-Notfall:

1. Warnsignale
2. Handeln im Notfall
3. Sicherheitskopien
4. Ausschalten oder nicht?



**Social Media**  
4 Videos  
8:00 min  
Fortschritt 0%

[Beginnen](#)



**Mobiles Arbeiten**  
5 Videos  
11:30 min  
Fortschritt 0%

[Beginnen](#)



**Umgang mit Informationen**  
4 Videos  
11:00 min  
Fortschritt 0%

[Beginnen](#)



**Menschliche Firewall**  
2 Videos  
5:00 min  
Fortschritt 0%

[Beginnen](#)



**Cyber Notfall**  
4 Videos  
8:30 min  
Fortschritt 0%

[Beginnen](#)

# Online-Training

## Vertiefende Lektionen zu Angriffsmitteln & Methoden

### Schadsoftware:

1. Viren & Würmer
2. Trojaner & Keylogger
3. Ransomware
4. Wie können Sie sich schützen?

### Verschlüsselungssoftware:

1. Schadsoftware - die Sichtbaren
2. Trojaner - das Transportmittel
3. Scareware - der Angstmacher
4. Wie können Sie sich schützen?

### Social Engineering:

1. Die menschliche Psyche
2. Arten von Social Engineering
3. Wie können Sie sich schützen?



**Schadsoftware**

4 Videos

8:00 min

Fortschritt 0%

[Beginnen](#)



**Verschlüsselungssoftware**

4 Videos

9:00 min

Fortschritt 0%

[Beginnen](#)



**Social Engineering**

3 Videos

8:30 min

Fortschritt 0%

[Beginnen](#)

# Zertifikate für Cybersicherheit & Datenschutz

## (DSGVO-/Versicherungs-Nachweise)

Die Perseus-Zertifikate für Cybersicherheit und Datenschutz unterstützen Sie bei der Einhaltung der EU-Datenschutz-Grundverordnung und sind ein wichtiger Nachweis bei eventuellen Prüfungen durch die Behörden.

### Immer auf neuestem Wissensstand

Auch nach dem Abschluss der Online-Trainings und dem Erhalt der Trainingszertifikate werden Ihre Mitarbeitenden weiterhin mit wichtigen Lerninhalten zu den Themen Cybersicherheit und Datenschutz informiert.

### Einfacher Download

Alle Ihre Mitarbeitenden können die von ihnen erworbenen Zertifikate leicht und schnell online herunterladen – zu Zwecken der Dokumentation oder zum Ausdrucken. Als Admin haben Sie sogar die Möglichkeit, alle Mitarbeitenden-Zertifikate gesammelt in einem einzigen Ordner herunterzuladen.

### Informationen auf dem Zertifikat:

- Trainingsinhalte
- Dauer des Kurses
- Art der Lernerfolgskontrolle
- Ende der Gültigkeit (Laufzeit)

**Das Abschlusszertifikat:** Das Zertifikat gilt als Nachweis einer Schulung im Sinne der DSGVO.

The image shows a sample of a Perseus training certificate. The certificate is titled 'TRAININGSZERTIFIKAT' and is issued to 'Monika Musterfrau' from 'Musterfirma'. It states that she successfully completed an online training course titled 'Cybersicherheits-Kurs'. The course content includes 'Grundlagen der Cybersicherheit' and 'Cybersicherheit in der Praxis'. The total duration is 15 minutes, and the certificate is valid until 19/01/2023. The certificate is issued by Perseus Technologies GmbH, located at Hardenbergstr. 32, 10623 Berlin, Germany. To the right of the certificate, there is a separate box titled 'Trainings-Zertifikate' which contains the text: 'Benötigen Sie alle abgeschlossenen Zertifikate Ihrer MitarbeiterInnen? Hier können Sie sich diese gebündelt als ZIP-Datei herunterladen.' Below this text is a checkbox labeled 'Zertifikate aus dem Archiv in den Download aufnehmen.' and a button labeled 'Zertifikate herunterladen'.

**Alle Zertifikate gesammelt laden:** Admins laden alle Mitarbeitenden-Zertifikate mit nur einem Klick herunter.

## Aktivierung von Mitarbeitenden

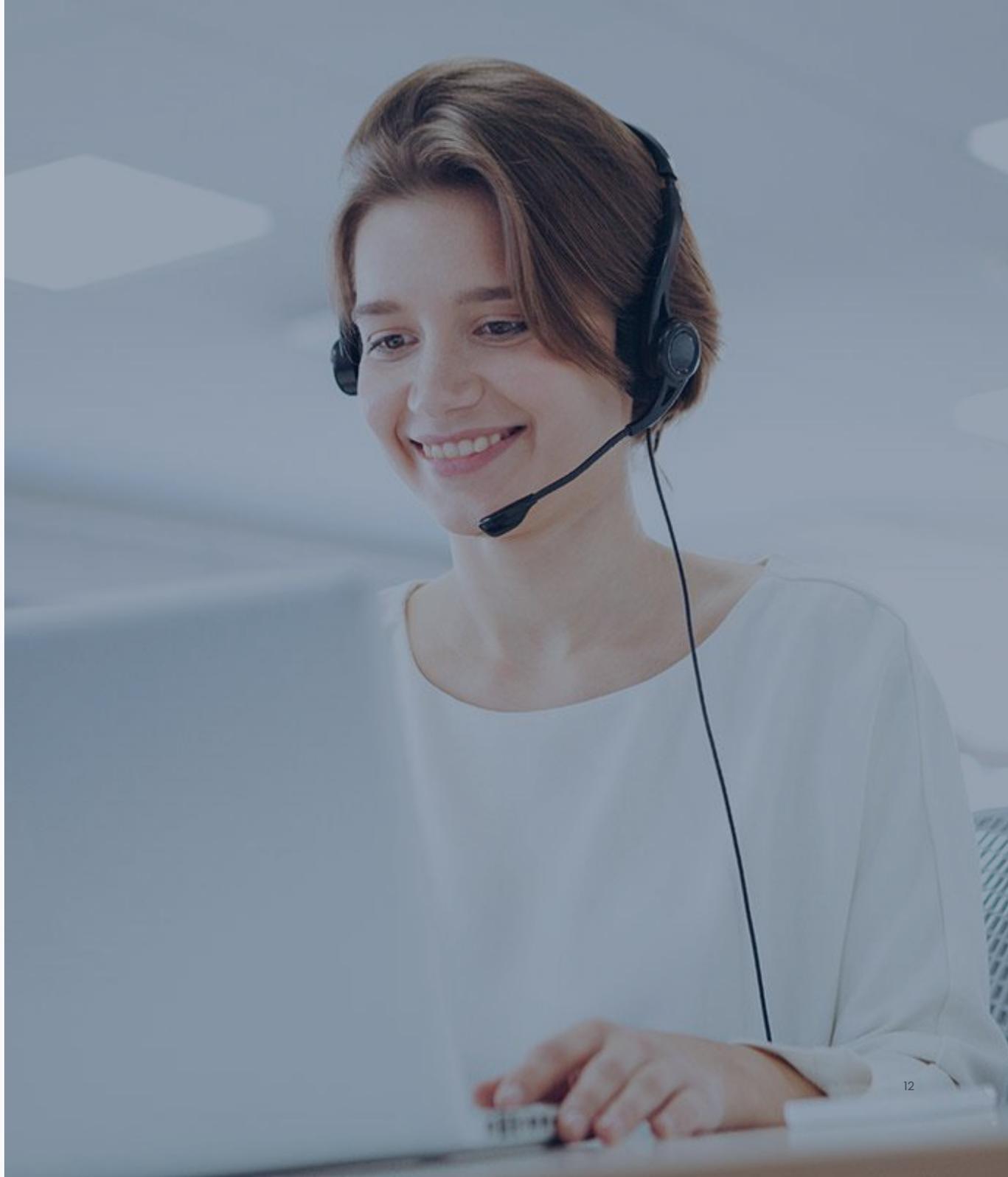
Auch wenn Sie und Ihre Mitarbeitenden Cybersicherheit in Ihrem Unternehmen ernst nehmen, geht der Fokus darauf in der täglichen Arbeit schnell verloren. Aus diesem Grund erinnert Perseus Sie und Ihre Mitarbeitenden regelmäßig daran, Online-Schulungen abzuschließen oder andere wichtige Maßnahmen durchzuführen.

### Zu Ihrer Entlastung erinnern wir Ihre Mitarbeitenden bspw. in automatischen E-Mails daran,...

- ... die Perseus-Anmeldung durchzuführen/abzuschließen,
- ... die Online-Trainings zu beginnen,
- ... die angefangenen Trainings zu beenden.

### Aktivierung von Verantwortlichen

Auch Admins werden wir durch gezielte und zweckgebundene E-Mails an wichtige Maßnahmen erinnern – zum Beispiel daran, Perseus-Einladungen an weitere Mitarbeitende zu versenden.



# Phishing-Simulation

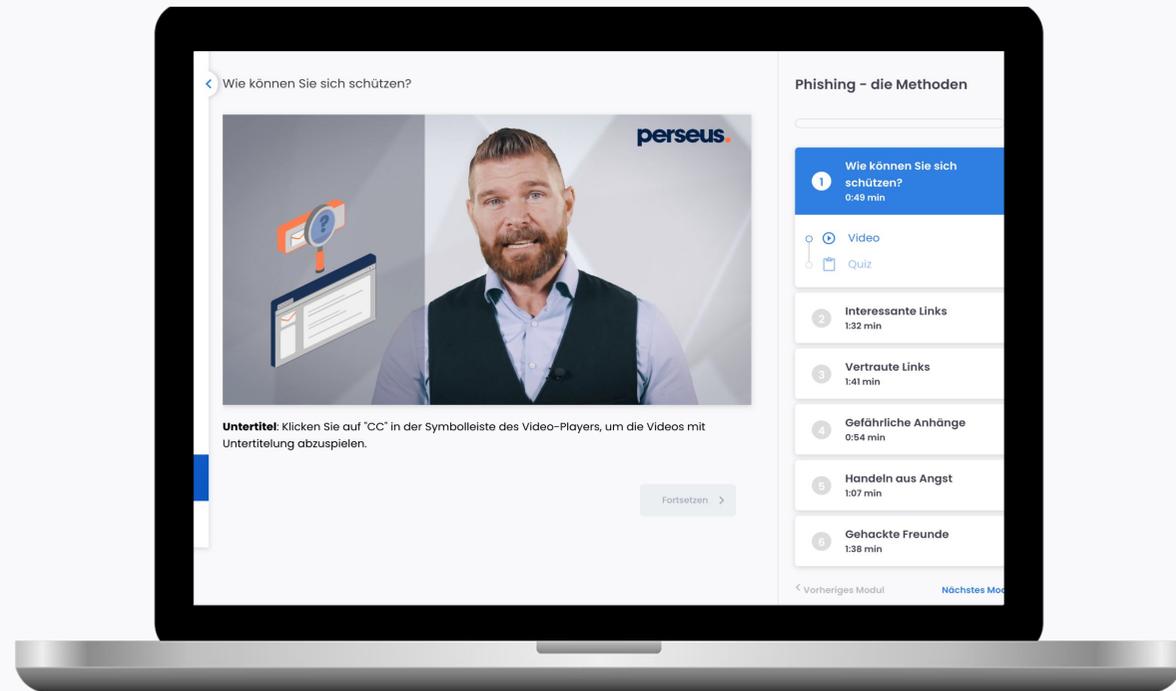
Mit simulierten Betrugs-E-Mails wird das Gefahrenbewusstsein Ihrer Mitarbeitenden kontinuierlich überprüft. Perseus führt in unregelmäßigen Abständen Phishing-Tests mit verschiedenen Vorlagen durch, die echten Phishing-Attacken nachempfunden sind.

## Theorie & Praxis effizient kombiniert

Phishing-Angriffe gehören zu den größten Cyberrisiken für Unternehmen. Unsere Phishing-Lernstrecke schult Ihre Mitarbeitenden mit leicht verständlichen Online-Videos, wie sie Gefahren erkennen und abwehren können. Im Anschluss wird dieses Wissen über Phishing-Simulationen im Arbeitsalltag beständig weiter trainiert.

## Lernen durch Sensibilisierung

Klicken Ihre Mitarbeitenden in einer unserer simulierten Phishing-Mails auf Anhänge oder Links, werden sie auf eine Trainingsseite weitergeleitet. Auf dieser Website werden Mitarbeitenden wiederholt über die Erkennungsmerkmale und Gefahren von Phishing-E-Mails aufgeklärt. Genau dieses wiederholte Training von Theorie und Praxis macht die Phishing-Lernstrecke von Perseus so effektiv und nachhaltig.



### Aktivierung

Mitarbeitende werden wiederholt an die Absolvierung der Phishing-Lernstrecke erinnert



### Online-Video-Training

Einfach verständliche Lernvideos klären Mitarbeitende über Phishing-Gefahren auf



### Phishing-Simulation

Simulierte Phishing-Mails testen Mitarbeitende auf Cyberwissen und bereiten sie auf den Ernstfall vor

# Phishing-Reporting

Admins können den Phishing-Status jederzeit einsehen und erhalten dadurch wichtige Informationen über die Cybersicherheit des Unternehmens.

## Kampagnen-Übersicht

Auf einen Blick erhalten Sie einen Überblick darüber, welche simulierten Phishing-Mails kürzlich an Ihre Mitarbeitenden verschickt wurden und wie erfolgreich Ihre Kolleginnen und Kollegen diese abwehren konnten. Falls Sie eine Dokumentation für ein internes Reporting benötigen, können Sie jederzeit per Klick eine ausführliche Statistik als XLS-Datei herunterladen.

## Sensibilisierung mit Abwechslung

Cyber-Awareness ist zwar ein ernstes Thema, doch Sensibilisierung kann auch Spaß machen. Bei richtigem Verhalten werden Mitarbeitende mit verschiedenen Phishing-Trophäen belohnt und können sich auf einer Rangliste mit ihren Kolleginnen und Kollegen messen. Das ermutigt, die eigenen Leistungen noch zu verbessern. Natürlich haben Mitarbeitende dabei die Möglichkeit, ihre Ergebnisse zu anonymisieren.



## Phishing-Trophäen

Mehr Lern-Anreiz durch Gamification-Elemente

Sie haben Fragen? Wir sind für Sie da.  
Telefon: 030/95 999 80 80  
(Mo - Fr 09:00-18:00)

**Zusammenfassung aller Mitarbeiter**  
Begleiten Sie die Fortschritte Ihrer Mitarbeiter. Erinnern Sie diese daran, ihr Training fortzusetzen und unsere Hilfsmittel zu nutzen, damit ihr Unternehmen geschützt bleibt.

Phishing erkannt ②  
Training absolviert  
Browser aktuell ③

### Phishing-Status des Unternehmens

Line chart showing phishing status from 27. Jan to 19. Feb. Y-axis: 0, 25, 50, 75, 100. X-axis: 27. Jan, 28. Jan, 30. Jan, 3. Feb, 10. Feb, 19. Feb. Legend: 40 Verschickt, 33 Geöffnet, 6 Geklickt.

11%  
Gesunken um -77%

### Kampagnen-Übersicht

Zeitspanne 21.01.2020 bis 20.02.2020 [Bericht herunterladen](#)

**Abmahnung**  
27.01.2020 - 27.01.2020  
3 Verschickt

**DSGVO**  
27.01.2020 - 28.01.2020  
3 Verschickt

### Top 3

Diesen Monat Immer

| Rang | Mitarbeiter        | 1 Punkt | 2 Punkte | 4 Punkte | Gesamtergebnis |
|------|--------------------|---------|----------|----------|----------------|
| 1    | Maxi Mustermann    | 23      | 2        | 1        | 30             |
| 2    | Anonym             | 22      | 1        | 1        | 26             |
| 3    | Max Beispiel       | 19      | 1        | 1        | 25             |
| 4    | Paul Fischer (Sie) | 19      | 0        | 1        | 23             |

1 Punkt 2 Punkte 4 Punkte

**Bestenliste**  
Spielerischer Wettbewerb kann Phishing-Ergebnisse und die Sicherheit des Unternehmens verbessern

# Werkzeugkasten für Cybersicherheit

Im Mitgliederbereich von Perseus finden Sie und Ihre Mitarbeitenden praktische und einfach zu bedienende Tools, um den Arbeitsalltag noch sicherer zu gestalten. Sobald Sie und Ihre Kolleginnen und Kollegen unsere Online-Trainings für Cybersicherheit und Datenschutz absolviert haben, werden Sie Hintergrund und Wichtigkeit unserer Werkzeuge verstehen und diese mühelos in die tägliche Arbeit integrieren.

Einen ersten Überblick über ihre Funktionalität und warum unsere Fachleute für Cybersicherheit Ihnen die Benutzung der Tools so dringend empfehlen, finden Sie auf dieser Seite. Die digitale Welt verändert sich und damit auch ihre Bedrohungen. Aus diesem Grund wird Perseus den Werkzeugkasten für Cybersicherheit für Ihr Unternehmen fortlaufend optimieren und neue Werkzeuge hinzufügen.



## Darknet-Scan

Wurde Ihre E-Mail-Adresse im Zusammenhang mit einem Daten- und Sicherheitsvorfall gemeldet, finden Sie das mit nur einem Klick heraus und können Maßnahmen ergreifen (bspw. Passwörter ändern).



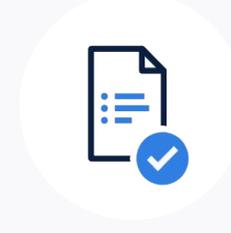
## Browser-Check

Veraltete Browser-Versionen sind ein enormes Sicherheitsrisiko und Einfallstor für kriminelle Hacker. Browser-Anbieter optimieren die Sicherheit ihrer Software regelmäßig. Sind die Browser in Ihrer Firma auf dem neuesten Stand? Mit unserem Werkzeugkasten finden Sie es im Nu heraus.



## Passwort-Erinnerung

Wahlweise können Ihre Mitarbeitenden die automatische Passwort-Erinnerung aktivieren. So werden sie alle 8 Wochen daran erinnert, ein neues und sicheres Passwort für Ihre betrieblichen Accounts zu erstellen.



## E-Mail-Scanner

Zur Verwendung für alle Ihre Mitarbeitenden ist im Werkzeugkasten die E-Mail-Adresse unseres Malware-Scanners hinterlegt. Einfach verdächtige E-Mail weiterleiten und in wenigen Minuten erfahren, ob Dateianhänge gefährlich oder unbedenklich sind. Denken Sie daran: 70 % der erfolgreichen Cyberangriffe erfolgen durch E-Mails.

## Darknet-Scan

Sind Ihre Daten im Darknet? Jeden Tag werden über eine Millionen Zugangsdaten gestohlen. Finden Sie heraus, ob Ihre Mitarbeitenden bereits betroffen sind.

Perseus durchsucht das Internet nach gestohlenen Daten, die von Hackern veröffentlicht wurden und lässt Sie wissen, ob eine der E-Mail-Adressen Ihres Unternehmens bei einer Sicherheitslücke entdeckt wurde. Anschließend helfen wir Ihnen, sich vor Datendiebstahl zu schützen.

Überprüfen Sie noch heute, ob Ihre Daten in Zusammenhang mit Sicherheitsvorfällen genannt werden.

### Darknet-Scan für Ihre Unternehmensdomain:

Wir überprüfen anhand Ihrer Unternehmens-Domain (z. B. @perseus.de), ob es Sicherheitsvorfälle im Zusammenhang mit Ihren Firmen-E-Mail-Adressen gab.

Ihre überprüfte Domain:  
**perseus.de**

✓ Für die Domain **perseus.de** ist kein Sicherheitsvorfall bekannt.



**Darknet & Erpressung**  
Hacker verkaufen Daten für Profit online oder erpressen betroffene Unternehmen



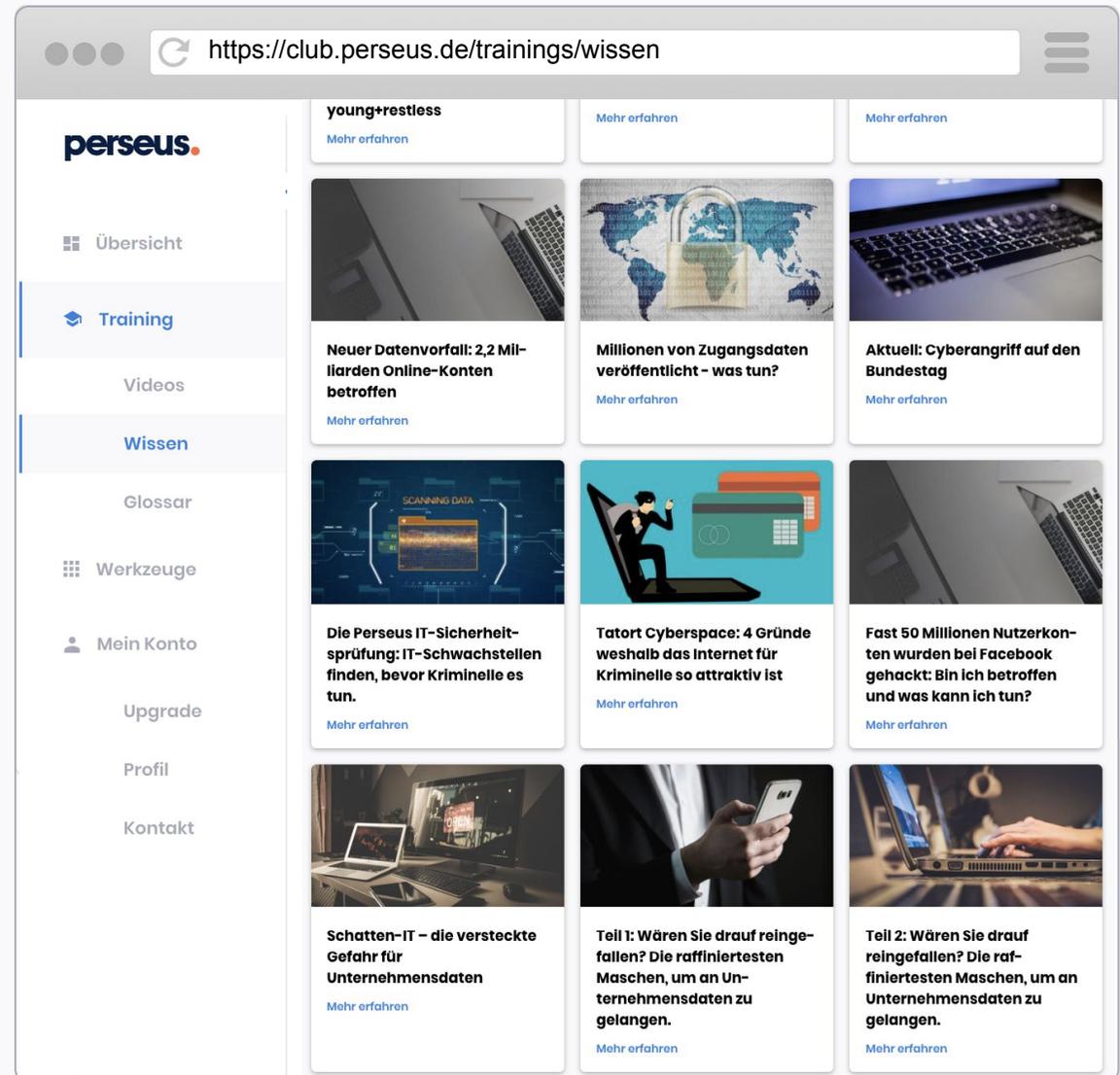
**Rache & Willkür**  
Kriminelle handeln auch aus politischen oder privaten Gründen oder wollen sich profilieren

# Blog, Newsletter & Glossar

Als Mitglied von Perseus werden Sie und Ihre Mitarbeitenden über aktuelle gesellschaftliche, rechtliche und technische Entwicklungen im Bereich Cybersicherheit informiert.

Wir wissen, was unser Geschäftsklientek bewegt und stellen regelmäßig neue Artikel mit Hintergrundinformationen und konkreten Handlungsempfehlungen in den Wissensbereich. Ausgewählte Themen stellen wir ebenfalls im Newsletter vor.

Sie haben keine Ahnung, was ein Botnet ist? Oder was bspw. Doxing oder Spoofing bedeutet? Kein Problem. In unserem fortlaufend aktualisierten Cyber-Glossar finden Sie und Ihre Mitarbeitenden die gängigen Begriffe aus der Welt der Cybersicherheit anschaulich und mit nützlichem Kontext erklärt.



# Gefahrenwarnung

Regelmäßig sorgen Hacker-Attacken, Datendiebstähle, Sicherheitslücken oder andere Cybervorfälle für Risiken in der digitalen Welt. Damit unsere Mitglieder rechtzeitig über mögliche neue Gefahren Bescheid wissen, gibt es die Perseus-Gefahrenwarnung.

Unsere Cybersicherheits-Fachleute erfahren frühzeitig von neuen Gefahren für Ihr Unternehmen und informieren Sie sofort per E-Mail.

## Handlungsempfehlung bei Gefahren

Neben Hintergründen und einer Einschätzung der Gefahren geben wir Ihnen und Ihren Mitarbeitenden natürlich auch direkte Empfehlungen dafür, wie Sie der neuen Gefahr vorbeugen können oder handeln sollten, falls Sie betroffen sind.

# In Zukunft sicher mit Perseus

Online-Portal für  
Cybersicherheit

Jetzt Demo anfragen

Sie haben Fragen? Wir sind für Sie da.

Hagelberger Str. 53-54  
10965 Berlin

030/95 999 80 80  
support@perseus.de

© 2017-2023 Perseus Technologies GmbH

## Über Perseus

Die Perseus Technologies GmbH wurde im September 2017 mit der Vision gegründet, dauerhaft IT-Sicherheit und Datenschutz zu ermöglichen. Ziel des mitarbeiterzentrierten Angebots von Perseus ist die Etablierung einer langfristigen Cybersicherheitskultur entlang aller Phasen einer Cyberattacke. Das Perseus-Konzept umfasst unter anderem browserbasierte Mitarbeitertrainings, Sensibilisierung durch Phishing-Simulationen, Tools für bessere Cybersicherheit, eine 24/7-Cyber-Notfallhilfe sowie Risikobewertung.

Der Unternehmensname Perseus lehnt sich an die Legende des Perseus an. Dieser Held der griechischen Mythologie steht für Schutz und Sicherheit. Für sein Engagement wurde Perseus im Dezember 2018 von Google und der Süddeutschen Zeitung mit dem Digitalen Leuchtturm Award für innovative Versicherungsprodukte ausgezeichnet.

Unsere mehr als 50 Mitarbeitenden kommen aus über 15 Nationen und arbeiten gemeinsam im Fintech Hub H:32 in Berlin. Perseus ist seit dem 1. Februar 2020 zu 100 Prozent Teil der HDI Gruppe.