

FOKUSTHEMA

Digitale
Bürgerportale



DsiN SicherheitsIndex 2020

Digitale Sicherheitslage von
Verbraucher*innen in Deutschland

DsiN-Schirmherrschaft:



Bundesministerium
des Innern, für Bau
und Heimat

Eine Studie von:



**Deutschland
sicher im Netz**



sicher-im-netz.de

Verbraucheraufklärung wirksam gestalten



Rita Hagl-Kehl

Die Teilhabe der gesamten Gesellschaft an der Digitalisierung ist ein wichtiges Ziel dieser Bundesregierung. Mit den Folgen der COVID-19-Pandemie ist die Bedeutung digitaler Medien im Alltag nochmals gestiegen. Es gilt nun umso mehr, den Zugang zu digitalen Angeboten und Technologien für alle Verbraucherinnen und Verbraucher zu erleichtern und die erforderlichen Kompetenzen zu einem sicheren und selbstbestimmten Umgang breitenwirksam zu vermitteln. Der Sicherheitsindex von Deutschland sicher im Netz e.V. (DsiN) ist hier ein wichtiger Gradmesser für das Bundesministerium der Justiz und für Verbraucherschutz, um Entwicklungen der digitalen Sicherheitslage besser zu verstehen und Handlungsbedarfe bei Verbraucherinnen und Verbrauchern zur Erhöhung ihrer Schutzkompetenzen nachzuvollziehen.

Erfreulicherweise steigt der DsiN-Sicherheitsindex in diesem Jahr bereits das zweite Jahr in Folge. Ausschlaggebend dafür sind die zunehmenden Schutzkompetenzen in der Bevölkerung, die sogar einen neuen Höchststand erreichen. Bei genauerer Betrachtung werden aber auch Unterschiede erkennbar: Während einige Nutzergruppen weiter zulegen und noch sicherer im Internet agieren als im Vorjahr, fallen andere Nutzergruppen dahinter zurück. Dabei ist es wichtig, dass wir einem digitalen Sicherheitsgefälle in Deutschland konsequent entgegenwirken und es verhindern. Niemand darf digital abgehängt werden. Der Index liefert hier konkrete Anknüpfungspunkte, welche Nutzergruppen zusätzlicher Aufklärungsmaßnahmen bedürfen – und worauf diese abzielen.

Wir verstehen die Ergebnisse des DsiN-Sicherheitsindex aber auch als Signal für eine Aufklärungsarbeit, die geeignete und wirksame Maßnahmen erfordert. Dabei ist von entscheidender Bedeutung, dass engagierte Akteure aus Wirtschaft, Gesellschaft und Staat zusammenarbeiten und ihre jeweiligen Stärken einbringen.

Projekte wie der Digital-Kompass, in dem eine Vielzahl von Initiativen und Netzwerken an künftig rund hundert regionalen Standorten eingebunden sind, sind daher der richtige Weg, um digitale Kompetenzen wirksam zu vermitteln. Es geht um das Engagement von Verbrauchern für Verbraucher, das über den Erfolg der digitalen Aufklärung entscheidet.

Ich danke Deutschland sicher im Netz e.V., mit dem Sicherheitsindex einen wichtigen Beitrag zur digitalen Aufklärung von Verbraucherinnen und Verbrauchern zu leisten.

Ihre

Rita Hagl-Kehl

Parlamentarische Staatssekretärin im Bundesministerium
der Justiz und für Verbraucherschutz

Aufklärungsenthusiasten gefragt!



Dr. Michael Littger



Thomas Tschersich

Der DsiN-Sicherheitsindex 2020 spricht eine klare Sprache: Digitale Sicherheit lässt sich nicht verordnen und ebenso wenig durch Appelle oder Kampagnen erreichen. Digitale Aufklärung muss langfristig gedacht und auf Lebensbereiche und Umstände ausgelegt sein, die so bunt und vielfältig wie das Leben selbst sind. Denn Digitale Sicherheit ist das, was die betroffenen Onliner daraus machen – welche Dienste und Medien sie nutzen, wie sie sich dabei verhalten, was sie wissen und welche Haltungen, Ängste und Hoffnungen sie mit diesen Aktivitäten verbinden.

Das digitale Sicherheitsgefälle, das der diesjährige Sicherheitsindex im Detail beleuchtet, ist umso relevanter, als mit der digitalen Expansion zunehmend alle Bereiche unseres Lebens betroffen sind. Wir sprechen von grundlegenden Fragen der sicheren und selbstbestimmten Gestaltung des Lebensalltags von Verbraucher*innen.

Wir müssen lernen, digitale Aufklärungsarbeit als eine Art Grundvoraussetzung zu begreifen, um allen Menschen eine Teilhabe am modernen Lebensalltag zu ermöglichen. Es geht um die Vermittlung grundlegender Kompetenzen zur souveränen Gestaltung des digitalisierten Alltags. Diese Anforderungen stehen auch nicht erst „seit Corona“ im Raum, wurden dadurch aber nochmals stark verdeutlicht. Der Index liefert einen breiten Fundus an Erkenntnissen, wo Aktivitäten künftig fokussiert werden müssen, etwa in der Ermunterung von Onlinern zur Umsetzung ihres erworbenen Wissens. Es geht zugleich um die Organisation von Aufklärungsarbeit, die nur als arbeitsteiliger Prozess zwischen engagierten Akteuren funktionieren kann

Die Mitglieder und vielen Partner von Deutschland sicher im Netz e.V. engagieren sich seit Jahren in der digitalen Aufklärungsarbeit – und leisten damit einen immer größeren Beitrag, durch Kooperation und Zusammenarbeit die digitale Aufklärung voranzubringen. Wir freuen uns, dass das Bundesministerium der Justiz und für Verbraucherschutz dieses Engagement schon frühzeitig sehr konsequent unterstützt hat und nicht zuletzt im Rahmen des DsiN-Sicherheitsindex entscheidend dazu beiträgt, die Erkenntnisse über unsere gemeinsamen Aufgaben einer breiteren Öffentlichkeit und der Politik zugänglich zu machen.

Eine aufklärende Lektüre wünschen,

Dr. Michael Littger
DsiN-Geschäftsführer

Thomas Tschersich
DsiN-Vorstandsmitglied

Inhalt

| | |
|---|-----------|
| Grußwort zum DsiN Sicherheitsindex 2020 | 1 |
| von Rita Hagl-Kehl, Parlamentarische Staatssekretärin im BMJV | |
| Vorwort: Aufklärungsenthusiasten gefragt! | 2 |
| von Dr. Michael Littger und Thomas Tschersich | |
| Toprends 2020: Digitale Gesellschaft in Bewegung | 4 |
| Ziel und Methode: Wie sicher ist Deutschland im Netz? | 6 |
| Kapitel 1 DsiN-Sicherheitsindex 2020: Erneuter Anstieg auf 62,8 Punkte | 7 |
| Indexwert 2020: Mit 62,8 Punkten geht es weiter aufwärts | 8 |
| Veränderungen 2020 bei den vier DsiN-Sicherheitsfaktoren | 10 |
| Blick von außen: Nutzerverhalten im Überblick | 12 |
| Kapitel 2 IT- Sicherheitsgefälle: Unterschiede zwischen Verbrauchertypen | 13 |
| Die digitale Gesellschaft: Nutzertypen im Netz | 14 |
| Außenstehende Nutzer*innen (46,0 Punkte) | 16 |
| Fatalistische Nutzer*innen (48,8 Punkte) | 18 |
| Gutgläubige Nutzer*innen (58,7 Punkte) | 20 |
| Antreibende Nutzer*innen (72,5 Punkte) | 22 |
| Bedachtsame Nutzer*innen (74,5 Punkte) | 24 |
| Einstellungen und Nutzungsgewohnheiten | 26 |
| Kapitel 3 Digitale Lebenswelten | 27 |
| Fokusthema: Digitale Bürgerportale | 28 |
| Smarte Versicherungstarife | 30 |
| Digitale Gesundheits- und Fitnessdienste | 31 |
| Digitale Vernetzung | 32 |
| Das vernetzte Zuhause | 33 |
| Einkaufen im Internet | 34 |
| Online-Banking | 35 |
| IT-Sicherheit neu denken | 36 |
| Kapitel 4 Digitale Aufklärung: Verstehen Befähigen Gestalten | 37 |
| Verstehen: Themen- und zielgruppengerechte Aufklärung | 38 |
| Befähigen: Aufbau von Risikobewusstsein und Eigenverantwortung | 40 |
| Gestalten: Förderung nachhaltiger Strukturen und offener Dialoge | 42 |
| Fazit: Drei-Punkte-Plan für wirksame Aufklärung | 44 |
| Über Deutschland sicher im Netz e.V. | 45 |
| DsiN-Angebote für mehr IT-Sicherheit | 45 |
| Impressum | 45 |

Toprends 2020: Digitale Gesellschaft in Bewegung

Der DsiN-Sicherheitsindex beantwortet zwei Fragen: Wie steht es um die digitale Sicherheitslage von Verbraucher*innen in Deutschland und was ist erforderlich, um ihre Sicherheitslage zu verbessern? Dabei wird die digitale Sicherheitslage in einem Indexwert auf einer Skala von 0 bis 100 abgebildet.

Indexwert 2020: Mit 62,8 Punkten geht es weiter aufwärts

Der Sicherheitsindex kann sich 2020 um 0,5 Punkte steigern, nachdem er nach 2016 zwei Jahre in Folge gefallen war. Damit hat sich die IT-Sicherheitslage in Deutschland bei Verbraucher*innen insgesamt weiter verbessert. Der gestiegene Indexwert ist auf den Rückgang der selbst registrierten Sicherheitsvorfälle sowie das wachsende Sicherheitswissen der Nutzer*innen zurückzuführen. Negativ hingegen wirkt sich das subjektive Verunsicherungsgefühl aus: Dieses erreicht 2020 mit einem Indexwert von 29,6 Punkten seinen bislang höchsten Wert.

Schere zwischen Sicherheitswissen und -verhalten wächst

Mit der Expansion der digitalen Möglichkeiten in immer mehr Lebensbereiche wachsen die Anforderungen der Verbraucher*innen an Schutzvorkehrungen. Erfreulich ist, dass das Sicherheitswissen insgesamt weiter zunimmt. Zugleich aber kann die tatsächliche Anwendung jenes Wissens nicht in gleichem Maße zulegen: Die Wissens-Verhaltens-Schere öffnet sich weiter. Hier sind zusätzliche Maßnahmen einer Aufklärungsarbeit gefordert, die stärker auf das tatsächliche Umsetzen von Maßnahmen im Alltag abzielt.

Wachsendes IT-Sicherheitsgefälle: Verbrauchergruppen unterschiedlich sicher im Netz

Der Sicherheitsindex unterscheidet nach fünf Verbrauchertypen, deren Sicherheitslage je nach

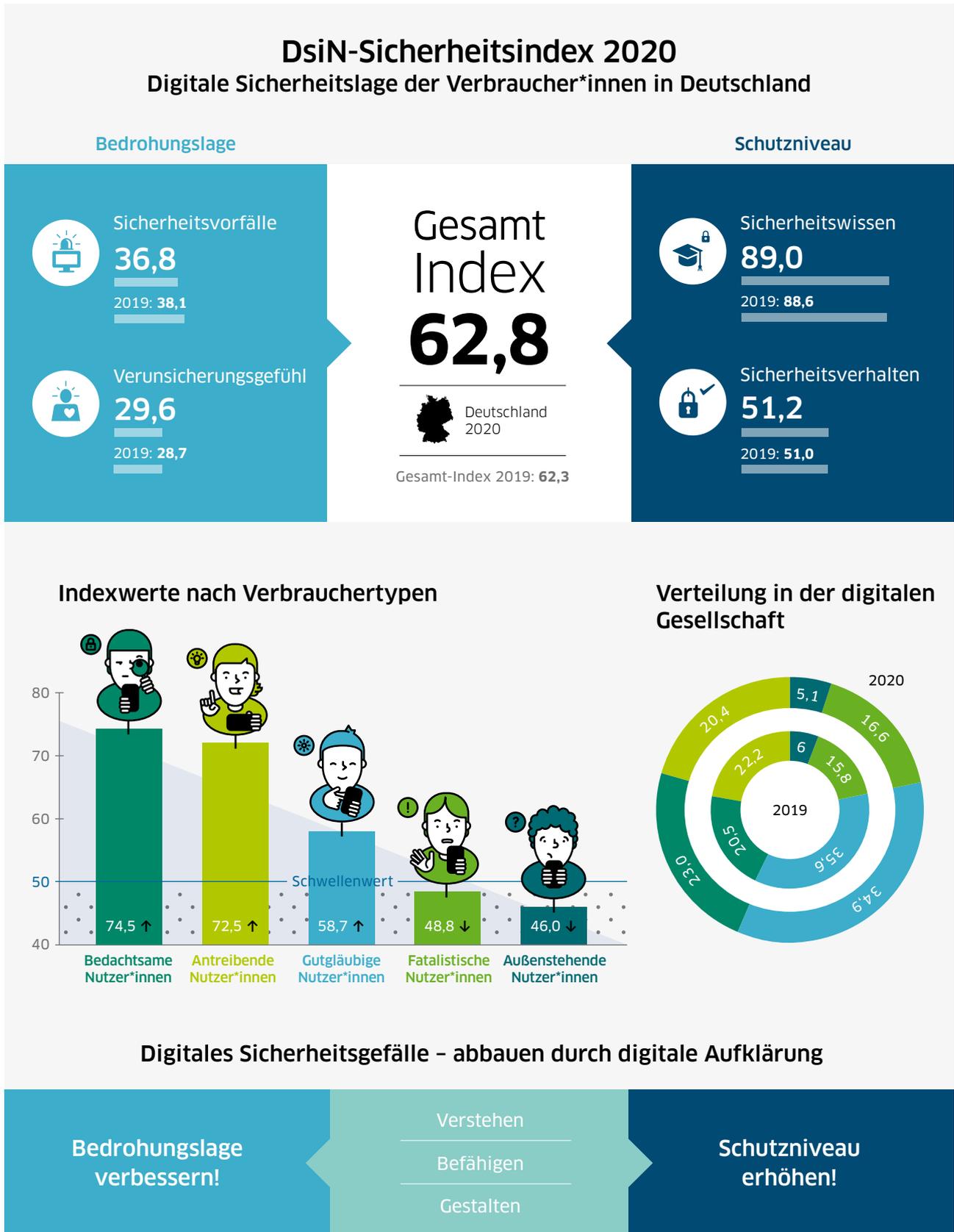
Wissen und Verhalten auffällig variiert: Während Außenstehende und Fatalisten 2020 unter dem kritischen Wert von 50 Punkten liegen, liegen Gutgläubige, Antreibende sowie Bedachtsame darüber, die beiden letzten Gruppen sogar deutlich mit Werten über 70 Punkten. Dieses IT-Sicherheitsgefälle hat sich in den vergangenen Jahren stetig vergrößert und nimmt auch im Jahr 2020 weiter zu. Es wird künftig darum gehen, zielgruppengerechte Aufklärungsmaßnahmen zur Verfügung zu stellen, die das Sicherheitsgefälle in der Gesellschaft abbauen und allen Menschen die gleichen Chancen für ein sicheres und selbstbestimmtes Internet ermöglichen.

Fokusthema digitale Bürgerportale: Großer Zuspruch, geringe Verbreitung

Der diesjährige DsiN-Sicherheitsindex beleuchtet im Fokusthema „digitale Bürgerportale“ die Kenntnisse, Vorteile und Vorbehalte aus Sicht der Verbraucher*innen. Deutlich wird, dass Kenntnisse über digitale Verwaltungsangebote bei den Befragten mäßig verbreitet sind, zugleich aber ein hohes Vertrauen in die Online-Angebote der öffentlichen Hand (80,4 Prozent) besteht und mehr Angebote gewünscht werden. Für zusätzliche Angebote zeigen Bürger*innen sogar eine bemerkenswerte „Kompromissbereitschaft“ in puncto IT-Sicherheit.

Abb. 1

DsiN-Sicherheitsindex 2020



Ziel und Methode: Wie sicher ist Deutschland im Netz?

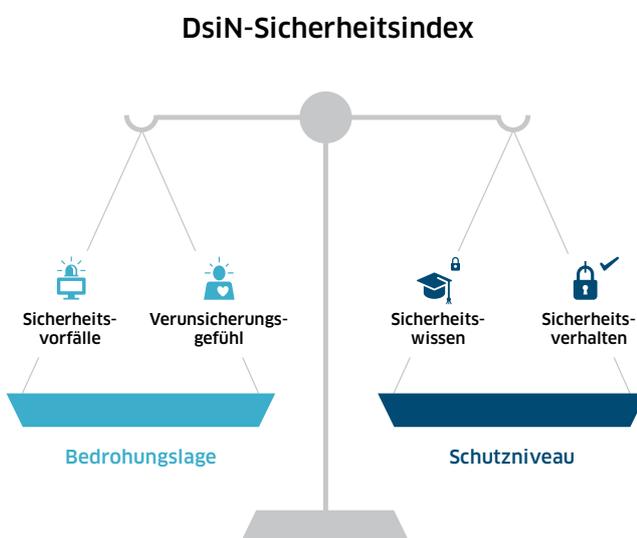
Die jährliche Verbraucherstudie von Deutschland sicher im Netz e.V. untersucht die digitale Sicherheitslage von deutschen Internetnutzer*innen und bildet diese – auf einer Skala von 0 bis 100 – in einer zentralen Kennziffer ab: dem DsiN-Sicherheitsindex. Seit nunmehr sieben Jahren (2014) zeigen die repräsentativen Ergebnisse des DsiN-Sicherheitsindex Entwicklungen, Trends und Bedarfe der IT-Sicherheitslage in Deutschland auf. Über 2.000 Verbraucher*innen über 16 Jahren werden hierbei befragt. Die Verbraucherstudie erfolgt in Zusammenarbeit mit dem Markt- und Meinungsforschungsinstitut KANTAR.

Bedrohungslage versus Schutzniveau

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

Abb. 2

Berechnung des DsiN-Sicherheitsindex: Verhältnis zwischen Bedrohungslage und Schutzniveau



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 bildet 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, wie zum Beispiel der Verwendung einer Zwei-Faktor-Authentisierung oder der Einrichtung einer Firewall. 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, desto sicherer sind deutsche User*innen im Netz. Liegt der Gesamtwert über 50 Indexpunkten, überwiegt das Schutzniveau der Nutzer*innen. Bei einem Wert darunter kippt die Sicherheitslage und die Bedrohungslage überwiegt.

Aufschlüsselung nach verschiedenen Nutzertypen und digitalen Lebenswelten

Der DsiN-Index unterscheidet auf Grundlage der Sicherheitslage der Onliner zwischen fünf verschiedenen Verbrauchertypen. 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 sind digitale Bürgerportale.



Kapitel 1

**Sicherheitsindex 2020:
Erneuter Anstieg
auf 62,8 Punkte**

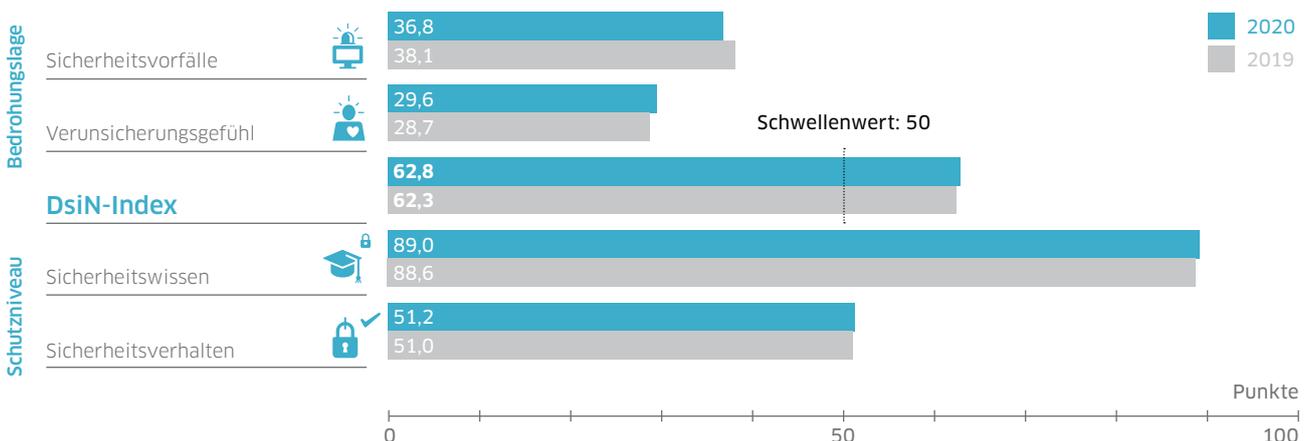
Indexwert 2020: Mit 62,8 Punkten geht es weiter aufwärts

Die digitale Sicherheitslage steigt im Jahr 2020 gegenüber dem Vorjahr um 0,5 Punkte auf 62,8 Punkte an. Damit hat sich das Sicherheitsniveau bei Verbraucher*innen im zweiten Jahr in Folge verbessern können und erreicht seinen Höchstwert seit vier Jahren (2016). Die Gründe für die Verbesserung liegen zum einen im Rückgang der durch die Befragten registrierten Sicherheitsvorfälle, zum anderen steigt das Sicherheitswissen bei Verbraucher*innen weiter an.

Abb. 3
Digitale Sicherheitslage im Siebenjahresvergleich



Abb. 4
Übersicht Index und Faktoren 2020



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 2020 folgende Veränderungen verzeichnen:

Entwicklungen der Bedrohungslage durch IT bei Verbraucher*innen :

- Sicherheitsvorfälle: 36,8 Punkte (- 1,3 I). Die Verbesserung des Indexwerts 2020 ist maßgeblich auf einen Rückgang der IT-Sicherheitsvorfälle gegenüber 2019 zurückzuführen, welche noch im Zeitraum 2016 bis 2018 stark angestiegen waren. Der Wert liegt nun bei 36,8 Indexpunkten (2019: 38,1 Punkte).
- Verunsicherungsgefühl: 29,6 Punkte (+0,9 I). Obwohl die erlebten Sicherheitsvorfälle rückläufig sind, fühlen sich Verbraucher*innen nicht sicherer: Das Verunsicherungsgefühl steigt 2020 um 0,9 Punkte auf einen Wert von 29,6 (2019: 28,7 Punkte). Das Gefühl der subjektiven Bedrohungslage erreicht damit seinen bislang höchsten Wert seit Erhebung des Index.

Entwicklungen beim IT-Schutzniveau von Verbrauchern

- Sicherheitswissen: 89,0 Punkte (+0,41). Die Sicherheitskompetenz der Nutzer*innen ist – wie schon in den vorausgegangenen Jahren – erneut angestiegen: Mit 89,0 Indexpunkten erreicht die Kompetenz 2020 einen neuen Höchstwert. Dies wirkt sich positiv auf den Gesamtindexwert aus.
- Sicherheitsverhalten: 51,2 Punkte (+0,21). Das Sicherheitsverhalten deutscher Nutzer*innen ist zwar nicht mehr rückläufig, stagniert jedoch weitestgehend und kann daher mit dem vergleichsweise hohen Sicherheitswissen nicht Schritt halten. Somit vergrößert sich 2020 die Wissens-Verhaltens-Schere erneut und verzeichnet die bislang größte Diskrepanz zwischen der Kenntnis von IT-Schutzmaßnahmen und ihrer Anwendung.

Trotz Anstieg des Gesamtindex: Digitale Verunsicherung der Nutzer*innen steigt

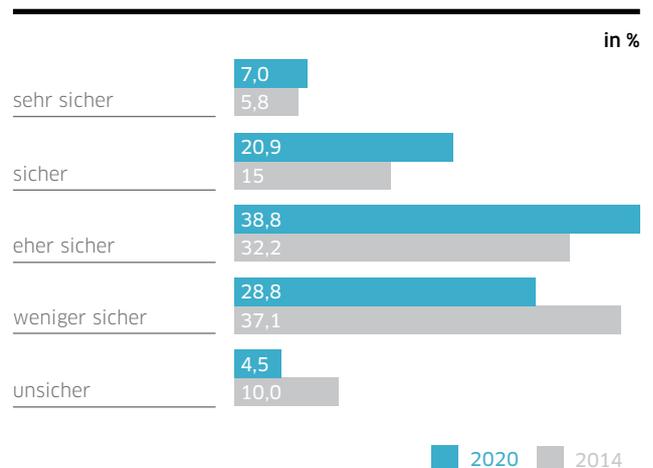
Verbraucher*innen fühlen sich so verunsichert wie nie zuvor. Obwohl die registrierten Sicherheitsvorfälle abgenommen haben, steigt das subjektive Gefühl einer Verunsicherung bezüglich möglicher IT-Risiken an. So scheint sich hier eine Entkopplung von tatsächlich erlebter IT-Sicherheit und dem subjektiven Gefühl einer Gefährdung zu manifestieren. Auch entwickelt sich das hohe Verunsicherungsempfinden gegenläufig zum gestiegenen Sicherheitskompetenz der Verbraucher*innen, die 2020 einen Höchstwert erzielt hat.

Verbraucher*innen fordern Stärkung des Risikobewusstseins

Das erhöhte Verunsicherungsempfinden der Verbraucher*innen im Jahr 2020 geht mit einem steigenden Bedürfnis nach Maßnahmen zur Stärkung des Risikobewusstseins einher. Hier steht die Forderung nach einem bewussteren Umgang

Abb. 5

Einschätzung der generellen Datensicherheit im Internet 2014 vs. 2020



mit Risiken und Chancen in der Schule an erster Stelle (68,4 Prozent). Gefolgt wird dies von dem Anliegen, dass Anbieter von Diensten und Programmen besser über Risiken aufklären (65,9 Prozent) sowie dem Wunsch nach einer breiteren öffentlichen Diskussion über Risiken (62,4 Prozent).

Defizite bei Umsetzung des Sicherheitswissens

Die Zunahme der Wissens-Verhaltens-Lücke bei Verbraucher*innen erreicht 2020 einen Höchststand. So kennen beispielsweise 90,5 Prozent der Nutzer*innen die Zwei-Faktor-Authentisierung, doch nutzen diese nur 54,4 Prozent auch wirklich aktiv. Von 90,7 Prozent der Onliner, die vom Passwort-Manager wissen, verwenden ihn sogar nur 30,1 Prozent. Hier gilt es nach wie vor, Nutzer*innen zu motivieren, ihr erlangtes Wissen zu aktivieren und umzusetzen: So wäre es für mehr als die Hälfte der Befragten hilfreich, wenn Sicherheitsfragen in ihrem privaten Umfeld thematisiert und aktiv angegangen würden.

Veränderungen 2020 bei den vier DsiN-Sicherheitsfaktoren

Bedrohungslage aus Sicht von Verbraucher*innen

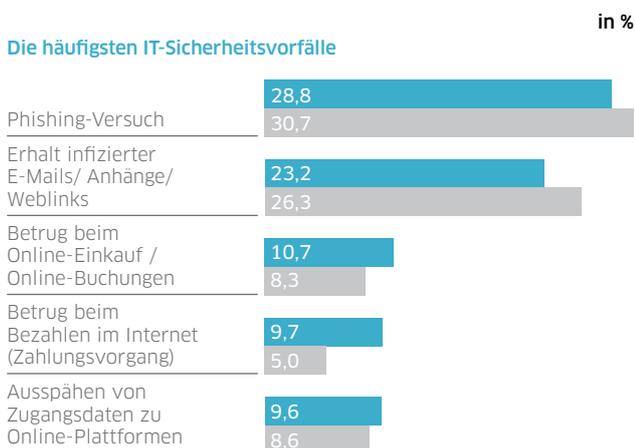
1. Registrierte Sicherheitsvorfälle

Bei den TOP 5 der häufigsten Sicherheitsvorfälle sind Szenarien wie das so genannte Phishing und der Onlinebetrug im Jahr 2020 erneut Spitzenreiter. Hinzugekommen ist der Betrug beim Bezahlen im Internet: Während dieser Vorfall 2019 Jahr noch auf Platz 13 der Vorfälle rangierte, liegt er nun auf Platz 4. Im Vergleich zum Vorjahr ist die Gesamtzahl aller Angriffe leicht zurückgegangen (-1,3 Punkte).



Abb. 6

Spitzenreiter und Schlusslichter Sicherheitsvorfälle



Die Schlusslichter unter den IT-Sicherheitsvorfällen



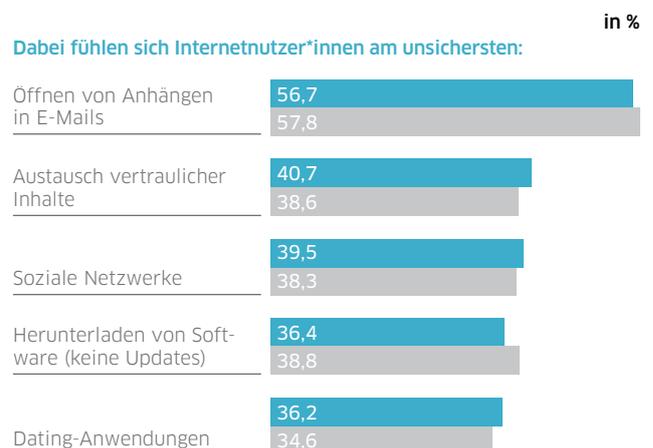
2. Verunsicherungsgefühl im Internet

Das Verunsicherungsgefühl erreicht 2020 seinen Höchststand: Bei genauer Betrachtung lässt sich feststellen, dass es bei rund zwei Drittel der Online-Aktivitäten gestiegen ist. Hier steht das Öffnen von Anhängen in E-Mails an erster Stelle. Auf den zweiten Platz vorge-rückt ist der Austausch vertraulicher Inhalte, gefolgt von den sozialen Netzwerken. Deutlich weniger gefährlich als im Vorjahr stufen die Onliner dagegen die Messenger-Nutzung auf mobilen Geräten ein (-4,6 Prozentpunkte).



Abb. 7

Spitzenreiter und Schlusslichter Verunsicherungsgefühl



Dabei fühlen sich Nutzer*innen am wenigsten unsicher:



Schutzniveau aus Sicht der Verbraucher

3. Sicherheitswissen bei Verbraucher*innen

Das digitale Sicherheitswissen deutscher Onliner erreicht 2020 seinen Höchstwert. Die bedachte Verwendung von Passwörtern wird hier als zentrale Maßnahmen von Verbraucher*innen betrachtet. Auf Platz zwei liegt jetzt das Ändern von Passwörtern. Von den abgefragten Sicherheitsmaßnahmen sind über 90 Prozent den Onlinern bekannt. Am unbekanntesten sind weiterhin das Auslesen des E-Mail-Headers und Plug-ins zur Erhöhung der Datensicherheit.



Abb. 8
Spitzenreiter und Schlusslichter Sicherheitswissen

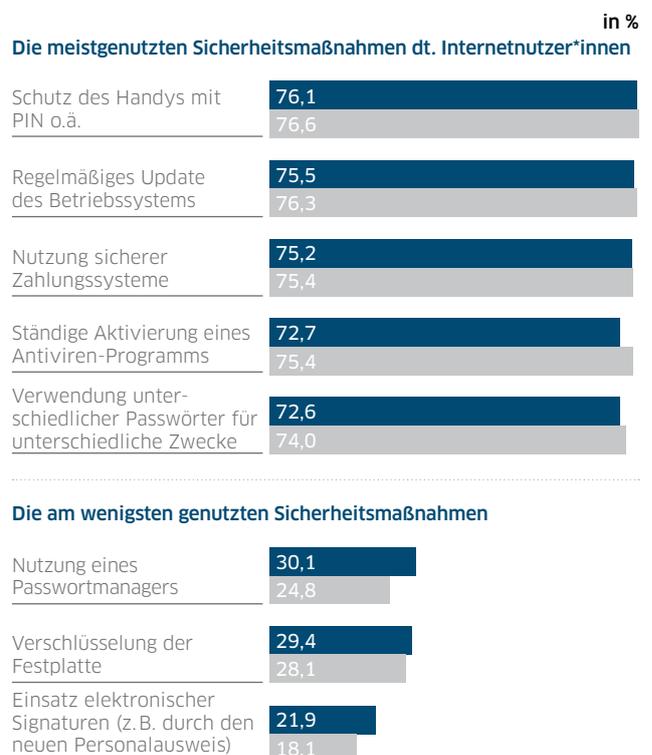


4. Sicherheitsverhalten im Alltag

Der Schutz des Handys mit PIN oder Ähnlichem ist in diesem Jahr erneut die meist genutzte Sicherheitsmaßnahme gefolgt vom regelmäßigen Update des Betriebssystems. Neu auf Position drei (Vorjahr Rang 5) ist aus Sicht der Onliner die Nutzung von sicheren Zahlungssystemen. Den größten Sprung nach vorne im Ranking machte die Zwei-Faktor-Authentisierung von Rang 33 auf 25.



Abb. 9
Spitzenreiter und Schlusslichter Sicherheitsverhalten



Blick von außen: Nutzerverhalten im Überblick

Grundlage für eine wirksame Aufklärung von Verbraucher*innen sind Kenntnisse über ihr typisches Online- und Schutzverhalten im Internet. Hier sind deutliche Unterschiede zwischen Verbrauchergruppen zu erkennen, die sich auf ihre digitale Sicherheitslage niederschlagen.

Nutzungszweck

Spitzenreiter der populärsten Online-Dienste sind „traditionelle“ Anwendungen wie das Schreiben von Mails und Onlineeinkäufe. Auch Soziale Netzwerke und Messenger-Dienste sind – über alle Verbrauchergruppen hinweg – weit verbreitet. In anderen Bereichen variiert das Nutzungsverhalten stark zwischen verschiedenen Altersgruppen: Während 57 Prozent der 16-19-Jährigen gerne Musik über das Internet hören, tun dies nur 9 Prozent der 60-69-Jährigen. Letztere wiederum nutzen das

Netz zu 68 Prozent, um Nachrichtenseiten zu lesen, während dieser Nutzungszweck nur bei 39 Prozent der Jugendlichen vertreten ist. Schlusslicht sind 2020 mit 5,7 Prozent Apps, die mit dem PKW vernetzt sind.

Mobiles Surfen wird zum Spitzenreiter

Während Laptops und Notebooks im Vorjahr noch am häufigsten zum Surfen verwendet wurden, sind internetfähige Handys bzw. Smartphones dieses Jahr auf Platz eins geklettert. Der Trend, dass Desktop-PCs zunehmend weniger genutzt werden, um online zu gehen, setzt sich auch 2020 fort. Sonstige vernetzte Geräte wie Wearables gewinnen hingegen an Bedeutung, liegen jedoch bislang noch weit hinter den populären Geräten.

Abb. 10

Nutzungszweck 2014 vs. 2020

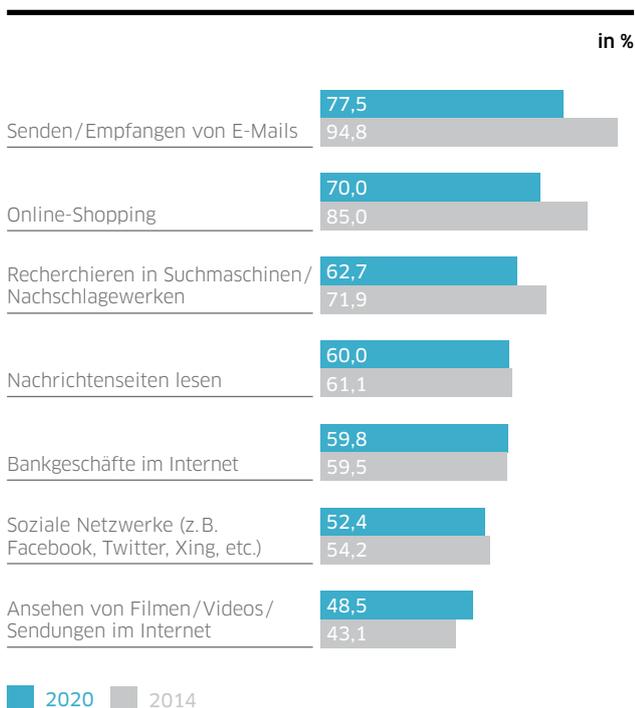
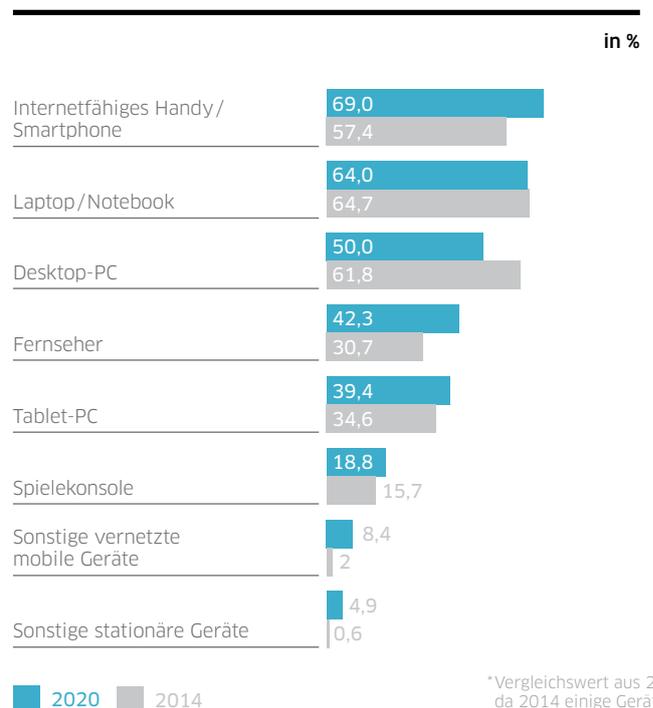


Abb. 11

Genutzte Geräte 2015 vs. 2020*



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



IT- Sicherheitsgefälle: Unterschiede zwischen Verbrauchertypen

Kapitel 2

Die digitale Gesellschaft: Nutzertypen im Netz

Die Verhaltensweisen und Kenntnisse der Onliner in Deutschland unterscheiden sich deutlich voneinander. Der DsiN-Index untersucht hier Kompetenzen, Erfahrungen und Verhaltensweisen von insgesamt fünf Verbrauchertypen. Dies ermöglicht eine differenzierte Sicht darauf, wie unterschiedlich sich deutsche Nutzer*innen im Netz verhalten – und welche Bedürfnisse sie bezüglich einer wirksamen und digitalen Aufklärungsarbeit aufweisen.

Sicherheitsgefälle in der digitalen Gesellschaft

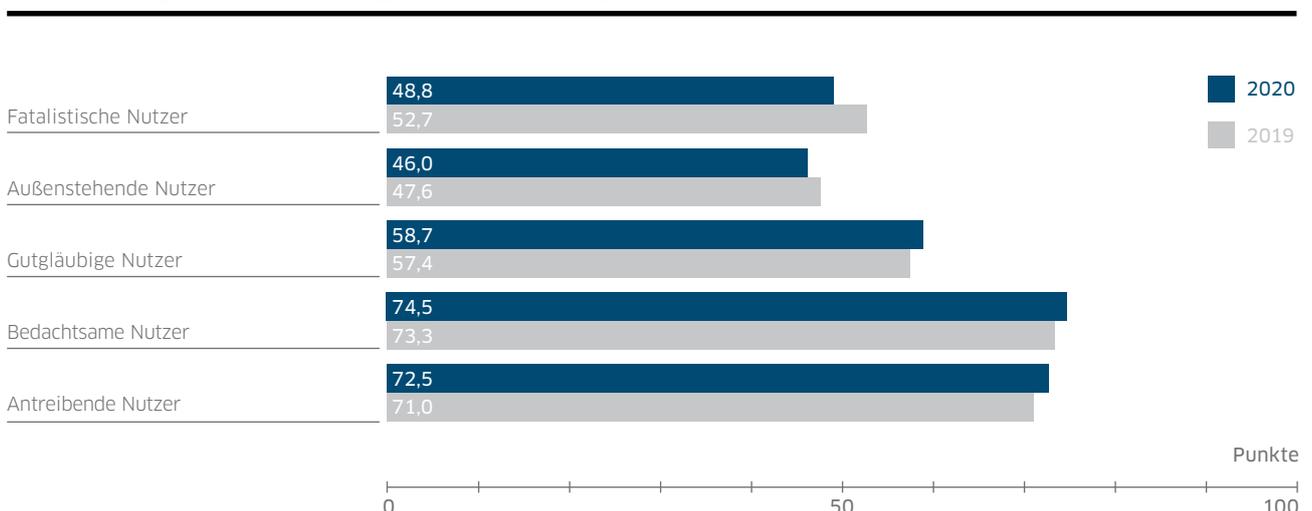
Die gute Nachricht ist, dass sich die digitale Sicherheitslage in Deutschland 2020 insgesamt erneut verbessern konnte. Zugleich wird aber auch deutlich, dass sich das Sicherheitsgefälle zwischen Verbrauchergruppen weiter verstärkt hat. Dieser Trend ist bereits seit der ersten Erhebung des Sicherheitsindex im Jahr 2014 zu erkennen: Trotz ähnlicher technologischer und regulatorischer Voraussetzungen zeigen sich bei der Analyse der einzelnen Nutzergruppen klare Unterschiede bei Kenntnissen und Verhaltensweisen.

Betrachtet man die einzelnen Sicherheitsfaktoren, wird deutlich:

- Sicherheitsvorfälle: Nahezu alle Gruppen haben in den vergangenen 12 Monaten weniger Sicherheitsvorfälle als im Vorjahr bei sich verzeichnet – mit Ausnahme der Fatalisten, bei denen es einen deutlichen Anstieg gab.
- Verunsicherungsgefühl: Das Verunsicherungsgefühl geht bei den antreibenden, bedachtsamen und gutgläubigen Nutzer*innen zurück. Anders bei den außenstehenden und fatalistischen Nutzer*innen: Hier erhöht sich das subjektive Gefühl einer Gefährdung teilweise deutlich.
- Sicherheitswissen: Herausragende Verbesserungen des Sicherheitswissens können in diesem Jahr die gutgläubigen Nutzer*innen verzeichnen. Diese Steigerung kann sogar die Rückgänge in den übrigen Nutzergruppen ausgleichen und sorgt damit für einen generellen Anstieg des Indexwerts.
- Sicherheitsverhalten: Das diesjährige Sicherheitsverhalten stagniert 2020 insgesamt und weist nur

Abb. 12

Übersicht: Digitales Sicherheitsgefälle der Nutzertypen



bei den Außenstehenden eine starke Verschlechterung auf. Der Nachholbedarf an verhaltenswirksamen Maßnahmen ist in dieser Nutzergruppe deshalb besonders groß.

Außenstehende Nutzer*innen sind auch in diesem Jahr bei einem Indexwert von 46,0 Punkten im Gruppenvergleich am unsichersten im Netz unterwegs. Ihre Gruppe verzeichnet gegenüber dem Vorjahr einen leichten Rückgang (2019: 47,6 Punkte). Sie liegen damit 2020 erneut unter dem kritischen Schwellenwert von 50 Punkten, an dem die Bedrohungslage das Schutzniveau übersteigt.

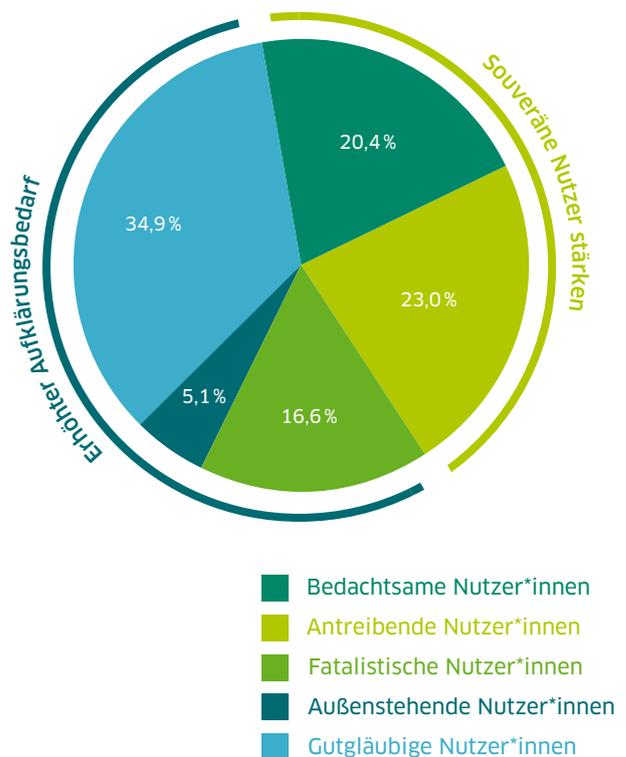
Fatalistische Nutzer*innen erreichen einen Indexwert von 48,8 Punkten und fallen damit dieses Jahr wieder unter die kritische Schwelle von 50 Indexpunkten. Sie landen damit noch leicht vor den außenstehenden Nutzer*innen auf dem vorletzten Platz. Im Vergleich zum Vorjahr hat sich ihr Indexwert um fast vier Punkte verringert. Hier fällt das starke Verunsicherungsgefühl besonders negativ ins Gewicht: Sie verzeichnen trotz ihres starken Sicherheitswissens nach wie vor die meisten Angriffe.

Gutgläubige Nutzer*innen befinden sich mit einem leicht verbesserten Indexwert von 58,7 Punkten wie auch im letzten Jahr auf dem dritten Platz. Ihre Defizite liegen in der Einschätzung von digitalen Risiken und in einer auffälligen Wissens-Verhaltens-Lücke, also einer mangelhaften Umsetzung von eigentlich bekannten Schutzmaßnahmen. Die gutgläubigen Nutzer*innen besitzen eine eher geringe Motivation hinsichtlich Kompetenzvermittlung und Verbesserung des Risikobewusstseins.

Antreibende Nutzer*innen können 2020 mit 1,5 Punkten die größte Steigerung ihres Indexwerts verzeichnen: Mit 72,5 Punkten bleiben sie auf Platz

Abb. 13

Anteil der Nutzertypen an der Gesamtheit der Onlineer



zwei. Die Gruppe weist in diesem Jahr das höchste Sicherheitswissen auf und setzt dieses auch am besten um. Sie gehören damit zu den souveränen Verbraucher*innen und probieren gerne neue digitale Dienste und Angebote aus (43 Prozent).

Bedachtsame Nutzer*innen steigern ihren Index um 1,2 auf 74,5 Punkte und erreichen damit erneut den höchsten Wert aller Nutzergruppen. Diese Gruppe besitzt die geringste Lücke zwischen Sicherheitswissen und -verhalten. 68 Prozent von ihnen geben an, dass sie sich zuerst mit Sicherheitsfragen beschäftigen, bevor sie neue digitale Angebote nutzen.



Außenstehende Nutzer*innen (46 Punkte)

Die Außenstehenden weisen in diesem Jahr erneut den niedrigsten Indexwert mit 46,0 Punkten auf und verschlechtern sich im Vergleich zum Vorjahr nochmals um 1,6 Punkte. Damit liegen sie nun deutlich unter der kritischen Marke von 50 Punkten. Allerdings sinkt der Anteil der außenstehenden Nutzer*innen an der Gesamtheit der Onliner auf nun 5,1 Prozent und damit auf den niedrigsten Wert seit 2014 (9,7 Prozent).

Bedrohungslage

Das Verunsicherungsgefühl der Außenstehenden hat im Vergleich zum Vorjahr um gut drei Indexpunkte zugenommen. Das Öffnen von E-Mail-Anhängen, gefolgt von Online-Banking, wird von dieser Nutzergruppe als besonderes riskant empfunden. Außenstehende sind mit 31,0 Punkten ähnlich oft von Sicherheitsvorfällen betroffen wie bedachtsame Onliner, allerdings bei einer geringeren Internetnutzung. Auffällig ist zudem, dass die Diskrepanz zwischen registrierten Sicherheitsvorfällen und der gefühlten Verunsicherung steigt.

Schutzniveau

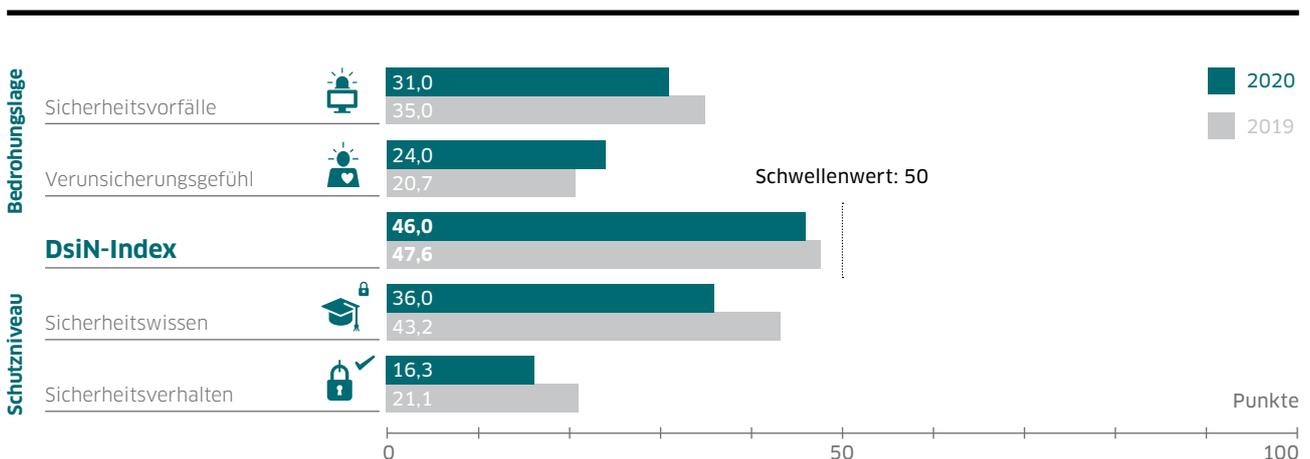
Das Sicherheitswissen und -verhalten hat sich bei den außenstehenden Nutzer*innen verschlechtert. Nach einem deutlichen Anstieg des Sicherheitswissens im letzten Jahr fällt es nun hinter die Werte von 2018 auf 36 Punkte zurück. Auch ihr Verhalten verschlechtert sich weiter und erreicht nur einen Indexwert von 16,3 – der niedrigste Wert im Vergleich der Nutzergruppen.

Verantwortungsgefühl stärken

Insgesamt fühlen sich die außenstehenden Nutzer*innen vom Digitalen überfordert: mit 41 Prozent der höchste Wert über alle Gruppen. Obwohl die Mehrheit (62 Prozent) die Verantwortung bezüglich IT-Sicherheitsfragen bei sich selbst sieht, vertraut diese Gruppe bei Sicherheitsvorfällen auch auf eine Intervention des Staates: 47 Prozent halten strengere Gesetze und 62 Prozent eine stärkere Verfolgung von Verstößen für sehr geeignet, um die Sicherheit im Netz zu erhöhen. Grundsätzlich ist es also wichtig, das Verantwortungsgefühl der Außenstehenden erneut zu stärken.

Abb. 14

DsiN-Indexwert für außenstehende Nutzer*innen



Steckbrief außenstehender Nutzer*innen

DsiN-SicherheitsIndex 2020

Außenstehende Nutzer*innen

Typische Merkmale:

- Ungefähr zu drei viertel weiblich (74 Prozent)
- Hoher Anteil älterer Nutzer über 60 Jahre (53,2 Prozent)
- Eher seltener online: meist weniger als 10 Stunden pro Woche (48,0 Prozent)
- Bevorzugen Laptops oder stationäre PCs
- Knapp die Hälfte fühlt sich von neuen digitalen Diensten überfordert

Indexwert 2020:

46,0 Punkte ↓



Anteil an der Gesamtheit:
5,1% ↓

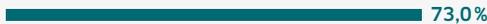


Beschreibung:



Wie Sicherheitsfälle reduzieren?

Vorsichtigerer Umgang mit den eigenen persönlichen Daten



Wie Risikobewusstsein stärken?

Der bewusste Umgang mit Risiken und Chancen sollte in der Schule mehr eingebunden werden



Wie Sicherheitswissen erweitern?

Die Informationen darüber, wie man sich im Internet besser schützen kann, müssten verständlicher sein.



Wie zu Sicherheitsverhalten motivieren?

Konkrete Ansprache durch mein privates Umfeld (z.B. Bekannte, Freunde, Familie)



DsiN-Angebote für Außenstehende:

[sicher-im-netz.de/
angebote-fuer-aussenstehende](https://sicher-im-netz.de/angebote-fuer-aussenstehende)



Sicherheitsvorfälle TOP 3

1. Phishing-Versuch **35,3%**
2. Erhalt infizierter E-Mails/Anhänge/Weblinks **27,3%**
3. Infizierung mit Erpressungssoftware **15,8%**



Verunsicherungsgefühl TOP 3

1. Öffnen von Anhängen in E-Mails **52,8%**
2. Bankgeschäfte im Internet/Online-Banking/-Brokering **50,4%**
3. Austausch vertraulicher Inhalte **44,3%**



Genutzte Schutzmaßnahmen TOP 3

1. Nutzung sicherer Zahlungssysteme **51,8%**
2. Schutz des Handys mit PIN o.ä. **50,4%**
3. Verwendung unterschiedlicher Passwörter **45,4%**



Unbekannte Schutzmaßnahmen TOP 3

1. Prüfung der Vertrauenswürdigkeit von Cloud-Diensten **98,6%**
2. Plug-ins zur Erhöhung der Datensicherheit **97,2%**
3. Inkognito-Funktion **96,2%**



Selten genutzte Schutzmaßnahmen TOP 3

1. Verschlüsselung von Dateien auf dem Computer **0,4%**
2. Einsatz elektronischer Signaturen **0,3%**
3. Verschlüsselung der Festplatte **0%**



Fatalistische Nutzer*innen (48,8 Punkte)

Im Vergleich zum Vorjahr ist der Indexwert der fatalistischen Nutzer*innen um 3,9 Punkte gefallen und erreicht nun 48,8 Punkte. Sie sind damit die am tiefsten gefallene Nutzergruppe und liegen 2020 unter der kritischen Schwelle von 50 Punkten. Fatalisten wissen relativ gut Bescheid, fühlen sich unsicher – und setzen ihr Schutzwissen dennoch nicht ausreichend ein.

Bedrohungslage

In diesem Jahr ist bei den Fatalisten der Wert der Sicherheitsvorfälle um 6,5 Punkte deutlich gestiegen. Mit diesem Anstieg geht eine noch höhere Verunsicherung einher: Das Verunsicherungsgefühl steigt erheblich um 8,8 Punkte auf 79,6 und ist damit auf den höchsten Stand seit Beginn der Messung im Jahr 2014. Als besonders gefährlich werden das Öffnen von Anhängen in E-Mails und das Veröffentlichen von eigenen Inhalten im Netz empfunden.

Schutzniveau

Die fatalistischen Nutzer*innen stagnieren in diesem Jahr in ihrem Sicherheitswissen: Mit 85,5 Punkten

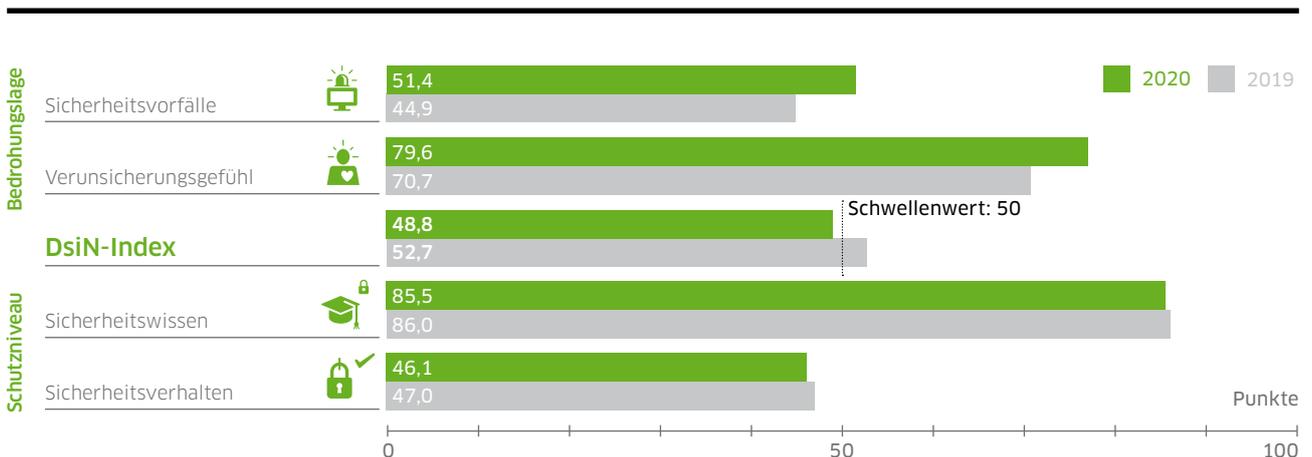
erreichen sie zwar einen hohen Wert, liegen damit jedoch knapp unter dem Vorjahresniveau. Typisch für diese Gruppe ist, dass sich ihr Sicherheitsverhalten trotz einer ausgesprochen hohen Unsicherheit nicht verbessert – es verschlechtert sich in diesem Jahr sogar noch weiter. Hohe Diskrepanzen zwischen Wissen und Verhalten bestehen unter anderem beim Thema Verschlüsselung.

Verunsicherungen entgegenwirken und zum Handeln motivieren

Die Fatalisten wissen, dass sie selbst in der Pflicht wären, ihre Daten zu schützen. Zwei Drittel halten dies für ein geeignetes Mittel, um die eigenen Sicherheitsvorfälle zu reduzieren; mehr als in jeder anderen Gruppe. Dennoch besteht bei ihnen große Unsicherheit darüber, wie dies in die Praxis umzusetzen ist. So behauptet fast ein Drittel, dass vor allem eine geringere Internetnutzung ein geeignetes Mittel zum Selbstschutz wäre, statt Sicherheitsmaßnahmen selbst aktiv anzuwenden. Hier gilt es, Nutzer*innen dazu zu motivieren, ihre Unsicherheiten abzubauen und ihr Wissen in die Tat umzusetzen.

Abb. 16

DsiN-Indexwert für fatalistische Nutzer*innen



Steckbrief fatalistischer Nutzer*innen

DsiN-SicherheitsIndex 2020

Fatalistische Nutzer*innen

Typische Merkmale:

- Sind in allen Geschlechtergruppen zu finden
- Am häufigsten zwischen 50 und 69 Jahre alt (29 Prozent)
- Meist zwischen 5 bis 10 Stunden online (19,5 Prozent)
- Nutzen Laptops und Smartphones am häufigsten
- Zweifel an der Wirksamkeit von Schutzmaßnahmen

Indexwert 2020:

48,8 Punkte ↓



Anteil an der Gesamtheit:
16,6% ↑



Beschreibung:



Wie Sicherheitsfälle reduzieren?

Stärkere Verfolgung von Gesetzesverstößen
85,7%



Wie Risikobewusstsein stärken?

Risiken müssten in der öffentlichen Diskussion stärker aufgegriffen werden
74,5%



Wie Sicherheitswissen erweitern?

Es müsste mehr professionelle Ansprechpartner geben, die persönliche Hilfestellung bieten
72,8%



Wie zu Sicherheitsverhalten motivieren?

Einfachere Sicherheitseinstellungen bei Programmen und Geräten
65,3%



DsiN-Angebote für Fatalisten:

[sicher-im-netz.de/
angebote-fuer-fatalisten](https://sicher-im-netz.de/angebote-fuer-fatalisten)



Sicherheitsvorfälle TOP 3

1. Phishing-Versuch **44,1%**
2. Erhalt infizierter E-Mails/Anhänge/Weblinks **30,9%**
3. Unbefugte Ortung der eigenen mobilen Geräte **26,1%**



Verunsicherungsgefühl TOP 3

1. Öffnen von Anhängen in E-Mails **90,6%**
2. Veröffentlichung von eigenen Inhalten **90,0%**
3. Soziale Netzwerke **86,7%**



Genutzte Schutzmaßnahmen TOP 3

1. Regelmäßiges Update des Betriebssystems **69,7%**
2. Schutz des Handys mit PIN o. ä. **69,1%**
3. Ständige Aktivierung eines Antiviren-Programms **69,1%**



Unbekannte Schutzmaßnahmen TOP 3

1. Plug-ins zur Erhöhung der Datensicherheit **20,7%**
2. Einsatz elektronischer Signaturen **19,8%**
3. Inkognito-Funktion **19,5%**



Selten genutzte Schutzmaßnahmen TOP 3

1. Plug-ins zur Erhöhung der Datensicherheit **30,8%**
2. Biometrische Identifizierung **28,5%**
3. Einsatz elektronischer Signaturen **27,5%**



Gutgläubige Nutzer*innen (58,7 Punkte)

Mit einem Indexwert von 58,7 Punkten befinden sich die gutgläubigen Nutzer*innen im Jahr 2020 erneut auf dem dritten Platz. Eines ihrer größten Defizite liegt nach wie vor in der Verharmlosung von digitalen Risiken. Doch auch die Wissens-Verhaltens-Lücke, also die unzureichende Umsetzung von eigentlich bekannten Schutzmaßnahmen, ist hier erheblich.

Bedrohungslage

Bei den gutgläubigen Nutzer*innen ist der Wert der Sicherheitsvorfälle um 2,5 Punkte auf knapp 33 Punkte zurückgegangen. Erneut weiter verringert hat sich auch das Verunsicherungsgefühl: 2020 sind es 1,4 Punkte weniger. Damit bleiben sie diejenigen Nutzer*innen, die eine nur geringe Verunsicherung empfinden. So schätzen lediglich 42 Prozent von ihnen das Öffnen von E-Mail-Anhängen als potenzielles Risiko ein.

Schutzniveau

2020 verbesserten die gutgläubigen Nutzer*innen ihr Sicherheitswissen auf 89,8 Punkte (2019: 88,2); gleichzeitig verbleibt das Sicherheitsverhalten auf

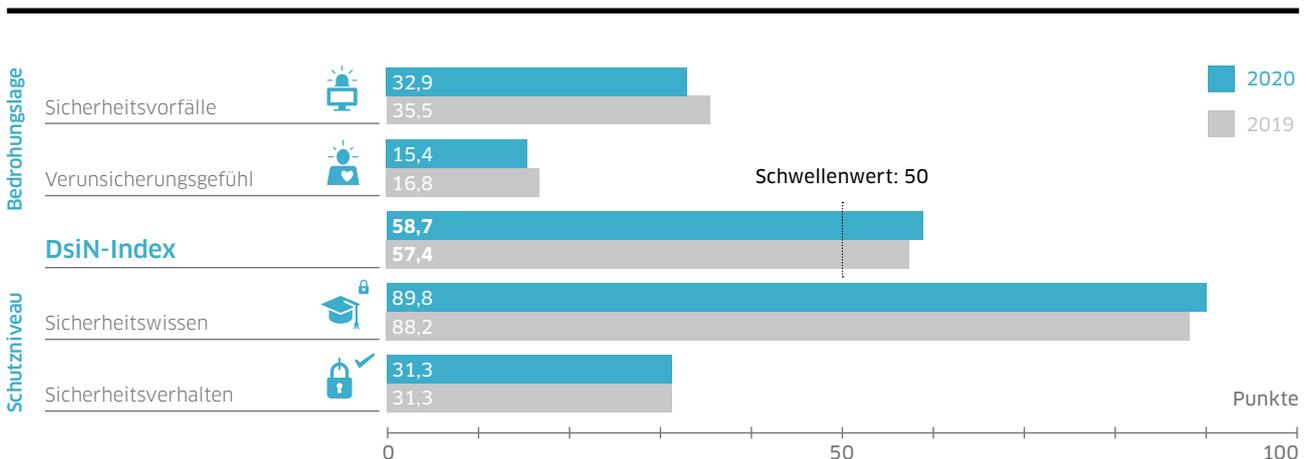
dem Vorjahresniveau. Mit einem Indexwert von 31,3 Punkten weisen sie weiter ein mangelhaftes Schutzverhalten auf, die Wissens-Verhaltens-Lücke wird entsprechend größer. Die am häufigsten genutzten Schutzmaßnahmen sind die Bezahlung über sichere Systeme (60,6 Prozent) und die Logout-Funktion (58,7 Prozent). Eine Firewall hingegen verwenden weniger als die Hälfte, obwohl sie 97,4 Prozent bekannt ist.

Vorhandenes Sicherheitswissen aktivieren und anwenden

Die Gutgläubigen weisen ein eher geringes Interesse an den Themen Aufklärung und Kompetenzvermittlung auf. Ihr Gesamtanteil in der Bevölkerung hat leicht abgenommen, sie stellen jedoch nach wie vor die größte Nutzergruppe dar. Auch aufgrund ihrer großen Wissens-Verhaltens-Lücke sollten sie besonders in der Aufklärungsarbeit berücksichtigt werden. Diese sollte die möglichen Risiken digitaler Dienste stärker hervorheben sowie die Folgen von vernachlässigtem Sicherheitsverhalten aufzeigen.

Abb. 18

DsiN-Indexwert für gutgläubige Nutzer*innen



Steckbrief gutgläubiger Nutzer*innen

DsiN-SicherheitsIndex 2020

Gutgläubige Nutzer*innen

Typische Merkmale:

- Das Geschlechterverhältnis ist relativ ausgeglichen
- Alle Altersgruppen sind vertreten
- Meist zwischen 10 und 20 Stunden wöchentlich online (25,4 Prozent)
- Nutzen Smartphones und Laptops gefolgt von Desktop-PCs
- Größte Diskrepanz zwischen Wissen und Verhalten

Indexwert 2020:

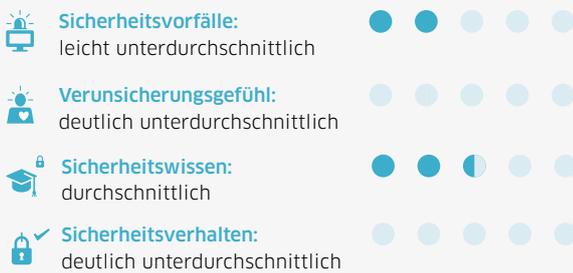
58,7 Punkte ↑



Anteil an der Gesamtheit:
34,9% ↓



Beschreibung:



Wie Sicherheitsfälle reduzieren?

Vorsichtigerer Umgang mit den eigenen persönlichen Daten

68,0%



Wie Risikobewusstsein stärken?

Anbieter von Diensten und Programmen müssten mehr über Risiken aufklären

54,9%



Wie Sicherheitswissen erweitern?

Die Informationen darüber, wie man sich im Internet besser schützen kann, müssten verständlicher sein

52,1%



Wie zu Sicherheitsverhalten motivieren?

Einfachere Sicherheitseinstellungen bei Programmen und Geräten

59,9%



DsiN-Angebote für Gutgläubige:

[sicher-im-netz.de/
angebote-fuer-gutglaeubige](https://sicher-im-netz.de/angebote-fuer-gutglaeubige)



Sicherheitsvorfälle TOP 3

1. Phishing-Versuch **20,4%**
2. Erhalt infizierter E-Mails/Anhänge/Weblinks **19,7%**
3. Betrug beim Online-Einkauf/Online-Buchungen **9,8%**



Verunsicherungsgefühl TOP 3

1. Öffnen von Anhängen in E-Mails **42,0%**
2. Austausch vertraulicher Inhalte **26,9%**
3. Soziale Netzwerke **24,0%**



Genutzte Schutzmaßnahmen TOP 3

1. Nutzung sicherer Zahlungssysteme **60,6%**
2. Logout-Funktion **58,7%**
3. Automatisches Update des Betriebssystems des Computers **57,1%**



Unbekannte Schutzmaßnahmen TOP 3

1. Inkognito-Funktion **18,1%**
2. Plug-ins zur Erhöhung der Datensicherheit **16,5%**
3. Auslesen der E-Mail Header **15,5%**



Selten genutzte Schutzmaßnahmen TOP 3

1. Plug-ins zur Erhöhung der Datensicherheit **11,5%**
2. Einsatz elektronischer Signaturen **8,4%**
3. Prüfung der Vertrauenswürdigkeit von Cloud-Diensten **8,2%**



Antreibende Nutzer*innen (72,5 Punkte)

Antreibende Nutzer*innen erreichen 2020 mit 72,5 Punkten einen um 1,5 Punkte höheren Indexwert und weisen insgesamt die zweitbeste Sicherheitslage auf. Sie haben mit den Bedachtsamen das höchste Sicherheitswissen, und setzen dieses zudem am besten um. Durch ihre vielseitige Internetnutzung sind sie jedoch häufiger von Sicherheitsvorfällen betroffen und haben daher nur die insgesamt zweitbeste digitale Sicherheitslage. Dennoch probiert keine andere Nutzergruppe so gerne neue digitale Angebote aus (43,2 Prozent).

Bedrohungslage

Obwohl sie die Gruppe mit den zweithäufigsten Sicherheitsvorfällen ist, sind diese bei den Antreibenden um 2,4 Punkte erneut zurückgegangen. Gleichzeitig hat sich auch das Gefährdungsgefühl um 1,5 Punkte auf nun 21,1 Punkte vermindert. Als besonders gefährlich wird das Öffnen von Anhängen in E-Mails (47,8 Prozent) empfunden, gefolgt vom Austausch vertraulicher Daten über das Netz (34,3 Prozent).

Schutzniveau

Trotz eines leichten Rückgangs der Sicherheitskom-

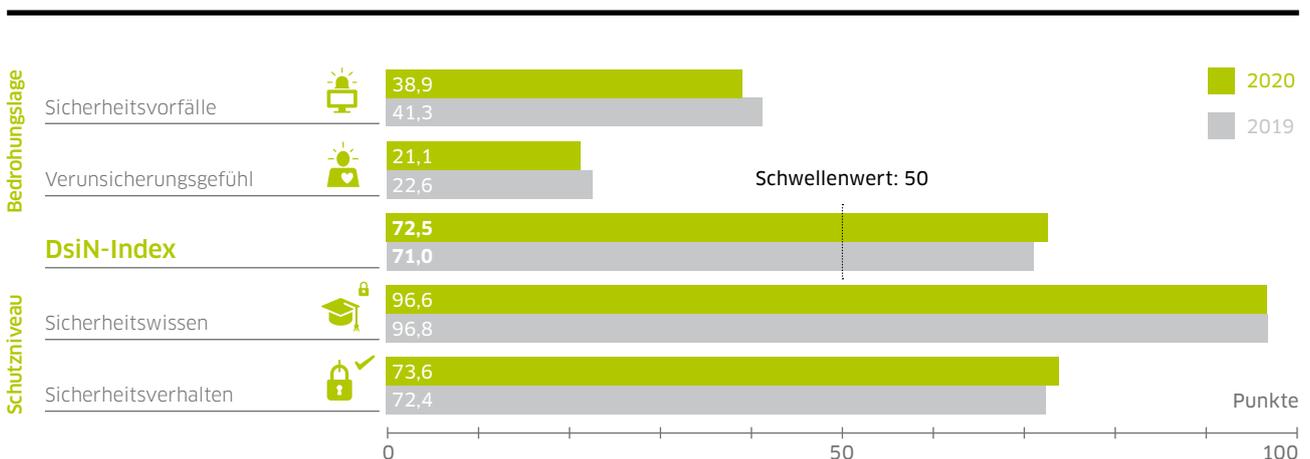
petenz um 0,2 Punkte kann diese Gruppe nach wie vor das beste Sicherheitswissen vorweisen. Alle bis auf eine abgefragte Sicherheitsmaßnahme sind den Antreibenden zu über 92 Prozent bekannt. Auch wenn es darum geht, dieses Wissen anzuwenden, sind sie sehr aktiv: So steigerte sich ihr Sicherheitsverhalten um 1,2 auf 73,6 Punkte. Damit überholen die antreibenden Nutzer*innen in diesem Punkt erstmals die Bedachtsamen.

Motivation bewahren und mit anderen Nutzergruppen zusammenarbeiten

Gemeinsam mit den Bedachtsamen weisen die Antreibenden die geringste Schere zwischen Sicherheitswissen und -verhalten auf. Dies hängt in erster Linie mit der hohen Motivation zusammen, ihr Sicherheitsverhalten weiter zu verbessern. Auch wünscht sich rund ein Drittel nach wie vor mehr Informationen zu möglichen Risiken. Diese Bereitschaft, ihr Sicherheitswissen auszubauen und anzuwenden, bietet großes Potenzial für die Zusammenarbeit mit anderen Nutzergruppen, deren Motivation in diesem Bereich verbesserungswürdig ist.

Abb. 20

DsiN-Indexwert für antreibende Nutzer*innen



Steckbrief antreibender Nutzer*innen

DsiN-SicherheitsIndex 2020

Antreibende Nutzer*innen

Typische Merkmale:

- Ausgeglichenes Geschlechterverhältnis
- Die Mehrheit ist zwischen 20 und 49 Jahren alt (51,5 Prozent)
- Vielnutzer: Meist zwischen 10 und 30 Stunden wöchentlich online (42,0 Prozent)
- Nutzen vor allem Smartphones, im Vergleich zu anderen auch häufiger TV und Konsole
- Probieren gerne neue digitale Dienste aus

Indexwert 2020:

72,5 Punkte ↑



Anteil an der Gesamtheit:
23,0% ↑



Beschreibung:



Wie Sicherheitsfälle reduzieren?

Vorsichtigerer Umgang mit den eigenen persönlichen Daten

81,5%

Wie Risikobewusstsein stärken?

Der bewusste Umgang mit Risiken und Chancen sollte in der Schule mehr eingebunden werden

78,2%

Wie Sicherheitswissen erweitern?

Es müsste mehr Aufklärungsangebote in beruflicher oder schulischer Aus- und Weiterbildung geben

72,4%

Wie zu Sicherheitsverhalten motivieren?

Einfachere Sicherheitseinstellungen bei Programmen und Geräten

81,6%



DsiN-Angebote für Antreibende:

[sicher-im-netz.de/
angebote-fuer-antreibende](https://sicher-im-netz.de/angebote-fuer-antreibende)



Sicherheitsvorfälle TOP 3

1. Phishing-Versuch **28,6%**
2. Erhalt infizierter E-Mails/Anhänge/Weblinks **28,5%**
3. Ausspähen von Zugangsdaten für das Online-Banking **11,7%**



Verunsicherungsgefühl TOP 3

1. Öffnen von Anhängen in E-Mails **47,8%**
2. Austausch vertraulicher Inhalte **34,3%**
3. Bankgeschäfte im Internet/Online-Banking/-Brokering **30,6%**



Genutzte Schutzmaßnahmen TOP 3

1. Nutzung sicherer Zahlungssysteme **93,9%**
2. Ständige Aktivierung eines Antiviren-Programms **91,3%**
3. Sicherung des W-Lan durch ein Passwort **91,3%**



Unbekannte Schutzmaßnahmen TOP 3

1. Auslesen der E-Mail Header **10,2%**
2. Einsatz elektronischer Signaturen **8,0%**
3. Inkognito-Funktion **7,0%**



Selten genutzte Schutzmaßnahmen TOP 3

1. Nutzung eines Passwortmanagers **45,7%**
2. Auslesen der E-Mail Header **43,9%**
3. Einsatz elektronischer Signaturen **37,3%**



Bedachtsame Nutzer*innen (74,5 Punkte)

Bedachtsame Nutzer*innen steigern dieses Jahr ihren Index um 1,2 auf 74,5 Punkte und erreichen damit erneut den höchsten Sicherheitswert aller Nutzergruppen. Diese Gruppe hat die geringste Lücke zwischen Sicherheitswissen und -verhalten. Sie gehören zudem zu den Onlinern, die am häufigsten (65,6 Prozent) auf Angebote verzichten, da sie skeptisch in puncto Sicherheit sind. Falls sie sich dennoch für ein neues digitales Angebot entscheiden, beschäftigen sie sich mehrheitlich (67,8 Prozent) mit Sicherheitsfragen.

Bedrohungslage

Die Zahl der Sicherheitsvorfälle der Bedachtsamen hat im Vergleich zum Vorjahr deutlich um 4,1 Punkte abgenommen. So ist es nicht verwunderlich, dass auch das Verunsicherungsgefühl um 1,8 auf 24,0 Punkte gesunken ist. Dennoch befinden sie sich gemeinsam mit den Außenstehenden diesbezüglich noch an zweiter Stelle und verhalten sich dementsprechend um einiges vorsichtiger als sie. Besonders problematisch empfinden die Bedachtsamen das Öffnen von Anhängen in E-Mails (65,3 Prozent) sowie die Nutzung von Sozialen Netzwerken (43,3 Prozent).

Schutzniveau

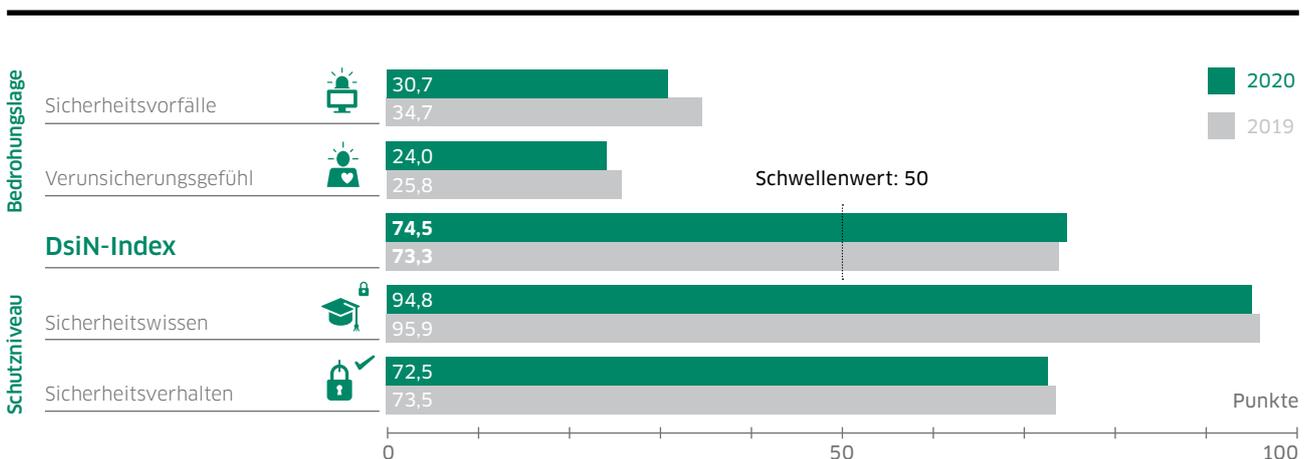
Beim Sicherheitswissen liegen die bedachtsamen mit 94,8 Punkten knapp hinter den antreibenden Nutzer*innen auf Platz zwei. Ähnlich sieht es in diesem Jahr bei dem Sicherheitsverhalten aus: Hier erreichen sie einen Wert von 72,5 Punkten und liegen damit ebenfalls geringfügig hinter den Antreibenden. Allerdings weisen die Bedachtsamen dafür eine geringere Wissens-Verhaltens-Lücke auf.

Sichere Lage ausbauen

Bedachtsame Nutzer*innen sehen in erster Linie sich selbst in der Pflicht, für ihre Onlinesicherheit zu sorgen: rund 90 Prozent meinen, dass ein vorsichtigerer Umgang mit den eigenen persönlichen Daten zu einer Reduzierung von Sicherheitsvorfällen führe. Sie selbst agieren auch nach diesem Prinzip und bewegen sich von allen Nutzergruppen am sichersten im Netz. Bedachtsame können zudem selbst als Vorbilder agieren und insbesondere die Gutgläubigen zu einem reflektierteren Umgang im Netz motivieren.

Abb. 22

DsiN-Indexwert für bedachtsame Nutzer*innen



Steckbrief bedachtsamer Nutzer*innen

DsiN-SicherheitsIndex 2020

Bedachtsame Nutzer*innen

Typische Merkmale:

- Das Geschlechterverhältnis ist relativ ausgeglichen
- Häufig zwischen 40 und 59 Jahren alt (49 Prozent)
- Meist 10 bis 20 Stunden pro Woche online
- Nutzen vor allem Smartphones, aber auch alle anderen Geräte
- Stehen neuen Angeboten prüfend-kritisch gegenüber

Indexwert 2020:

74,5 Punkte ↑



Anteil an der Gesamtheit:
20,4% ↓



Beschreibung:

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

Wie Sicherheitsfälle reduzieren?

Vorsichtigerer Umgang mit den eigenen persönlichen Daten
90,2%

Wie Risikobewusstsein stärken?

Der bewusste Umgang mit Risiken und Chancen sollte in der Schule mehr eingebunden werden
79,6%

Wie Sicherheitswissen erweitern?

Die Informationen darüber, wie man sich im Internet besser schützen kann, müssten verständlicher sein
71,3%

Wie zu Sicherheitsverhalten motivieren?

Einfachere Sicherheitseinstellungen bei Programmen und Geräten
80,6%



DsiN-Angebote für Bedachtsame

sicher-im-netz.de/angebote-fuer-bedachtsame



Sicherheitsvorfälle TOP 3

1. Phishing-Versuch **29,4%**
2. Erhalt infizierter E-Mails/Anhänge/Weblinks **16,1%**
3. Mobbing/Belästigungen/Rufschädigung **5,8%**



Verunsicherungsgefühl TOP 3

1. Öffnen von Anhängen in E-Mails **65,3%**
2. Soziale Netzwerke **43,3%**
3. Dating-Anwendungen **38,6%**



Genutzte Schutzmaßnahmen TOP 3

1. Regelmäßiges Update des Betriebssystems **95,3%**
2. Verschlüsselte Datenverbindung bei Online-Banking u. -Shopping **95,2%**
3. Nutzung sicherer Zahlungssysteme **94,8%**



Unbekannte Schutzmaßnahmen TOP 3

1. Auslesen der E-Mail Header **17,4%**
2. Plug-ins zur Erhöhung der Datensicherheit **11,8%**
3. Prüfung der Vertrauenswürdigkeit von Cloud-Diensten **8,6%**



Selten genutzte Schutzmaßnahmen TOP 3

1. Verschlüsselung der Festplatte **38,5%**
2. Biometrische Identifizierung **36,3%**
3. Einsatz elektronischer Signaturen **28,3%**

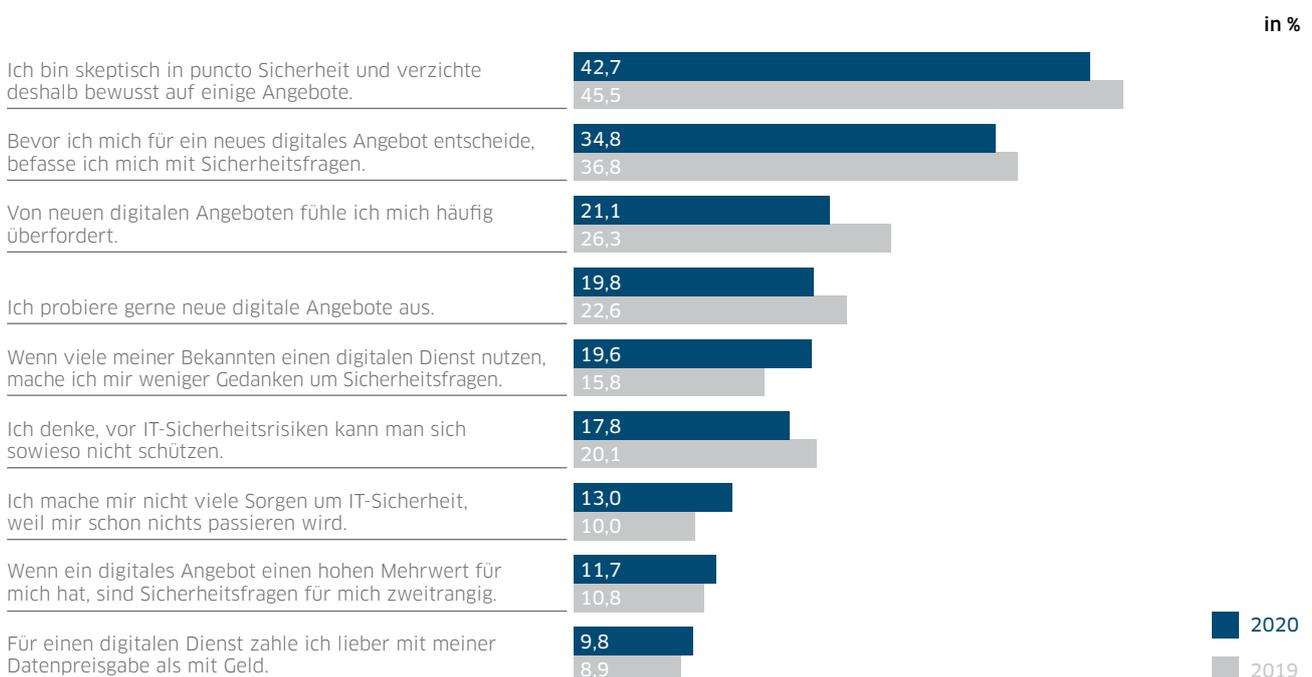
Einstellungen und Nutzungsgewohnheiten

Die unterschiedliche IT-Sicherheitslage der DsiN-Verbrauchertypen zeigt das Sicherheitsgefälle innerhalb der Internet-Gesellschaft. In Bezug auf digitale Sicherheit basiert dieses auf unterschiedlichen Haltungen, Interessen und Verhaltensregeln. Fest steht: Grundsätzlich halten nur rund ein Drittel der Verbraucher*innen das Internet für sicher. Dies wirkt sich auch auf die Digitalpraxis und Digitalerfahrung aus: Mit 19,8 Prozent probiert nur jeder Fünfte gerne neue digitale Angebote aus; das sind 2,8 Prozent weniger als im Vorjahr. Dennoch befassen sich lediglich 34,8 Prozent

der Verbraucher*innen mit Sicherheitsfragen, wenn sie sich für neue digitale Angebote entscheiden (-2 Prozentpunkte). Auch hier gilt es, Verbraucher*innen weiterhin dazu zu motivieren, sich mehr mit IT-Sicherheitsfragen auseinander-zusetzen.

Abb. 24

Wie würden Sie ganz allgemein Ihren Umgang mit dem Internet beschreiben?





Kapitel 3

**Digitale
Lebenswelten**

Fokusthema: Digitale Bürgerportale

Den Wohnsitz ummelden, Kindergeld beantragen oder den Pass erneuern lassen: In den nächsten Jahren soll bundesweit eine Vielzahl von Verwaltungsleistungen für Bürger*innen einheitlich online zugänglich gemacht werden. Diese Dienstleistungen betreffen in der Regel personenbezogene Daten und andere sensible Informationen, sodass Fragen nach Datenschutz und -sicherheit eine entscheidende Bedeutung zukommen. Das Index-Fokusthema beleuchtet in diesem Jahr die Kenntnisse, Vorteile und Vorbehalte aus Sicht deutscher Onliner hinsichtlich digitaler Bürgerportale.

Kenntnisse und Nutzung

Bislang sind die Kenntnisse über digitale Verwaltungsangebote der öffentlichen Hand bei Verbraucher*innen mäßig verbreitet: Von 15 abgefragten Angeboten sind nur drei knapp mehr als der Hälfte aller Onliner bekannt. Spitzenreiter ist die bundesweit verfügbare elektronische Steuererklärung (ELSTER) mit 68,1 Prozent. Mit 54,6 bzw. 51,6 Prozent

Bekanntheit folgen das Jobcenter-Portal sowie die Terminbuchung beim Arbeitsamt. Auch die Nutzung wird von der elektronischen Steuerklärung angeführt: 48,9 Prozent der Onliner, die das Angebot kennen, haben es bereits genutzt (von den Befragten insgesamt: 33,3 Prozent). Auf den Plätzen zwei bis vier folgen die Beantragung von höchstpersönlichen Dokumenten mit 42,3 Prozent, Terminbuchung beim Bürgeramt (42,2 Prozent) und das Arbeitsamt-/Jobcenter-Portal mit 42,0 Prozent.

Hohes Vertrauen in Bürgerdienste

80,4 Prozent der Verbraucher*innen halten die digitale Bürgerdienste insgesamt für sicher, davon 33,0 Prozent sogar für sicher bis sehr sicher. Lediglich 4,3 Prozent schätzen die Online-Angebote als unsicher bis sehr unsicher ein. 93,5 Prozent der Befragten haben noch keine Sicherheitsvorfälle in diesem Bereich erlebt. Insgesamt genießen Verwaltungsdienste in puncto Sicherheit ein grundsätzlich hohes Vertrauen.

Abb. 25

Digitale Bürgerportale aus Verbrauchersicht

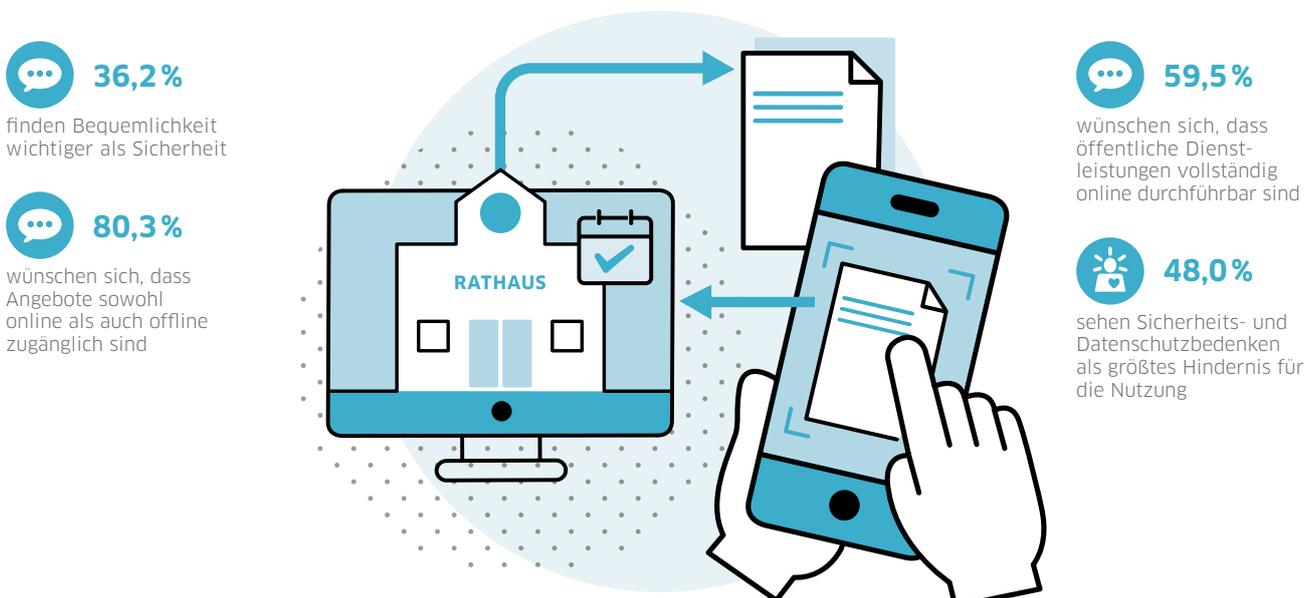
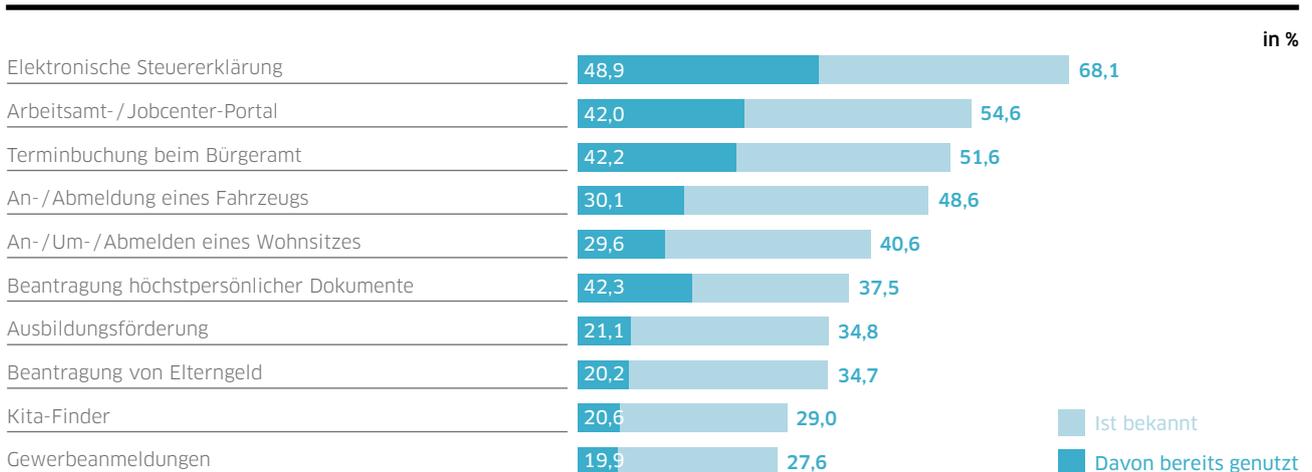


Abb. 26

Kenntnisse und Nutzung von Online-Angeboten der öffentlichen Hand



Zusätzlich herrscht eine bemerkenswerte „Kompromissbereitschaft“ bei Sicherheitsfragen vor: mehr als ein Drittel der Befragten (36,2 Prozent) geben an, dass sie bei entsprechenden Online-Angeboten Kompromisse hinsichtlich des Datenschutzes oder der IT-Sicherheit eingehen würden, wenn sich dafür Zeit und Geld einsparen ließe.

Mehrheit wünscht sich Onlineangebote

Aktuell wünscht sich die große Mehrheit der Befragten, dass mehr Dienstleistungen der Verwaltung online zugänglich gemacht werden. Angebote sollen jedoch weiterhin auch offline verfügbar bleiben (80,3 Prozent). Dass Verwaltungsangelegenheiten ausschließlich online zugänglich und durchführbar sein sollen, wünschen sich immerhin noch 59,5 Prozent. Die Offenheit der Onliner zusätzlich steigern würde der Abbau von Sicherheits- und Datenschutzbedenken (48,0 Prozent). 45,4 Prozent würden Angebote eher wahrnehmen, wenn Zugang, Auffindbarkeit und Nutzung einfacher wären. Diese Zahlen verdeutlichen, dass Unterstützung und Aufklärung auf der Ebene der Akzeptanz von entscheidender Bedeutung sind.

Aufklärungsangebote ausbauen und Dialoge stärken

Dadurch, dass sich die Mehrheit der Verbraucher*innen dafür ausspricht, Verwaltungsangelegenheiten verstärkt digital zugänglich zu machen, steigt zugleich der Bedarf an Aufklärung. Dabei sehen die Befragten sowohl die öffentliche Hand (67,4 Prozent), als auch unabhängige Institute (62,7 Prozent) in der Pflicht, über sichere Nutzungsmöglichkeiten von Online-Angeboten aufzuklären. Ebenso wichtig ist in diesem Zusammenhang ein stärkerer Austausch: So wünschen sich 62,4 Prozent der Befragten generell einen stärkeren Dialog; 61,4 Prozent wünschen sich diesen zudem auch in ihrem vertrauten Umfeld.

DsiN-Angebote
[sicher-im-netz.de/
digitale-buergerportale](https://sicher-im-netz.de/digitale-buergerportale)



Smarte Versicherungstarife

Seit einigen Jahren werden Versicherungen angeboten, die auf persönliche Daten wie Verhaltens- und Gesundheitsdaten zurückgreifen, um durch individuelle Bewertungen passgenaue Tarife und Vorsorge zu ermöglichen. Diese sogenannten „smarten Versicherungstarife“ waren Fokus-thema des Sicherheitsindex 2019. 22,3 Prozent der Internetnutzer*innen geben 2020 an, bereits ein Angebot für einen smarten Tarif erhalten zu haben – 2019 waren es noch 23,9 Prozent.

Aufklärungsbedarfe und Vorbehalte

Rund ein Drittel (29,1 Prozent) können sich vorstellen, sich grundsätzlich für einen smarten Tarif zu entscheiden. Dieser Wert ist gegenüber dem Vorjahr leicht rückläufig (36,1 Prozent). Vorbehalte bleiben weiterhin hoch, sind jedoch insgesamt zurückgegangen: Derzeit sehen 64,1 Prozent der Bürger*innen erhöhte Datenschutzrisiken wie Missbrauch und Manipulation (-8,3 Prozentpunkte zum Vorjahr).

63,1 Prozent sehen zudem die Gefahr, dass persönliche Daten auch von Dritten verwendet werden könnten.

Bei jedem dritten Onliner (30,8 Prozent) überwiegen positive Aspekte von smarten Versicherungstarifen: Sie meinen, dass das Tracking des Verhaltens oder Lebensstils dazu beitragen kann, Versicherungstarife zu einem gerechteren Preis anzubieten (-5,2 Prozentpunkte). Rund die Hälfte sieht den Grundgedanken einer Versicherungsgemeinschaft beeinträchtigt, wenn Tarife durch smarte Grundlagen stärker auf das individuelle Risiko ausgerichtet werden (48,8 Prozent).

DsiN-Angebote

[sicher-im-netz.de/
smarte-versicherungstarife](https://sicher-im-netz.de/smarte-versicherungstarife)



Abb. 27

Smarte Versicherungstarife aus Verbrauchersicht



22,3%

wurde schon ein smarter Versicherungstarif angeboten



29,1%

können sich vorstellen, sich für smarte Tarife zu entscheiden



64,1%

sehen ein erhöhtes Datenschutzrisiko bei der Speicherung persönlicher Daten



48,8%

sehen den Grundgedanken der Versicherungsgemeinschaft in Gefahr



63,1%

befürchten eine Weitergabe der Gesundheitsdaten an Dritte

Digitale Gesundheits- und Fitnessdienste

Zunehmende Unsicherheit bei Onlinediensten im Gesundheitswesen: Unterstützende Onlinedienste wie Online-Terminbuchung oder die elektronische Patientenakte werden in diesem Jahr als gefährlicher wahrgenommen. So halten 25,9 Prozent der Onliner die Nutzung für gefährlich oder sehr gefährlich, gegenüber 24,4 Prozent im Vorjahr.

Das höchste Risiko sehen die Onliner dabei im digitalen Austausch gesundheitsbezogener Daten (z. B. vom Smartphone des Patienten an den Arzt). 58,1 Prozent sind dieser Meinung. Im Sammeln und Analysieren von personenbezogenen Gesundheitsdaten in Datenbanken sehen die Befragten das zweithöchste Risiko (57,9 Prozent). Auf Platz drei folgt das Anlegen und Nutzen einer elektronischen Patientenakte (57,2 Prozent), gefolgt vom digitalen Austausch gesundheitsbezogener Daten zwischen Patient*innen, Ärzt*innen und anderen (54,1 Prozent). Trotz der Vorbehalte nimmt die Nutzung zu:

Statt 9,6 Prozent sind es in diesem Jahr bereits 13,1 Prozent der Internetnutzer*innen, die digitale Gesundheitsdienste in Anspruch nehmen.

Steigendes Vertrauen in Fitness-Apps

Anders sieht es bei den wahrgenommenen Risiken von Fitness- und Gesundheitsprogrammen aus, wie Apps zur Kontrolle des Schlafverhaltens oder zur Messung des Blutzuckers. Hier hat sich die Zahl der Nutzer*innen zwar von 14,3 Prozent (2019) auf 11,5 Prozent verringert, doch geben nur 21,1 Prozent an, sie für gefährlich oder sehr gefährlich zu halten. Damit hat sich das Gefährdungsempfinden hier diesem Jahr weiter leicht verringert (-0,9 Prozentpunkte).

DsiN-Angebote

[sicher-im-netz.de/
digitale-gesundheit](https://sicher-im-netz.de/digitale-gesundheit)



Abb. 28

Digitale Gesundheits- und Fitnessdienste aus Verbrauchersicht

57,2%
hat Sicherheitsbedenken beim Anlegen und Nutzen einer elektronischen Patientenakte

21,1%
halten Fitness- und Gesundheitsapps für gefährlich



13,1%
nutzen digitale Angebote zur medizinischen Versorgung, z. B. Online-Sprechstunden

11,5%
nutzen Fitness- und Gesundheitsapps

Digitale Vernetzung

Obgleich ihre Nutzung seit dem Vorjahr um 3,3 Prozentpunkte abgenommen hat, werden Soziale Netzwerke wie Facebook, Twitter und Co. weiterhin von mehr als der Hälfte aller Onliner genutzt (52,4 Prozent). 14,7 Prozent veröffentlichen dort zudem selbst Content wie Texte, Fotos oder Videos.

Verunsicherung nimmt weiter zu

Die Verunsicherung gegenüber Sozialen Netzwerken vergrößert sich auch in diesem Jahr: Mit 39,5 Prozent sind mehr Befragte als im Vorjahr der Meinung, dass sie gefährlich seien (+1,2 Prozentpunkte). Damit klettert das Verwenden Sozialer Netzwerke in die Top 3 der am gefährlichsten wahrgenommenen Tätigkeiten im Internet. Dies deckt sich mit den aufgetretenen Sicherheitsvorfällen: Während sich die Fälle von Identitätsdiebstahl um 3,5 Prozentpunkte auf 8,6 Prozent gestiegen sind, steigen die Fälle von Belästigungen in sozialen Netzwerken in diesem Jahr – von 6,3 Prozent im Vorjahr auf nun 9,2 Prozent.

Sicherheitsverhalten weiter stärken

Gerade angesichts ihrer hohen Popularität sollten Verbraucher*innen in Bezug auf Soziale Netzwerke weiterhin geschult und aufgeklärt werden. So passen aktuell nur 52,7 Prozent ihre Privatsphäre-Einstellungen an, obgleich 92,4 Prozent wissen, dass sie damit ihre Privatsphäre schützen können. 11,7 Prozent sind zudem immer noch der Meinung, dass ihnen Sicherheitsfragen zweitrangig sind, wenn ein digitales Angebot für sie einen hohen Mehrwert hat. Dennoch sollten digitale Aufklärungsangebote Verbraucher*innen gezielt anleiten, Sicherheitsrisiken in sozialen Netzwerken wahr- und ernst zu nehmen.

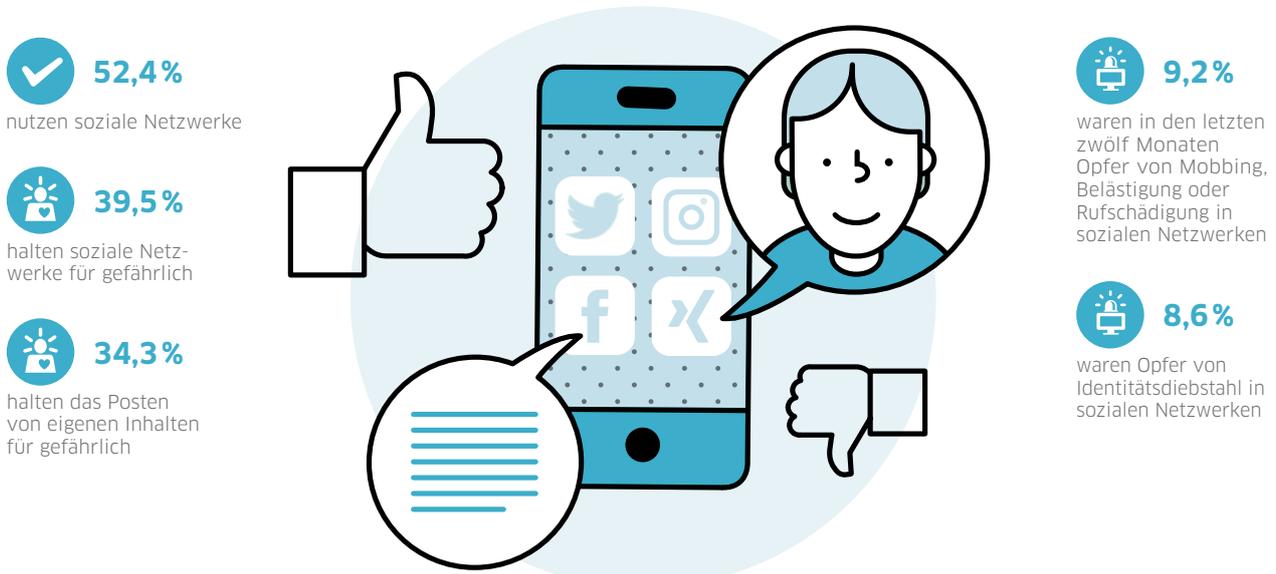
DsiN-Angebote

[sicher-im-netz.de/
digitale-vernetzung](https://sicher-im-netz.de/digitale-vernetzung)



Abb. 29

Digitale Vernetzung aus Verbrauchersicht



Das vernetzte Zuhause

Sogenannte IoT-Geräte (IoT: engl. „Internet of Things“, Internet der Dinge) und die zugehörigen Anwendungen finden zunehmende Verbreitung in deutschen Haushalten: Waren es im Jahr 2016 nur 3,6 Prozent der Befragten, die vernetzte Haustechnik einsetzen, hat sich diese Zahl 2020 bereits verdoppelt (7,0 Prozent). Ob vernetzte Haustechnik oder Unterhaltungselektronik – Verbraucher*innen sehen sich mit zahlreichen neuen Möglichkeiten aber auch Herausforderungen hinsichtlich IT-Sicherheit und Datenschutz konfrontiert.

Weniger Sicherheitsbedenken nehmen ab – trotz zunehmender Angriffe

Während die Nutzungszahlen von vernetzter Haustechnik steigen, nimmt die Verunsicherung hingegen leicht ab: 2019 empfanden noch 33,4 Prozent der Onliner Vernetzung von Haustechnik als gefährlich oder sogar als sehr gefährlich; 2020 sind es noch 32,4 Prozent.

Dennoch steigt die Zahl der Angriffe: In diesem Jahr geben 6,1 Prozent der Befragten an, dass sie einem Angriff auf ihre Haus- und Heimvernetzung ausgesetzt waren – 2,8 Prozentpunkte mehr als im Vorjahr.

Sicherheitswissen vor allem im Smarten Zuhause anwenden

Das Wissen bei Verbraucher*innen ist hinsichtlich wichtiger Grundlagen der Absicherung im Haus vorhanden – auffällig ist aber eine mangelnde Anwendung: So wissen zwar 95,8 Prozent, dass eine Firewall wichtig ist, diese wird jedoch nur von 59,5 Prozent tatsächlich eingesetzt – nochmals 9,8 Prozentpunkte weniger als im Vorjahr. Hier bedarf es neben konkreten Handlungsempfehlungen vor allem mehr Ermunterung zur Umsetzung des Sicherheitswissens, um Anwender*innen zum aktiven Selbstschutz zu motivieren.

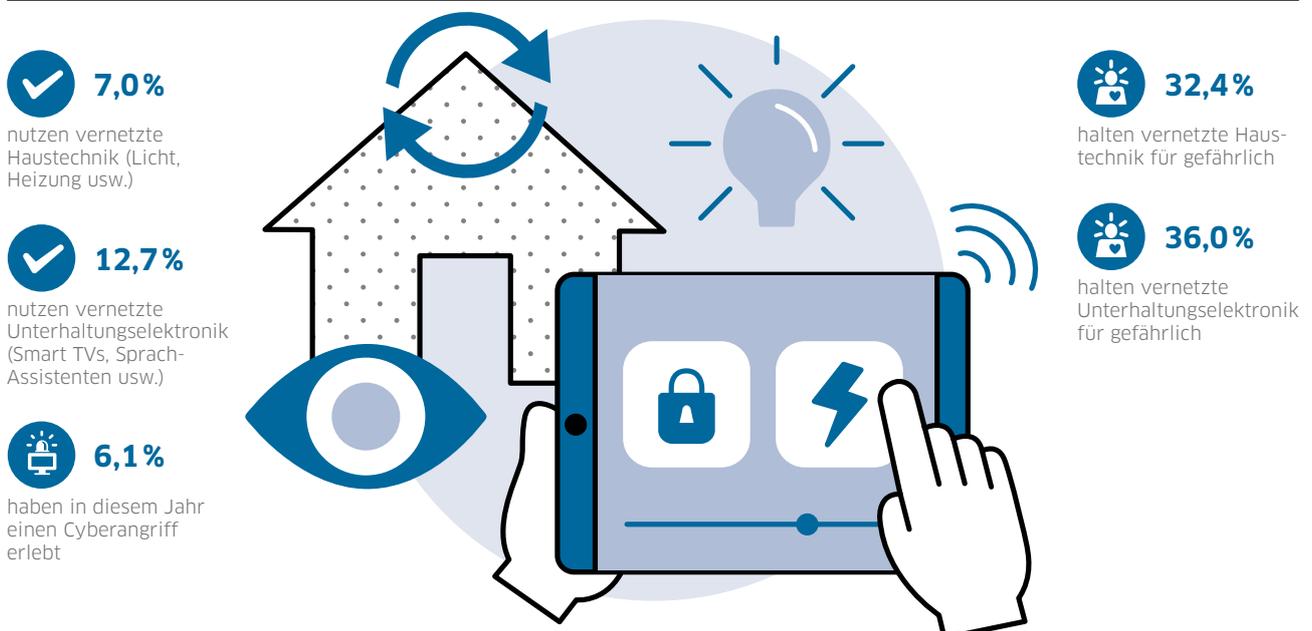
DsiN-Angebote

[sicher-im-netz.de/
vernetztes-zuhause](https://sicher-im-netz.de/vernetztes-zuhause)



Abb. 30

Das vernetzte Zuhause aus Verbrauchersicht



Einkaufen im Internet

Online-Shopping erfreut sich nach wie vor großer Beliebtheit: Nach dem Austausch von E-Mails ist es die zweithäufigste Online-Aktivität deutscher Verbraucher*innen (70,0 Prozent). Zwar ist das subjektive Verunsicherungsgefühl beim Einkaufen im Internet vergleichsweise gering (24,0 Prozent), doch hat es sich im Vergleich zum Vorjahr um 3,1 Prozentpunkte verstärkt.

Zahl der Sicherheitsvorfälle gestiegen

Im Vergleich zum Vorjahr ist der Anteil der Befragten, die Opfer eines Betrugs beim Online-Shopping wurden, um 2,4 Prozentpunkte auf 10,7 Prozent angestiegen; das Ausspähen von Zugangsdaten zu Online-Shops geben 8,3 Prozent der Befragten als Sicherheitsvorfall im letzten Jahr an (+ 1,4 Prozentpunkte). Beides scheint jedoch vergleichsweise gering, wenn man sich vor Augen hält, dass sich die Sicherheitsvorfälle bei Zahlungsvorgängen im Netz (von 5,0 auf 9,7 Prozent) sowie beim Kreditkarten-

betrug (von 4,5 auf 7,9 Prozent) im Vergleich zum Vorjahr nahezu verdoppelt haben.

Kennen vs. Nutzen

Fragt man hingegen nach den Sicherheitsmaßnahmen, so geben wie im Vorjahr 93,9 Prozent der Befragten (-1,6 Prozentpunkte) an, dass sie zwar sichere Zahlungssysteme für den Online-Einkauf kennen, jedoch nur 75,2 Prozent der Onliner solche Angebote nutzen. Gütesiegel, welche 91,5 Prozent der Verbraucher*innen bekannt sind, werden sogar nur von 57,9 Prozent berücksichtigt. Die digitale Aufklärung sollte daher Onliner vor allem dazu motivieren, ihr vorhandenes Sicherheitswissen aktiv anzuwenden.

DsiN-Angebote

[sicher-im-netz.de/
einkaufen-im-internet](https://sicher-im-netz.de/einkaufen-im-internet)



Abb. 31

Einkaufen im Internet aus Verbrauchersicht



Online-Banking

Die Nutzung von Online-Banking hat in diesem Jahr seit 2014 erstmalig wieder leicht abgenommen: 2020 sind es mit insgesamt 59,8 Prozent rund 2,4 Prozentpunkte weniger als im Vorjahr. Dafür ist das Vertrauen weiter gestiegen: Empfanden im Vorjahr noch 37,5 Prozent der befragten Internetnutzer*innen Bankgeschäfte als gefährlich bis sehr gefährlich, sind es aktuell nur noch 35,4 Prozent.

Mehr Vorfälle, weniger Schutzmaßnahmen

Zugenommen hat die Anzahl an Sicherheitsvorfällen beim Online-Banking: 9,4 Prozent der Verbraucher*innen geben an, dass ihre Zugangsdaten im letzten Jahr für Online-Banking-Anwendungen ausgespäht wurden – fast doppelt so viele wie im Vorjahr (4,8 Prozent). Dennoch setzt sich der Trend, Schutzmaßnahmen trotz besseren Wissens nicht in die Praxis umzusetzen, weiter fort. So sind verschlüsselte Verbindungen beim Online-Banking mit 91,1 Prozent fast allen Internetnutzer*innen

bekannt, doch geben nur 63,0 Prozent an, beim Online-Banking auch darauf zu achten.

Trotz neuer Sicherheitsrichtlinien Risiken verdeutlichen

Seit dem endgültigen Inkrafttreten der Zweiten europäischen Zahlungsdiensterichtlinie („PSD2“) im September 2019 sind europäische Bürger*innen dazu verpflichtet, zusätzliche Sicherheitsmaßnahmen beim Online-Banking anzuwenden. Obgleich dies zweifelsohne positive Auswirkungen auf die Sicherheitslage haben wird, sollten Onliner nach wie vor dazu angehalten werden, bekannte Schutzmaßnahmen umzusetzen, z. B. indem man ihnen die Folgen nachlässigen Handelns verdeutlicht. Hilfreich ist es, aufzuzeigen, dass der Schutz beim Online-Banking bereits durch einfache Maßnahmen wirksam erhöht werden kann.

DsiN-Angebote

[sicher-im-netz.de/
online-banking](https://sicher-im-netz.de/online-banking)



Abb. 32

Online-Banking aus Verbrauchersicht



IT-Sicherheit neu denken

Der Sicherheitsindex demonstriert anhand konkreter Zahlen, was wir in unserem eigenen Alltag erleben: Die Digitalisierung entwickelt sich nicht nur rasant weiter, sondern greift auch zunehmend in unsere persönlichen Lebensbereiche ein. Was 2016 noch als außergewöhnlich galt – zum Beispiel die vernetzte Haustechnik – gehört mittlerweile für viele Verbraucher*innen zur Standardausstattung. Dies muss nicht zwangsläufig ein Problem darstellen, erfordert jedoch zweifelsohne eine hohe Sensibilisierung für IT-Sicherheitsthemen.

Anwendung von Sicherheitswissen im Alltag – auch bei souveränen Nutzer*innen

Der generelle Trend, dass Onliner die ihnen bekannten Sicherheitsmaßnahmen nicht aktiv anwenden, zieht sich durch alle dargestellten Lebenswelten hindurch. Hier ist es in der digitalen Aufklärung wichtig, Sicherheitswissen nicht bloß als theoretische, sondern vor allem in Form von praxisorientierten Kompetenzen zu vermitteln. Dabei sollte hervorgehoben werden, dass selbst die souveränen Nutzergruppen nicht immer vor IT-Sicherheitsrisiken geschützt sind: Waren beispielsweise letztes Jahr nur 1,7 Prozent der antreibenden Nutzer*innen von dem Ausspähen ihrer Zugangsdaten beim Onlinebanking betroffen, waren es dieses Jahr bereits 11,7 Prozent.

So sollte auch Verbraucher*innen verdeutlicht werden, dass es nicht nur vor dem Hintergrund einer sich rasant entwickelnden digitalen Welt von großer Wichtigkeit ist, sich regelmäßig über aktuelle IT-Sicherheitsmaßnahmen zu informieren und diese zudem anzuwenden. Auch in ihrem Alltag, der sich zunehmend digitalisiert, haben sie einen Mehrgewinn von mehr IT-Sicherheit. Die Tatsache, dass schon kleine Maßnahmen wie das Auslesen eines E-Mail-Headers eine große Wirkung haben können, die eigenen Daten und Systeme zu schützen, kann Verbraucher*innen dazu motivieren, ihre IT-Umgebung auch im Alltag sicherer zu gestalten. Hierzu braucht es positive Beispiele und Vorbilder aus der Praxis.



Kapitel 4

**Digitale Aufklärung:
Verstehen
Befähigen
Gestalten**

Verstehen: Themen- und zielgruppengerechte Aufklärung

Die Ergebnisse des diesjährigen DsiN-Index zeigen: Digitale Aufklärungsarbeit erfordert ein umfassendes Paket an Maßnahmen, damit Menschen digitale Kompetenzen erwerben – und diese im Anschluss auch tatsächlich anwenden. Mehr denn je ist dafür ein direkter Austausch mit den jeweiligen Zielgruppen und ihren Erwartungen grundlegend. Dieser kann über vertraute Institutionen, Formate und Ansprechpartner*innen vor Ort erfolgen: Ob Freiwilligenagenturen, Volkshochschulen, Mehrgenerationenhäuser, Schulen, Seniorenbüros oder Vereine – es geht stets um den Austausch im persönlichen Umfeld und zielgruppengerechte Themen. Sie ermöglichen, Aufklärungsangebote an individuellen Bedürfnissen auszurichten und damit nachhaltiger zu verhaften.

Digitalisierung lokal denken

40 Prozent der Onliner wünschen sich mehr Informationsveranstaltungen in ihrer Nähe, und 57,8 Prozent der Befragten sind der Meinung, dass IT-Sicherheitsfragen schon in der schulischen Aus- und Weiterbildung stärker eingebunden werden müssten. Tatsächlich fördert die direkte Ansprache

und das Lernen mit digitalen Medien auch eine aktive Befassung mit digitalen Fragestellungen. Über die Einrichtung von geschützten Lernräumen werden zusätzliche Feedbackkanäle geschaffen, um auch individuelle Fragestellungen und Lernerfolge in der Aufklärungsarbeit zu berücksichtigen.

Individuelle Interessen berücksichtigen

Nahezu die Hälfte der Verbraucher*innen gibt an, dass es mehr auf sie abgestimmte Weiterbildungsangebote geben müsste (45,6 Prozent). Sie zeigen das Bedürfnis nach passgenauen Lernkanälen, um alle Verbraucher- und Lerngruppen zu erreichen. So geben zwar 71,7 Prozent der Senior*innen an, das Netz für digitale Bankgeschäfte zu verwenden, bei den Jugendlichen sind dies hingegen nur 22,0 Prozent. Letztere wiederum nutzen das Internet überdurchschnittlich gerne für Onlinespiele und dem Streamen von Medieninhalten, während dies für andere Altersgruppen kaum relevant ist. Diese Ergebnisse des DsiN-Sicherheitsindex verdeutlichen die unterschiedlichen Präferenzen von Verbraucher*innen in der digitalen Aufklärungsarbeit. Sie zeigen auf, dass sowohl die

Abb. 33

Welche Informationsquellen nutzen Sie, um sich über das Thema „Sicherheit im Internet“ zu informieren?

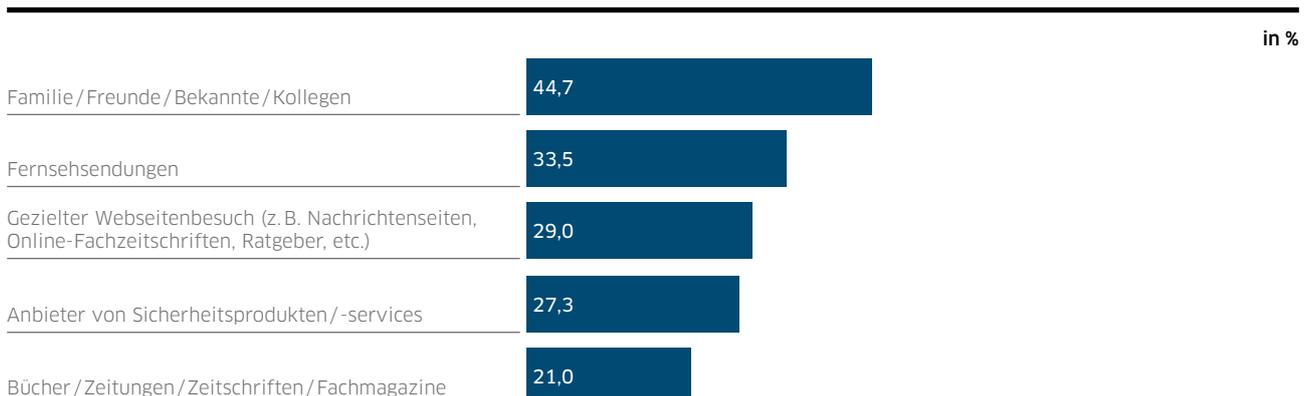
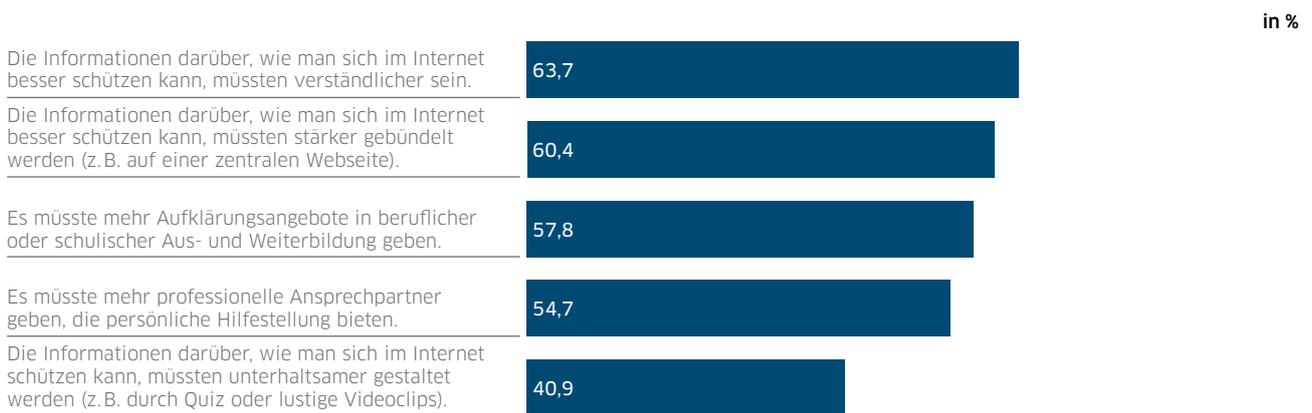


Abb. 34

Wie könnte Ihr Sicherheitswissen verbessert werden?



Lernumgebungen also auch die Vermittlungsmethoden der Aufklärung entscheidend sind.

Vielfältige Lernformate schaffen

Die Herausforderungen einer relevanten Ansprache zeigen sich auch in der Wahl des Formats für die Aufklärungsarbeit: Während Webinare und E-Learning-Angebote für Souveräne Nutzer*innen ein beliebtes Vermittlungsmedium darstellen, bevorzugen gerade Außenstehende zu Beginn noch Vor-Ort-Workshops; diese sind wiederum für Berufstätige oftmals schwer mit Beruf und Familie in Einklang zu bringen. Verzahnte Lernangebote, wie zum Beispiel eine Mischung aus Präsenzveranstaltungen, zusammenfassenden E-Learning-Angeboten sowie analogen Materialien können hier die notwendige Flexibilität bei der Ansprache sicherstellen, um unterschiedlichen Bedarfen zu entsprechen.

Handlungsempfehlungen:

- **Individuelle Fokusthemen:** Verschiedene Interessenfelder ansprechen
 - **Bewusstsein für Relevanz schaffen:** Eigene Betroffenheit verdeutlichen
 - **Vielfältige Lernkanäle bedienen:** Verschiedene Vermittlungswege ausbauen
- Ausgewählte DsiN-Angebote als Best-Practice-Beispiele, um Verbraucher individuell zu erreichen:**
- **IT-Fitness-Test:** Wissenscheck für Einsteiger
 - **Klnsights!** veranschaulicht interaktiv 13 Anwendungsszenarien für künstliche Intelligenz
 - **Mission IT-sicher:** App mit Lernquiz speziell für Auszubildende
 - **DsiN Sicherheitsbarometer (SiBa-App)** als News- und Ratgeber-App zu aktuellen Sicherheitsthemen
 - **Digitale Nachbarschaft** für Menschen im Ehrenamt, um sie über ihre Vereinstätigkeit zu erreichen
 - **DigiBitS – Digitale Bildung trifft Schule** greift Themen speziell von Lehrenden und Lernenden auf
 - **Cyberfibel:** Standardwerk für Multiplikator*innen in der digitalen Verbraucheraufklärung
- **Lokale Angebote:** Vermittlungsmöglichkeiten vor Ort nutzen

Befähigen: Aufbau von Risikobewusstsein und Eigenverantwortung

Der DsiN-Index zeigt eine erfreuliche Zunahme von IT-Sicherheitskompetenzen bei deutschen Onlinern. Zugleich wird deutlich, dass die Kompetenzen noch nicht ausreichend in der Praxis angewandt werden: Vielmehr wird hier eine wachsende Wissens-Verhaltens-Schere offenbart. Gleichzeitig stimmen 24,3 Prozent aller Nutzer*innen der Angabe zu, keinen Grund zu sehen, ihr Sicherheitsverhalten zu ändern, „solange nichts passiert“. Gelungene Aufklärungsarbeit muss daher auf die wirksame Ermunterung und Motivation bei Verbraucher*innen zielen, das erworbene Wissen in der Praxis anzuwenden.

Gesundes Risikobewusstsein schaffen

Die Befähigung zum sicheren Handeln erfordert grundsätzlich ein entsprechendes Risikobewusstsein. Dieses ist innerhalb der fünf Nutzergruppen des Sicherheitsindex jedoch unterschiedlich ausgeprägt. Während gutgläubige Nutzer*innen meinen, dass ihnen beim Surfen schon nichts passieren wird, lauern gemäß fatalistischen Onlinern überall Sicherheitsfallen, sodass sie Handeln daher für zwecklos halten. Hier gilt es, Nutzer*innen Orientierung zu bieten, um ihnen eine realistische Einschätzung von Gefahren zu ermöglichen – und sie zum Nutzen angemessener Schutzvorkehrungen anzuleiten. Die Chancen für eine erfolgreiche Motivation stehen gut, da die meisten Onliner – über alle Nutzertypen hinweg – einen bewussten Umgang mit Risiken und Chancen bereits in der Schule befürworten (68,4 Prozent). Auch Anbieter von Diensten und Programmen sehen Onliner in der Verantwortung, mehr über Risiken aufzuklären (65,9 Prozent).

Sicheres Handeln bedarf Eigenverantwortung

Die erfolgreiche Befähigung zum sicheren Handeln gründet vor allem in der Bereitschaft zur Eigenverantwortung. Dabei verorten die meisten Internetnutzer*innen in Deutschland die Verantwortung für

die Sicherheit im Netz bei sich selbst. 78,7 Prozent geben an, dass ein vorsichtigerer Umgang mit den eigenen persönlichen Daten gegen Sicherheitsvorfälle schützt. Aber auch den Gesetzgeber sehen die Verbraucher*innen in der Pflicht: So fordern 73,2 Prozent der Befragten eine strengere Verfolgung der Täter durch die Sicherheitsbehörden; 66,5 Prozent sehen die Verantwortung bei Anbietern. Grundsätzlich sollte hier das Bedürfnis aufrechterhalten werden, eigenverantwortlich und selbstbestimmt zur persönlichen IT-Sicherheit beizutragen.

Motivation über persönliche Ansprache

Gute Vorsätze: 71,7 Prozent aller Onliner geben an, ihr Sicherheitswissen öfter in die Tat umsetzen zu wollen. Wie also kommt die große Wissens-Verhaltens-Schere zustande? Eine Hürde könnte sein, dass wirksame Sicherheitsmaßnahmen als kompliziert empfunden werden – immerhin geben 69,5 Prozent an, dass einfachere Sicherheitseinstellungen bei Programmen und Geräten ihre Sicherheit beim Surfen erhöhen würden. Dabei reichen oft schon einfache Maßnahmen wie das Auslesen eines E-Mail-Headers aus, um Sicherheitsfallen zu entgehen. Wichtig ist hier zudem vor allem die regelmäßige Integration in den Alltag und das vertraute Umfeld von Verbraucher*innen: 52,5 Prozent sehen die Vorbildfunktion von Freunden und Familie als besonders motivierend an und 52,4 Prozent wünschen sich eine konkrete Ansprache durch ihr privates Umfeld.

Handlungsempfehlungen

- Risikoeinschätzungskompetenz in Abgrenzung zu Unbedarftheit und Verunsicherung fördern
- Umsetzungskompetenz durch Alltagsroutine trainieren
- Basiswissen und komplexe Kenntnisse
Je nach Bedarf zielgruppengerecht vermitteln

Ausgewählte DsiN-Angebote als Best-Practice-Beispiele, um Nutzer bedarfsgerecht anzuleiten und zu motivieren:

- **Digitaler Engel** als Aufklärungsmaßnahme, die Verbraucher zu ihren Themen vor Ort aufsucht
- **Digital-Kompass** mit Digitalen Stammtischen und Infomobilen für Senioren
- **Digitale Nachbarschaft** mit Multiplikatoren im Ehrenamt und Infomobilen für Vereine
- **DigiBits** - Digitale Bildung trifft Schule, um Lehrkräfte zur sicheren Mediennutzung im Schulalltag zu befähigen und zu Multiplikatoren weiterzubilden
- **Bottom-Up:** Berufsschüler für IT-Sicherheit, um Berufsschullehrkräfte und Auszubildende zu IT-Sicherheitsthemen zu schulen
- **myDigitalWorld Jugendwettbewerb**, um junge Menschen zu motivieren, sich mit dem Thema Sicherheit im Netz auseinanderzusetzen
- **Goldener Internetpreis** für Senioren, zur Anerkennung von Engagement im Netz

Abb. 35

Wissen-Verhaltenslücke im Jahresverlauf

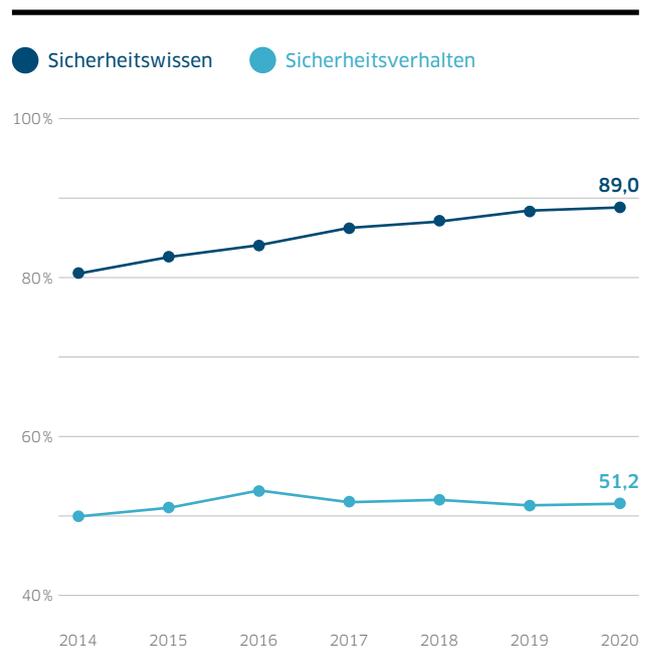
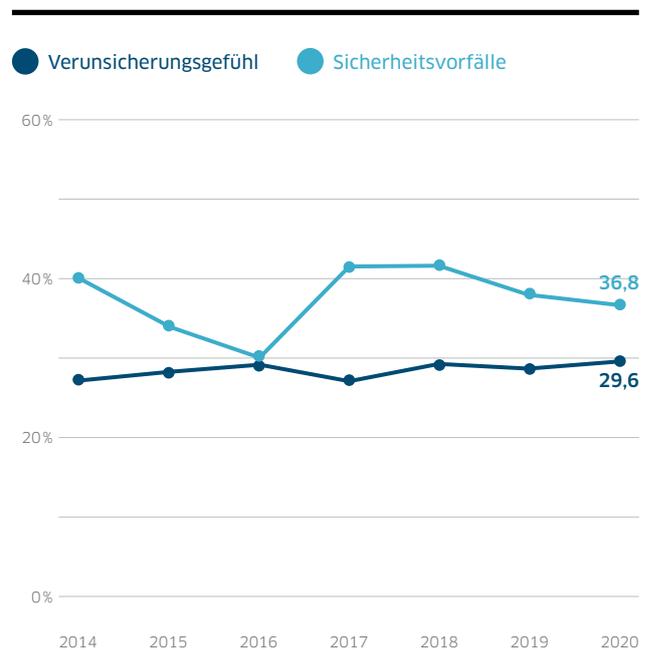


Abb. 36

Verunsicherungsgefühl vs. Sicherheitsvorfälle im Jahresverlauf



Gestalten: Förderung nachhaltiger Strukturen und offener Dialoge

Digitale Sicherheit geht alle an: Der DsiN-Sicherheitsindex verdeutlicht, dass mit wachsendem Verständnis und Handlungsfähigkeit ein Fokus auf die tatsächliche Gestaltungsbereitschaft erforderlich ist. Ein wachsendes Sicherheitsgefälle zwischen Nutzertypen lässt sich nur beheben, wenn offene Dialoge zum gegenseitigen Austausch stattfinden und sich Verbraucher*innen zudem in der Pflicht sehen, diese selbst aktiv mitzugestalten. Dabei sollte digitale Aufklärung als dynamischer Prozess gestaltet werden, in dem Strukturen und Verhaltensmuster aufgebaut und bei Bedarf angepasst werden.

Nachhaltige Strukturen vor Ort schaffen

Eine digitale Aufklärung, die zum selbstbestimmten und sicheren Gestalten motiviert, muss Verbraucher*innen längerfristig erreichen. Das Internet bietet eine Vielzahl von Aufklärungsinhalten und -angeboten, bei denen gerade außenstehende

Nutzergruppen womöglich schnell die Übersicht verlieren. So scheint es wenig verwunderlich, dass über die Hälfte aller Online-Aufklärungsangebote außerhalb des Internets wertschätzen (55,8 Prozent) – bei den außenstehenden Nutzer*innen im Jahr 2020 mit einem auffälligen Zuwachs um 19,5 Prozentpunkte. Es ist also erforderlich, Menschen bei der Orientierung und Umsetzung von Aufklärungsangeboten vor Ort zu begleiten, um einen nachhaltigen positiven Effekt für ihr Sicherheitsverhalten zu erreichen.

Dialoge fördern und fordern

Digitale Aufklärung ist wirksam, wenn sie Nutzer*innen motiviert, sicher und selbstbestimmt im Netz zu agieren. Lernangebote sollten daher so ausgelegt sein, dass sie langfristig zum autonomen Handeln ermuntern und Selbstvertrauen schaffen. Es geht darum, erworbenes Wissen für eigenständiges Lernen zu nutzen und weitergeben zu können. Dies fördert

Abb. 37

Wie Risikobewusstsein stärken?



Abb. 38

Was würde Sie zu einem sichereren Umgang mit Ihren Daten im Internet motivieren?

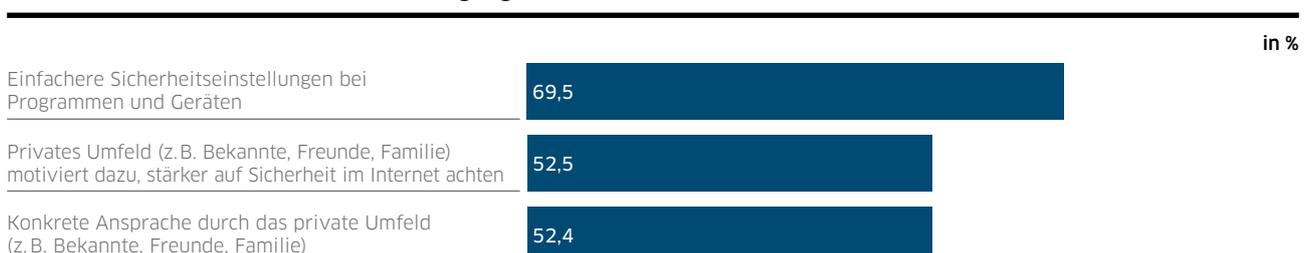
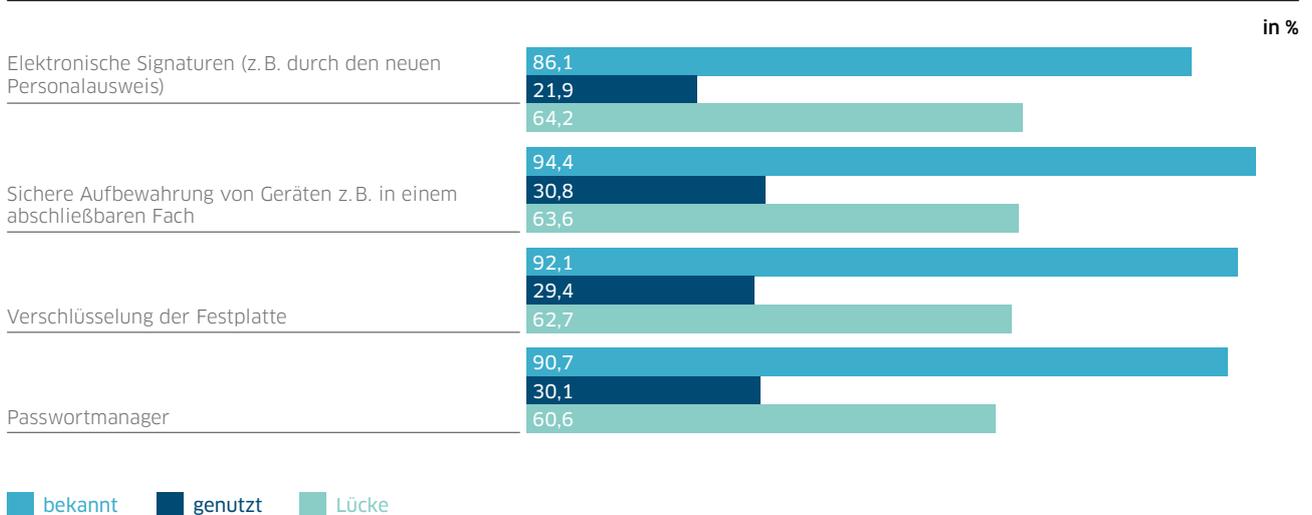


Abb. 39

Die größten Diskrepanzen zwischen Kenntnis und Nutzung



den Dialog zwischen Nutzergruppen: Wenn souveräne Nutzer ihre Kompetenzen als Wissensvermittler*innen an andere Nutzergruppen weitergeben, fördert dies gegenseitiges Verständnis sowie eine gesamtgesellschaftliche Teilhabe. Das Schaffen von Austausch- und Multiplikator*innenplattformen ist somit eine effektive Maßnahme, um diese Wirkung nachhaltig zu fördern.

Verantwortung - für sich selbst und andere

Auch im Jahr 2020 sind Familie, Freundeskreis, Bekannte und Kolleg*innen die bevorzugte Quelle, um sich zum Thema Sicherheit im Internet zu informieren (44,7 Prozent) und mehr als die Hälfte aller Verbraucher*innen wünscht sich eine konkrete Ansprache durch ihr privates Umfeld (52,4 Prozent). So kommt Vorbildern in der eigenen Umgebung eine besondere Rolle zu: Ob im informellen oder auch im didaktischen Kontext als Multiplikator*in: geteilte Verantwortung muss als Schlüsselaufgabe der Digitalisierung verstanden werden. Die Übernahme von digitaler Verantwortung für sich und andere ist damit

eine Grundlage, um Digitalisierung erfolgreich in der Gesellschaft zu verankern und alle zu erreichen.

Handlungsempfehlungen

- **Mitbestimmung fördern:** Verbraucher an Aufklärung teilhaben lassen
- **Sinnvolle Arbeitsteilung:** Durch Vernetzung und Kooperation
- **Entwicklung von Aufklärungsstandards:** Inhalte festlegen und Qualität steigern
- **Einbindung von Multiplikator*innen:** Souveräne Nutzer als Vorbilder

DsiN-Angebote

- **Cyberfibel** für digitale Aufklärung, um Standards der Verbraucherbildung zu setzen
- **Aktionsbund Digitale Sicherheit** als Materialsammlung zu Aufklärungsangeboten
- **DigiBitS – Digitale Bildung trifft Schule** mit über 300 gebündelten Angeboten im Online-Pool
- **Digitaler Engel:** der sich regional für die digitale Aufklärung Älterer einsetzt

Drei-Punkte-Plan für wirksame Aufklärung

Der DsiN-Sicherheitsindex zeigt: Die Sicherheitskompetenzen steigen, die Bereitschaft zur Umsetzung kann jedoch nicht Schritt halten. Es geht nun darum, Onliner zu einem sicheren Verhalten zu ermuntern, um die Wissens-Verhaltens-Schere zu verkleinern. Zugleich verzeichnet der Index ein wachsendes Sicherheitsgefälle zwischen Verbrauchergruppen: Entscheidend ist es daher, niemanden abzuhängen und wirklich allen die Chance auf eine sichere und selbstbestimmte digitale Welt zu ermöglichen. Dies erfordert eine koordinierte Vorgehensweise der Aufklärungsarbeit in drei Stufen:

1.

Individuelle Schutzbedarfe verstehen

Die Vielfalt der digitalen Möglichkeiten wird von Verbraucher*innen auf unterschiedliche Weise und mit unterschiedlichen Digitalkompetenzen genutzt. Daraus folgen individuelle Risikodispositionen und Anforderungen an IT-Sicherheitsvorkehrungen, deren Verständnis für eine wirksame Aufklärungsarbeit grundlegend ist. So schrecken außenstehende Nutzer*innen vor komplexeren Schutzvorkehrungen zurück, während einfache Standardvorkehrungen anderen bereits bekannt sind und somit oftmals wenig Wirkung erzielen. Auch unterscheiden sich Verbrauchertypen nach ihrer Bereitschaft, Schutzvorkehrungen anzuwenden, was von einer wirksamen Vermittlungsarbeit berücksichtigt werden sollte.

2.

Verhaltensorientierte Schutzstandards schaffen

Um einen sinnvollen Basisschutz für alle Onliner ermöglichen, ist ein breites Spektrum an Schutzmaßnahmen erforderlich, das den unterschiedlichen Schutzbedarfen gerecht wird. Dies setzt zugleich

ein Verständnis über die Ziele und Maßnahmen voraus, welche Kompetenzen ein „risikogerechter“ Basisschutz für Verbraucher*innen sinnvollerweise umfassen soll. Diese Kompetenzstandards wurden bereits 2018 angemahnt und sollen ab 2020 im Rahmen der Cyberfibel für Wissensvermittler*innen mit dem BSI veröffentlicht werden. Damit werden erstmals übergreifende Standards der Verbraucheraufklärung geschaffen. Auf ihrer Grundlage können bestehende Hilfsangebote für Verbraucher*innen kuratiert und bedarfsgerecht zugänglich gemacht werden.

3.

Professionelle Vermittlungsarbeit gewährleisten

Das Herzstück einer wirksamen Aufklärungsarbeit bleibt die nachhaltige Vermittlung der digitalen Kompetenzen durch eine zielgruppengerechte Ansprache. Sie setzen neben der fachlichen Expertise transparente Unterstützerstrukturen voraus, die wirksame Lernräume ermöglichen. Um Menschen in ihren individuellen Lernpräferenzen zu erreichen, können sie digital oder analog gestaltet sein – oder in einer hybriden Form. In Kern kommt es auf dauerhafte Befähigungsstrukturen an, die für bestehende Netzwerke der Zivilgesellschaft anschlussfähig sind und Wissensvermittler*innen aus dem betroffenen Umfeld einbindet.



Über Deutschland sicher im Netz e.V.

Deutschland sicher im Netz e.V. (DsiN) engagiert sich für Schutz, Sicherheit und Vertrauen in der digitalen Welt bei Verbraucher*innen und im Mittelstand. Getragen von Unternehmen, Verbänden und gesellschaftlichen Organisationen, entwickelt und betreibt DsiN bundesweit Projekte für konkrete Hilfestellungen im privaten und beruflichen Alltag.

Impressum

DsiN-Sicherheitsindex 2020

Studie von Deutschland sicher im Netz e.V. zur digitalen Sicherheitslage von Verbraucher*innen in Deutschland
1. Auflage

Verantwortlich: Dr. Michael Littger

Redaktion: Katharina Nagler (Leitung), Denis Schröder, Anne Schilling, Tobias Weber (KANTAR), Michael Weinzierl (KANTAR)

Studienpartner: KANTAR GmbH

Gestaltung und Infografiken: KRAUT&KONFETTI

Stand: Juni 2020

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: fizkes/shutterstock

Grußwort: Thomas Köhler/photothek

Vorwort: Thomas Rafalzyk/DsiN

Kap. 1: Dragon Images/shutterstock

Kap. 2: SFIO CRACHO/shutterstock

Kap. 3: Perfect Wave/shutterstock

Kap. 4: adriaticfoto/shutterstock

