SICHERHEIT IM INTERNET

VORTRAG SMARTPHONE-TRAINING

ZIEL DES HEUTIGEN TRAINING

Beantwortung von 3 Kernfragen:

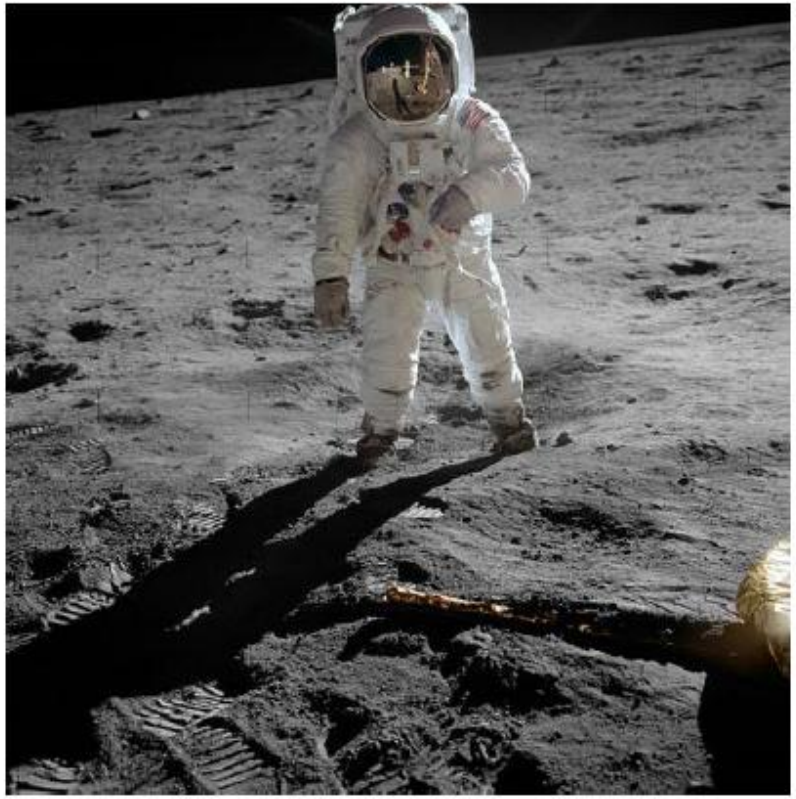
- **Warum** ist die Internetnutzung überhaupt sicherheitsrelevant?
- **Was** sind die wichtigsten Schutzmaßnahmen?
- **Wie** kann ich mich schützen?

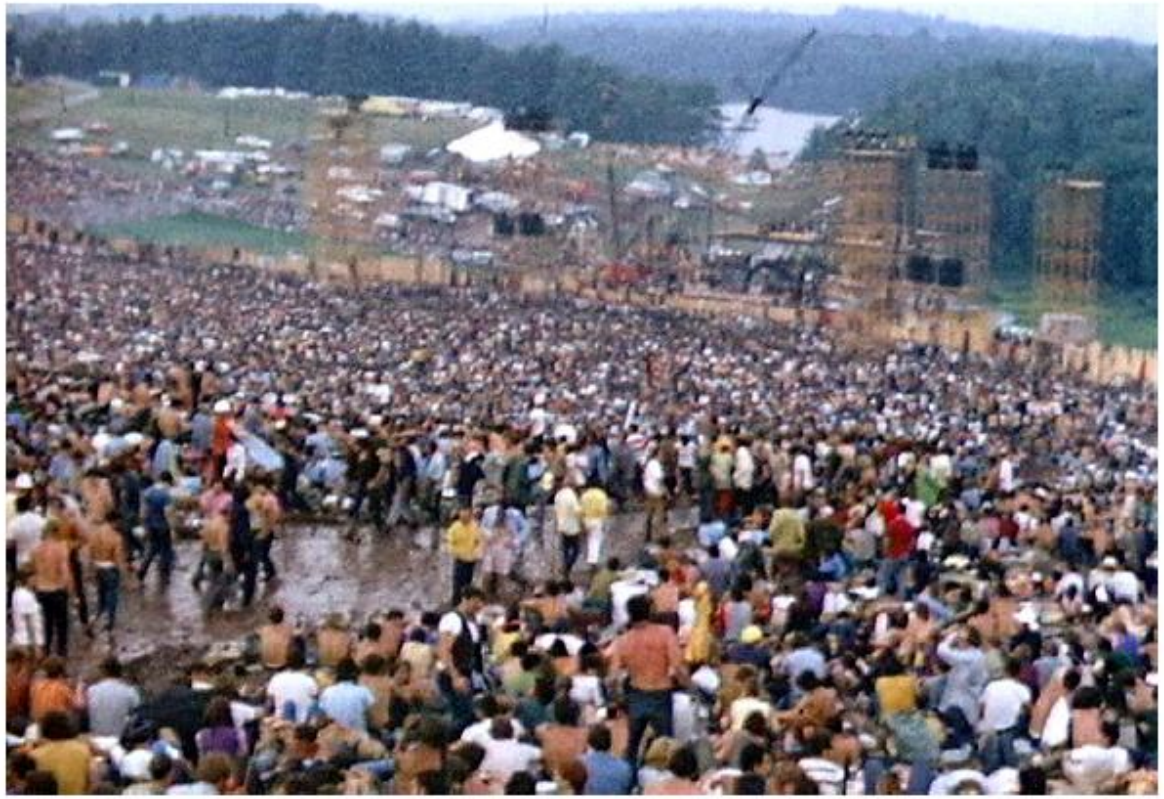
SICHERHEIT IM INTERNET

- **Angriffsziel Internet**
- Schutzmaßnahmen
- Stiftung Warentest

INTERNET: GEBURTSSTUNDE DES INTERNET – DAS JAHR 1969

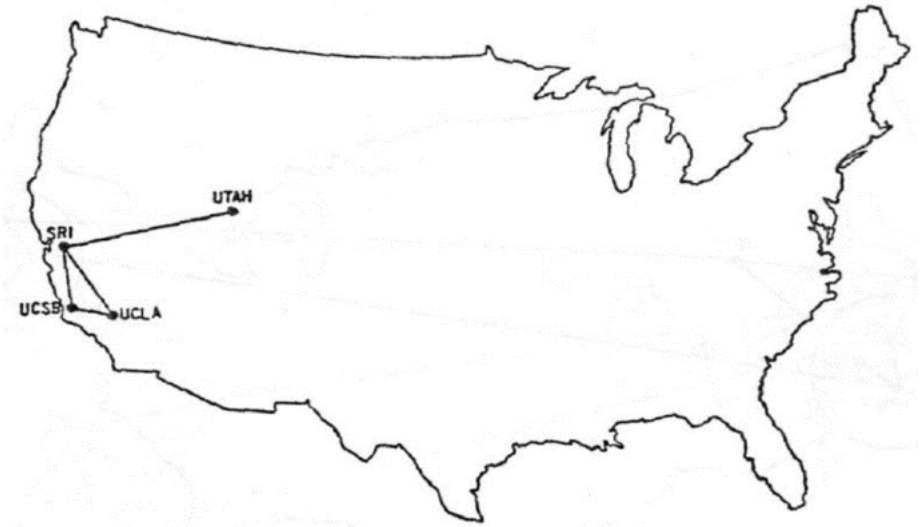
- **1969: Woran erinnern Sie sich?**





INTERNET: WIE FING ALLES AN?

- **Ziel: Wissenschaftlicher Austausch und Pilotierung**
  - Kann man über Plattform- und Netzwerkgrenzen hinweg kommunizieren?
  - Eine der ersten Anwendungen: Telnet erlaubte Wissenschaftlern, sich auf Rechner an einem entfernten Ort einzuloggen



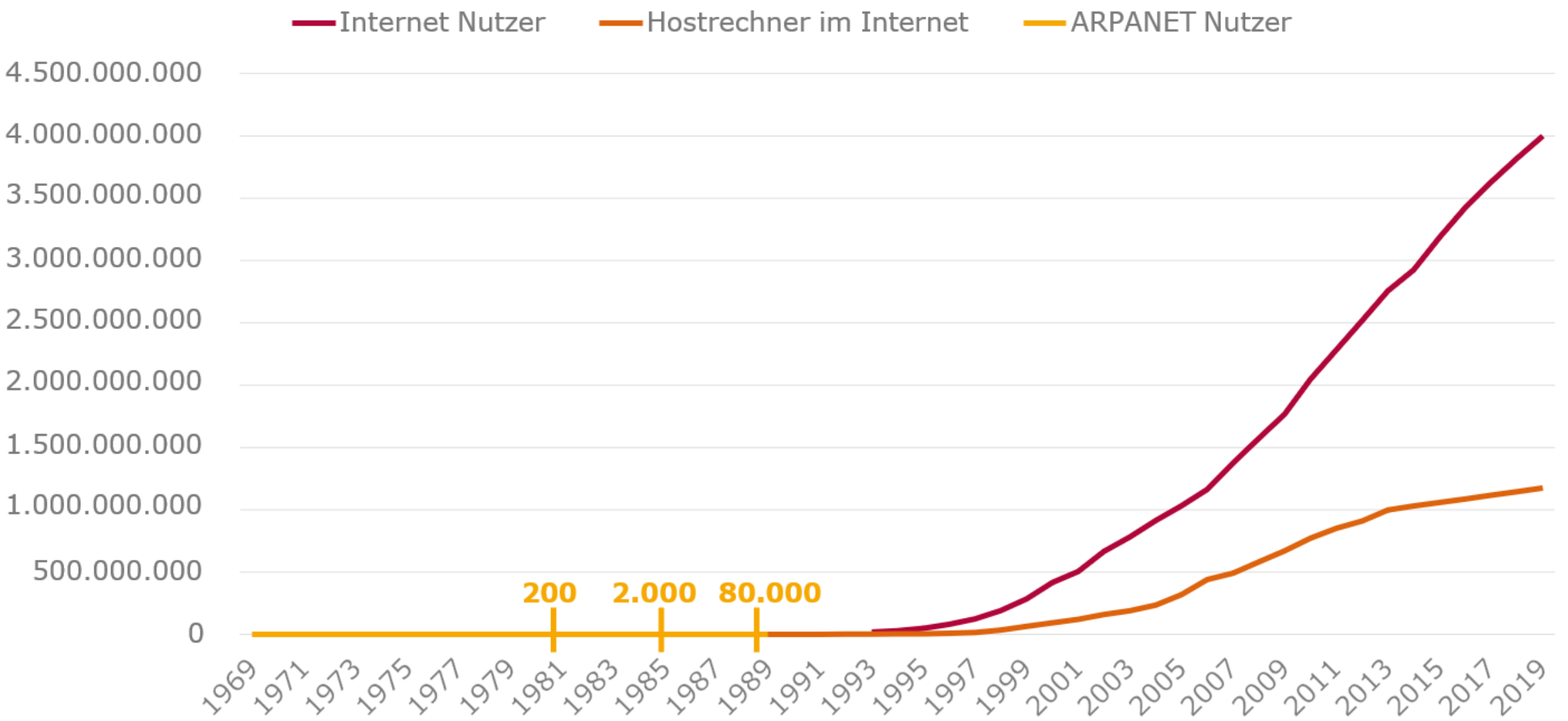
The ARPANET in December 1969

University of California, Santa Barbara
University of California, Los Angeles
Stanford Research Institute, San Francisco

Das **ARPANET** (englisch: Advanced Research Projects Agency Network) war ein Computernetzwerk und wurde ursprünglich im Auftrag der US Air Force ab 1968 von einer **kleinen Forschergruppe** unter der Leitung des **MIT und des US-Verteidigungsministeriums** entwickelt.

Es ist der **Vorläufer des heutigen Internets**.

INTERNET HEUTE: DAS NETZ DER NETZE



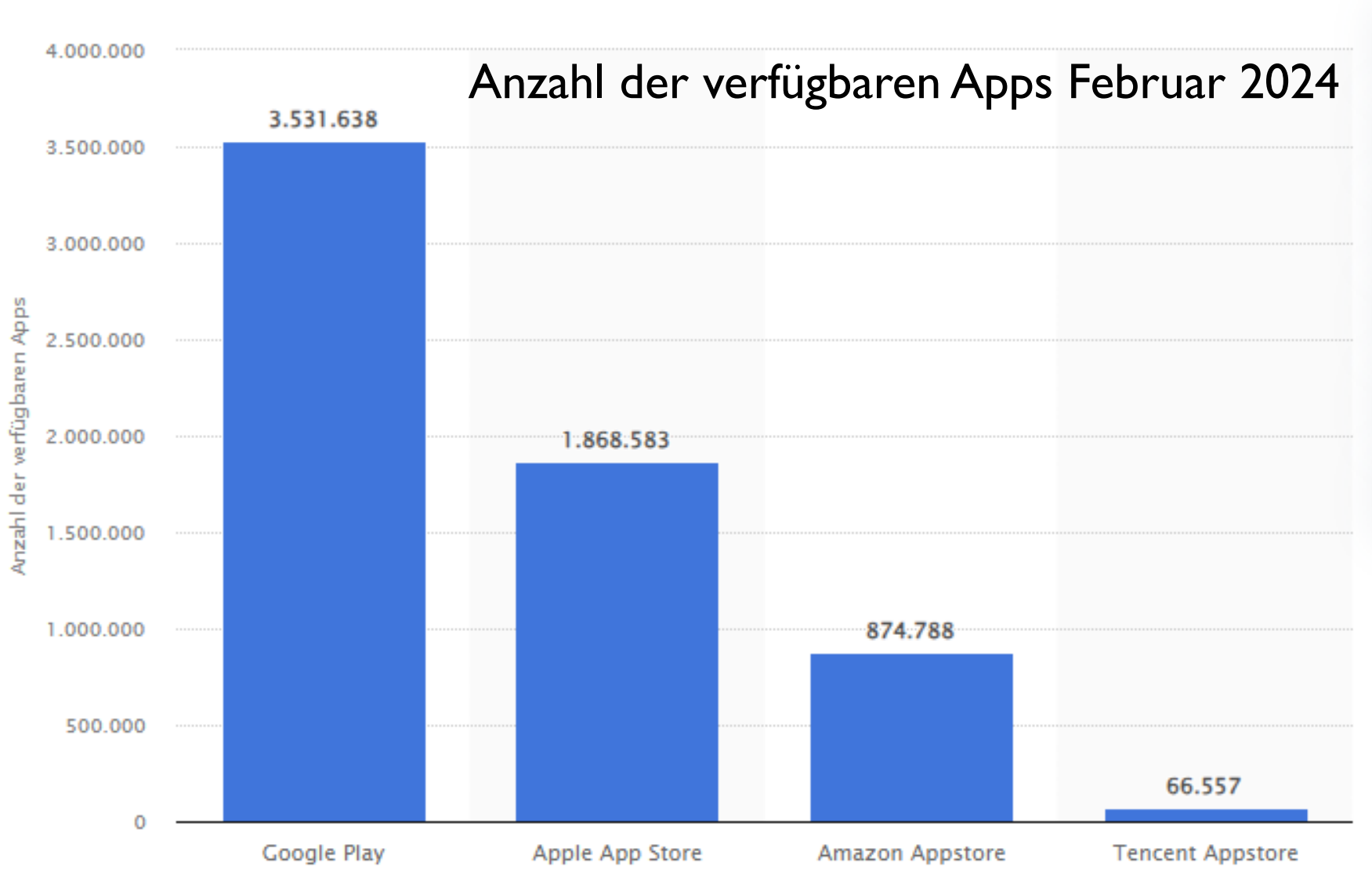
INTERNET HEUTE: SICHERHEITSPROBLEMATIK SYSTEMBEDINGT

- Internet begann als Forschungsprojekt
  - kleine Forschungsgemeinschaft mit überschaubaren und vertrauenswürdigen Klientel
- **Sicherheit war kein primärer Gesichtspunkt bei der Entwicklung von Internetprotokollen**
  - Typischer Satz in den Internet-Standards: „Sicherheitsfragen werden in diesem Memo nicht behandelt"
- **Internet ist Verbund unabhängiger Rechnernetze**: keine Internet-Behörde und keine staatliche Stelle kann das gesamte Internet kontrollieren
- **Time-to-Market**

INTERNET HEUTE: DAS NETZ DER NETZE

- Milliarden von Eintrittsstellen weltweit
- Millionen von miteinanderverbundenen Netzwerken
- Viele Design- und Konfigurationsfehler in Protokollen, Systemen und Anwendungen
- Große Anzahl an Schwachstellen und Sicherheitslücken

INTERNET HEUTE: SICHERHEITSPROBLEMATIK SYSTEMBEDINGT



SICHERHEIT IM INTERNET

- Angriffsziel Internet
- **Schutzmaßnahmen**
- Stiftung Warentest

WICHTIGE SCHUTZMASSNAHMEN

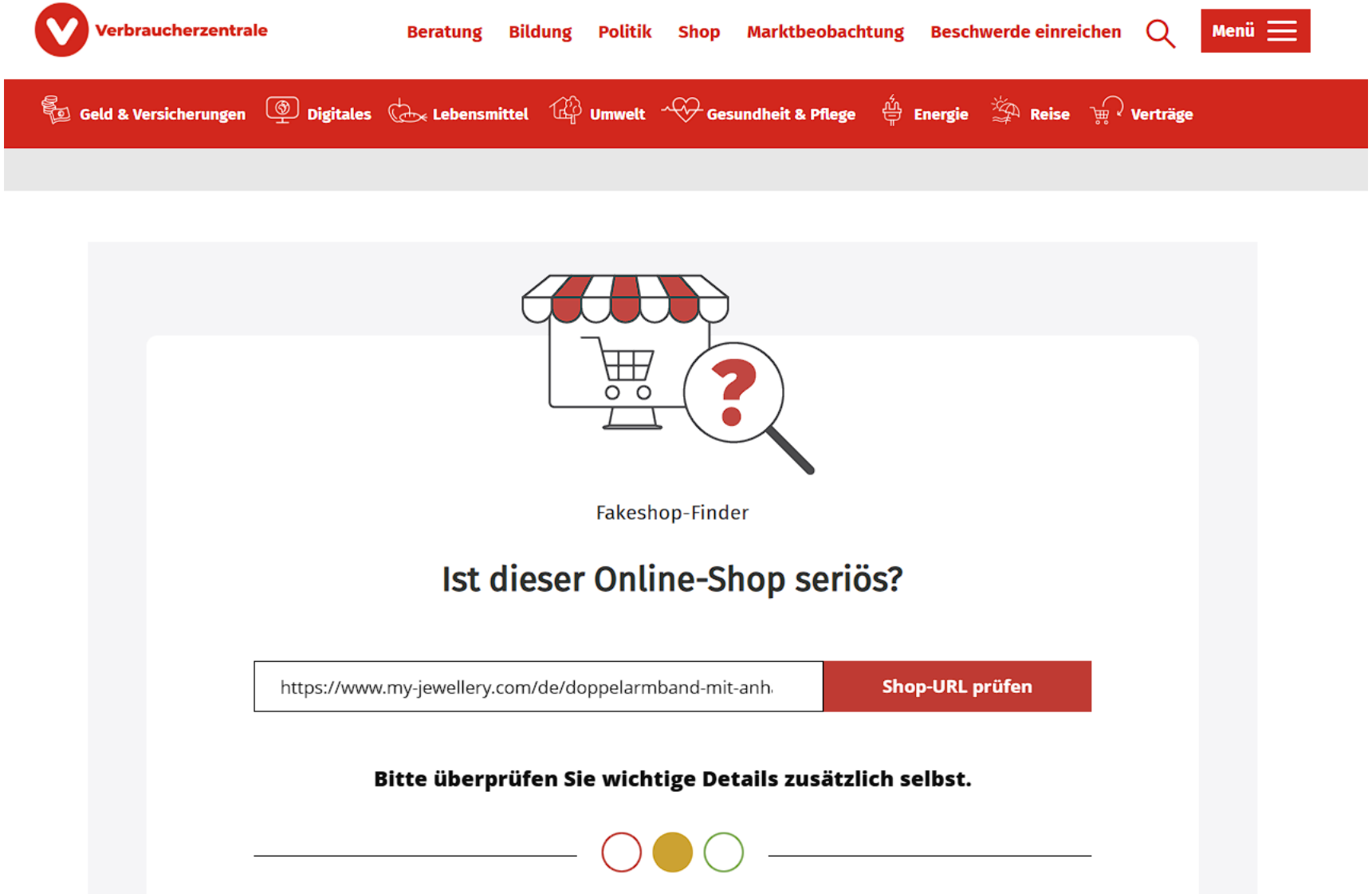
- Fakeshop Finder
- PHISHING EMAILS
- ANTI-VIRUS SOFTWARE
- ORGANISATORISCHE MASSNAHMEN
- SPERR-BILDSCHIRM
- Sicherheit und Datenschutz (Smartphone Einstellungen)

FAKESHOPS

Foto: Verbraucherzentrale

FAKESHOP FINDER

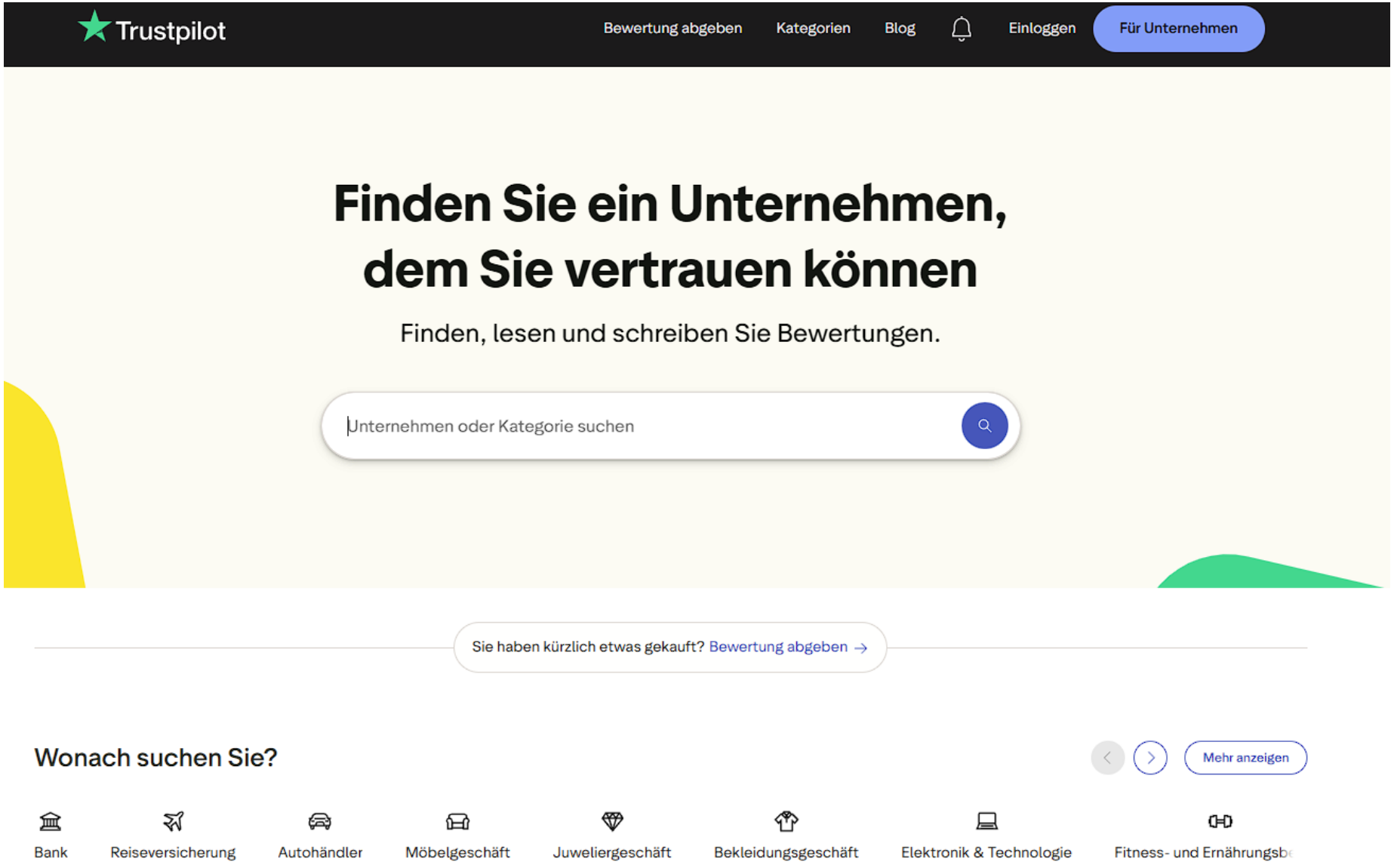
FINDER



FAKESHOP ERKENNUNGSKRITERIEN

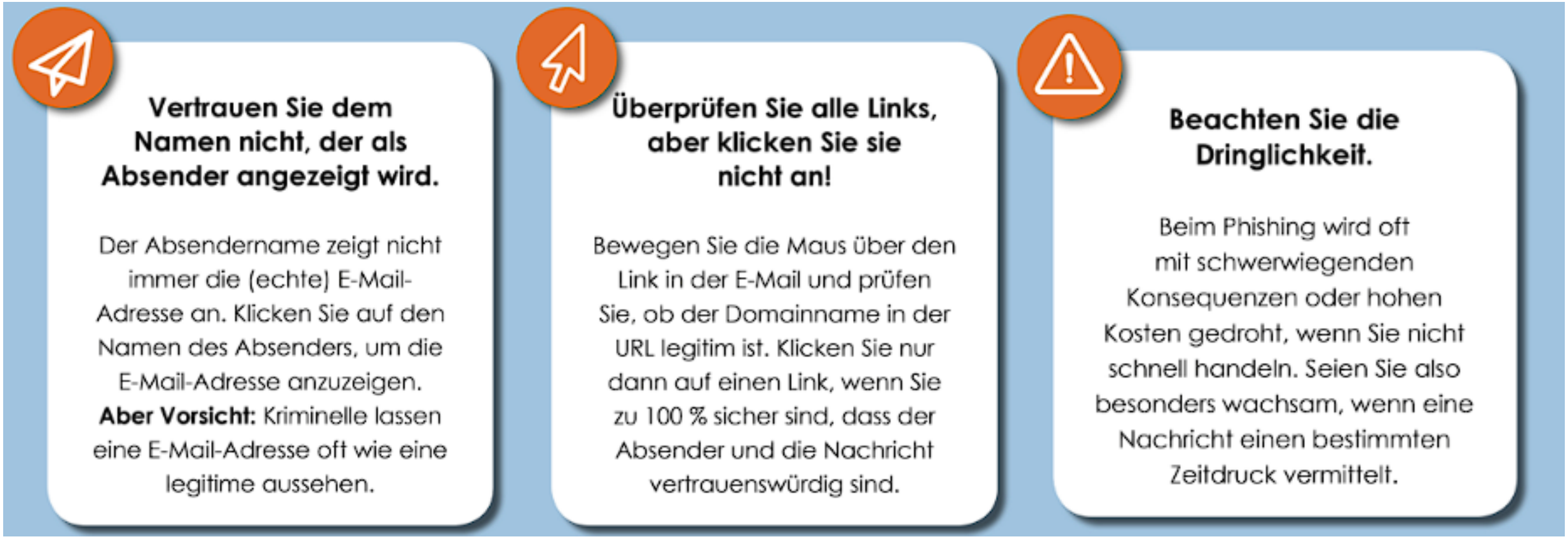
Kriterien

ONLINESHOP BEWERTUNGEN - TRUSTPILOT



PHISHING E-MAILS

PHISHING E-MAILS



Vertrauen Sie dem Namen nicht, der als Absender angezeigt wird.

Der Absendername zeigt nicht immer die (echte) E-Mail-Adresse an. Klicken Sie auf den Namen des Absenders, um die E-Mail-Adresse anzuzeigen. **Aber Vorsicht:** Kriminelle lassen eine E-Mail-Adresse oft wie eine legitime aussehen.

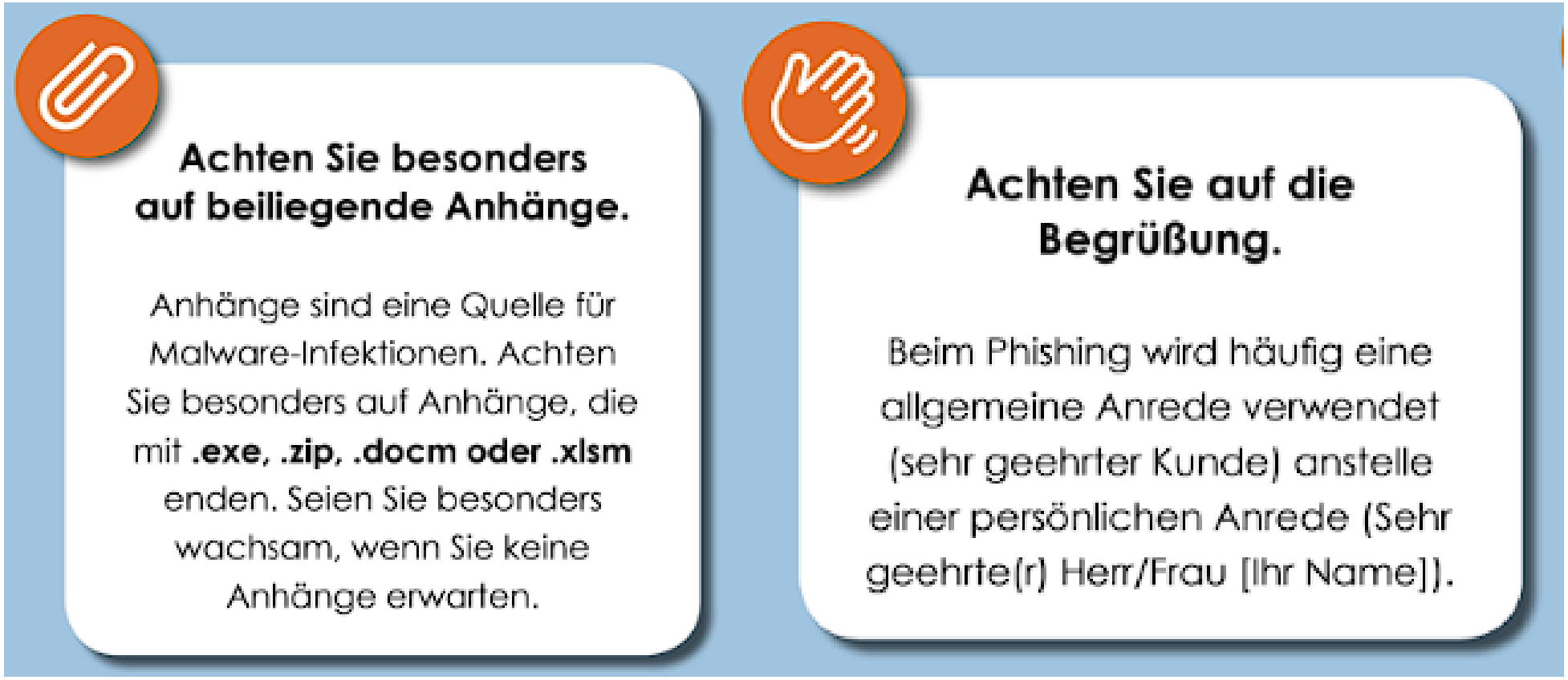
Überprüfen Sie alle Links, aber klicken Sie sie nicht an!

Bewegen Sie die Maus über den Link in der E-Mail und prüfen Sie, ob der Domainname in der URL legitim ist. Klicken Sie nur dann auf einen Link, wenn Sie zu 100 % sicher sind, dass der Absender und die Nachricht vertrauenswürdig sind.

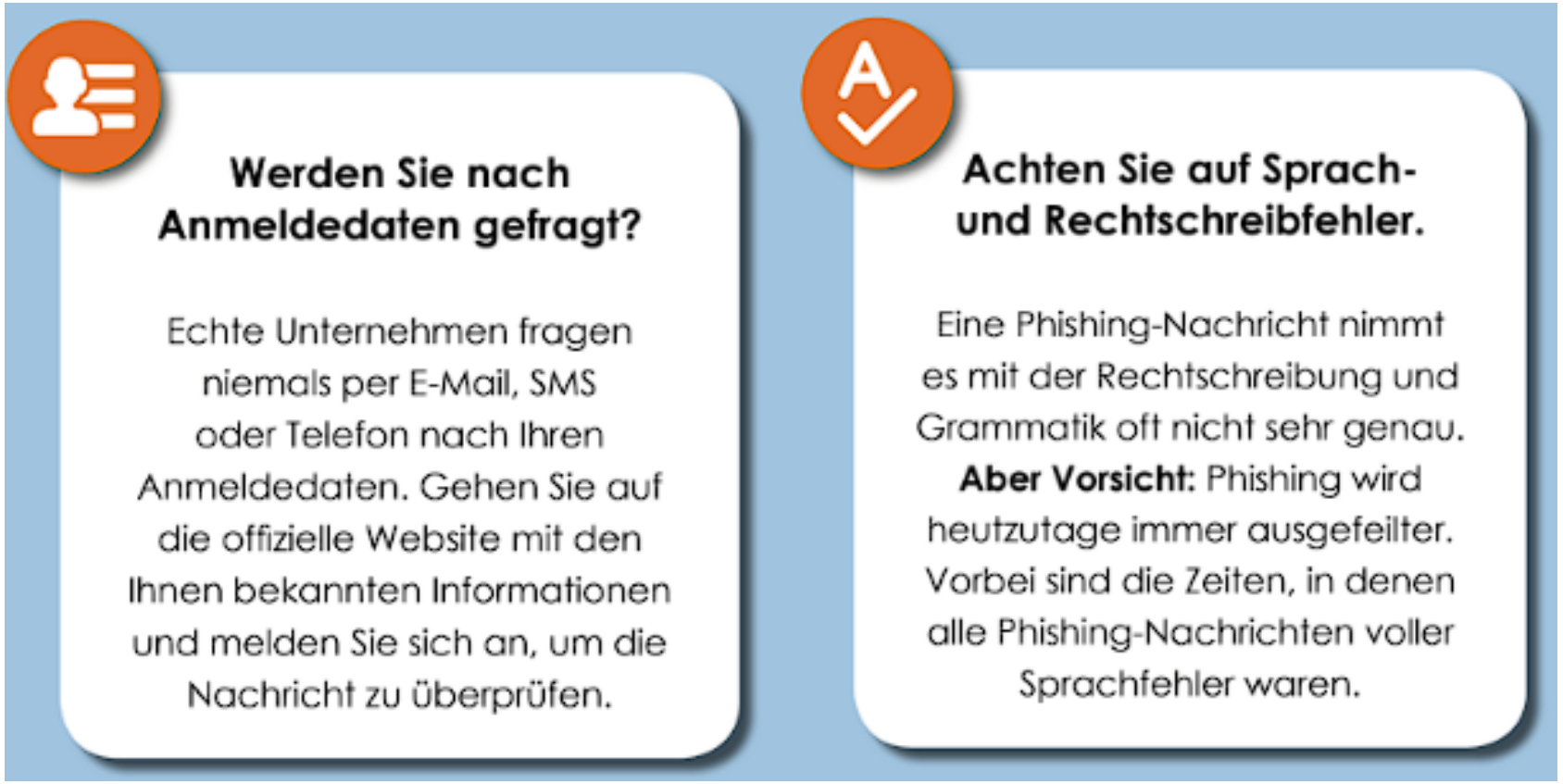
Beachten Sie die Dringlichkeit.

Beim Phishing wird oft mit schwerwiegenden Konsequenzen oder hohen Kosten gedroht, wenn Sie nicht schnell handeln. Seien Sie also besonders wachsam, wenn eine Nachricht einen bestimmten Zeitdruck vermittelt.

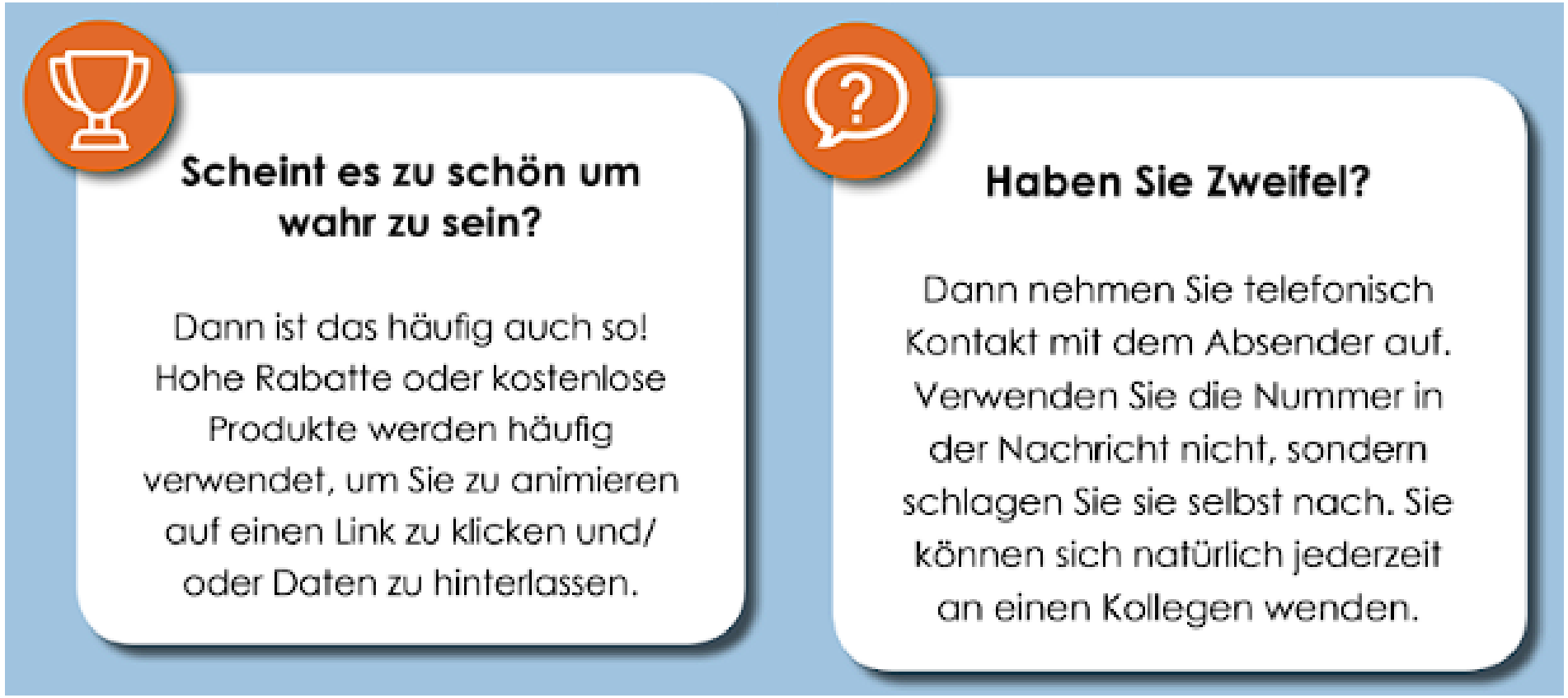
PHISHING E-MAILS



PHISHING E-MAILS

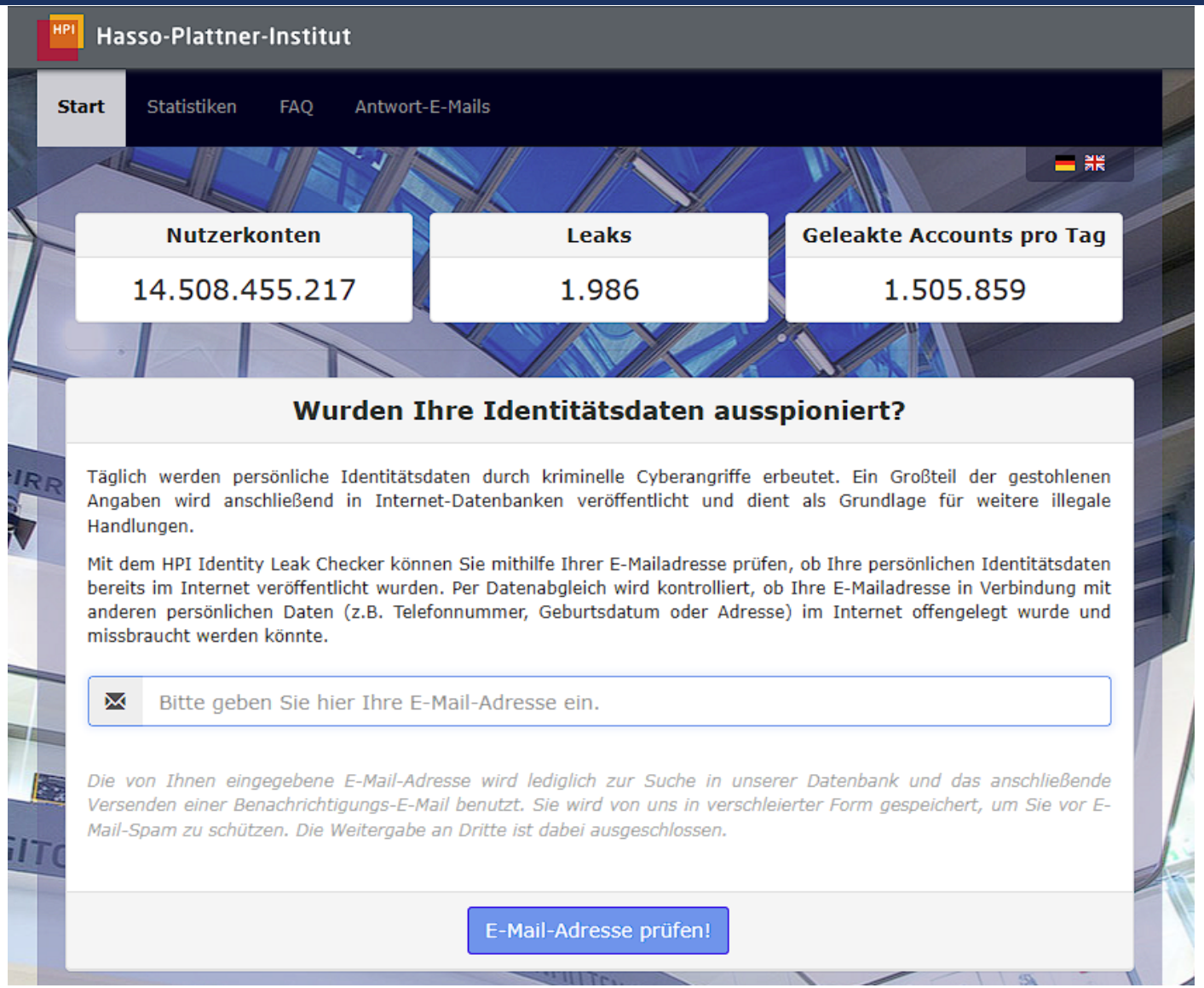


PHISHING E-MAILS



PHISHING E-MAILS

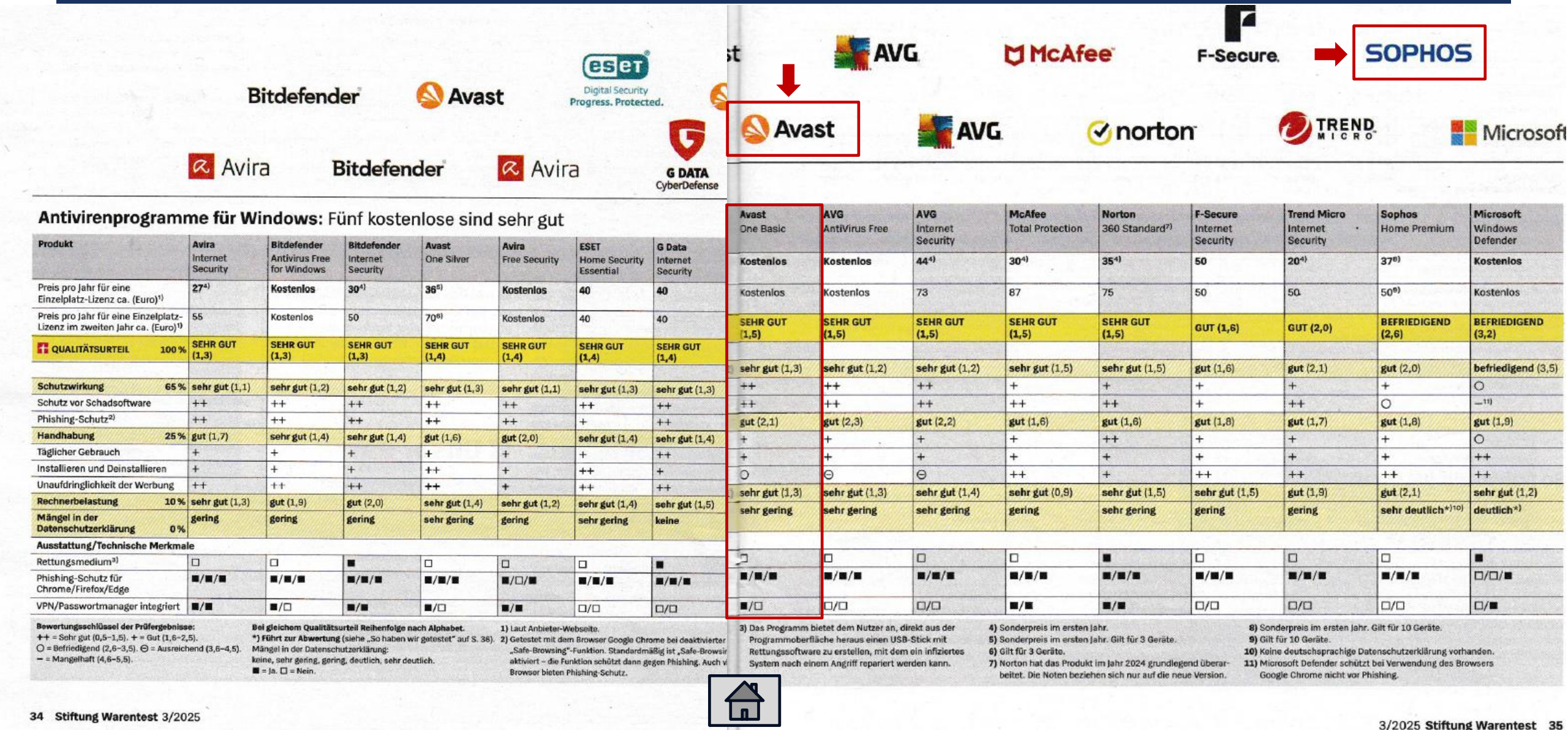
PHISHING E-MAILS



ANTIVIRUS SOFTWARE

- Programme bieten Verfahren zum Detektieren von Malware
- Erkennen neben Viren auch Würmer, Trojaner, Spyware und andere Schadsoftware
- Überwachen Internetverbindungen und warnen vor unsicheren Internetseiten
- Sind heute zwingender Bestandteil von Systemen
- **Muss stets auf neuestem Stand gehalten werden:** Ständig aktualisierte Virendefinitionen ermöglichen auch Auffinden neuer Viren und Malware
- **Durchsucht im Idealfall alle Datenquellen nach Viren:** Wechselmedien (Externe Festplatte, CD, USB-Sticks,…), Netzwerkverbindungen, …

ANTIVIRUS SOFTWARE **FÜR ANDROID**: STIFTUNG WARENTEST 3/2025



Bitdefender Avast ESET Digital Security Progress. Protected. Avira Bitdefender Avira G DATA CyberDefense

Antivirenprogramme für Windows: Fünf kostenlose sind sehr gut

Produkt	Avira Internet Security	Bitdefender Antivirus Free for Windows	Bitdefender Internet Security	Avast One Silver	Avira Free Security	ESET Home Security Essential	G Data Internet Security
Preis pro Jahr für eine Einzelplatz-Lizenz ca. (Euro)[1]	27[4]	Kostenlos	30[4]	36[5]	Kostenlos	40	40
Preis pro Jahr für eine Einzelplatz-Lizenz im zweiten Jahr ca. (Euro)[1]	55	Kostenlos	50	70[6]	Kostenlos	40	40
QUALITÄTSURTEIL 100 %	SEHR GUT (1,3)	SEHR GUT (1,3)	SEHR GUT (1,3)	SEHR GUT (1,4)	SEHR GUT (1,4)	SEHR GUT (1,4)	SEHR GUT (1,4)
Schutzwirkung 65 %	sehr gut (1,1)	sehr gut (1,2)	sehr gut (1,2)	sehr gut (1,3)	sehr gut (1,1)	sehr gut (1,3)	sehr gut (1,3)
Schutz vor Schadsoftware	++	++	++	++	++	++	++
Phishing-Schutz[2]	++	++	++	++	++	+	++
Handhabung 25 %	gut (1,7)	sehr gut (1,4)	sehr gut (1,4)	gut (1,6)	gut (2,0)	sehr gut (1,4)	sehr gut (1,4)
Täglicher Gebrauch	+	+	+	+	+	+	++
Installieren und Deinstallieren	+	+	+	++	+	++	+
Unaufdringlichkeit der Werbung	++	++	++	++	+	++	++
Rechnerbelastung 10 %	sehr gut (1,3)	gut (1,9)	gut (2,0)	sehr gut (1,4)	sehr gut (1,2)	sehr gut (1,4)	sehr gut (1,5)
Mängel in der Datenschutzerklärung 0 %	gering	gering	gering	sehr gering	gering	sehr gering	keine
Ausstattung/Technische Merkmale							
Rettungsmedium[3]	□	□	■	□	□	□	■
Phishing-Schutz für Chrome/Firefox/Edge	■/■/■	■/■/■	■/■/■	■/■/■	■/□/■	■/■/■	■/■/■
VPN/Passwortmanager integriert	■/■	■/□	■/■	■/□	■/■	□/□	□/□

Bewertungsschlüssel der Prüfergebnisse:
++ = Sehr gut (0,5–1,5). + = Gut (1,6–2,5).
○ = Befriedigend (2,6–3,5). ⊖ = Ausreichend (3,6–4,5).
– = Mangelhaft (4,6–5,5).

Bei gleichem Qualitätsurteil Reihenfolge nach Alphabet.
***) Führt zur Abwertung** (siehe „So haben wir getestet" auf S. 36).
Mängel in der Datenschutzerklärung:
keine, sehr gering, gering, deutlich, sehr deutlich.
■ = Ja. □ = Nein.

1) Laut Anbieter-Webseite.
2) Getestet mit dem Browser Google Chrome bei deaktivierter „Safe-Browsing"-Funktion. Standardmäßig ist „Safe-Browsir aktiviert – die Funktion schützt dann gegen Phishing. Auch v Browser bieten Phishing-Schutz.

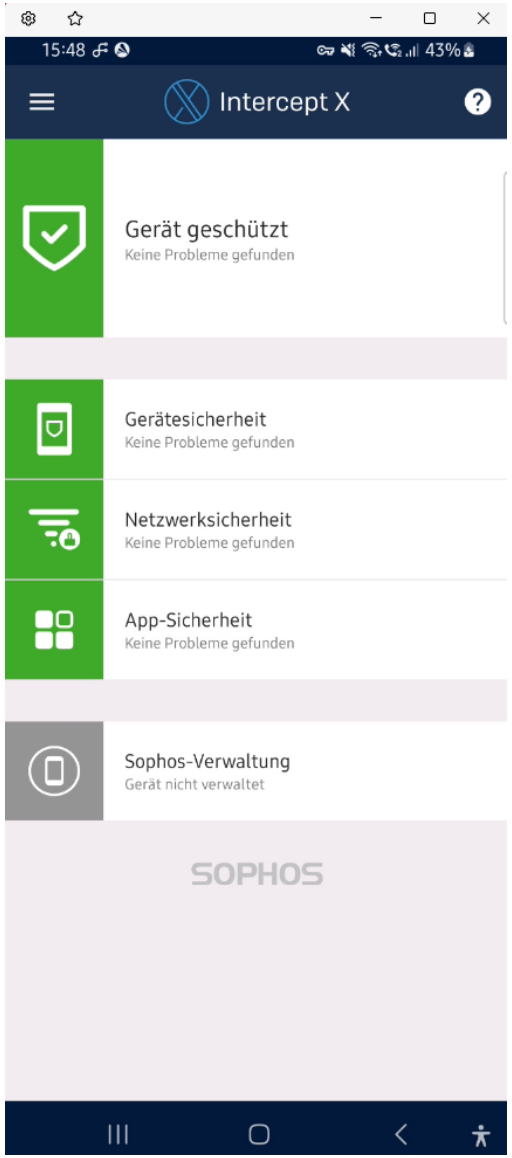
Avast AVG McAfee F-Secure SOPHOS

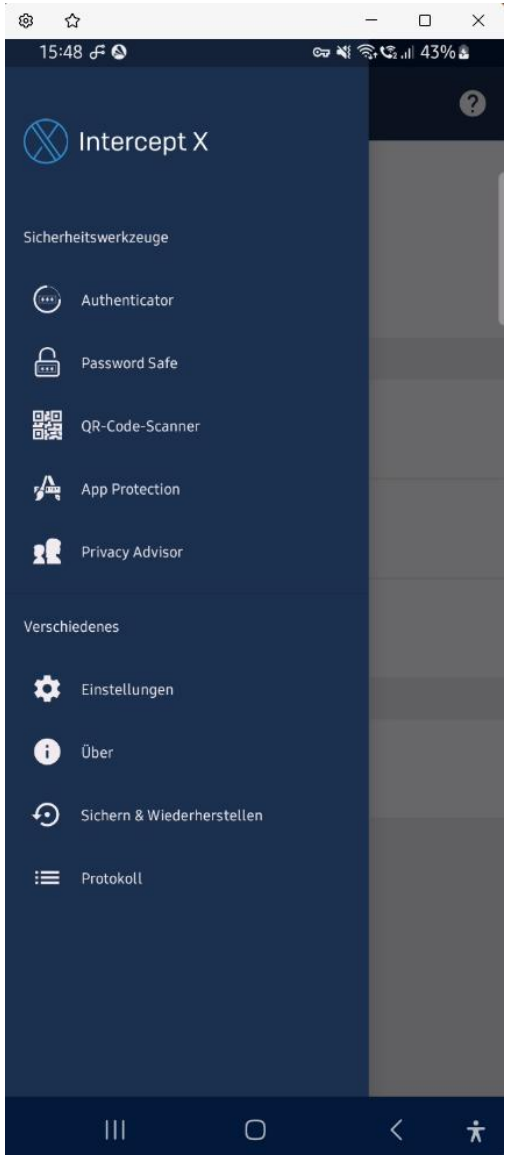
Avast AVG norton TREND MICRO Microsoft

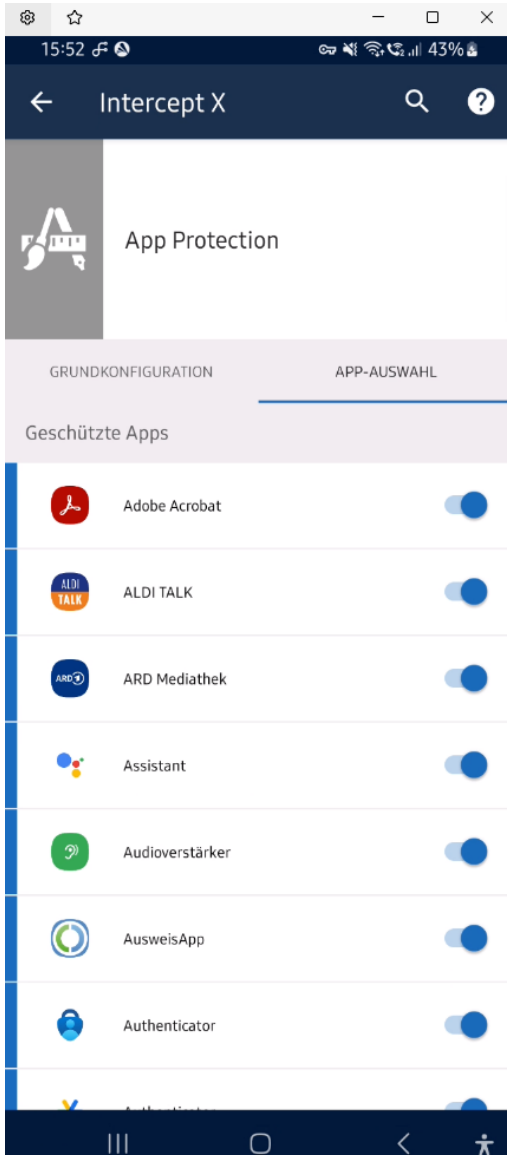
Avast One Basic	AVG AntiVirus Free	AVG Internet Security	McAfee Total Protection	Norton 360 Standard[7]	F-Secure Internet Security	Trend Micro Internet Security	Sophos Home Premium	Microsoft Windows Defender
Kostenlos	Kostenlos	44[4]	30[4]	35[4]	50	20[4]	37[8]	Kostenlos
Kostenlos	Kostenlos	73	87	75	50	50	50[9]	Kostenlos
SEHR GUT (1,5)	SEHR GUT (1,5)	SEHR GUT (1,5)	SEHR GUT (1,5)	SEHR GUT (1,5)	GUT (1,6)	GUT (2,0)	BEFRIEDIGEND (2,6)	BEFRIEDIGEND (3,2)
sehr gut (1,3)	sehr gut (1,2)	sehr gut (1,2)	sehr gut (1,5)	sehr gut (1,5)	gut (1,6)	gut (2,1)	gut (2,0)	befriedigend (3,5)
++	++	++	+	+	+	+	+	○
++	++	++	++	++	+	++	○	–[11]
gut (2,1)	gut (2,3)	gut (2,2)	gut (1,6)	gut (1,6)	gut (1,8)	gut (1,7)	gut (1,8)	gut (1,9)
+	+	+	+	++	+	+	+	○
+	+	+	+	+	+	+	+	++
○	⊖	⊖	++	+	++	++	++	++
sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,4)	sehr gut (0,9)	sehr gut (1,5)	sehr gut (1,5)	gut (1,9)	gut (2,1)	sehr gut (1,2)
sehr gering	sehr gering	sehr gering	gering	sehr gering	gering	gering	sehr deutlich*)[10]	deutlich*)
□	□	□	□	■	□	□	□	■
■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	□/□/■
■/□	□/□	□/□	■/■	■/■	□/□	□/□	□/□	□/■

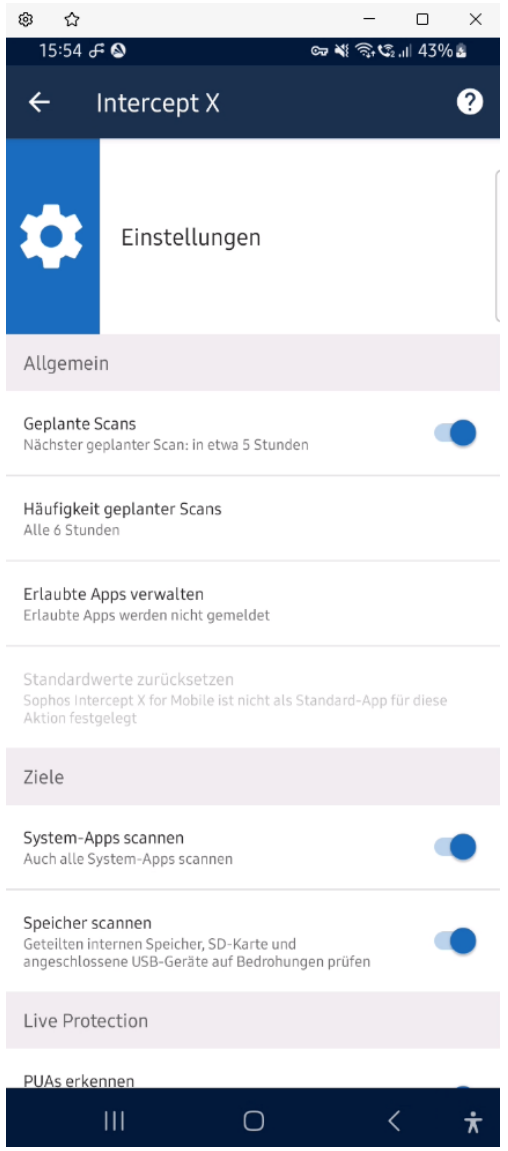
3) Das Programm bietet dem Nutzer an, direkt aus der Programmoberfläche heraus einen USB-Stick mit Rettungssoftware zu erstellen, mit dem ein infiziertes System nach einem Angriff repariert werden kann.
4) Sonderpreis im ersten Jahr.
5) Sonderpreis im ersten Jahr. Gilt für 3 Geräte.
6) Gilt für 3 Geräte.
7) Norton hat das Produkt im Jahr 2024 grundlegend überarbeitet. Die Noten beziehen sich nur auf die neue Version.
8) Sonderpreis im ersten Jahr. Gilt für 10 Geräte.
9) Gilt für 10 Geräte.
10) Keine deutschsprachige Datenschutzerklärung vorhanden.
11) Microsoft Defender schützt bei Verwendung des Browsers Google Chrome nicht vor Phishing.

ANTIVIRUS SOFTWARE – BEISPIEL INTERCEPT X (KOSTENLOS VERSION)

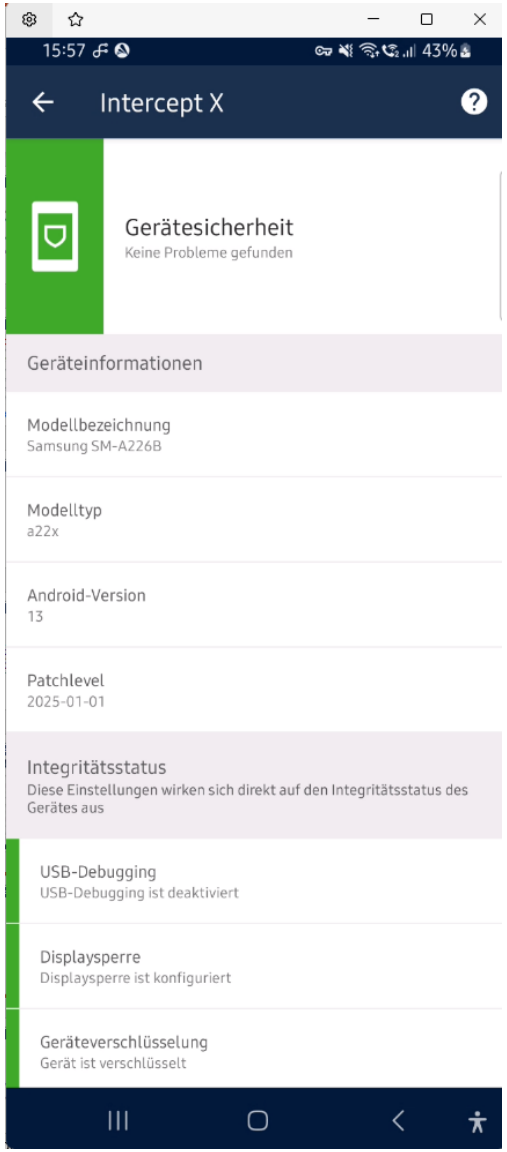


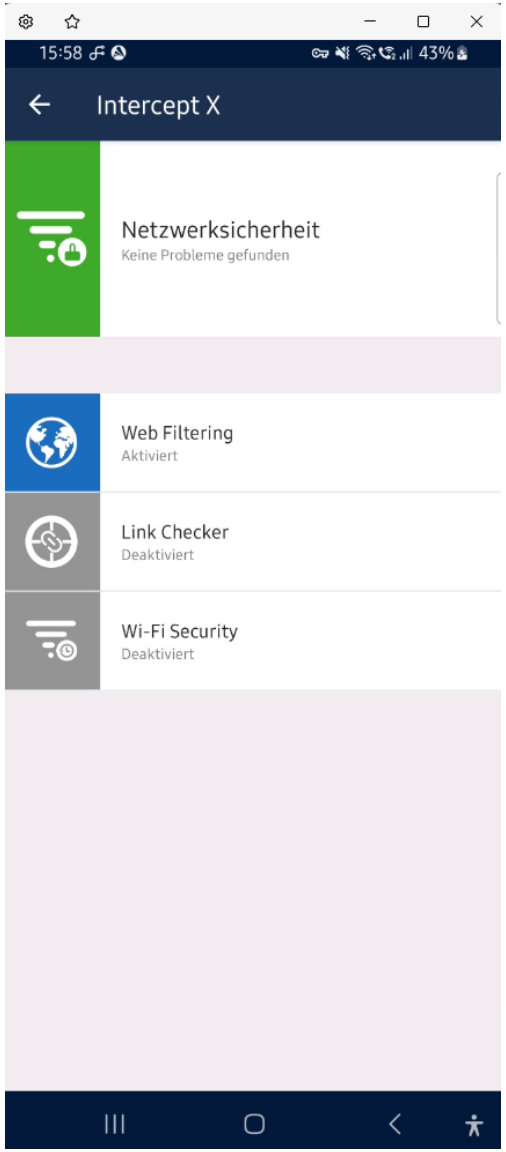


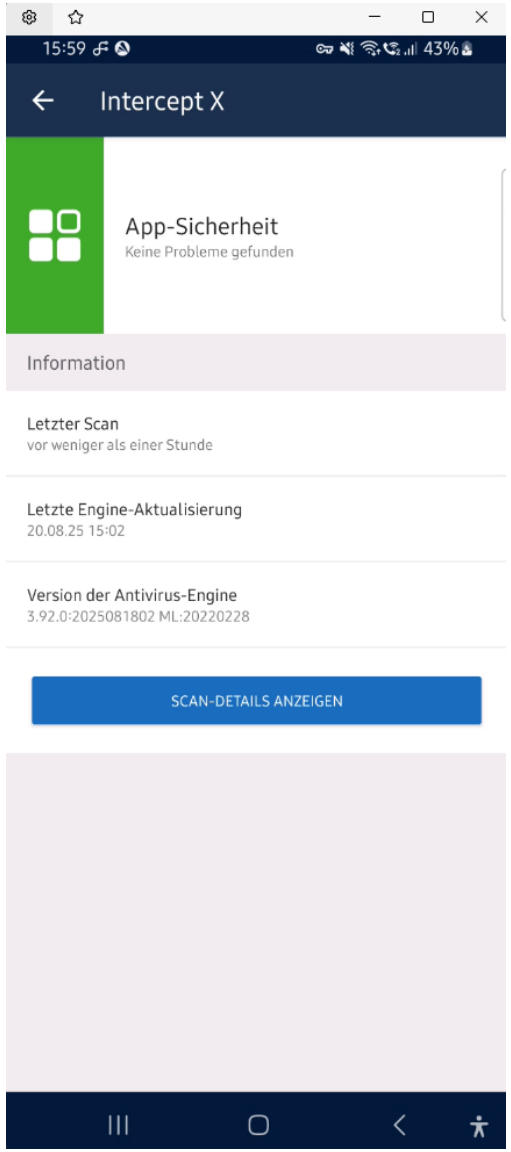




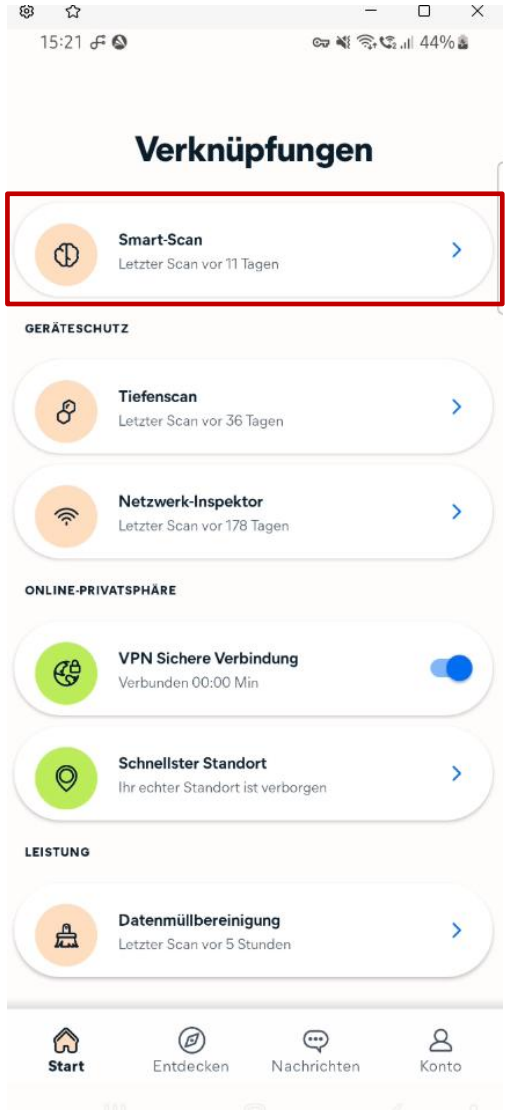
ANTIVIRUS SOFTWARE – BEISPIEL INTERCEPT X (KOSTENLOS VERSION)

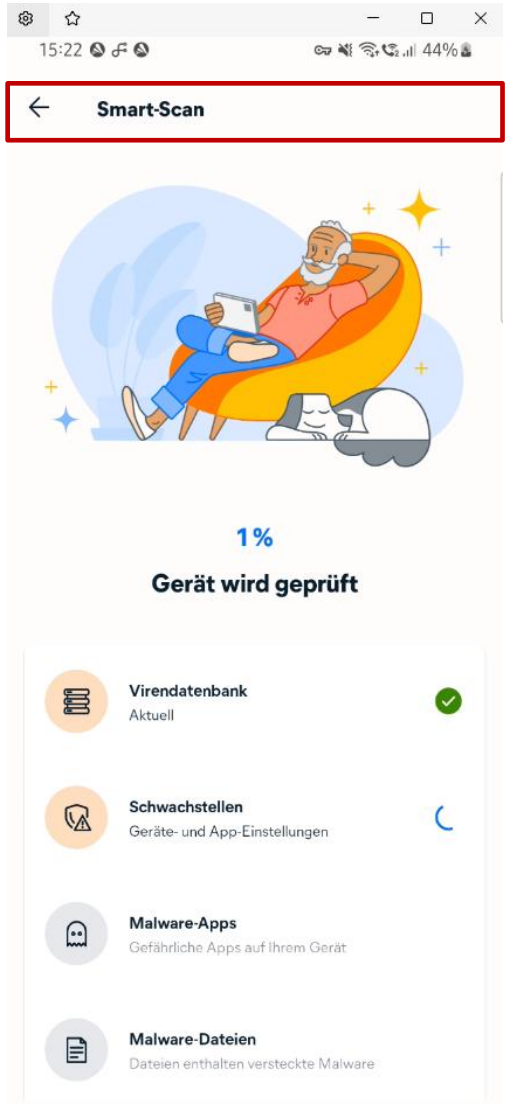


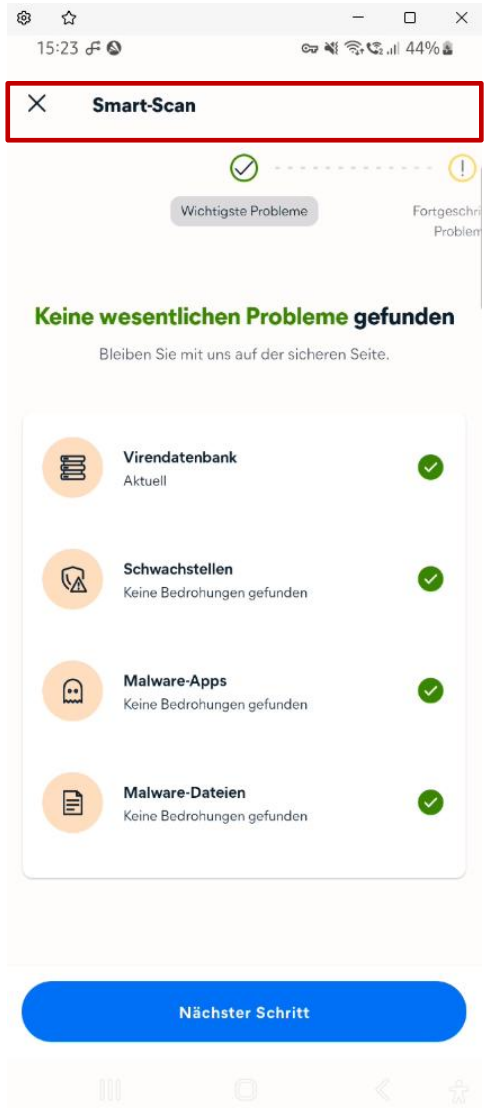




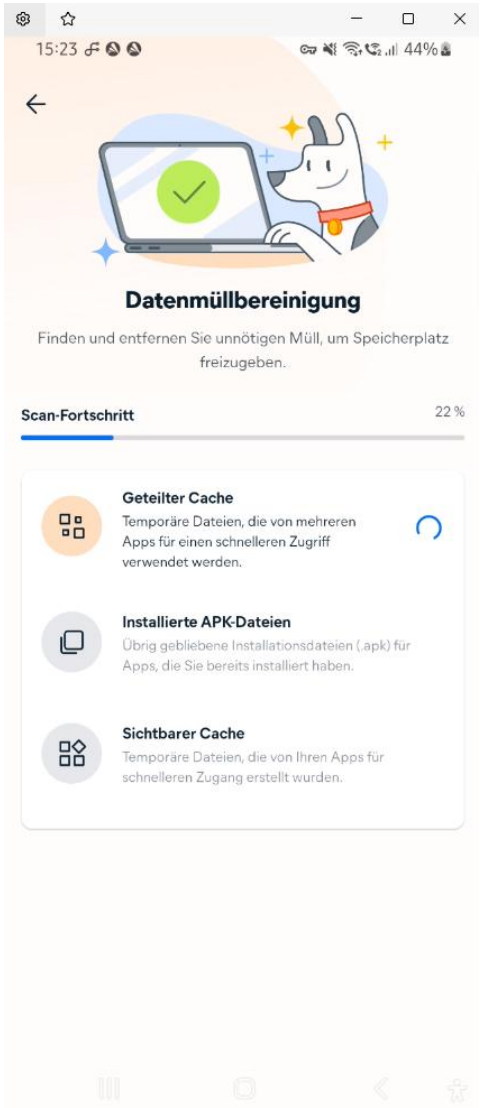
ANTIVIRUS SOFTWARE – BEISPIEL AVAST (KOSTENLOS VERSION)

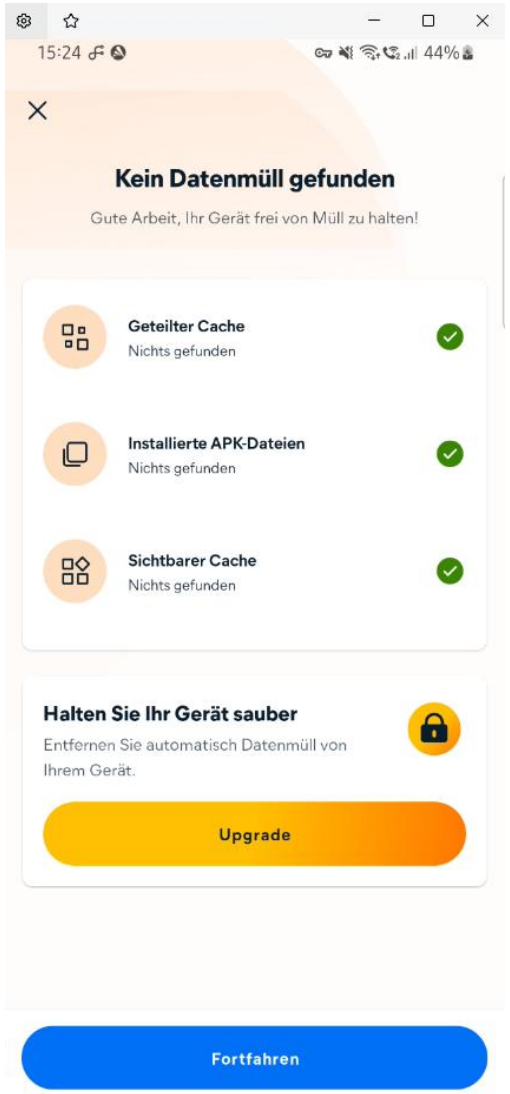




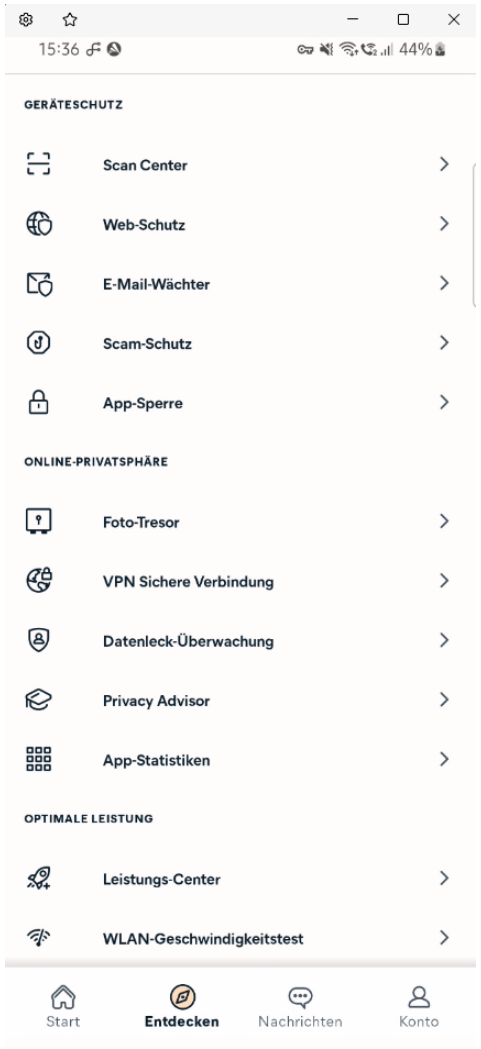


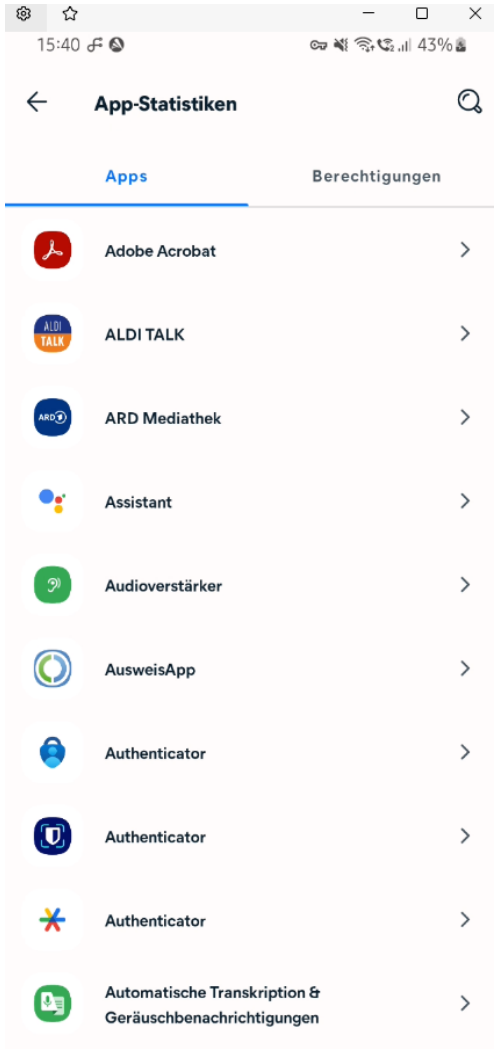
ANTIVIRUS SOFTWARE – BEISPIEL AVAST (KOSTENLOS VERSION)





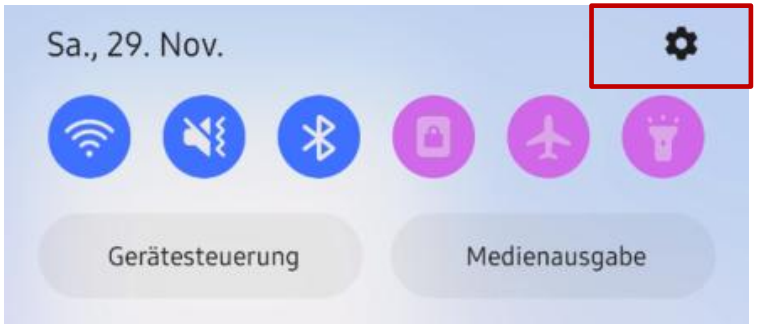
ANTIVIRUS SOFTWARE – BEISPIEL AVAST (KOSTENLOS VERSION)

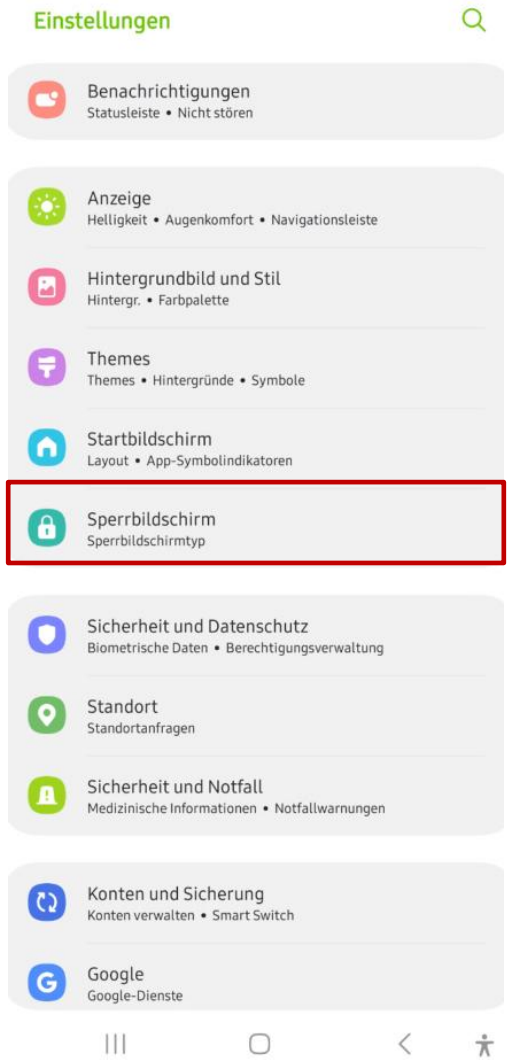


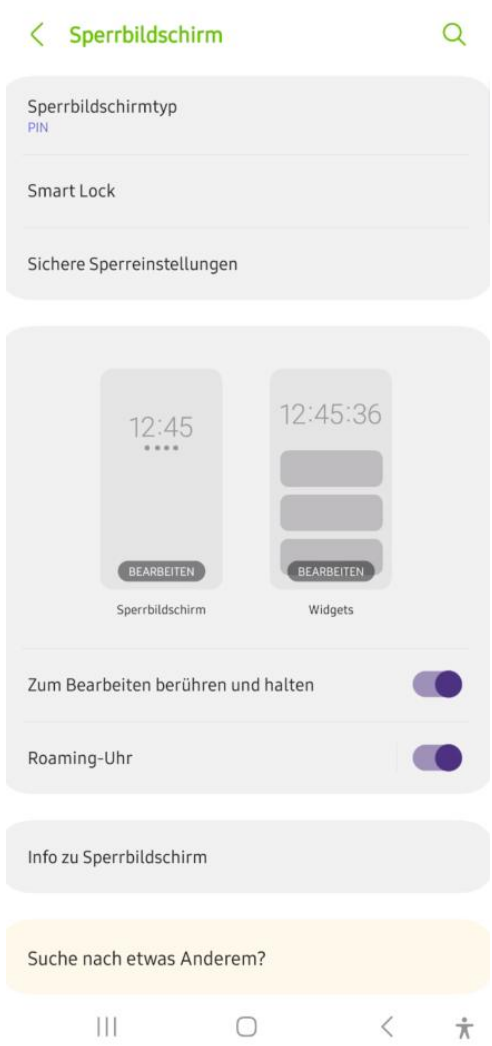


Hinweis: Nicht alle Funktionen der Kostenlos-Version sind ohne Upgrade zur Bezahlfunktion verfügbar. Aber die Basisfunktionen der Kostenlos-Funktionen geben einen Mindestschutz vor Viren.

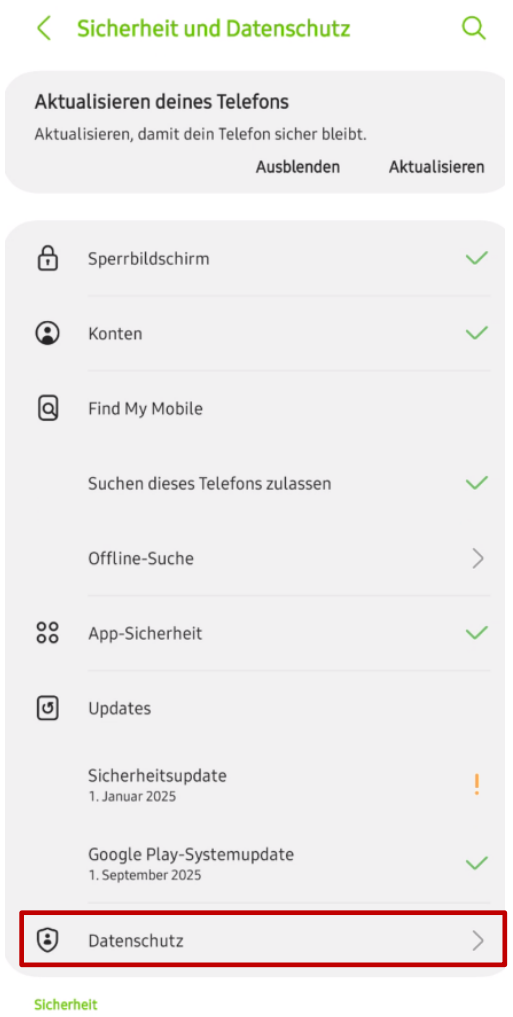
SPERR-BILDSCHIRM

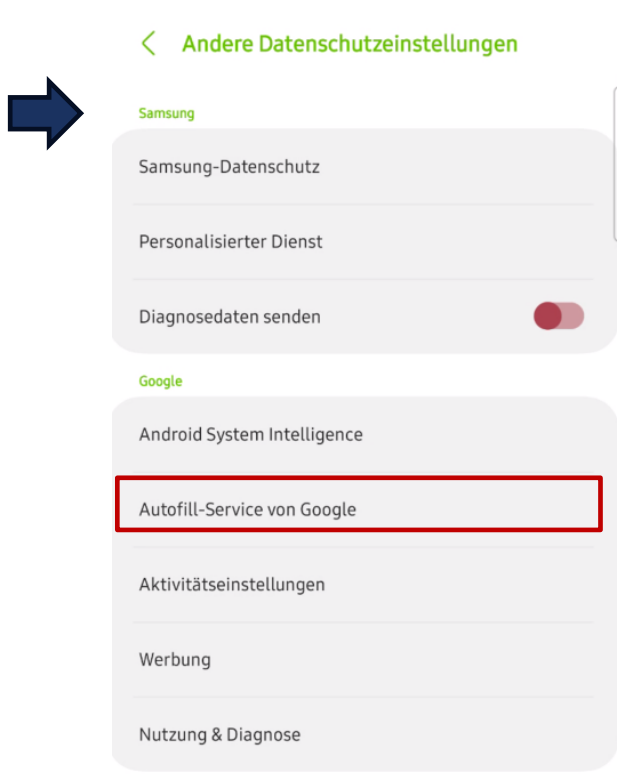


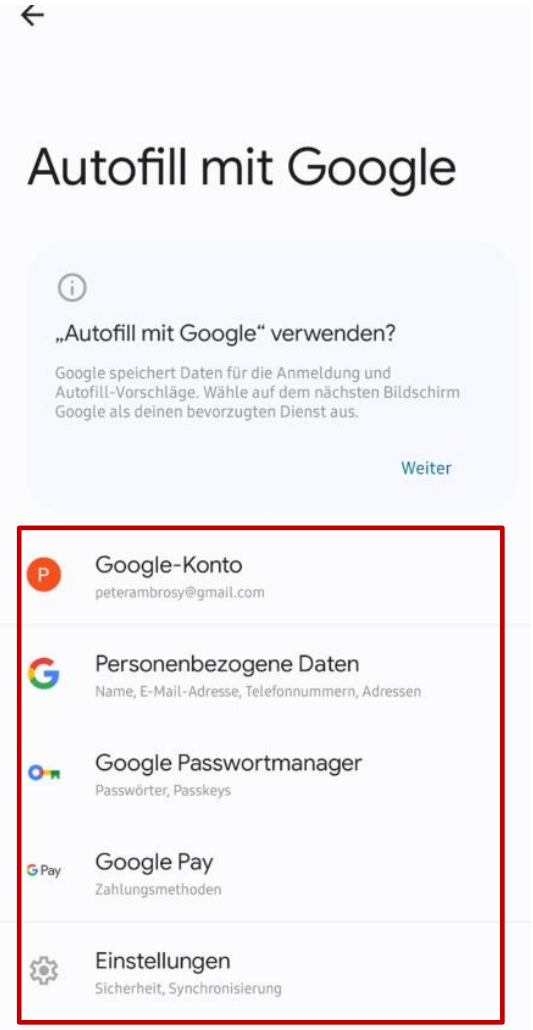




SICHERHEIT UND DATENSCHUTZ EINSTELUNGEN







WEITERE PERSÖNLICHE ORGANISATORISCHE MAßNAHMEN

- Datensparsamkeit
- Sichere Passwörter
- Back-Ups
- Programm-Updates
- 2-Faktor-Authentifizierung
- Datenträgerverschlüsselung

DATENSPARSAMKEIT

- **Leitprinzip der Datensparsamkeit**
  - Need-to-Know-Prinzip“ - nur so viele Informationen teilen wie für Bereitstellung/Nutzung eines Dienstes benötigt werden
  - nicht zwangsläufig Telefonnummer, Adresse oder Geburtsdatum herausgeben …
- **Zurückhaltung in sozialen Medien**
  - persönliche Details möglichst wenig teilen – macht es Angreifern schwerer, Identität vorzutäuschen
  - jede Information kann für gezielte Angriffe verwendet werden
    - – Informationen können zur Herleitung von Passwörtern, wirksamen Gestaltung von (Spear) Phishing Mails, … genutzt werden

PROGRAMM UPDATES

- **Programm-Updates schließen bekannt gewordene Schwachstellen und beseitigen Sicherheitsrisiken**
  - Verwendung älterer Software-Versionen = Sicherheitsrisiko
  - Gefahr des Missbrauchs öffentlich bekannter gewordener Schwachstellen
- **Updates installieren, sobald sie verfügbar sind**
  - Hersteller finden nicht alle Lücken während der Testphase
- **Viele Sicherheitslücken in Programmen werden oft erst im Gebrauch entdeckt**, z.B. durch Angriffe, Analysen externer Experten, …
  - Bekannt gewordene Sicherheitslücken können meist durch kleinere Updatepakete geschlossen werden

PROGRAMM UPDATES

- Heute geben Programme selbst automatisch Hinweise auf vorhandene Updates
- Es gibt Anwendungen, die automatisch nach Updates für die installierte Software suchen
- Auch gute Antivirusprogramme überprüfen Aktualität der installierten Software

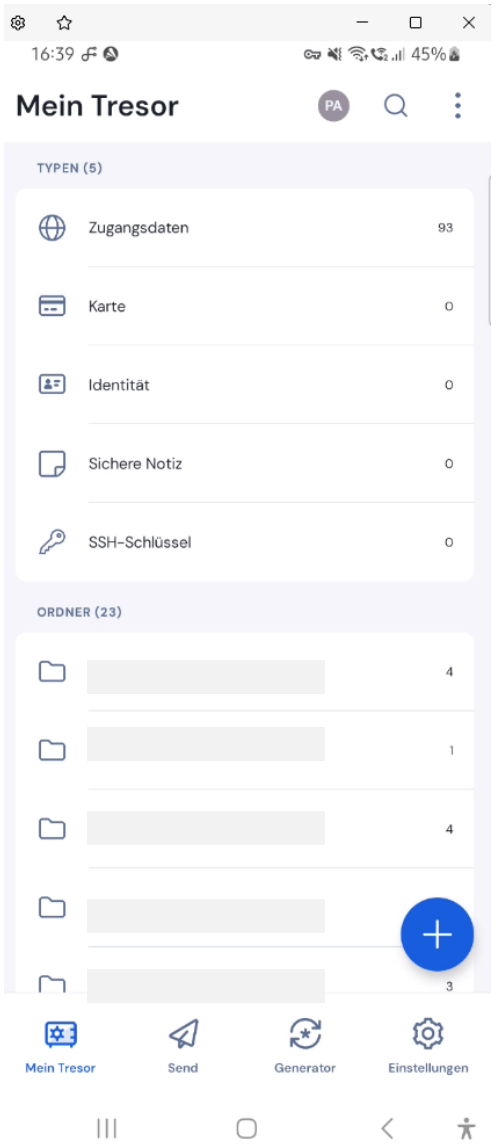
Doch bei allen Updates gilt:

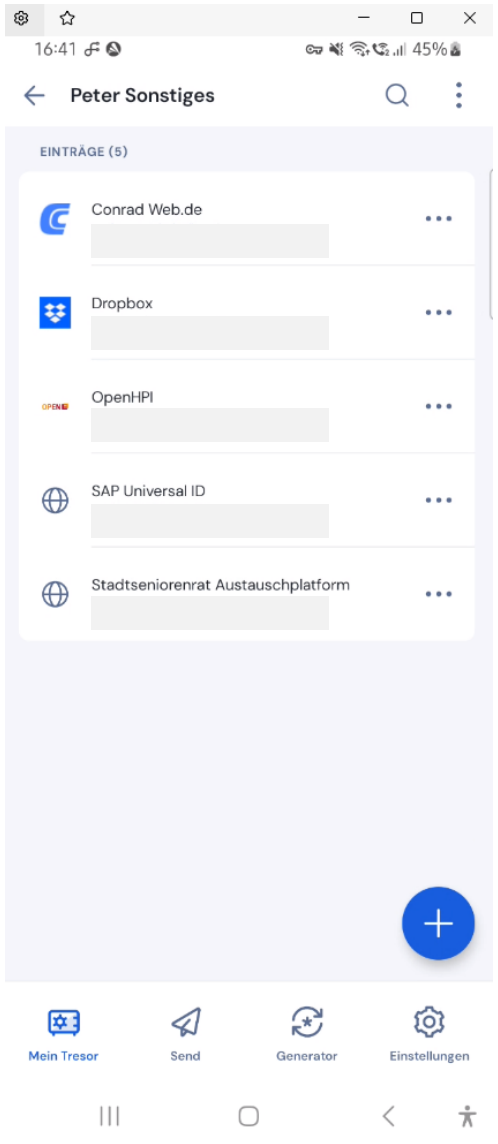
- Vertrauenswürdigkeit von Quelle und Updates müssen stets überprüft werden
- Ansonsten können Updates selbst zur Quelle neuer Angriffspunkte werden und zur Installation von Schadsoftware führen

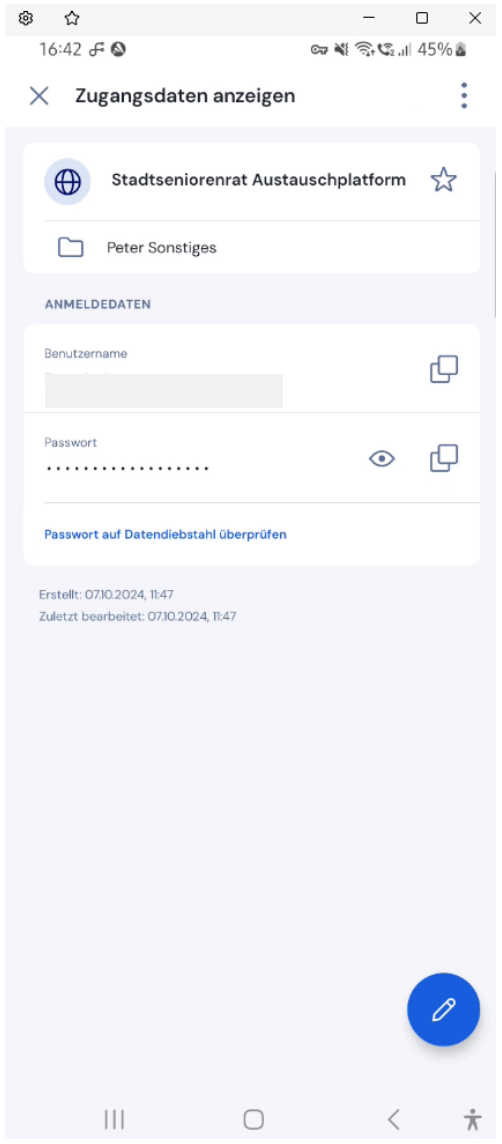
SICHERE PASSWÖRTER

- Passwörter sind gut, wenn sie schwer zu raten oder zu berechnen sind
  - **Groß- und Kleinschreibung** in Passwörtern mischen, auch Kombinationen mehrerer Wörter sind sinnvoll
  - Neben Buchstaben auch **Nummern und Sonderzeichen** ($%&:;-_?§!...) verwenden
  - Minimallänge: 12 Zeichen
  - Umso länger die Zeichenlänge, desto höher die Sicherheit:
  - mit jedem zusätzlichen Zeichen steigt Komplexität exponentiell
- Keine Passwörter aus Nutzerkontext oder Wörterbuch verwenden oder alte Passwörter, die schon einmal verwendet wurden
- **Nutzung Passwort-Manager** mit Passwortgenerierung

SICHERE PASSWÖRTER – PASSWORT-MANAGER BEISPIEL







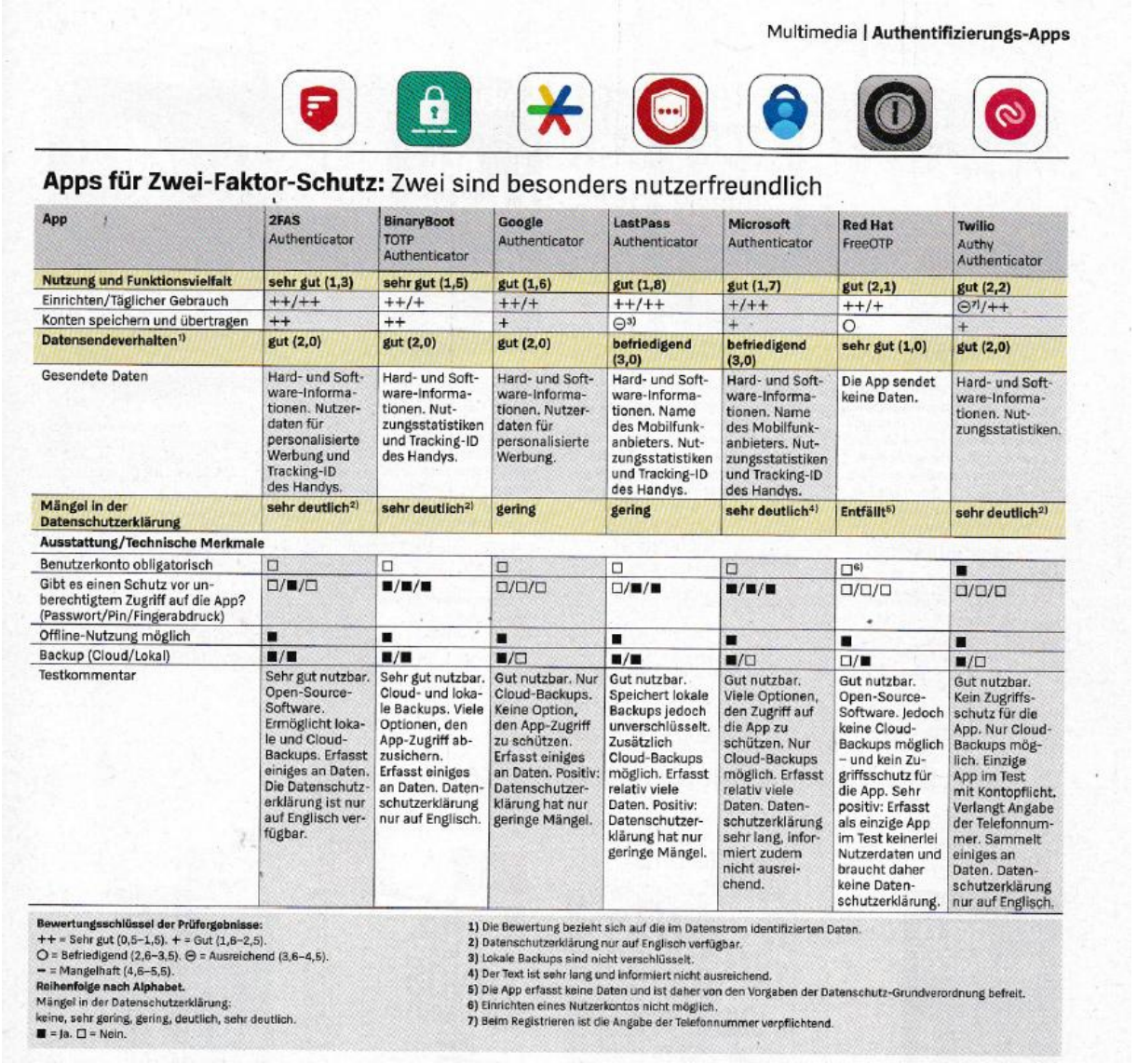
2-FAKTOR-AUTHENTIFIZIERUNG

- 3 Arten von Authentifizierungsmethoden
  - Authentifizierung durch **Wissen**, z.B. Passwort
  - Authentifizierung durch **Besitz**, z.B. TAN-Generator
  - Authentifizierung durch **Biometrie**, z.B. Fingerabdruck

- Immer mehr Internetdienste ermöglichen zusätzlich zur Passworteingabe die Verwendung weiterer Methoden (Faktoren)
  - **2-Faktor-Authentifizierung (Multifaktor-Authentifizierung):** Erst wenn Nutzer alle Authentifizierungsfaktoren erfüllt hat, gilt er als authentifiziert
- Authentifizierung ist aufwendiger, aber sicherer

2-FAKTOR AUTHENTIFIZIERUNGS-SOFTWARE

- Vielzahl von Anbietern
- Orientierung bietet Stiftung Warentest (Test 11/24)
- Quellen: Anbieter Webseiten, Microsoft Store, Google Playstore,….



Multimedia | **Authentifizierungs-Apps**

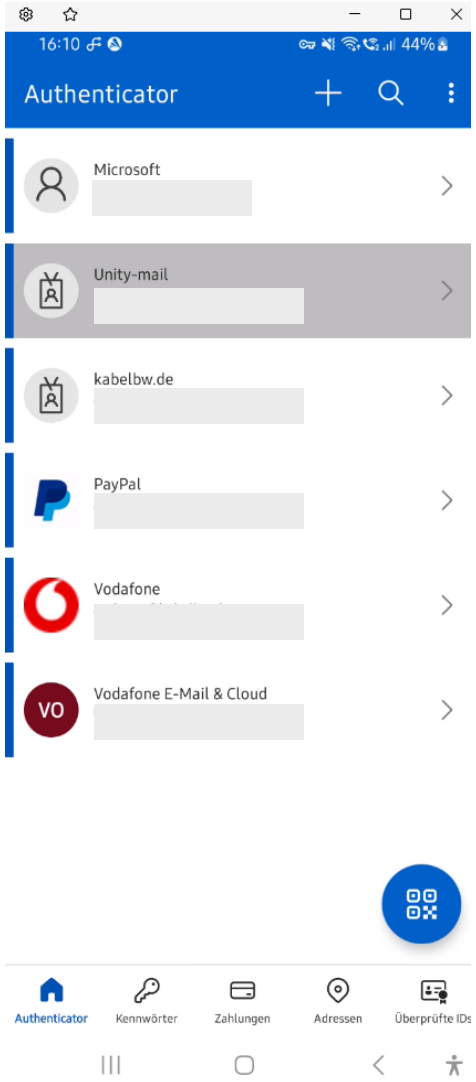
Apps für Zwei-Faktor-Schutz: Zwei sind besonders nutzerfreundlich

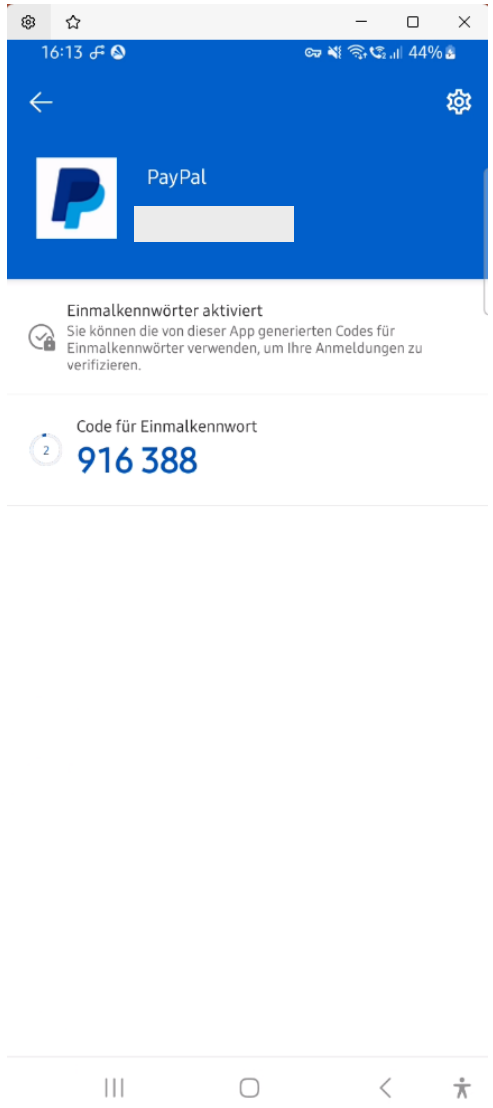
App	2FAS Authenticator	BinaryBoot TOTP Authenticator	Google Authenticator	LastPass Authenticator	Microsoft Authenticator	Red Hat FreeOTP	Twilio Authy Authenticator
Nutzung und Funktionsvielfalt	**sehr gut (1,3)**	**sehr gut (1,5)**	**gut (1,6)**	**gut (1,8)**	**gut (1,7)**	**gut (2,1)**	**gut (2,2)**
Einrichten/Täglicher Gebrauch	++/++	++/+	++/+	++/++	+/++	++/+	⊖[7]/++
Konten speichern und übertragen	++	++	+	⊖[3]	+	○	+
Datensendeverhalten[1]	**gut (2,0)**	**gut (2,0)**	**gut (2,0)**	**befriedigend (3,0)**	**befriedigend (3,0)**	**sehr gut (1,0)**	**gut (2,0)**
Gesendete Daten	Hard- und Software-Informationen. Nutzerdaten für personalisierte Werbung und Tracking-ID des Handys.	Hard- und Software-Informationen. Nutzungsstatistiken und Tracking-ID des Handys.	Hard- und Software-Informationen. Nutzerdaten für personalisierte Werbung.	Hard- und Software-Informationen. Name des Mobilfunkanbieters. Nutzungsstatistiken und Tracking-ID des Handys.	Hard- und Software-Informationen. Name des Mobilfunkanbieters. Nutzungsstatistiken und Tracking-ID des Handys.	Die App sendet keine Daten.	Hard- und Software-Informationen. Nutzungsstatistiken.
Mängel in der Datenschutzerklärung	**sehr deutlich[2]**	**sehr deutlich[2]**	**gering**	**gering**	**sehr deutlich[4]**	**Entfällt[5]**	**sehr deutlich[2]**
Ausstattung/Technische Merkmale							
Benutzerkonto obligatorisch	□	□	□	□	□	□[6]	■
Gibt es einen Schutz vor unberechtigtem Zugriff auf die App? (Passwort/Pin/Fingerabdruck)	□/■/□	■/■/■	□/□/□	□/■/■	■/■/■	□/□/□	□/□/□
Offline-Nutzung möglich	■	■	■	■	■	■	■
Backup (Cloud/Lokal)	■/■	■/■	■/□	■/■	■/□	□/■	■/□
Testkommentar	Sehr gut nutzbar. Open-Source-Software. Ermöglicht lokale und Cloud-Backups. Erfasst einiges an Daten. Die Datenschutzerklärung ist nur auf Englisch verfügbar.	Sehr gut nutzbar. Cloud- und lokale Backups. Viele Optionen, den App-Zugriff abzusichern. Erfasst einiges an Daten. Datenschutzerklärung nur auf Englisch.	Gut nutzbar. Nur Cloud-Backups. Keine Option, den App-Zugriff zu schützen. Erfasst einiges an Daten. Positiv: Datenschutzerklärung hat nur geringe Mängel.	Gut nutzbar. Speichert lokale Backups jedoch unverschlüsselt. Zusätzlich Cloud-Backups möglich. Erfasst relativ viele Daten. Positiv: Datenschutzerklärung hat nur geringe Mängel.	Gut nutzbar. Viele Optionen, den Zugriff auf die App zu schützen. Nur Cloud-Backups möglich. Erfasst relativ viele Daten. Datenschutzerklärung sehr lang, informiert zudem nicht ausreichend.	Gut nutzbar. Open-Source-Software. Jedoch keine Cloud-Backups möglich – und kein Zugriffsschutz für die App. Sehr positiv: Erfasst als einzige App im Test keinerlei Nutzerdaten und braucht daher keine Datenschutzerklärung.	Gut nutzbar. Kein Zugriffsschutz für die App. Nur Cloud-Backups möglich. Einzige App im Test mit Kontopflicht. Verlangt Angabe der Telefonnummer. Sammelt einiges an Daten. Datenschutzerklärung nur auf Englisch.

Bewertungsschlüssel der Prüfergebnisse:
++ = Sehr gut (0,5–1,5). + = Gut (1,6–2,5).
○ = Befriedigend (2,6–3,5). ⊖ = Ausreichend (3,6–4,5).
− = Mangelhaft (4,6–5,5).
Reihenfolge nach Alphabet.
Mängel in der Datenschutzerklärung:
keine, sehr gering, gering, deutlich, sehr deutlich.
■ = Ja. □ = Nein.

1) Die Bewertung bezieht sich auf die im Datenstrom identifizierten Daten.
2) Datenschutzerklärung nur auf Englisch verfügbar.
3) Lokale Backups sind nicht verschlüsselt.
4) Der Text ist sehr lang und informiert nicht ausreichend.
5) Die App erfasst keine Daten und ist daher von den Vorgaben der Datenschutz-Grundverordnung befreit.
6) Einrichten eines Nutzerkontos nicht möglich.
7) Beim Registrieren ist die Angabe der Telefonnummer verpflichtend.

2-FAKTOR-AUTHENTIFIZIERUNG BEISPIELE (MICROSOFT)





BACKUPS

Ergebnis vieler Angriffe im Internet ist der Verlust bzw. Beschädigung von Daten

- Bei Datenverlust durch Viren, Ransomware oder Beschädigung des Betriebssystems können Daten mithilfe von vorher angelegten **Sicherungskopien** – Backups – wiederhergestellt werden
- **Wichtige und persönliche Daten müssen regelmäßig gesichert werden**
- Systeme bieten automatische Datensicherung in vordefinierten Zeitabständen an
- (Verschlüsseltes) Backup auf externen Medien oder in abgetrennten Clouds speichern

DATENTRÄGERSCHLÜSSELUNG

- **Datenträgerverschlüsselung macht Daten für Unbefugte unlesbar**
- Laptop
  - Festplattenverschlüsselung z.B. mit Microsoft BitLocker,
  - Apple FileVault (Bestandteile des Betriebssystems) etc. möglich
- USB-Sticks / Externe Festplatten
  - Verwendung verschlüsselter Datencontainer, z.B. VeraCrypt oder BitLocker
- Smartphone
  - Verschlüsselung meist schon integriert, geschützt mittels Zugangspin/-passwort, Sperrbildschirm

SICHERHEIT IM INTERNET

- Angriffsziel Internet
- Schutzmaßnahmen
- **Stiftung Warentest**

ANTIVIRUS SOFTWARE

- Vielzahl von Anbietern
- Orientierung bietet Stiftung Warentest (Test 3/25)
- Quellen: Anbieter Webseiten, Microsoft Store, Google Playstore,….

ANTIVIRUS SOFTWARE **FÜR ANDROID**: STIFTUNG WARENTEST 3/2025

Antivirenprogramme für Windows: Fünf kostenlose sind sehr gut

Produkt	Avira Internet Security	Bitdefender Antivirus Free for Windows	Bitdefender Internet Security	Avast One Silver	Avira Free Security	ESET Home Security Essential	G Data Internet Security
Preis pro Jahr für eine Einzelplatz-Lizenz ca. (Euro)[1]	27[4]	Kostenlos	30[4]	36[5]	Kostenlos	40	40
Preis pro Jahr für eine Einzelplatz-Lizenz im zweiten Jahr ca. (Euro)[1]	55	Kostenlos	50	70[6]	Kostenlos	40	40
QUALITÄTSURTEIL 100 %	**SEHR GUT (1,3)**	**SEHR GUT (1,3)**	**SEHR GUT (1,3)**	**SEHR GUT (1,4)**	**SEHR GUT (1,4)**	**SEHR GUT (1,4)**	**SEHR GUT (1,4)**
Schutzwirkung 65 %	sehr gut (1,1)	sehr gut (1,2)	sehr gut (1,2)	sehr gut (1,3)	sehr gut (1,1)	sehr gut (1,3)	sehr gut (1,3)
Schutz vor Schadsoftware	++	++	++	++	++	++	++
Phishing-Schutz[2]	++	++	++	++	++	+	++
Handhabung 25 %	gut (1,7)	sehr gut (1,4)	sehr gut (1,4)	gut (1,6)	gut (2,0)	sehr gut (1,4)	sehr gut (1,4)
Täglicher Gebrauch	+	+	+	+	+	+	++
Installieren und Deinstallieren	+	+	+	++	+	++	+
Unaufdringlichkeit der Werbung	++	++	++	++	+	++	++
Rechnerbelastung 10 %	sehr gut (1,3)	gut (1,9)	gut (2,0)	sehr gut (1,4)	sehr gut (1,2)	sehr gut (1,4)	sehr gut (1,5)
Mängel in der Datenschutzerklärung 0 %	gering	gering	gering	sehr gering	gering	sehr gering	keine
Ausstattung/Technische Merkmale							
Rettungsmedium[3]	□	□	■	□	□	□	■
Phishing-Schutz für Chrome/Firefox/Edge	■/■/■	■/■/■	■/■/■	■/■/■	■/□/■	■/■/■	■/■/■
VPN/Passwortmanager integriert	■/■	■/□	■/■	■/□	■/■	□/□	□/□

Bewertungsschlüssel der Prüfergebnisse:
++ = Sehr gut (0,5–1,5). + = Gut (1,6–2,5).
○ = Befriedigend (2,6–3,5). ⊖ = Ausreichend (3,6–4,5).
− = Mangelhaft (4,6–5,5).

Bei gleichem Qualitätsurteil Reihenfolge nach Alphabet.
***) Führt zur Abwertung** (siehe „So haben wir getestet" auf S. 36).
Mängel in der Datenschutzerklärung:
keine, sehr gering, gering, deutlich, sehr deutlich.
■ = Ja. □ = Nein.

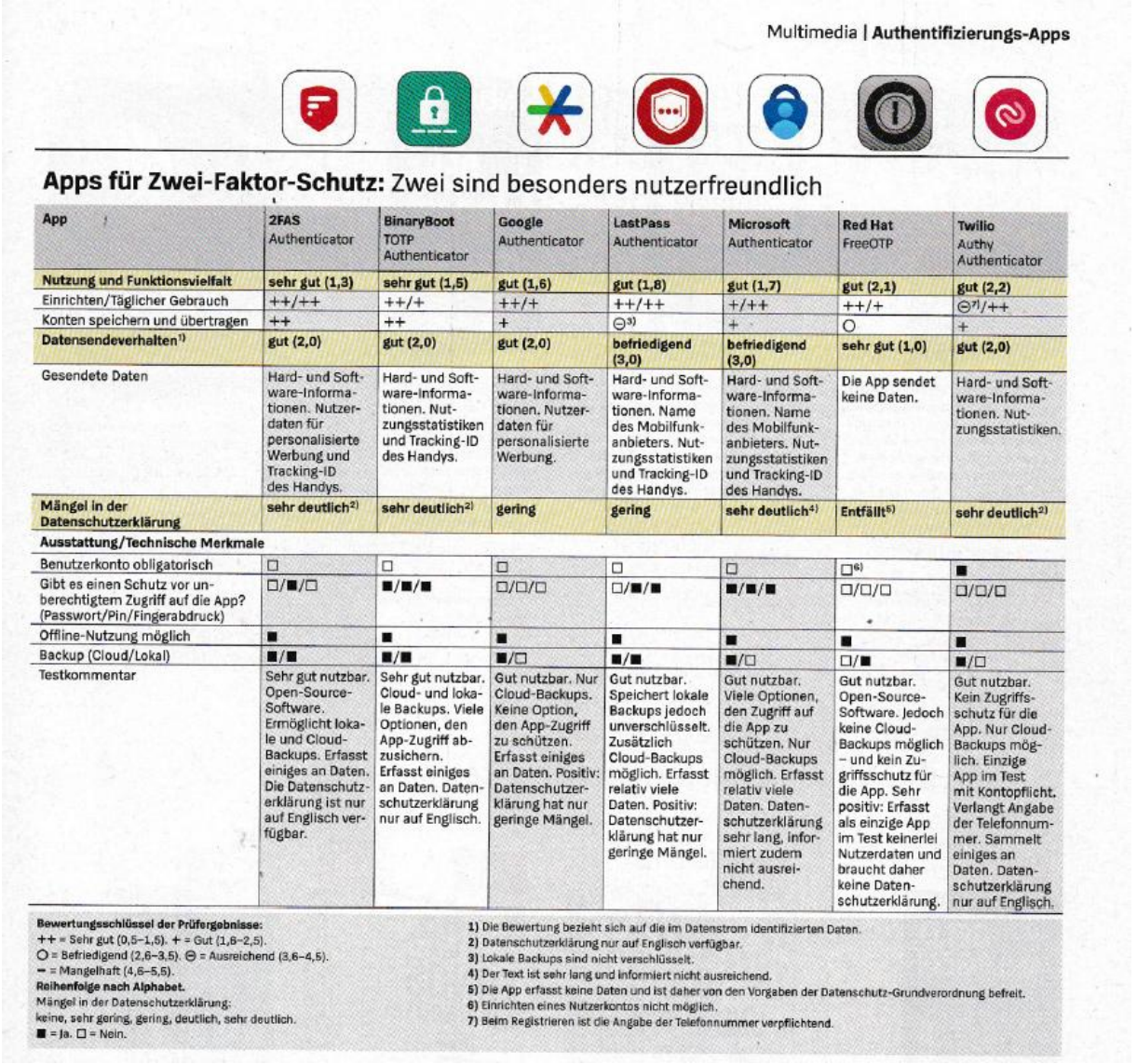
1) Laut Anbieter-Webseite.
2) Getestet mit dem Browser Google Chrome bei deaktivierter „Safe-Browsing"-Funktion. Standardmäßig ist „Safe-Browsir aktiviert – die Funktion schützt dann gegen Phishing. Auch v Browser bieten Phishing-Schutz.

Avast One Basic	AVG AntiVirus Free	AVG Internet Security	McAfee Total Protection	Norton 360 Standard[7]	F-Secure Internet Security	Trend Micro Internet Security	Sophos Home Premium	Microsoft Windows Defender
Kostenlos	**Kostenlos**	**44[4]**	**30[4]**	**35[4]**	**50**	**20[4]**	**37[8]**	**Kostenlos**
Kostenlos	Kostenlos	73	87	75	50	50	50[9]	Kostenlos
SEHR GUT (1,5)	**SEHR GUT (1,5)**	**SEHR GUT (1,5)**	**SEHR GUT (1,5)**	**SEHR GUT (1,5)**	**GUT (1,6)**	**GUT (2,0)**	**BEFRIEDIGEND (2,6)**	**BEFRIEDIGEND (3,2)**
sehr gut (1,3)	sehr gut (1,2)	sehr gut (1,2)	sehr gut (1,5)	sehr gut (1,5)	gut (1,6)	gut (2,1)	gut (2,0)	befriedigend (3,5)
++	++	++	+	+	+	+	+	○
++	++	++	++	++	+	++	○	−[11]
gut (2,1)	gut (2,3)	gut (2,2)	gut (1,6)	gut (1,6)	gut (1,8)	gut (1,7)	gut (1,8)	gut (1,9)
+	+	+	+	++	+	+	+	○
+	+	+	+	+	+	+	+	++
○	⊖	⊖	++	+	++	++	++	++
sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,4)	sehr gut (0,9)	sehr gut (1,5)	sehr gut (1,5)	gut (1,9)	gut (2,1)	sehr gut (1,2)
sehr gering	sehr gering	sehr gering	gering	sehr gering	gering	gering	sehr deutlich*)[10]	deutlich*)
□	□	□	□	■	□	□	□	■
■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	□/□/■
■/□	□/□	□/□	■/■	■/■	□/□	□/□	□/□	□/■

3) Das Programm bietet dem Nutzer an, direkt aus der Programmoberfläche heraus einen USB-Stick mit Rettungssoftware zu erstellen, mit dem ein infiziertes System nach einem Angriff repariert werden kann.
4) Sonderpreis im ersten Jahr.
5) Sonderpreis im ersten Jahr. Gilt für 3 Geräte.
6) Gilt für 3 Geräte.
7) Norton hat das Produkt im Jahr 2024 grundlegend überarbeitet. Die Noten beziehen sich nur auf die neue Version.
8) Sonderpreis im ersten Jahr. Gilt für 10 Geräte.
9) Gilt für 10 Geräte.
10) Keine deutschsprachige Datenschutzerklärung vorhanden.
11) Microsoft Defender schützt bei Verwendung des Browsers Google Chrome nicht vor Phishing.

2-FAKTOR AUTHENTIFIZIERUNGS-SOFTWARE

- Vielzahl von Anbietern
- Orientierung bietet Stiftung Warentest (Test 11/24)
- Quellen: Anbieter Webseiten, Microsoft Store, Google Playstore,….

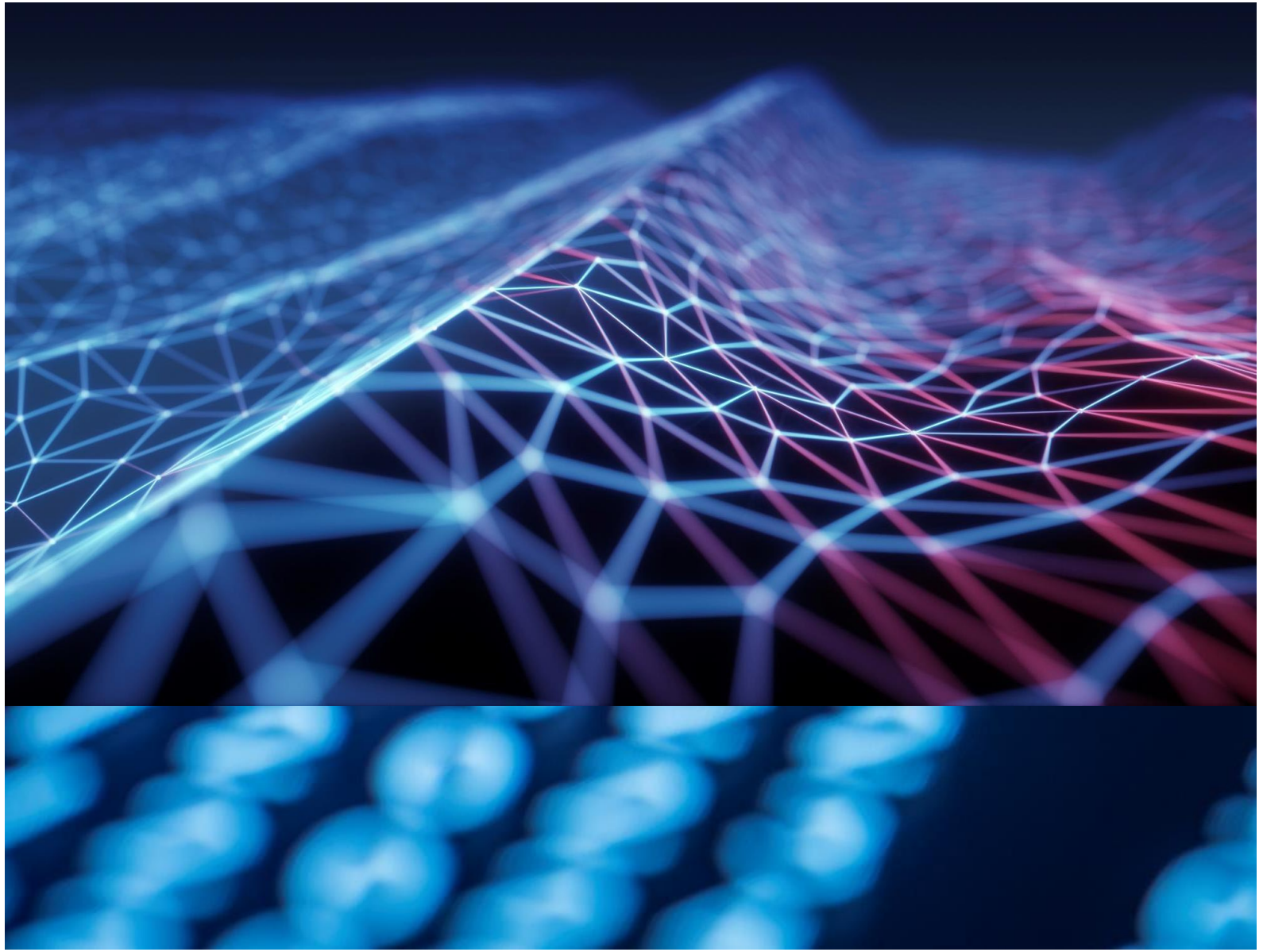


Apps für Zwei-Faktor-Schutz: Zwei sind besonders nutzerfreundlich

App	2FAS Authenticator	BinaryBoot TOTP Authenticator	Google Authenticator	LastPass Authenticator	Microsoft Authenticator	Red Hat FreeOTP	Twilio Authy Authenticator
Nutzung und Funktionsvielfalt	**sehr gut (1,3)**	**sehr gut (1,5)**	**gut (1,6)**	**gut (1,8)**	**gut (1,7)**	**gut (2,1)**	**gut (2,2)**
Einrichten/Täglicher Gebrauch	++/++	++/+	++/+	++/++	+/++	++/+	⊖[7]/++
Konten speichern und übertragen	++	++	+	⊖[3]	+	○	+
Datensendeverhalten[1]	**gut (2,0)**	**gut (2,0)**	**gut (2,0)**	**befriedigend (3,0)**	**befriedigend (3,0)**	**sehr gut (1,0)**	**gut (2,0)**
Gesendete Daten	Hard- und Software-Informationen. Nutzerdaten für personalisierte Werbung und Tracking-ID des Handys.	Hard- und Software-Informationen. Nutzungsstatistiken und Tracking-ID des Handys.	Hard- und Software-Informationen. Nutzerdaten für personalisierte Werbung.	Hard- und Software-Informationen. Name des Mobilfunkanbieters. Nutzungsstatistiken und Tracking-ID des Handys.	Hard- und Software-Informationen. Name des Mobilfunkanbieters. Nutzungsstatistiken und Tracking-ID des Handys.	Die App sendet keine Daten.	Hard- und Software-Informationen. Nutzungsstatistiken.
Mängel in der Datenschutzerklärung	**sehr deutlich[2]**	**sehr deutlich[2]**	**gering**	**gering**	**sehr deutlich[4]**	**Entfällt[5]**	**sehr deutlich[2]**
Ausstattung/Technische Merkmale							
Benutzerkonto obligatorisch	□	□	□	□	□	□[6]	■
Gibt es einen Schutz vor unberechtigtem Zugriff auf die App? (Passwort/Pin/Fingerabdruck)	□/■/□	■/■/■	□/□/□	□/■/■	■/■/■	□/□/□	□/□/□
Offline-Nutzung möglich	■	■	■	■	■	■	■
Backup (Cloud/Lokal)	■/■	■/■	■/□	■/■	■/□	□/■	■/□
Testkommentar	Sehr gut nutzbar. Open-Source-Software. Ermöglicht lokale und Cloud-Backups. Erfasst einiges an Daten. Die Datenschutzerklärung ist nur auf Englisch verfügbar.	Sehr gut nutzbar. Cloud- und lokale Backups. Viele Optionen, den App-Zugriff abzusichern. Erfasst einiges an Daten. Datenschutzerklärung nur auf Englisch.	Gut nutzbar. Nur Cloud-Backups. Keine Option, den App-Zugriff zu schützen. Erfasst einiges an Daten. Positiv: Datenschutzerklärung hat nur geringe Mängel.	Gut nutzbar. Speichert lokale Backups jedoch unverschlüsselt. Zusätzlich Cloud-Backups möglich. Erfasst relativ viele Daten. Positiv: Datenschutzerklärung hat nur geringe Mängel.	Gut nutzbar. Viele Optionen, den Zugriff auf die App zu schützen. Nur Cloud-Backups möglich. Erfasst relativ viele Daten. Datenschutzerklärung sehr lang, informiert zudem nicht ausreichend.	Gut nutzbar. Open-Source-Software. Jedoch keine Cloud-Backups möglich – und kein Zugriffsschutz für die App. Sehr positiv: Erfasst als einzige App im Test keinerlei Nutzerdaten und braucht daher keine Datenschutzerklärung.	Gut nutzbar. Kein Zugriffsschutz für die App. Nur Cloud-Backups möglich. Einzige App im Test mit Kontopflicht. Verlangt Angabe der Telefonnummer. Sammelt einiges an Daten. Datenschutzerklärung nur auf Englisch.

Bewertungsschlüssel der Prüfergebnisse:
++ = Sehr gut (0,5–1,5). + = Gut (1,6–2,5).
○ = Befriedigend (2,6–3,5). ⊖ = Ausreichend (3,6–4,5).
– = Mangelhaft (4,6–5,5).
Reihenfolge nach Alphabet.
Mängel in der Datenschutzerklärung:
keine, sehr gering, gering, deutlich, sehr deutlich.
■ = Ja. □ = Nein.

1) Die Bewertung bezieht sich auf die im Datenstrom identifizierten Daten.
2) Datenschutzerklärung nur auf Englisch verfügbar.
3) Lokale Backups sind nicht verschlüsselt.
4) Der Text ist sehr lang und informiert nicht ausreichend.
5) Die App erfasst keine Daten und ist daher von den Vorgaben der Datenschutz-Grundverordnung befreit.
6) Einrichten eines Nutzerkontos nicht möglich.
7) Beim Registrieren ist die Angabe der Telefonnummer verpflichtend.



VIELEN DANK