DsiN SICHERHEITS-INDEX 2022

Digitale Sicherheitslage von Verbraucher:innen in Deutschland

FOKUSTHEMA

KÜNSTLICHE INTELLIGENZ

DsiN-Schirmherrschaft:

Bundesministerium des Innern und für Heimat

Studien-Schirmherrschaft:

Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz

Eine Studie von

DsiN Deutschland sicher im Netz

Über Deutschland sicher im Netz e.V.

DsiN erreicht mit seinen Projekten und Initiativen jeden Monat über 100.000 Menschen im Dialog: konkrete Hilfsangebote befähigen Verbraucher:innen sowie Selbstständige und kleinere Unternehmen zum sicheren Umgang mit dem Internet. Der gemeinnützige Verein wurde 2006 im IT-Gipfelprozess der Bundesregierung (heute: Digital-Gipfel) initiiert und steht seit 2007 unter der persönlichen Schirmherrschaft der Bundesministerin des Innern und für Heimat. Als herstellerüber-greifende Plattform wird DsiN von engagierten Unternehmen und zivilgesellschaftlichen Initiativen getragen.

Impressum

DsiN-Sicherheitsindex 2022
Studie von Deutschland sicher im Netz e.V. zur digitalen Sicherheitslage von Verbraucher:innen in Deutschland

Verantwortlich: Dr. Michael Littger
Redaktion: Nadine Berneis (Leitung), Manfred Rump, Anna-Leona Bösl
Studienbegleitung: Tobias Weber (KANTAR), Michael Weinzierl (KANTAR)
Studienpartner: KANTAR GmbH
Gestaltung und Infografiken: KRAUT & KONFETTI

Deutschland sicher im Netz e.V.
Albrechtstraße 10c
10117 Berlin
Telefon: +49 30 767581 – 500
Telefax: +49 30 767581 – 509
www.sicher-im-netz.de
info@sicher-im-netz.de

Bildquellen:
Titel: Moyo Studio / iStock; Grußwort: Bundesregierung/Jesco Denzel; Vorwort: Michael Littger/DsiN, Udo Littke/Atos; Kapitel 1: stockfour / iStock; Kapitel 2: AnnaStills / iStock; Seite 28: miniseries / iStock; Kapitel 3: golero / iStock; Seite 50: AsiaVision / iStock; Kapitel 4: Nomad / iStock

1. Auflage, Juni 2022

sicher-im-netz.de

Dr. Bettina Hoffmann

Grußwort

Digitale Souveränität stärken – gesellschaftliche Teilhabe ermöglichen

Die Digitalisierung ist ein fester Bestandteil unseres Lebens und besitzt enorme Potenziale für unsere Gesellschaft. Sie kann den Alltag der Menschen erleichtern, neue Tätigkeitsfelder eröffnen und soziale Teilhabe ermöglichen. Allerdings wächst mit zunehmender Verbreitung und Vielfalt digitaler Anwendungen auch das Risiko potenzieller Bedrohungen – und damit die Relevanz von IT-Sicherheitsfragen. IT-Schutz bildet schließlich das Fundament für eine digitale Souveränität der Verbraucher:innen und ebnet damit den Weg für selbstbestimmtes Handeln in einer vernetzten Gesellschaft.

Während sich einige Verbraucher:innen den wandelnden Anforderungen bereits souverän anpassen und auf Sicherheitsrisiken adäquat reagieren können, verfügt ein Großteil der Menschen noch nicht über das ausreichende Sicherheitswissen und -verhalten für einen umfassenden Schutz bei alltäglichen digitalen Aktivitäten. Wie können wir die digitalen Kompetenzen der Verbraucher:innen nachhaltig stärken? Welche Defizite muss die Aufklärungsarbeit konkret adressieren und wie sieht eine zeitgemäße digitale Aufklärung angesichts der sich wandelnden Lebenswelten aus?

Die Ergebnisse in diesem Jahr zeigen: Die Bedeutung von Aufklärungsarbeit steigt. Die Anzahl der Sicherheitsvorfälle hat sich stark erhöht und lässt den Gesamtindex auf einen Tiefstwert von 59,8 Punkten fallen. Souveräne Nutzer:innen passen sich dieser gestiegenen Bedrohungslage besser an und eignen sich als Vorbilder digitaler Selbstbestimmung. Das Gros der Verbraucher:innen muss allerdings noch wirksamer dazu motiviert und befähigt werden, das Sicherheitswissen auch in die Praxis umzusetzen.

Es bedarf individueller Ansprachen, aufsuchender Aufklärung und niedrigschwelliger Angebote – regional vor Ort und digital im Netz. Dafür engagiert sich das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz in vielfältiger Weise. Für Menschen in der Seniorenarbeit, eine Bevölkerungsgruppe, die mir besonders am Herzen liegt, wendet sich der Digital-Kompass von Deutschland sicher im Netz e.V. gemeinsamen mit der Bundesarbeitsgemeinschaft der Seniorenorganisationen (BAGSO) mit einem regionalen Angebot an 100 Standorten in Deutschland. Ich freue mich, dass wir hier auch künftig neue Ansätze finden werden, verstärkt vulnerable Zielgruppen gemeinsam in den Blick zu nehmen. Mit dem neuen DsiN-Digitalführerschein (DiFü), den wir ebenfalls sehr begrüßen, werden wir darüber hinaus mehr Menschen erreichen, digitale Basiskompetenzen zu erwerben.

Digitale Aufklärung muss sich fortwährend an die neuen Anforderungen des digitalen Wandels anpassen – und erfordert das Engagement aller Akteur:innen, denen der sichere Umgang mit der Digitalisierung ein Anliegen ist. Daher wünsche ich mir, dass viele weitere Partner und Menschen den Weg zur digitalen Aufklärungsarbeit mit DsiN finden – für ein verbraucherfreundliches und hilfreiches Internet.

In diesem Sinne bedanke ich mich bei Deutschland sicher im Netz e.V. und seinen Mitgliedern für ihren Beitrag und freue mich auf die weitere Zusammenarbeit.

Ich wünsche allen Leserinnen und Lesern eine aufschlussreiche Lektüre!

Dr. Bettina Hoffmann

Dr. Bettina Hoffmann
Parlamentarische Staatssekretärin bei der Bundesministerin für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz

Vorwort

Liebe Leserinnen und Leser,

Dr. Michael Littger

Udo Littke

der DsiN-Sicherheitsindex 2022 wirft einen Blick auf die Sicherheitslage der Internetnutzenden im zweiten Jahr der Corona-Pandemie. Unter dem Eindruck einer digitalen Erschöpfung – tatsächlich waren Menschen zuletzt seltener im Netz aktiv als noch vor einem Jahr – hat sich auch die Sicherheitslage in vielfältiger Weise verschlechtert: Mit 59,8 Prozent erreicht der Index den niedrigsten Wert seiner Messungen!

Hinter dem Indexwert verbergen sich unterschiedliche Entwicklungen, die die Vielfältigkeit der Menschen im Internet bekräftigt und damit auch die Anforderungen an unsere Aufklärungsarbeit: Die Sicherheitslagen der Außenstehenden und Fatalisten haben sich deutlich verschlechtert, was in erster Linie auf eine massive Zunahme von erlebten Sicherheitsvorfällen zurückzuführen ist. Zwar haben auch die Nutzergruppen der Antreibenden und Bedachtsamen mehr Angriffe erfahren. Sie konnten sich jedoch wirksamer schützen und ihr Sicherheitsniveau damit fast konstant halten.

Damit zeigt der DsiN-Sicherheitsindex im Zeichen von Corona auf anschauliche Weise, dass die Sicherheitslage zunehmend vom Faktor Mensch abhängig ist. Mit anderen Worten: unter den selben regulativen und technologischen Rahmenbedingungen gelingt es einigen Bevölkerungsteilen, sich recht sicher im Netz zu bewegen (40,0 Prozent), während ein nicht unerheblicher Anteil von 23,0 Prozent unter dem kritischen Schwellenwert von 50 Indexpunkten fällt. Rund 37,0 Prozent liegen mit einem Indexwert von rund 58,0 Punkten im mäßigen Mittelfeld.

Welche zwei Lehren ziehen wir aus dieser Erkenntnis? Erstens, digitale Aufklärungsarbeit ist notwendiger als jemals zuvor: wenn das digitale Sicherheitsgefälle in Deutschland reduziert werden soll, gehört die dazugehörige Arbeit zu den zentralen Aufgaben unserer Zeit. Und zweitens folgt daraus eine weitere Professionalisierung der Aufklärungsarbeit, die nach unserer Überzeugung eine deutliche Klärung von Rollen und Aufgaben erfordert. Mit unseren reichweitenstarken Transferprojekten erreichen wir schon heute jeden Monat über 100.000 Menschen. Durch die Zusammenarbeit mit engagierten Akteuren aus der Wirtschaft, der Verwaltung und Wissenschaft können wir diese Erfolge weiter ausbauen.

Bitte werfen Sie auch einen Blick auf den neuen Fokus der diesjährigen Studie: Künstliche Intelligenz (KI). Während diese Technologie längst Einzug in unseren Alltag gefunden hat, ist sie für viele Verbraucher:innen ein noch wenig vertrautes „Neuland“ – grundsätzliches Wissen ist zwar mehrheitlich vorhanden, das Vertrauen dagegen noch ausbaufähig. Die Studie zeigt neben den Vorteilen auch Vorbehalte auf, die die Menschen im Umgang mit „KI“ heute wahrnehmen. Wir wollen das Thema daher künftig stärker – auch mit dem diesjährigen Studienpartner und neuem DsiN-Mitglied Atos – in die Aufklärungsarbeit von DsiN aufnehmen, dem „Neuland“ eine „Neugierde“ entgegensetzen. Denn Vertrauen und sicheres Verhalten beginnt auch bei KI oftmals mit einem Gespräch und verständlichen Antworten.

Wir wünschen eine aufklärende Lektüre.

Dr. Michael Littger
Geschäftsführer Deutschland sicher im Netz e.V.

Udo Littke
Geschäftsführer von Atos Deutschland

Inhalt

Toptrends 2022: mehr Bedrohungen bei unzureichendem Schutzniveau

Der DsiN-Sicherheitsindex liefert jährlich Antworten auf zwei Fragen: Wie steht es um die digitale Sicherheitslage von Verbraucher:innen in Deutschland und was ist erforderlich, um diese zu verbessern? Die Sicherheitslage wird dabei in einem Indexwert auf einer Skala von 0 bis 100 abgebildet.

Index 2022 fällt auf neuen Tiefstwert (59,8 Punkte)
Nachdem der Index im letzten Jahr leicht um 0,1 Indexpunkte zurückging, verringert er sich in diesem Jahr deutlich um 2,9 Indexpunkte und fällt damit auf den bisher tiefsten gemessenen Wert von 59,8. Die Sicherheitslage der deutschen Internetnutzer:innen erreicht so ihr niedrigstes Niveau seit Beginn der Erhebung 2014. Grund hierfür ist vor allem der starke Anstieg der Sicherheitsvorfälle (+8,3 Punkte) auf einen neuen Höchstwert von 43,4. Dementsprechend steigt auch das Verunsicherungsgefühl (+1,2 Punkte).

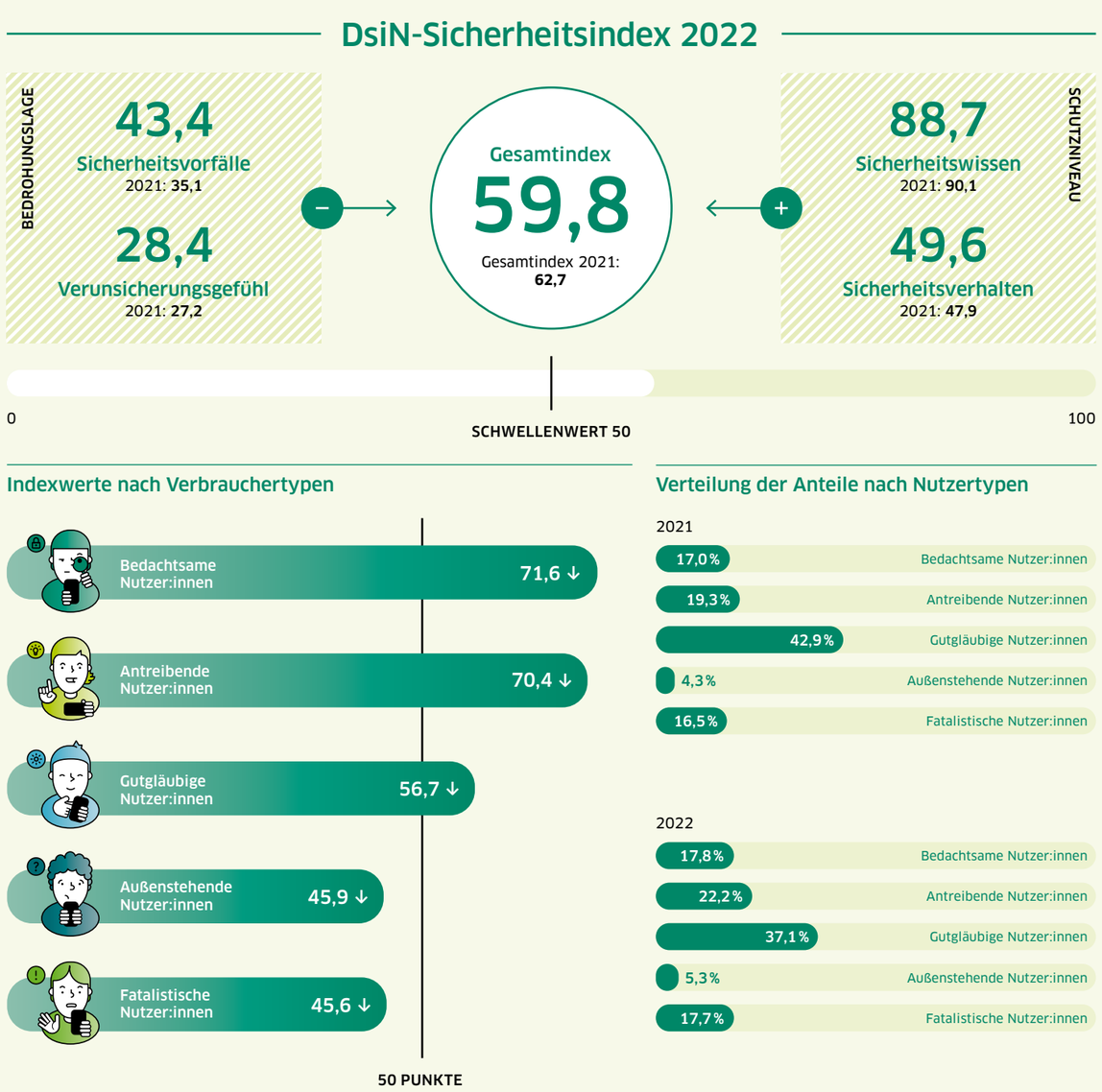
Sicherheitsverhalten und -niveau stagnieren
Die verschärfte Bedrohungslage trifft auf ein stagnierendes Schutzniveau. Das Sicherheitsverhalten hat sich in diesem Jahr mit einem Wert von 1,7 auf 49,6 Punkte nur leicht verbessert, das Sicherheitswissen dagegen ist um 1,4 Punkte gesunken. Dieser Stillstand markiert angesichts der gestiegenen Bedrohungslage einen Rückschritt und bestätigt die Warnungen von DsiN aus vorangegangen Publikationen: Wenn die Sicherheitsvorfälle steigen, ist das Schutzniveau nicht ausreichend entwickelt, um Verbraucher:innen angemessen zu schützen.

Eine Aufklärungsarbeit muss deshalb noch stärker auf die Handlungsfähigkeit und Anpassungskompetenz hinwirken, damit sich Verbraucher:innen im Sinne einer Cyberresilienz Gefahrensituationen selbstständig anpassen können. Verbraucher:innen sind mit ihrem Verhalten ein Baustein im Sicherheitskonzept und erkennen auch ihre Eigenverantwortung, gerade im vorsichtigeren Umgang mit den eigenen persönlichen Daten (77,7 Prozent). Dennoch nehmen Nutzer:innen auch Politik und Wirtschaft in die Pflicht – mehr dazu in Kapitel 1.

Das IT-Sicherheitsgefälle vergrößert sich
Auch die Indexwerte der Nutzersegmente weisen allesamt eine Tendenz nach unten auf. Am stärksten sinkt der Index bei den Fatalist:innen mit -7,3 auf 45,6 Punkte. Antreibende und bedachtsame Verbraucher:innen bleiben trotz eines Rückgangs um 1,2 Punkte die souveränen Verbraucher:innen und erreichen mit 70,4 bzw. 71,6 Punkten die Höchstwerte. Bei steigenden Sicherheitsvorfällen können sie ihr Sicherheitsverhalten ausbauen (+3,2 und +6,7) und damit deutlich besser auf die Bedrohungslage reagieren als die übrigen Verbrauchertypen. Diese Anpassungsfähigkeit gilt es in der Aufklärungsarbeit als besonders wirksame Schutzfähigkeit zu fördern – mehr dazu in Kapitel 2.

Fokusthema 2022: Künstliche Intelligenz
Nach den Fokusthemen Digitale Identität und Digitales Ich (2021) und Bürgerportale (2020) rückt in diesem Jahr das Thema „Künstliche Intelligenz“ (KI) in den Fokus. Für viele Nutzer:innen ist dieses Gebiet noch weitgehend unbekannt. Nur 59 Prozent der Befragten wissen, was man darunter versteht, obgleich KI in vielen Lebensbereichen bereits genutzt wird, etwa in der Kommunikation mit Textnachrichten (41,5 Prozent), beim Übersetzen (41 Prozent) und Navigieren (37,7 Prozent). 28,5 Prozent der Befragten sehen in KI eine Chance, etwa ebenso viele eine Gefahr (28,6 Prozent) – mehr dazu in Kapitel 3.

Abb. 1 / Sicherheitsindex 2022
DsiN-Sicherheitsindex 2022 – digitale Sicherheitslage der Verbraucher:innen in Deutschland



Digitales Sicherheitsgefälle – abbauen durch digitale Aufklärung

Bedrohungslage verbessern! → Dialoge stärken, Transfer vereinfachen, Akteur:innen einbinden → Schutzniveau erhöhen!

Facts und Figures aus dem Index

Allgemein zum Index

Index auf dem tiefsten gemessenen Wert von

59,8 ↓

PUNKTEN

Rückgang in diesem Jahr

2022

2,9 Punkte ↓

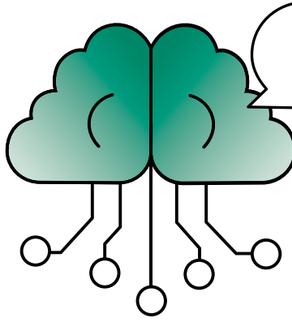
Rückgang im letzten Jahr

2021

0,1 Punkte ↘

!!!

Sicherheitslage der deutschen Internetnutzer:innen erreicht ihr **niedrigstes Niveau** seit Beginn der Erhebung 2014.



Fokusthema: **Künstliche Intelligenz (KI)**

59 % haben Kenntnisse, was man unter dem Thema „Künstliche Intelligenz" versteht.

Am Thema KI scheiden sich die Geister: **Chance (28,5 %) oder Gefahr (28,6 %)?**

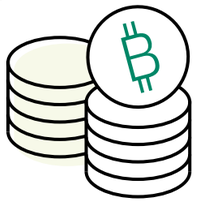
50,1 % fordern, dass KI nicht ohne Menschen Entscheidungen treffen können soll.

→ Seite 32 – 33

+3,7 % ↑

Betrug mit virtuellen Währungen

→ Seite 12



FATALISTISCHE NUTZER:INNEN

→ Seite 18

AUSSENSTEHENDE NUTZER:INNEN

→ Seite 20

GUTGLÄUBIGE NUTZER:INNEN

→ Seite 22

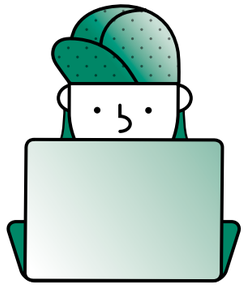
ANTREIBENDE NUTZER:INNEN

→ Seite 24

BEDACHTSAME NUTZER:INNEN

→ Seite 26

Digitale Sicherheitslage 2022 verschlechtert sich für alle fünf Verbrauchertypen



Digitales Ich

52,2 % glauben, dass sie als „gläserne Konsument:innen" nichts verbergen können.

Größte Risiken: Banking (**57,6 %**), Shopping (**57,3 %**) und Social Media (**56,6 %**)

Wunsch nach Aufklärung in der Schule: **76 %** meinen, dass das Thema **Digitales Ich** in der Schule behandelt werden müsste.

→ Seite 34 – 35

24,6 %

Digitale Bürgerportale

Gut ein Viertel der Befragten (**24,6 %**) nutzt digitale Bürgerportale. Das ist ein Plus von **7,5 Prozentpunkten** zum Vorjahr (**17,1 %**).

→ Seite 36 – 37

Smarte Versicherungstarife

34,1 %

können sich vorstellen, einen smarten Versicherungstarif in Anspruch zu nehmen. Das ist ein Zuwachs von **5,2 Prozentpunkten**.

→ Seite 38 – 39

Digitale Vernetzung

Die Vorfälle durch Mobbing sind um 2 Prozentpunkte auf **11,1 %** angestiegen.

→ Seite 40 – 41

Einkaufen im Internet

Ein Viertel der Verbraucher:innen (**25 Prozent**) halten Onlineshopping/Reisebuchungen für gefährlich oder sehr gefährlich. 2021 war es nur jede:r Fünfte (**20,7 Prozent**).

→ Seite 46 – 47

Digitale Gesundheits- und Fitnessdienste

Das höchste Risiko besteht für die Befragten zu **58,6 %** im Sammeln und Analysieren von personenbezogenen Gesundheitsdaten in Datenbanken (**+0,9 Prozentpunkte**).

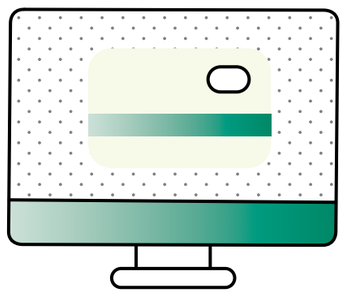
→ Seite 40 – 41

Das vernetzte Zuhause

11%

Haustechnik wird beliebter: das vernetzte Zuhause nutzen **11 %** (+0,7 Prozentpunkte zum Vorjahr).

→ Seite 44 – 45



Onlinebanking

Nur **58,5 %** der befragten Nutzer:innen achten auf eine verschlüsselte Datenverbindung beim Austausch sensibler Daten. Ein Jahr zuvor waren es noch **63,0 %**.

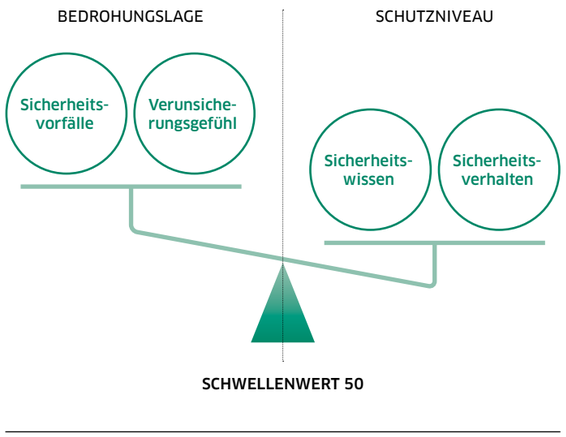
→ Seite 48 – 49

Cyberresilienz Anpassungsfähigkeit als Schlüsselkompetenz

→ Seite 28 – 29, 54 – 55

Ziel und Methode: Wie sicher ist Deutschland im Netz?

Abb. 2 / Sicherheitsindex 2022
Berechnung des DsiN-Sicherheitsindex: Verhältnis zwischen Bedrohungslage und Schutzniveau



Die jährliche Verbraucherstudie* von Deutschland sicher im Netz e. V. untersucht die digitale Sicherheitslage von deutschen Internetnutzer:innen und bildet diese auf einer Skala von 0 bis 100 in einer zentralen Kennziffer ab: dem DsiN-Sicherheitsindex.

Seit nunmehr neun Jahren zeigen die repräsentativen Ergebnisse des DsiN-Sicherheitsindex Entwicklungen, Trends und Bedarfe der IT-Sicherheitslage in Deutschland auf. Mehr als 2.000 Verbraucher:innen über 16 Jahren werden hierbei befragt. Die Verbraucherstudie erfolgt in Zusammenarbeit mit dem Markt- und Meinungsforschungsinstitut KANTAR.

Bedrohungslage vs. Schutzniveau
Um die Sicherheitslage der Internetnutzer:innen abzubilden, wird die Bedrohungslage der Verbraucher:innen ihrem Schutzniveau gegenübergestellt.

Die Bedrohungslage wird aus zwei Faktoren berechnet: Zum einen berichten Nutzer:innen von erlebten **Sicherheitsvorfällen**. Zum anderen geben die Befragten ihr Gefühl eines subjektiven Risikos im Umgang mit digitalen Diensten und Technologien (**Verunsicherungsgefühl**) an. Beide Werte zur Bedrohungslage wirken sich negativ auf den Gesamtindexwert aus.

Auch das Schutzniveau ergibt sich aus zwei Sicherheitsfaktoren: Zum einen geben Nutzer:innen Auskunft zu ihrem **Sicherheitswissen**, also der Kenntnis möglicher Schutzmaßnahmen, und zum anderen zu ihrem konkreten **Sicherheitsverhalten,** zum Beispiel der Verwendung einer Zwei-Faktor-Authentisierung oder der Nutzung von Sonderzeichen in Passwörtern etc. Der Wert für das Schutzniveau beeinflusst den Gesamtindexwert positiv.

Alle vier Sicherheitsfaktoren werden auf einer Skala von 0 bis 100 gemessen. Der Gesamtindexwert wird letztendlich ermittelt, indem die Bedrohungslage mit dem Schutzniveau der Verbraucher:innen ins Verhältnis gesetzt wird. Je höher der Indexwert ist, desto sicherer sind deutsche Nutzer:innen im Netz. Liegt der Gesamtwert über 50 Indexpunkten, überwiegt das Schutzniveau der User:innen. Bei einem Wert darunter überwiegt die Bedrohungslage und die Sicherheitslage kippt.

Fünf Verbrauchertypen und digitale Lebenswelten
Der DsiN-Index unterscheidet auf Grundlage der Sicherheitslage der Internetnutzer:innen fünf verschiedene Verbrauchertypen (Kapitel 2). Sie bilden die Basis für eine bedarfsorientierte Aufklärungsarbeit.

Die Untersuchung der Sicherheitslage im Internet umfasst außerdem praxisorientierte, digitale Lebenswelten, um spezielle Bedarfe von Nutzer:innen in Alltagskontexten zu beleuchten. Das diesjährige Fokusthema ist „Künstliche Intelligenz“ (Kapitel 3).

*Die im weiteren Verlauf erwähnten Begriffe wie „Verbraucherstudie“, „Verbrauchertyp“ oder „Nutzergruppe“ schließen sowohl das männliche, weibliche als auch diverse Geschlecht ein. Zur besseren Lesbarkeit wird die gängige Schreibweise verwendet.

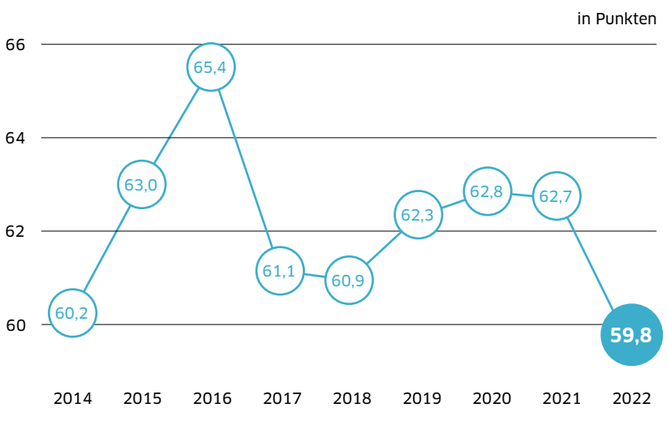
Kapitel 1

Sicherheitsindex 2022: 59,8 Punkte

Mit 59,8 Punkten verschlechtert sich die Sicherheitslage deutlich

Der Indexwert rutscht in diesem Jahr ab und landet mit 59,8 Punkten erstmals unter 60 Indexpunkten. Nach einem leichten Rückgang des Gesamtindex 2021 um 0,1 Indexpunkte verweist die Einbuße von 2,9 Punkten im Jahr 2022 auf eine deutlich verschlechterte Sicherheitslage. So erreichen die Sicherheitsvorfälle (43,4) ihren bisherigen Höchstwert, und zugleich wächst das Verunsicherungsgefühl (28,4). Weil das Sicherheitsverhalten nur leicht zulegen kann und das Sicherheitswissen erstmals sinkt, fällt die Diskrepanz zwischen Bedrohungslage und Schutzniveau besonders deutlich aus.

Abb. 3 / Sicherheitsindex 2022
Digitale Sicherheitslage im Neunjahresvergleich



Die Berechnung des Sicherheitsindex basiert auf vier Faktoren: Zwei Faktoren betreffen die Bedrohungslage, die beiden anderen Faktoren die Abwehrkompetenz sowie das daraus resultierende Schutzverhalten der Verbraucher:innen. Hier lassen sich 2022 folgende Veränderungen verzeichnen.

Entwicklungen der Bedrohungslage durch IT bei Verbraucher:innen

- Sicherheitsvorfälle: 43,4 Punkte (+8,3). Nach einer abnehmenden Tendenz seit 2019 steigt der Wert wieder an und erreicht mit 43,4 Indexpunkten einen neuen Höchststand. Dies hat eine maßgebliche Auswirkung auf den Gesamtindex.
- Verunsicherungsgefühl: 28,4 Punkte (+1,2). Die gestiegene Zahl der Sicherheitsvorfälle wirkt sich offenbar auch auf das Verunsicherungsgefühl aus. Es steigt mit 1,2 Punkten auf 28,4 und liegt damit aber immer noch deutlich unter dem bisherigen Höchstwert von 29,6 Punkten im Jahr 2020.

Entwicklungen des IT-Schutzniveaus von Verbraucher:innen

- Sicherheitswissen: 88,7 Punkte (-1,4). Die Sicherheitskompetenz entwickelt sich nach einem permanenten Anstieg auf zuletzt 90,1 Punkte erstmals rückläufig. Mit 88,7 Punkten fällt das Sicherheitsniveau fast auf den Wert von 2019 (88,6) zurück.
- Sicherheitsverhalten: 49,6 Punkte (+1,7). Trotz des gesunkenen Sicherheitswissens ist das Sicherheitsverhalten 2022 auf 49,6 Punkte angestiegen.

Handlungsbedarf bei der Wissens-Verhaltens-Lücke

Lediglich die zwei souveränen Verbrauchertypen verzeichnen Anstiege im Sicherheitsverhalten (Bedachtsame: +6,7; Antreibende: +3,2). Bei den übrigen fällt dieser Wert – und das bei einem insgesamt rückläufigen Sicherheitswissen. Die Wissens-Verhaltens-Lücke bleibt damit angesichts der allgemein verschärften Bedrohungslage insgesamt zu groß.

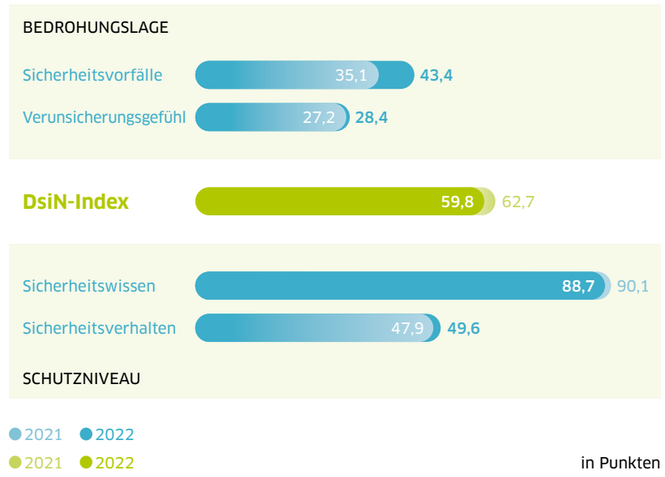
Exkurs: Eigenverantwortung, aber auch Politik und Wirtschaft gefragt

Verbraucher:innen sehen die Verantwortung für Onlinesicherheit wie bereits 2021 allen voran bei sich selbst. Das betrifft insbesondere den vorsichtigeren Umgang mit den eigenen persönlichen Daten (77,7 Prozent) sowie das häufigere Umsetzen des eigenen Sicherheitswissens (72,6 Prozent). Die Verbraucher:innen erneuern aber zugleich ihren Wunsch nach strengeren Gesetzen durch den Gesetzgeber (61,4 Prozent) und fordern eine schärfere Verfolgung von Gesetzesverstößen (76 Prozent). Auf Herstellerseite ist den Nutzer:innen daran gelegen, dass Dienste und Programme (68,2 Prozent) sowie Geräte (66,2 Prozent) sicherer gestaltet werden.

Niedrigschwellige Angebote für mehr Sicherheitswissen und Motivation

Um ihr Wissen zu verbessern, fordern Verbraucher:innen Informationen, die noch verständlicher (63,5 Prozent) sowie zentral auffindbar sind, zum Beispiel durch Bündelung auf einer Website (62,6 Prozent), und im beruflichen oder schulischen Aus- bzw. Weiterbildungsbereich vermittelt werden (59,6 Prozent). Auch das Risikobewusstsein ließe sich steigern, wenn der Umgang mit Risiken und Chancen bereits in der Schule eingebunden würde (69,4 Prozent). Niedrigschwelligkeit wird ebenfalls gegenüber der IT-Anbieterseite gefordert: Einfache Sicherheitseinstellungen bei Programmen und Geräten stellen für Nutzer:innen nach wie vor die größte Motivation (67 Prozent) dar, um sich sicher im Internet zu bewegen.

Abb. 4 / Sicherheitsindex 2022
Übersicht Index und Faktoren 2022



Entwicklungen 2022 bei den vier DsiN-Sicherheitsfaktoren

BEDROHUNGSLAGE
AUS SICHT VON
VERBRAUCHER:INNEN

SCHUTZNIVEAU
AUS SICHT VON
VERBRAUCHER:INNEN

1.

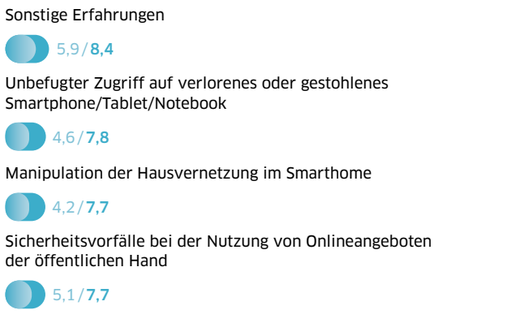
Registrierte Sicherheitsvorfälle

In nahezu allen abgefragten Bereichen beklagen Verbraucher:innen mehr Sicherheitsvorfälle als im Vorjahr. Mit Scam und Phishing per SMS steigen zwei Bedrohungen in die Liste der fünf häufigsten Bedrohungen ein, die 2022 erstmals im Index abgefragt wurden. Unbefugte Ortung der eigenen Mobilgeräte (+4,1 Prozentpunkte), Betrug mit virtuellen Währungen (+3,7 Prozentpunkte) und Manipulation von Hausvernetzung (+3,5 Prozentpunkte) verzeichnen im Vorjahresvergleich die größten Zuwächse.

Abb. 5 / Sicherheitsindex 2022

Die häufigsten IT-Sicherheitsvorfälle

Die Schlusslichter unter den IT-Sicherheitsvorfällen



in % 2021 2022

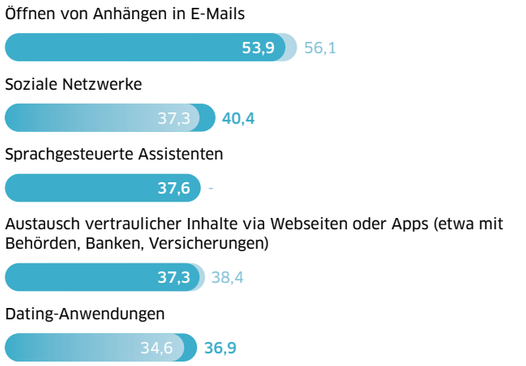
2.

Verunsicherungsgefühl im Internet

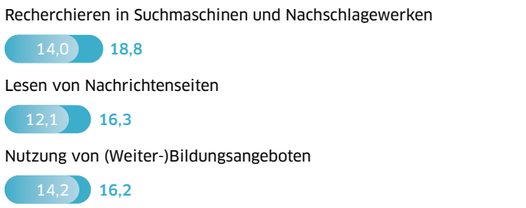
Das Verunsicherungsgefühl hat sich bei einem Großteil der abgefragten Aktivitäten erhöht. Spitzenreiter bleibt wie im Vorjahr das Öffnen von Anhängen in E-Mails (53,9 Prozent). Als zweitgefährlichste Tätigkeit mit 40,4 Prozent werden von den Nutzer:innen soziale Netzwerke eingestuft. Auf Position drei folgen die in diesem Jahr neu aufgenommenen sprachgesteuerten Assistenten (Siri, Alexa, Google Home etc.) mit 37,6 Prozent.

Abb. 6 / Sicherheitsindex 2022

Dabei fühlen sich Nutzer:innen am unsichersten



Dabei fühlen sich Nutzer:innen am wenigsten unsicher



in % 2021 2022

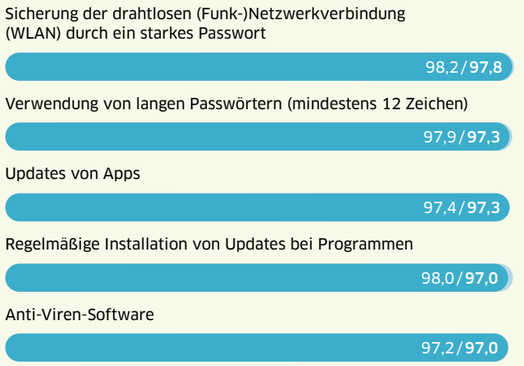
3.

Sicherheitswissen bei Verbraucher:innen

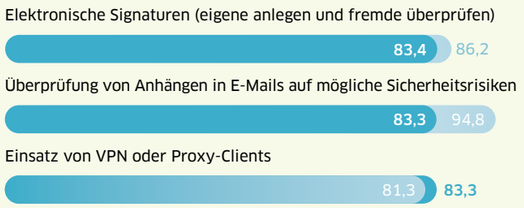
Beim Sicherheitswissen hat sich das Ranking auch 2022 wieder deutlich verändert. Neu auf der Spitzenposition ist der letztjährige Zweitplatzierte, die Sicherung der drahtlosen (Funk-)Netzwerkverbindung (WLAN) (97,8 Prozent). Am unbekanntesten bleibt mit 83,3 Prozent die Nutzung von VPN oder Proxy-Clients, die sich mit dem Überprüfen von Anhängen in E-Mails auf mögliche Sicherheitsrisiken (zum Beispiel Schadsoftware) den letzten Platz teilt.

Abb. 7 / Sicherheitsindex 2022

Die bekanntesten Sicherheitsmaßnahmen



Die unbekanntesten Sicherheitsmaßnahmen



in % 2021 2022

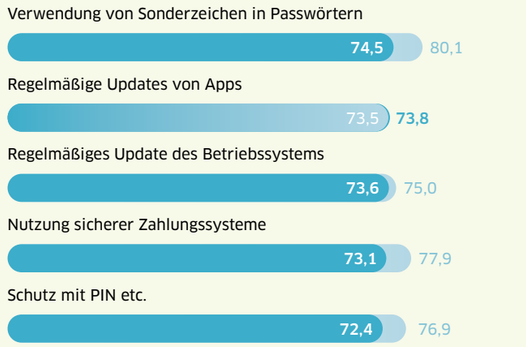
4.

Sicherheitsverhalten im Alltag

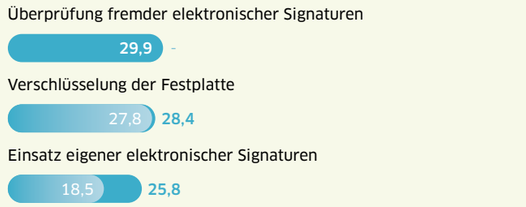
Die Nutzung des Sicherheitswissens bleibt an der Spitze unverändert. Das Verwenden von Sonderzeichen in Passwörtern führt auch das diesjährige Ranking an, trotz Rückgangs von 5,6 Prozentpunkten. Generell ist das Sicherheitsverhalten bei der Mehrheit der abgefragten Aktivitäten rückläufig. Am stärksten ist dies im Vergleich zum Vorjahr beim Log-out von Onlineaccounts nach Benutzung des Dienstes der Fall (-11,2 Prozentpunkte).

Abb. 8 / Sicherheitsindex 2022

Die meistgenutzten Sicherheitsmaßnahmen



Die am wenigsten genutzten Sicherheitsmaßnahmen



in % 2021 2022

Die Entwicklung der Internetnutzung im Überblick

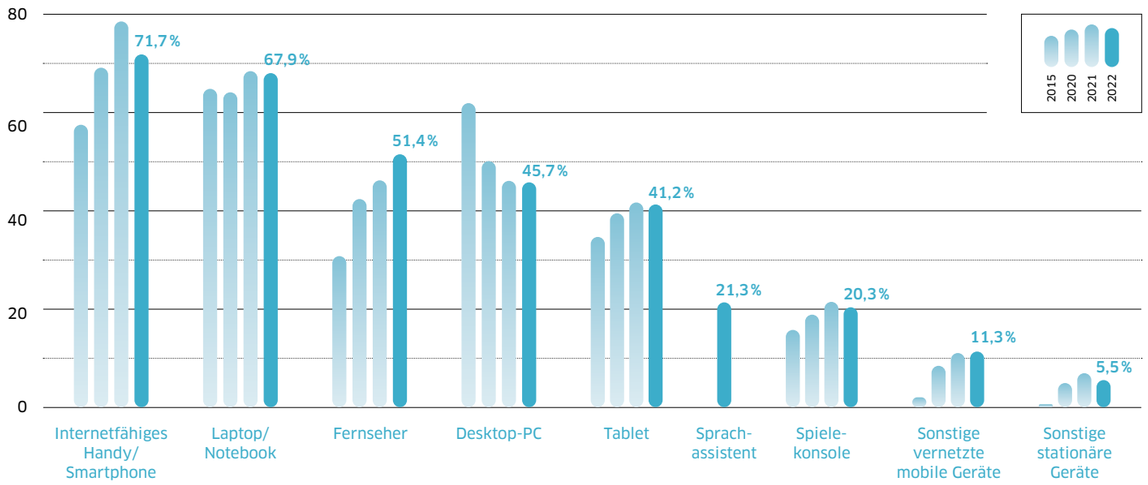
Wie gestalten sich die konkreten Nutzungsgewohnheiten der Verbraucher:innen? Für eine wirksame Aufklärungsarbeit mit bedarfsgerechten Hilfestellungen sind Erkenntnisse zur Entwicklung der Internetnutzung entscheidend. Hinsichtlich der Nutzungszwecke und Geräte zeigen sich nach dem zweiten Pandemiejahr folgende Entwicklungen.

Nutzungszweck
Das Senden und Empfangen von E-Mails führt die Liste der privaten Nutzungszwecke an (74,7 Prozent), gefolgt von Onlineshopping (72,7 Prozent) und dem Recherchieren in Suchmaschinen und Nachschlagewerken (61,7 Prozent). Auffallend ist, dass die Nutzung über die meisten Aktivitäten hinweg abgenommen hat. Besonders starke Einbußen verzeichnet das Streamen (zum Beispiel YouTube, Twitch, Onlinemediatheken) (44,2 Prozent) mit -10,5 Prozentpunkten. Dagegen reichlich zugelegt haben standortbezogene Dienste (zum Beispiel Navigator, Routenplaner, myTaxi, TripAdvisor) mit +9,3 Prozent. Nach zwei Jahren Pandemie sind Verbraucher:innen damit offenbar wieder mehr außerhalb der eigenen vier Wände unterwegs.

Smartphones weiter Spitzenreiter
In diesem Jahr festigen sich die Gerätepräferenzen aus 2021. Weiterhin Spitzenreiter trotz Einbußen ist das Smartphone (71,7 Prozent). Auf den beiden Plätzen dahinter rangieren Laptops (67,9 Prozent) und IT-basierte Fernseher (51,4 Prozent) in diesem Jahr erneut mit einem satten Plus von 5,3 Prozentpunkten. Neu auf Rang 4 steigen – erstmalig abgefragt – die Sprachassistenten ein. Insgesamt offenbart gerade der Vergleich mit 2015 eine Entwicklung hin zu einer heterogenen Gerätenutzung. Mobile Geräte werden öfter genutzt und von Verbraucher:innen um neue Geräte ergänzt, allerdings bleiben traditionelle Geräte nach wie vor relevant.

Abb. 9 / Sicherheitsindex 2022
Genutzte Geräte im Vergleich von 2015 und 2020/2021/2022*

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



Kapitel 2

IT-Sicherheitsgefälle: Unterschiede zwischen Verbrauchertypen

Digitale Sicherheit: Verbrauchertypen im Netz

Die Kenntnisse und Verhaltensweisen beim sicheren Umgang mit digitalen Angeboten gestalten sich von Mensch zu Mensch unterschiedlich. Wie sicher sich Verbraucher:innen durch das Netz bewegen, hängt vor allem vom individuellen Sicherheitswissen ab und der Bereitschaft, dieses auch regelmäßig im Alltag anzuwenden. Der DsiN-Index untersucht die IT-Sicherheitslage anhand der Kompetenzen, Erfahrungen und Verhaltensweisen von insgesamt fünf Verbrauchertypen.

Sicherheitsgefälle in der digitalen Gesellschaft: deutlicher Anstieg

Die digitale Sicherheitslage 2022 verschlechtert sich für alle fünf Verbrauchertypen. Besonders stark betroffen sind die Fatalist:innen mit 45,6 Punkten (-7,3) und Außenstehenden mit 45,9 Punkten (-6,3). Für die Gutgläubigen bedeutet das Minus von 2,8 einen neuen Tiefstwert von 56,7 Punkten, während Antreibende und bedachtsame Verbraucher:innen jeweils einen Rückgang um 1,2 Punkte verzeichnen. Damit erreichen sie traditionell die Höchstwerte unter den Verbrauchertypen mit 70,4 bzw. 71,6 Punkten.

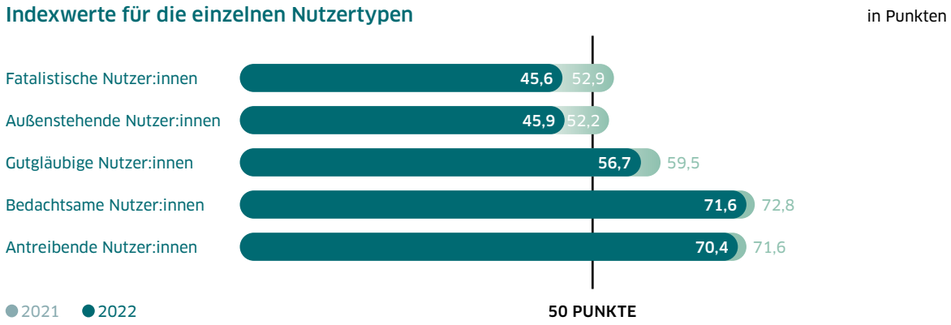
Aufgrund der starken Indexeinbußen der Fatalist:innen und außenstehenden Nutzer:innen vergrößert sich das IT-Sicherheitsgefälle. 26 Indexpunkte trennen die fatalistischen Verbraucher:innen von den Bedachtsamen. Zum Vergleich: Im letzten Jahr lag dieser Wert noch bei knapp 20 Punkten. Hieran zeigt sich die Wichtigkeit bedarfsgerechter Aufklärungsangebote, um die teils stark unterschiedlichen Voraussetzungen zu adressieren.

Betrachtet man die einzelnen Sicherheitsfaktoren, wird deutlich:

- Sicherheitsvorfälle: Die registrierten Sicherheitsvorfälle nehmen 2022 bei allen Gruppen teils kräftig zu, was sich negativ auf den Gesamtindex auswirkt. Fatalist:innen verzeichnen mit 17,2 Punkten das größte Plus.
- Verunsicherungsgefühl: Das Verunsicherungsgefühl steigt in diesem Jahr zwar insgesamt leicht an. Allerdings verzeichnen lediglich die Antreibenden (+0,3) und Fatalist:innen (+4,1) Zuwächse auf 19,7 bzw. 79,2 Punkte. Außenstehende landen mit -6,6 Punkten bei einem Tiefstwert von 19,9.
- Sicherheitswissen: Das Sicherheitswissen geht bei allen fünf Verbrauchergruppen zurück. Am stärksten ist dies der Fall bei den Außenstehenden mit -2,8 auf 35,1 Punkte. Bedachtsame Verbraucher:innen bleiben Spitzenreiter mit dem geringsten Rückgang von 0,3 Punkten auf 96,5 Punkten.
- Sicherheitsverhalten: Die Bedachtsamen weisen in diesem Jahr mit einem Plus von 6,7 auf 75,2 Punkten das höchste Wachstum aller Verbrauchergruppen auf und rangieren damit auf Platz eins. Bei drei Gruppen ist der Wert gefallen, besonders deutlich bei den Gutgläubigen mit -4,0 auf 29,5 Punkte.

Abb. 10 / Sicherheitsindex 2022

Digitales Sicherheitsgefälle der Verbrauchertypen

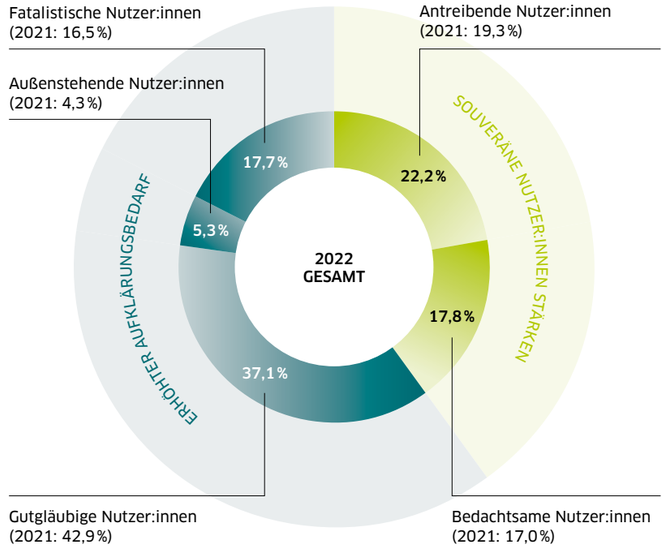


Anteil der Nutzertypen an der Gesamtbevölkerung

Das einzige Minus verzeichnen in diesem Jahr die Gutgläubigen. Dort geht der Anteil um 5,8 Prozentpunkte auf 37,1 Prozent zurück. Dennoch besitzen sie weiterhin mit Abstand den größten Anteil aller Verbrauchergruppen. Den höchsten Anteilszuwachs erreichen die antreibenden Verbraucher:innen mit 2,9 Prozent auf 22,2 Prozent. Das geringste Plus ergibt sich bei den Bedachtsamen mit 0,8 Prozent auf 17,8 Prozent.

Abb. 11 / Sicherheitsindex 2022

Anteil der Verbrauchertypen an der Gesamtheit der Internetnutzer:innen



Fatalistische Nutzer:innen landen mit einem Indexwert von 45,6 Punkten nicht nur deutlich unter der 50-Punkte-Marke, sondern auch auf dem letzten Platz der Verbrauchertypen. Sie verzeichnen mit einem Minus von 7,3 die größten Indexeinbußen. Ausschlaggebend dafür ist, dass sie die höchsten Anstiege bei den Sicherheitsvorfällen (+17,2) unter allen Nutzergruppen verzeichnen.

Außenstehende Nutzer:innen weisen in diesem Jahr mit einem Minus von 6,3 auf 45,9 Punkte den zweithöchsten Rückgang beim Indexwert auf. Sie bilden das Schlusslicht in puncto Sicherheitskompetenz (35,1 Punkte) und Sicherheitsverhalten (20,1 Punkte). Die Anzahl an Sicherheitsvorfällen (36,6 Punkte) hat 2022 um ganze 16,4 Punkte zugelegt.

Gutgläubige Nutzer:innen verschlechtern sich zwar mit -2,8 Indexpunkten, landen aber mit einem Gesamtwert von 56,7 Punkten wie in den letzten Jahren erneut auf dem dritten Platz. Charakteristisch bleibt auch 2022 ein geringes Risikobewusstsein mit einem neuen Tiefstwert von 14,5 sowie ein mangelndes Sicherheitsverhalten (29,5).

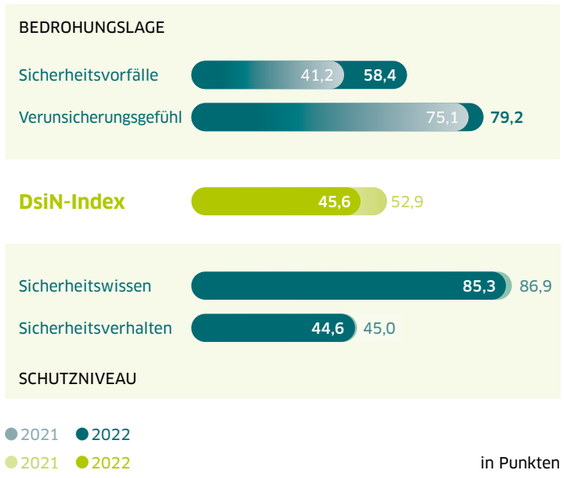
Antreibende Nutzer:innen fallen mit einem Minus von 1,7 Punkten in diesem Jahr auf einen Indexwert von 71,6 Punkten zurück und belegen Platz zwei hinter den Bedachtsamen. Antreibende reagieren mit einem gesteigerten Sicherheitsverhalten (+3,2) auf die zunehmenden Sicherheitsvorfälle (+6) und zeigen damit eine Anpassungsfähigkeit angesichts der gestiegenen Bedrohungslage.

Bedachtsame Nutzer:innen bleiben trotz des Rückgangs von 1,7 Punkten mit dem Indexwert von 78,2 Punkten das Maß aller Dinge. Zwar beklagen die Bedachtsamen mit einem Plus von 10 Punkten vergleichsweise viele Sicherheitsvorfälle, ihr Sicherheitsverhalten verzeichnet mit 6,7 Punkten jedoch den größten Zuwachs aller Gruppen und befähigt sie dazu, besonders gut auf die gehobene Bedrohungslage zu reagieren.

Fatalistische Nutzer:innen (45,6 Punkte)

„Überall lauern Gefahren – aber Schutzvorkehrungen bringen doch eh nichts!“

Abb. 12 / Sicherheitsindex 2022
DsiN-Indexwert für fatalistische Nutzer:innen



Die fatalistischen Verbraucher:innen fallen in diesem Jahr unter die kritische Schwelle von 50 Punkten, da sich ihr Gesamtindex um 7,3 Punkte auf 45,6 verringert. Damit weisen sie das schlechteste Sicherheitsverhalten unter den Verbrauchertypen auf. Der Anteil der Fatalist:innen steigt um 1,2 Prozentpunkte auf 17,7 Prozent. Sie bleiben die zweitkleinste Verbrauchergruppe, kommen aber sehr nahe an die Bedachtsamen heran.

Bedrohungslage
In diesem Jahr sind bei den Fatalist:innen die Sicherheitsvorfälle innerhalb aller Verbrauchergruppen am stärksten gestiegen, nämlich um +17,2 auf 58,4 Punkte. Das Verunsicherungsgefühl steigt ebenfalls und erreicht mit 79,2 Punkten (+4,1) den mit Abstand höchsten Wert unter den Verbrauchertypen. Und auch die Bedrohungslage insgesamt gestaltet sich damit im Gruppenvergleich am höchsten bei den Fatalist:innen.

Schutzniveau
Mit Blick auf die erhöhte Bedrohungslage können fatalistische Verbraucher:innen ihr Schutzniveau nicht entsprechend anpassen. Im Gegenteil: Sowohl ihr Sicherheitswissen (-1,6) als auch ihr Sicherheitsverhalten (-0,4) gehen in diesem Jahr auf 85,3 bzw. 44,6 Punkte zurück.

Selbstwirksamkeit herausstellen, Anpassungsfähigkeit stärken
Fatalist:innen erkennen seltener, dass ihr eigenes Verhalten ein wichtiger Baustein im Sicherheitskonzept ist. 62,8 Prozent sind der Meinung, dass eine geringere Internetnutzung als ein geeignetes Mittel zum Selbstschutz förderlich ist. In den anderen Verbrauchergruppen sind nur knapp über ein Drittel oder sogar nur ein Viertel dieser Meinung.

Primäres Ziel der Aufklärungsarbeit sollte deshalb die Sensibilisierung für Eigenverantwortung und Selbstwirksamkeit sein. Fatalist:innen müssen erleben, dass Schutzvorkehrungen wirken, um das vergleichsweise gut ausgeprägte Sicherheitswissen weiter zu stärken und zu dessen Anwendung zu motivieren.

Abb. 13 / Sicherheitsindex 2022
Steckbrief fatalistische Nutzer:innen

Typische Merkmale

- Stellen sich zu 52,1 Prozent aus Männern, zu 47,1 Prozent aus Frauen und zu 0,5 Prozent aus Diversen zusammen.
- Fast die Hälfte (48,3 Prozent) ist unter 40 Jahre alt, knapp jeder Dritte sogar unter 30 Jahre.
- Sind in der Regel fünf bis 20 Stunden in der Woche privat online, hauptsächlich mit Laptop (62,3 Prozent) und Smartphone (56,8 Prozent).

Ausprägung der Sicherheitsfaktoren

- Sicherheitsvorfälle: **überdurchschnittlich**
- Verunsicherungsgefühl: **überdurchschnittlich**
- Sicherheitswissen: **leicht unterdurchschnittlich**
- Sicherheitsverhalten: **leicht unterdurchschnittlich**

Indexwert 2022
45,6 Punkte

Anteil an der Gesamtheit: **17,7 %**

84,8 %
Wie Sicherheitsfälle reduzieren?
Stärkere Verfolgung von Gesetzesverstößen

80,0 %
Wie Risikobewusstsein stärken?
Der bewusste Umgang mit Risiken und Chancen sollte in der Schule mehr eingebunden werden.

70,2 %
Wie Sicherheitswissen erweitern?
Die Informationen darüber, wie man sich im Internet besser schützen kann, müssten verständlicher sein.

61,6 %
Wie zu Sicherheitsverhalten motivieren?
Einfachere Sicherheitseinstellungen bei Programmen und Geräten

TOP 3 Genutzte Schutzmaßnahmen

Regelmäßiges Update des Betriebssystems	67,5 %
Regelmäßige Updates von Apps	67,4 %
Nutzung von Spamfiltern	66,4 %

TOP 3 Sicherheitsvorfälle

37,8 %	Phishing-Versuch per SMS
37,2 %	Phishing-Versuch
36,3 %	Erhalt infizierter E-Mails / Anhänge / Weblinks

TOP 3 Unbekannte Schutzmaßnahmen

19,3 %	Einsatz von VPN oder Proxy-Clients
17,8 %	Überprüfung der Vertrauenswürdigkeit von Cloud-Diensten
16,7 %	Plug-ins zur Erhöhung der Datensicherheit

TOP 3 Verunsicherungsgefühl

Öffnen von Anhängen in E-Mails	90,5 %
Soziale Netzwerke	89,9 %
Upload eigener Dateien in Clouds auf dritten Webservern	88,3 %

TOP 3 Am wenigsten genutzte Schutzmaßnahmen

31,2 %	Anlegung und Überprüfung elektronischer Signaturen
31,1 %	Verschlüsselung der Festplatte
31,0 %	Nutzung von VPN oder Proxy-Clients

DsiN-Angebote für Fatalist:innen:
sicher-im-netz.de/angebote-fuer-fatalisten

Außenstehende Nutzer:innen (45,9 Punkte)

„Versteh’ ich nicht – und kann es auch nicht!“

Die außenstehenden Nutzer:innen verzeichnen in diesem Jahr mit einem Minus von 6,3 Punkten auf 45,9 den zweithöchsten Rückgang beim Indexwert. Damit fallen sie wieder unter die kritische Marke von 50 Punkten: Die Bedrohungslage übersteigt ihr Sicherheitsniveau. Der Anteil an der Gesamtheit der Internetnutzer:innen steigt derweil auf 5,3 Prozent an. Außenstehende bleiben dennoch mit Abstand die kleinste Verbrauchergruppe.

Bedrohungslage
Die Zahl der Sicherheitsvorfälle ist im Vergleich zum Vorjahr deutlich um 16,4 Punkte auf 36,6 angestiegen. Nach wie vor bemerkt diese Gruppe damit am seltensten eigene Sicherheitsvorfälle. Trotz des starken Anstiegs der Sicherheitsvorfälle fällt das Verunsicherungsgefühl in diesem Jahr um 6,6 auf 19,9 Punkte.

Schutzniveau
Sicherheitswissen und -verhalten haben sich bei den Außenstehenden in diesem Jahr verschlechtert. Ersteres fällt um 2,8 auf 35,1 Punkte, Letzteres um 1,5 auf 20,6 Punkte. Damit weisen sie weiterhin das mit Abstand niedrigste Schutzniveau aller Verbrauchergruppen auf.

Basiswissen und Verantwortungsgefühl bedarfsgerecht stärken
Außenstehende Verbraucher:innen fühlen sich von neuen digitalen Angeboten häufig überfordert (53 Prozent). Dennoch sehen sie sich bei der IT-Sicherheit selbst in der Verantwortung in Form eines vorsichtigeren Umgangs mit den eigenen persönlichen Daten (81,2 Prozent). Größte Motivation für den sichereren Umgang mit den eigenen Daten sind laut 67,5 Prozent einfachere Sicherheitseinstellungen bei Programmen und Geräten.

Um das Schutzniveau zu heben, bedarf es einfacher Anleitungen auf Anbieter- und Herstellerseite sowie persönlicher Begleitungen durch Ansprechpersonen. Aufklärungsarbeit muss das Bewusstsein für IT-Risiken durch Verdeutlichung der Relevanz und der persönlichen Betroffenheit fördern sowie einfache und wirksame Schutzmöglichkeiten aufzeigen.

Abb. 14 / Sicherheitsindex 2022
DsiN-Indexwert für außenstehende Nutzer:innen

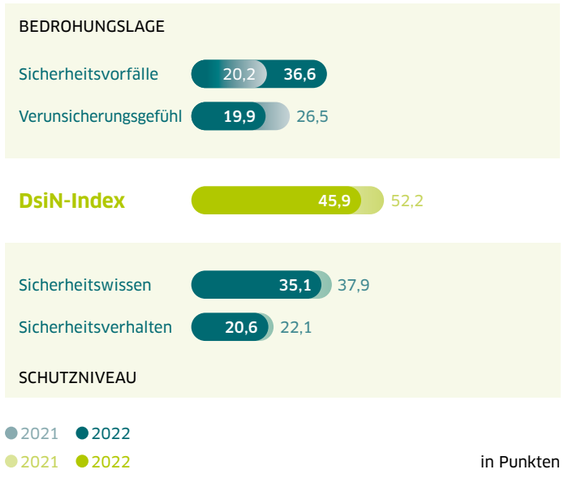


Abb. 15 / Sicherheitsindex 2022
Steckbrief außenstehende Nutzer:innen

Typische Merkmale

- Weisen mit 65,4 Prozent mit Abstand den höchsten Anteil an Frauen auf.
- Außenstehende sind zudem in der Regel älter: Über 70 Prozent sind 50 Jahre alt oder älter, über 47 Prozent sogar älter als 60 Jahre.
- Laptops gefolgt von Smartphones sind die bevorzugten Geräte, um ins Internet zu gelangen.
- In der Regel sind Außenstehende zwischen fünf und 20 Stunden online, bei über 45 Prozent ist dies der Fall.

Ausprägung der Sicherheitsfaktoren

- Sicherheitsvorfälle: **unterdurchschnittlich**
- Verunsicherungsgefühl: **leicht unterdurchschnittlich**
- Sicherheitswissen: **unterdurchschnittlich**
- Sicherheitsverhalten: **unterdurchschnittlich**

Indexwert 2022
45,9 Punkte

Anteil an der Gesamtheit: **5,3 %**

81,2 %
Wie Sicherheitsfälle reduzieren?
Vorsichtigerer Umgang mit den eigenen persönlichen Daten

76,5 %
Wie Risikobewusstsein stärken?
Der bewusste Umgang mit Risiken und Chancen sollte in der Schule mehr eingebunden werden.

64,5 %
Wie Sicherheitswissen erweitern?
Die Informationen darüber, wie man sich im Internet besser schützen kann, müssten verständlicher sein.

67,5 %
Wie zu Sicherheitsverhalten motivieren?
Einfachere Sicherheitseinstellungen bei Programmen und Geräten im Internet besser schützen kann, müssten verständlicher sein.

TOP 3 Genutzte Schutzmaßnahmen

- Verwendung von Sonderzeichen in Passwörtern 68,9 %
- Nutzung sicherer Zahlungssysteme 66,1 %
- Verwendung unterschiedlicher Passwörter für unterschiedliche Zwecke 59,0 %

TOP 3 Sicherheitsvorfälle

- 28,6 % Phishing-Versuch
- 12,1 % Phishing-Versuch per SMS
- 10,5 % Mobbing / Belästigungen / Rufschädigung (z. B. in sozialen Netzwerken)

TOP 3 Unbekannte Schutzmaßnahmen

- Plug-ins zur Erhöhung der Datensicherheit 94,2 %
- Überprüfung der Vertrauenswürdigkeit 92,7 %
- Überprüfung von Anhängen in E-Mails 91,6 %

TOP 3 Verunsicherungsgefühl

- 46,5 % Öffnen von Anhängen in E-Mails
- 42,5 % Austausch vertraulicher Inhalte via Webseiten oder Apps
- 42,2 % Erledigen von Bankgeschäften im Internet

TOP 3 Am wenigsten genutzte Schutzmaßnahmen

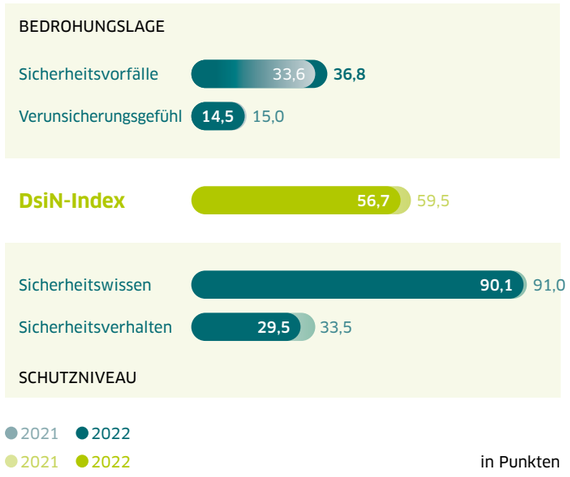
- 1,2 % Verschlüsselung von Dateien auf dem Computer
- 0,6 % Verschlüsselung der Festplatte
- 0,5 % Einsatz eigener elektronischer Signaturen

DsiN-Angebote für Außenstehende:
sicher-im-netz.de/angebote-fuer-aussenstehende

Gutgläubige Nutzer:innen (56,7 Punkte)

„Mir wird schon nichts passieren!“

Abb. 16 / Sicherheitsindex 2022
DsiN-Indexwert für gutgläubige Nutzer:innen



Mit einem Indexwert von 56,7 Punkten (-2,8 Punkte) belegen die gutgläubigen Verbraucher:innen erneut den dritten Platz. Anteilig stellen sie mit 37,1 Prozent die meisten Internetnutzer:innen, obgleich sie sich als einzige Gruppe verkleinern (-5,8 Prozent). Charakteristisch ist auch in diesem Jahr eine besonders hohe Diskrepanz zwischen Sicherheitswissen (90,1) und -verhalten (29,5). Keine andere Gruppe weist eine so große Wissens-Verhaltens-Lücke auf.

Bedrohungslage
Bei den Gutgläubigen hat sich die Bedrohungslage auf 36,8 Punkte erhöht. Mit einer Steigerung um 3,2 Punkte fällt diese aber bedeutend geringer aus als bei den anderen Gruppen. Trotzdem sinkt in diesem Jahr das Verunsicherungsgefühl um 0,5 auf 14,5 Punkte und erreicht damit einen historischen Tiefstwert. Damit untermauern die Gutgläubigen ihren Status als diejenigen, die sich am wenigsten Sorgen um eine Gefährdung machen.

Schutzniveau
Während das Sicherheitswissen in diesem Jahr mit 0,9 Punkten leicht auf 90,1 zurückfällt, verzeichnet das Sicherheitsverhalten stärkere Einbußen und landet mit einem Minus von 4 Punkten bei 29,5 Punkten. Damit klafft die Wissens-Verhaltens-Lücke in diesem Jahr besonders stark auseinander.

Vorhandenes Sicherheitswissen aktivieren und anwenden
Auffallend bei den Gutgläubigen ist ein geringes Interesse an Maßnahmen zur Gefahrenreduzierung. So liegt die Zustimmung zu allen abgefragten Themenkomplexen in diesem Zusammenhang im Vergleich zu den anderen Verbrauchergruppen immer niedriger. Den vorsichtigeren Umgang mit persönlichen Daten sehen etwa nur 66 Prozent als (sehr) geeignete Schutzmaßnahme. Bei allen anderen liegt die Zustimmung zwischen 80 und 90 Prozent.

Die Aufklärungsarbeit muss in erster Linie beim mangelnden Gefahrenempfinden ansetzen und darauf abzielen, das vorhandene Sicherheitswissen deutlich öfter in die Tat umzusetzen, etwa indem man den gutgläubigen Verbraucher:innen die Auswirkungen von nachlässigem Sicherheitsverhalten aufzeigt.

Abb. 17 / Sicherheitsindex 2022
Steckbrief gutgläubige Nutzer:innen

Typische Merkmale

- Überwiegt das weibliche Geschlecht leicht mit 50,6 Prozent. Der Männeranteil beträgt 48,4 Prozent.
- Der Anteil der Diversen liegt bei 1,0 Prozent und somit am höchsten innerhalb aller Verbrauchergruppen.
- Fast gleichauf liegen Notebook (65,4 Prozent) und das Smartphone (63,8 Prozent), wenn es darum geht, mit welchem Gerät Gutgläubige das Internet nutzen.
- Die Nutzungsdauer in einer Woche liegt meist zwischen 5 und 30 Stunden.

Ausprägung der Sicherheitsfaktoren

- Sicherheitsvorfälle: **leicht unterdurchschnittlich**
- Verunsicherungsgefühl: **leicht unterdurchschnittlich**
- Sicherheitswissen: **durchschnittlich**
- Sicherheitsverhalten: **unterdurchschnittlich**

Indexwert 2022
56,7 Punkte

Anteil an der Gesamtheit: **37,1 %**

66,6 % **Wie Sicherheitsfälle reduzieren?**
Vorsichtigerer Umgang mit den eigenen persönlichen Daten

53,5 % **Wie Risikobewusstsein stärken?**
Der bewusste Umgang mit Risiken und Chancen sollte in der Schule mehr eingebunden werden.

50,4 % **Wie Sicherheitswissen erweitern?**
Die Informationen darüber, wie man sich im Internet besser schützen kann, müssten verständlicher sein.

55,3 % **Wie zu Sicherheitsverhalten motivieren?**
Einfachere Sicherheitseinstellungen bei Programmen und Geräten

TOP 3 Genutzte Schutzmaßnahmen

- Verwendung von Sonderzeichen in Passwörtern **60,4 %**
- Nutzung sicherer Zahlungssysteme **54,9 %**
- Regelmäßiges Update des Betriebssystems **54,4 %**

TOP 3 Sicherheitsvorfälle

- **24,3 %** Phishing-Versuch
- **17,7 %** Erhalt infizierter E-Mails/Anhänge/Weblinks
- **16,4 %** Phishing-Versuch per SMS

TOP 3 Unbekannte Schutzmaßnahmen

- **15,6 %** Anlegung eigener und Überprüfung fremder elektronischer Signaturen
- **14,1 %** Einsatz von VPN oder Proxy-Clients
- **13,9 %** Überprüfung von Anhängen in E-Mails auf mögliche Sicherheitsrisiken

TOP 3 Verunsicherungsgefühl

- **33,4 %** Öffnen von Anhängen in E-Mails
- **23,0 %** Austausch vertraulicher Inhalte via Webseiten oder Apps
- **22,8 %** Dating-Anwendungen

TOP 3 Am wenigsten genutzte Schutzmaßnahmen

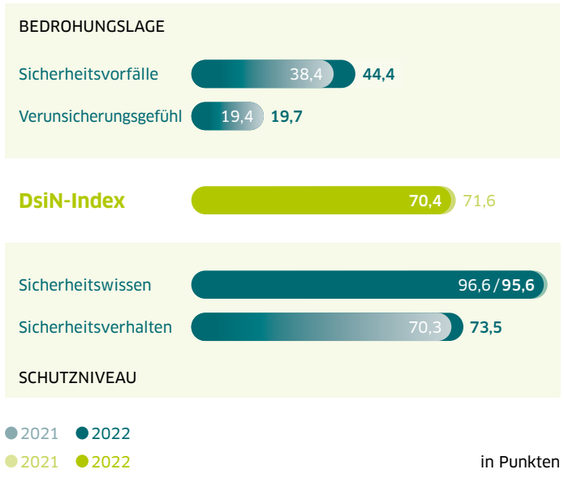
- **11,6 %** Anlegung eigener und Überprüfung fremder elektronischer Signaturen
- **11,5 %** Nutzung von VPN oder Proxy-Clients
- **10,4 %** Einsatz eigener elektronischer Signaturen

DsiN-Angebote für Gutgläubige:
sicher-im-netz.de/angebote-fuer-gutglaeubige

Antreibende Nutzer:innen (70,4 Punkte)

„Das möchte ich ausprobieren – aber sicher!“

Abb. 18 / Sicherheitsindex 2022
DsiN-Indexwert für antreibende Nutzer:innen



Der Indexwert der antreibenden Verbraucher:innen erreicht 2022 einen Wert von 70,4 Punkten und ist damit 1,2 Punkte schlechter als im Vorjahr. Erneut handelt es sich dabei um den zweithöchsten Indexwert hinter den bedachtsamen Nutzer:innen. Ihren Anteil an der Gesamtheit der Internetnutzer:innen können die Antreibenden um 2,9 Prozent auf 22,2 Prozent ausbauen. Dies ist die höchste Wachstumsquote aller Verbrauchergruppen.

Bedrohungslage
Obwohl sich die Zahl der Sicherheitsvorfälle bei den antreibenden Verbraucher:innen in diesem Jahr deutlich um 6,0 auf 44,4 Punkte erhöht hat, ist das Verunsicherungsgefühl nur leicht gestiegen, nämlich um 0,3 auf 19,7 Punkte. Daraus ergibt sich die zweitgrößte Diskrepanz von Sicherheitsvorfällen und Verunsicherungsempfinden (Sicherheits-Verunsicherungs-Lücke: 24,7) hinter den Außenstehenden (S/V-Lücke: 26,7).

Schutzniveau
Dem Anstieg der Sicherheitsvorfälle können die Antreibenden in diesem Jahr ein erhöhtes Schutzniveau entgegensetzen. Zwar hat sich das Sicherheitswissen um 1,0 auf 95,6 Punkte verschlechtert. Das Sicherheitsverhalten landet dagegen mit einem Zuwachs von 3,2 Punkten auf 73,5 Punkten. Nur die Bedachtsamen erreichen einen höheren Wert, die restlichen Gruppen liegen deutlich darunter. Bis auf eine abgefragte Sicherheitsmaßnahme sind alle den antreibenden Verbraucher:innen zu über 90 Prozent bekannt.

Agile Grundkompetenzen und aktuelle Informationen
Antreibende Verbraucher:innen sind offen für Neues und probieren im Vergleich zu den anderen Gruppen viel mehr neue digitale Dienste und Angebote aus (41,3 Prozent). In der Aufklärungsarbeit benötigen sie deshalb vor allem stets die aktuellen Informationen zu den neuesten Diensten sowie agile Basiskompetenzen, die sie selbst auf neue Umfelder übertragen können. Durch ihre Aufgeschlossenheit und Neugierde sind sie besonders als Multiplikator:innen in der Aufklärungsarbeit geeignet.

Abb. 19 / Sicherheitsindex 2022
Steckbrief antreibende Nutzer:innen

Typische Merkmale

- 56,3 Prozent sind männlich, 43,0 Prozent weiblich und 0,7 Prozent divers.
- Höchster Männeranteil in den Verbrauchergruppen
- Mit 48,1 Prozent sind knapp die Hälfte der Antreibenden 50 Jahre oder älter.
- Länger als 10 Stunden/Woche online (68,2 Prozent), fast jeder Fünfte sogar über 40 Stunden (17,8 Prozent)
- Am häufigsten Smartphone-Nutzung (85,6 Prozent), gefolgt von Laptops (76,8 Prozent)

Ausprägung der Sicherheitsfaktoren

- Sicherheitsvorfälle: **durchschnittlich**
- Verunsicherungsgefühl: **leicht unterdurchschnittlich**
- Sicherheitswissen: **überdurchschnittlich**
- Sicherheitsverhalten: **überdurchschnittlich**

Indexwert 2022
70,4 Punkte

Anteil an der Gesamtheit: **22,2%**

84,3 % **Wie Sicherheitsfälle reduzieren?**
Vorsichtigerer Umgang mit den eigenen persönlichen Daten

78,7 % **Wie Risikobewusstsein stärken?**
Der bewusste Umgang mit Risiken und Chancen sollte in der Schule mehr eingebunden werden.

79,3 % **Wie Sicherheitswissen erweitern?**
Es müsste mehr Aufklärungsangebote in beruflicher oder schulischer Aus- und Weiterbildung geben.

81,2 % **Wie zu Sicherheitsverhalten motivieren?**
Einfachere Sicherheitseinstellungen bei Programmen und Geräten

TOP 3 Genutzte Schutzmaßnahmen

Regelmäßige Updates von Apps	94,8 %
Nutzung sicherer Zahlungssysteme	94,1 %
Ausloggen bei Benutzerkonten auf Webseiten, insbesondere auf fremden Rechnern	93,5 %

TOP 3 Sicherheitsvorfälle

33,6 %	Phishing-Versuch
32,7 %	Erhalt infizierter E-Mails/Anhänge/Weblinks
26,6 %	Phishing-Versuch per SMS

TOP 3 Unbekannte Schutzmaßnahmen

12,6 %	Überprüfung von Anhängen in E-Mails auf mögliche Sicherheitsrisiken
9,2 %	Auslesen der E-Mail-Header
8,5 %	Plug-ins zur Erhöhung der Datensicherheit

TOP 3 Verunsicherungsgefühl

57,2 %	Öffnen von Anhängen in E-Mails
34,8 %	Soziale Netzwerke
32,6 %	Sprachgesteuerte Assistenten

TOP 3 Am wenigsten genutzte Schutzmaßnahmen

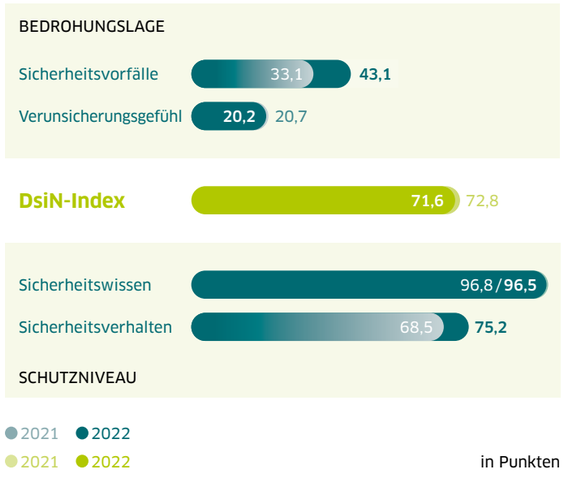
48,3 %	Verschlüsselung der Festplatte
46,7 %	Einsatz eigener elektronischer Signaturen
43,7 %	Sichere Aufbewahrung der Geräte

DsiN-Angebote für Antreibende:
sicher-im-netz.de/angebote-fuer-antreibende

Bedachtsame Nutzer:innen (71,6 Punkte)

„Sicherheit geht vor.“

Abb. 20 / Sicherheitsindex 2022
DsiN-Indexwert für bedachtsame Nutzer:innen



Die bedachtsamen Verbraucher:innen verzeichnen im Gesamtindex ein Minus von 1,2 Punkten, bleiben mit einem Wert von 71,6 aber weiterhin das Maß aller Dinge. Ihren Anteil an den gesamten Internetnutzer:innen kann diese Gruppe um 0,8 Prozentpunkte auf 17,8 Prozent erhöhen. Die Gruppe weist in diesem Jahr das höchste Sicherheitswissen auf und liegt auch bei dessen Umsetzung vorne.

Bedrohungslage
Die Zahl der Sicherheitsvorfälle hat bei den bedachtsamen Verbraucher:innen um 10 Punkte stark zugenommen und erreicht mit 43,1 Punkten einen neuen Höchstwert in dieser Gruppe. Das Verunsicherungsgefühl verzeichnet ein Minus von 0,5 Punkten und landet bei 20,2 Punkten. Damit verschärft sich die Bedrohungslage im Vergleich zum Vorjahr deutlich.

Schutzniveau
Beim Sicherheitswissen sind die Bedachtsamen auch in diesem Jahr führend. Mit einem leichten Minus von 0,3 auf 96,5 Punkte verschlechtert es sich zwar, allerdings weitaus weniger stark als bei anderen Verbrauchergruppen. Das Sicherheitsverhalten legt dagegen deutlich um 6,7 auf 75,2 Punkte zu. Dies ist ein neuer Höchstwert und beschert den Bedachtsamen das beste Schutzniveau unter allen Gruppen. Alle abgefragten Sicherheitsmaßnahmen sind den bedachtsamen Verbraucher:innen zu über 89 Prozent bekannt.

Souveränes Handeln bestärken
Bedachtsame Nutzer:innen sind Vorbilder für eine souveräne Internetnutzung. Sie stellen dies 2022 besonders durch ihre außergewöhnliche Anpassungsfähigkeit des Schutzniveaus angesichts der verstärkten Bedrohungslage unter Beweis. Noch nie zuvor hat eine Verbrauchergruppe ihr Sicherheitsverhalten im Jahresvergleich so stark ausbauen können.

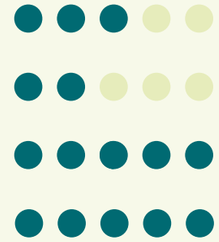
Gegenüber neuen digitalen Angeboten sind Bedachtsame am vorsichtigsten. 66,1 Prozent geben an, sich zuerst mit Sicherheitsfragen zu beschäftigen, bevor sie neue digitale Angebote nutzen. Die Vorbildfunktion der Bedachtsamen kann durch Anerkennung, beispielsweise durch Wettbewerbe, gewürdigt und sichtbar gemacht werden, um andere zur Nachahmung zu motivieren.

Abb. 21 / Sicherheitsindex 2022
Steckbrief bedachtsame Nutzer:innen

Typische Merkmale

- Die Mehrheit der bedachtsamen Verbraucher ist männlich (51,1 Prozent).
- In dieser Gruppe befinden sich zudem die wenigsten, die ihr Geschlecht mit divers angeben (0,2 Prozent).
- Fast die Hälfte der Bedachtsamen ist zwischen 50 und 69 Jahre alt (47,2 Prozent) und verbringt zumeist in der Woche fünf bis 20 Stunden im Internet.
- Mit Abstand am häufigsten wird dabei das Smartphone (89,4 Prozent) genutzt.

Ausprägung der Sicherheitsfaktoren



Indexwert 2022
71,6 Punkte

Anteil an der Gesamtheit: **17,8%**

88,6 % **Wie Sicherheitsfälle reduzieren?**
Vorsichtigerer Umgang mit den eigenen persönlichen Daten

78,5 % **Wie Risikobewusstsein stärken?**
Der bewusste Umgang mit Risiken und Chancen sollte in der Schule mehr eingebunden werden.

76,3 % **Wie Sicherheitswissen erweitern?**
Die Informationen darüber, wie man sich im Internet besser schützen kann, müssten stärker gebündelt werden (zum Beispiel auf einer zentralen Webseite).

79,1 % **Wie zu Sicherheitsverhalten motivieren?**
Einfachere Sicherheitseinstellungen bei Programmen und Geräten

TOP 3 Genutzte Schutzmaßnahmen

Nutzung sicherer Zahlungssysteme	98,5 %
Verwendung unterschiedlicher Passwörter für unterschiedliche Zwecke	95,9 %
Verwendung von Sonderzeichen in Passwörtern	95,8 %

TOP 3 Sicherheitsvorfälle

33,2 %	Phishing-Versuch
27,3 %	Phishing-Versuch per SMS
18,5 %	Erhalt infizierter E-Mails / Anhänge / Weblinks

TOP 3 Unbekannte Schutzmaßnahmen

10,2 %	Einsatz von VPN oder Proxy-Clients
9,6 %	Anlegung eigener und Überprüfung fremder elektronischer Signaturen
8,9 %	Überprüfung der Vertrauenswürdigkeit von Cloud-Diensten

TOP 3 Verunsicherungsgefühl

58,4 %	Öffnen von Anhängen in E-Mails
34,8 %	Soziale Netzwerke
31,9 %	Dating-Anwendungen

TOP 3 Am wenigsten genutzte Schutzmaßnahmen

42,6 %	Verschlüsselung der Festplatte
41,9 %	Auslesen der E-Mail-Header
30,3 %	Einsatz eigener elektronischer Signaturen

DsiN-Angebote für Bedachtsame:
sicher-im-netz.de/angebote-fuer-bedachtsame

Cyberresilienz – Anpassungsfähigkeit als Schlüsselkompetenz

Der diesjährige Sicherheitsindex ist geprägt von einer stark erhöhten Bedrohungslage. Sie betrifft alle Internetnutzer:innen, wirkt sich aber unterschiedlich stark auf die einzelnen Nutzergruppen aus. Die Anpassungsfähigkeit sticht dabei als zentrales Unterscheidungsmerkmal zwischen souveränen und nichtsouveränen Verbraucher:innen hervor.

Anpassungsfähigkeit als zentraler Schutzfaktor
In diesem Jahr können die souveränen Verbrauchergruppen ihre Stärken unter Beweis stellen: Bei Bedachtsamen und Antreibenden wächst das Schutzniveau mit der Bedrohungslage mit, weil sie ihr Sicherheitswissen noch häufiger in die Tat umsetzen – im Vergleich zum Vorjahr und insbesondere im Vergleich mit den anderen Verbrauchergruppen.

Diese Anpassungsfähigkeit ist Basis einer digitalen Resilienz. Sie stellt einen zentralen Schutzfaktor dar, auf den die Aufklärungsarbeit hinwirken muss. Es geht um die Kompetenz, auf steigende, wechselnde und unbekannte Anforderungen und Risiken souverän zu reagieren. Die positiven Folgen dieser Cyberresilienzkompetenz zeigen in diesem Jahr die souveränen Gruppen auf. Welche Auswirkungen ein Anpassungsdefizit mit sich bringt, lässt sich dagegen bei den übrigen Verbrauchertypen beobachten. Bei teils kräftigen Anstiegen der Sicherheitsvorfälle fällt das ohnehin schon niedrige Verhaltensniveau in diesem Jahr weiter ab. Ihnen fehlt die Befähigung sowie Motivation zur Umsetzung ihres Schutzwissens.

Die Bedachtsamen sowie Antreibenden reagieren als souveräne Verbraucher:innen aktiv auf die veränderte Bedrohungslage mit einer Anpassung ihres Sicherheitsverhaltens, wohingegen sich bei den übrigen Gruppen ein Anpassungsdefizit offenbart.

Cyberresilienz: Hilfe zur Selbsthilfe entscheidend
Cyberresilienz erfordert eine grundsätzliche Transferfähigkeit des vorhandenen Wissens, um Schutzkompetenzen stets auf neue Dienste übertragen zu können. Zum anderen geht es um Agilität bei der Umsetzung des Wissens: Verbraucher:innen müssen Risiken erkennen und realistisch einschätzen können, um selbstständig die passende Maßnahme auszuwählen.

So werden sie in die Lage versetzt, auch unbekannten Bedrohungsszenarien zu begegnen und mit der voranschreitenden Digitalisierung Schritt zu halten. Eine wesentliche Voraussetzung dafür ist die Fähigkeit, sich selbst weiterzubilden, weshalb eine Aufklärung die Hilfe zur Selbsthilfe der Verbraucher:innen ins Zentrum stellen sollte.

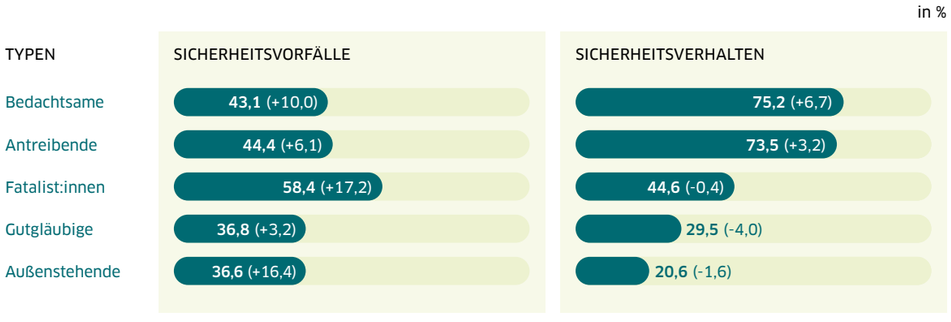
Eigenverantwortung und Motivation stärken
Während die Wissens-Verhaltens-Lücke bei den souveränen Verbrauchertypen bei 22,1 (Antreibende) bzw. 21,3 (Bedachtsame) liegt, öffnet sie sich bei den übrigen Gruppen teils kräftig. Gutgläubige kommen hier auf eine Differenz von 60,5 Punkten und Fatalist:innen erreichen 40,7 Punkte. Bei den Außenstehenden fällt dieser Wert mit 14,5 Punkten zwar geringer aus, allerdings liegt das Sicherheitsverhalten hier auch auf einem Tiefstwert von 20,6.

Auf dem Weg zur digitalen Resilienz muss die Aufklärungsarbeit folglich in erster Linie zu einer Umsetzung des Sicherheitswissens animieren, um dem vorherrschenden Motivationsdefizit in puncto Sicherheitsverhalten entgegenzuwirken.

Dies kann etwa durch das Aufzeigen von Risiken anhand des tatsächlichen Nutzungsverhaltens der Zielgruppe gelingen sowie durch die Anleitung zu einfachen und wirksamen Schutzmaßnahmen. Aufsuchende Aufklärungsarbeit ist hier der Schlüssel, um Umsetzungsbereitschaft und Motivation zu erzeugen (mehr dazu in Kapitel 4).

Abb. 22 / Sicherheitsindex 2022
Sicherheitsverhalten im Vergleich mit den Sicherheitsvorfällen nach Verbrauchertypen

in %



Exkurs: Einstellungen und Nutzungsgewohnheiten

Die unterschiedlichen IT-Sicherheitslagen der DsiN-Verbrauchertypen basieren auf verschiedenen Haltungen, Interessen und Verhaltensregeln. Diese zu erkennen und zu verstehen, ist Basis für eine bedarfsgerechte Aufklärungsarbeit. Übergeordnet lassen sich hierzu in diesem Jahr folgende Beobachtungen feststellen.

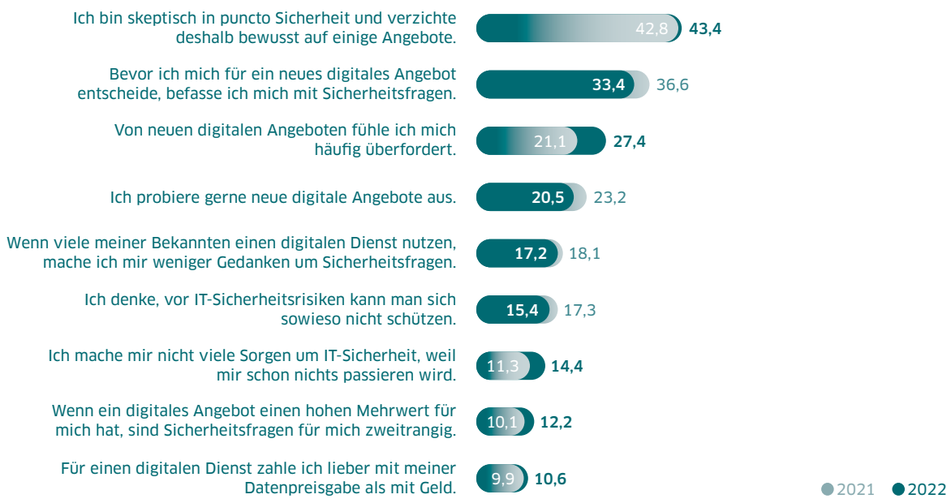
Weniger Anreiz, neue digitale Angebote auszuprobieren
Allen voran zeigt sich eine größere Skepsis in puncto Sicherheit, die verhindert, digitale Angebote zu nutzen (+0,6 Prozent). Weniger Verbraucher:innen als noch im Vorjahr haben folglich Lust, neue digitale Angebote zu testen (-2,7 Prozent). Besonders gering ist dabei der Anteil der Außenstehenden mit lediglich 4,7 Prozent.

Mehr Überforderung, weniger Sicherheitsbedenken
Ein Grund für diese Zurückhaltung ist die wachsende Überforderung von neuen digitalen Angeboten, die in diesem Jahr um 6,3 Prozentpunkte zulegt. Am deutlichsten ausgeprägt ist diese bei den Außenstehenden (53 Prozent). Sicherheitsfragen rücken unterdessen weiter in den Hintergrund und werden teilweise sogar bewusst ignoriert, etwa wenn das digitale Angebot einen hohen Mehrwert hat (+2,1 Prozent). Nur 33,4 Prozent (-3,2 Prozent) befassen sich mit ihnen, bevor sie sich für ein neues digitales Angebot entscheiden. 14,4 Prozent (+3,1 Prozent) machen sich nicht viele Sorgen um IT-Sicherheit, weil sie davon ausgehen, dass ihnen nichts passieren wird.

Gründe für Motivationsdefizite berücksichtigen
Hauptaugenmerk in der Aufklärungsarbeit sollte auf dem Motivationsdefizit bei der Umsetzung von Sicherheitswissen liegen. Wichtig ist es, bedarfsgerecht die unterschiedlichen Gründe zu adressieren, aus denen Verbraucher:innen der Sicherheit zu wenig Bedeutung beimessen. Die Ursachen dafür reichen von einer Überforderung bis hin zu einer Gutgläubigkeit gegenüber digitalen Diensten.

Abb. 23 / Sicherheitsindex 2022
Umgang mit dem Internet

Wie würden Sie allgemein Ihren Umgang mit dem Internet beschreiben? in %



Kapitel 3

Digitale Lebenswelten

FOKUSTHEMA 2022

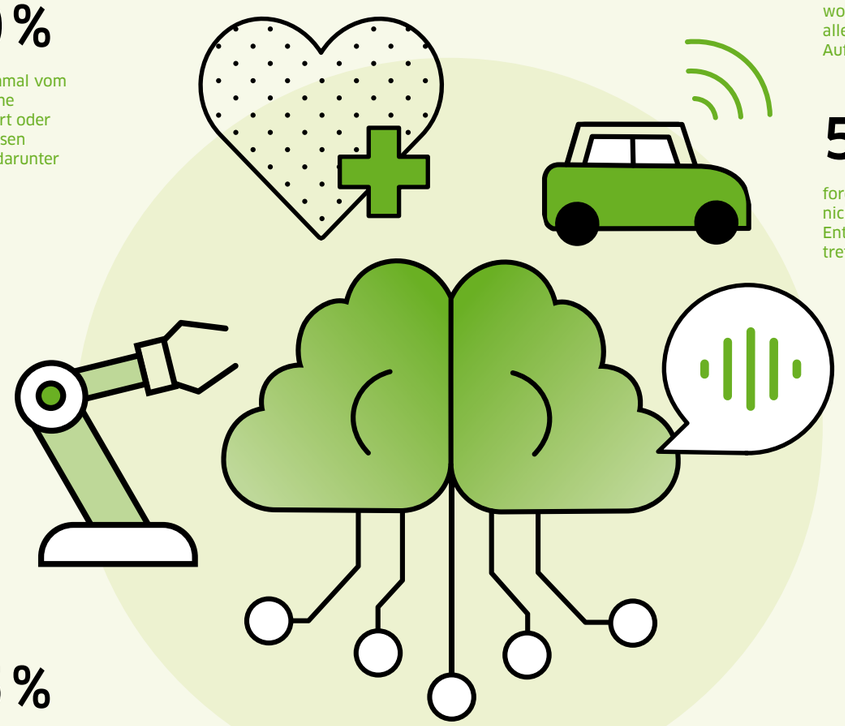
Künstliche Intelligenz

Abb. 24 / Sicherheitsindex 2022

Künstliche Intelligenz aus Verbrauchersicht

59,0 %

haben schon einmal vom Begriff Künstliche Intelligenz gehört oder gelesen und wissen auch, was man darunter versteht.



54,4 %

wollen, dass KI vor allemlebensgefährliche Aufgaben übernimmt.

50,1 %

fordern, dass KI nichtohne Menschen Entscheidungen treffen können soll.

28,5 %

sehen in KI eine Chance.

28,4 %

haben geringes oder sehr geringes Vertrauen in KI.

31,2 %

würden KI gerne im Zusammenhang mit medizinischen Programmen nutzen, die ihre Gesundheit/Fitness bewerten und/oder Krankheitsbilder prognostizieren.

Sprachassistenten, automatische Übersetzungen oder assistiertes Fahren – immer mehr Programme nutzen Künstliche Intelligenz (KI) und sind dadurch in der Lage, autonom Probleme zu lösen und ihre Ergebnisse durch eigenständige Lernerfolge zielgerichtet zu verbessern. Zunehmend viele Geräte und Dienste funktionieren nach diesem Prinzip und unterstützen Verbraucher:innen auf diese Weise in ihrem Alltag. Künstliche Intelligenz ist das diesjährige Fokusthema des DsiN-Sicherheitsindex.

Künstliche Intelligenz ist mehrheitlich bekannt
Die Mehrheit der Befragten (59 Prozent) haben Kenntnisse darüber, was man unter dem Thema „Künstliche Intelligenz“ versteht. Mit 71,3 Prozent kennen sich hier besonders die Bedachtsamen aus, bei den Außenstehenden sind es dagegen lediglich 41,7 Prozent. Mehr als jede:r Vierte (28,7 Prozent) aller Befragten hat zwar schon von KI gehört oder gelesen, kann sich aber nicht wirklich etwas darunter vorstellen. 12,3 Prozent dagegen haben vom Begriff Künstliche Intelligenz noch nicht gelesen oder gehört.

KI ist bereits Bestandteil vieler Lebensbereiche
Der ausbaufähige KI-Kenntnisstand erscheint überraschend, da entsprechende Anwendungen bereits Einzug in den Alltag der Verbraucher:innen halten. Textvorschläge beim Schreiben von Nachrichten sind die meistgenutzte KI-gestützte Anwendung (41,5 Prozent). Auf Platz zwei folgt die automatische Übersetzung mit 41 Prozent und auf Platz drei mit 37,7 Prozent Routenvorschläge und Navigation auf Grundlage von Echtzeit-Verkehrsüberwachung.

KI-Potenzial im Bereich der Risiko- und Zeiteinsparung
Verbraucher:innen sehen auch künftig weitere Einsatzpotenziale durch KI. Insbesondere verorten sie das Potenzial im Bereich der Risiko- und Zeiteinsparung für den (Berufs-)Alltag. Demnach soll Künstliche Intelligenz vor allem lebensgefährliche (54,4 Prozent) und monotone (53,4 Prozent) sowie komplexe Aufgaben (mit hohem Informations- und Datenanteil) (46,1 Prozent) übernehmen.

Auch Einsatzgebiete in sensiblen, körpernahen Bereichen sind immerhin noch für gut ein Drittel der Verbraucher:innen denkbar, etwa in Form von medizinischen Programmen, die die eigene Gesundheit und Fitness bewerten (31,2 Prozent), oder beim assistierten Fahren (30,9 Prozent).

Am Thema KI scheiden sich die Geister
Die Befragten sind sich aktuell allerdings insgesamt uneinig, ob KI eine Chance (28,5 Prozent) oder Gefahr (28,6 Prozent) darstellt. Der Großteil (33,2 Prozent) ist in dieser Frage unentschieden. Beim Vertrauen in KI sieht es ähnlich aus: Der Anteil der skeptischen Nutzer:innen mit (sehr) geringem Vertrauen liegt bei 28,4 Prozent. Knapp ein Viertel (24,2 Prozent) besitzt dagegen ein (sehr) hohes Vertrauen.

Gut jede:r vierte Nutzer:in bringt dementsprechend auch eine positive Einstellung gegenüber KI zum Ausdruck, wenn es um konkrete Lebensbereiche geht: 28,9 Prozent glauben etwa, dass KI zur Nachhaltigkeit beiträgt, und laut 27,1 Prozent macht KI den Alltag sicherer. Skeptisch sind die Verbraucher:innen dagegen vor allem mit Blick auf die Arbeitswelt: 46,7 Prozent glauben, dass durch KI viele Arbeitsplätze überflüssig werden.

Menschliche Kontrolle schafft Vertrauen
Für einen Vertrauensaufbau muss allen voran nachvollziehbar werden, wie die Ergebnisse von KI-Anwendungen zustande kommen (58,6 Prozent). 50,1 Prozent fordern außerdem, dass KI nicht ohne Menschen Entscheidungen treffen können soll. Für mehr Vertrauen würde laut 40,6 Prozent zudem sorgen, wenn klar ist, wer für Entscheidungen haftet, die eine KI trifft.

Weil KI bereits in vielen Alltagsbereichen zum Einsatz kommt und weitere Anwendungspotenziale von der Mehrheit der Befragten begrüßt werden, erscheint eine verstärkte Aufklärungsarbeit über die Wirkungsweise, Chancen und Risiken der Technologie umso wichtiger – und das von Bildungsanbieter:innen, Legislative und herstellenden Unternehmen gleichermaßen.

Digitale Identität und Digitales Ich

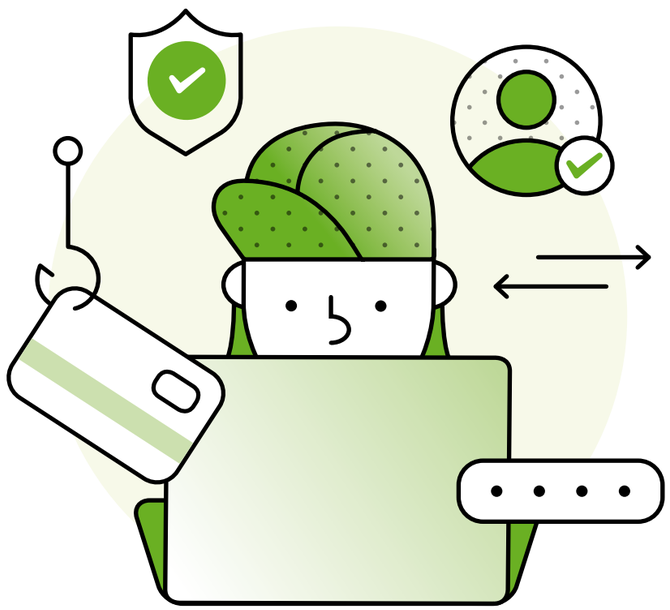
Urlaubsfotos in sozialen Netzwerken posten, neue Outfits am Laptop bestellen und Bankgeschäfte via Onlinebanking regeln – all diese Aktivitäten im Netz hinterlassen digitale Spuren. Miteinander verknüpft, führt die Gesamtheit dieser Spuren zu einer neuen Art von Online-Identität, dem Digitalen Ich – letztjähriges Fokusthema im DsiN-Sicherheitsindex.

Abb. 25 / Sicherheitsindex 2022
Das Digitale Ich aus Verbrauchersicht

64,2 %
haben Kontrolle über ihr Digitales Ich.

69,7 %
gehen sorgsam mit den Daten rund um das Digitale Ich um.

53,6 %
glauben, dass sie sich sowieso nicht gegen Datenmissbrauch schützen können.



56,6 %
sehen Missbrauch von persönlichen Daten in sozialen Netzwerken als Risiko.

57,6 %
fürchten sich vor Identitätsbetrug beim Onlinebanking.

Mittelmäßige Kontrolle über das Digitale Ich
69,7 Prozent glauben, sie gehen sehr sorgsam mit Daten um und hoffen so, Risiken für ihr Digitales Ich zu reduzieren. Trotzdem schätzen die Verbraucher:innen die Kontrolle über ihr Digitales Ich insgesamt eher mittelmäßig ein. Fast die Hälfte der Befragten (48,5 Prozent) ist dieser Meinung. Allerdings hat sich das Kontrollempfinden im Vergleich zum letzten Jahr etwas erhöht. 35,9 Prozent – und damit 4,1 Prozentpunkte weniger als im Vorjahr – geben an, nur eine geringe oder sehr geringe Kontrolle darüber zu haben. 15,7 Prozent (+1,7 Prozent) haben dagegen eine hohe oder sehr hohe Kontrolle über ihr Digitales Ich.

Dennoch befürchtet mehr als jede:r zweite Verbraucher:in (53,6 Prozent), dass die technischen Möglichkeiten eines Missbrauchs der Daten zum Digitalen Ich so vielfältig sind, dass man sich sowieso nicht gut schützen könne. Ähnlich viele Nutzer:innen glauben zudem, dass sie als „gläserne Konsument:innen“ nichts verbergen können (52,2 Prozent).

Risiken: Banking, Shopping und Social Media
Die größten Risiken für ihr Digitales Ich sehen die Nutzer:innen in Form eines Missbrauchs der persönlichen Daten beim Onlinebanking (57,6 Prozent), dicht gefolgt von Onlineshopping (57,3 Prozent), und in sozialen Netzwerken oder ähnlichen Diensten (56,6 Prozent).

Die größten Risiken für ihr Digitales Ich sehen die Nutzer:innen in Form eines Missbrauchs der persönlichen Daten beim Onlinebanking, dicht gefolgt von Onlineshopping

Besonders hoch schätzen Verbraucher:innen im Alter von 60 bis 69 Jahren diese Risiken ein: Der Betrug beim Onlineshopping erreicht mit 74,2 Prozent einen Spitzenwert, gefolgt von Datenmissbrauch bei Onlinebanking (71,3 Prozent) und Social Media oder ähnlichen Diensten (68,2 Prozent).

Wunsch nach Versicherung und Aufklärung in der Schule
Folglich würden sich in diesem Jahr noch mehr Menschen (+4,0 Prozentpunkte) am liebsten gegen Missbrauch der Daten versichern, um im Falle eines Falles eine Entschädigung zu bekommen (51,4 Prozent). Auch der Wunsch nach Aufklärung bleibt entsprechend stark ausgeprägt: 76,0 Prozent der Befragten sind der Meinung, dass das Thema „Digitales Ich“ bereits in der Schule behandelt werden müsste. 71,7 Prozent wünschen sich zudem eine zentrale Stelle, die die Menschen bei Fragen zum Digitalen Ich berät. Hier sollten speziell ältere Nutzer:innen mit ihren Sorgen stärker berücksichtigt werden.

DsiN-Angebote zum Thema „Digitales Ich“

Cyberfibel: Was müssen Verbraucher:innen wissen, um sich selbstbestimmt und sicher durch die digitale Welt bewegen zu können und ihr Digitales Ich zu schützen? Dazu informiert die Lebenswelt „Online einkaufen und bezahlen“:
cyberfibel.de

Digitalführerschein (DiFü): Tagesaktuelle Informationen zu Themen und Anwendungen des digitalen Alltags und die Möglichkeit, die eigene digitale Kompetenz auszubauen und zu zertifizieren: Der DiFü ist ein deutschlandweit einheitliches Weiterbildungsangebot, um digitale Teilhabe zu stärken:
difü.de

DsiN-Ratgeberreihe: Die DsiN-Ratgeberreihe informiert rund um Themen für einen sicheren digitalen Alltag. 2022 auch zum Thema „Das Digitale Ich – selbstbestimmt surfen“:
sicher-im-netz.de/ratgeberreihe

Abb. 26 / Sicherheitsindex 2022

Digitale Bürgerportale aus Verbrauchersicht

37,6 %

halten die Nutzung für sicher oder sehr sicher.

35,3 %

finden Bequemlichkeit im Umgang wichtiger als Sicherheit und Datenschutz.

18,8 %

halten die Nutzung von Angeboten der öffentlichen Hand für gefährlich.

44,4 %

sehen Sicherheits- und Datenschutzbedenken als größtes Hindernis für die Nutzung.

44,4 %

würden Angebote stärker nutzen, wenn Zugang, Auffindbarkeit und Nutzung einfacher wären.

39,9 %

würden Angebote stärker nutzen, wenn es mehr Unterstützung bei Fragen (auch Datensicherheit) geben würde.

Digitale Bürgerportale

Digitale Angebote der öffentlichen Hand ermöglichen es für Bürger:innen, Verwaltungsleistungen online durchzuführen und erleichtern auf diese Weise etwa die Ummeldung des Wohnsitzes oder die Beantragung des Kindergeldes. Gut ein Viertel der Befragten (24,6 Prozent) nutzt diese Angebote 2022. Das sind mit einem Plus von 7,5 Prozentpunkten deutlich mehr Verbraucher:innen als noch im Vorjahr (17,1 Prozent).

Erhöhtes Sicherheitsempfinden trotz vermehrter Vorfälle

Mit der wachsenden Verbreitung hat sich auch die Zahl der Sicherheitsvorfälle bei der Nutzung der Onlineangebote der öffentlichen Hand erhöht. 2022 geben 7,7 Prozent an, dass sie Sicherheitsprobleme hatten. 2021 waren es noch 5,1 Prozent. Dennoch ist die Einschätzung der Sicherheit dieser Angebote deutlich angestiegen. 37,6 Prozent der Befragten halten die Angebote für sicher oder sehr sicher. Dies ist eine Steigerung um 8,8 Prozentpunkte im Vergleich zum Vorjahr.

Forderung nach mehr Datenschutz und besserem Zugang

Bei der Frage, was die Verbraucher:innen motivieren würde, die Onlineangebote der öffentlichen Hand stärker zu nutzen, spielen zwei Punkte eine gleich wichtige Rolle: Zum einen geben die Befragten hier den Abbau von Sicherheits- und Datenschutzbedenken an. Zum anderen wünschen sich Nutzer:innen einen leichteren Zugang, eine bessere Auffindbarkeit und einfachere Nutzung. Jeweils 44,4 Prozent der Verbraucher:innen sind dieser Meinung. Zusätzliche Unterstützung, zum Beispiel beim Thema Datensicherheit, wünschen sich 39,9 Prozent.

Rund ein Drittel der Befragten (35,3 Prozent) gibt allerdings an, dass sie Kompromisse bei Datenschutz oder Datensicherheit eingehen würden, wenn sie dadurch Zeit oder Geld sparen. 2021 war nur knapp jede vierte befragte Person dieser Meinung (28,4 Prozent).

Die Bereitschaft, digitale Angebote der öffentlichen Hand zu nutzen, steigt.

Popularität wächst – und mit ihr die Anforderungen

Die Bereitschaft, digitale Angebote der öffentlichen Hand zu nutzen, steigt. Damit noch mehr Verbraucher:innen online auf Verwaltungsservices zugreifen, ist die Anbieterseite gefordert, die bestehenden Sicherheits- und Datenschutzbedenken zu adressieren, Zugangsbarrieren abzubauen und eine einfachere Nutzung der Dienste im Sinne der Verbraucher:innen sicherzustellen.

DsiN-Angebote zum Thema „Digitale Bürgerportale“

Cyberfibel: Was müssen Verbraucher:innen wissen, um sich selbstbestimmt und sicher durch die digitale Welt bewegen zu können und ihr Digitales Ich zu schützen? Dazu informiert die Lebenswelt „Online einkaufen und bezahlen“:
cyberfibel.de

Digital-Kompass: Der Digital-Kompass stellt kostenfreie Angebote für Senior:innen rund um Internet und Co. bereit, darunter Lehr- und Lernmaterialien, Seminare und Schulungen, u. a. zum Thema „Digitales Rathaus“:
digital-kompass.de

Digitaler Engel: Sicherer Einstieg in das Internet mit dem Digitalen Engel für ältere Menschen: Auf der (digitalen) Aufklärungstour vermittelt das Team Kompetenzen für die digitale Welt aus dem Alltag von Senior:innen:
digitaler-engel.org

SiBa-App: Das Sicherheitsbarometer (SiBa) informiert über relevante und aktuelle Cyberangriffe und -risiken, gibt passende Sicherheitstipps und zeigt konkrete Schutzmöglichkeiten auf:
sicher-im-netz.de/sicherheitsbarometer

DsiN-Angebote
sicher-im-netz.de/digitale-buergerportale

Smarte Versicherungstarife

Smarte Versicherungen greifen auf persönliche Daten wie Verhaltens- und Gesundheitsdaten zurück, um durch individuelle Bewertungen passgenaue Tarife und eine entsprechende Vorsorge zu ermöglichen. Sie bestehen etwa bei Gebäude-, Auto- oder Gesundheitsversicherungen. Smarte Versicherungstarife waren 2019 Fokusthema des Sicherheitsindex und wachsen seither in ihrer Bekanntheit weiter an. Mit 28,8 Prozent steigt der Anteil der Befragten, denen schon ein smarter Versicherungstarif angeboten wurde, um 7,3 Prozentpunkte.

Abb. 27 / Sicherheitsindex 2022
Smarte Versicherungstarife aus Verbrauchersicht

Offenheit gegenüber smarten Versicherungstarifen wächst
Immer mehr Verbraucher:innen (34,1 Prozent) können sich vorstellen, einen smarten Versicherungstarif in Anspruch zu nehmen. Das ist ein Zuwachs von 5,2 Prozentpunkten. Ebenfalls sind mit einem Plus von 8,2 Prozentpunkten auch mehr Nutzer:innen (37,2 Prozent) der Meinung, dass das Tracking des Verhaltens oder Lebensstils dazu beiträgt, Versicherungstarife zu einem gerechteren Preis anzubieten.

Grundskepsis bleibt vorhanden
Nach wie vor sind die Vorbehalte gegen smarte Versicherungstarife jedoch hoch. 63,6 Prozent der Verbraucher:innen bleiben skeptisch und glauben, dass das Sammeln und Auswerten von Daten zum eigenen Lebensstil zu erhöhten Datenschutzrisiken wie Missbrauch, Manipulation und Diebstahl führen können. 62,8 Prozent sind der Meinung, dass von Versicherungen gesammelte Daten auch von Unternehmen, Arbeitgebern oder dem Staat zu anderen Zwecken genutzt werden. Allerdings zeigt sich bei diesen Vorbehalten eine leicht rückläufige Tendenz (-1,2 Prozentpunkte und -1,5 Prozentpunkte). Mit 52 Prozentpunkten sehen 2022 jedoch mehr Befragte einen Grundgedanken der Versicherungsgemeinschaft („alle für einen“) in Gefahr (+4,9 Prozentpunkte).

63,6 Prozent der Verbraucher:innen bleiben skeptisch und glauben, dass das Sammeln und Auswerten von Daten zum eigenen Lebensstil zu erhöhten Datenschutzrisiken führen können.

Versicherer und Versicherte gleichermaßen verantwortlich
Wenn es darum geht, wer für die Sicherheit beim Thema „Versicherung 2.0“ verantwortlich ist, schreiben die Befragten sowohl den Versicherten als auch den Versicherern gleichermaßen eine wichtige Rolle zu: 65,2 Prozent der Verbraucher:innen sehen die Versicherer in der Pflicht und 62,9 Prozent verorten die Verantwortung bei sich selbst.

DsiN-Angebote zum Thema „Smarte Versicherungstarife“

Deutschland Dialog für digitale Aufklärung: Im Dialog wirken engagierte Organisationen aus Wirtschaft und Zivilgesellschaft im Verbund mit der Bundesregierung zusammen, um den direkten Dialog mit Menschen im privaten und beruflichen Umfeld aktiv zu gestalten.
sicher-im-netz.de/deutschland-dialog-für-digitale-aufklärung

KInsights!: Künstliche Intelligenz (KI) wird heute bereits in vielen Bereichen genutzt. Mit KInsights! kann man sie spielerisch entdecken, z. B. in den Themenwelten „Risikobewertung“ und „Schaden online melden“:
kinsights.de

SiBa-App: Das Sicherheitsbarometer (SiBa) informiert über relevante und aktuelle Cyberangriffe und -risiken, gibt passende Sicherheitstipps und zeigt konkrete Schutzmöglichkeiten auf:
sicher-im-netz.de/sicherheitsbarometer

DsiN-Angebote
sicher-im-netz.de/smarte-versicherungstarife

Abb. 28 / Sicherheitsindex 2022

Digitale Gesundheits- und Fitnessdienste aus Verbrauchersicht

58,0 %

haben Sicherheitsbedenken beim Anlegen und Nutzen einer elektronischen Patientenakte.

54,5 %

halten Fitness- und Gesundheitsapps für gefährlich und sehr gefährlich.

25,3 %

finden unterstützende Onlinedienste im Gesundheitswesen (Onlineterminbuchung, elektronische Patientenakte, Video- und Onlinesprechstunde etc.) gefährlich oder sehr gefährlich.

13,6 %

nutzen Fitness- und Gesundheitsprogramme.

15,5 %

nutzen digitale Angebote zur medizinischen Versorgung (Onlinesprechstunde etc.).

Digitale Gesundheits- und Fitnessdienste

Ob Fitnessuhr, Schrittzähler oder Onlineterminbuchungen in Arztpraxen – digitale Geräte und Dienste im Gesundheits- und Fitnessbereich erfreuen sich bei Verbraucher:innen in Deutschland einer wachsenden Popularität. 13,6 Prozent der Verbraucher:innen nutzen Fitness- und Gesundheitsprogramme (Apps zur Kontrolle des Schlafverhaltens, zur Messung des Blutzuckers etc.) (+0,2 Prozentpunkte) und 15,5 Prozent greifen auf unterstützende Onlinedienste im Gesundheitswesen (Onlineterminbuchung, Video- und Onlinesprechstunde etc.) zurück (+1,9 Prozentpunkte).

Allgemeine Unsicherheit wächst
Das Verunsicherungsgefühl steigt 2022 etwas stärker. Im letzten Jahr empfanden 20,7 Prozent Fitness- und Gesundheitsprogramme (Apps zur Messung von Schlafverhalten, zur Kontrolle des Blutzuckers etc.) als gefährlich oder sehr gefährlich, in diesem Jahr sind es 23,3 Prozent (+2,6 Prozentpunkte). Auch unterstützende Onlinedienste im Gesundheitswesen wie Onlineterminbuchung, elektronische Patientenakte oder Video- und Onlinesprechstunde werden von den deutschen Nutzer:innen 2022 – verglichen mit dem Vorjahr – als risikoreicher eingeschätzt. Ein Viertel ist dieser Meinung (25,3 Prozent). 2021 waren es noch 22,2 Prozent der Befragten.

Risikoempfinden nimmt zu
Mehr als jede:r zweite Verbraucher:in sieht dabei allem voran drei Gefahrenquellen. Das höchste Risiko besteht für die Befragten zu 58,6 Prozent im Sammeln und Analysieren von personenbezogenen Gesundheitsdaten in Datenbanken (+0,9 Prozentpunkte). Auf Rang zwei folgt mit 58,1 Prozent der digitale Austausch gesundheitsbezogener Daten zwischen Patient:innen, ärztlichen Fachkräften und anderen (+2,4 Prozentpunkte). Das dritthöchste Risiko wird von 58 Prozent im Anlegen und der Nutzung einer elektronischen Patientenakte gesehen (+1,5 Prozentpunkte).

Das höchste Risiko besteht für die Befragten im Sammeln und Analysieren von personenbezogenen Gesundheitsdaten in Datenbanken.

Am wenigsten kritisch, aber ebenso mit einem Zuwachs versehen, ist für Verbraucher:innen die Nutzung von Onlineterminvereinbarungen in Arztpraxen. 35,1 Prozent empfinden hier ein Risiko und damit sind es 3,8 Prozent mehr als im Vorjahr.

Adressieren der Risiken in der Aufklärung und Gestaltung
Angesichts der wachsenden Verbreitung digitaler Gesundheits- und Fitnessdienste gilt es, die zunehmende Unsicherheit und das Risikoempfinden der Nutzer:innen, insbesondere von Anbieterseite aus, zu adressieren und bei der Ausgestaltung der Dienste zu berücksichtigen.

DsiN-Angebote zum Thema „Digitale Gesundheits- und Fitnessdienste“

Digital-Kompass: Der Digital-Kompass stellt kostenfreie Angebote für Senior:innen rund um Internet und Co. bereit, darunter Lehr- und Lernmaterialien, Seminare und Schulungen, u. a. zum Thema „Gesundheit digital“:
digital-kompass.de

Digitaler Engel: Sicherer Einstieg in das Internet mit dem Digitalen Engel für ältere Menschen: Auf der (digitalen) Aufklärungstour vermittelt das Team Kompetenzen für die digitale Welt aus dem Alltag von Senior:innen:
digitaler-engel.org

KInsights!: Künstliche Intelligenz (KI) wird heute bereits in vielen Bereichen genutzt. Mit KInsights! kann man sie spielerisch entdecken, z. B. in den Szenarien „Medizinische Diagnostik“ und „Unterstützung bei Sehbehinderungen“:
kinsights.de

SiBa-App: Das Sicherheitsbarometer (SiBa) informiert über relevante und aktuelle Cyberangriffe und -risiken, gibt passende Sicherheitstipps und zeigt konkrete Schutzmöglichkeiten auf:
sicher-im-netz.de/sicherheitsbarometer

DsiN-Angebote
sicher-im-netz.de/digitale-gesundheit

Digitale Vernetzung

Soziale Netzwerke wie Facebook, Twitter und Co. sowie Messenger auf mobilen Geräten (WhatsApp, Telegram etc.) werden von der Mehrheit der Verbraucher:innen genutzt, nämlich zu 54,3 und 56 Prozent. Allerdings ist die Nutzung mit -3,8 Prozentpunkten und -5,1 Prozentpunkten in beiden Fällen leicht rückläufig. Gleichzeitig werden die sozialen Netzwerke, verglichen mit dem Vorjahr, von mehr Verbraucher:innen (40,4 Prozent) als gefährlich oder sehr gefährlich eingestuft (+3,1 Prozentpunkte).

Abb. 29 / Sicherheitsindex 2022
Digitale Netzwerke aus Verbrauchersicht

40,4 %
halten soziale Netzwerke für gefährlich oder sehr gefährlich.

34,5 %
halten die Veröffentlichung von eigenen Inhalten für gefährlich oder sehr gefährlich.

11,1 %
waren in den letzten zwölf Monaten Opfer von Mobbing/Belästigungen/Rufschädigung in sozialen Netzwerken.

9,4 %
waren Opfer von Identitätsdiebstahl in sozialen Netzwerken.

54,3 %
nutzen soziale Netzwerke .

19,0 %
veröffentlichen Content.

Anzahl an Sicherheitsvorfällen auf Social Media hat sich erhöht
Social-Media-Nutzer:innen sind 2022 etwas aktiver. 19 Prozent veröffentlichen Content (Texte, Fotos, Videos in einem Blog, bei Instagram, YouTube etc.) und damit 1,9 Prozentpunkte mehr als im Vorjahr. Mit 34,5 Prozent halten mehr Nutzer:innen dies für gefährlich oder sehr gefährlich (+3,4 Prozentpunkte).

Entsprechend beklagen Verbraucher:innen mehr Sicherheitsvorfälle als noch 2021. So stiegen die Vorfälle durch Mobbing/Belästigung/Rufschädigung um 2 Prozentpunkte auf 11,1 Prozent an. Die Vorfälle aufgrund von sogenanntem Spoofing (Identitätsdiebstahl/missbräuchliche Nutzung personenbezogener Daten durch Dritte) erhöhten sich sogar um 3,2 Prozentpunkte auf 9,4 Prozent.

Fatalismus, Überforderung und Skepsis steigen
12,2 Prozent der befragten Nutzer:innen (+2,1 Prozentpunkte) geben an, dass Sicherheitsfragen für sie zweitrangig sind, wenn ein digitales Angebot einen hohen Mehrwert besitzt. 27,4 Prozent (+6,3 Prozentpunkte) fühlen sich von neuen digitalen Angeboten überfordert. Da ist es nicht verwunderlich, dass die Zahl derer, die gerne neue digitale Angebote ausprobieren, um 2,7 Prozentpunkte auf 20,5 Prozent zurückgegangen ist.

Aufklärung über Risiken und Schutzmaßnahmen
Soziale Netzwerke und Messenger stehen bei den Verbraucher:innen weiterhin hoch im Kurs. Die steigenden Sicherheitsvorfälle treffen auf eine wachsende Überforderung der Nutzer:innen bei der Anwendung digitaler Dienste, während das Verunsicherungsgefühl in diesem Bereich rückläufig ist. So kommt es, dass zwar 93,9 Prozent die Privatsphäre- und Zugriffsrechteeinstellungen bei Messenger-Diensten etc. kennen, allerdings nur jede:r zweite Befragte (55,4 Prozent) diese auch anpasst.

Digitale Aufklärungsarbeit sollte entsprechend darauf abzielen, für die Risiken bei fehlenden Sicherheitsmaßnahmen zu sensibilisieren, zu einer Umsetzung der verfügbaren Sicherheitseinstellungen zu motivieren und im Zuge dessen auch verständliche Schutzanleitungen zur Verfügung zu stellen.

DsiN-Angebote zum Thema „Digitale Vernetzung“

Cyberfibel: Was müssen Verbraucher:innen wissen, um sich selbstbestimmt und sicher durch die digitale Welt bewegen zu können und ihr Digitales Ich zu schützen? Dazu informiert die Lebenswelt „Online einkaufen und bezahlen“:
cyberfibel.de

Digitalführerschein (DiFü): Tagesaktuelle Informationen zu Themen und Anwendungen des digitalen Alltags und die Möglichkeit, die eigene digitale Kompetenz auszubauen und zu zertifizieren: Der DiFü ist ein deutschlandweit einheitliches Weiterbildungsangebot, um digitale Teilhabe zu stärken:
difü.de

Digital-Kompass: Der Digital-Kompass stellt kostenfreie Angebote für Senior:innen rund um Internet und Co. bereit, darunter Lehr- und Lernmaterialien, Seminare und Schulungen, u. a. zum Thema „Gesundheit digital“:
digital-kompass.de

Digitale Nachbarschaft: Die Digitale Nachbarschaft macht Vereine und ehrenamtlich Engagierte fit für’s Netz – mit Workshops, Handbüchern, Lernvideos und vielem mehr, u. a. zum Thema „Social-Media-Nutzung im Ehrenamt“:
digitale-nachbarschaft.de

DsiN-Angebote
sicher-im-netz.de/digitale-vernetzung

Abb. 30 / Sicherheitsindex 2022
Das vernetzte Zuhause aus Verbrauchersicht

25,4 %
halten vernetzte Unterhaltungselektronik für gefährlich oder sehr gefährlich.

31,1 %
halten vernetzte Haustechnik für gefährlich oder sehr gefährlich.

7,7 %
haben in den letzten zwölf Monaten Manipulation der Hausvernetzung erlebt.

15,4 %
nutzen vernetzte Unterhaltungselektronik (Streaming-Boxen, Smart-TVs, Home Assistants wie Alexa, Google Home etc.).

11,0 %
nutzen vernetzte Haustechnik (Jalousien, Heizung, SmartMeter, Streaming-Boxen etc.).

Das vernetzte Zuhause

Geräte und Anwendungen, die eine digitale Steuerung des Wohnraums ermöglichen, etwa die Steuerung von Licht oder Heizung, zählen zum Internet of Things (kurz: IoT). Auch Unterhaltungselektronik wie Smart-TVs und Home Assistants lassen sich diesem Smarthome-Bereich zuordnen.

Haustechnik wird beliebter, Unterhaltungselektronik stagniert
Die vernetzte Haustechnik hat sich in den letzten Jahren mehr und mehr in Deutschland verbreitet. In diesem Jahr erreicht die Nutzung 11 Prozentpunkte (+0,7 Prozentpunkte). Zum Vergleich: 2015 lag dieser Wert noch bei 2,3 Prozent. Der Bereich der Unterhaltungselektronik dagegen ist in diesem Jahr leicht rückläufig. Haben 2021 noch 16,5 Prozent der Befragten eine Nutzung angegeben, sind es nun nur noch 15,4 Prozent (-1,1 Prozent).

Verunsicherungsgefühl der Haustechnik steigt mit der Nutzung
Parallel zur steigenden Verbreitung von Geräten und Anwendungen der vernetzten Haustechnik fühlen sich die Verbraucher:innen in diesem Jahr in diesem Bereich auch stärker gefährdet. So steigt das Verunsicherungsgefühl von 27,9 auf 31,1 Prozent und damit um 3,2 Prozentpunkte an. Anders sieht es bei der Unterhaltungselektronik aus. Hier hat sich das Verunsicherungsgefühl deutlich um 6,4 Prozentpunkte auf 25,4 Prozent verringert.

Zahl der Sicherheitsvorfälle nimmt zu

Insgesamt ist die Anzahl der Sicherheitsvorfälle in den letzten zwölf Monaten gestiegen.

Insgesamt ist die Anzahl der Sicherheitsvorfälle in den letzten zwölf Monaten gestiegen. 7,7 Prozent der Verbraucher:innen gaben an, dass ihre Hausvernetzung manipuliert worden ist. Im Vergleich zu 2021 ist dies ein Plus von 3,5 Prozentpunkten. Mit Blick auf alle weiteren abgefragten IT-Sicherheitsvorfälle bleibt dies jedoch der niedrigste Wert.

Dennoch gilt, dass mit wachsender Nutzung tendenziell auch das Gefahrenpotenzial steigt. Angesichts der wachsenden Verbreitung von vernetzter Haustechnik sollten Verbraucher:innen frühzeitig ausreichend über mögliche Risiken informiert werden.

DsiN-Angebote zum Thema „vernetztes Zuhause“

Cyberfibel: Was müssen Verbraucher:innen wissen, um sich selbstbestimmt und sicher durch die digitale Welt bewegen zu können und ihr Digitales Ich zu schützen? Dazu informiert die Lebenswelt „Online einkaufen und bezahlen“:
cyberfibel.de

Digitalführerschein (DiFü): Tagesaktuelle Informationen zu Themen und Anwendungen des digitalen Alltags und die Möglichkeit, die eigene digitale Kompetenz auszubauen und zu zertifizieren: Der DiFü ist ein deutschlandweit einheitliches Weiterbildungsangebot, um digitale Teilhabe zu stärken:
difü.de

Digital-Kompass: Der Digital-Kompass stellt kostenfreie Angebote für Senior:innen rund um Internet und Co. bereit, u. a. zum Thema „Smart Home“ und „Digitale Alltagshelfer“:
digital-kompass.de

KInsights!: Künstliche Intelligenz (KI) wird heute bereits in vielen Bereichen genutzt. Mit KInsights! kann man sie spielerisch entdecken, z. B. im Szenario „KI-gestütztes Smart Home“:
kinsights.de

DsiN-Angebote
sicher-im-netz.de/vernetztes-zuhause

Einkaufen im Internet

Auch nach dem zweiten Jahr der Coronapandemie erfreut sich Onlineshopping einer großen Beliebtheit. Mit 72,7 Prozent nutzen 2022 allerdings weniger Befragte das Internet zum Einkaufen als noch im letzten Jahr (-3,9 Prozentpunkte). Grund hierfür kann ein deutlich erhöhtes Verunsicherungsgefühl sein. 2021 waren 20,7 Prozent der Nutzer:innen der Meinung, das Einkaufen im Internet sei gefährlich oder sehr gefährlich. In diesem Jahr ist es genau ein Viertel.

Abb. 31 / Sicherheitsindex 2022
Einkaufen im Internet aus Verbrauchersicht

25,0 %
halten Onlineshopping/ Reisebuchungen für gefährlich oder sehr gefährlich.

13,0 %
waren in den letzten zwölf Monaten Opfer von Betrug beim Onlineeinkauf.

10,6 %
waren in den letzten zwölf Monaten vom Ausspähen ihrer Zugangsdaten zu einem Onlineshop betroffen.

72,7 %
haben schon mal online eingekauft.

73,1 %
nutzen sichere Zahlungssysteme für den Onlineeinkauf.

53,6 %
achten auf Gütesiegel bei Onlineshops.

Mehr Sicherheitsvorfälle als 2021
Dieses Verunsicherungsgefühl spiegelt sich auch konkret in einem Anstieg der Sicherheitsvorfälle wider. Die Zahl derer, die in den letzten zwölf Monaten Opfer eines Betrugs beim Onlineshopping wurden, hat sich 2022 weiter um 1,6 Prozentpunkte auf 13 Prozent erhöht.

Es geben auch mehr Befragte an, dass ihre Zugangsdaten zu Onlineshops ausgespäht wurden. Bei 10,6 Prozent ist dies 2022 der Fall. Im letzten Jahr waren nur 7,8 Prozent betroffen. Mehr Sicherheitsvorfälle beklagen die Befragten ebenso beim Bezahlen im Internet und bei der Nutzung von Kreditkarten. 10,7 Prozent der Befragten (+3,4 Prozentpunkte) wurden 2022 beim Bezahlen betrogen und 8,9 Prozent (+2,3 Prozentpunkte) geben Sicherheitsvorfälle beim Nutzen der Kreditkarte im Internet an.

Geringeres Sicherheitsverhalten als im Vorjahr
Während sich 2022 die Bekanntheit von sicheren Zahlungssystemen nur geringfügig um 0,1 Prozentpunkte auf 95,3 Prozent erhöht hat, ist die Nutzung deutlich um 4,8 Prozentpunkte auf 73,1 Prozent zurückgegangen. 90,1 Prozent der Verbraucher:innen geben außerdem an, dass ihnen Gütesiegel für Onlineshops bekannt sind und 53,6 Prozent diese beim Einkaufen im Internet beachten. Das sind Einbußen von 2,3 Prozentpunkten hinsichtlich der Bekanntheit und 6,1 Prozentpunkten bezüglich der Nutzungsrate.

Ein ähnliches Bild zeigt sich bei der Überprüfung der Vertrauenswürdigkeit von Webseiten. 91,5 Prozent (-0,9 Prozentpunkte) kennen zwar die Funktionsweise und Anwendungsmöglichkeiten dieser Sicherheitsmaßnahme, lediglich 55,3 Prozent wenden dieses Wissen auch an. 2021 waren es noch 58 Prozent.

Anwendung von Sicherheitswissen bleibt verbesserungswürdig
Auch wenn sich das Sicherheitswissen in Teilen leicht verbessert, bleibt die Schere zwischen der Kenntnis und Umsetzung relevanter Sicherheitsmaßnahmen im Bereich des Onlineshoppings deutlich zu groß. Die Aufklärungsarbeit muss so gestaltet sein, dass sie Verbraucher:innen dazu motiviert, ihr Sicherheitswissen aktiv anzuwenden.

DsiN-Angebote zum Thema „Einkaufen im Internet“

Cyberfibel: Was müssen Verbraucher:innen wissen, um sich selbstbestimmt und sicher durch die digitale Welt bewegen zu können und ihr Digitales Ich zu schützen? Dazu informiert die Lebenswelt „Online einkaufen und bezahlen“:
cyberfibel.de

Digital-Kompass: Der Digital-Kompass stellt kostenfreie Angebote für Senior:innen rund um Internet und Co. bereit, u. a. zum Thema „Smart Home“ und „Digitale Alltagshelfer“:
digital-kompass.de

Digitaler Engel: Sicherer Einstieg in das Internet mit dem Digitalen Engel für ältere Menschen: Auf der (digitalen) Aufklärungstour vermittelt das Team Kompetenzen für die digitale Welt aus dem Alltag von Senior:innen:
digitaler-engel.org

DsiN-Ratgeberreihe: Die DsiN-Ratgeberreihe informiert rund um Themen für einen sicheren digitalen Alltag. Auch zum Thema „Online einkaufen und bezahlen - sicher shoppen“:
sicher-im-netz.de/ratgeberreihe

DsiN-Angebote
sicher-im-netz.de/einkaufen-im-internet

Onlinebanking

Die Nutzung von Bankgeschäften im Internet ist in diesem Jahr rückläufig. Nachdem 2021 noch 61,1 Prozent der Befragten im Bereich Onlinebanking aktiv waren, sind es 2022 nur noch 56,4 Prozent (-4,7 Prozentpunkte). Ein möglicher Grund ist die wachsende Gefahreneinschätzung. 36,6 Prozent sehen Onlinebankgeschäfte als (sehr) gefährlich an, im Vorjahr lag dieser Wert noch 2,5 Prozentpunkte darunter bei 34,1 Prozent.

Abb. 32 / Sicherheitsindex 2022
Onlinebanking aus Verbrauchersicht

56,4 %
tätigen Onlinebankgeschäfte.

36,6 %
halten Onlinebanking für gefährlich oder sehr gefährlich.

9,9 %
waren vom Ausspähen der Zugangsdaten zum Onlinebanking betroffen.

21,5 %
nutzen kontaktloses Bezahlen via Smartphone.

58,5 %
achten auf verschlüsselte Datenverbindung bei Onlinebanking/Onlineshopping.

Mehr Sicherheitsvorfälle, weniger Sicherheitsverhalten
Mit Blick auf die Sicherheitsvorfälle und das Sicherheitswissen offenbaren sich beim Onlinebanking ähnliche Entwicklungen wie im Bereich des Onlineshoppings. 9,9 Prozent der Nutzer:innen vermelden, dass bei ihnen in den letzten zwölf Monaten Zugangsdaten für Onlinebankinganwendungen ausgespäht wurden. Das entspricht einem Anstieg von 3,3 Prozentpunkten.

Die wachsende Wissens-Verhaltens-Lücke bietet eine Erklärung hierfür. Nahezu unverändert bleibt das Wissen der Verbraucher:innen in Bezug auf verschlüsselte Verbindungen beim Onlinebanking. 93,4 Prozent (Vorjahr: 93,3 Prozent) der Befragten ist diese Möglichkeit bekannt. Dagegen wenden 2022 deutlich weniger dieses Wissen auch an. Nur 58,5 Prozent der befragten Nutzer:innen tun dies. Ein Jahr zuvor waren es noch 63,0 Prozent.

Um diesem Motivationsdefizit beizukommen, gilt es allen voran aufzuzeigen, dass sich der eigene Schutz bei Bankgeschäften im Internet bereits durch einfache Schritte wirksam erhöhen lässt.

Sicherheitswissen wird zu selten angewandt
Die Sicherheitsrisiken sind den Verbraucher:innen durchaus bewusst. Schließlich machen sie die größten Gefahren für ihr Digitales Ich bei einem Missbrauch der persönlichen Daten beim Onlinebanking aus (57,6 Prozent). Dennoch wird das vorhandene Sicherheitswissen viel zu selten auch in der Praxis umgesetzt.

Um diesem Motivationsdefizit beizukommen, gilt es allen voran aufzuzeigen, dass sich der eigene Schutz bei Bankgeschäften im Internet bereits durch einfache Schritte wirksam erhöhen lässt.

DsiN-Angebote zum Thema „Onlinebanking“

Cyberfibel: Was müssen Verbraucher:innen wissen, um sich selbstbestimmt und sicher durch die digitale Welt bewegen zu können und ihr Digitales Ich zu schützen? Dazu informiert die Lebenswelt „Online einkaufen und bezahlen“:
cyberfibel.de

Digitalführerschein (DiFü): Tagesaktuelle Informationen zu Themen und Anwendungen des digitalen Alltags und die Möglichkeit, die eigene digitale Kompetenz auszubauen und zu zertifizieren: Der DiFü ist ein deutschlandweit einheitliches Weiterbildungsangebot, um digitale Teilhabe zu stärken:
difü.de

Digital-Kompass: Der Digital-Kompass stellt kostenfreie Angebote für Senior:innen rund um Internet und Co. bereit, u. a. zum Thema „Smart Home“ und „Digitale Alltagshelfer“:
digital-kompass.de

Digitale Nachbarschaft: Die Digitale Nachbarschaft macht Vereine und ehrenamtlich Engagierte fit für’s Netz – mit Workshops, Handbüchern, Lernvideos und vielem mehr, u. a. zum Thema „Social-Media-Nutzung im Ehrenamt“:
digitale-nachbarschaft.de

DsiN-Angebote
sicher-im-netz.de/online-banking

Bewusstsein für Selbstwirksamkeit stärken

Mit der Verbreitung digitaler Angebote steigt auch die Anzahl an Sicherheitsvorfällen – obwohl die Sicherheitskompetenz auf hohem Niveau bleibt. Der Hauptgrund: Das Sicherheitswissen wird zu selten angewandt, um ausreichenden IT-Schutz zu gewährleisten. Die Auswirkungen dessen zeigen sich in diesem Jahr besonders deutlich – und offenbaren ein fehlendes Bewusstsein der Selbstwirksamkeit.

Mehr Sicherheitsvorfälle in nahezu allen Lebensbereichen
In fast allen abgefragten Lebensbereichen beklagen Verbraucher:innen mehr Sicherheitsvorfälle als noch 2021. Das betrifft die Bereiche, die in diesem Jahr ein Nutzungsplus erfahren wie etwa IoT-Anwendungen oder Dienste der öffentlichen Hand, gilt aber auch für Gebiete, die 2022 weniger stark genutzt werden. So verzeichnen Onlinebanking, Onlineshopping und soziale Netzwerke zwar Einbußen in der Nutzungsrate, legen jedoch allesamt bei den Sicherheitsvorfällen zu.

Bildungsarbeit mit Bezug zur Lebenswelt
Angesichts der sich stetig verändernden Anwendungsbereiche ist ein zentraler Faktor in der Aufklärungsarbeit, die Schutzkompetenzen der Verbraucher:innen fortwährend weiterzuentwickeln. Dabei gilt es, neue Trends sowie eine sich wandelnde Alltagsgestaltung zu berücksichtigen, die mit der Nutzung neuer digitaler Anwendungen einhergeht.

Digitale Bildungsarbeit muss folglich stets einen lebensweltlichen Bezug herstellen und kann etwa durch anschauliche Praxisbeispiele die Relevanz von IT-Sicherheit für den Alltag verdeutlichen. Im Kern muss dabei die Vermittlung von transferfähigem Basiswissen stehen, das sich agil auf neue Dienste übertragen lässt.

Resignation entgegenwirken, Berührungsängste abbauen
In allen Lebenswelten zeigt sich jedoch in diesem Jahr anhand der zunehmenden Sicherheitsvorfälle auf drastische Weise, was passiert, wenn das vorhandene Sicherheitswissen nicht zum Einsatz kommt und sich deren Anwendung sogar rückläufig entwickelt. Die Gründe hierfür sind insbesondere einer fehlenden Motivation anzulasten.

Mit Blick auf die Aufklärungsarbeit liefern zwei Entwicklungen zusätzliche Erkenntnisse: Abseits der souveränen Nutzertypen reagieren die Verbraucher:innen auf die gestiegene Bedrohungslage zum einen mit Resignation. Mehr als die Hälfte (53,6 Prozent) glaubt beispielsweise nicht, ihr Digitales Ich überhaupt schützen zu können.

Zum anderen ist eine vermehrte Abkehr von digitalen Diensten zu beobachten: 43,4 Prozent verzichten wegen Sicherheitsbedenken bewusst auf einige Angebote und die als besonders risikoreich bewerteten Lebenswelten (Onlineshopping, Onlinebanking, soziale Netzwerke) verzeichnen rückläufige Nutzungsraten. Zudem sorgen neue komplexe Bereiche wie Künstliche Intelligenz insbesondere zu Beginn für Unsicherheiten.

Selbstwirksamkeit als Schlüsselkompetenz
Beides deutet auf ein mangelndes Bewusstsein für die Selbstwirksamkeit des Schutzverhaltens hin, dessen Sensibilisierung folglich einen Schlüssel in der Aufklärungsarbeit darstellen kann.

Verbraucher:innen müssen noch stärker darauf aufmerksam gemacht werden, dass sie durchaus selbst wirksamen Schutz erlangen können, wenn sie ihr Wissen in die Praxis umsetzen und dass sie mit transferfähigem Wissen zudem in der Lage sind, eigenständig auf neue Dienste und Anforderungen zu reagieren. Zielführend dabei ist eine passgenaue Ansprache, die Verbraucher:innen nicht überfordert, sondern dazu motiviert, ihr Sicherheitswissen praktisch in ihren digitalen Lebensalltag einzubinden.

Kapitel 4

Digitale Aufklärung im Jahr 2022: Basiswissen erhöhen und Cyberresilienz stärken

Basiswissen verbessern – Transferkompetenzen fördern

Entscheidend für wirksamen IT-Schutz durch Nutzer:innen ist das vorhandene Sicherheitswissen. Seine wirksame Verwendung hängt von der Transferfähigkeit ab. Je besser Verbraucher:innen in der Lage sind, ihr Wissen mit der voranschreitenden Digitalisierung weiterzuentwickeln und auf neue digitale Dienste und Risiken zu übertragen, desto besser sind sie im Netz geschützt.

Transferfähige Basiskompetenzen vermitteln
Mit der zunehmenden Digitalisierung müssen sich die Schutzkompetenzen der Verbraucher:innen fortlaufend weiterentwickeln. Kenntnisse, die jetzt noch ausreichend schützen, sind womöglich in einem oder mehreren Jahren bereits veraltet. Daher bedarf es einer Transferkompetenz, die vorhandenes Wissen auf neue Trends und veränderte Nutzungsanforderungen übertragen kann.

Die Transferkompetenz sollte auf Basiswissen ausgerichtet werden, das Verbraucher:innen auch bei noch unbekannten Anforderungen und Risiken anwenden können. Beispielsweise sollte das Sicherheitswissen zu Messenger-Diensten auf die Grundprinzipien verweisen, die Verbraucher:innen bei der Nutzung gleichartiger Anwendungen umsetzen können.

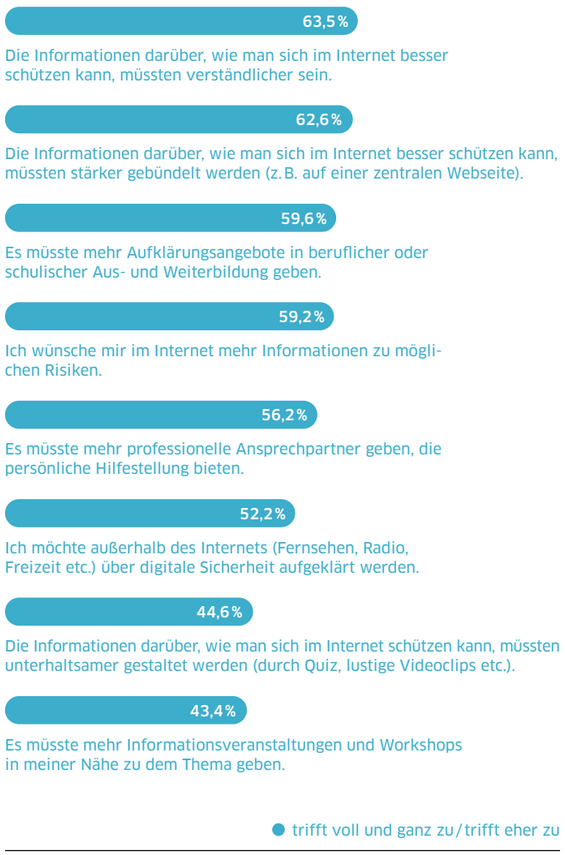
Individuelle Bedarfe berücksichtigen
Das steigende Sicherheitsgefälle in diesem Jahr zeigt, dass Aufklärungsarbeit Menschen auf unterschiedliche Weise einbinden muss. Digitale Aufklärung wirkt, wenn Inhalte die individuellen Ausgangslagen berücksichtigen. Dazu gehört nach Überzeugung der Verbraucher:innen auch, dass Wissen möglichst barrierefrei vermittelt werden muss.

Aus Sicht der Internetnutzer:innen sollen Informationen zudem verständlicher (63,5 Prozent) und etwa durch Bündelung an einer zentralen Anlaufstelle auffindbar sein (62,6 Prozent) sowie im beruflichen oder schulischen Aus- bzw. Weiterbildungsbereich vermittelt werden (59,6 Prozent). Ebenso mehrheitlich verlangt wird persönliche Hilfestellung (56,2 Prozent) – auch abseits des Internets (52,2 Prozent). Auch die Aufbereitung des Wissens spielt eine entscheidende Rolle, so bedarf es einer unterhaltsameren Gestaltung der Informationen gerade für Antreibende (62,3 Prozent) und Fatalist:innen (55 Prozent).

Aufsuchende Aufklärungsarbeit stärken
Die aufsuchende Aufklärungsarbeit wendet sich proaktiv und oftmals persönlich an die Verbraucher:innen und schafft unmittelbare Anknüpfungspunkte in den alltäglichen Lebenswelten. Gerade bei Außenstehenden und Gutgläubigen können persönliche Anleitungen und leichte Zugänge die Wissensaneignung fördern. Denn für beide Gruppen ist das persönliche Umfeld mit Abstand die wichtigste Informationsquelle (47,4 und 38,1 Prozent). Menschen aus dem vertrauten Umfeld und Bekanntenkreis sollten eingebunden werden, um als Multiplikator:innen in der Praxis zu wirken.

Darüber hinaus kann digitale Aufklärung, die sich nach den Bedürfnissen der Menschen richtet, auf vielfältige Weise gestaltet werden. Sie kann sowohl digital als auch regional stattfinden, wo Menschen zusammenkommen: im näheren sozialen, familiären, schulischen und beruflichen Umfeld. So bieten sich Informationsveranstaltungen für Eltern und Kinder im schulischen Kontext an, für ehrenamtlich Aktive sind dies meist Schulungen im Vereins- und Engagiertenumfeld bei regionalen Anlaufstellen. Zusätzlich können Onlineportale oder Newsletter aktuelle Informationen zielgruppengerecht und überregional vermitteln.

Abb. 33 / Sicherheitsindex 2022
Verbesserung von Sicherheitswissen/-kompetenz



Eigenverantwortung durch Selbstlernangebote stärken
Der Index 2022 zeigt, dass souveräne Verbraucher:innen wieder anderen Anforderungen unterliegen. Sie bevorzugen es, sich selbstständig an veränderte Sicherheitslagen anzupassen und weiterzubilden. Dazu bedarf es entsprechender Angebote zum selbst gesteuerten Lernen und zur individuellen Weiterbildung, beispielsweise mit Onlineselbstlernkursen. Darüber hinaus sollten orientierungsgebende Angebote bestehen, um eine Einschätzung zum persönlichen Kenntnisstand und eventueller Wissenslücken zu erhalten.

Handlungsempfehlungen

- Transferkompetenzen vermitteln: Es gilt zu fördern, Grundkompetenzen der IT-Sicherheit auf wechselnde und unbekannte Anforderungen übertragen zu können.
- Verfügbarkeit verbessern: Eine stärkere regionale Präsenz und bessere Verfügbarkeit von Hilfsangeboten im individuellen Alltag erhöhen die Wirkung von Aufklärungsarbeit.
- Hilfsangebote individualisieren: Die wachsende Bandbreite an Fragestellungen erfordert eine permanente Weiterentwicklung der Hilfsangebote entlang individueller Bedarfe.
- Selbstlernangebote ausbauen: Aktuelles Wissen spricht insbesondere souveräne Nutzergruppen an und muss daher unmittelbar und zur selbstständigen Aneignung verfügbar sein.

Best Practice bei DsiN

DsiN stärkt bereits anhand aktueller Angebote und Programme die regionale Präsenz und individuelle Ansprache.

Digital-Kompass: Angebote für Menschen in der Seniorenarbeit mit persönlicher Umgebung und deutschlandweit 100 Standorten

Digitale Nachbarschaft: bundesweite Stärkung regionaler Standorte für Verein und Ehrenamt (DiNa-Treffs) zu individuellen Bedarfen

DigiBitS – Digitale Bildung trifft Schule: Vermittlung digitaler Kompetenzen im Fachunterricht für Lehrkräfte in weiteren Bundesländern

Digitaler Engel: persönliche Kompetenzförderung für Ältere vor Ort über Kompetenzteams, auch in ländlichen Regionen nach Vereinbarung

Hilfe zur Selbsthilfe leisten

Abb. 34 / Sicherheitsindex 2022

Einschätzung der generellen Datensicherheit im Internet 2014 vs. 2022

Sicherheitswissen allein ist eine Grundlage für wirksamen IT-Schutz, die Anforderungen gehen jedoch darüber hinaus. Der diesjährige Index verdeutlicht, dass wirksame Aufklärungsarbeit noch stärker auf die dynamische Anwendung des Wissens hinwirken muss. Der Anstieg der Sicherheitsvorfälle erfordert aktives und adaptives Handeln der Nutzer:innen. Die aktuelle Wissens-Verhaltens-Lücke muss daher reduziert sowie die Abwehrbereitschaft auf dynamische Bedrohungen (Cyberresillienz) auf Nutzerseite insgesamt erhöht werden.

Selbsthilfekompetenz stärken
Grundlage eines sicheren und souveränen Verhaltens im Netz wird für Verbraucher:innen die Fähigkeit, das erworbene Transferwissen und Handeln auf aktuelle Bedrohungen und Risiken souverän anzuwenden. Dazu muss Aufklärungsarbeit aktivieren und zur Selbsthilfe motivieren. Verbraucher:innen gilt es mit transferfähigem Wissen auszustatten und auch in ihrer Anwendungskompetenz und -bereitschaft zu stärken und damit resilient gegen vielfältige Risiken im Alltag zu machen.

Diese Cyberresilienzkompetenz ermöglicht eine grundsätzliche Eigenständigkeit, auf wachsende und sich verändernde IT-Sicherheitsbelange zu reagieren. Sie richten die Aufmerksamkeit auf eine vorausschauende Aufklärungsarbeit, die veränderte Nutzungsgegebenheiten und stärker dynamische Handlungsempfehlungen in den Blick nimmt.

Aufklärungsarbeit muss zum Handeln motivieren
Souveräne Verbraucher:innen zeichnen sich durch ihre Kompetenz aus, Risikovorfälle zu erkennen und ihr Wissen sowie Verhalten darauf auszurichten. Bei den übrigen Nutzergruppen prägt dagegen ein Motivationsdefizit bei der Anwendung ihres Wissens ihre Sicherheitslage. Um diesem Defizit entgegenzuwirken, bieten ausgewählte Push- und Pull-Maßnahmen neue Lösungsperspektiven.

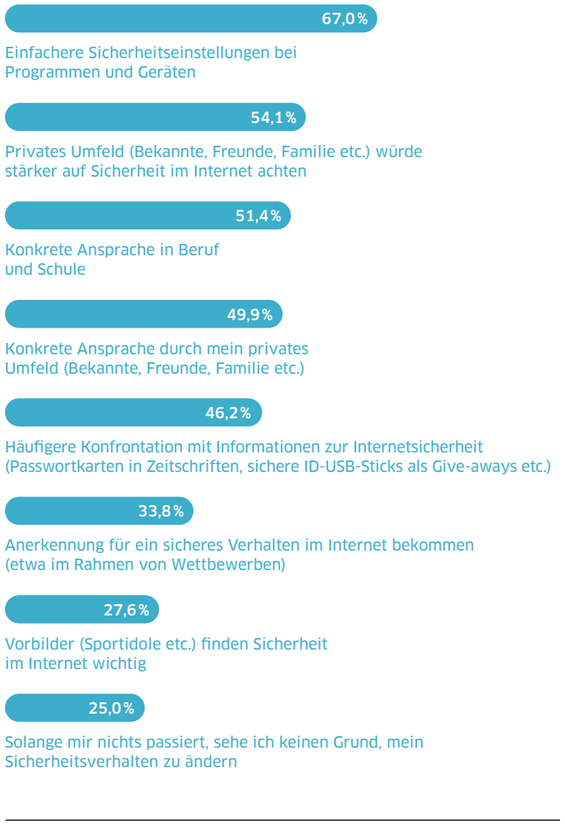
Push-Maßnahmen: Allgemein, aber vor allem bei Gutgläubigen ist die gefühlte Datensicherheit auch bei erhöhter Bedrohungslage hoch. In Abgrenzung zu unbegründeter Verunsicherung oder digitaler Gutgläubigkeit zielt digitale Aufklärung deshalb auf eine nachvollziehbare Risikoeinschätzung, die dazu befähigt, selbstständig die passenden Handlungsmaßnahmen zu erkennen und zu ergreifen. Dabei können Negativbeispiele helfen, die Erfolge von wirksamen Schutzmaßnahmen aufzeigen und auf diese Weise Handlungsmotivation erzeugen.

Pull-Maßnahmen: Anreize, die zugleich persönliche Vorteile adressieren, können das Engagement der Verbraucher:innen für aktive Schutzmaßnahmen anregen. Dazu zählen Schulungen mit Zertifizierungen, die berufliche Vorteile schaffen, oder Wettbewerbe, die soziale Anerkennung und Gewinne versprechen. Wettbewerbe erfahren mit 5,1 Prozentpunkten das stärkste Plus unter den abgefragten Motiven für einen sicheren Umgang mit den eigenen Daten.

Selbstwirksamkeit im Zentrum
Ein Hebel der Motivations- und Verhaltensförderung ist die Betonung der Selbstwirksamkeit. Gerade Verbraucher:innen, die in ihrem Sicherheitsverhalten

Abb. 35 / Sicherheitsindex 2022

Was könnte dafür sorgen, dass Sie stärker zu einem sicheren Umgang mit Ihren Daten im Internet motiviert werden?



resignieren (Fatalist:innen) oder sich von digitalen Diensten aus Verunsicherung abwenden, ist darzulegen, dass sie bereits mit einfachen Handlungen wirksamen Schutz erlangen können.

Ein solches Empowerment der Verbraucher:innen umfasst den Appell an die Eigenverantwortung, indem die Wirkkraft des individuellen Verhaltens aufgezeigt wird. Das kann etwa anhand relevanter Beispiele gelingen und sollte immer unter Einbezug der individuellen Lebenswelt erfolgen: Vorbilder (Sportidole etc.) (+1,9 Prozentpunkte) und souveräne Bekannte, Freunde und Familienmitglieder (+1,4 Prozentpunkte) werden von Verbraucher:innen in diesem Jahr verstärkt als Motivator:innen für ein besseres Sicherheitsverhalten genannt.

Handlungsempfehlungen

- Cyberresilienz fördern: Aufklärung muss Hilfe zur Selbsthilfe leisten und dazu befähigen, Transferkompetenzen der IT-Sicherheit selbstständig auf neue Anforderungen zu übertragen.
- Bewusstsein für Relevanz schaffen: Praxisbezüge verdeutlichen die eigene Betroffenheit und Notwendigkeit einer fortwährenden Anpassung des Sicherheitsverhaltens.
- Verantwortungsgefühl stärken: Selbstwirksamkeit lässt sich mit zielgruppenrelevanten Beispielen und unter Einbezug des persönlichen Umfelds sichern.

Best Practice bei DsiN

DsiN stärkt bereits anhand aktueller Angebote und Programme die regionale Präsenz und individuelle Ansprache.

DsiN-Digitalführerschein: Digitalkompetenznachweis für Beruf und Alltag in Zusammenarbeit mit Kompetenzpartnern sowie Verbraucher- und Berufsnetzwerken

Digital-Kompass: einfach lesbare Handreichungen sowie digitale Stammtische für digitale Fragen im Alltag von Senior:innen

DsiN-Computercheck: Selbstcheck gegen Viren, Spionagesoftware und Datendiebe mit Unterstützungsangeboten zur Fehlerbehebung

SiBa-App (Sicherheitsbarometer): Informiert in Zusammenarbeit mit der Wirtschaft und Sicherheitsbehörden über aktuelle Sicherheitsvorfälle und Verhaltenstipps

Transferinfrastruktur ausbauen – Rollenverteilung professionalisieren

Um die IT-Sicherheit in der Bevölkerung nachhaltig zu steigern, braucht es ganzheitliche Ansätze der Aufklärung, die die unterschiedlichen Rollen in der Aufklärungsarbeit abbilden. Dies ermöglicht, alltagsnahe Aufklärungsarbeit weiter zu professionalisieren. Standardisierte Vermittlungspraktiken, die durch überregionale Strukturen flächendeckend etabliert werden, können Kompetenzen nachhaltig und zielgruppengerecht bereitstellen.

Aufklärungsstrukturen professionalisieren und standardisieren
Um die individuelle Aufklärungsarbeit in der Fläche zu etablieren, gilt es, die Befähigungsketten im Rahmen der Transferinfrastrukturen zu festigen. Ein fortwährender Dialog zwischen drei Akteursgruppen kann diesen Rahmen bilden:

1. vorausschauende Expert:innen, die Risiken identifizieren und Verhaltensregeln und Vorgaben zur sicheren Nutzung digitaler Angebote entwickeln,
2. kompetente Didaktiker:innen, die Themen und Inhalte methodisch sinnvoll und auf eine Transferfähigkeit hin aufbereiten,
3. engagierte Menschen aus dem persönlichen Umfeld der Verbraucher:innen, insbesondere Antreibende und Bedachtsame, die als Multiplikator:innen in der Praxis wirken.

Aus einem permanenten Austausch von Erfahrungen und Best Practices der digitalen Aufklärung sowie Feedback der Verbraucher:innen können standardisierte Verfahren entstehen, die darüber hinaus eine Messung digitaler Kompetenzen vereinfachen. Auf diese Weise können skalierbare Vermittlungsformate eingebunden werden, die zusätzlich an Verbreitung gewinnen.

Individuelle und alltagsnahe Aufklärungsarbeit etablieren
Mit zunehmender Digitalisierung der Lebensbereiche diversifizieren sich die Mediennutzung sowie das Verhalten und die Einstellung gegenüber IT-Sicherheit zunehmend. Umso wichtiger wird es, die sich teils stark unterscheidenden Lebenswelten einzelner Verbraucher:innen in der Aufklärungsarbeit bedarfsgerecht anzusprechen. Auch hier können Transferinfrastrukturen einen zentralen Beitrag leisten. Angesichts der sich wandelnden Anforderungen wird eine agile und vorausschauende digitale Aufklärung notwendig. Sie muss sich vermehrt damit beschäftigen, neue Trends zu identifizieren sowie individuelle Handlungsempfehlungen auszusprechen.

Ergänzende Faktoren zur Aufklärungsarbeit
Getragen wird der Aufklärungsansatz vom Sicherheitsverhalten und der Bereitschaft zum verantwortlichen Umgang mit den eigenen Daten (77,7 Prozent). Aus Sicht der Verbraucher:innen kommt darüber hinaus dem exekutiven und regulativen Rahmen eine wachsende Bedeutung zu, etwa bei der Verfolgung von Gesetzesverstößen (+2,5 auf 76 Prozent) sowie strengeren Regularien (+3,5 auf 61,4 Prozent).

Zu den weiteren Faktoren zählen Verbraucher:innen die Anbieter- und Herstellerseite von IT, so es um die sicherere Gestaltung von Soft- (68,2 Prozent) und Hardware (66,2 Prozent) sowie um die Barrierefreiheit geht: Einfache Sicherheitseinstellungen bei Programmen und Geräten sind für Verbraucher:innen die größte Motivation (67 Prozent) für einen sicheren Umgang mit Daten im Internet.

Abb. 36 / Sicherheitsindex 2022
Für wie geeignet halten Sie diese Maßnahmen, um Ihre Sicherheit im Internet zu erhöhen?

Handlungsempfehlungen

- Bildungsarbeit individualisieren: Bedarfsgerechte Aufklärungsarbeit muss auf die individuellen Lebenswelten zugeschnitten und zeitgemäß sowie unterhaltsam gestaltet sein.
- Rollen professionalisieren: Mit den zusätzlichen Freiräumen für Aufklärungsarbeit können standardisierte und messbare Angebote entwickelt und bereitgestellt werden.
- Dialog intensivieren: Ein wachsender Dialog der Verbraucher:innen mit den Akteur:innen der Aufklärungsarbeit hilft, die Anforderungen im Alltag besser zu verstehen und das Schutzniveau ganzheitlich und nachhaltig zu heben.

Best Practice bei DsiN

DsiN bindet engagierter Akteur:innen und Netzwerke anhand ausgewählter Angebote ein.

Cyberfibel für Wissensvermittler:innen: Standardwerk von BSI und DsiN in der digitalen Verbraucheraufklärung

DigiBitS – Digitale Bildung trifft Schule: digitale Kompetenzvermittlung für Lehrkräfte mit bundesweit über 300 Referenzen auf kuratierte Angebote

Digitale Nachbarschaft: Unterstützungsnetzwerk für Vereine und Ehrenamt in Zusammenarbeit mit dem Bundesnetzwerk Bürgerschaftliches Engagement (BBE) und der Verbraucher Initiative (VI)

DsiN-Website: vielfältige Informationen und Angebote auf **sicher-im-netz.de**

Drei-Punkte-Plan für wirksame Aufklärung

Der DsiN-Sicherheitsindex sendet in diesem Jahr eine klare Botschaft: Digitale Aufklärung muss sich auf die wirksame Umsetzung des erworbenen Sicherheitswissens konzentrieren. Persönliche Ansprache und praxisnahe Beispiele unter Berücksichtigung der individuellen Lebenswelten sind dabei entscheidend. Die Cyberresilienz der Verbraucher:innen wird zum Leitstern der Bildungsarbeit und stellt die Befähigung zum selbstständigen Handeln in den Fokus.

1.

Basiswissen und Transferkompetenzen

Verbraucher:innen müssen durch die Vermittlung digitaler Transferkompetenzen in die Lage versetzt werden, sich an wandelnde Herausforderungen anpassen zu können. Basiswissen muss dazu einerseits fortwährend neue Trends und verändertes Nutzungsverhalten mit einbeziehen. Andererseits bedarf es didaktischer Konzepte, die die Sicherheitsaspekte und Funktionsweisen einzelner Dienste und Geräte insoweit abstrahieren, als dass sie unabhängig von einzelnen Anwendungsszenarien verstanden werden können. Dadurch wird Wissen transferfähig und kann in der Folge auf neue digitale Dienste und Risiken angewandt werden.

Je nach individueller Lebenswelt gilt es, die Angebote regional und digital zu positionieren und die unterschiedlichen Bedarfe der Verbrauchertypen zu adressieren. Der direkte, persönliche Austausch ist dafür der zentrale Schlüssel. Das private Umfeld, die Schule sowie der berufliche Kontext stellen etablierte Netzwerke dar, in denen souveräne Nutzer:innen als Multiplikator:innen wirken können.

2.

Cyberresilienz durch Hilfe zur Selbsthilfe

Dem Defizit bei der Handlungsbereitschaft gilt es, durch eine Motivationsarbeit entgegenzuwirken, die auf eine Umsetzung des Sicherheitswissens abzielt und die Selbstwirksamkeit in den Fokus stellt. Dazu müssen die Verbraucher:innen in ihrem Alltag mit grundlegenden Sicherheitsfragen erreicht, Betroffenheit und Mehrwerte aufgezeigt und die Risikobewusstseinskompetenz gefördert werden. Wettbewerbe und Zertifikate zur digitalen Kompetenz können weitere Anreize schaffen.

Anknüpfend an die Anwendungsbereitschaft muss die Aufklärungsarbeit die Transferkompetenz der Verbraucher:innen stärken und auf eine grundsätzliche Eigenständigkeit in IT-Sicherheitsfragen hinwirken. Im Sinne einer Hilfe zur Selbsthilfe gilt es, Verbraucher:innen dazu zu befähigen, selbstständig auf die dynamischen Anforderungen und veränderten Nutzungsgegebenheiten reagieren zu können und dadurch resilient gegen vielfältige Cyberrisiken zu werden.

3.

Kooperative Ausrichtung verstärken

Die wachsende Vielfalt digitaler Lebenswelten erfordert einen integrierenden Aufklärungsansatz mit einer stärkeren Arbeitsteilung: Expert:innen verknüpfen ein fortlaufendes Monitoring der Bedrohungslage mit Handlungsempfehlungen, an die eine bedarfsgerechte Vermittlung durch geschulte Didaktiker:innen anschließt. Verbraucher:innen vervollständigen mit ihren Feedbacks einen iterativen Prozess, aus dem flächendeckend standardisierte und zeitgemäße Bildungsangebote hervorgehen können.

Eine durchlässige Kommunikationsstruktur ist hierfür Grundvoraussetzung. Die Dialogfähigkeit der Transferinfrastrukturen ermöglicht Aufschlüsse über die Bedarfe und Defizite in der Praxis, welche den Akteur:innen der Gesetzgebung und Wirtschaft zur Verfügung gestellt werden können und sie in die Lage versetzen, die Herausforderungen der IT-Sicherheit praxisnah zu adressieren – und das Schutzniveau über bedarfsgerechte Angebote und Initiativen zu fördern.

Glossar

Digitale Aufklärung
Maßnahmen der Verbraucherbildung, um Anwender:innen zu informieren, sensibilisieren und zur gelebten IT-Sicherheit zu befähigen.

DsiN-Sicherheitsindex
Sicherheitslage deutscher Onliner:innen in einer Zahl – als gewichteter Mittelwert aus den vier Sicherheitsfaktoren.

Indexpunkte
Der DsiN-Index sowie die vier Faktoren werden auf einer Skala von 1 bis 100 gemessen.

Schwellenwert 50
Bei Werten unter 50 Indexpunkten kippt die Sicherheitslage, das heißt, die Bedrohungslage ist höher als das Schutzniveau.

Verbrauchertypen
Eine Clusterung der deutschen Onlinertypen. Die Studie sieht fünf Verbrauchergruppen vor, die sich durch typisierte Sicherheitsfaktoren unterscheiden: Außenstehende, Fatalist:innen, Gutgläubige, Antreibende und Bedachtsame. Die beiden letzteren Typen werden auch als „Souveräne“ bezeichnet.

Cyberresilienz
Abwehrkompetenz, die Nutzer:innen dazu befähigt, eigenständig auf sich verändernde IT-Sicherheitsbelange zu reagieren.

Scam
Scam ist das englische Wort für Betrug und meint im Digitalen den Betrug durch Kontaktaufnahme mit falschen Versprechungen, zum Beispiel auf Dating-Plattformen oder in sozialen Netzwerken.

Phishing
Das Wort Phishing setzt sich aus den englischen Begriffen „fishing“ (deutsch: angeln, fischen) und „password harvesting“ (deutsch: Passwort sammeln) zusammen. Beim Phishing setzen Hacker:innen auf die detailgetreue Imitation von E-Mails und Websites bekannter Anbieter:innen wie Banken. Phishing via SMS wird umgangssprachlich „Smishing” genannt.

VPN
VPN steht für Virtual Private Network. VPN-Verbindungen werden über spezielle Server geleitet, die die Kommunikation verschlüsseln und die IP-Adresse verbergen.

Proxy-Client
Bei einem Proxy-Client handelt es sich um einen Computer oder eine Software, die mit einem Proxy-Server kommuniziert. Ein Proxy-Server kann als Schnittstelle zwischen einem privaten Netzwerk und dem Internet dienen, um lokale Endgeräte zu schützen.

Sicherheitsfaktoren:

Sicherheitsvorfälle
IT-sicherheitsrelevante Vorfälle, die von den Onliner:innen registriert wurden

Verunsicherungsgefühl
Das persönliche Gefühl der Verunsicherung bei der Nutzung digitaler Anwendungen

Sicherheitskompetenz
Selbstauskunft über die Kenntnis von IT-Schutzmaßnahmen

Sicherheitsverhalten
Selbstauskunft über die Anwendung von IT-Schutzmaßnahmen

NOTIZEN

sicher-im-netz.de

Ein Handlungsversprechen von:

Atos