SICHERHEIT IM INTERNET

VORTRAG SMARTPHONE-TRAINING

ZIEL DES HEUTIGEN TRAINING

Beantwortung von 3 Kernfragen:

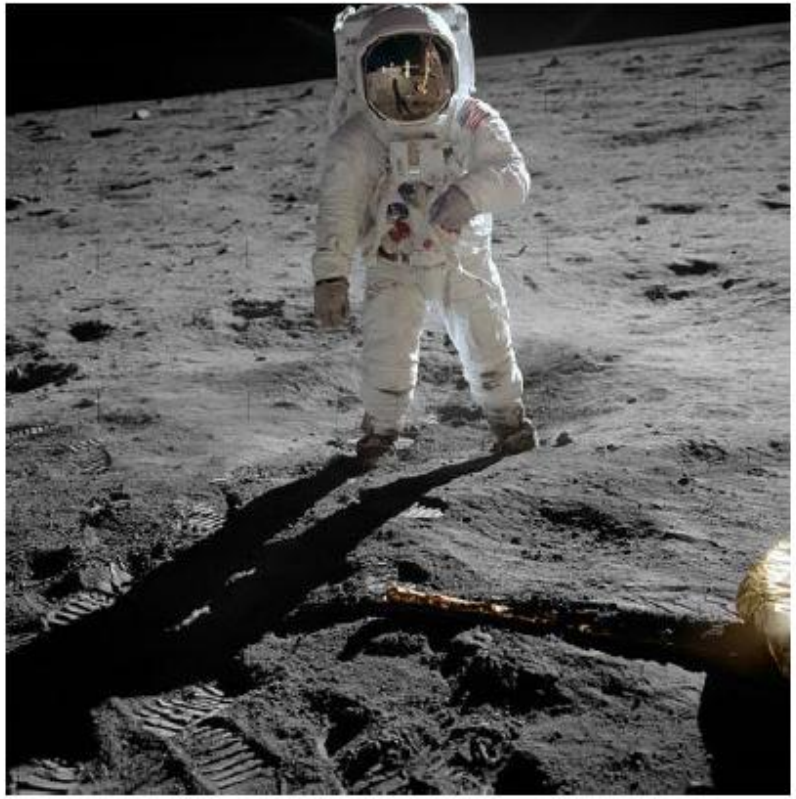
- **Warum** ist die Internetnutzung überhaupt sicherheitsrelevant?
- **Was** sind die wichtigsten Schutzmaßnahmen?
- **Wie** kann ich mich schützen?

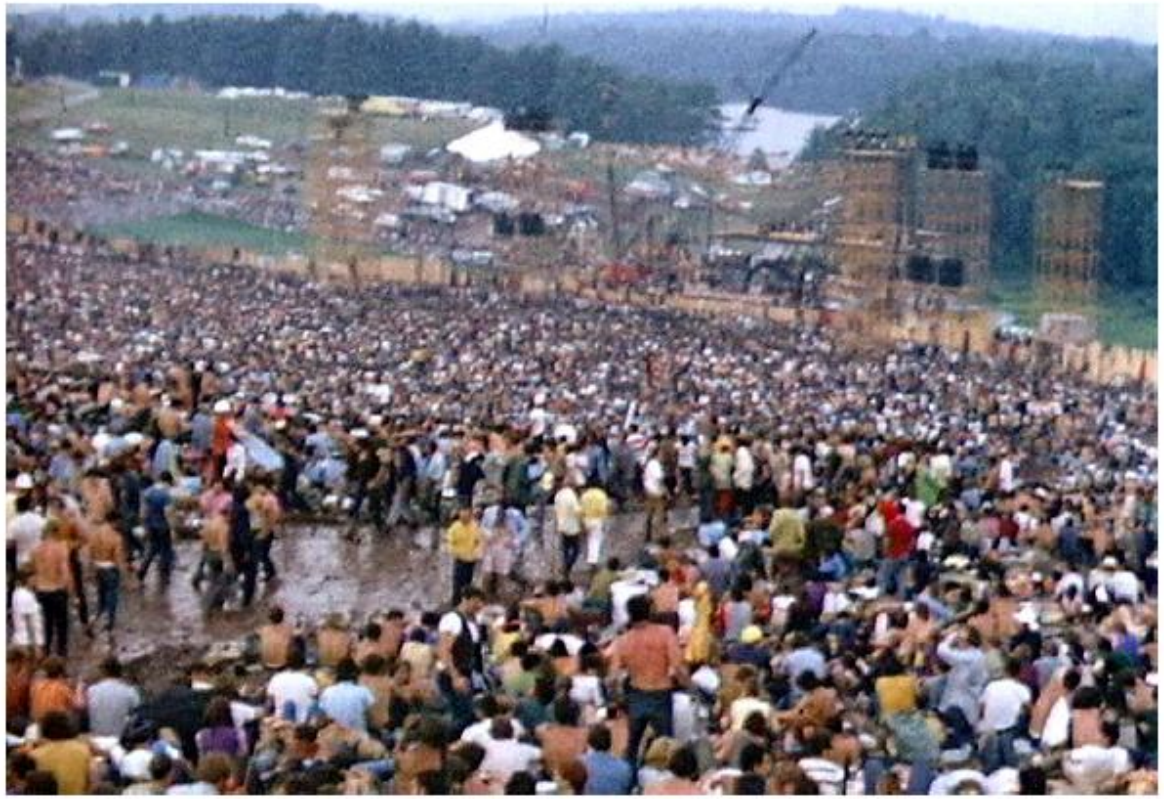
SICHERHEIT IM INTERNET

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

INTERNET: GEBURTSSTUNDE DES INTERNET – DAS JAHR 1969

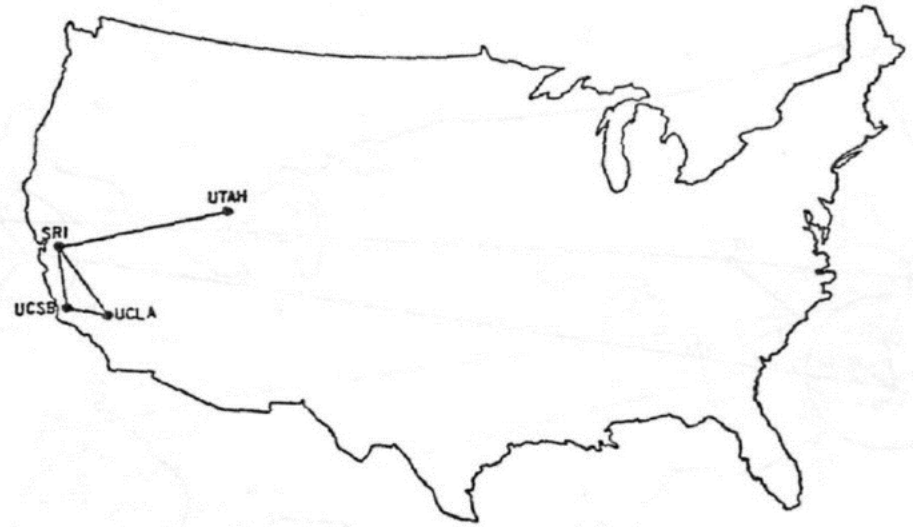
- **1969: Woran erinnern Sie sich?**





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



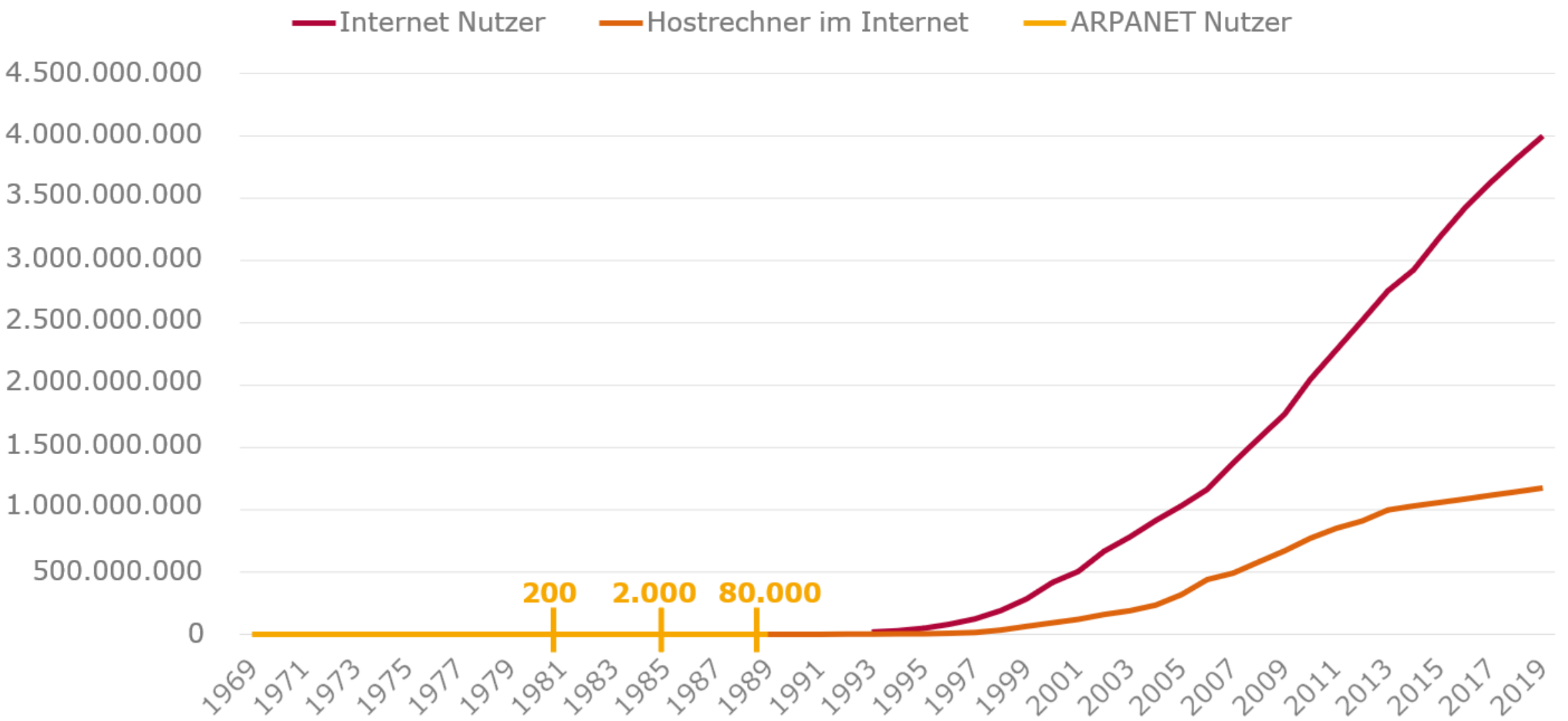
The ARPANET in December 1969

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

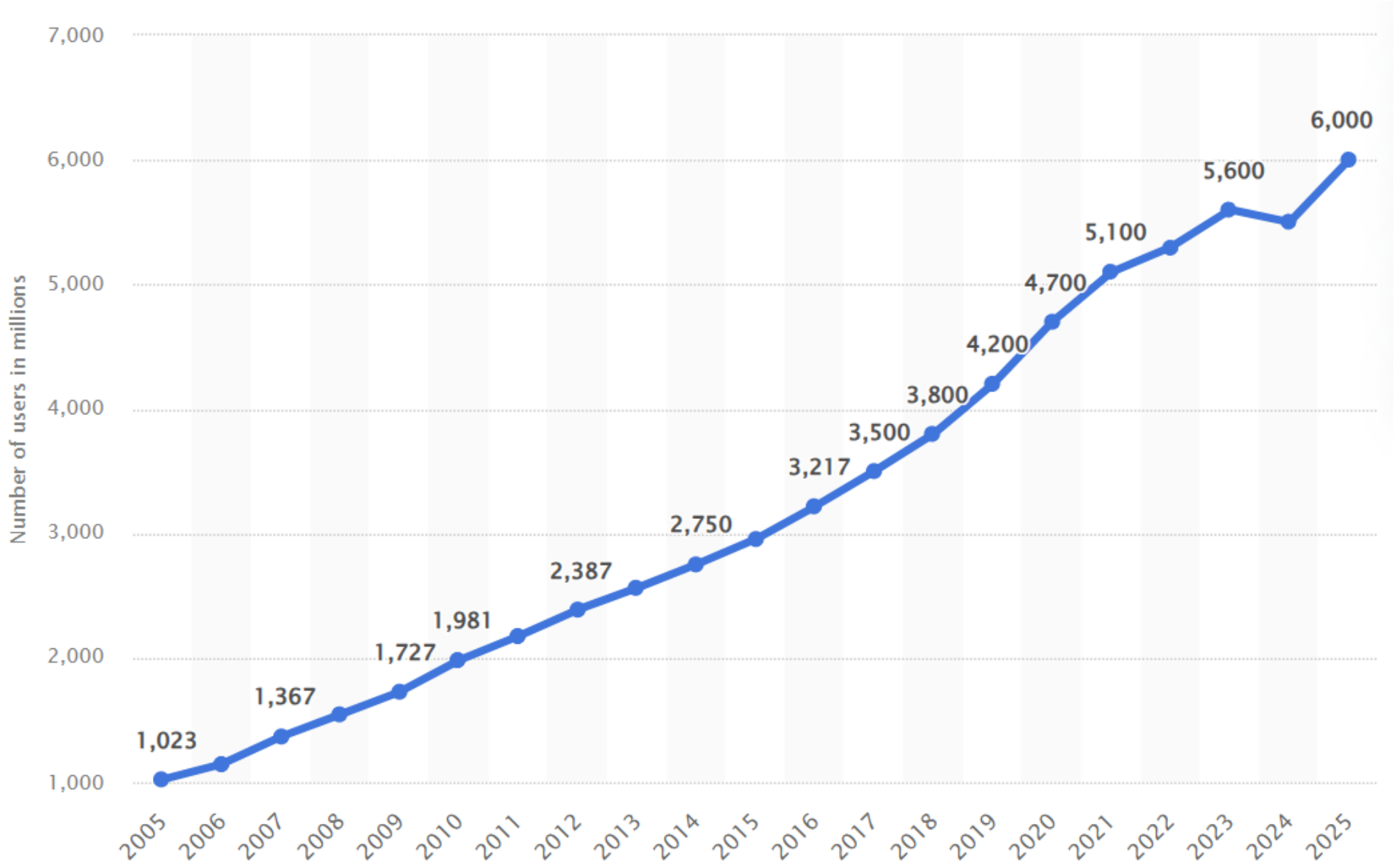
Das **ARPANET** (englisch: Advanced Research Projects Agency Network) war ein Computernetzwerk und wurde ursprünglich im Auftrag der US Air Force ab 1968 von einer **kleinen Forschergruppe** unter der Leitung des **MIT und des US-Verteidigungsministeriums** entwickelt.

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

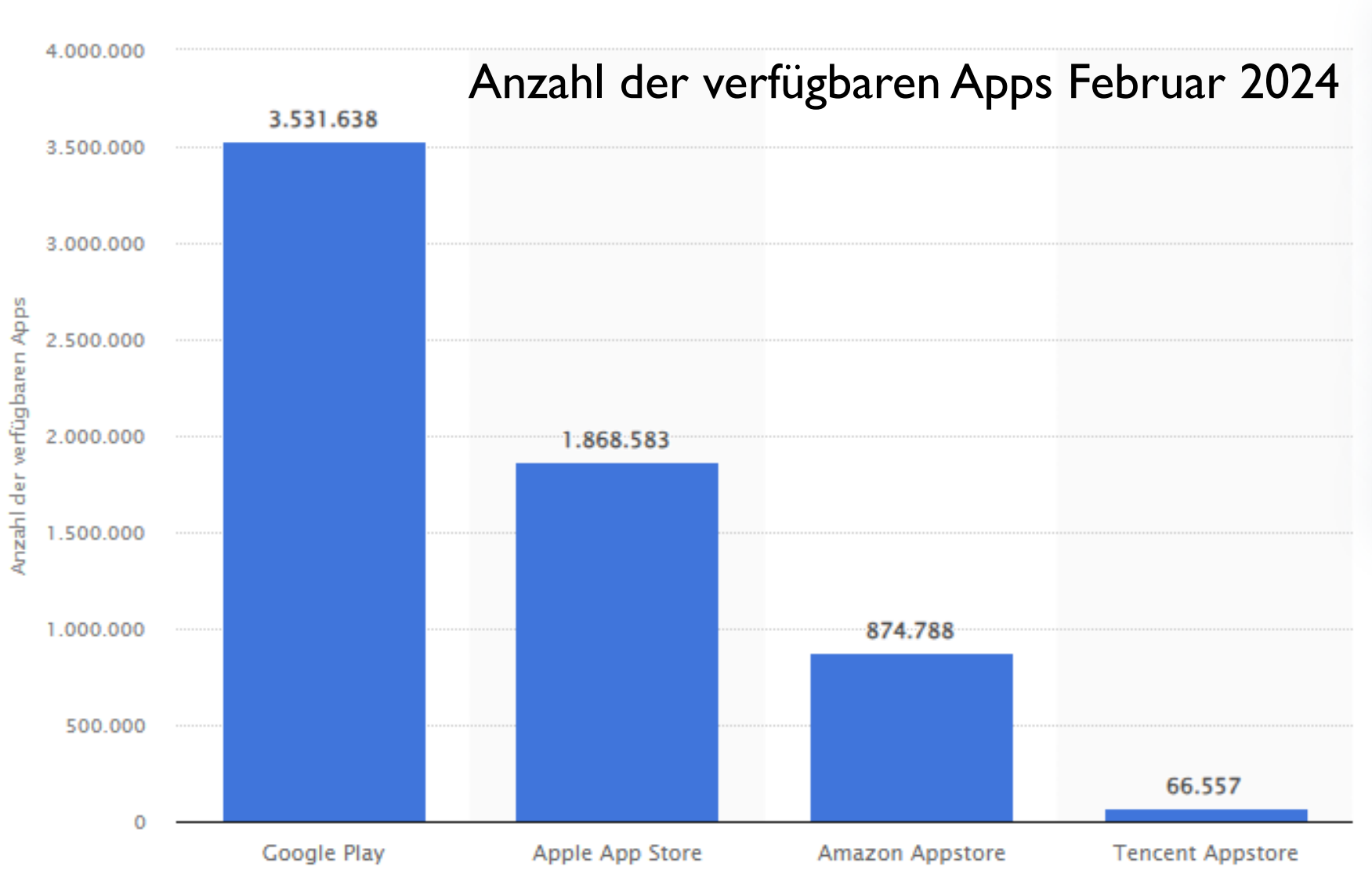
INTERNET HEUTE: DAS NETZ DER NETZE



INTERNET HEUTE: DAS NETZ DER NETZE



INTERNET HEUTE: SICHERHEITSPROBLEMATIK SYSTEMBEDINGT



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: SICHERHEITSPROBLEMATIK SYSTEMBEDINGT

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

SICHERHEIT IM INTERNET

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

FAKESHOP ERKENNUNGSKRITERIEN

https://www.smartfa...de

SmartFakeShop
SmartFakes & more

Wir machen das Beste aus Deinem Geld!

0 Produkte im Warenkorb: 0.00 €

- SMARTPHONES
- TABLETS
- KONSOLEN
- E-BOOK-READER
- WEARABLES
- SPEICHERKARTEN
- ZUBEHÖR

Geben Sie Ihren Suchbegriff ein

MONSUNG Dynasty 9

Prozessor: Octa Core (8 Kerne)
Speicher: 8 GB, 64 GB interner Speicher
Display: 6" AMOLED, 2960 x 1440
Kamera: 20 Megapixel, **Video:** UHD
LTE: Ja, **USB:** 3.1, **Akku:** 5000 mAh
+ HiFi Kopfhörer, 256 GB microSD-Karte!
Mehr zu diesem Produkt

~~€ 699,-~~
€ 369,-
inkl. MwSt. zzgl. Versandkosten

ANMELDEN

Zahlung: **Vorauskasse**
Artikel lagernd.
Sofort lieferbar!

100% PREMIUM MARKE GARANTIE

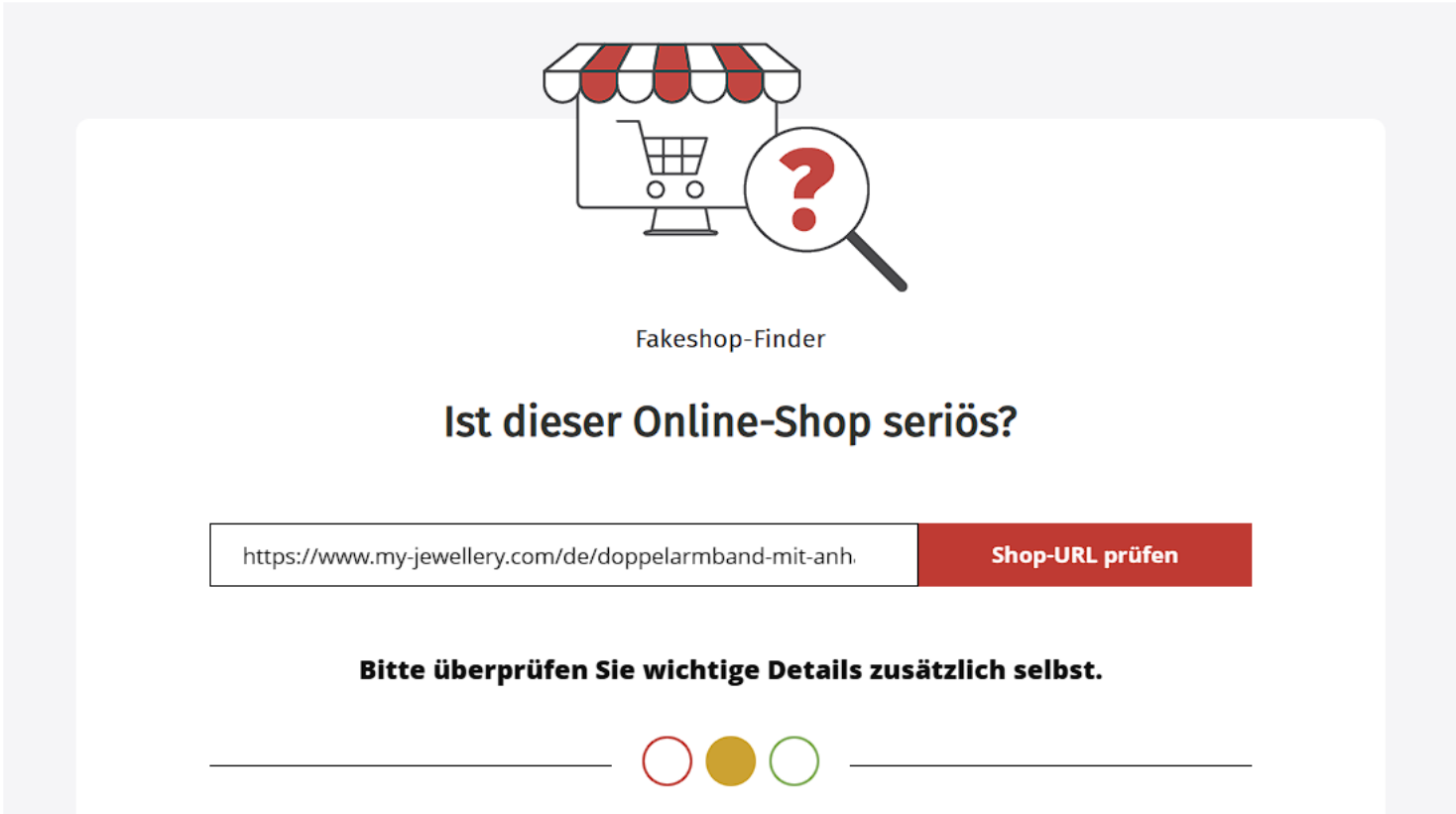
Und das meinen unsere Kunden:

- ★★★★★ Ali G. aus Bonn: **"Schon das dritte Handy bestellt, alles Top!"**
- ★★★★★ Uwe S. aus Heide: **"Preisleistungsverhältnis - unschlagbar!"**
- ★★★★★ Brigitte P. aus Berlin: **"Schnelle Lieferung, Top Produkt - 1A"**
- ★★★★★ Boris B. aus Ulm: **"Erste Liga, Spitzenplatz, immer wieder gerne"**

WIDERRUFSBELEHRUNG | AGB | KONTAKT | IMPRESSUM

FAKESHOP FINDER

https://www.verbraucherzentrale.de/fakeshopfinder-71560



PHISHING E-MAILS

Wichtige Hinweise zu Ihrer Steuererklärung

BF Bundeszentralamt fur Steuern <develop@sitetelekom.com.tr>

An

Antworten | Allen antworten | Weiterleiten | ...

Do 05.03.2026 02:33

Referenznummer: 091B7969

Gesetzlicher Hinweis: Kryptowährungen und Steuern

Sehr geehrte Damen und Herren,

Übermittlungen von Kryptoanbietern an die Finanzverwaltung sind bereits erfolgt. Dennoch wurden entsprechende Gewinne oder Vermögenswerte nicht durchgängig in den Steuererklärungen angegeben.

Wir setzen Ihnen hiermit eine Frist von drei Werktagen zur vollständigen Deklaration Ihrer Krypto-Vermögenswerte. Nach fruchtlosem Ablauf dieser Frist können auf Grundlage der Abgabenordnung (AO) entsprechende Geldbußen festgesetzt werden.

Weiteres Vorgehen:

- Loggen Sie sich mit Ihrem Zertifikat im Portal Mein ELSTER ein.
- Ergänzen Sie dort Ihre Krypto-Wallets entsprechend den bereitgestellten Hinweisen.

Mein ELSTER

Hinweis zur Datenprüfung

Vertrauen Sie dem Namen nicht, der als Absender gezeigt wird!

Überprüfen Sie die Links, aber klicken Sie diese nicht an!

Seien Sie misstrauisch, wenn zeitlicher Druck ausgeübt wird!

Klicken Sie nicht auf Anhänge (.com, .exe, zip, xlsm, docm).!

Achten Sie auf die Anrede!

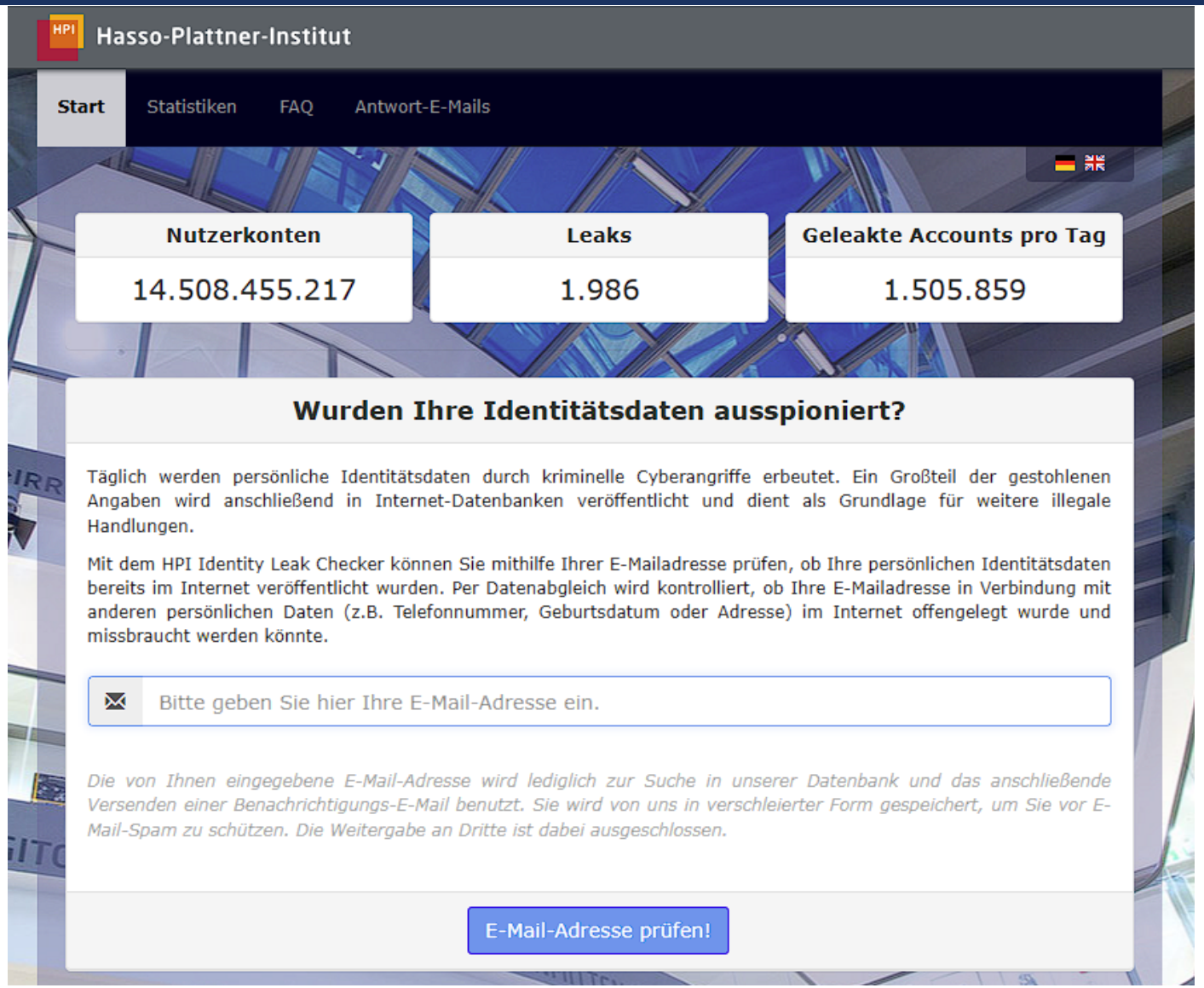
Achten Sie auf grammatikalisch korrekten Text!

Misstrauen Sie Rabatten etc. Ist es wirklich zu schön, um wahr zu sein?

Haben Sie Zweifel – Vertrauen Sie ihrem ersten „Bauchgefühl“!

PHISHING E-MAILS

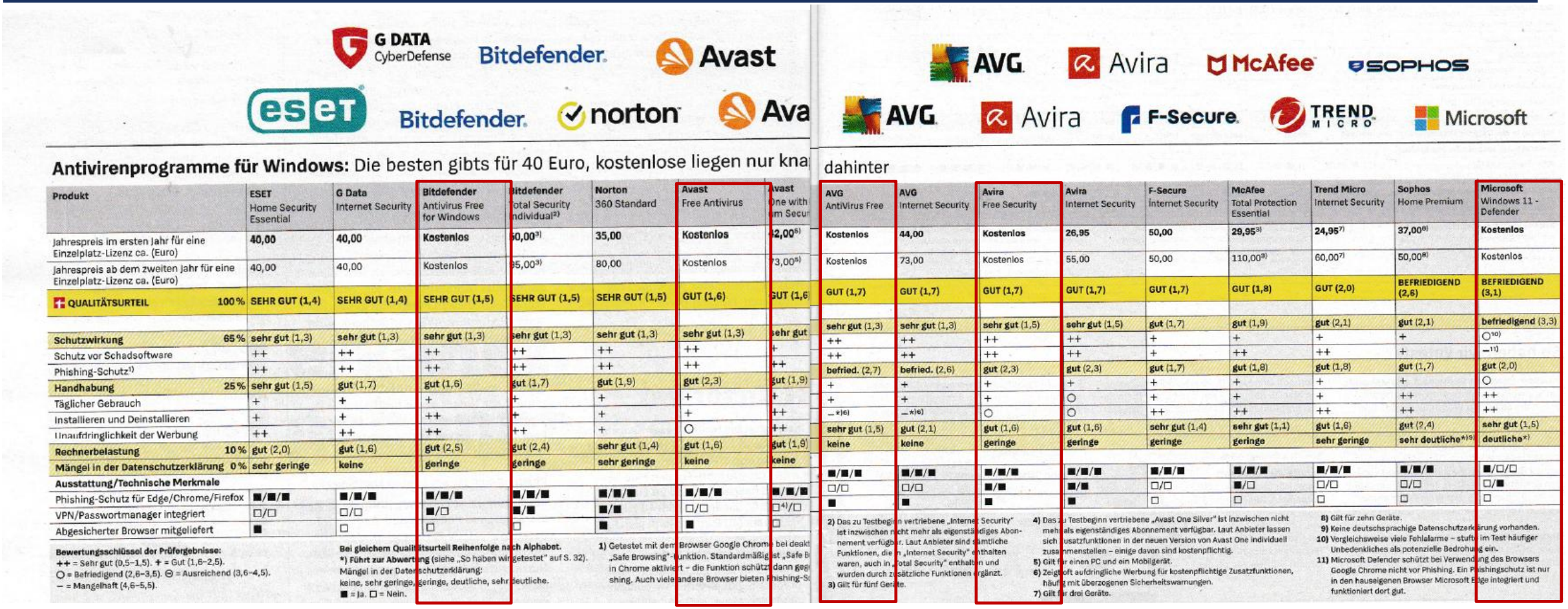
PHISHING E-MAILS



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 3/2026



Antivirenprogramme für Windows: Die besten gibts für 40 Euro, kostenlose liegen nur kna dahinter

Produkt		ESET Home Security Essential	G Data Internet Security	Bitdefender Antivirus Free for Windows	Bitdefender Total Security Individual[2]	Norton 360 Standard	Avast Free Antivirus	Avast One with Secur
Jahrespreis im ersten Jahr für eine Einzelplatz-Lizenz ca. (Euro)		40,00	40,00	Kostenlos	50,00[3]	35,00	Kostenlos	42,00[5]
Jahrespreis ab dem zweiten Jahr für eine Einzelplatz-Lizenz ca. (Euro)		40,00	40,00	Kostenlos	95,00[3]	80,00	Kostenlos	73,00[5]
QUALITÄTSURTEIL	100 %	SEHR GUT (1,4)	SEHR GUT (1,4)	SEHR GUT (1,5)	SEHR GUT (1,5)	SEHR GUT (1,5)	GUT (1,6)	GUT (1,6
Schutzwirkung	65 %	sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,3)	sehr gut
Schutz vor Schadsoftware		++	++	++	++	++	++	+
Phishing-Schutz[1]		++	++	++	++	++	++	++
Handhabung	25 %	sehr gut (1,5)	gut (1,7)	gut (1,6)	gut (1,7)	gut (1,9)	gut (2,3)	gut (1,9)
Täglicher Gebrauch		+	+	+	+	+	+	+
Installieren und Deinstallieren		+	+	++	+	+	+	++
Unaufdringlichkeit der Werbung		++	++	++	++	+	○	++
Rechnerbelastung	10 %	gut (2,0)	gut (1,6)	gut (2,5)	gut (2,4)	sehr gut (1,4)	gut (1,6)	gut (1,9)
Mängel in der Datenschutzerklärung	0 %	sehr geringe	keine	geringe	geringe	sehr geringe	keine	keine
Ausstattung/Technische Merkmale								
Phishing-Schutz für Edge/Chrome/Firefox		■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■
VPN/Passwortmanager integriert		□/□	□/□	■/□	■/■	■/■	□/□	□[4]/□
Abgesicherter Browser mitgeliefert		■	□	□	□	■	■	□

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).

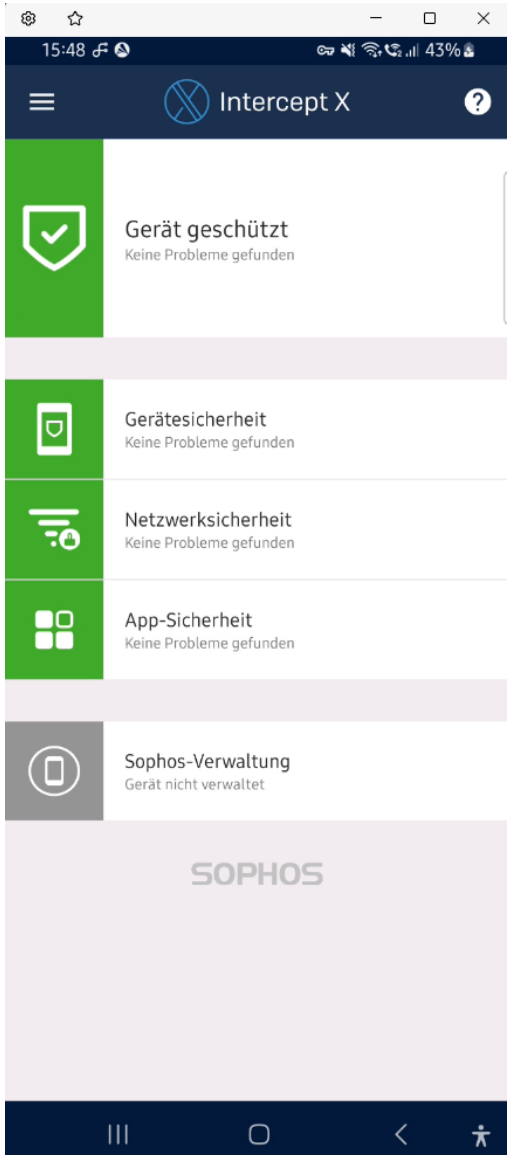
Bei gleichem Qualitätsurteil Reihenfolge nach Alphabet.
***) Führt zur Abwertung** (siehe „So haben wir getestet" auf S. 32).
Mängel in der Datenschutzerklärung:
keine, sehr geringe, geringe, deutliche, sehr deutliche.
■ = Ja. □ = Nein.

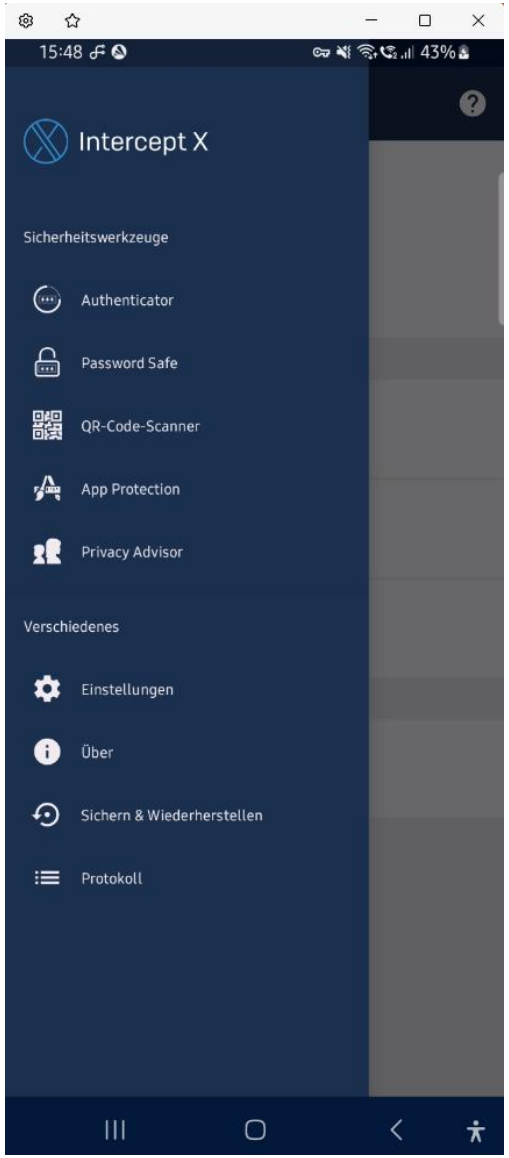
1) Getestet mit dem Browser Google Chrome bei deakt „Safe Browsing"-Funktion. Standardmäßig ist „Safe B in Chrome aktiviert – die Funktion schützt dann gegen shing. Auch viele andere Browser bieten Phishing-S

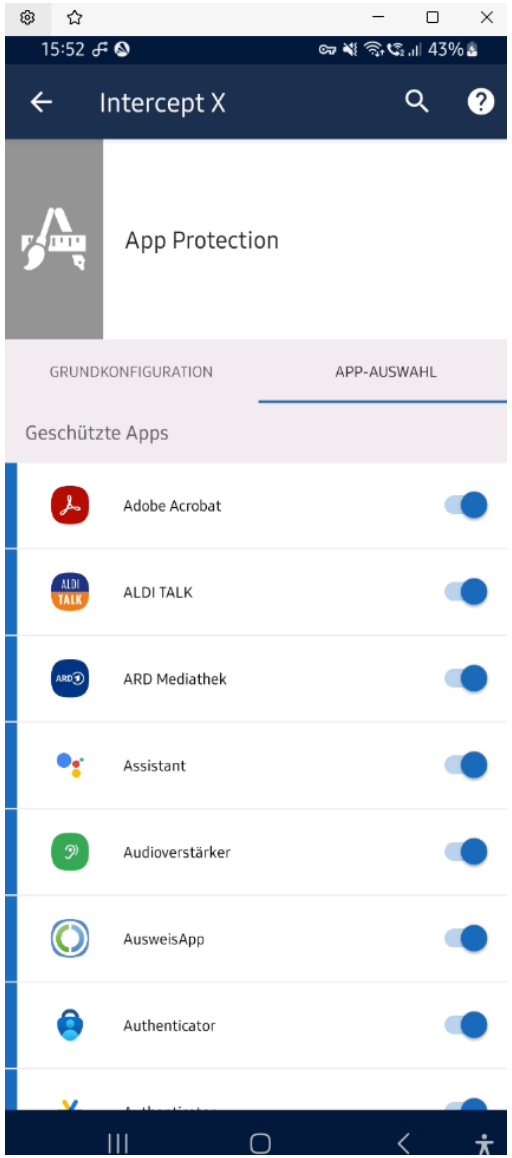
Produkt		AVG AntiVirus Free	AVG Internet Security	Avira Free Security	Avira Internet Security	F-Secure Internet Security	McAfee Total Protection Essential	Trend Micro Internet Security	Sophos Home Premium	Microsoft Windows 11 - Defender
Jahrespreis im ersten Jahr für eine Einzelplatz-Lizenz ca. (Euro)		Kostenlos	44,00	Kostenlos	26,95	50,00	29,95[3]	24,95[7]	37,00[8]	Kostenlos
Jahrespreis ab dem zweiten Jahr für eine Einzelplatz-Lizenz ca. (Euro)		Kostenlos	73,00	Kostenlos	55,00	50,00	110,00[3]	60,00[7]	50,00[8]	Kostenlos
QUALITÄTSURTEIL	100 %	GUT (1,7)	GUT (1,7)	GUT (1,7)	GUT (1,7)	GUT (1,7)	GUT (1,8)	GUT (2,0)	BEFRIEDIGEND (2,6)	BEFRIEDIGEND (3,1)
Schutzwirkung	65 %	sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,5)	sehr gut (1,5)	gut (1,7)	gut (1,9)	gut (2,1)	gut (2,1)	befriedigend (3,3)
Schutz vor Schadsoftware		++	++	++	++	+	+	+	+	○[10]
Phishing-Schutz[1]		++	++	++	++	+	++	++	+	–[11]
Handhabung	25 %	befried. (2,7)	befried. (2,6)	gut (2,3)	gut (2,3)	gut (1,7)	gut (1,8)	gut (1,8)	gut (1,7)	gut (2,0)
Täglicher Gebrauch		+	+	+	+	+	+	+	+	○
Installieren und Deinstallieren		+	+	+	○	+	+	+	++	++
Unaufdringlichkeit der Werbung		–*)6)	–*)6)	○	○	++	++	++	++	++
Rechnerbelastung	10 %	sehr gut (1,5)	gut (2,1)	gut (1,6)	gut (1,6)	sehr gut (1,4)	sehr gut (1,1)	gut (1,8)	gut (2,4)	sehr gut (1,5)
Mängel in der Datenschutzerklärung	0 %	keine	keine	geringe	geringe	geringe	geringe	sehr geringe	sehr deutliche*)9)	deutliche*)
Ausstattung/Technische Merkmale										
Phishing-Schutz für Edge/Chrome/Firefox		■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/□/□
VPN/Passwortmanager integriert		□/□	□/□	■/■	■/■	□/□	■/□	□/□	□/□	□/■
Abgesicherter Browser mitgeliefert		■	■	■	■	□	□	□	□	□

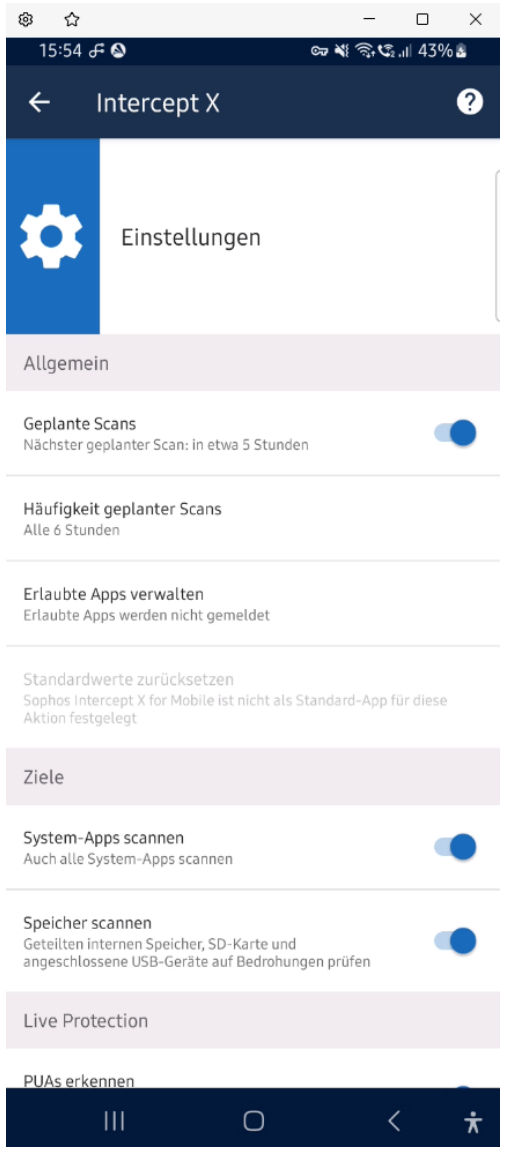
2) Das zu Testbeginn vertriebene „Internet Security" ist inzwischen nicht mehr als eigenständiges Abonnement verfügbar. Laut Anbieter sind sämtliche Funktionen, die in „Internet Security" enthalten waren, auch in „Total Security" enthalten und wurden durch zusätzliche Funktionen ergänzt.
3) Gilt für fünf Geräte.
4) Das zu Testbeginn vertriebene „Avast One Silver" ist inzwischen nicht mehr als eigenständiges Abonnement verfügbar. Laut Anbieter lassen sich Zusatzfunktionen in der neuen Version von Avast One individuell zusammenstellen – einige davon sind kostenpflichtig.
5) Gilt für einen PC und ein Mobilgerät.
6) Zeigt oft aufdringliche Werbung für kostenpflichtige Zusatzfunktionen, häufig mit überzogenen Sicherheitswarnungen.
7) Gilt für drei Geräte.
8) Gilt für zehn Geräte.
9) Keine deutschsprachige Datenschutzerklärung vorhanden.
10) Vergleichsweise viele Fehlalarme – stuft im Test häufiger Unbedenkliches als potenzielle Bedrohung ein.
11) Microsoft Defender schützt bei Verwendung des Browsers Google Chrome nicht vor Phishing. Ein Phishingschutz ist nur in den hauseigenen Browser Microsoft Edge integriert und funktioniert dort gut.

ANTIVIRUS SOFTWARE – BEISPIEL INTERCEPT X (KOSTENLOS VERSION)

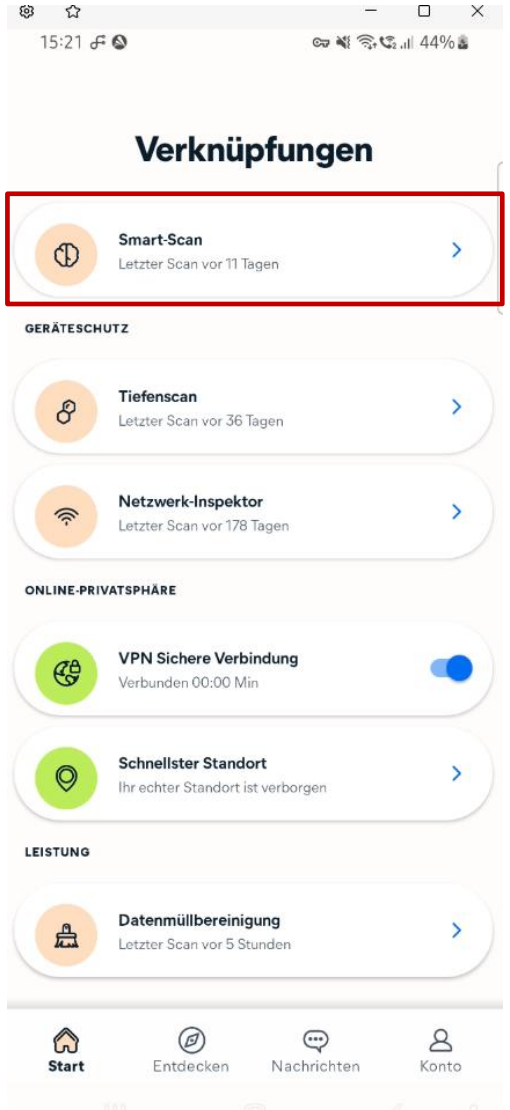


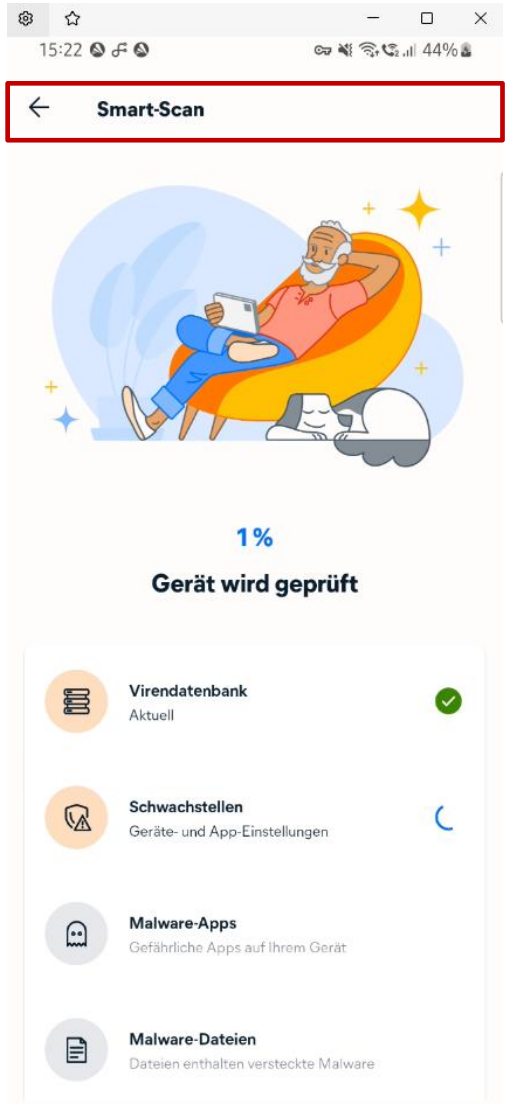


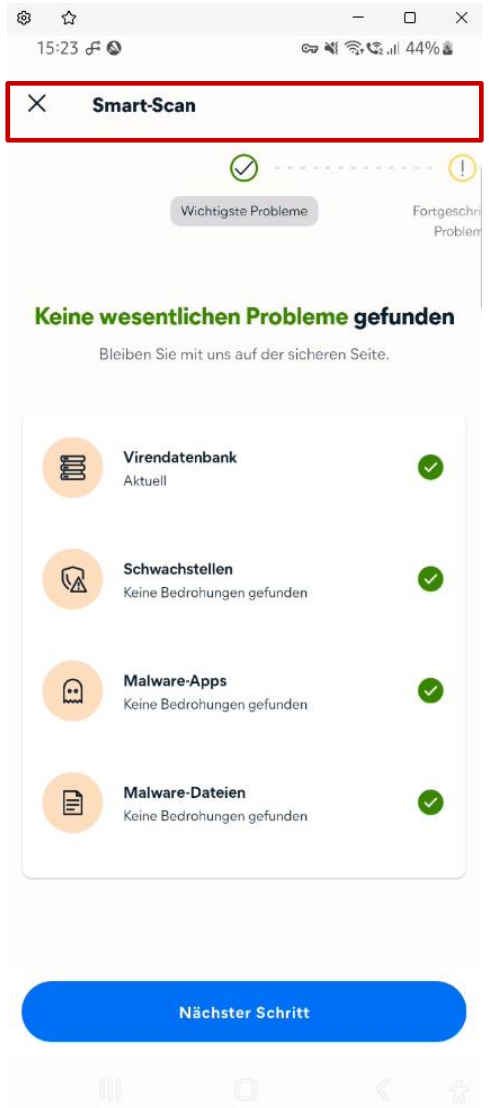




ANTIVIRUS SOFTWARE – BEISPIEL AVAST (KOSTENLOS VERSION)







WEITERE PERSÖNLICHE ORGANISATORISCHE MAßNAHMEN

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

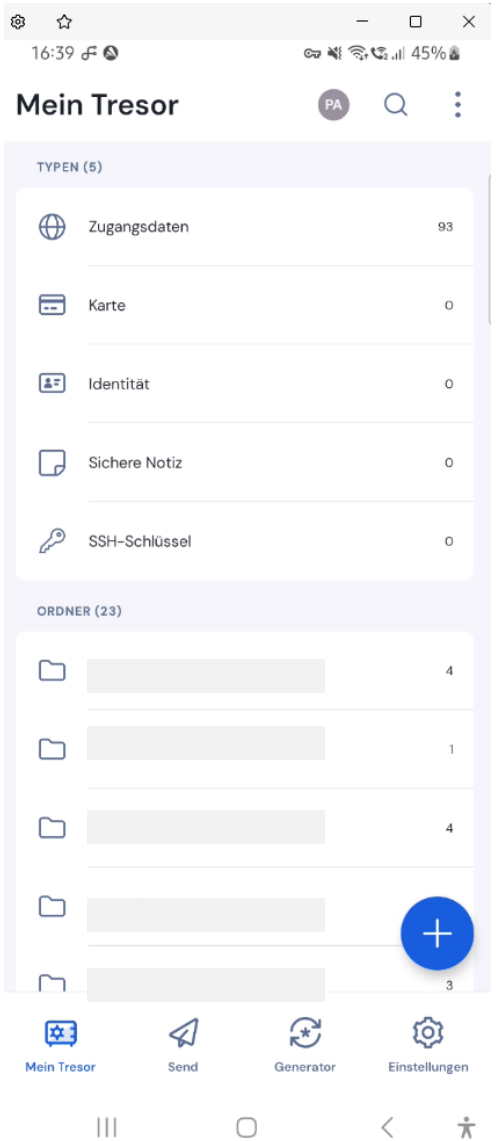
Doch bei allen Updates gilt:

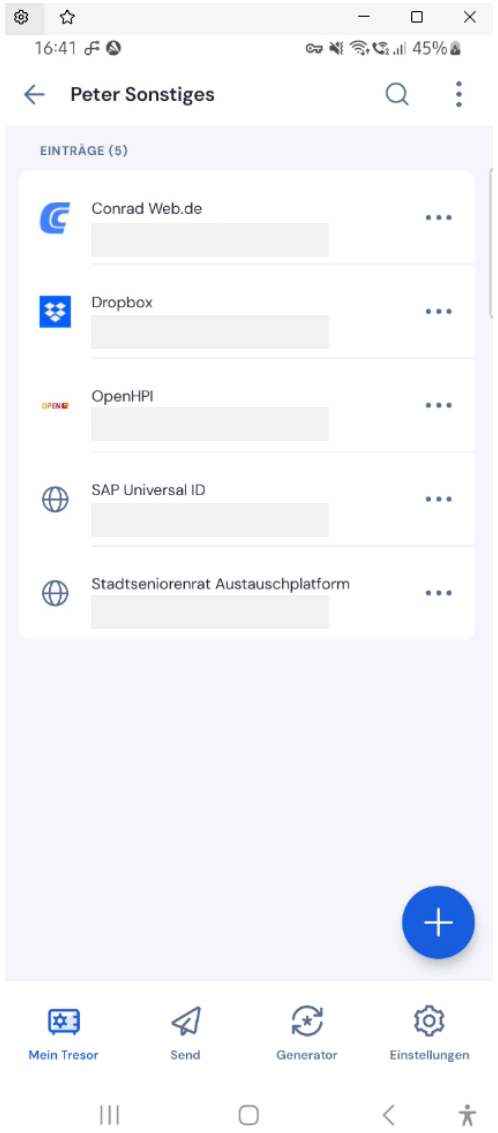
- Vertrauenswürdigkeit von Quelle und Updates müssen stets überprüft werden
- Ansonsten können Updates selbst zur Quelle neuer Angriffspunkte werden und zur Installation von Schadsoftware führen

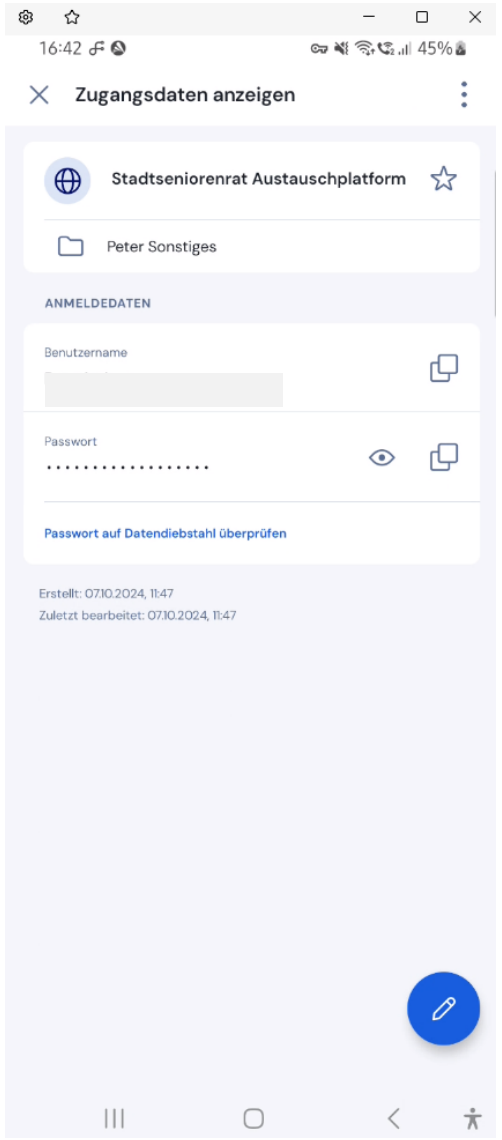
SICHERE PASSWÖRTER

- 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







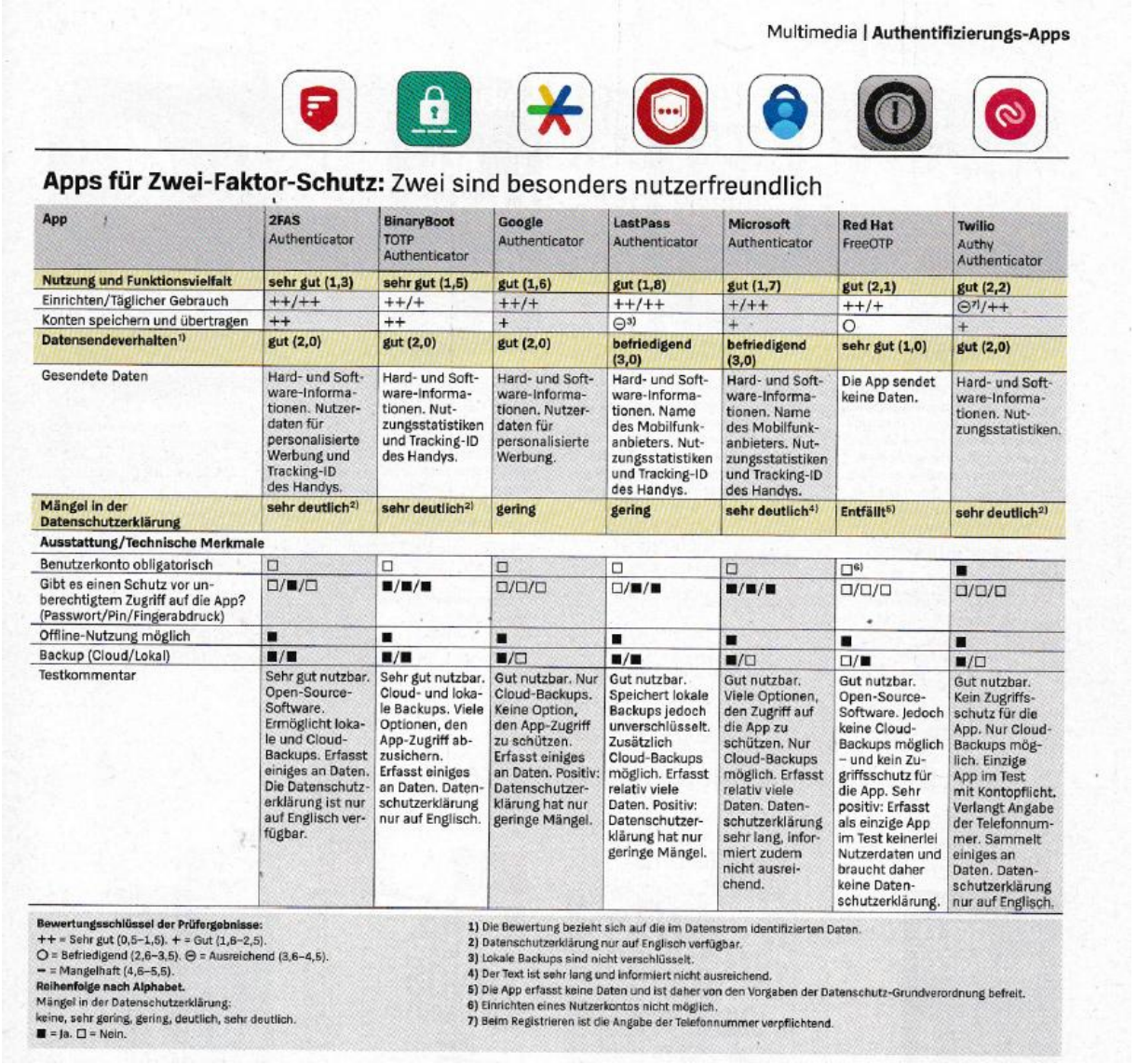
2-FAKTOR-AUTHENTIFIZIERUNG

- 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,….



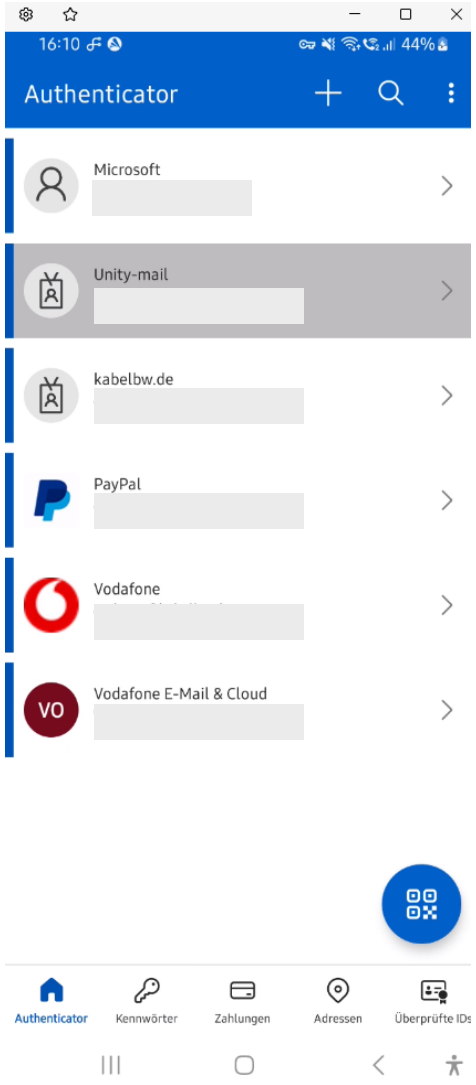
Apps für Zwei-Faktor-Schutz: Zwei sind besonders nutzerfreundlich

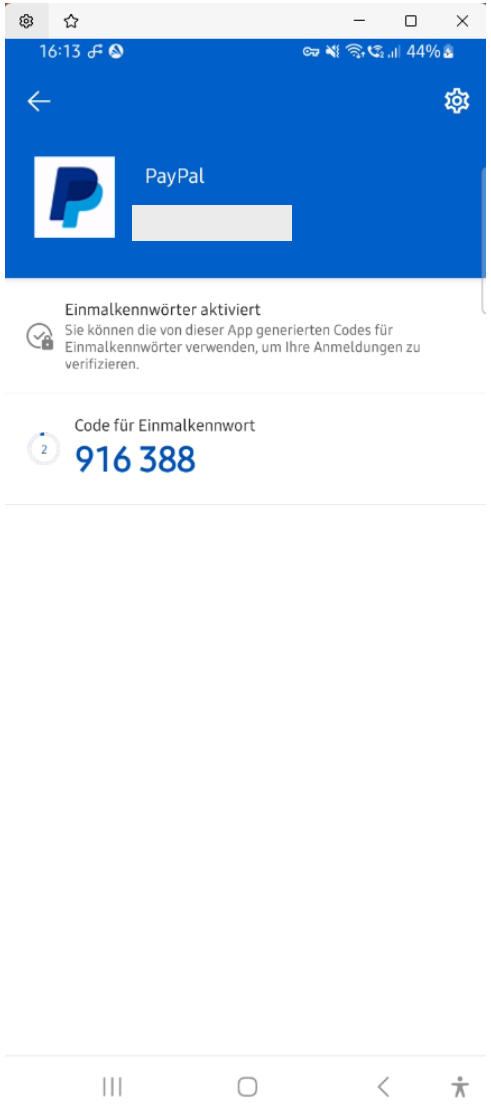
App	2FAS Authenticator	BinaryBoot TOTP Authenticator	Google Authenticator	LastPass Authenticator	Microsoft Authenticator	Red Hat FreeOTP	Twilio Authy Authenticator
Nutzung und Funktionsvielfalt	**sehr gut (1,3)**	**sehr gut (1,5)**	**gut (1,6)**	**gut (1,8)**	**gut (1,7)**	**gut (2,1)**	**gut (2,2)**
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

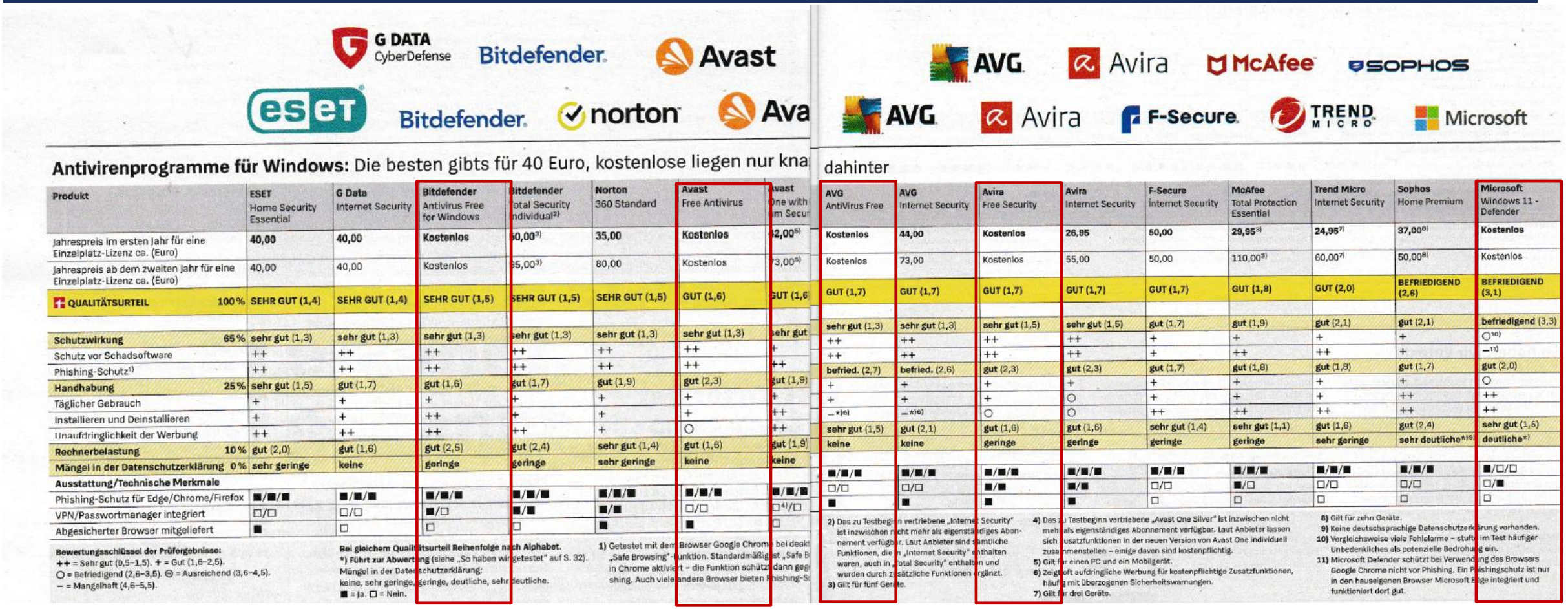
SICHERHEIT IM INTERNET

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

ANTIVIRUS SOFTWARE

- Vielzahl von Anbietern
- Orientierung bietet Stiftung Warentest (Test 3/25, 3/26)
- Quellen: Anbieter Webseiten, Microsoft Store, Google Playstore,….

ANTIVIRUS SOFTWARE **FÜR ANDROID**: STIFTUNG WARENTEST 3/2026



Antivirenprogramme für Windows: Die besten gibts für 40 Euro, kostenlose liegen nur kna dahinter

Produkt		ESET Home Security Essential	G Data Internet Security	Bitdefender Antivirus Free for Windows	Bitdefender Total Security Individual[2]	Norton 360 Standard	Avast Free Antivirus	Avast One with Secur
Jahrespreis im ersten Jahr für eine Einzelplatz-Lizenz ca. (Euro)		40,00	40,00	Kostenlos	50,00[3]	35,00	Kostenlos	42,00[5]
Jahrespreis ab dem zweiten Jahr für eine Einzelplatz-Lizenz ca. (Euro)		40,00	40,00	Kostenlos	95,00[3]	80,00	Kostenlos	73,00[5]
QUALITÄTSURTEIL	100 %	SEHR GUT (1,4)	SEHR GUT (1,4)	SEHR GUT (1,5)	SEHR GUT (1,5)	SEHR GUT (1,5)	GUT (1,6)	GUT (1,6
Schutzwirkung	65 %	sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,3)	sehr gut
Schutz vor Schadsoftware		++	++	++	++	++	++	+
Phishing-Schutz[1]		++	++	++	++	++	++	++
Handhabung	25 %	sehr gut (1,5)	gut (1,7)	gut (1,6)	gut (1,7)	gut (1,9)	gut (2,3)	gut (1,9)
Täglicher Gebrauch		+	+	+	+	+	+	+
Installieren und Deinstallieren		+	+	++	+	+	+	++
Unaufdringlichkeit der Werbung		++	++	++	++	+	○	++
Rechnerbelastung	10 %	gut (2,0)	gut (1,6)	gut (2,5)	gut (2,4)	sehr gut (1,4)	gut (1,6)	gut (1,9)
Mängel in der Datenschutzerklärung	0 %	sehr geringe	keine	geringe	geringe	sehr geringe	keine	keine
Ausstattung/Technische Merkmale								
Phishing-Schutz für Edge/Chrome/Firefox		■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■
VPN/Passwortmanager integriert		□/□	□/□	■/□	■/■	■/■	□/□	□[4]/□
Abgesicherter Browser mitgeliefert		■	□	□	□	■	■	□

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. 32).
Mängel in der Datenschutzerklärung:
keine, sehr geringe, geringe, deutliche, sehr deutliche.
■ = Ja. □ = Nein.

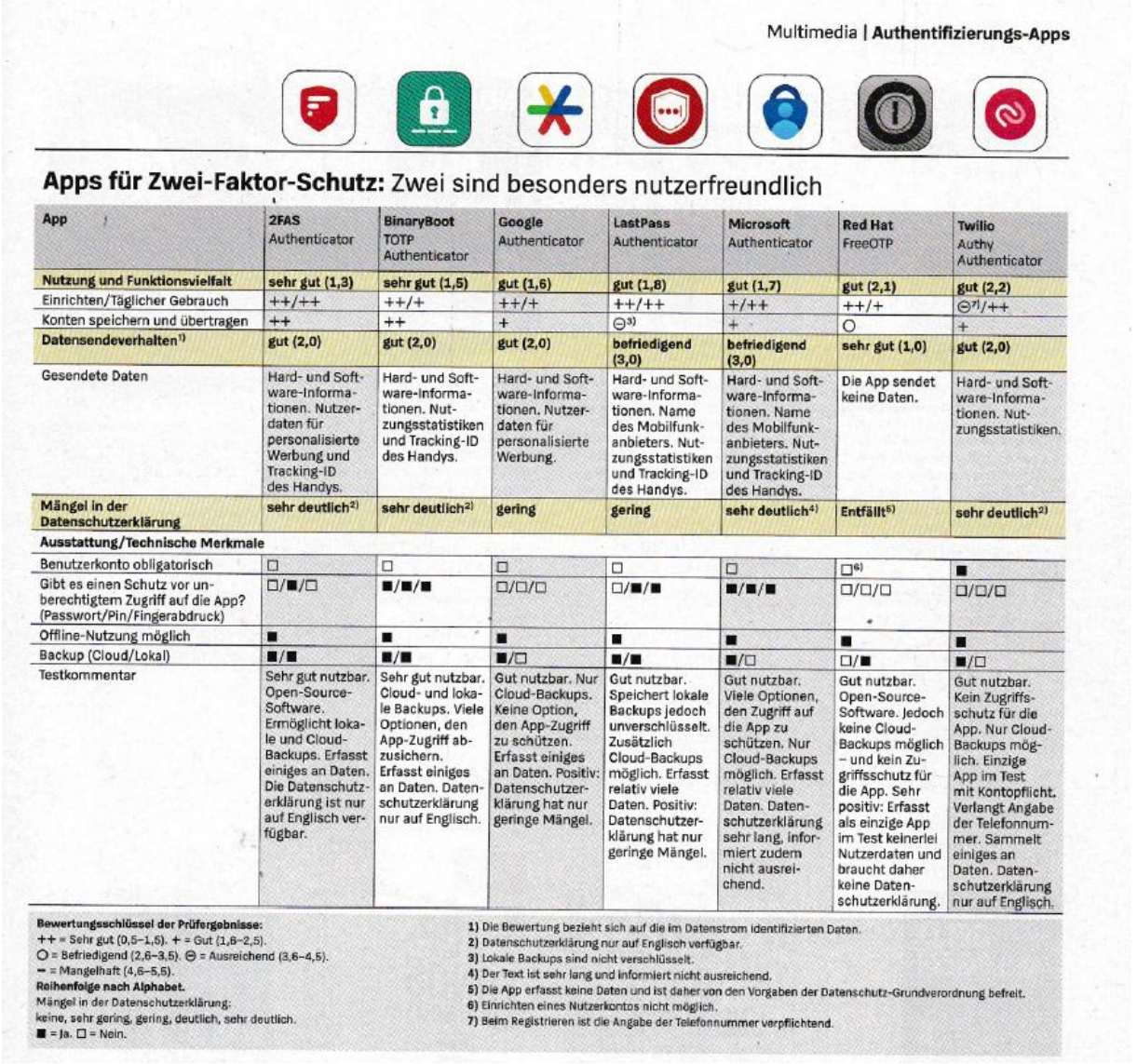
1) Getestet mit dem Browser Google Chrome bei deakt „Safe Browsing"-Funktion. Standardmäßig ist „Safe B in Chrome aktiviert – die Funktion schützt dann gegen shing. Auch viele andere Browser bieten Phishing-S

Produkt		AVG AntiVirus Free	AVG Internet Security	Avira Free Security	Avira Internet Security	F-Secure Internet Security	McAfee Total Protection Essential	Trend Micro Internet Security	Sophos Home Premium	Microsoft Windows 11 - Defender
Jahrespreis im ersten Jahr für eine Einzelplatz-Lizenz ca. (Euro)		Kostenlos	44,00	Kostenlos	26,95	50,00	29,95[3]	24,95[7]	37,00[8]	Kostenlos
Jahrespreis ab dem zweiten Jahr für eine Einzelplatz-Lizenz ca. (Euro)		Kostenlos	73,00	Kostenlos	55,00	50,00	110,00[3]	60,00[7]	50,00[8]	Kostenlos
QUALITÄTSURTEIL	100 %	GUT (1,7)	GUT (1,7)	GUT (1,7)	GUT (1,7)	GUT (1,7)	GUT (1,8)	GUT (2,0)	BEFRIEDIGEND (2,6)	BEFRIEDIGEND (3,1)
Schutzwirkung	65 %	sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,5)	sehr gut (1,5)	gut (1,7)	gut (1,9)	gut (2,1)	gut (2,1)	befriedigend (3,3)
Schutz vor Schadsoftware		++	++	++	++	+	+	+	+	○[10]
Phishing-Schutz[1]		++	++	++	++	+	++	++	+	–[11]
Handhabung	25 %	befried. (2,7)	befried. (2,6)	gut (2,3)	gut (2,3)	gut (1,7)	gut (1,8)	gut (1,8)	gut (1,7)	gut (2,0)
Täglicher Gebrauch		+	+	+	+	+	+	+	+	○
Installieren und Deinstallieren		+	+	+	○	+	+	+	++	++
Unaufdringlichkeit der Werbung		–*)6)	–*)6)	○	○	++	++	++	++	++
Rechnerbelastung	10 %	sehr gut (1,5)	gut (2,1)	gut (1,6)	gut (1,6)	sehr gut (1,4)	sehr gut (1,1)	gut (1,8)	gut (2,4)	sehr gut (1,5)
Mängel in der Datenschutzerklärung	0 %	keine	keine	geringe	geringe	geringe	geringe	sehr geringe	sehr deutliche*)9)	deutliche*)
Ausstattung/Technische Merkmale										
Phishing-Schutz für Edge/Chrome/Firefox		■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/□/□
VPN/Passwortmanager integriert		□/□	□/□	■/■	■/■	□/□	■/□	□/□	□/□	□/■
Abgesicherter Browser mitgeliefert		■	■	■	■	□	□	□	□	□

2) Das zu Testbeginn vertriebene „Internet Security" ist inzwischen nicht mehr als eigenständiges Abonnement verfügbar. Laut Anbieter sind sämtliche Funktionen, die in „Internet Security" enthalten waren, auch in „Total Security" enthalten und wurden durch zusätzliche Funktionen ergänzt.
3) Gilt für fünf Geräte.
4) Das zu Testbeginn vertriebene „Avast One Silver" ist inzwischen nicht mehr als eigenständiges Abonnement verfügbar. Laut Anbieter lassen sich Zusatzfunktionen in der neuen Version von Avast One individuell zusammenstellen – einige davon sind kostenpflichtig.
5) Gilt für einen PC und ein Mobilgerät.
6) Zeigt oft aufdringliche Werbung für kostenpflichtige Zusatzfunktionen, häufig mit überzogenen Sicherheitswarnungen.
7) Gilt für drei Geräte.
8) Gilt für zehn Geräte.
9) Keine deutschsprachige Datenschutzerklärung vorhanden.
10) Vergleichsweise viele Fehlalarme – stuft im Test häufiger Unbedenkliches als potenzielle Bedrohung ein.
11) Microsoft Defender schützt bei Verwendung des Browsers Google Chrome nicht vor Phishing. Ein Phishingschutz ist nur in den hauseigenen Browser Microsoft Edge integriert und funktioniert dort gut.

2-FAKTOR AUTHENTIFIZIERUNGS-SOFTWARE

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

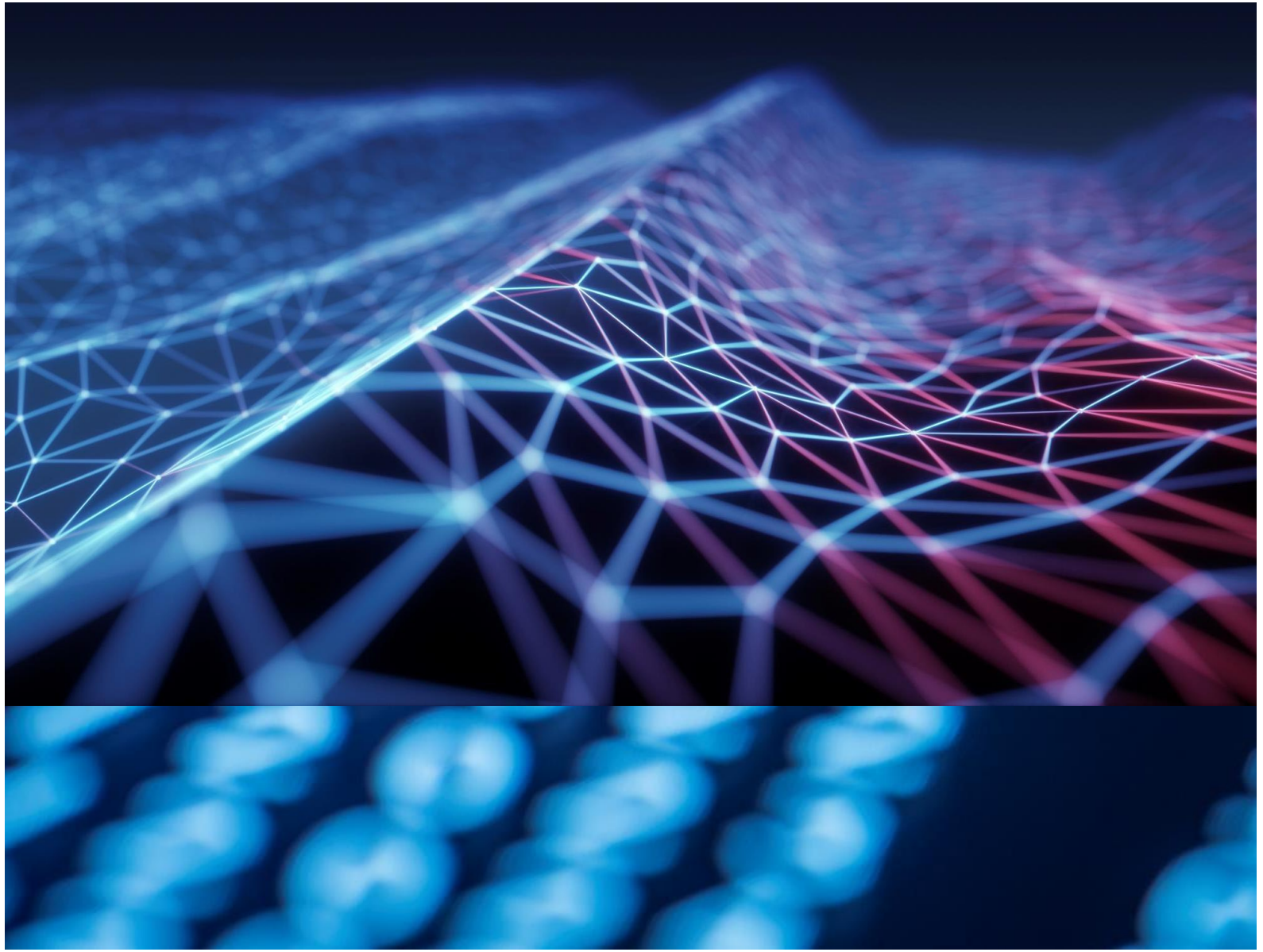


Apps für Zwei-Faktor-Schutz: Zwei sind besonders nutzerfreundlich

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