Digitale Sicherheitslage von Verbraucher:innen in Deutschland

DsiN SICHERHEITS-INDEX 2025

FOKUSTHEMA

VERTRAUEN IN DER DIGITALEN WELT

DsiN-Schirmherrschaft:

Bundesministerium des Innern

Studien-Schirmherrschaft:

Bundesministerium der Justiz und für Verbraucherschutz

Eine Studie von:

DsiN Deutschland sicher im Netz

Grußwort

Frank Schwabe

Sehr geehrte Leser:innen,

Digitalpolitik ist Gesellschaftspolitik. Starke digitale Kompetenzen sind essentiell für gesellschaftliche Teilhabe, eine resiliente Demokratie und die Wettbewerbsfähigkeit unserer Wirtschaft. Zu diesen Kompetenzen gehören ein souveräner, sicherer und kritischer Umgang mit digitalen Tools. Um diese Kompetenzen zu erlangen, braucht es uns alle: Start-ups, Wirtschaft, Zivilgesellschaft, öffentliche Bildungsträger und Sozial- sowie Verbraucherschutzverbände. Der Verein „Deutschland sicher im Netz“ gehört seit Jahren zu eben diesen Akteuren und trägt praktisch dazu bei, Wissen und Verhaltenstipps zu vermitteln, dank derer Verbraucher:innen sich sicher und vertrauensvoll im Netz bewegen können. Mit dem jährlich veröffentlichten Sicherheitsindex leistet DsiN zudem einen wichtigen Beitrag dazu, die Sicherheitslage der Verbraucher:innen in der digitalen Welt einzuschätzen.

Der aktuelle Sicherheitsindex 2025 zeigt in seinem Fokusthema „Vertrauen in die digitale Welt“ dabei abermals ein ambivalentes Bild. Verbraucher:innen fühlen sich so sicher wie noch nie. Das subjektive Verunsicherungsgefühl der Internetnutzer:innen ist um 3,0 Indexpunkte auf 18,9 Indexpunkte gesunken. Das ist ein Tiefstand. Auch das Sicherheitswissen verbessert sich im Vergleich zum Vorjahr auf 90,5 Indexpunkte. Das Sicherheitsverhalten ist hingegen leicht gesunken, um 0,7 Indexpunkte auf 52,9 Indexpunkte. Nur 15,6 % der Nutzer:innen zeigen sich mit ihren eigenen digitalen Kompetenzen zufrieden.

Gleichzeitig ist die Bedrohungslage weiter angespannt, insbesondere das sogenannte Phishing stellt eine verbreitete Gefahr für Verbraucher:innen dar. Mit 61,6 Indexpunkten liegt der Bedrohungsindex bei einem neuen Höchstwert.

Digitaler Selbstschutz muss daher ein zentraler Baustein einer sicheren Nutzung digitaler Dienste und Produkte bleiben. Zur Stärkung des digitalen Selbstschutzes will die Bundesregierung eine altersübergreifende digitale Kompetenzoffensive starten und sich auf europäischer Ebene für Verbraucherinteressen im digitalen Raum und insbesondere für die Schließung von Schutzlücken im Verbraucherrecht einsetzen. Unser Ziel ist, dass digitale Angebote schon „by design“ und „by default“ verbraucherfreundlich gestaltet werden. Der im Oktober 2024 verabschiedeten Cyber Resiliance Act war hier bereits ein wichtiger Schritt. Er führt für viele Verbraucherprodukte neue Mindeststandards in der IT-Sicherheit ein und wird stufenweise bis 2027 voll anwendbar sein.

Ich freue mich, DsiN dabei weiter als engagierten Mitstreiter zu wissen, damit wir alle gemeinsam dieses Ziel auch erreichen. Für diese Arbeit danke ich den Verantwortlichen ganz herzlich und wünsche allen Leser:innen viel Erkenntnisgewinn aus dem diesjährigen Sicherheitsindex 2025.

Ihr

Frank Schwabe

Parlamentarischer Staatssekretär bei der Bundesministerin für Justiz und Verbraucherschutz

Vorwort

Isabelle Rosière

Pierre Du Bois

Liebe Leser:innen,

digitale Sicherheit geht uns alle an. Rund 96 % der Menschen in Deutschland ab 14 Jahren sind laut Statistischem Bundesamt im Jahr 2025 im Netz unterwegs. Der DsiN-Sicherheitsindex untersucht, wie sie online unterwegs sind, welche Dienste sie nutzen und vor allem, wie sicher sie dabei agieren. Das bildet die Studie in einer zentralen Kennziffer auf einer Skala von 0 bis 100 ab – dem DsiN-Sicherheitsindex.

In diesem Jahr stagniert er auf einem historisch schlechten Niveau mit nur 55,7 Punkten. Es zeigt sich, dass nicht nur außenstehende und fatalistische Nutzergruppen weiter an digitaler Sicherheit einbüßen. Auch im klassischen „Mittelfeld" verschlechtert sich die Situation. Die größte Gruppe unter den deutschen Onliner:innen liegt mit ihrem Index-Wert in diesem Jahr erstmalig unter der kritischen Schwelle von 50 Punkten: Ihre Bedrohungslage übersteigt ihr persönliches Schutzniveau. Das Sicherheitsgefälle innerhalb der digitalen Gesellschaft verschärft sich damit weiter.

Was positiv ist: 77,8 % der Befragten sagen, dass ein vorsichtigerer Umgang mit den eigenen persönlichen Daten eine geeignete Maßnahme ist, um die eigene Sicherheit im Internet zu erhöhen. Was der Index aber auch zeigt: Viele brauchen nach wie vor Unterstützung dabei, dieses Wissen im Alltag auch in die Praxis umzusetzen. Dass in diesem Jahr so viele Sicherheitsvorfälle registriert wurden wie noch nie, ist ein wichtiges Signal: Wir müssen dringend nachsteuern, um unsere digitale Gesellschaft besser zu schützen.

Mit den Ergebnissen des DsiN-Sicherheitsindex möchten wir allen Akteur:innen der digitalen Aufklärungsarbeit wichtige Grundlagen an die Hand geben, um aktuelle Trends und langjährige Entwicklungen im digitalen Raum besser zu verstehen. Die Stagnation der digitalen Sicherheitslage in Deutschland ist für uns ein Auftrag, mehr in Cybersicherheit und digitale Aufklärung zu investieren. Wer hierfür aus Sicht der Internetnutzenden die Verantwortung trägt, wird aus dem DsiN-Sicherheitsindex deutlich. 61 % wünschen sich mehr Aufklärung durch Anbieter, 59 % wünschen sich mehr Aufklärung im öffentlichen Diskurs. Ganze 65,7 % geben zu: Sie könnten ihre digitale Sicherheit erhöhen, indem sie ihr vorhandenes Sicherheitswissen in die Tat umsetzen.

Damit es gelingt, dass bei der digitalen Sicherheit aus abstraktem Wissen gelebte Praxis wird, braucht es das Zusammenspiel aus Zivilgesellschaft, Wirtschaft und Politik für digitale Aufklärungsarbeit nah am Menschen. Deutschland sicher im Netz e.V. steht dafür mit der breiten Expertise aus seinem Mitglieder- und Partner-Netzwerk zur Verfügung.

Im Namen von DsiN wünschen wir eine spannende Lektüre.

Isabelle Rosière
Geschäftsführerin, Deutschland sicher im Netz e.V.

Pierre Du Bois
DsiN-Vorstand und Head of Communications, Kleinanzeigen

Inhalt

Ziel und Methode – wie sicher ist Deutschland im Netz? 6
Toptrends 2025: Stagnation auf Rekordtief – Bedrohungslage steigt, Sicherheitsverhalten nimmt ab 8
Der DsiN Sicherheitsindex 2025 in Zahlen und Fakten 10

Kapitel 1
Sicherheitsindex 2025: 55,7 Punkte 12

55,7 Punkte: Keine Entwarnung bei der digitalen Sicherheit 14
Entwicklungen 2025 bei den vier DsiN-Sicherheitsfaktoren 16
Internetnutzung 2025 im Überblick 18

Kapitel 2
Digitale Sicherheit: Verbrauchertypen im Wandel 20

Einleitung 22
Außenstehende Nutzer:innen 24
Fatalistische Nutzer:innen 26
Gutgläubige Nutzer:innen 28
Antreibende Nutzer:innen 30
Bedachtsame Nutzer:innen 32

Kapitel 3
Digitale Lebenswelten 2025 34

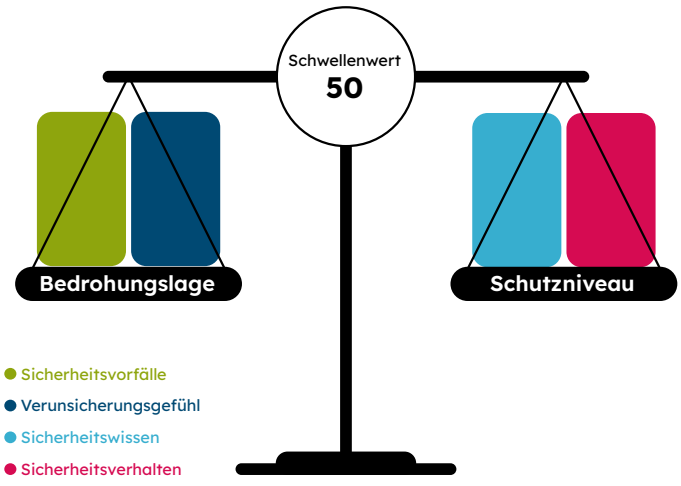
Wo und wie nutzen Menschen das Internet? 36
Vertrauen in der digitalen Welt 38
Kommunikation im Netz 40
Digitale Fitness- und Gesundheitsdienste 40
Das vernetzte Zuhause 41
Einkaufen im Internet 41
Onlinebanking 42
Digitale Identität 42

Kapitel 4
Fazit 44

Was uns der DsiN-Sicherheitsindex 2025 sagt 46
Vertrauen als digitale Zukunftsfrage 48
Sicher die digitale Gegenwart und Zukunft gestalten 50

Ziel und Methode – wie sicher ist Deutschland im Netz?

Abb. 1 / Sicherheitsindex 2025
Berechnung



DsiN-Sicherheitsindex 2025
Seit 2014 untersucht der DsiN-Sicherheitsindex die digitale Sicherheitslage von Verbraucher:innen im Netz: Wie sicher fühlen sie sich? Welche Art von Cyberangriffen erleben sie? Wie gut ist ihr digitales Sicherheitswissen? Und welche Sicherheitsmaßnahmen werden angewendet? Der DsiN-Sicherheitsindex beantwortet diese Fragen und bildet sie auf einer Skala von 0 bis 100 Punkten ab.

Die repräsentativen Ergebnisse der Studie geben Aufschluss über Trends, Entwicklungen und Bedarfe im Bereich der IT-Sicherheit. Dafür schlüsselt der DsiN-Sicherheitsindex seine Ergebnisse nach unterschiedlichen Nutzungsgruppen auf und gibt Einblicke in die Nutzungsgewohnheiten in relevanten digitalen Lebenswelten. Für die aktuelle Erhebung 2025 wurden 1.000 Internetnutzer:innen ab 16 Jahren in Deutschland über ihr Nutzungsverhalten in den vergangenen zwölf Monaten befragt. Die Befragung wurde vom Forschungsinstitut ARIX im Auftrag von Deutschland sicher im Netz e.V. durchgeführt.

2025 liegt ein besonderer Fokus auf dem Thema „Vertrauen in der digitalen Welt“. Der Fragenkatalog wurde entsprechend erweitert, um Zusammenhänge zwischen Sicherheitsverhalten, Risikowahrnehmung und Vertrauen in digitale Dienste, Technologien und Akteur:innen sichtbar zu machen.

Berechnung des DsiN-Sicherheitsindex
Um die Sicherheitslage der Internetnutzer:innen zu erfassen, stellt der DsiN-Sicherheitsindex die Bedrohungslage der Verbraucher:innen deren Schutzniveau gegenüber.

Die Bedrohungslage ergibt sich aus zwei Indikatoren:
- Tatsächlich erlebte Sicherheitsvorfälle
- Subjektives Gefährdungsempfinden
- Beide Faktoren wirken sich negativ auf den Indexwert aus.

Das Schutzniveau basiert ebenfalls auf zwei Faktoren:
- Sicherheitswissen: Kenntnis von Schutzmaßnahmen
- Sicherheitsverhalten: Anwendung dieser Maßnahmen im Alltag
- Beide Faktoren wirken sich positiv auf den Indexwert aus.
- Alle vier Faktoren werden auf einer Skala von 0 bis 100 gemessen. Der Gesamtindexwert wird durch das Verhältnis von Bedrohungslage und Schutzniveau ermittelt.
- Index › 50 Punkte: Das Schutzniveau überwiegt.
- Index ‹ 50 Punkte: Die Bedrohungslage überwiegt – die digitale Sicherheitslage kippt.

Fünf Verbrauchertypen – Orientierung für zielgerichtete Aufklärung
Die Studie unterscheidet auf Grundlage der Sicherheitslage fünf verschiedene Verbrauchertypen. Diesen werden die individuellen Nutzer:innen anhand ihres Nutzungsprofils und Sicherheitsverhaltens zugeordnet. Die unterschiedlichen Nutzungstypen bilden die Basis für eine differenzierte Aufklärungsarbeit und ermöglichen eine passgenaue Ansprache nach Sicherheitsbewusstsein, Verhalten und Risikowahrnehmung.

Digitale Lebenswelten im Fokus: Vertrauen in der digitalen Welt
Der Index befragt Nutzer:innen außerdem zu ihrem Verhalten und ihrer Einstellung gegenüber unterschiedlichen digitalen Lebensbereichen – von Online-Shopping, digitaler Kommunikation, Gesundheits- und Fitnessdiensten bis hin zu KI-Anwendungen im Alltag.

Das diesjährige Fokusthema beleuchtet die Rolle von Vertrauen im Kontext digitaler Sicherheit: Wem vertrauen Verbraucher:innen im Netz? Welche Rolle spielt Vertrauen bei digitalen Angeboten? Kapitel 3 beleuchtet zentrale Fragen und zeigt, wie Vertrauen in Technologien entsteht und gestärkt werden kann.

„Mir wird schon nichts passieren – das Internet funktioniert doch ganz gut.“
42,6 %
Gutgläubige Nutzer:innen
„Ich informiere mich, bevor ich handle – und schütze mich bewusst.“
18,0 %
Bedachtsame Nutzer:innen
26,9 %
Antreibende Nutzer:innen
„Ich will Neues entdecken – aber sicher.“
5,5 %
Außenstehende Nutzer:innen
„Versteh’ ich nicht – und kann es auch nicht.“
7,1 %
Fatalistische Nutzer:innen
„Man kann sowieso nichts tun – das Internet bleibt gefährlich.“

Toptrends 2025: Stagnation auf Rekordtief – Bedrohungslage steigt, Sicherheitsverhalten nimmt ab

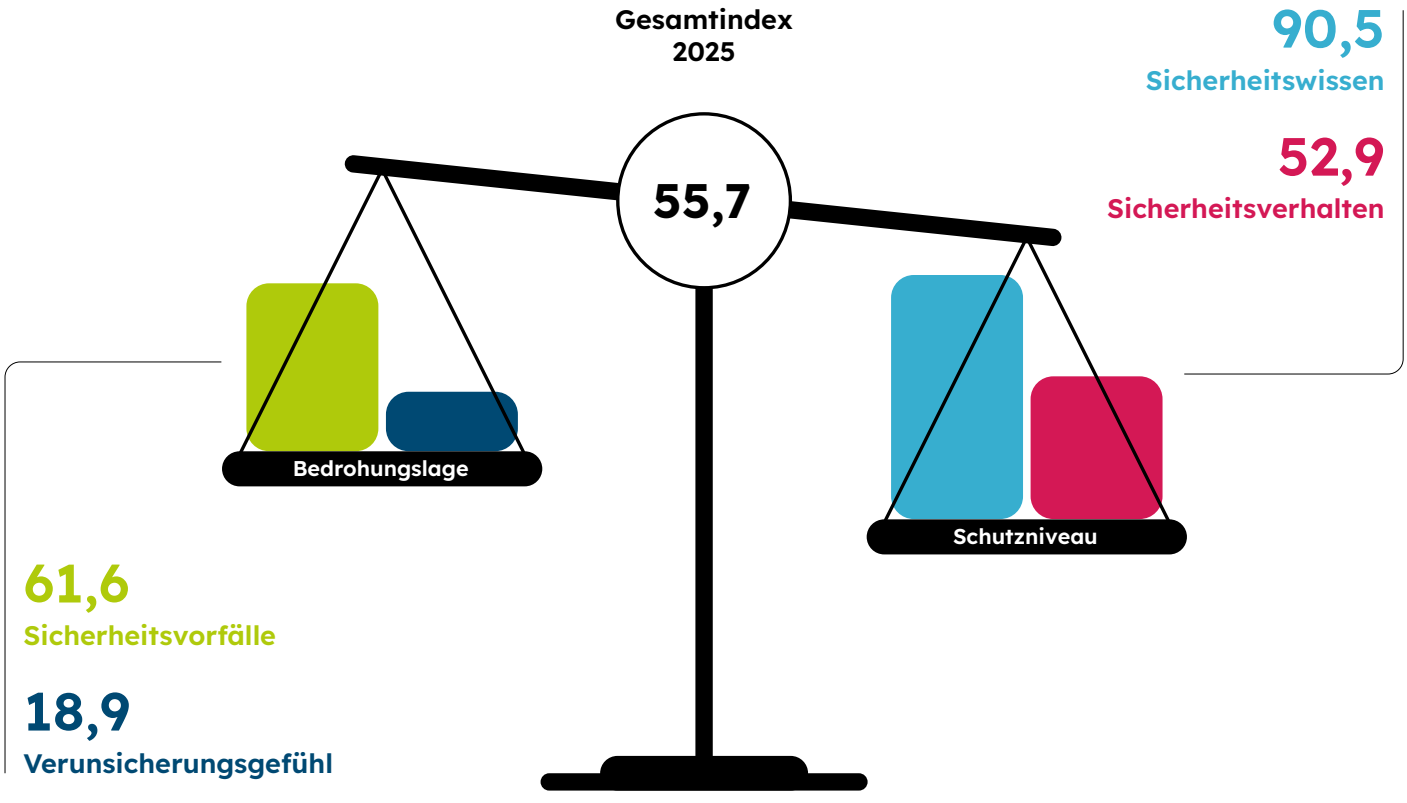
Auch im zwölften Jahr liefert der DsiN-Sicherheitsindex einen umfassenden Überblick über die digitale Sicherheitslage der Verbraucher:innen in Deutschland. Die Ergebnisse zeigen eine Stagnation auf niedrigem Niveau: Die Sicherheitsvorfälle sind im Vergleich zum Vorjahr leicht angestiegen, gleichzeitig ist das Sicherheitsverhalten weiter rückläufig und erreicht in diesem Jahr einen neuen Tiefststand. Während das digitale Sicherheitswissen bei den meisten Internetnutzenden weiterhin gute Werte erzielt, geht die Wissens-Verhaltensschere weiter auseinander. Der digitale Alltag wird für viele Nutzer:innen außerdem diverser: Immer mehr Geräte sind online, neue Technologien und Nutzungsformen nehmen weiter zu.

Rekord bei Sicherheitsvorfällen

2025 bleibt der DsiN-Sicherheitsindex mit 55,7 Punkten auf dem niedrigsten jemals gemessenen Niveau seit Beginn der Erhebungen im Jahr 2014. Seit 2020 hat der Indexwert als Indikator für die digitale Sicherheitslage von Internetnutzenden in Deutschland kontinuierlich abgenommen. Treiber dieser Entwicklung bleibt die anhaltend hohe Zahl von Sicherheitsvorfällen. Mit 61,6 Punkten erreicht dieser Wert ein neues Rekordniveau. Phishing-Angriffe über Messenger und SMS wurden 2025 von 33,5 % der Nutzer:innen gemeldet – ein Rückgang um 1,3 Prozentpunkte gegenüber dem Vorjahr. Dennoch verdrängen sie erstmals das klassische Phishing per E-Mail vom Spitzenplatz, das 2025

Abb. 2 / Sicherheitsindex 2025

Digitale Sicherheitslage der Verbraucher:innen in Deutschland in Punkten



deutlich stärker um 7,7 Prozentpunkte auf 31,6 % zurückgeht. An dritter Stelle bleibt wie im Vorjahr der Erhalt infizierter E-Mails, Anhänge oder Weblinks, der mit 27,8 % gemeldet wird – ein Minus von 4,1 Prozentpunkten.

Dennoch sinkt das subjektive Gefährdungsempfinden der Nutzer:innen auf nur noch 18,9 Punkte. Während es grundsätzlich zu begrüßen ist, dass Internetnutzende sich sicherer im Netz fühlen, darf dies nicht über reale Gefahren des digitalen Alltags hinwegtäuschen.

Wissens-Verhaltens-Lücke wächst

Das Sicherheitsverhalten der Verbraucher:innen ist 2025 erneut rückläufig, nachdem es 2024 auf einen bescheidenen Höchstwert von 53,6 Punkten geklettert war. Mit 52,9 Punkten ist der Wert um 0,7 Punkte zurückgefallen. Gleichzeitig bleibt das Sicherheitswissen mit 90,5Punkten nahezu konstant hoch. Die Wissens-Verhaltens-Lücke wächst damit aber auf 37,6 Punkte. Während einfache Schutzmaßnahmen wie starke Passwörter (77,8 %) und sichere WLAN-Einstellungen (76,7 %) weiterhin verbreitet sind, bleiben anspruchsvollere Maßnahmen wie Verschlüsselung (28,6 %) oder elektronische Signaturen (22,0 %) auf sehr niedrigem Niveau. Die Zahlen verdeutlichen: Wissen allein führt nicht zu sicherem Verhalten – der Transfer ins digitale Alltagsleben bleibt ein zentrales Defizit, um Menschen zu mehr digitaler Sicherheit zu befähigen.

Im Jahr 2025 verändert sich der digitale Alltag der Verbraucher:innen weiter:

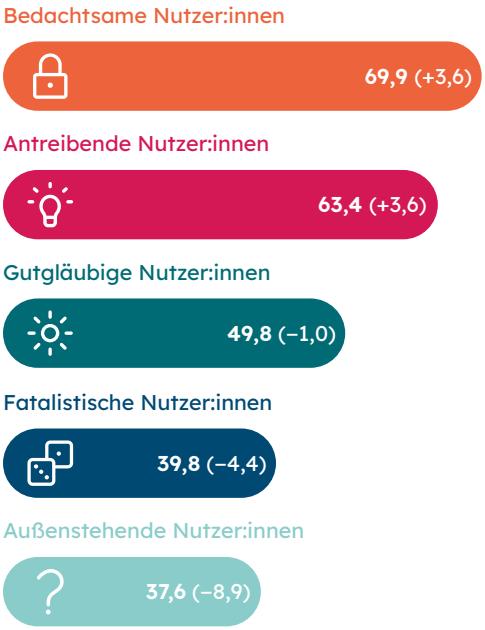
Die Nutzung verlagert sich zunehmend in mobile, vernetzte und alltagsnahe Kontexte. Sprachassistenten werden häufiger genutzt (20,4 %, +4,7), ebenso wie Geräte wie Smartwatches, die nun von 15,1 % (+8,7) regelmäßig verwendet werden. Kontaktloses Bezahlen wird von 23,6 % der Nutzer:innen verwendet – ein Rückgang um 6,6 Prozentpunkte gegenüber dem Vorjahr.

Demgegenüber ist die Nutzung klassischer Geräte rückläufig: Desktop-PCs (42,3 %), Tablets (40,8 %) und Smartphones (72,5 %) verzeichnen Rückgänge. Besonders stark betroffen sind stationäre vernetzte Geräte wie Smart-Home-Steuerungen, deren Nutzung von 22,8 % auf 5,1 % fällt. Diese Entwicklung zeigt einen klaren Trend hin zu mobilen, flexiblen Technologien, die sich in den Alltag integrieren lassen und hohe Akzeptanz erfahren.

Allerdings wird dieser digitale Wandel nicht von einer entsprechenden Veränderung des Sicherheitsverhaltens begleitet. Viele Nutzer:innen passen ihre Schutzmaßnahmen nicht an neue Geräte und Kontexte an. Die Folge ist eine wachsende Wissens-Verhaltens-Lücke: Digitale Risiken werden oft nicht erkannt oder unterschätzt, was neue Bedrohungen erzeugt.

Abb. 3 / Sicherheitsindex 2025

Indexwerte nach Verbrauchertypen (in Punkten)



Verbrauchertypen im Netz

Gutgläubige Nutzer:innen bilden mit 42 % der Internetnutzenden erneut die größte Gruppe. Ihr Indexwert sinkt in diesem Jahr erstmalig unter die kritische Marke von 50 Punkten. Während Sicherheitsvorfälle zunehmen (+4,2 Punkte), bleibt ihr Gefährdungsempfinden mit 13,8 Punkten niedrig.

Souveräne Nutzer:innen entwickeln sich positiv: Bedachtsame Nutzer:innen steigern ihren Indexwert um 3,6 Punkte auf 69,9, Antreibende erreichen 63,4 Punkte (+3,6). Allerdings zählen nur noch 44,9 % der Internetnutzenden zu diesen Gruppen, ein Rückgang von 4,3 %.

Fatalistische Nutzer:innen (39,8 Punkte, –4,4) und außenstehende Gruppen (37,6 Punkte, –8,9) verschlechtern sich deutlich. Damit ist die Hälfte der Internetnutzenden unzureichend geschützt, was langfristig ernsthafte Risiken für die Gesellschaft bedeutet.

Insgesamt trauen sich nur 55 % zu, digitale Risiken selbst zu beurteilen. 77 % wünschen sich mehr Unterstützung, Orientierung und Hilfe. 31,5 % sehen digitale Technologien eher als Risiko, nur 20,9 % verbinden sie mit Chancen.

Vertrauen, transparente Lösungen und zielgerichtete Aufklärung sind entscheidend, um digitales Verhalten zu stärken und eine stabile digitale Gesellschaft zu ermöglichen.

Der DsiN-Sicherheitsindex 2025 in Zahlen und Fakten

Trends 2025

Sicherheitsvorfälle erreichen neuen Höchstwert von

61,6 (+0,4)

Punkten

Gefährdungsempfinden auf historischem Tief von

18,9 (−3,0)

Punkten

Sicherheitswissen erneut bei Höchststand von

90,5 (+0,1)

Punkten

Phishing:
Messenger-Dienste

33,5 %

überholen E-Mail

31,6 %

als Angriffsziel

Wofür Menschen das Internet nutzen
Top 10 der Nutzungszwecke in Prozent

	2024	2025	
1. E-Mails	72,9 %	74,2 %	+1,3 %
2. Online-Shopping	71,1 %	74,9 %	−3,8 %
3. Bankgeschäfte	59,6 %	61,1 %	−1,5 %
4. Suchmaschinen / Online-Nachschlagewerke	57,2 %	63,8 %	−6,6 %
5. Messenger-Nutzung	57,0 %	59,3 %	−2,3 %
6. Nachrichtenseiten	56,7 %	60,1 %	−3,4 %
7. Soziale Netzwerke	53,8 %	60,7 %	−6,9 %
8. Video- und Streaming-Angebote	46,6 %	52,7 %	−6,1 %
9. Herunterladen von Updates	43,3 %	50,1 %	−6,8 %
10. Musik- und Podcast-Angebote	41,5 %	44,1 %	−2,6 %

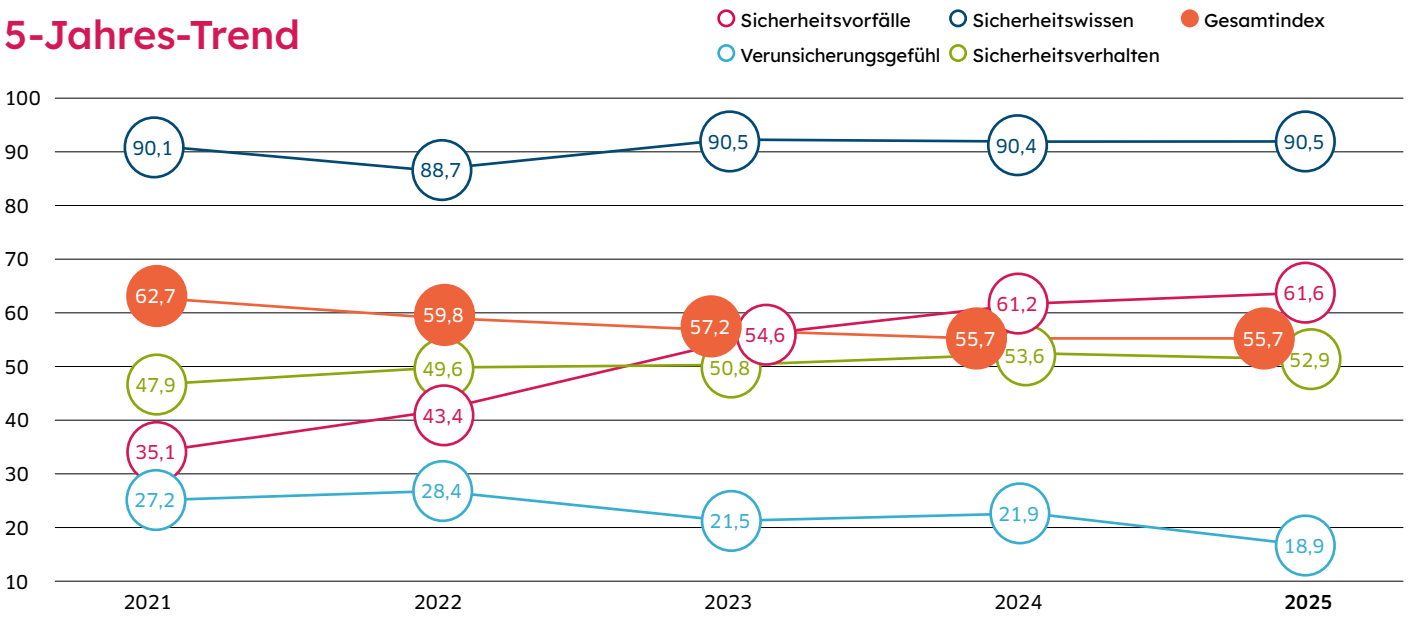
2024 2025

Wo sich Menschen über Sicherheit im Internet informieren
Top 10 der Informationsquellen in Prozent

	2024	2025	
1. Familie / Freunde / Bekannte / Kollegen	45,7 %	46,1 %	+0,4 %
2. Fernsehsendungen	30,0 %	30,9 %	+0,9 %
3. Nachrichtenseiten, Online-Fachzeitschriften & -Ratgeber	26,5 %	31,0 %	−4,5 %
4. Anbieter von Sicherheitsprodukten und -services	24,6 %	25,3 %	+0,7 %
5. Nachlesen in sozialen Netzwerken / Blogs / Foren	20,8 %	23,6 %	−2,8 %
6. Bücher / Zeitungen / Zeitschriften / Fachmagazine	18,6 %	20,1 %	+1,5 %
7. Angebote von allgemeinen Verbraucherorganisationen	18,5 %	19,2 %	+0,7 %
8. Nachfragen in sozialen Netzwerken / Blogs / Foren	13,1 %	13,7 %	−0,6 %
9. Angebote von Aufklärungs-Initiativen	12,6 %	12,9 %	−0,3 %
10. Behörden / Verwaltungen / öffentliche Einrichtungen	11,7 %	11,8 %	−0,1 %

2024 2025

5-Jahres-Trend



Digitale Lebenswelten

Kommunikation im Netz

E-Mail-Nutzung ist nach Abwärtstrend in diesem Jahr um 1,3 Prozentpunkte gestiegen und damit wieder beliebteste Aktivität im Netz. Die Messenger-Nutzung fällt um 2,3 Prozentpunkte.

Digitale Gesundheitsdienste

Das Sammeln und Analysieren personenbezogener Gesundheitsdaten in Datenbanken für Diagnose- und Therapiemaßnahmen wird von 55,5 % als risikoreich eingestuft (+3,9 Prozentpunkte im Vergleich zum Vorjahr).

Das vernetzte Zuhause

Lediglich 9 % der Befragten geben an, vernetzte Haustechnik zu nutzen – ein Rückgang um 5,1 Prozentpunkte. Vernetzte mobile Geräte legen stark zu, Sprachassistenten auf 20,4 %.

Einkaufen im Internet

Online-Shopping ist mit 71,1 % nur noch die zweitbeliebteste Onlineaktivität deutscher Internetnutzenden – ein Minus von 3,8 Prozentpunkten im Vergleich zu 2024.

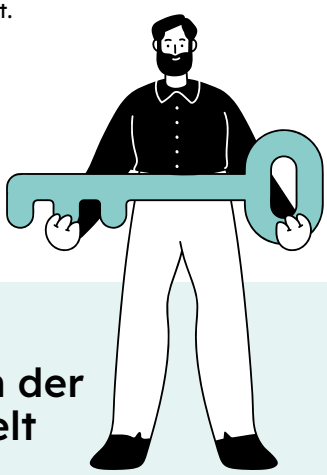
Onlinebanking

59,6 % der Internetnutzenden verwenden Onlinebanking. Nur noch 27,4 % halten Onlinebanking für gefährlich oder sehr gefährlich – ein Rückgang um 5,6 Prozentpunkte.

Digitales Ich

Nur 3,5 % schätzen die Kontrolle über ihr eigenes digitales Ich als sehr hoch ein. Onlineshopping (52,1 %) soziale Netzwerke (50,9 %) und Online-Banking (48,6 %) gelten als größte Risiken.

- Die **digitale Sicherheitslage** hat sich seit 2021 deutlich **verschlechtert.**
- Die **Bedrohungslage steigt** seit 2021 kontinuierlich an.
- Das **Sicherheitswissen** erreicht ein Plateau auf **hohem Niveau.**
- Das **Sicherheitsverhalten nimmt zu,** hält jedoch nicht Schritt.



Fokusthema:

Vertrauen in der digitalen Welt

86,8 %

sagen: Der Schutz persönlicher Daten ist mir wichtig oder sehr wichtig beim Thema Vertrauen in der digitalen Welt.

67,6 %

sagen: Fake News und Desinformation stellen ein großes oder sehr großes Problem in der digitalen Welt dar.

28,7 %

halten digitale Medienangebote grundsätzlich für nicht oder weniger vertrauenswürdig.

Kapitel 1

Sicherheitsindex 2025: 55,7 Punkte

55,7 Punkte: Keine Entwarnung bei der digitalen Sicherheit

Die Sicherheitslage von Verbraucher:innen in Deutschland verharrt 2025 auf einem historischen Tiefstand von 55,7 Punkten. Der Abwärtstrend seit 2020 hat sich damit zwar nicht fortgesetzt, doch von einer Entspannung kann keine Rede sein: Vielmehr zeigt sich eine besorgniserregende Stagnation auf niedrigem Niveau. Die digitale Gefährdungslage bleibt hoch, während gleichzeitig das Risikobewusstsein der Verbraucher:innen auf ein Rekordtief sinkt.

Der Haupttreiber dieser Entwicklung bleibt die hohe Zahl erlebter Sicherheitsvorfälle, die mit 61,6 Punkten einen neuen Höchststand erreicht. Gleichzeitig sinkt das Gefährdungsempfinden auf den niedrigsten Wert seit Beginn der Erhebung (18,9 Punkte). Während das Sicherheitswissen konstant auf hohem Niveau bleibt (90,5 Punkte), verschlechtert sich das Sicherheitsverhalten der Nutzer:innen leicht auf 52,9 Punkte – und unterstreicht damit erneut die wachsende Lücke zwischen Wissen und Verhalten.

Bedrohungslage weiter gestiegen

Die Bedrohungslage im Netz bleibt auch 2025 auf einem hohen Niveau. Die Zahl der registrierten Sicherheitsvorfälle steigt erneut – wenn auch mit einem geringeren Zuwachs von 0,4 Punkten – auf den bisherigen Höchststand von 61,6 Punkten. Im Klartext heißt das: In den vergangenen 12 Monaten haben Verbraucher:innen so viele Sicherheitsvorfälle erlebt wie noch nie seit Beginn der Erhebung. Besonders auffällig ist dabei die Verschiebung der Vorfälle: Phishing-Angriffe über Messenger und SMS sind 2025 mit 33,5 % erstmals der häufigste gemeldete Vorfall und lösen damit klassische Phishing-Versuche per E-Mail ab, deren Anteil deutlich auf 31,6 % zurückgeht. Am seltensten werden weiterhin Angriffe auf die Hausvernetzung gemeldet (5,9 %).

Trotz wachsender Gefährdung nimmt das subjektive Verunsicherungsgefühl der Nutzer:innen weiter ab. Mit einem Rückgang von 3 Indexpunkten sinkt es auf nur noch 18,9 Punkte. Die Nutzer:innen fühlen sich so sicher im Internet wie noch nie. Allerdings gewöhnen sie sich scheinbar zunehmend an Risiken im Netz, ohne sie adäquat einzuschätzen.

Schutzniveau weiterhin unzureichend

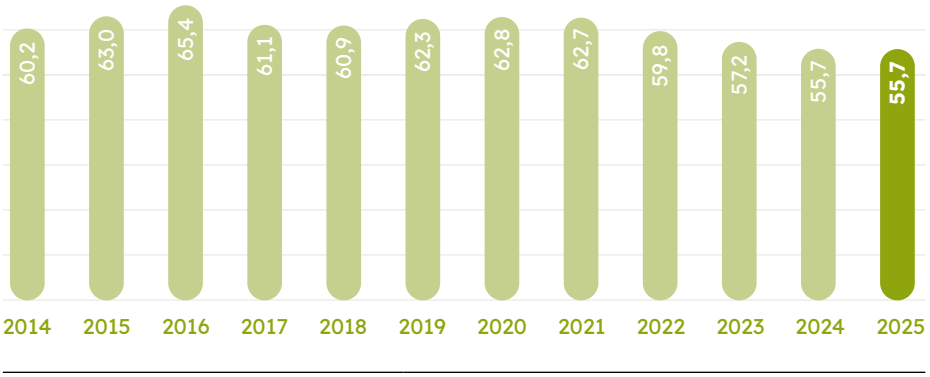
Das Schutzniveau der Verbraucher:innen zeigt 2025 eine bedenkliche Stagnation. Während das Sicherheitswissen der Onliner:innen mit 90,5 Punkten nahezu unverändert auf sehr hohem Niveau bleibt (+0,1 Punkte), verschlechtert sich das tatsächliche Sicherheitsverhalten leicht um 0,7 Punkte auf 52,9 Punkte. Damit wächst die Wissens-Verhaltens-Lücke in diesem Jahr weiter auf 37,6 Punkte an – ein neuer Höchstwert.

Die Ergebnisse zeigen: Auch wenn Nutzer:innen die wichtigsten Schutzmaßnahmen kennen, gelingt es vielen nicht, dieses Wissen konsequent in den Alltag zu übertragen. Die bekannteste Sicherheitsmaßnahme bleibt der Schutz des WLAN mit einem starken Passwort (98,5 %). Immerhin 76,7 % setzen das im Alltag um. Fast ein Viertel der Nutzer:innen ist damit aber in ungesicherten Netzwerken online.

Bei der Nutzung der Schutzmaßnahmen steht weiterhin das starke Passwort an erster Stelle (77,8 %), gefolgt von der oben genannten Sicherung des WLAN und regelmäßigen Updates von Apps (76,6 %). Am wenigsten verbreitet bleibt der Einsatz eigener elektronischer Signaturen (22,0 %).

Abb. 4 / Sicherheitsindex 2025

Digitale Sicherheitslage im Vergleich der letzten 12 Jahre in Punkten



Sicherheitswissen besser zugänglich machen

Das Interesse von Verbraucher:innen an besser zugänglichem und verständlichem IT-Sicherheitswissen ist weiterhin hoch. 67,7 % der Befragten wünschen sich eine zentrale Bündelung von Informationen zum sicheren Umgang mit Daten im Netz. Fast ebenso viele (65,2 %) fordern, dass solche Informationen einfacher und verständlicher gestaltet werden müssen.

Die Vermittlung von Risiken und Sicherheitskompetenzen bereits im schulischen Umfeld bleibt dabei die am häufigsten genannte Forderung: 71,7 % der Onliner:innen sprechen sich dafür aus, den Umgang mit Risiken im Netz frühzeitig im Unterricht zu verankern.

Auch die Rolle der Anbieter wird hervorgehoben: 61,0 % der Befragten erwarten von ihnen eine aktivere Aufklärung über Risiken und Bedrohungen. Dabei sehen 59,2 % der Internetnutzenden einen zusätzlichen Bedarf an mehr Informationen zu digitalen Gefahren – ein Zeichen dafür, dass die öffentliche Debatte über IT-Sicherheit weiterhin als nicht ausreichend wahrgenommen wird. Gleichzeitig zeigen die Zahlen, dass es nicht nur um eine bloße Wissensvermittlung geht, sondern dass es innovativer Angebote bedarf, die Sicherheitsverhalten im Alltag fördern.

Verantwortung für IT-Sicherheit gerecht verteilen

Auch 2025 sehen die Internetnutzer:innen sich selbst in der Verantwortung, wenn es um mehr Sicherheit im Netz geht. 77,8 % geben an, dass ein vorsichtigerer Umgang mit persönlichen Daten ein wirksamer Hebel zur Vermeidung von Sicherheitsvorfällen sei.

Gleichzeitig wächst der Anspruch an Anbieter und Gerätehersteller: 69,3 % der Befragten erwarten bessere Sicherheitsvorkehrungen durch die Anbieter von Diensten und Programmen, 68,5 % richten diese Forderung an die Hersteller der Geräte selbst. Die Erwartung an den Staat bleibt hoch – vor allem hinsichtlich einer konsequenteren Verfolgung von Verstößen gegen bestehende Gesetze (67,7 %).

Auffällig ist jedoch auch, dass 32,5 % der Nutzer:innen die Reduzierung der eigenen Internetnutzung als mögliche Maßnahme sehen, um Sicherheitsrisiken zu minimieren – ein Anstieg um 2,4 Prozentpunkte im Vergleich zum Vorjahr. Damit bleibt dieser Ansatz weiterhin am wenigsten favorisiert, zeigt jedoch einen Trend zur resignativen Haltung bei einem Teil der Nutzer:innen. Immerhin 27,5 % stimmen der Aussage zu „Solange mir nichts passiert, sehe ich keinen Grund, mein Sicherheitsverhalten zu ändern“. Hier muss dringend mehr getan werden, um Menschen für wirksame präventive Maßnahmen zu erreichen und zu sensibilisieren.

Entwicklungen 2025 bei den vier DsiN-Sicherheitsfaktoren

Bedrohungslage aus Sicht von Verbraucher:innen

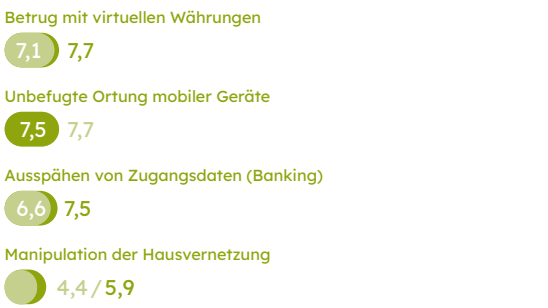
#1

Registrierte Sicherheitsvorfälle
2025 dominieren weiterhin Phishing-Angriffe als häufigster Sicherheitsvorfall. Besonders Phishing-Versuche per Messenger oder SMS bleiben mit 33,5 % der am häufigsten registrierte Vorfall – und verdrängen damit klassische Phishing-Versuche per E-Mail, die mit 31,6 % an zweiter Stelle liegen. An dritter Stelle folgen infizierte E-Mails, Anhänge und Weblinks (27,8 %). Insgesamt zeigt sich eine Verschiebung hin zu Angriffen über mobile Endgeräte und Messaging-Dienste.

Abb. 5 / Sicherheitsindex 2025
Sicherheitsvorfälle (in Prozent) ● 2024 ● 2025

Die häufigsten IT-Sicherheitsvorfälle

Die Schlusslichter unter den IT-Sicherheitsvorfällen

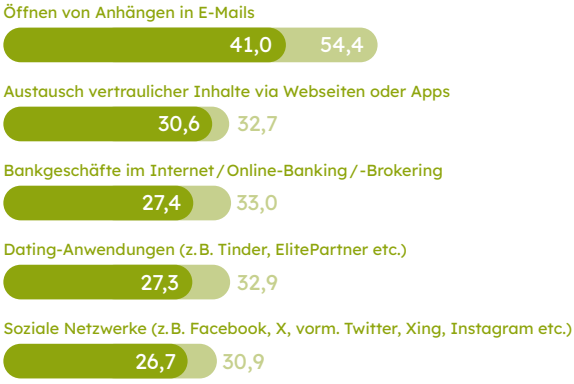


#2

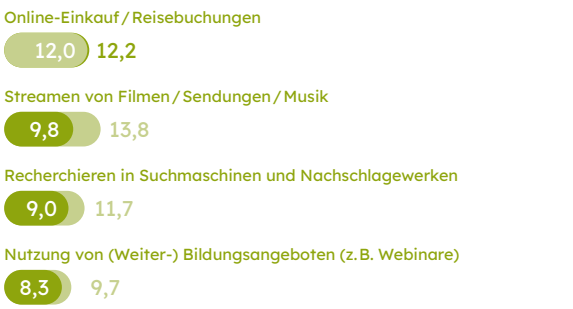
Verunsicherungsgefühl im Internet
Trotz steigender Sicherheitsvorfälle sinkt 2025 das Verunsicherungsgefühl der Verbraucher:innen weiter und erreicht mit 18,9 Punkten einen historischen Tiefstwert. Am meisten Unsicherheit empfinden Nutzer:innen weiterhin beim Öffnen von E-Mail-Anhängen (41,0 %), gefolgt vom Austausch vertraulicher Inhalte über Websites oder Apps (30,6 %) und Bankgeschäften im Internet (27,4 %). Am wenigsten Verunsicherung gibt es beim Online-Einkauf (12,2 %), bei Streaming-Diensten (9,8 %) Suchmaschinen (9,0 %) und (Weiter-)Bildungsangeboten (8,3 %).

Abb. 6 / Sicherheitsindex 2025
Verunsicherungsgefühl (in Prozent) ● 2024 ● 2025

Dabei fühlen sich Nutzer:innen am unsichersten



Dabei fühlen sich Nutzer:innen am wenigsten unsicher



Schutzniveau aus Sicht von Verbraucher:innen

#3

Sicherheitswissen der Verbraucher:innen
Das Sicherheitswissen der Onliner:innen bleibt 2025 auf konstant hohem Niveau. Mit einem Indexwert von 90,5 Punkten (+0,1 Punkte) bewegt sich der Wert nahezu auf dem Vorjahresniveau. Bekannteste Maßnahmen sind der Schutz des WLAN durch ein starkes Passwort (98,5 %), der Schutz mobiler Geräte mittels PIN (98,4 %), die regelmäßige Installation von Updates bei Programmen (98,3 %) sowie die Nutzung von Anti-Viren-Software (98,3 %). Die Verwendung starker Passwörter (98,2 %) und das Update des Betriebssystems (98,1 %) komplettieren die Liste der am häufigsten bekannten Schutzmaßnahmen.

#4

Sicherheitsverhalten im Alltag
Das Sicherheitsverhalten ist leicht rückläufig (–0,7 Punkte) Spitzenreiter bleibt weiterhin das starke Passwort (77,8 %), gefolgt von der Sicherung des WLAN (76,7 %) und regelmäßigen Updates von Apps (76,6 %). Am seltensten eingesetzt werden weiterhin eigene elektronische Signaturen (22,0 %), die Verschlüsselung der Festplatte (28,6 %), die Überprüfung fremder elektronischer Signaturen (29,2 %) sowie das Auslesen von E-Mail-Headern (29,7 %).

Abb. 7 / Sicherheitsindex 2025
Sicherheitswissen (in Prozent) — 2024 — 2025

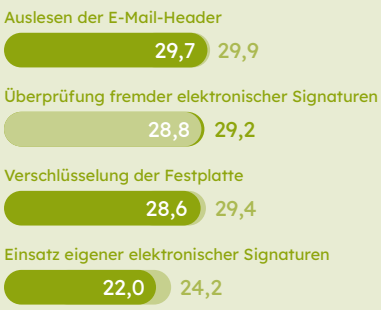
Die bekanntesten Sicherheitsmaßnahmen

Die unbekanntesten Sicherheitsmaßnahmen

Abb. 8 / Sicherheitsindex 2025
Sicherheitsverhalten (in Prozent) — 2024 — 2025

Die meistgenutzten Sicherheitsmaßnahmen

Die am wenigsten genutzten Sicherheitsmaßnahmen



Internetnutzung 2025 im Überblick

Mit welchen Geräten Nutzer:innen im Internet sind, differenziert sich 2025 weiter aus: Immer noch auf Platz zwei mit 60,8 % ist der Laptop oder das Notebook. Doch ein Abwärtstrend in der Nutzung setzt sich weiter fort. Spitzenreiter bei den Onliner:innen bleibt das Smartphone, das von 72,5 % verwendet wird, um ins Internet zu gelangen. In diesem Jahr ist jedoch erstmalig ein Abwärtstrend in der Nutzung zu verzeichnen. Auch Tablets werden weniger genutzt als noch im Vorjahr.

Während die Nutzung von Desktop-PCs weiter abnimmt (nur noch 42,3 % Nutzung statt 61,8 % im Jahr 2015), sind andere Geräte weiter auf dem Vormarsch: Der vernetzte Fernseher legt im Vergleich zum Vorjahr um 0,7 Prozentpunkte auf 52,2 zu, Sprachassistenten verbessern sich von 17 % auf 20,4 % in der Nutzungsverbreitung. Den größten Sprung machen sonstige vernetzte Geräte: Während 2024 nur 6,4 % entsprechende Smartwatches, Smart Cars und ähnliche Geräte verwendeten, ist dieser Wert 2025 auf 15,1 % angestiegen.

Die Nutzung von stationären Smart-Home-Geräten ist hingegen deutlich zurückgegangen: auf 5,1 Prozent.

Diese Entwicklungen zeigen: Die digitale Nutzung wird vielfältiger, der Fokus verlagert sich zunehmend auf spezialisierte, mobile und sprachgesteuerte Geräte. Gleichzeitig verlagern sich damit auch die potenziellen Sicherheitsrisiken – insbesondere im Umgang mit persönlichen Daten und in der Absicherung neuer Gerätetypen bleiben große Defizite bestehen, wie die weiterhin bestehende Lücke zwischen Wissen und Verhalten zeigt.

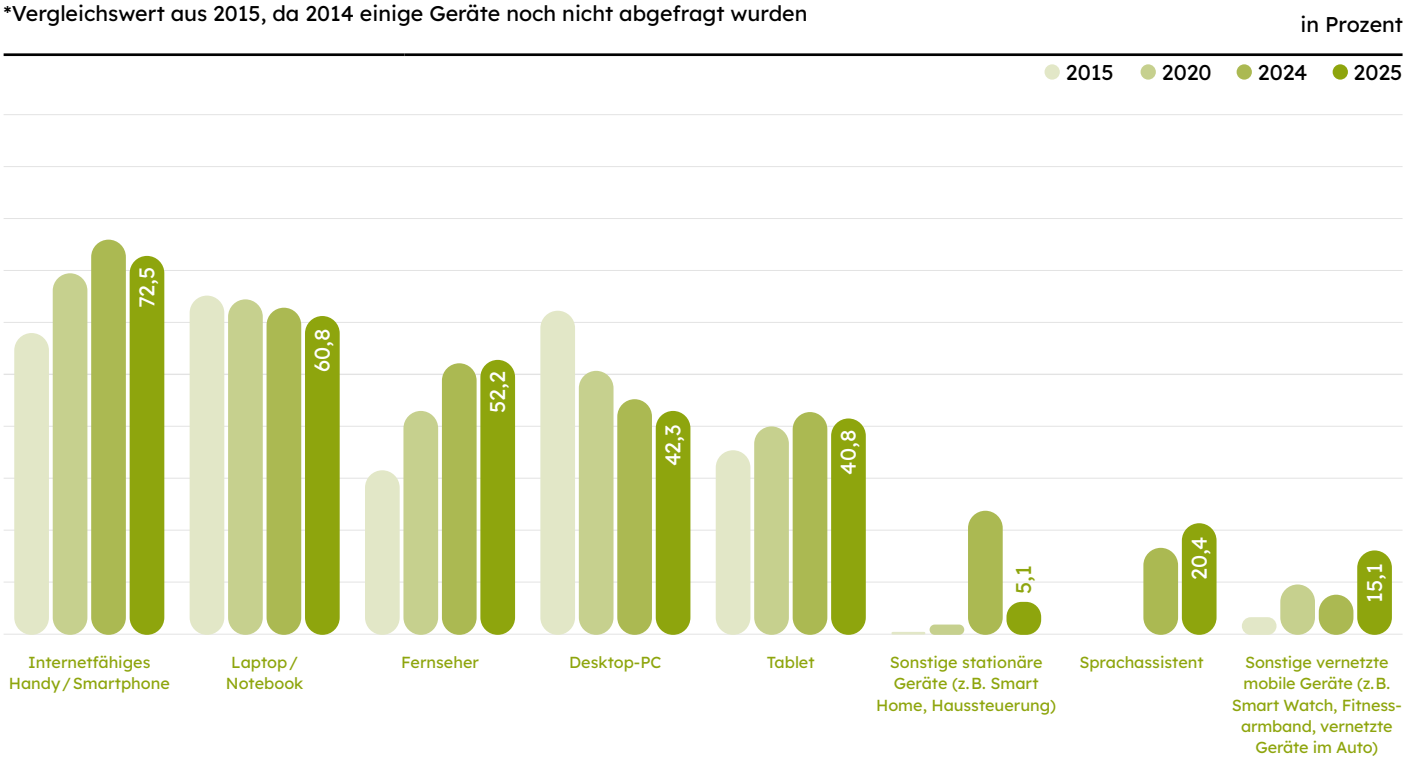
Nutzungsszenarien: mehr Komfort, unterschätzte Risiken

2025 ist das Senden und Empfangen von E-Mails mit 74,2 % die mit Abstand am häufigsten genutzte Onlineaktivität. Online-Shopping landet mit 71,1 % auf Platz 2. Gleichzeitig bleibt Betrug bei Online-Einkäufen und Buchungen ein häufig gemeldeter Sicherheitsvorfall: Mit einer

Abb. 9 / Sicherheitsindex 2025

Genutzte Geräte im Verlauf der Erhebung (2015*/2020/2024/2025)

*Vergleichswert aus 2015, da 2014 einige Geräte noch nicht abgefragt wurden



Betroffenheitsrate von 15,5 % liegt diese Gefahr weiterhin unter den Top 5 der IT-Sicherheitsvorfälle – Tendenz steigend. Dennoch zeigt der DsiN-Index, dass gerade in diesem Umfeld viele Verbraucher:innen die Risiken häufig unterschätzen, was sich an der weiterhin großen Wissens-Verhaltens-Lücke bei Schutzmaßnahmen wie sicheren Zahlungsarten oder der Überprüfung von Anbieter-Seriosität zeigt. Auch der digitale Zahlungsverkehr bleibt relevant, doch die Nutzung kontaktloser Bezahlmöglichkeiten über mobile Geräte ist rückläufig: 23,6 % der Verbraucher:innen greifen 2025 darauf zurück – ein Minus von 6,3 Prozentpunkten im Vergleich zu 2024. Diese Entwicklung birgt neue Sicherheitsanforderungen, etwa im Bereich mobiler Geräteabsicherung, App-Berechtigungen oder Schutz vor Phishing und Betrug über Payment-Apps.

Die hohe Sensibilität personenbezogener Daten in diesem Nutzungskontext – etwa Zahlungsdaten, Ausweisdokumente oder Gesundheitsnachweise – steht dabei im Widerspruch zum vergleichsweise niedrigen Sicherheitsbewusstsein der Nutzer:innen. Auch hier zeigt sich, dass bestehendes Wissen oft nicht konsequent umgesetzt wird. So nutzen beispielsweise nur 75,3 % der Befragten sichere Zahlungssysteme, obwohl 98,0 % deren Bedeutung kennen.

Unterschiede zwischen den Nutzergruppen

Die unterschiedlichen Nutzungstypen innerhalb der digitalen Gesellschaft zeigen auch 2025 deutliche Unterschiede in der Nutzung von Geräten und digitalen Diensten. Bedachtsame und Antreibende bleiben die Gruppen mit der höchsten Gerätevielfalt – sie nutzen im Alltag sowohl mobile als auch stationäre Geräte in Kombination, zeigen dabei jedoch ein deutlich höheres Sicherheitsbewusstsein.

Außenstehende und Gutgläubige hingegen bleiben stark auf das Smartphone fokussiert, oft ohne flankierende Schutzmaßnahmen. Gerade in diesen Gruppen werden neue Risiken durch Smart Home oder mobiles Bezahlen oft nicht als solche erkannt oder adressiert.

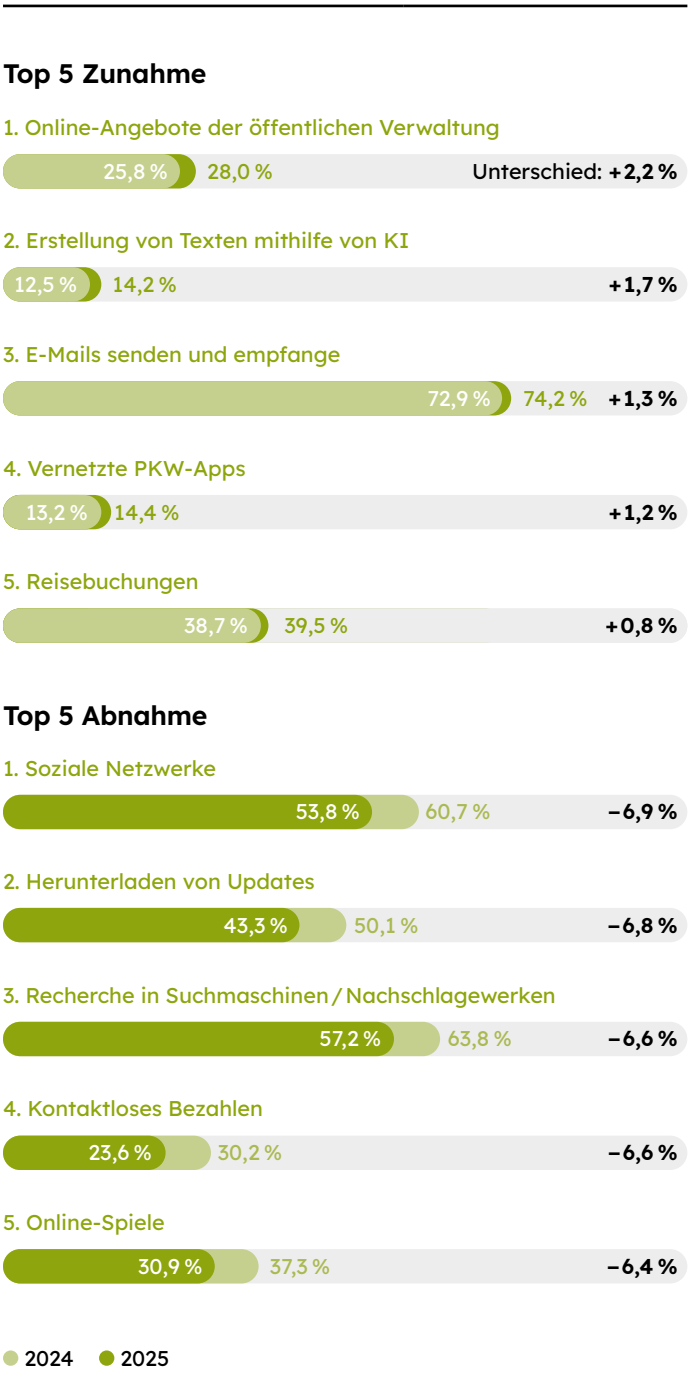
Stagnation auf hohem Gefährdungsniveau – Sicherheitslücke bleibt gravierend

Der DsiN-Sicherheitsindex 2025 verdeutlicht, dass dringend mehr getan werden muss, um der Stagnation der digitalen Sicherheitslage in Deutschland entgegenzusteuern. Nutzer:innen sind mit neuen Geräten und digitalen Entwicklungen konfrontiert. Zeitgleich bleibt trotz insgesamt guten IT-Sicherheitswissens in der Bevölkerung die Schere zum tatsächlichen Schutzverhalten im Alltag groß.

Neue Nutzungstrends wie der starke Anstieg vernetzter Geräte oder kontaktloses Bezahlen erweitern die Angriffsflächen für potenzielle Angriffe – ohne dass das Sicherheitsbewusstsein der Nutzer:innen Schritt hält. Um die digitale Sicherheitslage nachhaltig zu verbessern, braucht es verstärkt alltagsnahe Angebote zur Kompetenzförderung sowie eine konsequente Verankerung von Sicherheitswissen und -verhalten in Alltag und Beruf. Daher wollen wir in den kommenden Kapiteln genauer auf die unterschiedlichen Nutzungstypen und ihre Bedarfe blicken, und im Anschluss die digitalen Lebenswelten, in denen sie sich bewegen, genauer unter die Lupe nehmen.

Abb. 10 / Sicherheitsindex 2025

Veränderungen bei den Nutzungsaktivitäten: Top 5 Abnahme und Zunahme



Kapitel 2

Digitale Sicherheit: Verbrauchertypen im Wandel

Einleitung

Fast alle Menschen nutzen das Internet – aber auf ganz unterschiedliche Weise: manche vor allem, um mit anderen in Kontakt zu bleiben, etwa über Messenger oder soziale Netzwerke. Andere shoppen online, organisieren ihre Finanzen oder streamen Filme und Musik. Wieder andere steuern smarte Geräte in ihrem Zuhause oder erkunden neue digitale Services.

Abb. 11 / Sicherheitsindex 2025

Digitales Sicherheitsgefälle der Verbrauchertypen in Punkten

Indexwerte für die einzelnen Nutzertypen

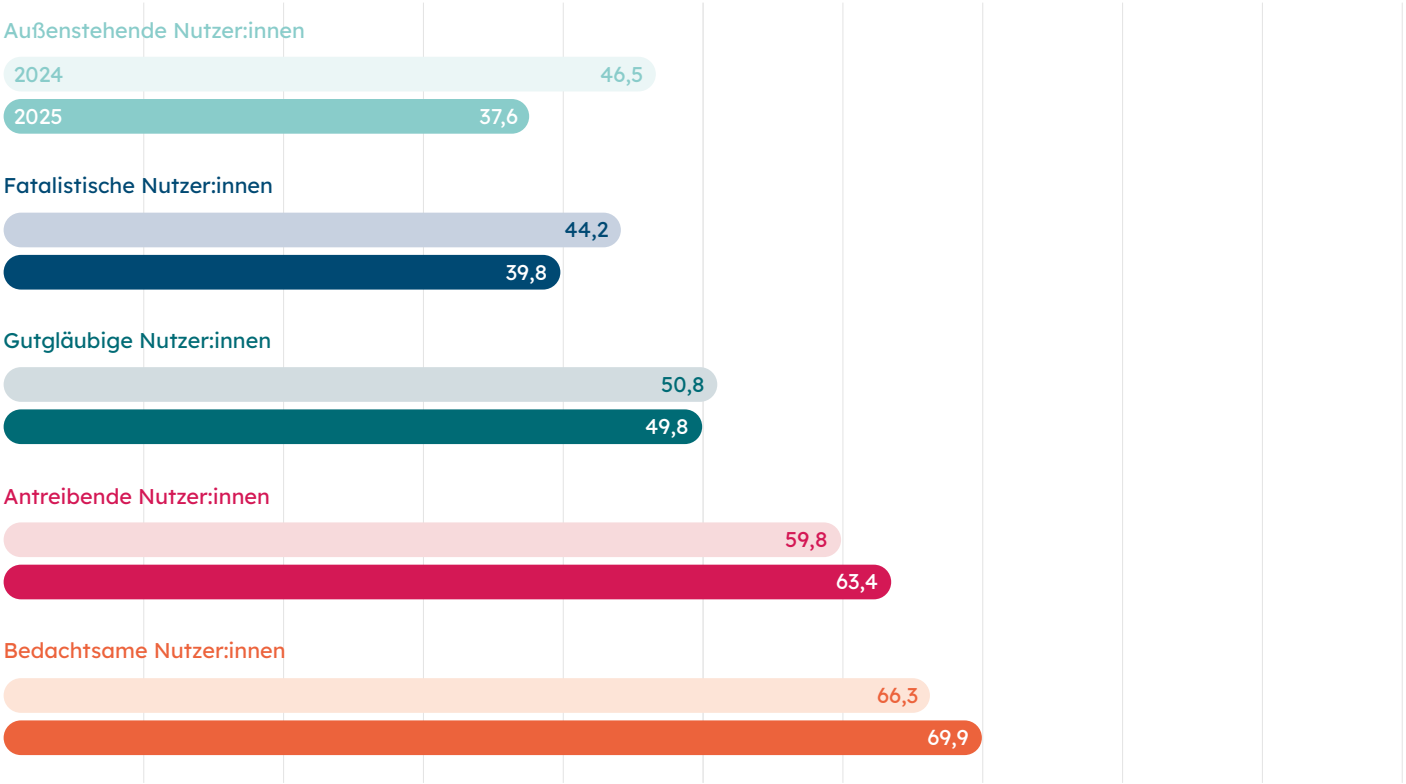
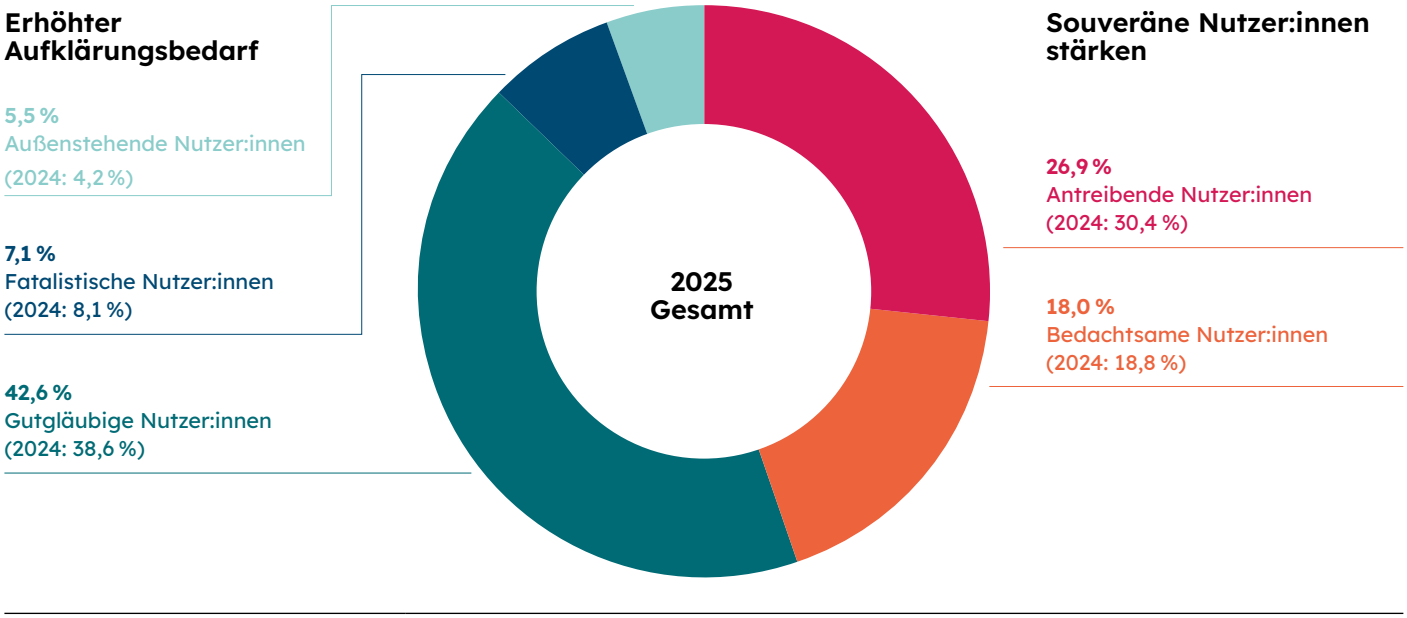


Abb. 12 / Sicherheitsindex 2025

Anteil der Verbrauchertypen an der Gesamtheit der Internetnutzer:innen



Diese vielfältigen Nutzungsmuster spiegeln sich auch im Umgang mit digitalen Risiken wider. Denn wer das Internet anders nutzt, begegnet auch anderen Bedrohungen – und geht unterschiedlich damit um. Genau hier setzt der DsiN-Sicherheitsindex 2025 an: Er unterscheidet fünf verschiedene Verbrauchertypen, die sich durch ihr Sicherheitswissen, ihr Verhalten und ihr Vertrauen im Netz voneinander abheben.

Die Typologie gibt Einblick in eine digitale Gesellschaft im Wandel – und zeigt, wie unterschiedlich Menschen heute auf Gefahren im Netz reagieren. Sie macht deutlich: Digitale Sicherheit ist keine Einheitslösung, sondern muss sich an den jeweiligen Bedürfnissen und Erfahrungen der Nutzer:innen orientieren.

2025 setzt sich fort, was sich in den vergangenen Jahren zunehmend abgezeichnet hat: Die digitale Gesellschaft driftet weiter auseinander. Nicht alle Nutzer:innen können auf dieselben Sicherheitskompetenzen und Schutzvorkehrungen zurückgreifen. Während sich die digitale Sicherheitslage für digitalaffine Gruppen – wie die bedachtsamen und antreibenden Nutzer:innen – ihre Sicherheitslage weiter verbessern, verschlechtert sich die Situation bei den meisten Alltagsuser:innen: Gutgläubige, Außenstehende und Fatalistische machen 55,2 % des Gesamtanteils der Internetnutzenden aus. Bei Ihnen liegt der Indexwert inzwischen unter der kritischen Schwelle von 50 Punkten: Die individuelle Bedrohungslage überwiegt das persönliche Schutzniveau. Erstmals wirft der DsiN-Sicherheitsindex 2025 auch einen gezielten Blick auf das Vertrauensverhalten der Nutzer:innen. Für alle fünf Nutzungstypen wurde ein eigenes Vertrauens-profil erstellt, das zeigt, wem sie im digitalen Raum vertrauen – und wie dieses Vertrauen ihr Sicherheitsverhalten beeinflusst. Damit wird deutlich: Vertrauen ist kein einheitlicher Wert, sondern individuell geprägt und eng verknüpft mit digitalem Wissen und Alltagserfahrungen. Die neue Perspektive erlaubt es, digitale Aufklärung noch gezielter an den Bedürfnissen und Haltungen der einzelnen Gruppen auszurichten.

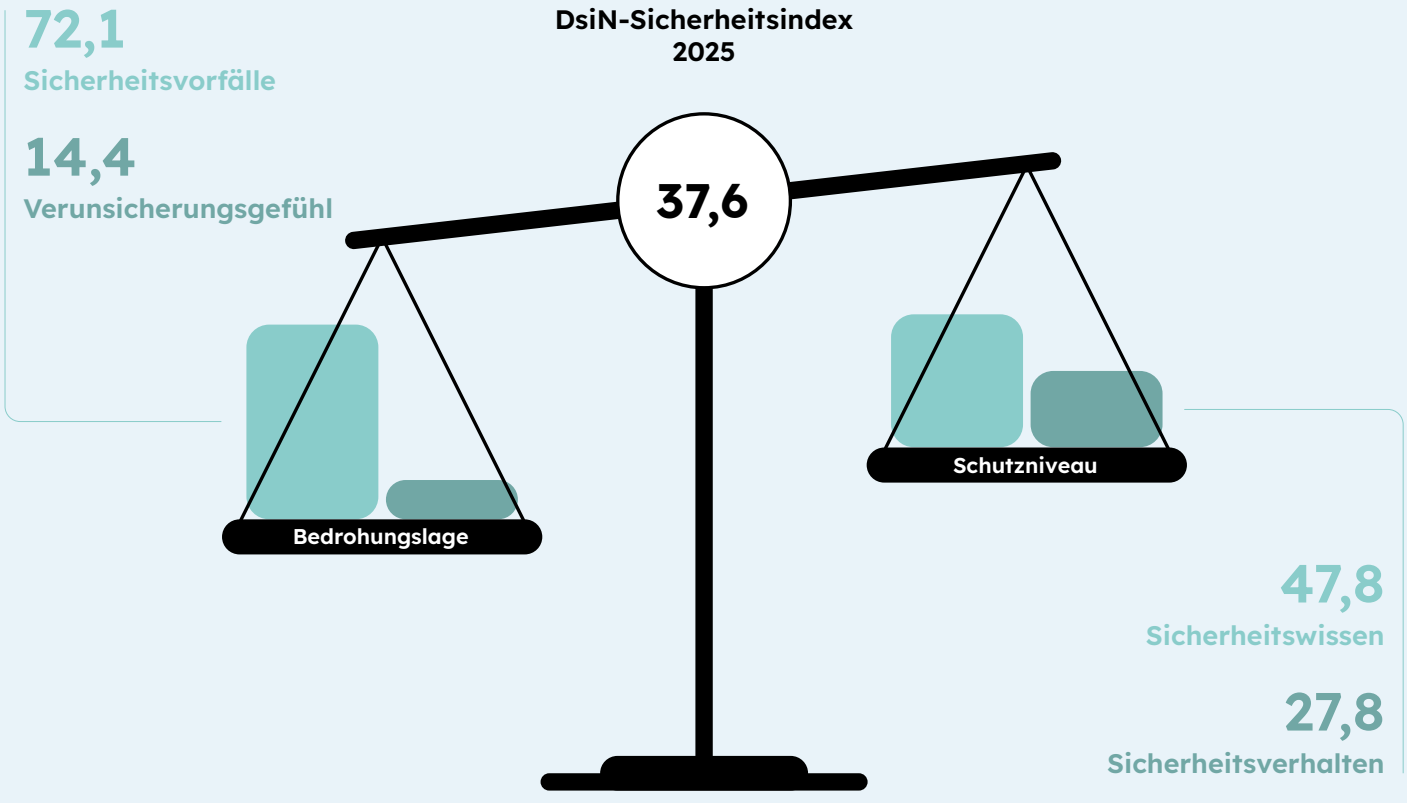
Doch wie sehen diese unterschiedlichen Nutzungstypen im Netz aus? Die folgenden Typenporträts zeigen, wie unterschiedlich Verbraucher:innen auf Bedrohungen reagieren – und wie Vertrauen als Schlüssel zur digitalen Resilienz gestärkt werden kann.

Außenstehende Nutzer:innen

„Versteh' ich nicht – und kann es auch nicht."

Abb. 13 / Sicherheitsindex 2025

DsiN-Indexwert für außenstehende Nutzer:innen in Punkten



Soziodemografie & Nutzungsmuster
Außenstehende Nutzer:innen bilden mit 5,5 % die kleinste, zugleich aber am stärksten gefährdete Gruppe unter den Verbraucher:innen im Netz. Sie sind mehrheitlich älter als 50 Jahre, jede:r Fünfte sogar über 70. Frauen sind mit 53,7 % leicht überrepräsentiert. Die private Internetnutzung bleibt eher gering: 53,2 % der Außenstehenden sind zwischen 10 und 30 Stunden pro Woche online, meist über Handys. Neue digitale Angebote werden kaum ausprobiert – nur 6,3 % geben an, daran interessiert zu sein. Stattdessen berichtet die Hälfte (50,3 %), sich von technischen Entwicklungen schnell überfordert zu fühlen.

Digitale Sicherheitslage
Mit einem Indexwert von 37,6 Indexpunkten verlieren die Außenstehenden gegenüber dem Vorjahr dramatisch – −8,9 Indexpunkte markieren den stärksten Rückgang aller Gruppen. Damit liegt ihr Wert weit unter der kritischen 50-Punkte-Marke und macht sie zur am stärksten gefährdeten Gruppe von Nutzer:innen im Netz.

Besonders auffällig ist der starke Anstieg bei erlebten Sicherheitsvorfällen: Der entsprechende Teilindex springt um 31,8 Bedrohungspunkte nach oben – ein beispielloser Anstieg. Trotz dieser realen Bedrohung sinkt ihr subjektives Verunsicherungsgefühl paradoxerweise um 7,1 auf nur noch 14,4 Bedrohungspunkte. Diese Diskrepanz deutet auf eine wachsende Abstumpfung gegenüber Risiken hin – oder auf ein fehlendes Verständnis dafür, wann ein Vorfall sicherheitsrelevant ist.

Beim Sicherheitswissen verzeichnen Außenstehende zwar den höchsten Zuwachs aller Gruppen (+8,3 Schutzpunkte), erreichen mit 47,5 Schutzpunkten aber weiterhin den niedrigsten Wert im Vergleich. Das Sicherheitsverhalten verbessert sich zwar ebenfalls leicht auf 27,8 Schutzpunkte (+2,8), bleibt aber weit unter dem Durchschnitt aller Gruppen.

Vertrauensprofil
Außenstehende Nutzer:innen vertrauen stark auf externe Akteur:innen, also Anbieter, Gerätehersteller oder das persönliche Umfeld. Eigenverantwortung spielt im Sicherheitsverständnis eine untergeordnete Rolle. Die Vorstellung, man selbst könne digitale Risiken aktiv vermeiden, ist in dieser Gruppe kaum verbreitet. Stattdessen dominiert der Wunsch nach sicher voreingestellten Systemen („safety by default“) und verständlicher Begleitung im Alltag.

Ein wachsendes Bedürfnis nach Aufklärung ist dennoch erkennbar: 79 % der Außenstehenden wünschen sich mehr Informationen über Online-Risiken in ihrer unmittelbaren Umgebung – ein Zuwachs von über 19 Prozentpunkten im Vergleich zum Vorjahr. Auch der Wunsch nach persönlicher Unterstützung durch Vertrauenspersonen, etwa in Familie oder Nachbarschaft, ist besonders hoch.

Fazit & Bedarfe
Außenstehende Nutzer:innen sind 2025 so stark von digitalen Risiken betroffen wie nie zuvor – und gleichzeitig so wenig sensibilisiert wie kaum eine andere Gruppe. Dieses Missverhältnis macht sie besonders verwundbar. Klassische Appelle an Selbstverantwortung greifen hier zu kurz. Stattdessen braucht es:

- niedrigschwellige, persönliche Aufklärung
- sichere Grundeinstellungen bei Software und Geräten
- verlässliche Ansprechpartner:innen im analogen Raum

Gerade in einer zunehmend digitalisierten Gesellschaft muss diese kleine, aber gefährdete Gruppe stärker in den Fokus rücken – denn digitale Teilhabe darf nicht vom Kompetenzgrad abhängen.

Abb. 14 / Sicherheitsindex 2025
Top 3 Sicherheitsvorfälle

32,0 %
Phishing-Versuch per SMS oder Messenger

23,3 %
Phishing-Versuch per Mail

19,5 %
Betrug oder Fehlinformation durch manipulierte oder gefälschte Bilder im Netz

Abb. 15 / Sicherheitsindex 2025
TOP 3 Verunsicherungsgefühl (Gefährdungspotential)

30,4 %
Austausch vertraulicher Inhalte via Webseiten oder Apps (z. B. mit Behörden, Banken, Versicherungen)

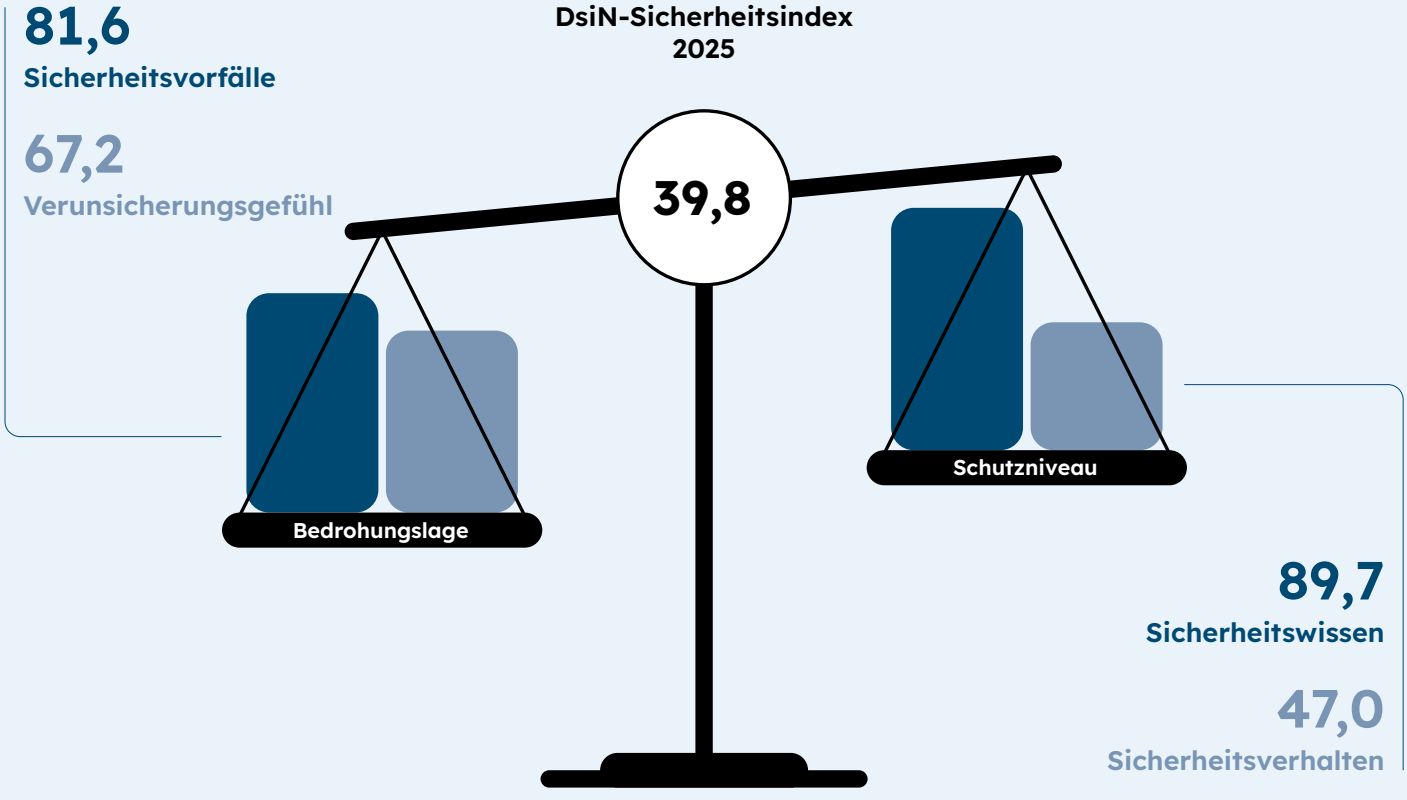
27,7 %
Bankgeschäfte im Internet / Online-Banking / -Brokering

26,0 %
Dating-Anwendungen (z. B. Tinder, ElitePartner etc.)

Fatalistische Nutzer:innen

Abb. 16 / Sicherheitsindex 2025

DsiN-Indexwert für fatalistische Nutzer:innen in Punkten



Soziodemografie & Nutzungsmuster
Die Gruppe der fatalistischen Nutzer:innen umfasst 7,1 % der Internetbevölkerung – leicht rückläufig gegenüber dem Vorjahr (–1,0 %). Männer und Frauen sind nahezu gleich verteilt. Auffällig ist die Altersstruktur: 35,4 % dieser Gruppe sind älter als 60 Jahre. Sie nutzen das Internet zwar regelmäßig, aber zurückhaltend Informationsbeschaffung, E-Mails und einfache Onlinekäufe stehen im Vordergrund. Für sicherheitsrelevante Anwendungen wie Onlinebanking oder Cloud-Dienste besteht dagegen eine hohe Skepsis.

Digitale Sicherheitslage
Der Indexwert der Fatalist:innen sinkt 2025 auf 39,8 Indexpunkte – ein Rückgang um 4,4 Indexpunkte im Vergleich zum Vorjahr. Damit liegt die Gruppe weiterhin deutlich unter der kritischen 50-Punkte-Schwelle und zählt zu den am stärksten gefährdetenGruppen von Nutzer:innen.

Besonders kritisch bleibt die Bedrohungslage: Die Zahl registrierter Sicherheitsvorfälle steigt um 12,5 Bedrohungspunkte auf 81,6 – der höchste Wert aller Gruppen. Gleichzeitig bleibt das Verunsicherungsgefühl mit 67,2 Bedrohungspunkten extrem hoch. Anders als bei den Außenstehenden erleben Fatalist:innen die Bedrohung nicht nur real, sondern auch emotional intensiv – was zu Rückzug und Vermeidung führt.

Beim Sicherheitswissen legen sie leicht zu (+2,1 auf 89,7 Schutzpunkte) – ein hoher Wert im Vergleich –, jedoch sinkt das Sicherheitsverhalten leicht auf 47,0 Schutzpunkte (–0,3). Die Schere zwischen Wissen und Handeln bleibt damit weit geöffnet. Viele wissen zwar, wie sie sich schützen könnten, glauben aber nicht daran, dass dies im Alltag wirksam ist.

Vertrauensprofil
Fatalist:innen zeigen ein ausgeprägt niedriges Vertrauen in ihre eigene digitale Handlungsfähigkeit. Gleichzeitig setzen sie Hoffnung in externe Schutzmechanismen – etwa strengere Gesetze, technische Voreinstellungen oder bessere Überwachung durch den Staat. 83 % wünschen sich eine konsequentere Durchsetzung bestehender Regeln im Netz, 70 % befürworten eine stärkere Kontrolle digitaler Dienste.

Eigenverantwortliches Handeln tritt in den Hintergrund – nicht aus Ignoranz, sondern aus Resignation. Diese Haltung begünstigt Vermeidungsverhalten: Überdurchschnittlich viele Fatalist:innen reduzieren ihre Onlineaktivitäten oder meiden bestimmte Dienste vollständig, obwohl sie um deren Nutzen wissen.

Fazit & Bedarfe
Fatalist:innen sind digital nicht unwissend – aber desillusioniert. Ihr hohes Verunsicherungsgefühl, kombiniert mit der Erfahrung häufiger Sicherheitsvorfälle, erzeugt eine innere Distanz zum digitalen Raum. Diese Nutzer:innen benötigen keine neuen Informationen, sondern neue Perspektiven:

- Ermutigung statt Warnung
- positive Erfahrungsräume mit Schutzmaßnahmen
- sicherheitserprobte Formate, die konkrete Wirksamkeit erlebbar machen

Aufklärungsarbeit sollte das Ziel verfolgen, Selbstwirksamkeit zu stärken. Nur wer erlebt, dass Schutz funktioniert, wird Schutz auch anwenden. Vertrauen in die eigene Kompetenz ist bei Fatalist:innen der entscheidende Hebel für digitale Resilienz.

Abb. 17 / Sicherheitsindex 2025
Top 3 Sicherheitsvorfälle

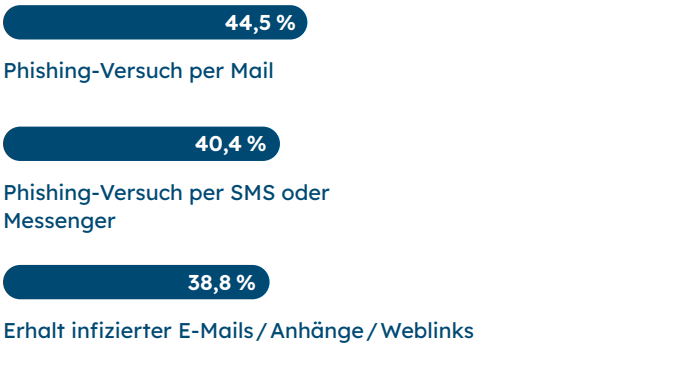
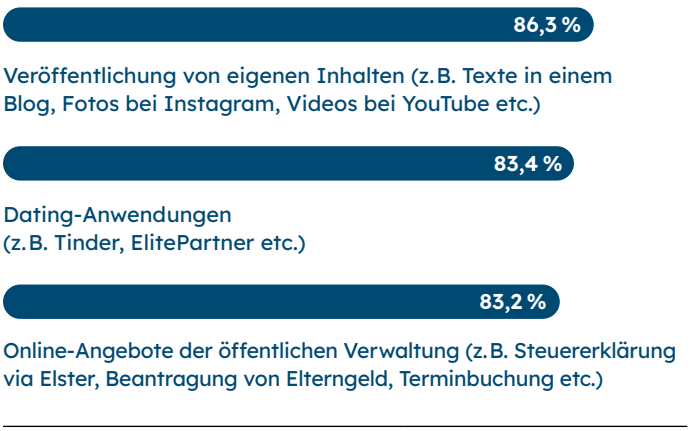


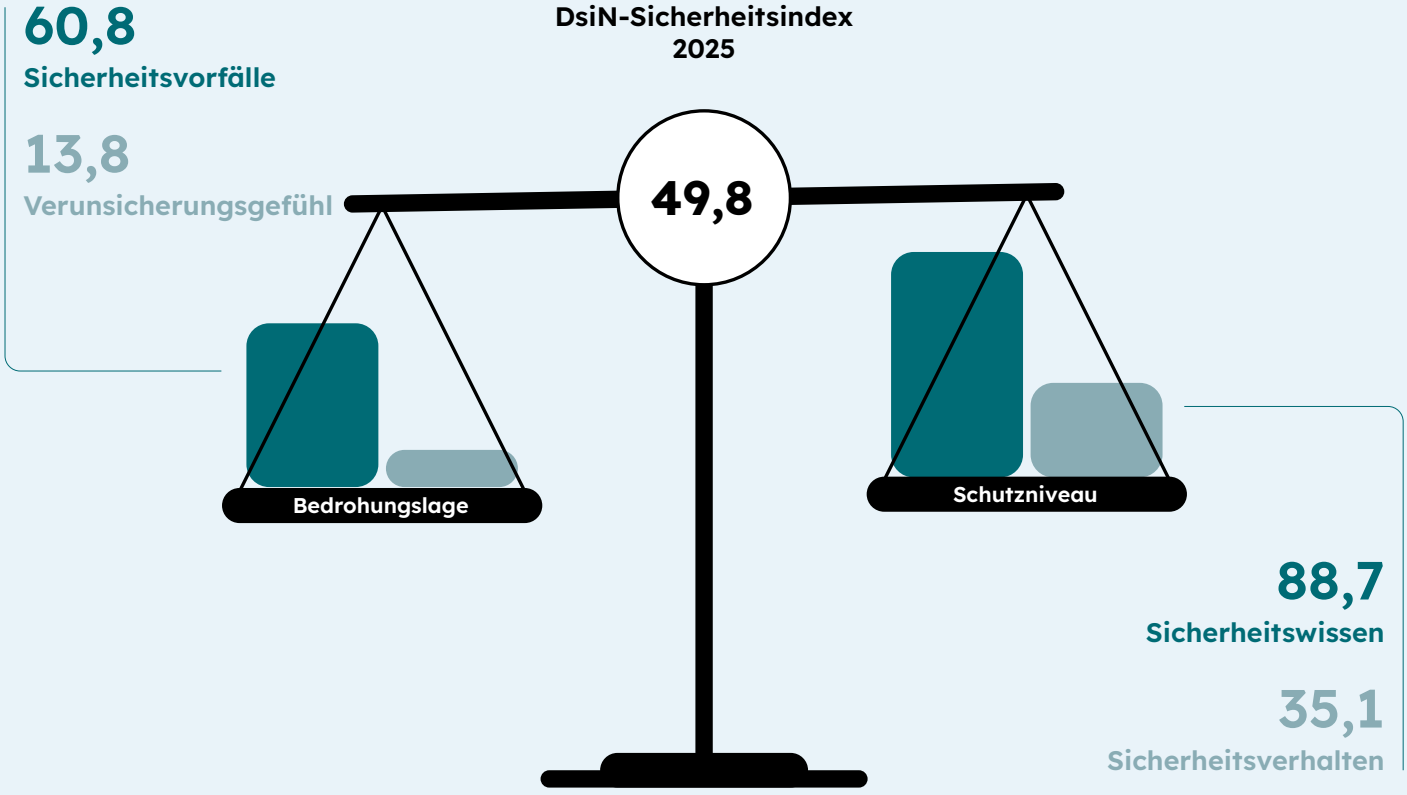
Abb. 18 / Sicherheitsindex 2025
TOP 3 Verunsicherungsgefühl (Gefährdungspotential)



Gutgläubige Nutzer:innen

Abb. 19 / Sicherheitsindex 2025

DsiN-Indexwert für gutgläubige Nutzer:innen in Punkten



Soziodemografie & Nutzungsmuster
Mit einem Anteil von 42,6 % stellen die gutgläubigen Nutzer:innen die mit Abstand größte Gruppe unter den Verbraucher:innen im Netz – und verzeichnen zugleich den stärksten Zuwachs aller Typen (+4,0 %). Sie sind heterogen zusammengesetzt, was Alter, Bildung und Online-Erfahrung betrifft. Frauen sind mit rund 52,1 % etwas überrepräsentiert. Die meisten sind regelmäßig online – zwischen 10 und 30 Stunden pro Woche – und nutzen digitale Angebote vielfältig: Online-Shopping, Kommunikation, Streaming und Social Media sind feste Bestandteile ihres Alltags.

Digitale Sicherheitslage
Erstmals fällt der Sicherheitsindex dieser Gruppe unter die kritische 50-Punkte-Marke: Mit 49,8 Indexpunkten (–1,0) überwiegt die Bedrohungslage das individuelle Schutzniveau – eine alarmierende Entwicklung angesichts der Größe dieser Nutzergruppe.

Die Zahl der Sicherheitsvorfälle steigt moderat um +4,2 auf 60,8 Bedrohungspunkte, während das Verunsicherungsgefühl leicht abnimmt (–1,8), aber mit 13,8 Bedrohungspunkten weiterhin das niedrigste unter allen Gruppen bleibt.
Viele Mitglieder dieser Gruppe nehmen digitale Bedrohungen kaum als persönliche Gefahr wahr.

Das Sicherheitswissen geht leicht zurück (–0,6 auf 88,7 Schutzpunkte), liegt aber weiterhin im oberen Bereich. Problematisch bleibt das Sicherheitsverhalten: Mit 35,1 Schutzpunkten liegt es deutlich unter dem Durchschnitt – obwohl der Wert im Vergleich zum Vorjahr leicht steigt (+1,0). Die Gruppe weiß also durchaus, wie Schutz funktioniert – wendet dieses Wissen jedoch nur unzureichend an.

Vertrauensprofil
Gutgläubige Nutzer:innen zeichnen sich durch ein hohes Grundvertrauen aus – in technische Systeme, Plattformen und insbesondere in die Integrität von Dienstanbietern.
Sie gehen davon aus, dass „das schon alles funktionieren wird“, und verlassen sich auf automatische Schutzmechanismen oder das Prinzip „bisher ist ja auch nichts passiert“.

Diese Haltung führt zu einer gefährlichen Diskrepanz zwischen realer Bedrohung und gefühlter Sicherheit. Viele unterschätzen die potenziellen Folgen eines sorglosen Umgangs mit persönlichen Daten – und sind besonders anfällig für Phishing, Identitätsdiebstahl oder betrügerische Inhalte.

Zudem fehlt häufig das Bewusstsein dafür, dass vertrautes Verhalten nicht gleichbedeutend mit sicherem Verhalten ist. Vertrauen ersetzt hier Risikobewertung – und erschwert eine kritische Auseinandersetzung mit Sicherheitsmaßnahmen.

Fazit & Bedarfe
Die gutgläubigen Nutzer:innen sind ein zentrales Zielsegment für zukünftige Aufklärungsmaßnahmen. Ihre schiere Größe im digitalen Raum bedeutet, dass ihr Verhalten direkten Einfluss auf das Gesamtsicherheitsniveau hat. Aufklärung für diese Gruppe muss:

- Alltagssituationen aufgreifen, die Risiken sichtbar machen,
- emotionale Zugänge schaffen („Was passiert, wenn …?“),
- und praktische Schutzschritte als einfache Gewohnheiten vermitteln.

Vertrauen ist in dieser Gruppe kein Mangel, sondern eine Ressource – allerdings eine, die kritische Reflektion und Handlungskompetenz braucht, um nicht zur Schwachstelle zu werden. Ziel ist es, den Schritt vom „Es wird schon gutgehen“ zum „Ich kann etwas dafür tun, dass es gutgeht“ zu ermöglichen.

Abb. 20 / Sicherheitsindex 2025
Top 3 Sicherheitsvorfälle

28,9 %
Phishing-Versuch per SMS oder Messenger

27,9 %
Phishing-Versuch per Mail

23,2 %
Erhalt infizierter E-Mails / Anhänge / Weblinks

Abb. 21 / Sicherheitsindex 2025
TOP 3 Verunsicherungsgefühl (Gefährdungspotential)

34,5 %
Öffnen von Anhängen in E-Mails

22,0 %
Austausch vertraulicher Inhalte via Webseiten oder Apps (z. B. mit Behörden, Banken, Versicherungen)

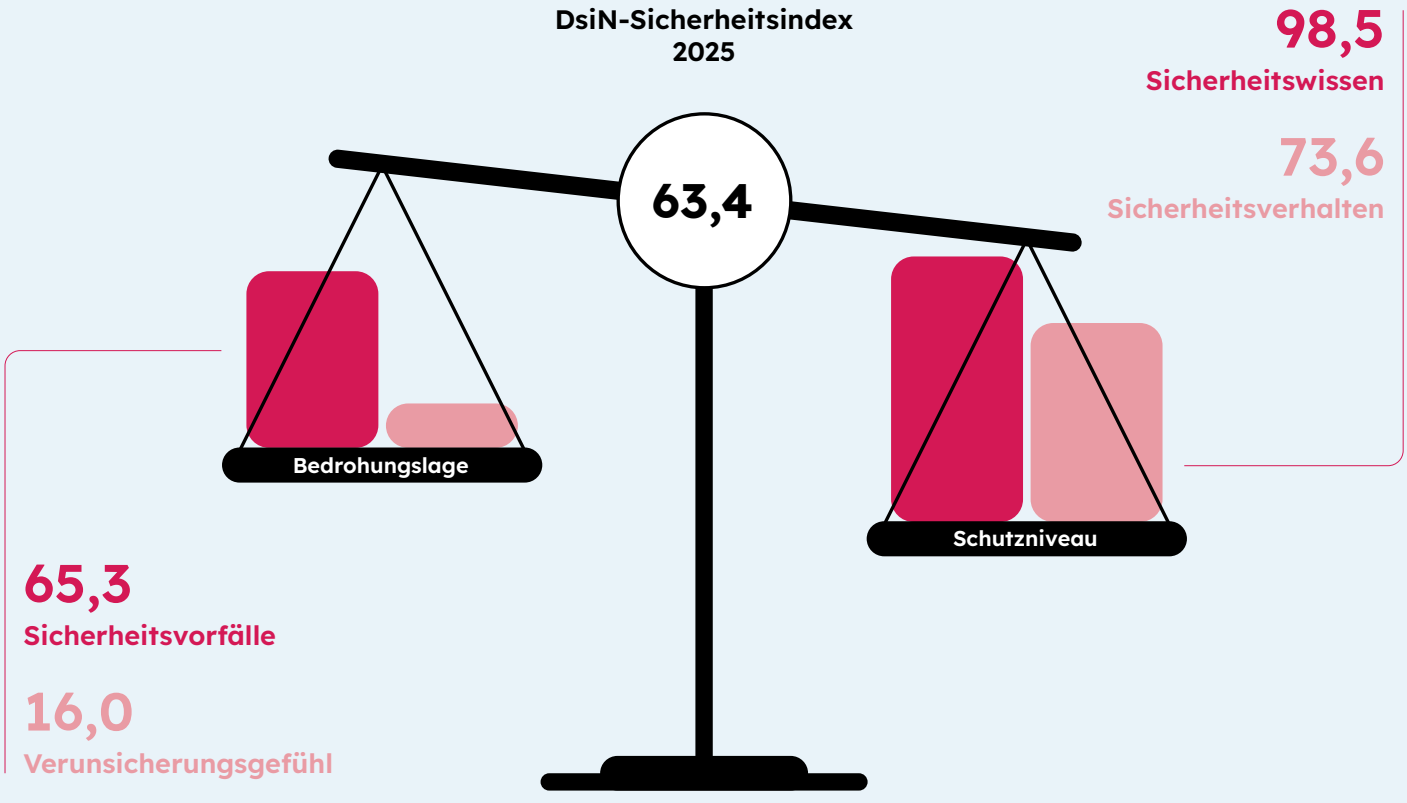
20,3 %
Bankgeschäfte im Internet / Online-Banking / -Brokering

Antreibende Nutzer:innen

„Ich will Neues entdecken – aber sicher.“

Abb. 22 / Sicherheitsindex 2025

DsiN-Indexwert für antreibende Nutzer:innen in Punkten



Soziodemografie & Nutzungsmuster
Antreibende Nutzer:innen sind technologieoffen, lernbereit und vielseitig digital unterwegs. Sie machen 2025 26,9 % der Onlinebevölkerung aus – ein Rückgang um 3,5Prozentpunkte im Vergleich zum Vorjahr. Ihr Altersdurchschnitt liegt unter dem anderer Gruppen: 60 % der Antreibenden sind zwischen 30 und 60 Jahren alt, überdurchschnittlich oft berufstätig, gut gebildet und technikaffin. Sie nutzen eine breite Palette digitaler Dienste – von Onlinebanking bis zu Smart-Home-Anwendungen – und probieren gern neue Tools, Apps oder Plattformen aus.

Digitale Sicherheitslage
Mit 63,4 Indexpunkten erreichen die Antreibenden einen deutlichen Zuwachs von +3,6 Indexpunkten – das zweitbeste Ergebnis aller Gruppen nach den Bedachtsamen. Sie verbessern ihr Schutzniveau, während die Bedrohungslage zurückgeht – ein positives Signal in einem insgesamt angespannten digitalen Umfeld.

Die Zahl der Sicherheitsvorfälle sinkt um 6,4 Bedrohungspunkte. Auch das Verunsicherungsgefühl geht leicht zurück (–2,3 auf 16,0 Bedrohungspunkte), bleibt aber – trotz hoher Aktivität – auf einem moderaten Niveau.

Das Sicherheitswissen steigt auf 98,5 Schutzpunkte (+2,3) – der höchste Wert im gesamten Index. Gleichzeitig verbessert sich das Sicherheitsverhalten auf 73,6 Schutzpunkte (+1,6), womit die Antreibenden auch in der Umsetzung von Schutzmaßnahmen an der Spitze liegen.

Vertrauensprofil
Antreibende Nutzer:innen sind selbstbewusst, aber nicht sorglos. Sie vertrauen auf ihre Fähigkeit, Informationen einzuordnen, Risiken zu bewerten und passende Schutzmaßnahmen zu wählen. Ihr Vertrauen basiert auf Wissen und Erfahrung – nicht auf blinden Annahmen.

Gleichzeitig erwarten sie von digitalen Angeboten Transparenz und Kontrollmöglichkeiten. Dienste, die intransparent agieren oder keine klaren Sicherheitseinstellungen bieten, stoßen bei dieser Gruppe schnell auf Ablehnung. Besonders wichtig ist ihnen der Zugang zu aktuellen Informationen über neue Bedrohungen – sie möchten proaktiv handeln können.

Diese Gruppe ist offen für Aufklärung – allerdings nur, wenn sie schnell, fundiert und praktisch relevant ist. Übermäßige Vereinfachungen oder „pädagogischer Ton“ wirken eher abschreckend.

Fazit & Bedarfe
Antreibende Nutzer:innen sind ein entscheidender Multiplikator für digitale Sicherheitskompetenz. Sie bringen eine hohe Motivation mit, ihr Wissen weiterzugeben – im Freundeskreis, im Beruf oder in der Familie. Damit können sie Brücken schlagen zu anderen Gruppen, die weniger souverän sind. Um dieses Potenzial zu nutzen, braucht es:

- zielgruppengerechte Informationsangebote auf hohem Niveau
- aktuelle Sicherheitsupdates, die Trends und neue Angriffsformen adressieren
- Austauschformate, z.B. Peer-Learning, Tech-Communities oder Tandems

Diese Gruppe will gestalten, nicht nur reagieren. Mit dem richtigen Angebot kann sie zum Motor für digitale Resilienz in der Gesellschaft werden.

Abb. 23 / Sicherheitsindex 2025
Top 3 Sicherheitsvorfälle

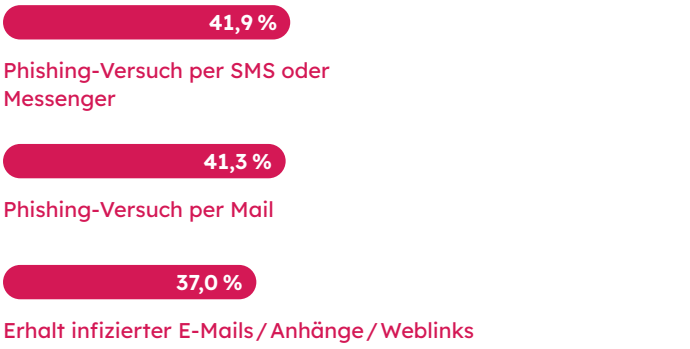
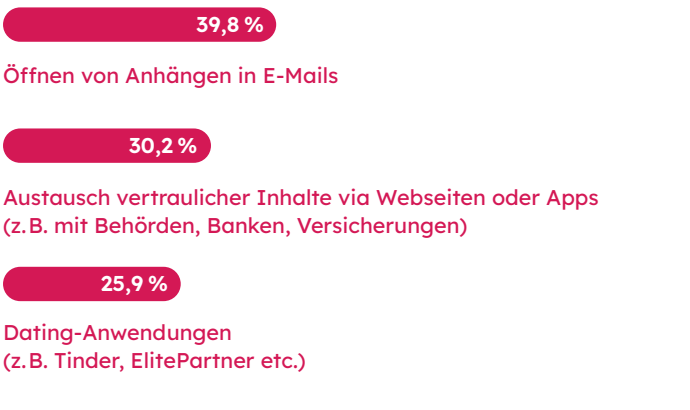


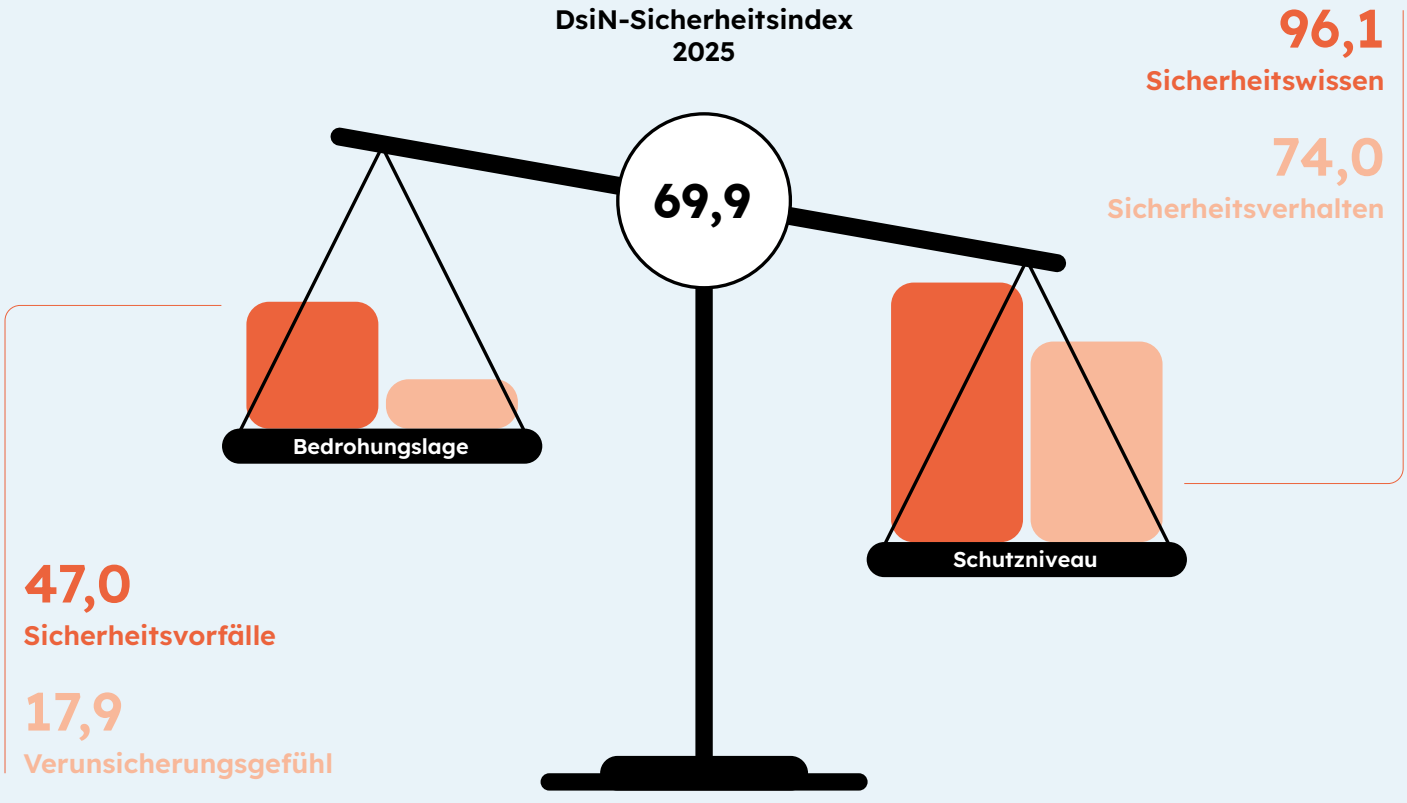
Abb. 24 / Sicherheitsindex 2025
TOP 3 Verunsicherungsgefühl (Gefährdungspotential)



Bedachtsame Nutzer:innen

Abb. 25 / Sicherheitsindex 2025

DsiN-Indexwert für antreibende Nutzer:innen in Punkten



Soziodemografie & Nutzungsmuster
Mit einem Anteil von 18,0 % (–0,8 %) bilden bedachtsame Nutzer:innen eine konstant souveräne Gruppe, die trotz leichtem Rückgang weiterhin mit Abstand die höchsten Sicherheitswerte aufweist. Sie sind mehrheitlich über 50 Jahre alt – 14,1 % sogar über 70. Nur ein sehr kleiner Anteil (4,6 %) ist unter 30. Das Geschlechterverhältnis ist nahezu ausgeglichen. Sie gelten als reflektierte Nutzer:innen, die sich gezielt informieren, technische Neuerungen prüfen und ihre Geräte aktiv verwalten.

Ihre Nutzung ist bewusst, nicht zögerlich: Onlinebanking, Cloud-Anwendungen, E-Government-Dienste oder Zwei-Faktor-Authentifizierungen gehören zum digitalen Alltag – aber nur, wenn sie als sicher eingeschätzt werden.

Digitale Sicherheitslage
Mit einem Indexwert von 69,9 Indexpunkten (+3,6) erreichen die Bedachtsamen erneut den höchsten Gesamtwert aller Nutzer:innengruppen. Sie reduzieren ihre Bedrohungslage, während sie gleichzeitig ihr bereits hohes Schutzniveau weiter ausbauen.

Die Sicherheitsvorfälle gehen um 7,9 Bedrohungspunkte zurück – ein klarer Erfolg, der auf effektive Prävention hinweist. Auch das Verunsicherungsgefühl sinkt auf 17,9 Bedrohungspunkte (–2,7) – trotz hoher Aktivität im Netz. Diese Gruppe begegnet Risiken mit Wissen, Struktur und Gelassenheit.

Das Sicherheitswissen bleibt mit 96,1 Schutzpunkten stabil (–0,1), während das Verhalten weiter leicht steigt: auf 74,0 Schutzpunkte (+0,8). Damit setzen sie bekannte Schutzmaßnahmen konsequent um und achten auf Updates, starke Passwörter, sichere Verbindungen und datensparsame Nutzung.

Vertrauensprofil
Bedachtsame Nutzer:innen vertrauen – aber nicht blind. Sie überprüfen Quellen, informieren sich über Anbieter und Dienste, und haben ein feines Gespür für mögliche Manipulation oder Intransparenz. Ihr Vertrauen basiert auf informierter Einschätzung und kontrollierter Offenheit.

Gleichzeitig engagieren sie sich oft als digitale Ratgeber:innen in ihrem Umfeld: in Familien, Vereinen, am Arbeitsplatz. Ihr Wissen teilen sie aktiv – und übernehmen Verantwortung, etwa beim Einrichten sicherer Geräte für andere.

Im Kontext des diesjährigen Fokusthemas „Vertrauen in der digitalen Welt“ sind sie der Inbegriff digitaler Souveränität: Sie verbinden Technikverständnis mit reflektiertem Umgang und dem Wunsch, sich und andere zu schützen.

Fazit & Bedarfe
Bedachtsame Nutzer:innen sind digitale Vorbilder, an denen sich andere Gruppen orientieren können. Um ihre Rolle als Multiplikator:innen weiter zu stärken, braucht es:

- wertschätzende, nicht belehrende Kommunikation
- Anerkennung ihrer digitalen Fürsorgearbeit, etwa im Familien- oder Vereinskontext
- Tools und Ressourcen, mit denen sie ihr Wissen effektiv weitergeben können

Sie sind die Brücke zwischen technischer Kompetenz und gesellschaftlicher Verantwortung. Ihre Perspektive sollte strategisch eingebunden werden, wenn es um neue Aufklärungsformate, digitale Teilhabe oder vertrauenswürdige Technologien geht.

Abb. 26 / Sicherheitsindex 2025
Top 3 Sicherheitsvorfälle

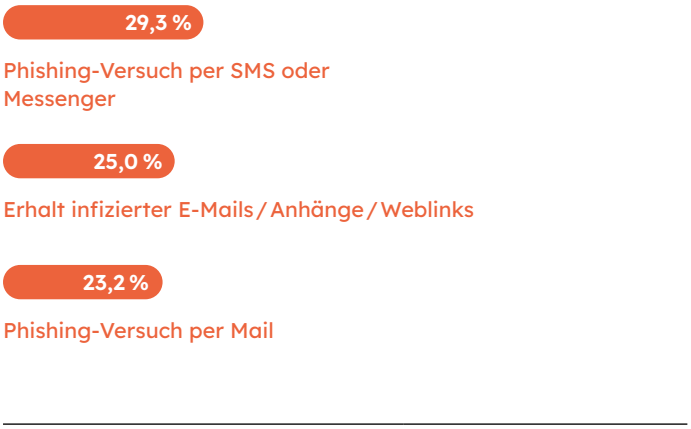
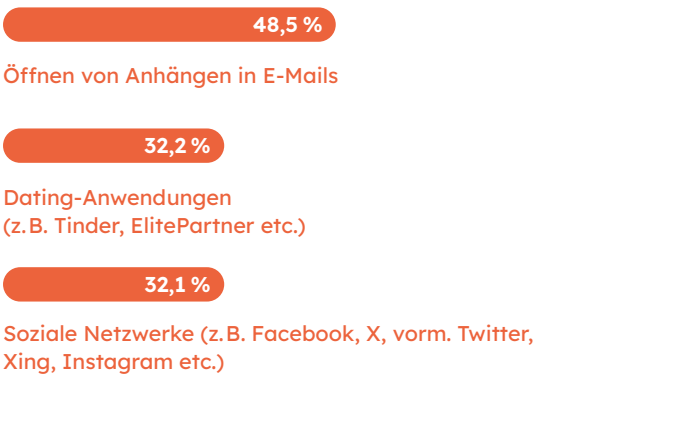


Abb. 27 / Sicherheitsindex 2025
TOP 3 Verunsicherungsgefühl (Gefährdungspotential)



Kapitel 3

Digitale Lebenswelten 2025

Wo und wie nutzen Menschen das Internet?

Das Internet ist für die meisten Menschen ein wichtiger Teil des Alltags. Wir schreiben Nachrichten, kaufen online ein, machen Bankgeschäfte oder speichern unsere Gesundheitsdaten digital. Auch das Zuhause wird immer vernetzter – etwa durch Sprachassistenten oder smarte Geräte.

Doch nicht alle fühlen sich im digitalen Raum sicher. Manche Menschen wissen nicht genau, wie sie sich schützen können – laut DsiN-Sicherheitsindex 2025 kennt etwa jede:r Zehnte gängige Schutzmaßnahmen wie Datensicherung oder Virenschutz nur schlecht oder gar nicht. Andere machen schlechte Erfahrungen, zum Beispiel durch falsche Informationen oder Betrug.

Der DsiN-Sicherheitsindex 2025 zeigt: Viele Menschen wünschen sich mehr Unterstützung, mehr Orientierung und mehr Schutz im digitalen Alltag. Ein zentrales Thema dabei ist das Vertrauen in der digitalen Welt. Denn wer digitalen Angeboten nicht vertraut, wird sie seltener nutzen – oder gar nicht.

In diesem Kapitel zeigen wir, wie sich Menschen in Deutschland in der digitalen Welt bewegen:

- Welche Angebote nutzen sie besonders häufig?
- Wo fühlen sie sich sicher?
- Wo braucht es mehr Schutz, klare Regeln oder Aufklärung?

Dabei geht es um sieben Bereiche des digitalen Lebens: Kommunikation, Online-Shopping, Gesundheitsdienste, Onlinebanking, das vernetzte Zuhause, digitale Identität – und als roter Faden durch alles: das Vertrauen.

Kommunikation

Häufige Nutzung von Messenger-Apps und E-Mails

Sorge: Datenschutz & Desinformation

74,2 % der Befragten nutzen E-Mails – häufigste private Onlineaktivität

77,8 % geben an, vorsichtiger mit ihren persönlichen Daten umgehen zu müssen.

Onlinebanking

Häufige Nutzung, v.a. mobil

Sorge: Phishing, technisches Verständnis

59,6 % nutzen Onlinebanking

27,4 % empfinden es als gefährlich oder sehr gefährlich

Online-Shopping

Beliebt bei Jung & Alt

Sorge: Betrug & unseriöse Anbieter

71,1 % kaufen online ein

15,5 % wurden Opfer von Online-Betrug

Digitale Identität

Anmeldung mit eID, digitale Nachweise

Sorge: Identitätsdiebstahl

77,8 % sehen sich selbst in der Verantwortung für Sicherheit

69,3 % fordern bessere Sicherheitsvorkehrungen von Anbietern

Vernetztes Zuhause (Smart Home)

Sprachassistenten, vernetzte Geräte

Sorge: Überwachung & Datensicherheit

9,0 % nutzen vernetzte Haustechnik

22,7 % stufen Sprachassistenten und Smart-Home-Anwendungen als gefährlich ein

Gesundheitsdienste

E-Rezept, Online-Sprechstunden

Sorge: Vertraulichkeit sensibler Daten

17,2 % nutzen digitale Gesundheits- und Fitnessdienste

55,5 % sehen ein hohes Risiko in der Sammlung & Analyse von Gesundheitsdaten

Vertrauen

Digitale Sicherheit beginnt mit Vertrauen – und wächst durch Kompetenz, klare Regeln und gemeinsames Handeln

78,5 %
halten Vertrauen für (sehr) wichtig

15,6 %
fühlen sich digital kompetent.

Vertrauen in der digitalen Welt

Wie wichtig ist Vertrauen im Netz?
Vertrauen in der digitalen Welt prägt zunehmend den Alltag der Verbraucher:innen und beeinflusst, wie sie digitale Angebote wahrnehmen. Rund 78,5 % der Befragten empfinden dieses Thema als wichtig oder sogar sehr wichtig, während lediglich 3,4 % ihm nur geringe Bedeutung beimessen. Allerdings beschäftigen sich 26,2 % der Onliner:innen regelmäßig damit, 46,2 % tun dies zumindest gelegentlich. Immerhin knapp ein Viertel (25,8 Prozent) findet Vertrauen im digitalen Raum nicht wichtig.

Der Schutz der persönlichen Daten im Netz bleibt der zentrale Aspekt für das Vertrauen im digitalen Raum. So empfinden 86,8 % der Befragten den Umgang mit ihren personenbezogenen Daten als entscheidend. Dicht gefolgt von der Kontrolle der Sicherheitseinstellungen, die 83,9 % als essenziell bewerten, und der Glaubwürdigkeit von Online-Informationen, der 82,8 % Bedeutsamkeit beimessen. Auf Platz fünf folgen Jugendschutzeinstellungen, die von 72,1 % als wichtig für digitales Vertrauen eingestuft werden.

Wem vertrauen Nutzer:innen im Netz?
Insgesamt ist die Skepsis im Internet groß: Als vertrauenswürdigste Quellen gelten Öffentliche Stellen mit 63,1 Prozent, gefolgt von Ergebnissen einschlägiger Suchmaschinen (51,9 Prozent) und Inhalten gemeinnütziger Organisationen (50,6 Prozent). Immerhin mehr als die Hälfte vertraut großen Medienhäusern nicht: Sie gelten nur 48,1 der Nutzer:innen als verlässliche Quelle. Inhalte von Influencer:innen vertrauen 51,3 % der Nutzer:innen weniger oder gar nicht – was bei 45,9 % auch für Informationen aus sozialen Netzwerken gilt.

Wie reagieren Nutzer:innen auf vermeintliche Falschinformationen im Netz?
28,7 % der Befragten stoßen häufig oder sehr häufig auf widersprüchliche oder unklare Inhalte im Internet. Knapp die Hälfte (46,7 Prozent) begegnet ihnen zumindest gelegentlich, während 24,6 % angeben, selten oder nie damit konfrontiert zu werden.

Was tun, wenn Informationen unzuverlässig erscheinen?
53,3 % suchen aktiv nach weiteren Berichten, um die Richtigkeit der Informationen zu bestätigen oder zu widerlegen. 45,2 % überprüfen die Quelle der Nachricht, während lediglich 11,3 % den Schritt wagen, diese direkt der Plattform oder dem Anbieter zu melden. 24,7 % entscheiden sich, die Informationen zu ignorieren, wenn Zweifel bestehen. Bei der Überprüfung von Nachrichten aus sozialen Netzwerken zeigt sich, dass 31,1 % diese Inhalte regelmäßig oder häufig kritisch hinterfragen, während 26,4 % auch die Aussagen von Influencer:innen überprüfen. Inhalte aus beruflichen Netzwerken werden mit 17,9 % am seltensten kontrolliert, und nur 20,5 % der Befragten nutzen regelmäßig KI-Chatbots als Prüfwerkzeug – 44,6 % tun dies nur selten oder gar nicht.

Wie kann digitales Vertrauen gestärkt werden?
55 % der Befragten fordern zur Stärkung des digitalen Vertrauens klare Regeln und Sanktionen gegen Desinformation. Gleichzeitig sehen 54,1 % die Anbieter in der Verantwortung, aktiv gegen falsche Informationen vorzugehen, während 53,3 % es als wichtig erachten, dass unabhängige Institutionen Inhalte regelmäßig auf ihre Richtigkeit prüfen.

Das Thema Desinformation wird von gut zwei Dritteln der Befragten (67,6 Prozent) als gravierendes Problem im digitalen Raum wahrgenommen. Dabei machen 46,5 % die Verstärkung falscher Informationen durch Algorithmen sozialer Netzwerke verantwortlich, während 45,3 % betonen, dass seriöse Plattformen dennoch vertrauenswürdige Informationen liefern. Dennoch gibt ein gutes Viertel der Befragten an, Schwierigkeiten dabei zu haben, verlässliche von falschen Informationen zu unterscheiden.

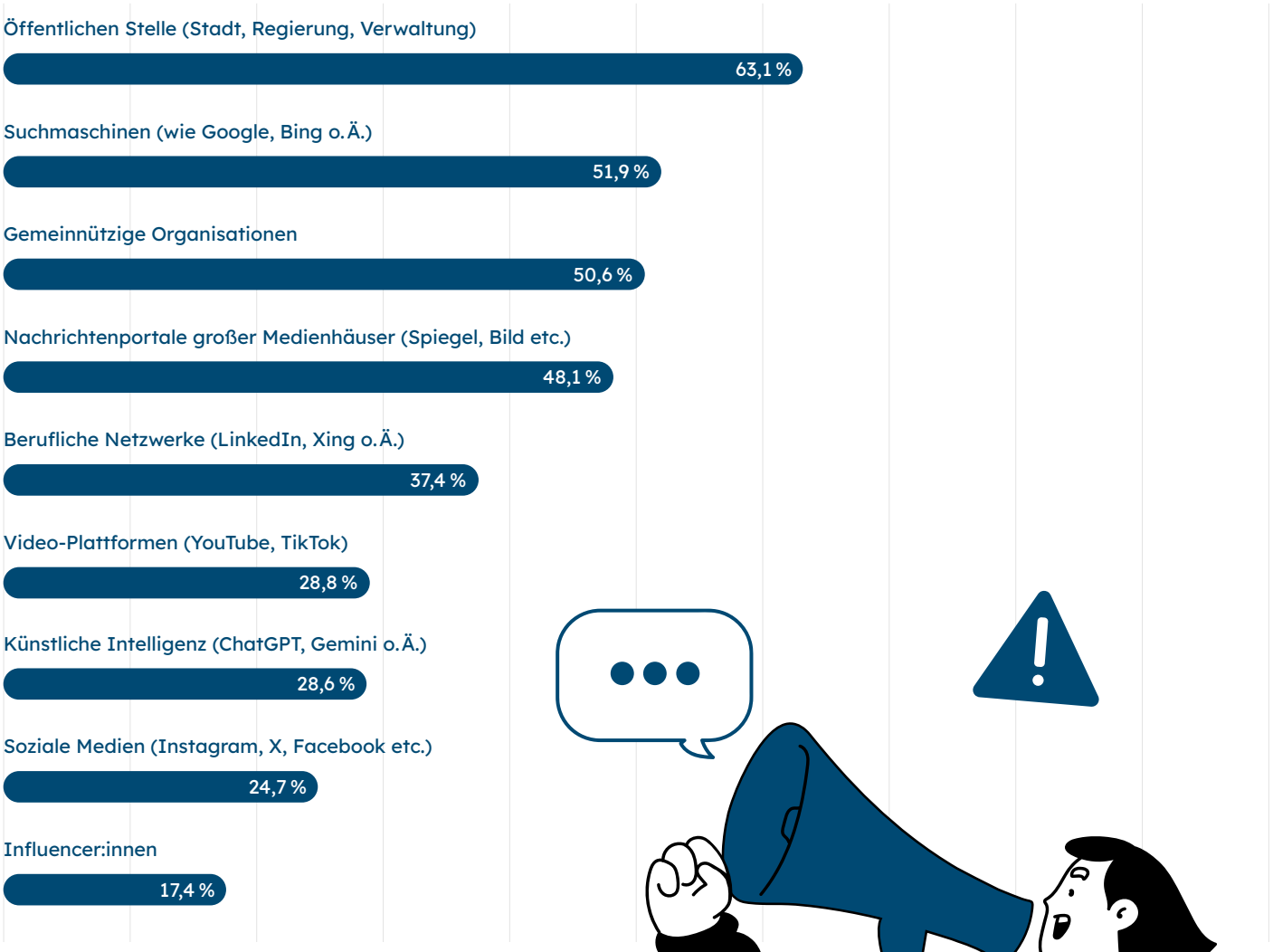
Das Thema Desinformation wird von gut zwei Dritteln der Befragten als gravierendes Problem im digitalen Raum wahrgenommen.

Welche Unterstützung wünschen sich Nutzer:innen?
Ein erhöhtes Informationsbedürfnis bezüglich digitaler Technologien zeigt sich bei knapp 20 % der Nutzer:innen, während 19,3 % regelmäßig aktiv nach weiterführenden Informationen suchen, um digitale Angebote besser zu verstehen. 37,1 % tun dies jedoch selten oder gar nicht. Betrachtet man den Weiterbildungsbedarf, so steht das Erkennen von Fake News an erster Stelle – 51,6 % der Onliner:innen würden gern ihre Kompetenzen in diesem Bereich ausbauen, gefolgt von Datenschutz (48,3 Prozent). Nur 15,6 % fühlen sich vollständig sicher im Umgang mit den eigenen digitalen Kompetenzen.

Abb. 28 / Sicherheitsindex 2025

Vertrauen in verschiedene digitale Informationsquellen unter Internetnutzenden

Wem vertrauen Internetnutzende?



Kommunikation im Netz

Digitale Kommunikation ist für die meisten Menschen ein fester Bestandteil des Alltags. Ob per E-Mail, über Messenger oder mithilfe digitaler Plattformen – der Austausch findet zunehmend online statt. Doch wie steht es dabei um das Bewusstsein für Sicherheit?

Ein Großteil der Internetnutzer:innen sieht sich selbst in der Verantwortung, Sicherheitsvorfälle zu vermeiden. 77,8 % geben an, vorsichtiger mit ihren persönlichen Daten umgehen zu müssen – ein leichter Rückgang im Vergleich zum Vorjahr (–2,7 %). Gleichzeitig fordern 69,3 % strengere Sicherheitsvorkehrungen von Anbietern digitaler Dienste (–1,9 %) und 68,5 % von Geräteherstellern (+0,6 %). Besonders auffällig ist, dass die Forderung nach einer strengeren Verfolgung von Gesetzesverstößen um 7,2 Prozentpunkte auf 67,7 % gesunken ist.

Die klassische E-Mail bleibt ein beliebtes Kommunikationsmittel – doch nicht jede:r weiß, wie man sie sicher nutzt.

Zwar kennt ein Großteil der Nutzer:innen die Möglichkeit, E-Mails zu verschlüsseln – insgesamt 92 % geben an, davon schon einmal gehört zu haben. Doch bei der tatsächlichen Umsetzung zeigt sich ein anderes Bild: Nur 33,2 % nutzen die E-Mail-Verschlüsselung auch aktiv.

Auch weitere Schutzmaßnahmen rund um digitale Kommunikation sind vielen bekannt – von Spamfiltern bis hin zu elektronischen Signaturen – aber die Nutzungsraten bleiben oft hinter dem Kenntnisstand zurück.

Die digitale Kommunikation verlagert sich zunehmend aufs Smartphone – sei es über Messenger oder andere Apps. Dabei zeigt sich: Viele Nutzer:innen achten inzwischen stärker auf die Sicherheit ihrer mobilen Endgeräte. So aktivieren beispielsweise 73,4 % eine PIN zum Schutz ihres Geräts, und 75,2 % führen regelmäßige Updates des Betriebssystems durch. Auch die Nutzung von Sicherheitsprogrammen und Anti-Viren-Software ist mit 59,6 % bzw. 67,6 % vergleichsweise hoch.

Tun wir genug für unsere digitale Privatsphäre?
Auch wenn nicht alle Nutzer:innen spezielle Tools einsetzen, um ihre Kommunikation zu schützen, ist ein grundlegendes Bewusstsein für Datenschutz vorhanden. So geben 42,8 % der Befragten an, gezielt die Sicherheitseinstellungen ihres Browsers verändert zu haben – etwa zur Kontrolle über Tracking oder Sichtbarkeit. Dies deutet auf eine wachsende Sensibilität für digitale Selbstbestimmung hin – auch wenn hier noch Potenzial besteht.

Digitale Fitness- und Gesundheitsdienste

Pulskontrolle und Schrittzählung mittels Fitness-Uhr, Online-Terminbuchungen bei Ärzt:innen oder das Speichern von Gesundheitsdaten in der elektronischen Patientenakte – digitale Dienstleistungen im Gesundheitsbereich erfreuen sich in Deutschland weiterhin großer Beliebtheit. Trotz dieser positiven Entwicklungen bleibt die Verunsicherung groß, da viele Verbraucher:innen insbesondere Zweifel hinsichtlich der Sicherheit ihrer Gesundheitsdaten äußern.

Im Vergleich zum Vorjahr verzeichnet die Nutzung von Gesundheits- und Fitnessdiensten 2025 einen leichten Rückgang um 0,6 Prozentpunkte auf nun 17,2 %. Unterstützende Onlinedienste im Gesundheitswesen werden von 17,3 % der Befragten als gefährlich oder sehr gefährlich eingeschätzt, während diese Sorge bei Fitness- oder Gesundheitsprogrammen von 13,9 % geäußert wird.

Welche Bedenken haben Verbraucher:innen?
Bezogen auf den Umgang mit personenbezogenen Gesundheitsdaten sehen die Befragten das größte Risiko in der Sammlung und Analyse dieser Daten in Datenbanken, die für die Weiterentwicklung von Diagnose- und Therapiemaßnahmen genutzt werden – hier geben 19,2 % an, dass sie ein hohes Risiko sehen. Auf dem zweiten Rang folgt das Anlegen und Nutzen einer elektronischen Patientenakte, das von 17,6 % als problematisch bewertet wird. Weiterhin wird die digitale Dokumentation personenbezogener Daten durch Gesundheitsprogramme von 12,9 % als riskant eingeschätzt, während der digitale Austausch gesundheitsbezogener Daten – sowohl zwischen Ärzt:innen und Krankenkassen als auch zwischen Patient:innen und Ärzt:innen – jeweils von 15,3 % der Befragten als gefährlich bewertet wird.

Die digitale Dokumentation personenbezogener Daten durch Gesundheitsprogramme wird von 12,9 % als riskant eingeschätzt.

Diese Entwicklungen verdeutlichen den anhaltenden Bedarf an kontinuierlicher Aufklärungsarbeit und transparenter Kommunikation, um das Vertrauen in digitale Gesundheitsdienste zu stärken und Sicherheitsbedenken der Nutzer:innen effektiv zu adressieren.

Das vernetzte Zuhause

Im vernetzten Zuhause, auch als Smart Home bekannt, werden verschiedene Geräte wie Beleuchtung, Heizung, Haushaltsgeräte und Unterhaltungselektronik mittels Funkverbindung miteinander vernetzt, um zentral gesteuert zu werden – häufig auch über mobile Apps. Ergänzt wird dieses System durch sprachgestützte Assistenten, intelligente Fernsehgeräte und smarte Lautsprecher, die den Komfort im Alltag erhöhen.

Aktuell geben lediglich 9 % der Befragten an, vernetzte Haustechnik oder Unterhaltungselektronik zu nutzen – ein deutlicher Rückgang um 5,1 Prozentpunkte im Vergleich zum Vorjahr. Dieser Rückgang steht im Kontrast zu früheren Jahren, in denen Smart-Home-Anwendungen zunehmend Verbreitung fanden.

Welche Sicherheitsrisiken fürchten Verbraucher:innen?
Auch in puncto Sicherheitsrisiko zeigt sich ein differenziertes Bild: Sprachgestützte Assistenten und Smart-Home-Anwendungen werden von jeweils 22,7 % der deutschen Onliner:innen als gefährlich oder sehr gefährlich eingestuft. Im Vergleich dazu empfinden 16,3 % der Befragten die Steuerung und Vernetzung von Unterhaltungselektronik als riskant.

Welche Maßnahmen werden gebraucht?
Der Rückgang in der Nutzung korreliert mit einer gestiegenen Sensibilität gegenüber potenziellen Sicherheitsrisiken im digitalen Zuhause. Um das Vertrauen in Smart-Home-Technologien wieder zu stärken, sind transparente Informationen über die bestehenden Risiken und effektive Schutzmaßnahmen unerlässlich – insbesondere angesichts der fortschreitenden Integration Künstlicher Intelligenz in moderne Haustechnologien.

Einkaufen im Internet

Das Internet bietet zahlreiche Möglichkeiten, online einzukaufen – von Onlineshops großer Marken über Angebote kleiner Manufakturen bis hin zu Anzeigenportalen für neue und gebrauchte Waren. So ermöglicht die digitale Welt den bequemen Erwerb verschiedenster Produkte, erfordert jedoch auch digitale Kompetenzen, um Geld- und Datenverluste zu vermeiden.

Im Jahr 2025 ist das Online-Shopping mit 71,1 % der Befragten nur noch die zweithäufigste private Onlineaktivität – hinter dem Senden und Empfangen von E-Mails, das von 74,2 % genutzt wird. Dies entspricht einem Rückgang um 3,8 Prozentpunkte im Vergleich zum Vorjahr.

Auch wenn das Einkaufen im Internet von nur 12,2 % der Befragten als gefährlich oder sehr gefährlich eingeschätzt wird, zeigen sich in puncto Sicherheitsvorfälle alarmierende Tendenzen. Der Anteil der Personen, die in den letzten 12 Monaten Opfer von Betrug bei Online-Einkäufen wurden, ist um 1,9 Prozentpunkte auf 15,5 % gestiegen. Zudem geben 10,7 % an, dass ihre Zugangsdaten zu einem Online-Shop ausgespäht wurden oder ein entsprechender Versuch unternommen wurde. Auch beim Online-Kreditkartenbetrug ist mit 8,8 % ein Anstieg um 2,0 Prozentpunkte zu verzeichnen.

Welche Sicherheitsmaßnahmen kennen und nutzen Verbraucher:innen?
Die Kenntnis von sicheren Zahlungssystemen hat leicht abgenommen und liegt nun bei 98 Prozent, ebenso wie die Vertrautheit mit Gütesiegeln für Onlineshops, die von 94,6 % der Befragten genannt wird. Entsprechend sinkt auch die tatsächliche Nutzung: So setzen 75,3 % sichere Zahlungssysteme ein (rückläufig um 5,3 Prozentpunkte), während

57,6 % beim Online-Shopping auf Gütesiegel achten. Diese Entwicklungen unterstreichen die Notwendigkeit, Verbraucher:innen weiterhin über die Risiken und Schutzmaßnahmen beim Online-Einkauf aufzuklären, um trotz sinkender Nutzung das Vertrauen in digitale Einkaufsangebote zu stärken.

Onlinebanking

Den Kontostand kontrollieren, Überweisungen tätigen, Daueraufträge einrichten oder gar in Finanzmärkte investieren – Onlinebanking bietet vielfältige Möglichkeiten, Bankgeschäfte bequem über das Internet abzuwickeln. Dennoch ist die Nutzung dieser digitalen Finanzdienstleistungen im vergangenen Jahr leicht zurückgegangen: Nur 59,6 % der Befragten nutzen Onlinebanking, was einem Rückgang von 1,5 Prozentpunkten entspricht. Dieser leichte Rückgang könnte darauf hindeuten, dass Verbraucher:innen vermehrt alternative Finanzdienstleistungen ausprobieren oder dass Sicherheitsbedenken eine Rolle spielen.

Onlinebanking bietet vielfältige Möglichkeiten, Bankgeschäfte bequem über das Internet abzuwickeln.

Wie gefährlich ist Online-Banking?
Bezüglich der Sicherheitsaspekte schätzen 27,4 % der Verbraucher:innen Onlinebanking als gefährlich oder sehr gefährlich ein – ein Rückgang um 5,6 Prozentpunkte gegenüber dem Vorjahr, was auf einen leichten Vertrauensgewinn hindeuten mag. Dennoch berichteten 7,5 % der Befragten von Versuchen, ihre Zugangsdaten auszuspähen – ein leichter Anstieg um 0,9 Prozentpunkte, der zeigt, dass kriminelle Aktivitäten im digitalen Finanzbereich weiterhin präsent sind und das Sicherheitsrisiko nicht vollständig gebannt werden konnte.

Positiv hervorzuheben ist das Sicherheitsbewusstsein: 93,6 % der Befragten kennen verschlüsselte Datenverbindungen, und 62,7 % achten aktiv darauf, dass sie beim Onlinebanking über eine verschlüsselte Verbindung verfügen. Dies verdeutlicht, dass ein Großteil der Nutzer:innen sich der Bedeutung sicherer Datenübertragung bewusst ist. Gleichzeitig ist jedoch klar, dass weiterführende Aufklärungsarbeit notwendig bleibt, um auch in Zukunft das Vertrauen in digitale Finanzdienstleistungen zu stärken. Vor dem Hintergrund der stetigen Weiterentwicklung von Onlinebanking-Angeboten und der zunehmenden Verbreitung digitaler Finanztechnologien müssen Verbraucher:innen kontinuierlich über aktuelle Sicherheitsstandards und den richtigen Umgang mit sensiblen Daten informiert werden. So kann langfristig das Risiko unautorisierter Zugriffe minimiert und das Vertrauen in die digitale Abwicklung von Finanzgeschäften weiter gefestigt werden.

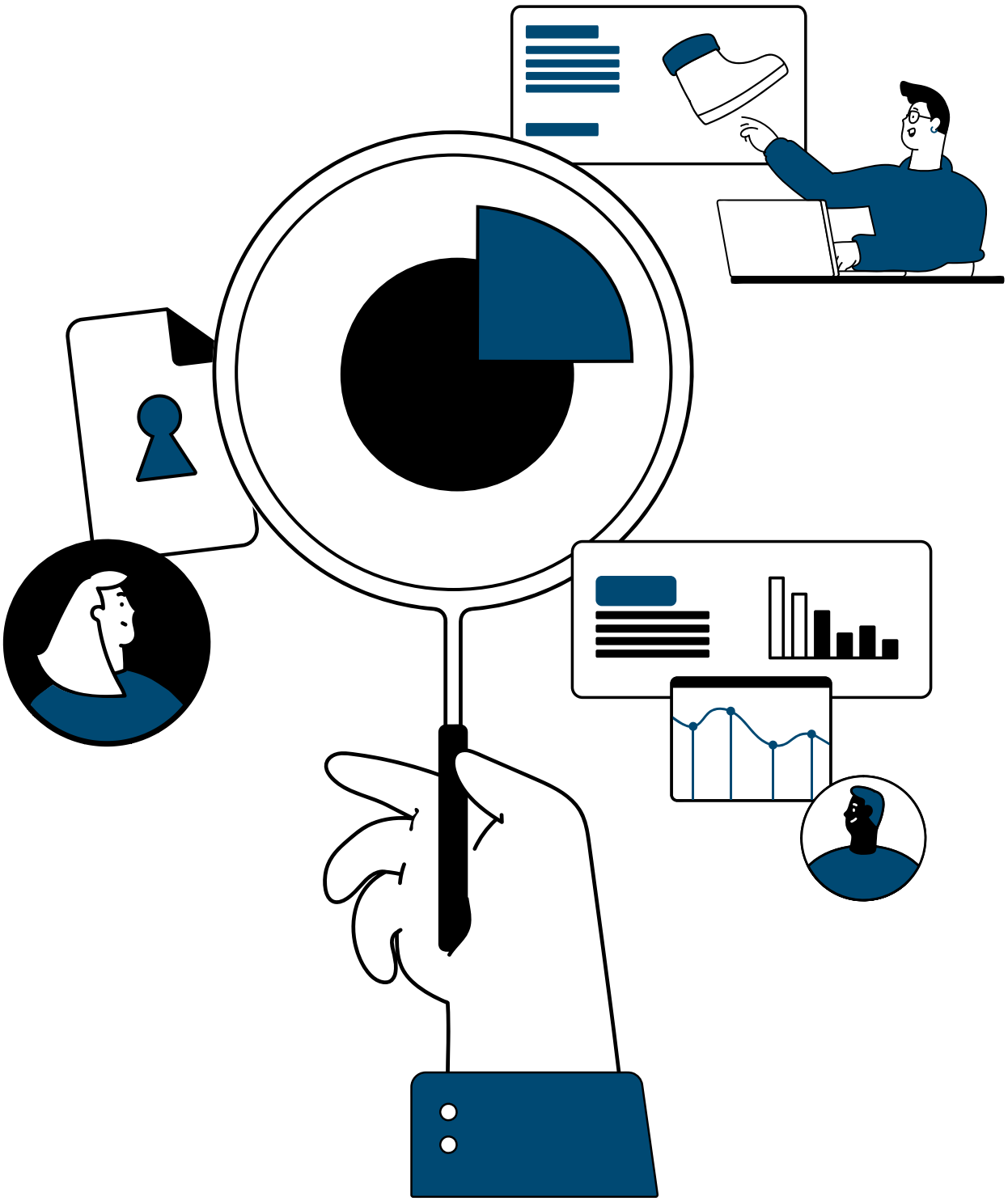
Digitale Identität

Der Blick in die verschiedenen Lebenswelten zeigt, dass jede Online-Aktivität digitale Spuren hinterlässt, aus denen sich eine individuelle Online-Identität – das digitale Ich – zusammensetzt. Wie detailliert dieses Profil ausfällt und inwieweit Verbraucher:innen Einfluss auf das entstehende Bild nehmen können, hängt maßgeblich von ihren Digitalkompetenzen ab. Im aktuellen Jahr offenbaren sich in diesem Zusammenhang veränderte Einstellungen und Forderungen, die den Schutz persönlicher Daten und die Kontrolle der eigenen digitalen Präsenz betreffen.

Wer trägt Verantwortung für den Schutz der digitalen Identität?
Verbraucher:innen legen nach wie vor großen Wert darauf, ihre digitalen Spuren im Griff zu behalten. So betonen 77,8 % der Befragten, dass sie selbst einen wesentlichen Beitrag zur Reduzierung von Sicherheitsvorfällen leisten müssen – ein Rückgang um 2,7 Prozentpunkte gegenüber dem Vorjahr. Gleichzeitig fordern 69,3 % der Nutzer:innen verbesserte Sicherheitsvorkehrungen seitens der Anbieter digitaler Dienste, während 68,5 % auch von Geräteherstellern höhere Standards erwarten. Interessanterweise ist der Ruf nach einer strengeren Verfolgung von Gesetzesverstößen mit 67,7 % um 7,2 Prozentpunkte gesunken, was auf eine veränderte Wahrnehmung der Effektivität bestehender Regulierungen hindeuten könnte. Lediglich 32,5 % erachten die eingeschränkte Nutzung des Internets als sinnvolle Methode, die eigene Datensicherheit zu erhöhen – hier verzeichnet man einen moderaten Zuwachs von 2,4 Prozentpunkten.

Welche Unterstützung wünschen sich Onliner:innen?
Die Verbesserung des Sicherheitswissens wird von 67,7 % der Befragten über eine zentrale Informationsplattform begrüßt, auch wenn dieser Wert um 0,9 Prozentpunkte zurückgeht. Zudem sind 65,2 % der Meinung, dass Informationen zum Schutz der eigenen Daten verständlicher aufbereitet sein müssen, während 63,5 % eine stärkere Einbindung von Aufklärungsangeboten in der schulischen

und beruflichen Ausbildung fordern – ein Wert, der im Vergleich zum Vorjahr um 5,8 Prozentpunkte gesunken ist. Ergänzend wünschen sich 71,7 % der Onliner:innen, dass die Möglichkeit zur einfachen Anpassung von Sicherheitseinstellungen bei Programmen und Geräten weiter verbessert wird. Gleichzeitig zeigt sich, dass 27,5 % der Befragten – ein Anstieg um 2,9 Prozentpunkte – keine Notwendigkeit sehen, ihr eigenes Sicherheitsverhalten zu ändern, solange sie selbst bislang keine negativen Erfahrungen gemacht haben.



Kapitel 4

Fazit

Was uns der DsiN-Sicherheitsindex 2025 sagt

Zum zweiten Jahr in Folge verharrt der DsiN-Sicherheitsindex auf einem historischen Tiefstand von 55,7 Indexpunkten. Bereits seit 2020 geht die digitale Sicherheit für Verbraucher:innen in Deutschland zurück. Im Vergleich zu seinem Höchststand von 65,4 Indexpunkten im Jahr 2016 ist er um fast zehn Punkte zurückgefallen.

Neue Technologien werden schnell Teil unseres Alltags – das birgt erhebliche Risiken für die individuelle IT-Sicherheit und die gesamtgesellschaftliche digitale Resilienz. Ein Beispiel: Nur 16,1 Prozent der Internetnutzenden halten die Messenger-Nutzung auf mobilen Geräten für gefährlich oder sehr gefährlich. Dabei haben 33,5 Prozent selbst Phishing-Versuche in Messenger-Diensten erlebt. Auch in puncto Sicherheitsvorkehrungen bleiben die meisten Nutzer:innen hinter dem zurück, was es für einen sicheren digitalen Alltag benötigt (nur 58,3 Prozent prüfen Links vor dem Öffnen auf mögliche Sicherheitsrisiken).

Insbesondere die Schere zwischen Wissen und Verhalten bleibt eine zentrale Herausforderung: In diesem Jahr klettert der Wert für das Sicherheitswissen zwar wieder auf seinen historischen Höchstwert aus dem Jahr 2023 von 90,5 Sicherheitspunkten, zugleich verschlechtert sich aber das Sicherheitsverhalten um 0,7 Sicherheitspunkte auf 52,9. In der Theorie wissen also viele, wie sie sich schützen sollten. Doch in der Praxis setzen nach wie vor zu wenige ihr Wissen konsequent um. Dieses Auseinanderklaffen zeigt sich in allen Bevölkerungsgruppen und digitalen Lebenswelten und erfordert neue Wege, Menschen im Alltag dazu zu bewegen, digitale Sicherheitsmaßnahmen selbstverständlich umzusetzen.

Ein typisches Alltagsbeispiel macht diese Wissens-Verhaltens-Lücke greifbar: Frau M. erhält eine E-Mail von einem angeblichen Paketdienst, der sie zur Bestätigung ihrer Adresse auffordert – inklusive eines harmlos wirkenden Links. Sie hat schon oft gehört, man solle bei unerwarteten Mails vorsichtig sein und keinen Links folgen. Dennoch klickt sie in Eile darauf, weil sie tatsächlich auf ein Paket wartet. Kurz darauf ist ihr Computer mit Malware infiziert. Dieses Szenario ist kein Einzelfall: 27,8 Prozent der Verbraucher:innen haben in den vergangenen 12 Monaten (wissentlich) eine E-Mail mit infizierten Inhalten erhalten. Die schiere Menge der Vorfälle ist dabei Teil des Erfolgsrezepts von Betrügern: Viele Nutzer:innen kennen die gängigen Sicherheitsempfehlungen, handeln im Alltag aber aus Bequemlichkeit, Stress, Unaufmerksamkeit oder sonstiger Faktoren trotzdem falsch. Genau hier gilt es anzusetzen. Aufklärung muss nicht nur Informationen vermitteln, sondern muss auch beim Verhaltenstraining im Alltag unterstützen.

28,7 %

der Internetnutzenden halten digitale Medienangebote grundsätzlich nicht für vertrauenswürdig.

Abb. 29 / Sicherheitsindex 2025

Verbesserung von Sicherheitswissen/-kompetenz

Digitale Kompetenzen für sichere digitale Teilhabe

Die digitale Bedrohungslage ist nicht gleichmäßig in der Gesellschaft verteilt. Zwar konnten souveräne Nutzungsgruppen ihre Index-Werte weiter ausbauen, gleichzeitig sind über die Hälfte der Internetnutzenden nicht ausreichend vor digitalen Gefahren geschützt. Die gutgläubigen Nutzer:innen, die mit 42,6 Prozent die mit Abstand größte Gruppe im Netz darstellen und sich in der Regel aus IT-Sicherheitssicht im Mittelfeld bewegen, fallen erstmals unter die 50-Indexpunkte-Marke. Mangelnde IT-Sicherheit ist damit kein Phänomen bei außenstehenden und fatalistischen Nutzer:innen, sondern breitet sich auch bei Alltagsnutzer:innen weiter aus.

Diese digitale Fragmentierung birgt Sprengstoff für den gesellschaftlichen Zusammenhalt. Wenn sich ein Teil der Menschen kompetent und sicher im Netz bewegt, während ein anderer Teil unsicher ist, zurückbleibt oder aus Angst digitale Angebote meidet, entsteht eine Kluft, die über die Technik hinausgeht. Digitale Spaltung kann soziale Spaltung nach sich ziehen – etwa dann, wenn ältere Generationen den Anschluss verlieren oder vulnerable Gruppen sich aus der vernetzten Welt ausschließen. Das Vertrauen zwischen den „digital Souveränen“ und den „digital Abgehängten“ kann leiden, Missverständnisse und Vorurteile können wachsen. Umgekehrt bedeutet mehr digitale Teilhabe und Sicherheit für alle auch mehr gesellschaftliches Miteinander. Deshalb geht es bei digitaler Sicherheit nicht nur um individuelle Risiken, sondern um einen gemeinsamen Rahmen, in dem alle sicher partizipieren können. Nur wenn wir die Wissens- und Kompetenzlücken schließen, bleibt die digitale Gesellschaft als Ganzes handlungsfähig.

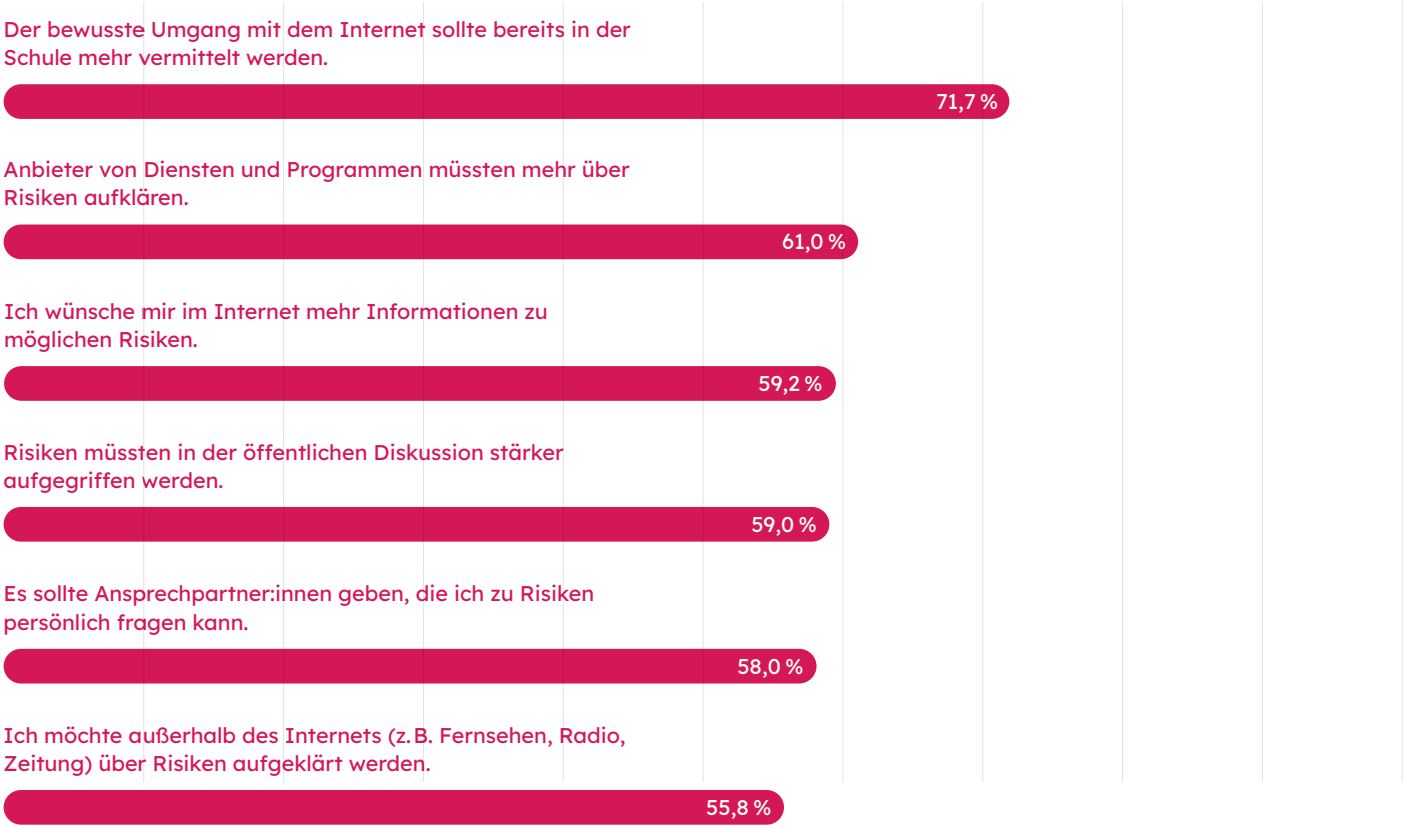
Vertrauen als digitale Zukunftsfrage

Aus dem Fokusthema der Studie – Vertrauen in der digitalen Welt – leiten sich Fragen ab, die zentral sind, um die digitale Sicherheitslage und Nutzungsverhalten in Deutschland zu verstehen. Denn: Ob Menschen ihre Kenntnisse anwenden und neue Technologien nutzen, hängt maßgeblich davon ab, ob sie dem digitalen Umfeld trauen können.

Abb. 30 / Sicherheitsindex 2025

Wie wollen Nutzer:innen über digitale Sicherheit informiert werden?

Diese Maßnahmen halten Nutzer:innen für geeignet oder sehr geeignet



Vertrauen entscheidet, ob wir digitale Chancen ergreifen oder aus Angst vor Risiken einen Schritt zurücktreten. Gleichzeitig stellt sich die Frage, wem Nutzer:innen zutrauen, sie verlässlich über digitale Sicherheit aufzuklären und für Risiken zu sensibilisieren. Und auch das zeigt letzlich der Index: Dabei geht es nicht nur um die bloße Wissensvermittlung, sondern die zielgruppengenaue Unterstützung bei der Umsetzung von Maßnahmen im Alltag.

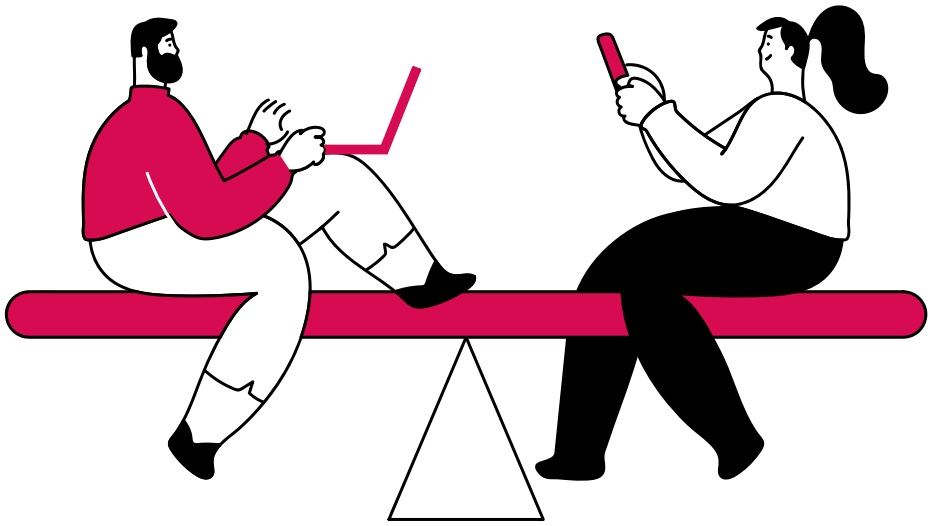
Nur wenn Nutzer:innen darauf vertrauen, dass Technologien, Dienste und auch das eigene Urteilsvermögen zuverlässig sind, werden sie aktiv für ihre Sicherheit sorgen. Fehlt dieses Vertrauen, drohen zwei Extreme: Entweder nutzen Menschen digitale Dienste gar nicht mehr – oder sie nutzen sie zwar, handeln aber fatalistisch und verdrängen die Risiken. Beide Reaktionen wären eine Gefahr für die digitale Zukunft. Daher gilt es, eine vertrauensvolle digitale Kultur zu fördern, in der Wachsamkeit und Zuversicht Hand in Hand gehen.

Ein Blick nach vorn zeigt dabei besondere Herausforderungen durch neue Technologien wie Künstliche Intelligenz (KI). KI hält Einzug in unseren Alltag – und stellt das Vertrauen der Verbraucher:innen auf die Probe. Aktuell halten nur 7,2 % der Internetnutzenden Ergebnisse von KI-Chatbots für sehr glaubwürdig. Damit schlagen sie immerhin Informationen aus sozialen Netzwerken (6,6 %) und Inhalten von Influencer:innen (6,0 %), liegen in puncto Vertrauen derzeit aber auf den hintersten Plätzen. Wenn KI-Anwendungen künftig breite Akzeptanz in der Gesellschaft finden sollen, müssen wir mehr tun, um Menschen nicht nur Vorbehalte zu nehmen, sondern sie zu befähigen, selbstbewusst realistische Risikoabschätzungen zu treffen. Es geht darum, das Verständnis über Funktionsweisen und Möglichkeiten, aber auch Gefahren digitaler Tools zu vermitteln. Nur dann gelingt es, im nächsten Schritt zu einer sicheren Nutzung im Alltag anzuleiten. Vertrauensbildung ist dabei nicht allein Aufgabe der Nutzer:innen.

Auch Unternehmen und Plattformen stehen in der Verantwortung, eine vertrauenswürdige digitale Umgebung zu schaffen. Vertrauen entsteht, wenn Technologien transparent, verlässlich und sicher gestaltet werden. Konkret heißt das zum Beispiel: Anbieter von Kommuni-kations-Apps könnten einen technischen Schutz vor stimmmanipulierten Betrugsanrufen integrieren oder zumindest Warnhinweise geben, wenn Unregelmäßigkeiten erkannt werden. Soziale Netzwerke und Medienplattformen können KI-generierte Bilder und Videos kennzeichnen, damit Nutzer:innen Fälschungen schneller erkennen.

Die Wirtschaft insgesamt hat ein großes Interesse an digitalem Vertrauen – denn es ist die Grundlage dafür, dass Menschen neue Dienste nutzen und Innovationen akzeptieren. Wenn Hersteller und Diensteanbieter höchsten Wert auf Datenschutz, IT-Sicherheit und Nachvollziehbarkeit von KI-Systemen legen, senden sie ein Signal: Ihr könnt unseren Produkten vertrauen. Die Politik kann das mit einem fairen rechtlichen Rahmen und klaren Regulierungen für alle Beteiligten unterstützen. Das nimmt Nutzer:innen die diffuse Angst vor dem Neuen und schafft die Basis dafür, dass sie digitale Angebote kompetent und verantwortungsbewusst einsetzen. Kurzum: Vertrauen ist eine gemeinsame Aufgabe.

Nutzer:innen, Wirtschaft und auch die Politik müssen an einem Strang ziehen, um Leitplanken für neue Technologien zu entwickeln, die Transparenz schaffen und Missbrauch eindämmen. Gelingt das, bleibt die digitale Transformation auf Kurs – getragen von Menschen, die den digitalen Wandel mit Zuversicht statt mit Zweifel gestalten.



Sicher die digitale Gegenwart und Zukunft gestalten

Angesichts all dieser Herausforderungen kommt es jetzt darauf an, ins Handeln zu kommen. Der Abwärtstrend der digitalen Sicherheitslage in Deutschland braucht dringend Antworten. Wir brauchen neue Anreize, um digitale Kompetenzen zu fördern, Vertrauen zu stärken und alle Bürger:innen mitzunehmen.

Die zentrale Botschaft des DsiN-Sicherheitsindex 2025 ist klar: Die Wissens-Verhaltensschere im digitalen Raum muss endlich nachhaltige Antworten von Anbietern und Aufklärungs-Akteuren finden. Vertrauen ist dafür eine zentrale Voraussetzung. Der Index zeigt: Immer mehr regelmäßige Alltagsuser:innen drohen, bei der digitalen Sicherheit abgehängt zu werden. Deshalb dürfen wir nicht nur außenstehende und fatalistische Nutzer:innen stärken, sondern müssen digitale Sicherheit wieder stärker in die Breite tragen, um alle Menschen mit ihren individuellen Bedürfnissen fit zu machen für unsere digitale Gesellschaft. Wichtig dabei: Die vielen bereits engagierten Akteur:innen und Netzwerke bieten eine unerlässliche Grundlage, um Menschen für das Thema zu erreichen.

Multiplikator:innen befähigen und Wissensvermittlung ausbauen
Wie es gelingen kann, aus unsicheren Nutzer:innen sogar Multiplikator:innen für digitales Sicherheitswissen zu machen, zeigt unter anderem der Digital-Kompass (das folgende Fallporträt wurde zur Wahrung der Anonymität aus mehreren realen Fällen zusammengesetzt): Frau S. ist 68 Jahre alt und war vor einem Jahr noch unsicher im Umgang mit digitalen Medien. Dann schloss sie sich dem Digital-Kompass an, der ältere Menschen bei der sicheren Internetnutzung unterstützt.

Anfangs ließ sie sich von einem ehrenamtlichen Internet-Lotsen zeigen, wie man auf dem Smartphone Nachrichten nur in vertrauenswürdigen Gruppen teilt und Phishing-Mails erkennt. Sie war erstaunt, wie viel sicherer sie sich mit ein paar einfachen Verhaltensregeln fühlte. Mit der Zeit wuchs ihr Selbstvertrauen so weit, dass sie selbst aktiv wurde. Inzwischen gibt Frau S. ihr Wissen als ehrenamtliche Trainerin an andere Senior:innen weiter. Ihr Lieblingsmoment ist, wenn eine ältere Teilnehmerin lachend feststellt: „So schwer ist das ja gar nicht!“ – ein Aha-Erlebnis, das Frau S. nur zu gut nachempfinden kann.

So wirkt digitale Kompetenzförderung nachhaltig: Ein Mensch wird befähigt und gibt dieses Wissen an andere weiter. Aus Unsicherheit wird Schritt für Schritt digitale Souveränität.

DsiN-Aktionsplan für mehr IT-Sicherheit im Alltag
Für Deutschland sicher im Netz leiten sich aus dem Sicherheitsindex drei zentrale Handlungsfelder ab, in denen jetzt gemeinsames Handeln gefragt ist, um den Abwärtstrend der digitalen Sicherheitslage umzudrehen.

#1 Netzwerke stärken – Wissen teilen

DsiN bringt Akteur:innen aus Politik, Wirtschaft und Zivilgesellschaft zusammen, um digitales Wissen verständlich und praxisnah aufzubereiten. Unser Ziel: Menschen dort erreichen, wo sie stehen – und sie befähigen, digitale Chancen sicher zu nutzen. Ein Beispiel dafür ist der Digitalführerschein (DiFü): Als etablierte Lernplattform mit einer aktiven Nutzerbasis vermittelt er zentrale Kompetenzen der IT-Sicherheit – einfach, alltagsnah und wirksam.

#2 Vertrauen stärken – Ängste abbauen

DsiN-Angebote wie der Digitale Engel und der Digital-Kompass, die sich an ältere Menschen richten, der Jugendwettbewerb myDigitalWorld oder Politiker:innen sicher im Netz haben in den letzten Jahren Vertrauen geschaffen. Dieses Vertrauen wollen wir gezielt nutzen, um Menschen für IT-Sicherheit im Alltag zu sensibilisieren – verständlich, nahbar und alltagsrelevant. Denn nur wenn Vertrauen da ist, können Sicherheitsmaßnahmen nachhaltig verankert werden.

#3 Sicherheit stärken – digitale Teilhabe ermöglichen

Praktische Materialien wie die DsiN-Ratgeberreihe oder die SiBa-App unterstützen Menschen dabei, digitale Risiken besser einzuschätzen und sicher zu handeln – im Alltag und in der Arbeitswelt. Sie bieten Orientierung und stärken die digitale Selbstbestimmung. Auch Multiplikator:innen profitieren: Mit diesen Tools können sie ihr Wissen gezielt weitergeben und andere bei einer sicheren digitalen Teilhabe begleiten.

Weiterführende DsiN-Angebote zum DsiN-Sicherheitsindex gibt es hier:

https://sicher-im-netz.de/sicherheitsindex-best-practice/

Impressum

DsiN-Sicherheitsindex 2025
Studie von Deutschland sicher im Netz e. V. zur digitalen Sicherheitslage von Verbraucher:innen in Deutschland

Verantwortlich: Joachim Schulte, Isabelle Rosière
Redaktion: Jan Lietz, Denis Schröder
Studienpartner: ARIX Business Intelligence GmbH
Studienbegleitung: Tobias Weber (ARIX), Michael Weinzierl (ARIX)
Gestaltung und Infografiken: KRAUT & KONFETTI

Deutschland sicher im Netz e. V.
Albrechtstraße 10c
10117 Berlin
Telefon: +4930767581–500
www.sicher-im-netz.de
info@sicher-im-netz.de

Bildquellen:
Die Illustrationen des Covers und der vier Kapiteltrenner sind mit dem Text-zu-Bild-Generator DreamStudio erstellt worden.

1. Auflage, Juni 2025

sicher-im-netz.de

Mit Unterstützung von:

kleinanzeigen