



DsiNIndex 2014

**Digitale Sicherheitslage
der Verbraucher in Deutschland**

Schirmherrschaft:





Ulrich Kelber

Geleitwort

Das Internet hat für uns alle erhebliche Erleichterungen im Alltag gebracht: die schnelle Informationsrecherche, das Einkaufen nach Feierabend, das Auffinden von Bildern oder Urlaubsorten. Wir pflegen soziale Kontakte über das Internet und beteiligen uns an öffentlichen Debatten. Und das ist wohl erst der Anfang eines enormen Umbruchs – ob man es nun als „digitaler Wandel“ oder gar als „digitale Revolution“ bezeichnet.

Die Entwicklung bietet Chancen und Risiken für die Verbraucherinnen und Verbraucher und für die ganze Gesellschaft. Wir wissen nicht, welche technischen und organisatorischen Umwälzungen durch das Internet noch auf uns zukommen werden. Eines ist aber nach den Debatten über Abhöraffaires und Missbrauch von Daten gewiss: Verbraucherinnen und Verbraucher erwarten ein zuverlässiges, sicheres Internet – sowie Möglichkeiten, sich selbst zu schützen. Und das durch einfache klare Handhabung der Technik. Sicherheit und Schutz der Daten sind zentrale Querschnittsthemen der Digitalisierung – so hat es auch die Bundesregierung in ihrer Digitalen Agenda beschlossen.

Wie ist es aber um die Sicherheit der Verbraucher im Netz bestellt? Der DsiN-Index hat in einer repräsentativen Umfrage Menschen nach ihren Erfahrungen im Internet gefragt und die Ergebnisse in Kennzahlen zusammengefasst. Damit wird die Sicherheitslage im Netz deutlicher – und vergleichbar. Indem der Index jährlich erhoben wird, sind Entwicklungen über einen längeren Zeitraum erkennbar. Sie ermöglichen auch einen Vergleich zwischen den unterschiedlichen Nutzergruppen im Internet. Denn auch das ist richtig: Es gibt nicht „den“ Internetnutzer – die Verhaltensweisen von gelegentlichen Onlinern und Intensivnutzern sind zu unterschiedlich.

Die Studie zeigt: Es gibt noch viel zu tun. Nahezu ein Fünftel der Befragten gab an, dass ihr Computer von Viren befallen wurde. Die Untersuchung hat zu Tage gefördert, dass zuweilen Unwissen über Risiken und Schutzmöglichkeiten besteht. Sie zeigt auch, dass die „außenstehenden Nutzer“ – gerade auch ältere Onliner – oft noch zu wenig über Schutzmaßnahmen im Netz wissen.

Hier setzt die Arbeit von DsiN an, aber auch die des Bundesministeriums der Justiz und für Verbraucherschutz. Wir unterstützen zahlreiche Projekte zur Förderung der Medienkompetenz der Internetnutzer, gerade was besondere Nutzergruppen wie Kinder, Jugendliche und die ältere Generation betrifft.

Der DsiN-Index kann uns helfen, besser zu erkennen, wo wir noch aktiv werden müssen.

Ulrich Kelber

Parlamentarischer Staatssekretär beim
Bundesminister der Justiz und für Verbraucherschutz



Dr. Christian P. Illek



Dr. Michael Littger

Digitale Aufklärung 2.0 – Sicherheitsgefälle abbauen

Mit dem DsiN-Index zur digitalen Sicherheitslage der Verbraucher gehen wir einen neuen Weg: Gemessen werden Bedrohungslage und Schutzniveau der Internetnutzer in Deutschland, um daraus zielgenaue Aufklärungsmaßnahmen abzuleiten. Die Dimensionen von Sicherheit im Internet fasst der DsiN-Index dabei erstmals in einer Kennzahl zusammen. Durch eine jährliche Erhebung werden Status Quo sowie Entwicklungen der digitalen Sicherheit sichtbar und vergleichbar.

Die erfreuliche Botschaft: Die Bekanntheit von IT-Schutzmaßnahmen ist bei Verbrauchern überraschend gut ausgeprägt. Zugleich besteht aber ein erhebliches Sicherheitsgefälle im Netz zwischen verschiedenen Nutzergruppen: Auffällig ist, dass gerade bei älteren und jüngeren Bevölkerungsanteilen die Sicherheitslage abfällt. Ein weiteres Ungleichgewicht: Schutzmaßnahmen werden trotz Kenntnissen nicht angewendet.

Der DsiN-Index offenbart, dass Aufklärungsangebote stärker auf die Bedürfnisse der jeweiligen Nutzergruppen zugeschnitten werden müssen, um die individuelle Sicherheitslage zu verbessern. Dazu liefert der Index wichtige Impulse – für die Arbeit von DsiN und zur Verbesserung der IT-Sicherheit in Deutschland.

Denn klar ist: Die Vorteile der Digitalisierung für die Gesellschaft können sich erst entfalten, wenn alle Nutzer souverän im Netz sind. Wir verstehen Aufklärung 2.0 daher auch als Verantwortung aller Stakeholder in der digitalen Gesellschaft. Mit DsiN stehen wir dafür ein, das Engagement für eine unabhängige Aufklärung zu bündeln und im Dialog mit Politik, Wirtschaft und Wissenschaft wirksam zu verstärken.

Wir freuen uns, Ihnen mit unserem Studienpartner TNS Infratest den ersten DsiN-Index zu präsentieren und laden Sie ein zum gemeinsamen Dialog für mehr IT-Sicherheit.

Wir wünschen eine aufschlussreiche Lektüre!

Dr. Christian P. Illek
Vorstandsvorsitzender
Deutschland sicher im Netz e. V.

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

Inhalt

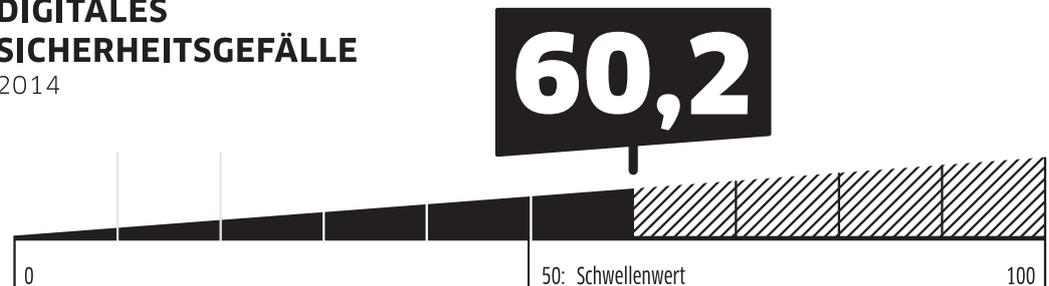
Geleitwort	3
Digitale Aufklärung 2.0 – Sicherheitsgefälle abbauen	4
Inhaltsverzeichnis	5
Executive Summary	6
Studiendesign	8
KAPITEL 1: DsiN-Index: 60,2 Punkte	9
Indexwerte nach Bedrohungs- und Schutzlage	10
Die vier DsiN-Sicherheitsfaktoren	11
KAPITEL 2: Sicherheitsgefälle in Deutschland	13
Sicherheitslage nach Verbrauchertypen	14
1. Fatalistische Nutzer (44,2 Punkte)	16
2. Außenstehende Nutzer (45,8 Punkte)	18
3. Gutgläubige Nutzer (58,1 Punkte)	20
4. Souveräne Nutzer (72,0 Punkte)	22
Exkurs: Index im Bundesländervergleich	24
KAPITEL 3: Themenfokus: Digitale Lebenswelten	25
E-Mail und Social Media	26
Shopping online	27
Digitale Bankschalter	28
KAPITEL 4: Handlungsfelder Digitale Aufklärung 2.0	29
Sicherheitswissen praktikabel vermitteln	30
Umsetzungsbereitschaft und -kompetenz stärken	32
Sensibilisieren und Vertrauen aufbauen	34
Dialog mit Stakeholdern vertiefen	35
Fahrplan zur Digitalen Aufklärung 2.0	36
DsiN-Index – Mastergrafik	37
Glossar	38
Über Deutschland sicher im Netz e.V.	39
Impressum	40

Digitales Sicherheitsgefälle in Deutschland

Zentrales Ergebnis des DsiN-Index 2014 ist das Vorliegen eines digitalen Sicherheitsgefälles in Deutschland. Dabei zeigt der DsiN-Indexwert von 60,2 Punkten zunächst, dass die durchschnittliche Sicherheitslage aller Verbraucher in Deutschland etwa zehn Punkte über dem Schwellenwert von 50 Punkten liegt, unterhalb dessen die Sicherheitsbalance zwischen Bedrohungslage und Schutzniveau zu kippen droht. Um einen Rückgang des Gesamtwerts zu vermeiden, sollte daher schon insgesamt ein positiver Trend angestoßen werden.

Ein Sicherheitsgefälle ergibt sich auch im Umgang der Verbraucher mit den vier Sicherheitsfaktoren, die dem DsiN-Index zu Grunde liegen: So übersteigt der Wert registrierter Sicherheitsvorfälle bei Verbrauchern mit 40,1 Punkten deutlich das Gefährdungsempfinden (27,2 Punkte), vor allem aber liegt der Bekanntheitswert von Sicherheitsmaßnahmen mit 80,6 Punkten deutlich über der tatsächlichen Nutzung (49,6 Punkte). Dieses Gefälle zwischen Wissen und Verhalten zieht sich – in unterschiedlichem Maße – durch alle Benutzer-

DIGITALES SICHERHEITSGEFÄLLE 2014



Ein Blick hinter den Indexwert von 60,2 Punkten offenbart ein erhebliches Gefälle der Sicherheitslage zwischen den einzelnen Nutzergruppen in Deutschland. Besonders betroffen sind die Gruppe der *fatalistischen Nutzer* mit einem Indexwert von nur 44,2 Punkten sowie die Gruppe der *außenstehenden Nutzer* mit 45,8 Punkten. Auch die Gruppe der *gutgläubigen Nutzer* liegt mit 58,1 Punkten noch erkennbar unter dem Durchschnitt. Nahezu entkoppelt von der Mehrheit der Deutschen genießt die Gruppe *souveräner Nutzer* eine gute Sicherheitslage mit 72,0 Punkten – fast 12 Punkte über dem Bundesdurchschnitt.

gruppen und beeinflusst nachhaltig die digitale Sicherheitslage. Ein eigener Studienfokus beleuchtet die Auswirkungen auf E-Mail, Social Media, Shopping und Banking.

Digitale Aufklärung 2.0 für mehr Sicherheit

Für die Arbeit von Deutschland sicher im Netz untermauern die Ergebnisse den Bedarf nach einer neuen Aufklärungsarbeit, die die spezifischen Bedürfnisse der Nutzergruppen stärker berücksichtigt. Denn die Verhaltensweisen und konkreten Kenntnisse der Verbraucher im Netz – auch das zeigt die Studie – haben

maßgeblichen Einfluss auf die digitale Sicherheitslage. Folgende Nutzergruppen stehen im Fokus:

- **Fatalistische Nutzer** mit sehr häufigen Sicherheitsvorfällen, hohem Gefährdungsempfinden, jedoch kaum Schutzvorkehrungen (16 Prozent der Onliner).
- **Außenstehende Nutzer** mit geringen Kenntnissen und geringer Internetaffinität sowie kaum wirksamen Schutzvorkehrungen (10 Prozent der Onliner).
- **Gutgläubige Nutzer** ohne Gefährdungsempfinden und seltenem Einsatz von Schutzmaßnahmen, trotz guter Bekanntheit (35 Prozent der Onliner).
- **Souveräne Nutzer** mit hoher Nutzung von Schutzmaßnahmen, größerer Risikoexposition, aber durchschnittlich häufigen Sicherheitsvorfällen (40 Prozent der Onliner).

Für eine digitale Aufklärungsarbeit 2.0 fasst die Studie Handlungsempfehlungen spezifisch zusammen. Beim gutgläubigen Nutzer steht Sensibilisierung im Vordergrund, beim fatalistischen Nutzer die realen Wirkungen von Schutzvorkehrungen. Die außenstehenden Nutzer müssen mit Grundwissen und Umsetzungskompetenzen stärker vertraut gemacht werden. Souveräne Nutzer hingegen sollten auf dem aktuellen Stand gehalten werden. Aus diesem „Aufklärungsmix“ für die vier Nutzergruppen zeichnen sich übergreifende Handlungsfelder ab, die für einen Fahrplan zur Digitalen Aufklärung 2.0 von besonderer Relevanz sind, insbesondere

- **Sensibilisieren und Vertrauen aufbauen**, indem Risikoeinschätzung im Netz verbessert und Schutzmaßnahmen durch

breit angelegte Aufklärungskampagnen vermittelt werden

- **Sicherheitswissen praktikabel vermitteln** durch gestuften Ansatz mit Basiswissen in die Fläche und der bedarfsweisen Vermittlung komplexerer Schutzmechanismen.
- **Umsetzungsbereitschaft und -kompetenz stärken**, um die tatsächliche Anwendung von Schutzwissen zu stärken.
- **Zusammenarbeit mit Politik, Wissenschaft, Gesellschaft vertiefen** für höhere Wirksamkeit der Aufklärungsmaßnahmen im Verbund mit mehr Initiativen der Wirtschaft.

Schon heute bietet die Arbeit von DsiN Aufklärungsangebote, die in der Studie speziellen Bedürfnissen der Verbrauchergruppen zugeordnet werden. Darüber hinaus möchte DsiN seine Arbeit künftig mit neuen Mitgliedern verstärken, die sich für eine Digitale Aufklärung 2.0 engagieren in Zusammenarbeit mit Politik, Wissenschaft und anderen Akteuren der digitalen Gesellschaft. In einer jährlichen Neuauflage wird der DsiN-Index dafür über Status und Entwicklung der digitalen Sicherheitslage informieren.

Stakeholder der digitalen Gesellschaft aus Politik und Wissenschaft für wirksame Aufklärungsarbeit einbinden

**Aufklärung 2.0
zielt auf konkrete
Bedürfnisse
der Verbraucher.**

DsiN-Index gewichtet Bedrohungslage und Schutzniveau

Der Index von Deutschland sicher im Netz errechnet die digitale Sicherheitslage der Verbraucher in einer Kennzahl, dem DsiN-Index. Durch eine jährliche Erhebung des Indexwertes wird die Sicherheitslage der Verbraucher über einen längeren Zeitraum vergleichbar. Zusätzlich schafft der Indexwert eine direkte Vergleichbarkeit der Sicherheitslage zwischen unterschiedlichen Nutzergruppen. Grundlage des DsiN-Index ist eine repräsentative Umfrage von TNS Infratest bei 1005 Internetnutzern in Deutschland.

Der DsiN-Sicherheitsindex errechnet sich aus einem Gesamtwert der Bedrohungslage von Verbrauchern einerseits und ihrem digitalen Schutzniveau andererseits (Abb. 1). Um die Bedrohungslage zu erfassen, wurden über hundert Indikatoren mit einem Schwerpunkt auf konkreten Anwendungen und



Digitale Sicherheitslage wird transparent und vergleichbar – in einer Kennzahl.

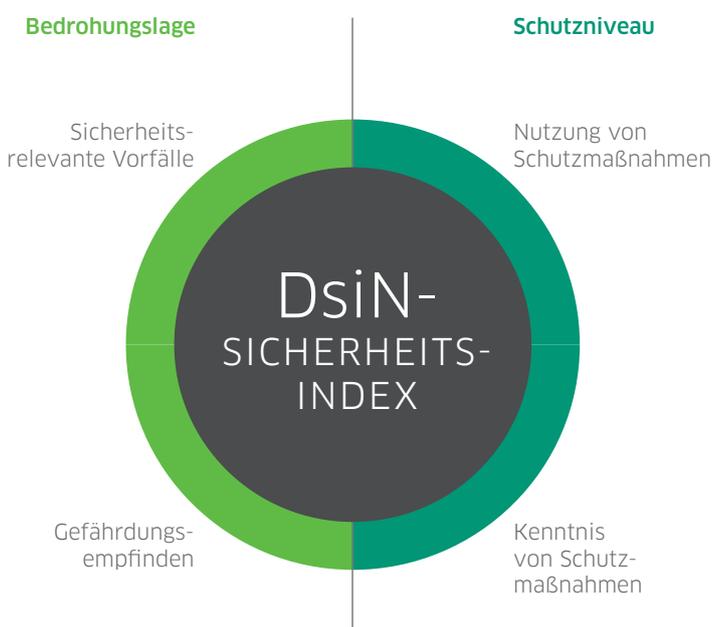
Technologien abgefragt. Für die Ermittlung des Schutzniveaus der Internetnutzer wurden die Onliner zur Kenntnis von Schutzmaßnahmen befragt sowie auch, welche der bekannten Schutzmaßnahmen tatsächlich angewandt werden.

Neben dem Erkenntniswert des DsiN-Index ist die praktische Verwertung der Ergebnisse für Aufklärung und Unterstützung der Verbraucher ein zentrales Ziel. Dazu sieht der Index eine Segmentierung der Onliner nach Nutzereigenschaften vor, die es erlaubt,



Vier Faktoren als Grundlage des DsiN-Index

Abb. 1, DsiN-Index: Bedrohungslage und Schutzniveau



konkrete Sicherheitsschwachstellen und Bedürfnisse für spezifische Zielgruppen zu erkennen. Dadurch können Maßnahmen für eine zielgenaue Aufklärungsarbeit abgeleitet werden.



Kapitel 1

**DsiN-Index:
60,2 Punkte**

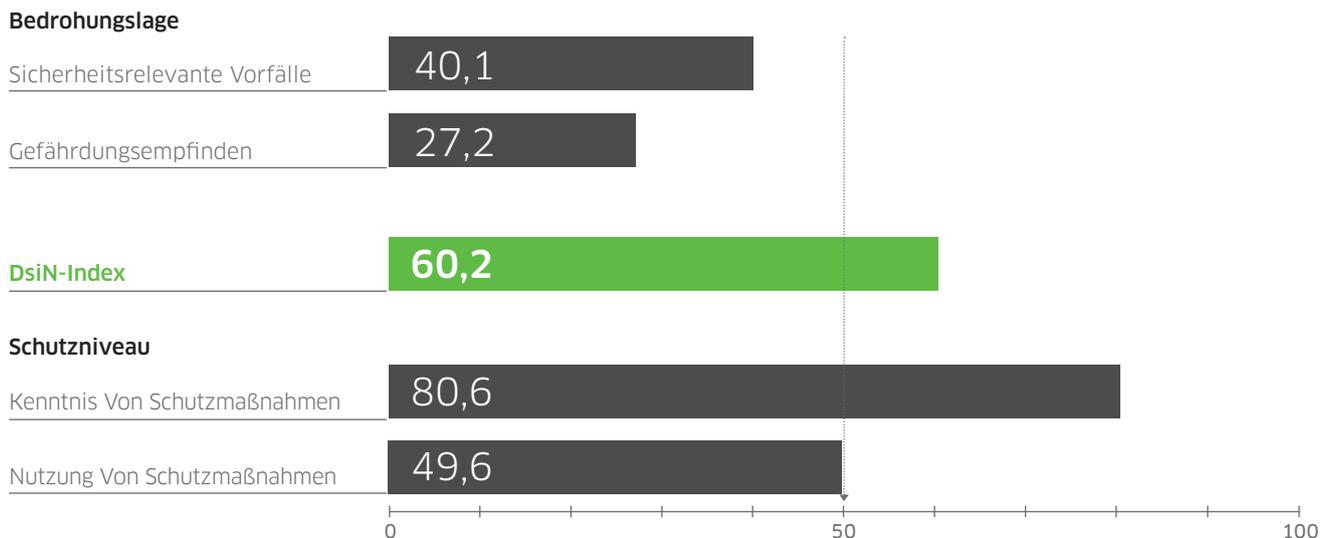


Abb. 2, DsiN-Index 2014 (Punktwerte)

Indexwerte nach Bedrohungs- und Schutzlage

Der Indexwert von 60,2 Punkten liegt bei seiner erstmaligen Berechnung gut 10 Punkte über dem Schwellenwert von 50 Punkten. Unterhalb dieses Schwellenwertes überwiegt die Bedrohungslage das Schutzniveau, sodass ein „Kippen“ der Sicherheitslage drohen würde. Der Wert von 60,2 Punkten konkretisiert sich dabei wesentlich durch die Betrachtung der zu Grunde liegenden Nutzertypen, zwischen denen ein Gefälle der Sicherheitslage deutlich wird, dazu siehe Kapitel 2.

Um eine Verschlechterung der aktuellen Sicherheitslage von 60,2 Punkten zu vermeiden, sollte insgesamt ein positiver Sicherheitstrend angestoßen werden. Dafür müssen die Sicherheitsfaktoren der vier Index-Säulen einbezogen werden (Abb. 2): Hier zeigt sich eine deutliche Diskrepanz von 13 Punkten zwischen Sicherheitsvorfällen und Gefährdungsempfinden (Bedrohungslage) auf der einen Seite sowie zwischen Bekanntheit und Nutzung der Schutzmaßnahmen (Schutzlage) von 31 Punkten auf der anderen.

- **Bedrohungslage** Die Nutzer fühlen sich trotz konkret erlebter Sicherheitsvorfälle (40,1 Punkte) meist relativ sicher im Netz (27,1 Punkte). Dazu trägt wahrscheinlich

bei, dass zahlreiche Sicherheitsvorfälle wie zum Beispiel das Empfangen von Spam-Mails als nicht gravierend eingeschätzt werden.

- **Schutzniveau** Schutzmaßnahmen sind mit 80,6 Punkten in der Regel sehr gut bekannt. Allerdings variieren die Werte je nach Themengebiet und Nutzergruppe deutlich. Vom Wissen um Schutzmaßnahmen weicht die tatsächliche Nutzung (49,6 Punkte) teilweise erheblich ab.

Anknüpfungspunkte für eine Digitale Aufklärung 2.0

Komplementär zu den Befragungen zu den vier Sicherheitsfaktoren ergeben sich vier Themenfelder, über die die Sicherheitslage angehoben werden kann; dazu ausführlich in Kapitel 4:

- **Sicherheitswissen praktikabel vermitteln** Spezifische Wissenslücken schließen
- **Umsetzungsbereitschaft und -kompetenz stärken** Diskrepanz zwischen Wissen und Verhalten im Netz reduzieren
- **Sensibilisieren und Vertrauen aufbauen** Über Risiken im Netz sachlich und fundiert aufklären
- **Dialog verstärken:** Aufklärung 2.0 im Dialog mit Politik, Wissenschaft und Gesellschaft vorantreiben.

60,2

DsiN-Indexwert 2014

DsiN-Sicherheitsfaktoren

1. Sicherheitsrelevante Vorfälle

An erster Stelle der selbst registrierten Vorfälle stehen Viren und Malware, gefolgt vom Versenden unerwünschter E-Mails im eigenen Namen. Aber auch konkrete Erfahrungen mit Betrug im Bereich Buchungen oder Shopping liegen vorn. *Ausführlich S. 35.*

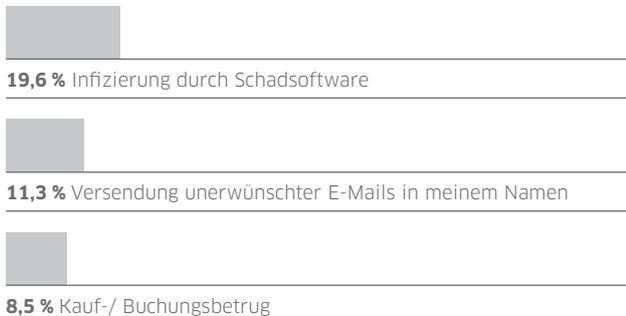


Abb. 3a TOP 3 der Sicherheitsvorfälle

2. Gefährdungsempfinden

Unsicherheit im Netz empfinden knapp 60 Prozent der Nutzer beim Öffnen von Anhängen in E-Mails. An zweiter Stelle steht das Teilen von vertraulichen Inhalten über das Internet, z.B. mit Behörden, Banken oder Versicherungen. An dritter Stelle folgt das Gefährdungsgefühl im Umgang mit Banking. *Ausführlich S. 34.*

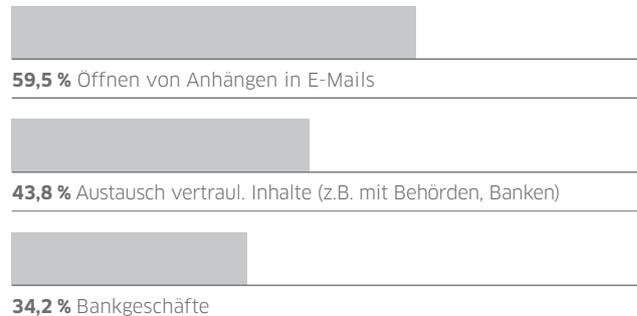


Abb. 3b TOP 3 des Gefährdungsempfindens

3. Bekanntheit von Schutzmaßnahmen

Kenntnisse über Schutzmaßnahmen bejahen fast 99 Prozent bei der Passwortstärke, gleichauf mit Passwortwechsel. Das Einrichten von Benutzerprofilen liegt deutlich dahinter an zweiter Stelle mit 92 Prozent gefolgt von der Verwendung von Antivirenprogrammen (91 Prozent). *Ausführlich S. 30.*

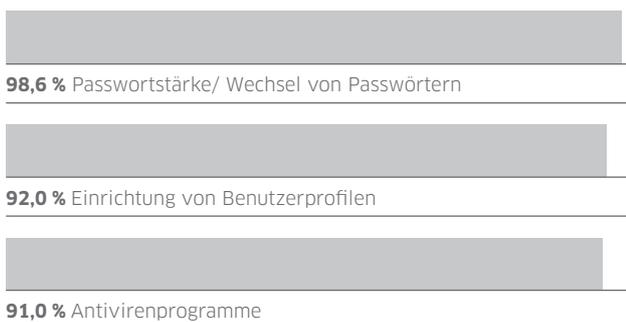


Abb. 3c TOP 3 der Bekanntheit von Schutzmaßnahmen

4. Nutzung von Schutzmaßnahmen

Auffällig bei der Nutzung von Sicherheitsmaßnahmen ist das Gefälle gegenüber der Bekanntheit. Immerhin 14 Prozent der Onliner nutzen keine Antiviren-Programme. An Platz zwei der meist genutzten Schutzmaßnahmen steht die Logout-Funktion mit 79 Prozent. Ein Viertel nutzt keine sicheren Zahlungssysteme. *Ausführlich S. 32.*

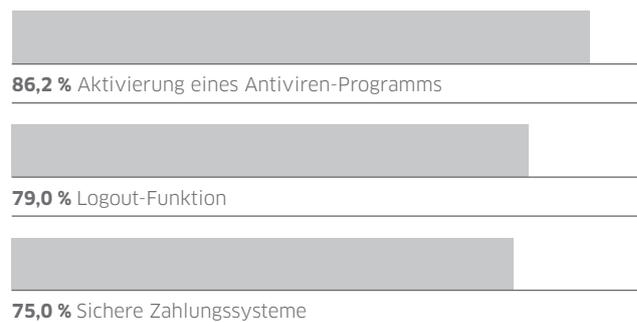


Abb. 3d TOP 3 der Nutzung von Schutzmaßnahmen

Verlust meiner Anonymität **NSA-Spionage**

Der Nutzer selbst Bei W-Lan kann sich jeder reinhacken

Beobachtung meiner Gewohnheiten **Dass Bankdaten**

Beim Online-Banking **abgegriffen werden**

einen Virus zu bekommen **Zuviel preisgeben**

Dass jemand Passwörter knackt

Software, die mitliest, was ich mache Nutzung meiner

Verlust meiner Daten von nicht autorisierten Personen

Anonymität

Bezahlen über Kreditkarte

Beobachtung meiner Gewohnheiten

NSA-Spionage

Bei W-Lan kann sich jeder reinhacken

Offene Nennungen

Die größten

Risiken im Internet

Zuviel preisgeben

Beobachtung meiner Gewohnheiten

Nutzung meiner Daten von nicht autorisierten

Zuviel preisgeben

Beim Online-Banking einen Virus zu bekommen

Personen
Zuviel preisgeben

Wenn wieder mal der Server meines

Viren auf Mail-Anbieters gehackt wird

meinen Computer bekommen

Beim Online-Banking **Auf Betrüger reinzufallen, die einen Virus zu bekommen** einen auf falsche Seiten lotsen

Dass Bankdaten abgegriffen werden

Beobachtung meiner Gewohnheiten Nutzung meiner Daten von nicht autorisierten Personen



Kapitel 2

Sicherheitsgefälle in Deutschland

Sicherheitslage nach Verbrauchertypen

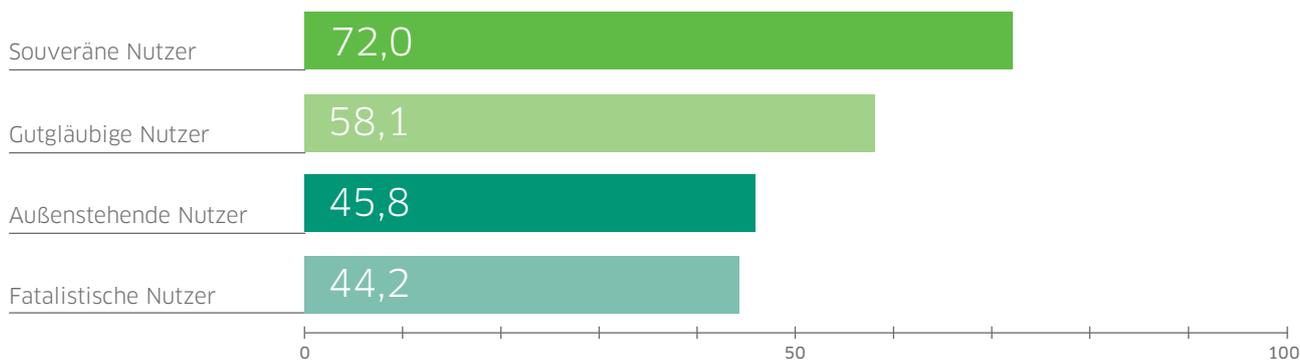


Abb. 5 Verbrauchertypen mit unterschiedlicher Sicherheitslage im Netz (DsiN-Indexwerte)

Die Sicherheitslage der Verbraucher im Netz variiert mit ihrem individuellen Verhalten im Netz. Eine Clusterung der Verbraucher nach Gewohnheiten sowie auch Wissensniveau im Umgang mit dem Internet ergibt vier eigenständige Nutzertypen mit unterschiedlicher Sicherheitslage. Diese Segmentierung ermöglicht typische Verhaltensweisen besser zu beschreiben und daraus zielgenaue Angebote zu entwickeln, um die Sicherheitslevel konkret zu verbessern:

Fatalistische Nutzer gehören eher der jüngeren Bevölkerungsgruppe an und liegen mit **44,2 Punkten** deutlich unter dem Schwellenwert. Sie sind überdurchschnittlich häufig von Sicherheitsvorfällen betroffen – trotz hohen Gefährdungsempfindens. Sie unterlassen Sicherheitsmaßnahmen, obwohl sie Risiken und Schutzmaßnahmen überdurchschnittlich gut kennen.

DsiN Erforderlich ist insbesondere eine Ermutigung zu Schutzmaßnahmen.

Außenstehende Nutzer sind meist ältere Verbraucher und schneiden mit **45,8 Punkten**

kaum besser als die fatalistischen Nutzer ab. Im Vergleich zu den anderen Nutzergruppen sind die Defizite bei der Kenntnis (42 Punkte) und der Nutzung von Schutzmaßnahmen (18 Punkte) auffällig.

DsiN Vermittlung von Sicherheitswissen und Umsetzungskompetenz stehen im Fokus.

Gutgläubige Nutzer stammen aus allen Altersgruppen und liegen mit **58,1 Punkten** noch 8 Punkte über dem Schwellenwert. Gleichwohl verfügen sie über ein nur sehr gering ausgeprägtes Gefährdungsempfinden mit 15 Punkten und nutzen Schutzmaßnahmen kaum (36 Punkte).

DsiN Ermutigung zum sicheren Verhalten und Sensibilisierung genießen Priorität.

Souveräne Nutzer liegen mit **72 Punkten** deutlich über dem allgemeinen DsiN-Index von 60,2 Punkten. Sie verfügen bereits über eine hohe Kompetenz und wenden Schutzmaßnahmen meist auch an (73,4 Punkte).

DsiN Schulung über aktuelle Entwicklung und Vorbild-/Lehrfunktion.

Fast zwei Drittel benötigen aktive Unterstützung

Ein Blick auf die Verteilung der Verbrauchertypen in der gesamten Bevölkerung zeigt, dass die Gruppe der souveränen Nutzer – absolut gesehen – den größten Anteil ausmacht. Gleichwohl ergeben die drei weiteren Gruppen in der Summe eine überwiegende Mehrheit von über 60 Prozent. Ihre Sicherheitslage liegt unter dem DsiN-Index und teilweise sogar unterhalb des Schwellenwerts von 50 Punkten. Damit zeigt sich schon insgesamt ein enormes Bedürfnis an Aufklärungsarbeit, die eine große Breitenwirkung erfordert. Die Herausforderung für eine erfolgreiche Verbesserung der Sicherheitslage liegt aber darin, die spezifischen Bedürfnisse der vier Verbrauchertypen angemessen zu berücksichtigen. So verfügt der gutgläubige Nutzer bereits über ein gutes Grundwissen der Sicherheitsmaßnahmen, geht aber dennoch zu sorglos

mit den potentiellen Bedrohungen um. Hier würden Aufklärungsmaßnahmen, die sich allein auf die Vermittlung von Grundwissen konzentrieren, ins Leere laufen. Hingegen sind die außenstehenden Nutzer oftmals Opfer von Sicherheitsvorfällen, setzen dennoch kaum wirksame Schutzmaßnahmen ein. Bloße Hinweise auf die Bedrohungslage im Netz würden zu keinen weiteren Erfolgen

60

Prozent der deutschen Onliner haben erheblichen Aufklärungsbedarf



DsiN-Index zeigt vier Nutzertypen, die sich im Sicherheitslevel deutlich unterscheiden

verhelfen. Umgekehrt sind die fatalistischen Nutzer sehr misstrauisch im Netz und verhalten sich trotz Sicherheitswissen im Netz in Bezug auf Sicherheitsmaßnahmen sehr passiv.

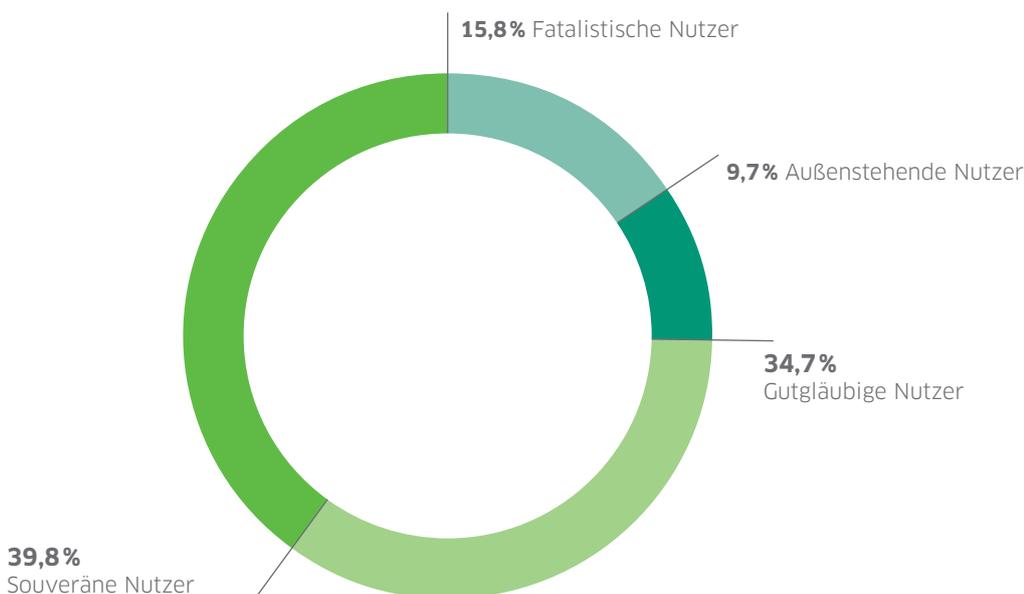


Abb. 6: Anteil der der Nutzergruppen an der Gesamtheit der Onliner

Fatalistische Nutzer (44,2 Punkte)



Der fatalistische Nutzer

Indexwert

Der DsiN-Index für diese Gruppe liegt bei **44,2 Punkten** und ist damit im Vergleich zu anderen Nutzergruppen am geringsten.

Typische Merkmale

Der fatalistische Nutzer ist typischerweise unter 30 Jahren. Insbesondere die 16- bis 19-jährigen sind überproportional vertreten. Der Nutzer verfügt oftmals über ein Einkommen von unter 1.000 Euro im Monat. Fast 80 Prozent der Onliner sind privat bis zu 20 Stunden in der Woche aktiv im Netz. Die betroffenen Nutzer machen fast 16 Prozent aller Onliner in Deutschland aus.

Bedrohungslage

Dieser Nutzertyp hatte in den vergangenen 12 Monaten ein deutlich erhöhtes Vorkommen von **Sicherheitsvorfällen** (52 Punkte). Mit gut 23 Prozent wurden häufiger E-Mail-Konten übernommen als bei anderen Onli-

nern (11,3 Prozent). Auch wurde sie überdurchschnittlich oft von Viren befallen (25 im Vergleich zu 20 Prozent). Charakteristisch für den fatalistischen Nutzer ist ein vergleichsweise sehr hohes **Gefährdungsempfinden** mit 70,4 Punkten. Soziale Netzwerke halten 88 Prozent für gefährlich (andere: 34 Prozent). Misstrauen liegt auch beim Daten-Upload (87 zu 33 Prozent) und dem Austausch vertraulicher Daten vor (86 zu 44 Prozent).

Schutzniveau

Sicherheitswissen (68 Punkte) und **Sicherheitsverhalten** (38,1 Punkte) müssen deutlich verbessert werden. So nutzen fast 23 Prozent der fatalistischen Nutzer kein Antivirenprogramm und auch bei der Passwortsicherheit gibt es Nachholbedarf: 33 Prozent verwenden immer dieselben Passwörter, nur 72 Prozent geben an, aus ihrer Sicht starke Passwörter zu verwenden.

Bedrohungslage



DsiN-Sicherheitsindex

44,2

Schutzniveau

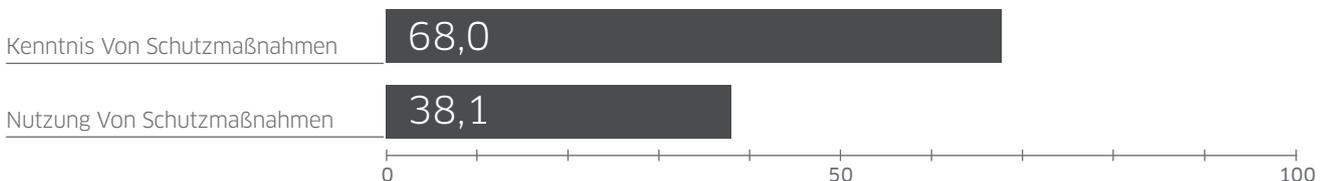


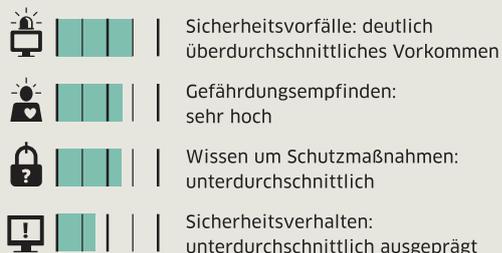
Abb. 7 DsiN-Index Punkte für fatalistischen Nutzer

Der fatalistische Nutzer

44,2 Punkte



Beschreibung:



Typische Merkmale

hoher Anteil jüngerer Menschen, insbesondere 16- bis 19-jährige
Einkommen häufig unter 1.000 Euro monatlich
hohe Internetnutzung, meist bis zu 20 Stunden pro Woche



Sicherheitsrelevante Vorfälle: TOP 3

1. Erhalt unerwünschter E-Mails („Spam“) **64,2%**
2. Erhalt infizierter E-Mails / Anhänge / Weblinks **44,9%**
3. Infizierung durch Schadsoftware (z.B. Viren oder Malware) **24,7%**



Gefährdungsempfinden TOP 3

1. Auslagern eigener Dateien auf dritte Webserver **86,7%**
2. Austausch vertraulicher Inhalte (z.B. mit Behörden) **86,4%**
3. Herunterladen von Software **83,7%**



Unbekannte Schutzmaßnahmen TOP 3

1. Passwortverwaltung (Tresor) **52,7%**
2. Passwort auf fremden Rechnern **54,4%**
3. Privates Surfen (inkognito) **59,1%**



Nutzung von Schutzmaßnahmen TOP 3

1. Passwortverwaltung **10,8%**
2. Nutzung eines Passwortmanagers **11,5%**
3. Verschlüsselung von E-Mails **17,7%**

Abb. 8 Der fatalistische Nutzer

Wirkung von Schutzmaßnahmen erklären

Das überraschende Bild dieser eher jüngeren Onliner ist, dass sie ein fast schon überzogenes Misstrauen im Netz haben und über durchschnittliches Sicherheitswissen verfügen. Allerdings setzen sie ihr Potential nicht um; sie vertrauen darauf, dass es „schon gut geht“ oder der Schaden so gering bleibt, dass er den Aufwand für Sicherheitsmaßnahmen nicht lohnt.

Dieser Gruppe sollte die reale Wirkung von Schutzmaßnahmen besser erklärt werden sowie über die Folgen einer gleichgültigen Haltung im Netz – für die Personen selbst und ihre Umgebung. Vorbilder aus der Peergroup könnten dazu beitragen, dass umsichtiges Verhalten im Internet auch sozial akzeptiert wird. Für eine erfolgreiche Verinnerlichung sind praktische Tipps sowie konkrete Trainings zu empfehlen.



DsiN Angebote für fatalistische Nutzer:

- **IT-Fitness Test**
Training zum sicheren Umgang mit Daten
- **DsiN-Bundesjugendwettbewerb My Digital World**
Jugendliche tragen zum souveränen Umgang im Netz bei
- **Juki – Kindervideoplattform**
Mit Sicherheit kreativ im Netz
- **Medien in die Schule**
Unterrichtsmaterial für Schüler

Außenstehende Nutzer (45,8 Punkte)



Der außenstehende Nutzer

Indexwert

Der DsiN-Sicherheitsindex dieser Gruppe liegt mit **45,8 Punkten** unter dem Schwellenwert von **50 Punkten** und nur leicht über dem Wert fatalistischer Nutzer.

Typische Merkmale

Zu den außenstehenden Nutzern gehören eher ältere Menschen zwischen 60 und 69 Jahren, fast 80 Prozent Frauen. Sie gehen über stationäre PCs und Laptops ins Internet, selten nur über Smartphones oder Tablets. Die private Nutzung liegt unter 10 Stunden. Außenstehende Nutzer machen fast 10 Prozent aller Onliner in Deutschland aus.

Bedrohungslage

Sicherheitsvorfälle dieser Gruppe liegen im Durchschnitt der Bundesbevölkerung (36,6 Punkte), bedingt durch eine kürzere Nutzungsdauer ist die Risikoexposition dieser Gruppe vergleichsweise gering. Das

Gefährdungsempfinden liegt leicht unter dem bundesweiten Durchschnitt von 22,5 Punkten, aber über dem des fatalistischen Nutzers. Allein beim Austausch vertraulicher Daten sind außenstehende Nutzer sensibler als der Bundesdurchschnitt.

Schutzniveau

Außenstehende Nutzer haben großen Aufholbedarf bei der **Kenntnis von Sicherheitsmaßnahmen**. Mit 42 Punkten liegt der Wissensstand deutlich unter dem Durchschnitt. Ebenso das Wissensspektrum: 90 Prozent aller Onliner kennen 17 relevante Sicherheitsmaßnahmen, während bei den außenstehenden Nutzern nur zwei bekannt sind. Auffällig ist auch das niedrige **Sicherheitsverhalten** mit nur 18,8 Punkten. 33 Prozent der Nutzer nutzen gar kein Anti-Viren-Programm und 35 Prozent verzichten auf unterschiedliche Passwörter.

Bedrohungslage

Sicherheitsrelevante Vorfälle **36,6**

Gefährdungsempfinden **22,5**

DsiN-Sicherheitsindex **45,8**

Schutzniveau

Kenntnis Von Schutzmaßnahmen **42,0**

Nutzung Von Schutzmaßnahmen **18,8**

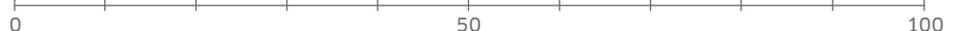


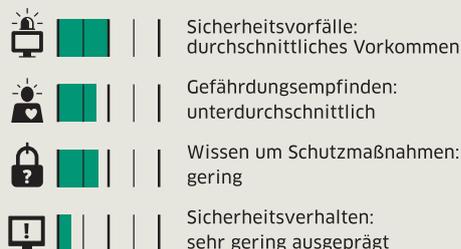
Abb. 9: DsiN-Index Punkte für außenstehende Nutzer

Der außenstehende Nutzer

45,8 Punkte



Beschreibung:



Typische Merkmale

hoher Anteil älterer Menschen insbesondere 60 - 69-jährige und hoher Anteil von Frauen

geringerer Anteil von Gutverdienern (Einkommen über 3.000 Euro und mehr monatlich)

Internet wird in geringerem Umfang genutzt



Sicherheitsrelevante Vorfälle: TOP 3

1. Erhalt unerwünschter E-Mails („Spam“)
 59,9%
2. Erhalt infizierter E-Mails / Anhänge / Weblinks
 39,3%
3. Infizierung durch Schadsoftware (z.B. Viren oder Malware)
 24,5%



Gefährdungsempfinden TOP 3

1. Öffnen von Anhängen in E-Mails
 59,1%
2. Austausch vertraulicher Inhalte (z.B. mit Behörden)
 50,2%
3. Herunterladen von Software
 43,8%



Unbekannte Schutzmaßnahmen TOP 3

1. Inkognito-Funktion
 18,1%
2. Phishing-Filter
 23,9%
3. Passwortverwaltung (Tresor)
 24,7%



Nutzung von Schutzmaßnahmen TOP 3

1. Verschlüsselung der Festplatte
 0%
2. Passwortverwaltung (Tresor)
 0%
3. Verschlüsselung von Daten auf dem Computer
 0,5%

Abb. 10 Der außenstehende Nutzer

Grundwissen praktikabel vermitteln

Diese Nutzergruppe liegt bei allen vier Sicherheitsfaktoren deutlich zurück. Auch finden sich hier die typischen Diskrepanzen zwischen Wissen und Verhalten einerseits und Sicherheitsvorfällen und Gefährdungsempfinden andererseits; damit zeigt sich das besondere Bedürfnis für eine Unterstützung auf allen Ebenen.

Entscheidend ist die einfache Vermittlung von Grundwissen mit einem Schwerpunkt in der tatsächlichen Umsetzung von angeeignetem Wissen. Erlern werden muss auch eine realistische Einschätzung der Risiken im Netz. Hilfreich kann hier die Ansprache über Multiplikatoren sein, die Vertrauen in der Zielgruppe genießen.



DsiN Angebote für außenstehende Nutzer:

- **Kaufen mit Verstand: Sicher Shoppen**
Informationsportal zum sicheren Online-Handel
- **DsiN-Filmkampagne für sicheres Verhalten im Netz**
Surfen, Kommunizieren und Einkaufen im Netz
- **„Die schönen Seiten des Internets“**
Wettbewerb für Senioren, der souveränes Verhalten im Netz fördert
- **Handbücher für Lernende und Einsteiger**
IT-Sicherheit zum Lernen und Lehren im handlichen Format

Gutgläubige Nutzer (58,1 Punkte)



Der gutgläubige Nutzer

Indexwert

Mit 58,1 Punkten liegt der Index gutgläubiger Nutzer 12 Punkte über dem Wert der außenstehenden Nutzer, aber nur 8 Punkte über dem Schwellenwert (50 Punkte).

Typische Merkmale

Gutgläubige Nutzer sind meist zwischen 30 und 59 Jahren. Sie nutzen Desktop-PCs gefolgt vom Laptop. Mobile Endgeräte wie Smartphones werden nur von 37 Prozent verwandt, Tablets von 20 Prozent. Die Nutzungsdauer ist heterogen, die Mehrheit surft privat unter 10 Wochenstunden, über 30 Stunden surfen nur 16 Prozent. Zum gutgläubigen Nutzer zählen 35 Prozent aller Onlineer.

Bedrohungslage

Gutgläubige Nutzer werden seltener Opfer von Sicherheitsvorfällen als der durchschnittliche Onlineer (36 Punkte zu 40 Punkte). Die

gutgläubigen Nutzer verfügen mit 15 Punkten über ein auffallend geringes Gefährdungsempfinden. Konkret sieht die Hälfte im Öffnen von Anhängen in E-Mails eine Gefahr (andere: 60 Prozent). Den Austausch von vertraulichen Daten betrachten 30 Prozent mindestens als gefährlich.

Schutzniveau

Der gutgläubige Nutzer hat mit 81 Punkten eine sehr gute Kenntnis von Schutzmaßnahmen. 90 Prozent kennen mindestens 33 von 40 Schutzmaßnahmen. Das tatsächliche Verhalten steht dazu im starken Kontrast. Der Indexwert von 36,2 Punkten liegt hier deutlich unter dem Bundesdurchschnitt (49 Punkte). Nur 39 Prozent informieren sich über Apps vor dem Download (gesamt: 66 Prozent), nur 44 Prozent deaktivieren Übertragungsfunktionen wie W-Lan oder Bluetooth bei Nichtnutzung.

Bedrohungslage

Sicherheitsrelevante Vorfälle 36,6

Gefährdungsempfinden 15,3

DsiN-Sicherheitsindex 58,1

Schutzniveau

Kenntnis Von Schutzmaßnahmen 81,3

Nutzung Von Schutzmaßnahmen 36,2



Abb. 11: DsiN-Index Punkte für außenstehende Nutzer

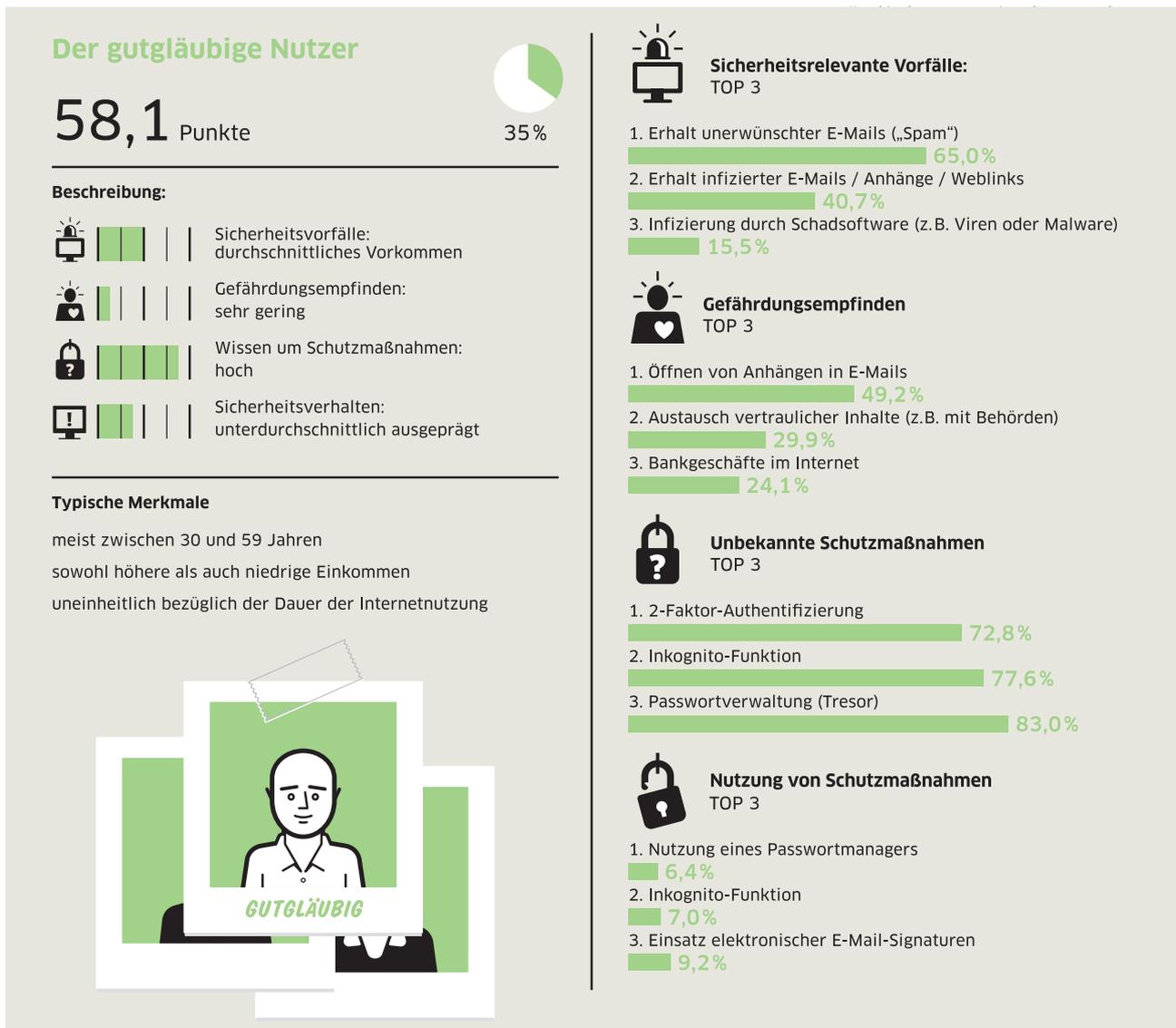


Abb. 12 Der gutgläubige Nutzer

Sensibilisierung und Umsetzungskompetenz stärken

Charakteristisch für den gutgläubigen Nutzer ist ein unterentwickeltes Sicherheitsempfinden im Netz bei zugleich hohem Kenntnisstand über Schutzmaßnahmen. Dieser Gruppe mangelt es an der Motivation zum sicheren Verhalten aufgrund vermuteter Gefahrenlosigkeit im Internet. Diese Erfahrungen stehen durchaus im Widerspruch zu den tatsächlich bereits erlebten Sicherheitsvorfällen.

In dieser Gruppe muss daher das Gefährdungsempfinden im Sinne einer Risikoaufklärung gestärkt werden. Die möglichen Folgen unbedachter Handlungen im Netz sollten dieser Nutzergruppe konkret vor Augen geführt werden; für einen nachhaltigen Erfolg erscheinen Wiederholungseffekte der Aufklärungsmaßnahmen sinnvoll.



DsiN Angebote für gutgläubige Nutzer:

- **IT-Fitness Online Academy**
Unterstützung für jede Altersgruppe
- **Sicherheitsbarometer**
wöchentlich aktuelle Sicherheitsmeldungen
- **„Einfach gemacht“ – Verschlüsselung von Daten**
Tipps zum sicheren Umgang mit Daten
- **Gut zu wissen**
DsiN-Infos zu Kernthemen der IT-Sicherheit

Souveräne Nutzer (72,0 Punkte)



Der souveräne Nutzer

Indexwert

Der DsiN-Sicherheitsindex für diese Gruppe liegt bei weit überdurchschnittlichen 72 Punkten.

Typische Merkmale

Der souveräne Nutzer ist meist zwischen 40 und 49 Jahren alt, selten über 60. Er verfügt über eine höhere Bildung und findet sich im Bereich der Gutverdienenden mit über 4.000 € Haushaltseinkommen. Er surft mehr als 10 Stunden in der Woche privat, 40 Prozent über 20 Stunden. Die Mehrheit nutzt Tablets, 80 Prozent auch das Smartphone.

Bedrohungslage

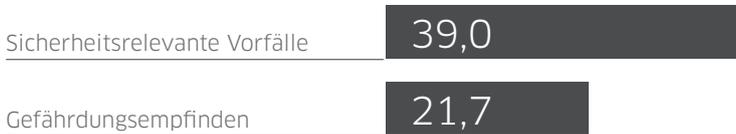
Bei den **sicherheitsrelevanten Vorfällen** liegt diese Gruppe mit 39 Punkten nur leicht über dem Durchschnitt, bedingt durch intensivere Nutzung und höhere Risikoexposition. Auch das **Gefährdungsempfinden**

ist mit 21,7 Punkten weniger ausgeprägt. Gerade bei alltäglichen Anwendungen des Smartphones wie Messenger-Diensten (14,3 Prozent gegenüber 24,7 Prozent) oder standortbezogenen Diensten haben kompetenten Nutzer eher geringe Bedenken (8,1 Prozent gegenüber 17,7 Prozent).

Schutzniveau

Das **Kenntnisniveau** des souveränen Nutzers ist mit 94,6 Punkten sehr hoch. 90 Prozent der kompetenten Nutzer sind 37 von 40 Schutzmaßnahmen bekannt. Schlechter bekannt sind Inkognito-Funktion im Browser (89 Prozent) und 2-Faktor-Authentifizierung (86 Prozent). Die **genutzten Schutzmaßnahmen** liegen mit 73,4 Punkten sehr hoch und zeigen das geringste Gefälle gegenüber der Bekanntheit. Im Einzelfall gibt es dennoch Verbesserungsbedarf: 48 Prozent verschlüsseln ihre Mails nicht, 64 Prozent verzichten auf die Verschlüsselung der Festplatte.

Bedrohungslage



DsiN-Sicherheitsindex



Schutzniveau

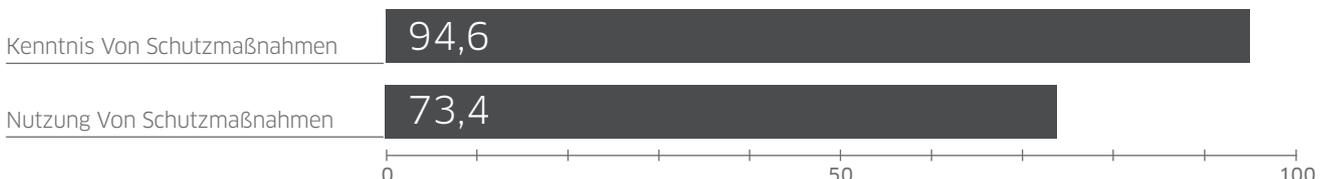


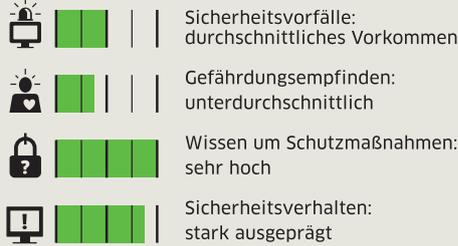
Abb. 13, DsiN-Index Punkte für souveräne Nutzer

Der souveräne Nutzer

72 Punkte

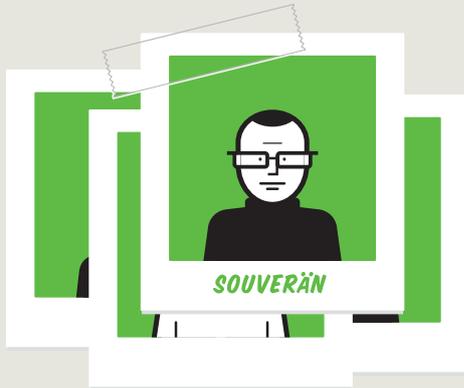


Beschreibung:



Typische Merkmale

meist zwischen 40 und 49 Jahren
Einkommen häufig über 4.000 Euro monatlich
nutzt das Netz privat meist mehr als 10 Stunden pro Woche



Sicherheitsrelevante Vorfälle: TOP 3

1. Erhalt unerwünschter E-Mails („Spam“) **77,5%**
2. Erhalt infizierter E-Mails / Anhänge / Weblinks **58,3%**
3. Infizierung durch Schadsoftware (z.B. Viren oder Malware) **19,9%**



Gefährdungsempfinden TOP 3

1. Öffnen von Anhängen in E-Mails **62,0%**
2. Austausch vertraulicher Inhalte (z.B. mit Behörden) **37,5%**
3. Herunterladen von Software (keine Updates) **33,0%**



Unbekannte Schutzmaßnahmen TOP 3

1. 2-Faktor-Authentifizierung **86,2%**
2. Passwortverwaltung (Tresor) **88,0%**
3. Inkognito-Funktion **89,4%**



Nutzung von Schutzmaßnahmen TOP 3

1. Passwortverwaltung (Tresor) **31,6%**
2. Nutzung eines Passwortmanagers **34,0%**
3. Verschlüsselung der Festplatte **36,3%**

Abb. 14 Der souveräne Nutzer

Kontinuierliche Aufklärungsarbeit

Der souveräne Nutzer muss durch laufende Verbesserung der Schutzmöglichkeiten auf hohem Niveau gehalten und kontinuierlich informiert werden. Dies umfasst auch die Darstellung konkreter Risiken, um die Notwendigkeit von Maßnahmen besser einschätzen zu können und aktiv zu werden. Da mit steigender Aktivität im Netz auch die Wahrscheinlichkeit eines Sicherheitsvorfalls steigt, sollte über zusätzliche Maßnahmen aufgeklärt werden, die aufgrund des hohen Grundverständnisses leichter vermittelbar sind. Der souveräne Nutzer sollte als Multiplikator für andere gewonnen werden, die ihn zum Vorbild im Umgang mit dem Netz nehmen könnten.



DsiN Angebote für souveräne Nutzer:

- „Einfach gemacht“ –
Verschlüsselung von Daten
Tipps zum sicheren Umgang mit Daten
- **Security-News-App**
Aktuelle Sicherheitsrisiken auf das Smartphone
- **DsiN-Passwort-Wechsel App**
Leichtes Merken von wechselnden Passwörtern
- **Internetbeschwerdestelle**
Machen Sie auf rechtswidrige Inhalte aufmerksam

Exkurs: Index im Bundesländervergleich

In einer Segmentierung der Ergebnisse nach Bundesländern fallen die Ergebnisse unterschiedlich aus. Das Saarland erreichte im Durchschnitt fast den Wert der souveränen Nutzer. Demgegenüber liegt Hamburg fast 9 Punkte unter dem Bundesdurchschnitt. Bei allen Bundesländern liegt der Sicherheits-index über dem Schwellenwert von 50 Punkten.

Ausschlagend für die Unterschiede ist die unterschiedliche Häufung von Sicherheitsvorfällen in den vergangenen 12 Monaten. Hier belegt Hamburg einen „Spitzenrang“ während das Saarland seltener betroffen war. Unterschiede beim tatsächlichen Verhalten der Schutzmaßnahmen oder dem Gefährdungsempfinden fallen demgegenüber insgesamt nicht ins Gewicht.

69,1	Saarland
66,2	Sachsen-Anhalt
66,1	Hessen
65,2	Berlin
64,9	Rheinland-Pfalz
64,5	Sachsen
63,9	Niedersachsen
63,9	Thüringen
63,5	Mecklenburg-Vorpommern
60,7	Brandenburg
62,0	Bremen
60,2	Deutschland
60,0	Nordrhein-Westfalen
55,7	Baden-Württemberg
55,0	Schleswig-Holstein
54,5	Bayern
51,3	Hamburg

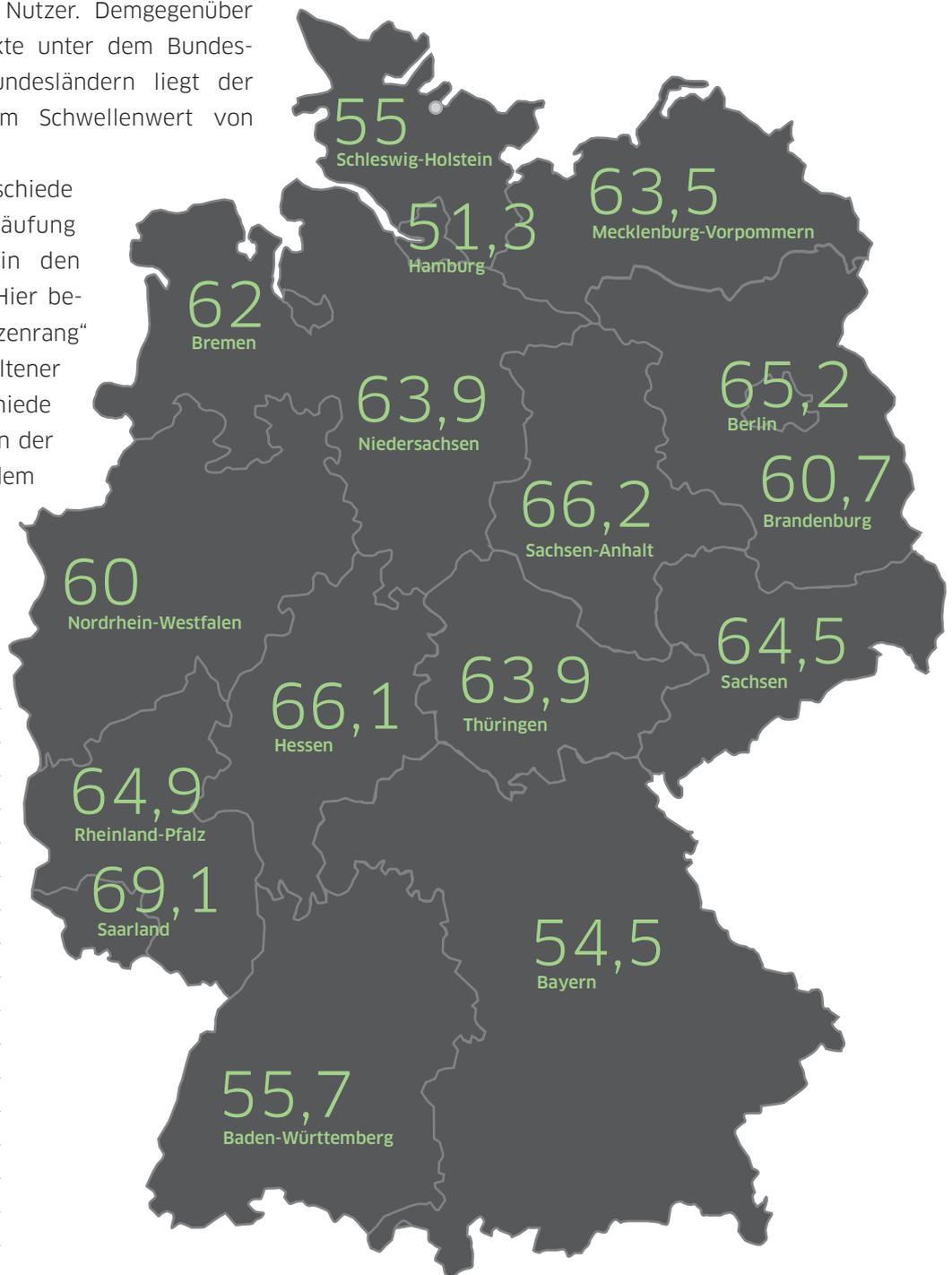


Abb. 15: Index nach Bundesländern

Mobile Banking

Login:

Password:

Kapitel 3

Themenfokus: Digitale Lebenswelten

E-Mail und Social Media

Die private Onlinekommunikation findet heute meist über E-Mail oder Soziale Netzwerke statt. Ein Überblick zeigt Unterschiede und Gemeinsamkeiten bei der sicheren Nutzung dieser Kommunikationskanäle.

38 Prozent öffnen E-Mails ohne Prüfung

- 12 Prozent hielten E-Mails für gefährlich.
- 70 Prozent erhielten Spam-E-Mails.
- 48 Prozent erhielten infizierte Mails.

Social Media: Identitätsdiebstahl bei jedem 17. Nutzer

- 6 Prozent waren Opfer von Identitätsdiebstahl.
- 5 Prozent waren betroffen von Mobbing oder Belästigungen.

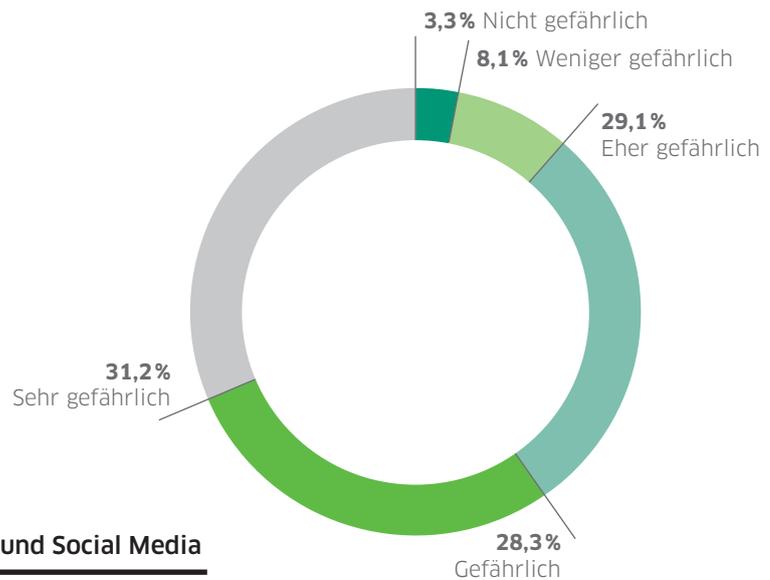


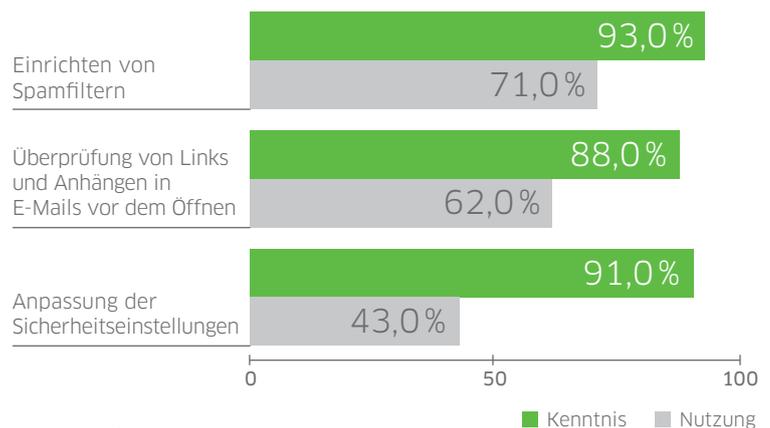
Abb. 16: Gefährdungsempfinden bei E-Mail und Social Media

Fast alle Onliner nutzen E-Mails (95 Prozent); die Kenntnis von Sicherheitsoptionen ist hoch.

93 Prozent kennen Spamfilter, 91 Prozent kennen die Einstellungen ihres E-Mail-Clients und 88 Prozent der Onliner meinen, ihre E-Mails auf Vertrauenswürdigkeit prüfen zu können. Die Nutzungsraten fallen hingegen ernüchternd aus. 71 Prozent verwenden Spamfilter, 62 Prozent prüfen Mails oder Anhänge auf Vertrauenswürdigkeit, nur 43 Prozent passen ihre Sicherheitseinstellungen an.

Die Bedrohungslage durch infizierte Mails indes ist relativ hoch, wie durch Übernahme von Mailkonten zur Spam-Versendung oder dem Versand unautorisierter E-Mails. (11 Prozent). 54 Prozent der Onliner nutzen Soziale Netzwerke gelegentlich, 34 Prozent halten sie für gefährlich. Datenschutz und Persönlichkeitsschutz stehen im Vordergrund.

Abb. 17: Diskrepanz – Wissen und Verhalten



DsiN Angebot für sichere Nutzung von E-Mail und Social Media

- **Sichere E-Mail Kommunikation:** DsiN-Leitfaden für Sicherheit im privaten und beruflichen Umfeld
- **Social Media – Mit Sicherheit:** DsiN-Leitfaden für ein sicheres Social Web

Shopping online

Online-Einkaufen gehört zu den stark wachsenden Aktivitäten der Onliner im Internet. So gaben 85 Prozent der befragten Nutzer an, zumindest gelegentlich im Internet einzukaufen. Hinter der zunehmenden Relevanz bleiben die Sicherheitsmaßnahmen teilweise erheblich zurück.

Kreditkartenbetrug bei 6 Prozent

- 57 Prozent finden Online-Shopping wenig bzw. nicht gefährlich.
- 9 Prozent wurden schon betrogen.
- Bei 7 Prozent wurden die Zugangsdaten ausgespäht.
- 6 Prozent sind Opfer von Kreditkartenbetrug geworden.

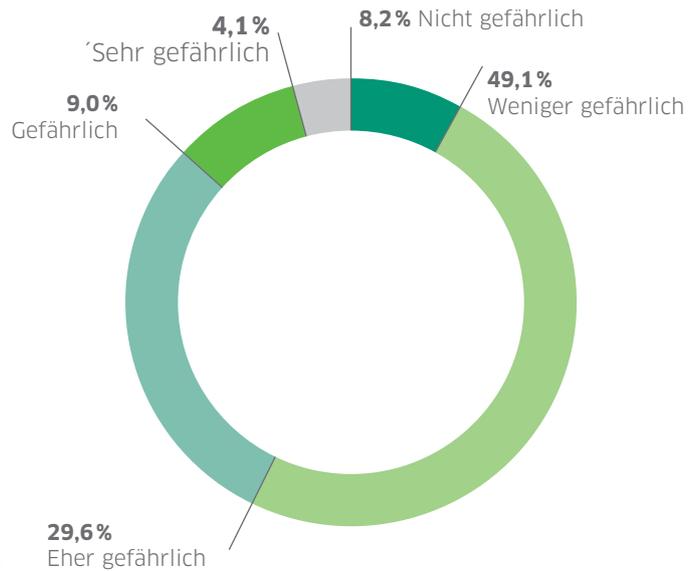


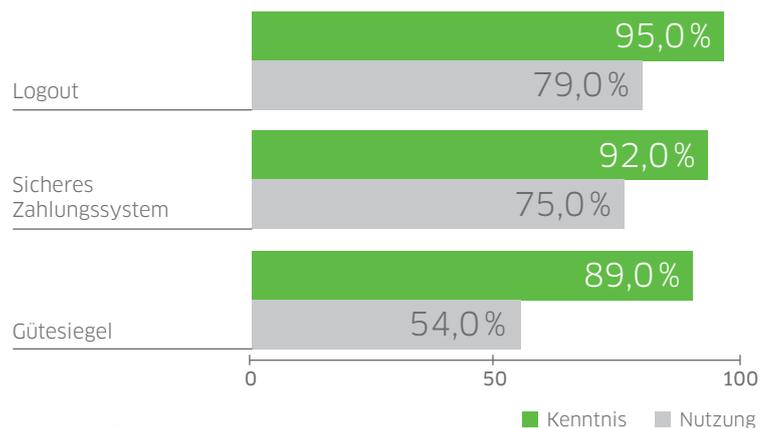
Abb. 18: Gefährdungsempfinden beim Shopping

Beim Thema Online-Shopping wussten 92 Prozent der deutschen Onliner, dass es sichere Zahlungssysteme zum Einkauf im Internet gibt, aber nur drei Viertel nutzen diese auch.

Bei der Verwendung von Gütesiegeln (z.B. TÜV, Trusted Shops) ist die Bekanntheit mit fast 89 Prozent ebenfalls hoch. Aber nur 54 Prozent der befragten Surfer geben an, dass sie beim Interneteinkauf auf Gütesiegel achten.

Die Werte zeigen, dass dem Verbraucher Vertrauen in die Anbieter des Internethandels wichtig ist und ein klares Bedürfnis für Aufklärungsarbeit besteht.

Abb. 19: Diskrepanz – Wissen und Verhalten



DsiN Angebot für sicheres Einkaufen im Netz

- **Kaufen mit Verstand: Sicher Shoppen**
Darauf sollten Sie beim Einkaufen im Netz achten.
- **DsiN-Passwort-Wechsel App**
Leichtes Ändern von Passwörtern

Digitale Bankschalter

Bankgeschäfte im Netz werden heute von einer Mehrheit der Internetnutzer getätigt, im Unterschied zu Online Shopping wird das Sicherheitsrisiko bei Online Banking allerdings als hoch eingeschätzt.

Banking - 6 Prozent Opfer von Ausspähattacken

- 34 Prozent der Nutzer halten Online-Banking für gefährlich oder sehr gefährlich.
- 32 Prozent halten Bankgeschäfte im Internet für nicht oder weniger gefährlich.
- Bei 6 Prozent der befragten Nutzer wurden in den letzten 12 Monaten ihre Zugangsdaten zum Online-Banking ausgespäht.
- 42 Prozent achten nicht auf verschlüsselte Verbindungen

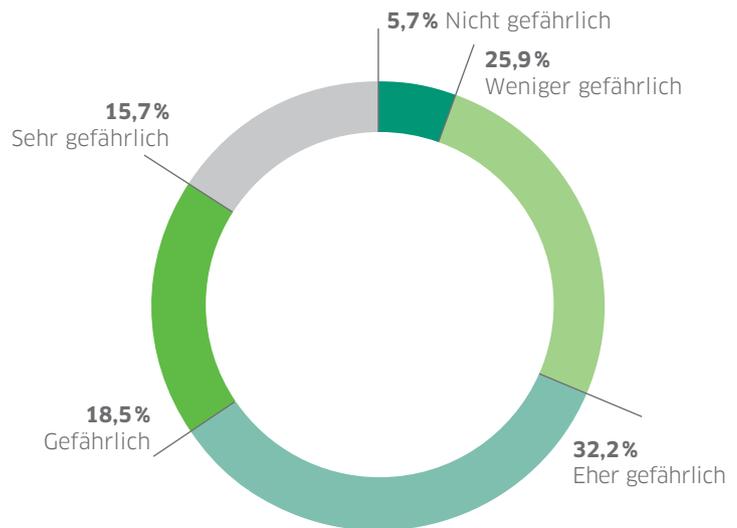


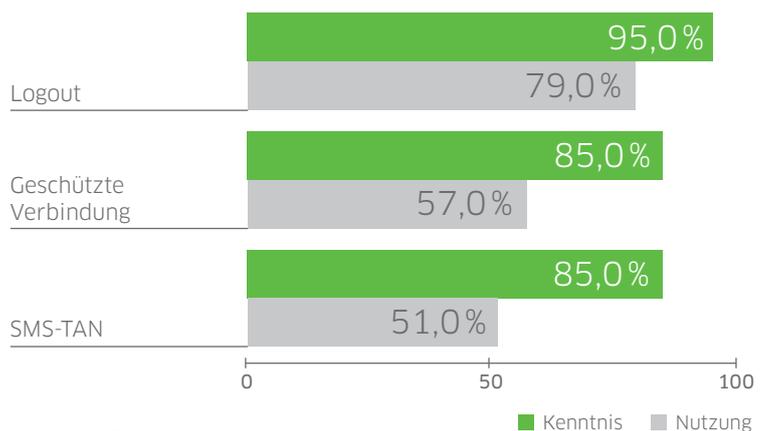
Abb. 20: Gefährdungsempfinden bei Online-Banking

Angesichts der relativ häufigen Sicherheitsvorfälle ist gerade im Bereich der Bankgeschäfte die Relevanz von IT-Sicherheit besonders stark.

Entsprechend sollte das Interesse der Nutzer an einem sicheren Umgang sein - oder das Wissen dazu. Tatsächlich kennen immer noch 15 Prozent der Nutzer keine verschlüsselten Datenverbindungen und dass darauf geachtet werden muss. Genauso viele kennen das Prinzip der Push-TAN nicht. 51 Prozent der deutschen Onliner nutzen wenigstens gelegentlich SMS-TANs.

43 Prozent der Internetnutzer geben an, beim Online-Banking nicht auf verschlüsselte Verbindungen zu achten.

Abb. 21: Diskrepanz - Wissen und Verhalten



DsiN Angebot für Online-Banking

- „Einfach gemacht“ - Verschlüsselung von Daten
Tipps zum sicheren Umgang mit Daten
- DsiN-Passwort-Wechsel App
Leichtes Ändern von Passwörtern



Kapitel 4

Handlungsfelder der digitalen Aufklärung 2.0

Sicherheitswissen praktikabel vermitteln

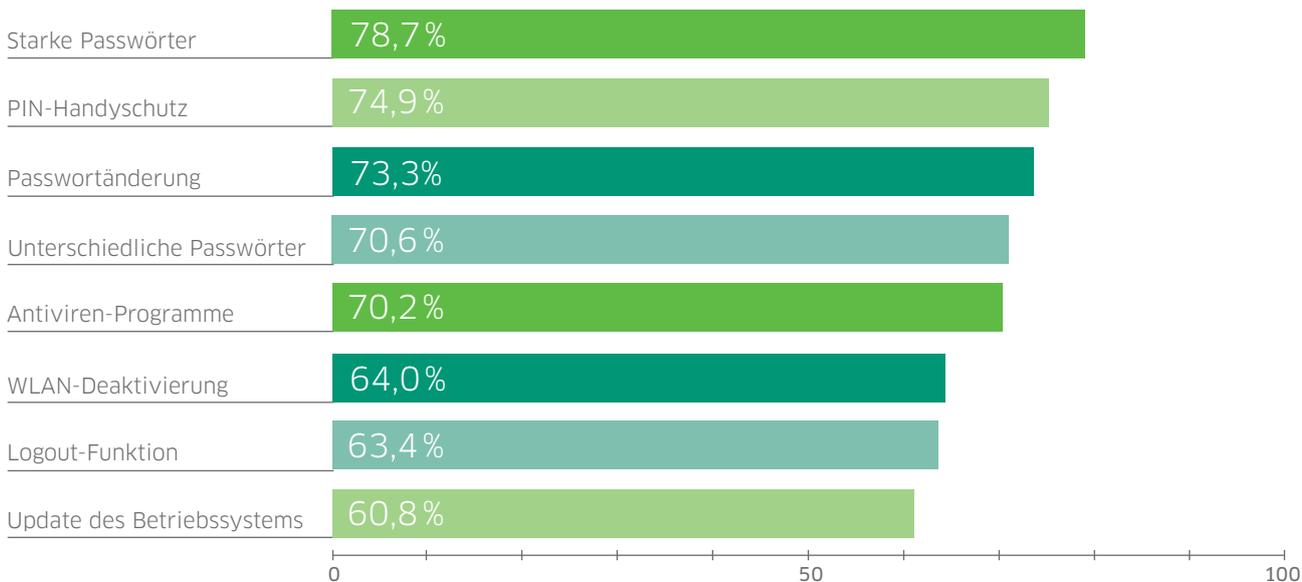


Abb. 22: „Gute“ Sicherheitskenntnisse – vordere Plätze

Differenzierung nach Bekanntheitsgrad

Die Unterschiede zwischen den Nutzergruppen zur Bekanntheit von Sicherheitsmaßnahmen wurden aufgezeigt. Dabei zeigte sich gerade bei den außenstehenden Nutzern ein konkreter Aufholbedarf mit 42 Punkten, während souveräne Nutzer mit 96 Punkten eher über neue Entwicklungen informiert werden sollten.

Eine übergreifende Betrachtung für alle Nutzergruppen des Kenntnisgrades von *gut* und *sehr gut* bis zu *eher gering* zeigt, dass *mindestens gute* Kenntnisse bei grundlegenden Sicherheitsmaßnahmen überwiegen, während anspruchsvollere Maßnahmen seltener gut bekannt sind.

Basiswissen flächendeckend ausbauen (Abb. 22)

Knapp 79 Prozent der Nutzer kennen sich bei der Gestaltung von starken Passwörtern gut aus. Die regelmäßige Änderung von Passwörtern (73 Prozent) sowie die Verwendung unterschiedlicher Passwörter (71 Prozent) sind ebenfalls gut bekannt. Dies betrifft auch die Kenntnisse zum Schutz von mobilen Geräten: 75 Prozent der Smartphone-Nutzer geben an, ihr Gerät mit einer PIN vor unbefugtem Zugriff schützen zu können, 70 Prozent wissen über Antiviren-Software Bescheid und immerhin noch 64 Prozent können drahtlose Verbindungen bedarfsweise deaktivieren. Trotz der vergleichsweise guten Verbreitung zeigt sich, dass ein Viertel der Onliner am Wissen nicht partizipieren. Um den Kenntnisstand über grundlegende Sicherheitsmaßnahmen erfolgreich zu verbreiten, sollte ein Schwerpunkt auf die Gruppen der außenstehenden sowie fatalistischen Nutzer gelegt werden.

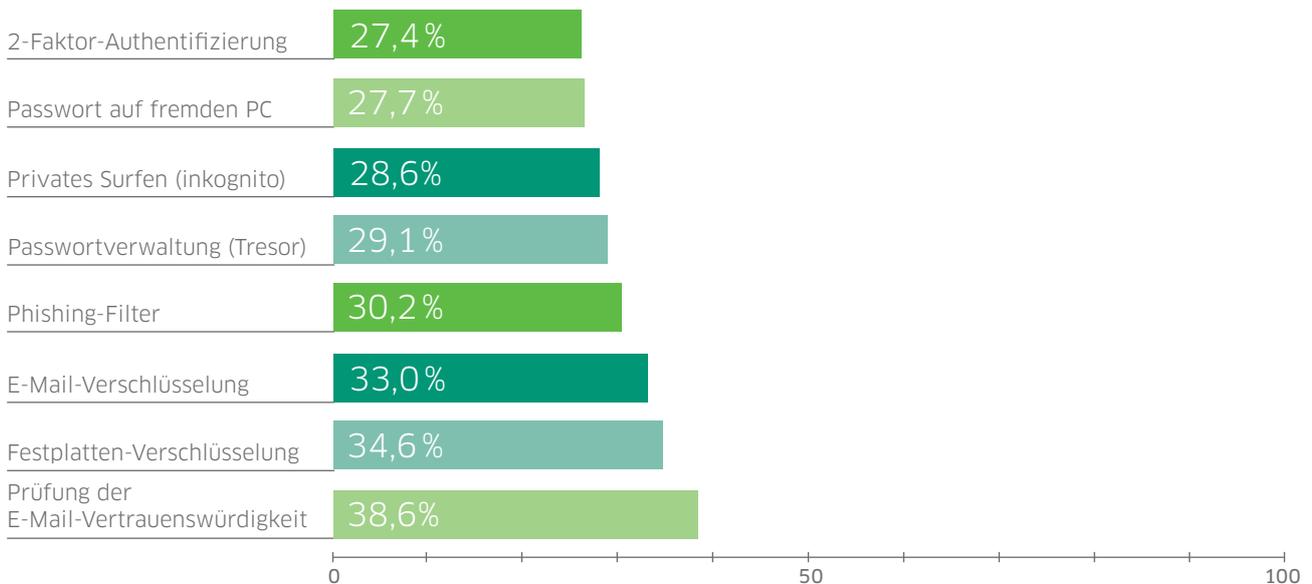


Abb. 23: „Gute“ Sicherheitskenntnisse – hintere Plätze

Komplexere Schutzmechanismen vermitteln (Abb. 23)

Im Vergleich zu den vorderen Werten liegen komplexere Sicherheitsmaßnahmen eher auf den hinteren Plätzen. So hat die E-Mail-Verschlüsselung im Zuge der NSA-Affäre mit 83 Punkten medial zu einer gewissen Bekanntheit geführt. Über *sehr gute* oder *gute* Kenntnisse verfügt allerdings nur jeder dritte Onliner (33 Prozent). Gerade bei anspruchsvolleren Sicherheitsmaßnahmen kann der Grad der Kenntnis damit bereits über ihre Anwendbarkeit entscheiden.

Entsprechend niedrig ist auch der mindestens gute Kenntnisstand bei der Datenverschlüsselung. Nur 35 Prozent kennen sich mit der Festplattenverschlüsselung entsprechend aus, kaum mehr bei der Verschlüsselung einzelner Dateien auf dem Computer (36 Prozent). Da gutgläubige Nutzer in der Regel über ein gutes Grundverständnis verfügen, sollten hier gerade auch komplexere Sicherheitsanforderungen vermittelt werden.



Handlungsempfehlungen Digitale Aufklärung 2.0

- **Grundwissen ausbauen**
Alle Onliner mit Basiswissen vertraut machen
- **Kenntnisse vertiefen**
Komplexere Anforderungen außenstehenden und fatalistischen Nutzern vermitteln
- **Kenntnisgrad halten**
Aktuelle Sicherheitsmaßnahmen für souveräne Nutzer bereit halten
- **Defizite definieren**
Weiterführende Tools je nach Relevanz für die Nutzergruppe näher bringen
- **DsiN-Tools für Wissen**
DsiN-Sicherheitsbarometer, IT-Fitness Test und Academy, DsiN-Filmkampagne, Handbuch für Lernende und Lehrende, Security-News-App

Umsetzungsbereitschaft und -kompetenz stärken

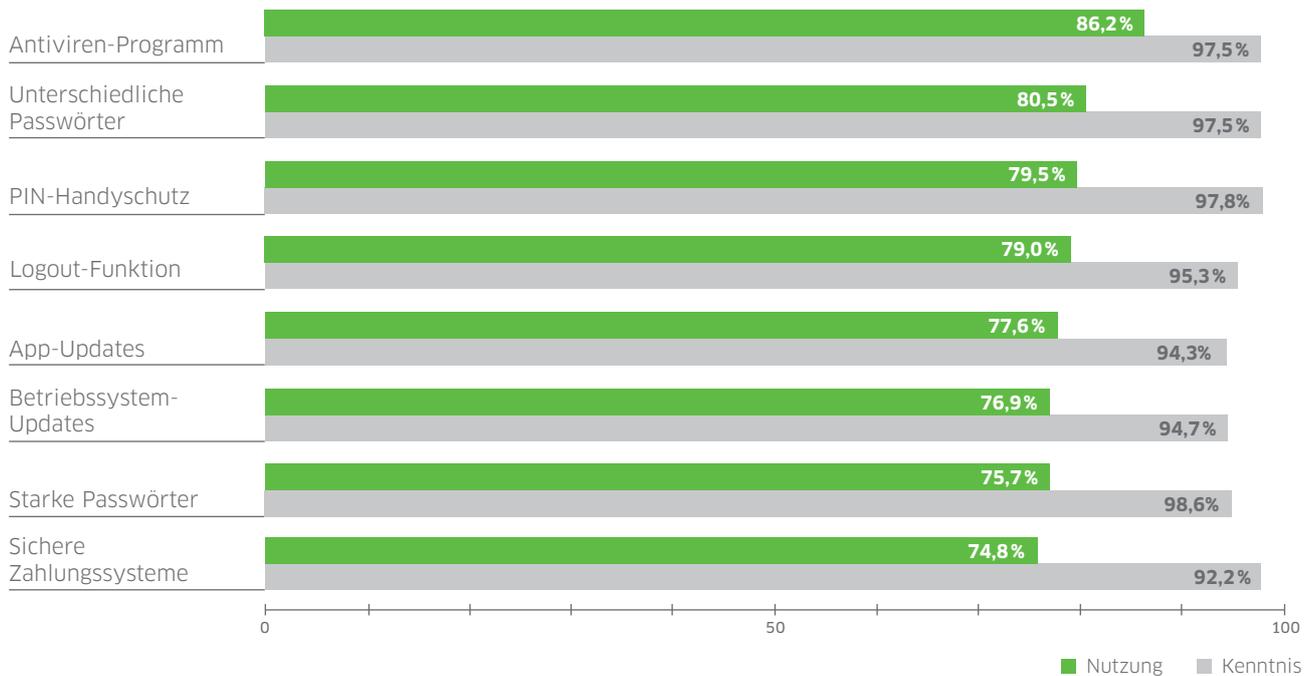


Abb. 24: Nutzung versus Kenntnis von Sicherheitsmaßnahmen – vordere Plätze

Einfache Sicherheitstools erklären

Die Diskrepanz zwischen Kenntnis und tatsächlicher Umsetzung von Schutzmaßnahmen ist bei allen Nutzergruppen gegeben; dabei stechen die gutgläubigen Nutzer heraus, die trotz überdurchschnittlicher Kenntnisse mit 81 Punkten Sicherheitsmaßnahmen kaum anwenden (36 Punkte). Auch die fatalistischen und außenstehenden Nutzer prägt eine mangelnde Umsetzungsbereitschaft bzw. -kompetenz bei einem insgesamt niedrigerem Wissensstand. Eine übergreifende Betrachtung der Diskrepanz zwischen Sicherheitswissen und Umsetzung zeigt, dass Sicherheitsmaßnahmen angewendet werden, wenn sie einfacher zu handhaben sind. Geringere Kenntnisse sowie geringerer Aufwand für die Umsetzung erhöhen danach die Wahrscheinlichkeit für eine tatsächliche Anwendung. Als Ausnahme erscheinen

sichere Zahlungssysteme, die nicht per se zu den einfachen Sicherheitssystemen gezählt werden können, s. Abb. 24. Konkret gehören Antivirens Scanner (86 Prozent), unterschiedliche Passwörter (81 Prozent) sowie der PIN-Handyschutz (80 Prozent) zu den häufigsten Sicherheitsmaßnahmen. Diese Zahlen zeigen, dass gleichwohl knapp 14 Prozent der Onliner über keinen Virenschutz verfügen. Noch höher liegt die Zahl der Internetnutzer, die stets dasselbe Passwort verwenden (20 Prozent) und 22 Prozent verzichten auf Updates ihrer Apps. Dies zeigt einen Aufklärungsbedarf auch bei den einfachen Sicherheitsmaßnahmen mit einem Schwerpunkt auf Umsetzungskompetenzen. Die Bereitschaft zur Durchführung wird vergleichsweise wenig Überzeugungsarbeit erfordern.

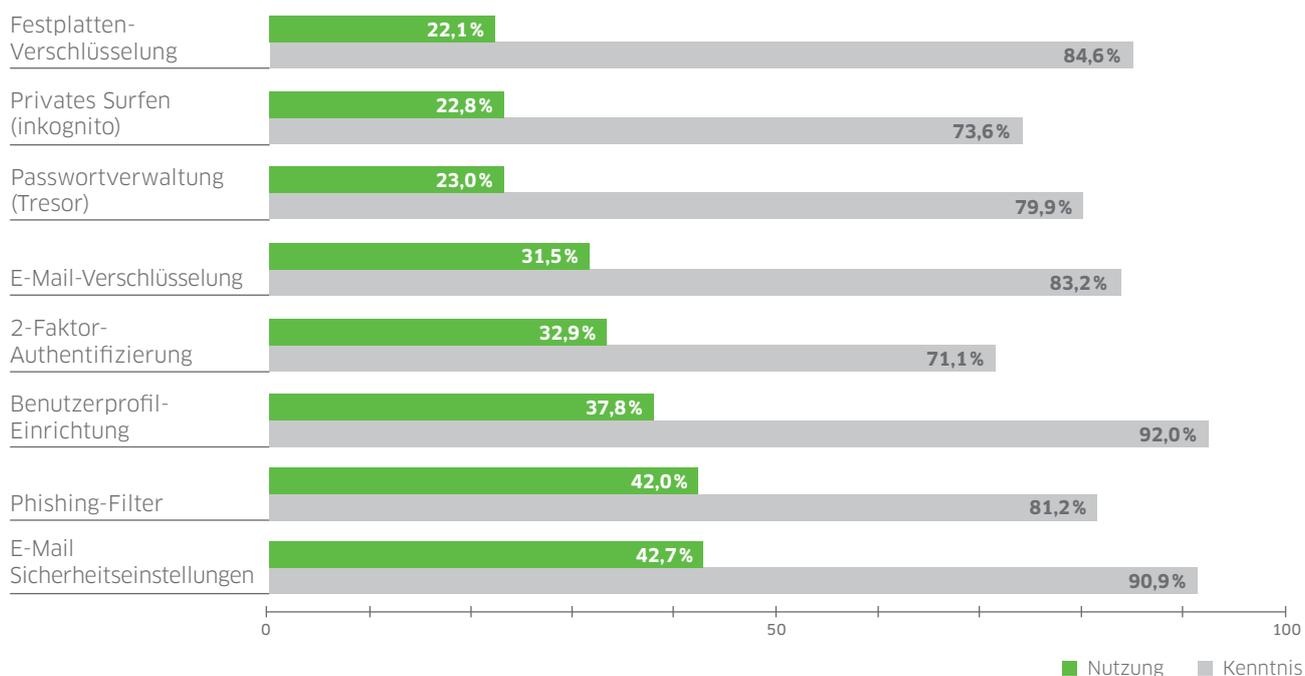


Abb. 25: Nutzung versus Kenntnis von Sicherheitsmaßnahmen – hintere Plätze

Komplexere Maßnahmen trainieren

Geringe Verbreitung im Vergleich zur Bekanntheit finden Maßnahmen, die erweiterte Kenntnisse im Umgang mit digitalen Anwendungen erfordern: Verschlüsselung von Festplatten und E-Mails, anonymes Surfen sowie die Passwortverwaltung. Die Diskrepanz zwischen Kenntnis und Umsetzung liegt hier bei 60 Prozentpunkten. Ähnlich ist es beim Phishing-Filter und der Einrichtung von Benutzerprofilen.

Die hohe Schutzwirkung der komplexeren Maßnahmen rechtfertigt einen höheren Aufwand bei der Aufklärung. Entscheidend ist hier die Motivation zur Umsetzung, etwa über Anreize und Folgebetrachtung. Nutzergruppen mit gewissen Vorkenntnissen haben gegenüber den außenstehenden Nutzern Vorteile. Souveräne Nutzer sollten über die jeweils neuesten Entwicklungen informiert werden.



Handlungsempfehlungen Digitale Aufklärung 2.0

- **Sicherheitstools vermitteln**
Nutzung von Standardmaßnahmen zum Internetstart verinnerlichen
- **Kompetenzen stärken**
Umsetzungsbereitschaft und -kompetenz verstärken
- **Umsetzungsmotivation**
Die Umsetzungsbereitschaft von Maßnahmen durch Anreize verstärken
- **DsiN-Tools für Umsetzung**
Medien in die Schule, Kaufen mit Verstand, Sicherheitsbarometer, „Einfach gemacht“ – Verschlüsselung von Daten, DsiN-Passwort-Wechsel App

Sensibilisieren und Vertrauen aufbauen

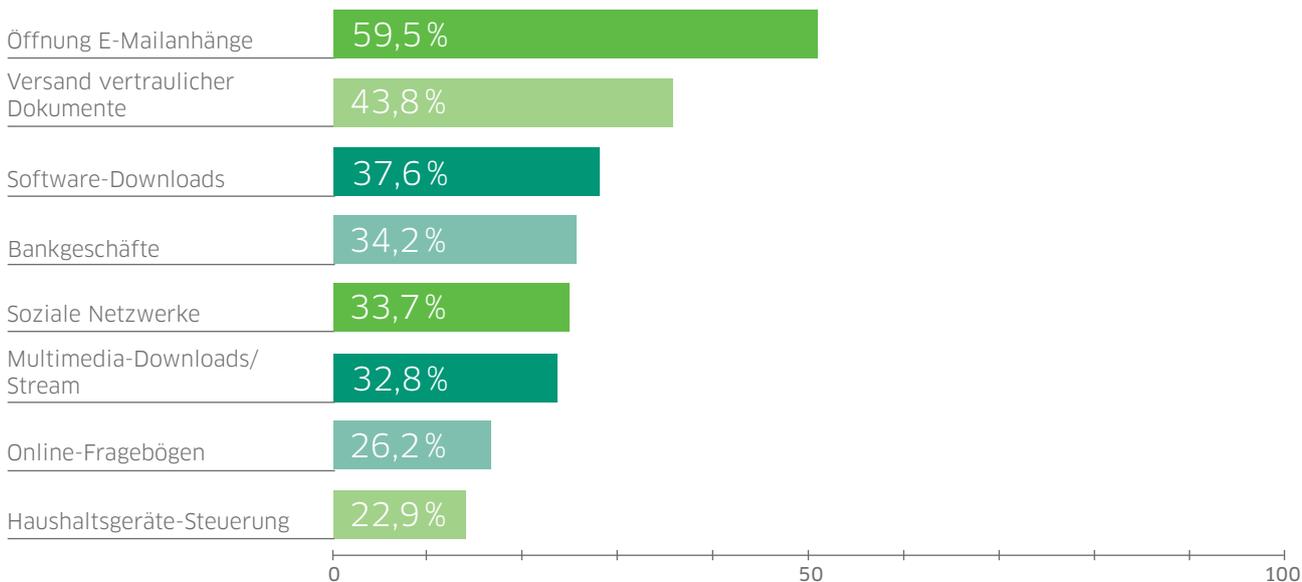


Abb. 26: Registrierte Sicherheitsvorfälle

Hälfte der Onliner fehlt Vertrauen

Beim Vertrauen im Netz zeigen sich erhebliche Unterschiede: Während gutgläubige Nutzer kaum Gefährdung empfinden haben, zeigen fatalistische Nutzer mit 70 Punkten echtes Misstrauen. Eine gruppenübergreifende Betrachtung zeigt besonders wenig Vertrauen bei alltäglichen Diensten wie E-Mail und Downloads. Insgesamt fühlt sich fast die Hälfte unsicher oder weniger sicher im Netz (47 Prozent).

Wirksamkeit von Schutzmaßnahmen aufzeigen

Wichtig ist, dass dem Umgang im Netz eine möglichst reale Risikoeinschätzung zu Grunde liegt, Skepsis also nicht zu Angst, sondern zu umsichtigen Verhalten führt. Sachliche Aufklärung über Risiken und die Erläuterung der Selbstschutzmaßnahmen sind dafür unerlässlich.



Handlungsempfehlungen Digitale Aufklärung 2.0

- **Risikoeinschätzung**
Kompetenzen zur Einschätzung individueller Risiken im Netz stärken
- **Selbstschutz erklären**
Instrumente zum Selbstschutz als Korrelat zur Bedrohungslage erklären
- **DsiN-Tools für Vertrauen:**
DsiN-Bundesjugendwettbewerb
„My Digital World“, DsiN-Filmkampagne,
Gut zu wissen, Internetbeschwerdestelle

Dialog mit Stakeholdern vertiefen

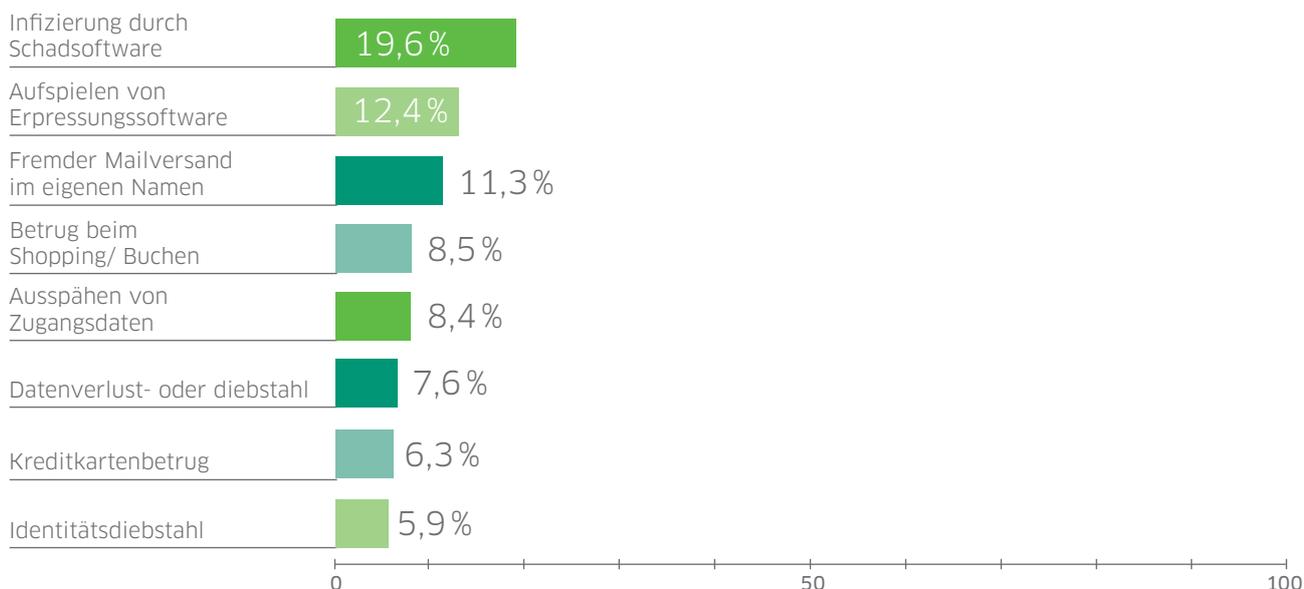


Abb. 27: Registrierte Sicherheitsvorfälle

Aufklärungsarbeit gemeinsam verbessern

Die digitale Aufklärungsarbeit 2.0 für Verbraucher steht erst am Anfang. Um Nutzer zum sicheren Umgang im Netz zu befähigen, sind zusätzliche Aufklärungsarbeit und Engagement erforderlich, die von DsiN koordiniert werden können. Eine stärkere Zusammenarbeit zwischen allen Stakeholdern der digitalen Gesellschaft trägt dazu bei, Aufklärungsarbeit wirksamer zu gestalten.

Gemeinsam können Anreize wirksam gesetzt werden, um beispielsweise die Bereitschaft zu grundlegenden Sicherheitsmaßnahmen zu fördern. Der Dialog mit Partnern – der Politik, Wissenschaft und Wirtschaft – über Aufklärungsstrategie 2.0 sollte daher Priorität haben.



Handlungsempfehlungen Digitale Aufklärung 2.0

- Zusammenarbeit stärken**
 Initiativen zur Aufklärung von Verbrauchern vorantreiben und koordinieren, Defizite definieren und im Verbund Lösungen entwickeln
- Dialog ausbauen**
 Zusammenarbeit aller Stakeholder; Politik, Gesellschaft, Wissenschaft für eine wirksamere Aufklärungsarbeit stärken
- DsiN-Angebote für Dialog:**
 DsiN-Jahreskongress 2015, DsiNsights-Breakfast, DsiN-Newsletter und DsiN Webportal für Verbraucher

Fahrplan zur Digitalen Aufklärung 2.0

Der DsiN-Index 2014 zeigt das Erfordernis, den souveränen Umgang von Verbrauchern im Internet für eine verbesserte Sicherheitslage zu stärken. Drei Faktoren sind entscheidend: Mehr Engagement für eine koordinierte Aufklärungsarbeit, die Berücksichtigung von Verhaltens- und Kenntnisunterschieden bei Verbrauchern durch einen Mix von Maßnahmen sowie ein intensives Zusammenwirken aller Akteure der digitalen Gesellschaft.

Verstärktes Engagement der Wirtschaft

Die Digitale Agenda der Bundesregierung erklärt die IT-Sicherheit zum Querschnittsthema für die ganze digitale Gesellschaft; dazu soll auch die Zusammenarbeit und Unterstützung von DsiN ausgebaut werden. DsiN freut sich, diese Verantwortung zu übernehmen und möchte dafür

- weitere Unternehmen zur Aufklärungsarbeit motivieren und als Mitglieder für eine produktunabhängige und herstellernerneutrale Aufklärungsarbeit gewinnen.
- bestehende und künftige Initiativen der Wirtschaft bündeln, bedarfsweise koordinieren und als Plattform für Verbraucher in Abstimmung mit allen Partnern einfacher zugänglich zumachen.
- DsiN-eigene Angebote verstärken sowie auch die Zusammenarbeit mit Initiativen von Bund und Ländern wie beispielsweise die IT-Initiative „IT-Sicherheit in der Wirtschaft“ des BMWi verstärken.

Aufklärungsangebote bedarfsorientiert anpassen

Für eine wirksame Verbreitung der Aufklärungsarbeit

sind sicherheitsrelevante (Vor-)Kenntnisse und Verhaltensweisen der Verbraucher im Internet entscheidend. Dafür möchte DsiN künftig verstärkt

- sämtliche Handlungsversprechen und Projekte unter dem Dach von DsiN auf die vier Nutzertypen zuschneiden und bedarfsweise weiterentwickeln.
- Angebote des DsiN-Netzwerkes für Verbraucher auf dem DsiN-Webportal zugänglich machen.
- die Aufgeschlossenheit für die Sicherheit im Netz durch direkte und zielgruppengerechte Ansprachen im jeweiligen Lebensumfeld von Jugendlichen, Senioren und Familien verbessern.

Zusammenwirken aller Akteure vertiefen

Eine wirksame Aufklärungsarbeit gelingt nur im Zusammenwirken aller Akteure der digitalen Gesellschaft – Politik, Wissenschaft, Wirtschaft und Bildungswesen. Daher freuen wir uns über die zunehmende übergreifende Aufmerksamkeit für das Thema und unterstützen einen gemeinsamen Dialog für

- Innovationen im Austausch mit Wissenschaft und Bildung, um Dienste und Geräte für ein souveränes Verhalten im Netz nachhaltig anzupassen.
- mögliche Anreize zur Anwendung bestehender Sicherheitsmaßnahmen durch Verbraucher, um die Anwendung von Schutzmaßnahmen zu verbessern.
- eine breite bundesweite Aufklärungskampagne für mehr souveränes Verhalten im Netz im Verbund mit DsiN-Partnern und Trägern von Aufklärungsinitiativen.

DsiN-Index 2014

Digitale Sicherheitslage der Verbraucher in Deutschland

Die DsiN Sicherheitskriterien

BEDROHUNGSLAGE



IT-Sicherheitsvorfälle

40,1



Gefährdungsempfinden

27,3

SCHUTZNIVEAU



Bekanntheit von Schutzmaßnahmen

80



Nutzen von Schutzmaßnahmen

49

DIGITALE SICHERHEITSGEFÄLLE

60,2



44,2

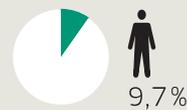
Fatalistische Nutzer



Wirkung von Schutzmaßnahmen erklären

45,8

Außenstehende Nutzer



Grundwissen praktikabel vermitteln

58,1

Gutgläubige Nutzer



Sensibilisieren und Umsetzungs-kompetenz stärken

72

Souveräne Nutzer



Kontinuierliche Aufklärungsarbeit

DIGITALE AUFKLÄRUNG 2.0

Sicherheitswissen praktikabel vermitteln - Umsetzungsbereitschaft und -kompetenz stärken
Sensibilisieren und Vertrauen aufbauen
Zusammenarbeit zwischen Politik, Wirtschaft, Wissenschaft und Gesellschaft verstärken

Abb. 28: DsiN-Index 2014

Glossar

Aufklärung 2.0	Um die digitale Sicherheitslage zu verbessern, werden Aufklärungsangebote stärker auf die Bedürfnisse der Verbraucher zugeschnitten – gemeinsam mit allen Stakeholdern.
Bedrohungsempfinden	Das von den deutschen Onlinern selbst eingeschätzte Risiko von Nutzung ausgesuchter Technologien und Anwendungen.
Bedrohungslage	Zusammenfassung der Faktoren sicherheitsrelevanter Vorfälle und Bedrohungsempfinden.
Der DsiN-Index	Die Sicherheitslage der deutschen Onliner in einer Zahl. Gewichteter Mittelwert aus den vier Faktoren Sicherheitsvorfälle, Bedrohungsempfinden, Bekanntheit und Nutzung von Schutzmaßnahmen.
DsiN-Nutzertypen	<p>Eine Clusterung der deutschen Onliner. Es gibt 4 Nutzertypen, die sich durch typische Verhaltensweisen auszeichnen.</p> <p>Außenstehende Nutzer: Haben im Vergleich zu den anderen Nutzergruppen deutliche Defizite bei der Kenntnis und der Nutzung von Schutzmaßnahmen.</p> <p>Fatalistische Nutzer: Sie unterlassen Sicherheitsmaßnahmen, obwohl sie Risiken und Schutzmaßnahmen überdurchschnittlich gut kennen, geringes Gefährdungsempfinden.</p> <p>Gutgläubige Nutzer: Sie verfügen über ein nur sehr gering ausgeprägtes Gefährdungsempfinden und nutzen Schutzmaßnahmen kaum.</p> <p>Souveräne Nutzer: Sie verfügen bereits über eine hohe Kompetenz und wenden Schutzmaßnahmen meist auch an.</p>
Indexpunkte	Der DsiN-Index wird auf einer Skala von 1 bis 100 gemessen. Der Wert 50 stellt dabei den Punkt dar, an dem die Sicherheitslage kippt.
Kenntnis von Schutzmaßnahmen	Selbstauskunft der Nutzer, ob sie bestimmte Schutzmaßnahmen kennen oder nicht.
Nutzung von Schutzmaßnahmen	Selbstauskunft der Nutzer, ob sie ausgesuchte Schutzmaßnahmen auch tatsächlich anwenden.
Sicherheitsvorfälle	Für die Sicherheit der Nutzer relevante Vorfälle, die von den Onlinern bemerkt wurden, z. B. Passwortdiebstahl, Virenbefall, o. ä.
Schutzniveau	Zusammenfassung von Kenntnis und Nutzung von Schutzmaßnahmen.
Schwellenwert	Bei Werten unter 50 Indexpunkten ist die Bedrohungslage höher als das Schutzniveau, bei Werten über 50 ist es umgekehrt.

Über DsiN

Die DsiN-Mission ist die Verbesserung des Sicherheitsbewusstseins und Verhaltens von Verbrauchern sowie kleinen und mittleren Unternehmen im Netz durch konkrete Hilfestellungen – im Verbund mit Unternehmen, Verbänden und Vereinen. Dafür bietet DsiN praktische Orientierungshilfen und Anleitungen. Als produktunabhängige Plattform für Aufklärungsinitiativen ist DsiN für neue Mitglieder offen.

In der Digitalen Agenda der Bundesregierung wurde ein Ausbau der Zusammenarbeit und Unterstützung von DsiN beschlossen. Schon heute verstärkt DsiN seine Aufklärungsarbeit: Für Verbraucher stehen Anleitungen zum souveränen digitalen Umgang im Netz im Mittelpunkt wie die Passwort Wechsel App für Verbraucher sowie das neue DsiN-Webportal.

Gegründet wurde DsiN als gemeinnütziger Verein im Nationalen IT-Gipfelprozess der Bundesregierung und steht seit 2007 unter der Schirmherrschaft des Bundesministeriums des Innern. DsiN möchte seine Aufklärungsarbeit im Dialog mit der Politik, der Wissenschaft und weiteren Akteuren der digitalen Gesellschaft weiter stärken.

Impressum

DsiN Index 2014 I Digitale Sicherheitslage der Verbraucher in Deutschland
Eine Studie von Deutschland sicher im Netz e.V.

Verantwortlich: Dr. Michael Littger

Redaktion: Tobias Weber (Autor, TNS Infratest), Dr. Heiko Dobel (Pflüger Rechtsforschung),
Peter Gerlicher (DsiN e.V.), Janis Oberlechner (TNS Infratest), Angelika Pelz (DsiN e.V.)

Studienpartner: TNS Infratest

Gestaltung: ideengut | Agentur für Kommunikation

Fotoquelle: fotolia: © Bacho, © goodluz, © tashka, Shotshop.com: © danstar

Oktober 2014

Deutschland sicher im Netz e.V.
Albrechtstr. 10 b
10117 Berlin
Telefon +49 30 27576 - 310
Telefax +49 30 2757651 - 310
www.sicher-im-netz.de
info@sicher-im-netz.de