

DAS DIGITALE ICH

SELBST- BESTIMMT SURFEN



Schirmherrschaft:



Bundesministerium
des Innern
und für Heimat



Deutschland
sicher im Netz

#

#dasDigitaleIch

#Datenschutz

#ElektronischerAusweis

#Identitätsdiebstahl

#digitalerNachlass

Das Digitale Ich selbstbestimmt surfen

Ob Sie eine Reise buchen, Produkte online bestellen, Suchmaschinen nutzen oder Beiträge in sozialen Netzwerken veröffentlichen: Sie hinterlassen Datenspuren. In Form von persönlichen Ausweisdaten, Kreditkarten- und Bankdaten oder mit Ihrer E-Mail-Adresse. Die Gesamtheit aller Daten, die Sie im Netz über sich hinterlassen, wird Digitales Ich genannt, auch digitale Identität. Erfahren Sie in diesem Ratgeber, wie Sie Ihr Digitales Ich im Netz selbstbestimmt gestalten und vor Identitätsdiebstahl schützen können. Sie erhalten Tipps zum Schutz Ihrer Daten, Informationen zum elektronischen Ausweisdokumenten und zum Umgang mit dem „digitalen Nachlass“.



Mehr Tipps und weiterführende Links erhalten Sie auf unseren Webseiten. Einfach QR-Code mit Ihrem Smartphone oder Tablet abfotografieren und mehr erfahren.

sicher-im-netz.de/das-digitale-ich-selbstbestimmt-surfen-0

Was meint ... das Digitale Ich?

- ... bezeichnet die Gesamtheit aller Onlinepräsenzen und -aktivitäten einer Person.
- ... basiert auf digitalen Daten, die einer realen Person zugeordnet werden können.
- ... bezeichnet das Bild, das ein Dritter von einem Nutzer oder einer Nutzerin im Wege der Onlineaktivitäten erhält.
- ... Digitale Identitätsmerkmale sind beispielsweise hinterlegte Daten in Benutzerkonten.
- ... ist die Gesamtheit aller nachvollziehbaren Aktivitäten im Internet wie Beiträge, Kommentare, Fotos, Standorte sowie persönliche Daten, Name, Beruf, Wohnort.
- ... kann missbräuchlich verwendet werden und ist deshalb besonders schutzbedürftig.



DsiN-Tipps

- ✓ Eigene Datenspuren kennen und ausfindig machen. Dazu zählen auch veröffentlichte Standorte, Bilder, Selfies und Texte.
- ✓ Bewusster entscheiden, welche privaten Informationen in welchem Kreis veröffentlicht werden, z. B. über Privatsphäre-Einstellungen der sozialen Netzwerke.
- ✓ Ziele für den Auftritt im Netz formulieren und entscheiden, welche Informationen im Netz veröffentlicht werden sollen.
- ✓ Zweck und Notwendigkeit vor Preisgabe persönlicher Daten im Netz daraufhin kritisch prüfen.
- ✓ Professionelle Hilfe sowie Angebote zur Kontrolle und zum Schutz Ihres Digitalen Ichs in Anspruch nehmen.



Mehr Tipps und weiterführende Links erhalten Sie auf unseren Webseiten. Einfach QR-Code mit Ihrem Smartphone oder Tablet abfotografieren und mehr erfahren.

sicher-im-netz.de/das-digitale-ich-selbstbestimmt-surfen

Was ist ... Datenschutz?



- ... bezeichnet den Schutz personenbezogener analoger sowie digitaler Daten, insbesondere vor unbefugtem Zugriff durch Dritte.
- ... bezweckt, dass natürliche Personen die Kontrolle über ihre eigenen Daten haben.
- ... umfasst alle Daten, die auf eine natürliche Person zurückzuführen sind und über die die Person eindeutig identifizierbar ist.
- ... zu personenbezogenen Daten zählen beispielsweise Name, Geburtsdatum, Adresse, Kontodaten aber auch die E-Mail-Adresse und Teile der IP-Adresse.
- ... regelt den Schutz besonders sensibler Daten, beispielsweise über die Gesundheit.
- ... wird gesetzlich in Europa einheitlich durch die Datenschutzgrundverordnung (DSGVO) geregelt.
- ... ist nicht gleichzusetzen mit Datensicherheit, die aber durch technische (nicht die rechtlichen) Maßnahmen zum Datenschutz beiträgt.

DsiN-Tipps

- ✓ Sparsam im Umgang und mit der Preisgabe von persönlichen Daten im Internet sein.
- ✓ Keine leichtfertige Weitergabe persönlicher Daten im Internet.
- ✓ Starke Passwörter mit Buchstaben, Zahlen und Sonderzeichen nutzen.
- ✓ Keine Passwörter wählen, die sich aus öffentlich zugänglichen Informationen erschließen lassen.
- ✓ Privatsphäre-Einstellungen nach Errichtung eines Benutzerkontos oder Profils individuell anpassen.
- ✓ Software-Updates durchführen und Anti-Viren Programme installieren.
- ✓ Digitale Kommunikation möglichst verschlüsselt nutzen, insbesondere für Messenger-Dienste als auch E-Mails.
- ✓ Beim Erhalt von E-Mails Absenderadresse, Rechtschreibung, Optik und Inhalt gründlich prüfen und bei Bedenken sofort löschen.
- ✓ Vorsicht gilt immer dann, wenn persönliche Daten in einer E-Mail abgefragt werden oder enthaltene Links auf Formulare führen, in denen Daten eingetragen werden sollen.



Mehr Tipps und weiterführende Links erhalten Sie auf unseren Webseiten. Einfach QR-Code mit Ihrem Smartphone oder Tablet abfotografieren und mehr erfahren.

sicher-im-netz.de/das-digitale-ich-datenschutz

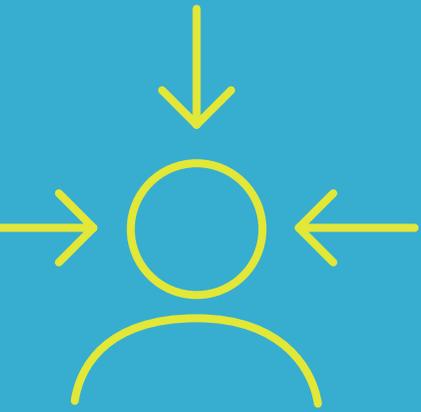
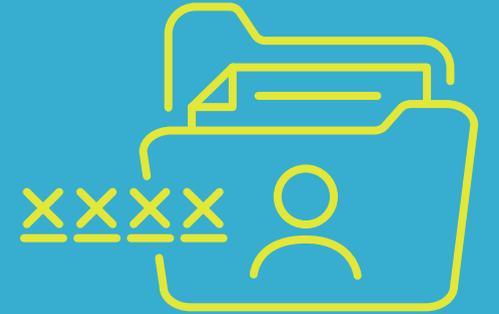
39%

haben sich noch nie mit ihrem Digitalen Ich befasst¹



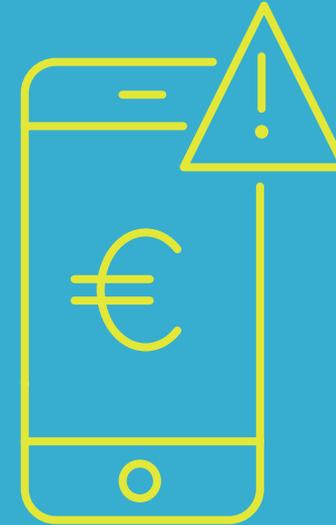
40%

haben ihren digitalen Nachlass geregelt²



75%

sehen die Verantwortung für ihre digitale Identität bei sich selbst¹



56%

fürchten Identitätsdiebstahl beim Online-Shopping¹

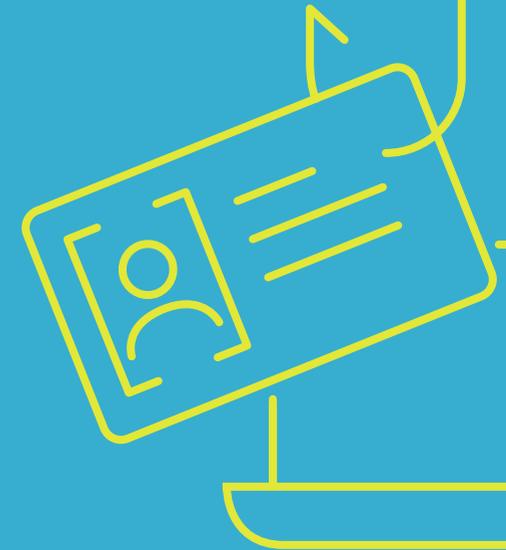
61%

sehen Missbrauch persönlicher Daten in sozialen Netzwerken als Risiko¹



24%

fürchten Identitätsbetrug bei staatlichen Dienstleistungen¹



¹ Q.: DsiN-Sicherheitsindex (2021)

² Q.: Bitkom-Studie zum Digitalen Nachlass (2021)

Was ist ... ein elektronischer Ausweis?

- ... bezeichnet die digitalisierte Form des gängigen Personalausweises im Chipkartenformat.
- ... wird auch „eID-Funktion“ genannt.
- ... ermöglicht es, einige Behördengänge, Anträge und geschäftliche Angelegenheiten digital zu erledigen.
- ... wird technisch über einen Chip auf dem analogen Personalausweis ermöglicht.
- ... steht jede:r Bürger:in, die im Besitz eines deutschen Personalausweises ist, zur Verfügung.
- ... für die Nutzung wird ein Ausweis, eine selbstgewählte sechsstellige PIN sowie ein Smartphone oder ein Kartenlesegerät benötigt.
- ... die Ausweisdaten werden immer Ende-zu-Ende-verschlüsselt übermittelt und können daher nicht abgefangen oder eingesehen werden.
- ... spart Zeit, Kosten und Wege.
- ... mit der Online-Ausweisfunktion können Nutzer:innen selbst festlegen, ob und wem die persönlichen Daten verschlüsselt übermittelt werden.



Tagesaktuelle
Sicherheitshinweise aufs
Smartphone liefert
die SiBa-App.

sicher-im-netz.de/sicherheitsbarometer

DsiN-Tipps

- ✓ Über Funktionen und Vorteile bei Beantragung eines Personalausweises und Nutzung der eID-Funktion informieren.
- ✓ Die „AusweisApp 2“ der Bundesregierung installieren.
- ✓ Prüfen, welche Unternehmen und Behörden Zugriff auf Daten erhalten dürfen.
- ✓ Wissen über Online-Ausweis mit Freunden und Familie teilen und bei der Nutzung unterstützen.



Mehr Tipps und weiterführende Links erhalten Sie auf unseren Webseiten. Einfach QR-Code mit Ihrem Smartphone oder Tablet abfotografieren und mehr erfahren.

sicher-im-netz.de/das-digitale-ich-elektronischer-ausweis

Was ist ... Identitätsdiebstahl?

- ... umfasst z.B. den Missbrauch von Daten im Internet.
- ... Angreifende sind an allen Arten von Zugangsdaten interessiert.
- ... gestohlen werden häufig Namen, Fotos und Adressen, aber auch Zahlungsinformationen wie Kreditkartendaten oder Telefonnummern.
- ... oft werden zunächst Daten gesammelt, später dann „Geschäftsmodelle“ zur illegalen Verwendung entwickelt.
- ... wird oft genutzt, um Waren unter falschen Namen und Adresse zu bestellen und liefern zu lassen.
- ... ein weiteres Szenario ist die gezielte Bedrohung und Erpressung von Personen.
- ... wird durch schlechte Absicherung von Benutzerkonten vereinfacht.
- ... Betroffene von Identitätsdiebstahl erfahren davon in der Regel erst, wenn unberechtigte Rechnungen oder Mahnungen zugestellt werden.



DsiN-Tipps

- ✓ Profile auf privat stellen.
- ✓ Sichereren Login mit einer 2-Faktor-Authentifizierung und einem starken Passwort einrichten.
- ✓ Fake-Profile an Betreiber von Webseiten oder sozialen Netzwerken melden.
- ✓ Nicht nachvollziehbaren Zahlungsaufforderungen und Rechnungen widersprechen, nicht ignorieren.
- ✓ Vorsicht vor Phishing: Nachricht auf Spam-Verdacht prüfen und ggf. sofort löschen.
- ✓ Banken, seriöse Händler und Dienstleister fordern nie via E-Mail oder SMS dazu auf, Daten, PINs oder Passwörter einzugeben.
- ✓ Bei Identitätsdiebstahl die Geschäftspartner informieren, um Missverständnisse und Betrug zu vermeiden.
- ✓ Polizei informieren und möglichst viele Beweise sichern.
- ✓ Im Notfall: Zentrale Sperrnotrufnummer 116 116 kontaktieren und betroffene Bankkarte, SIM-Karte, E-Personalausweis usw. sperren lassen.



Mehr Tipps und weiterführende Links erhalten Sie auf unseren Webseiten. Einfach QR-Code mit Ihrem Smartphone oder Tablet abfotografieren und mehr erfahren.

sicher-im-netz.de/das-digitale-ich-identitaetsdiebstahl

Was ist ... ein digitaler Nachlass?

- ... wird auch digitales Erbe oder digitales Testament genannt.
- ... beinhaltet alle Daten, die Internetnutzende zu Lebzeiten im Netz hinterlassen.
- ... dazu zählen Benutzerkonten, Profile in sozialen Netzwerken, Foreneinträge, Fotos, Mitgliedschaften, Verträge u. v. m.
- ... ist wie das Erbe von Gegenständen zu behandeln.
- ... sämtliche Rechte und Pflichten sowie die Nutzerdaten des/der Verstorbenen gehen auf die Erben über.



DsiN-Tipps

- ✓ Überblick über die eigenen Online-Aktivitäten verschaffen und dokumentieren.
- ✓ Dies geht gut über das Sortieren und Rückverfolgen des E-Mail-Postfachs, da i.d.R. alle Anmeldungen und Käufe mit einer E-Mail-Bestätigung abgeschlossen werden.
- ✓ Zudem eine Übersicht über alle Benutzerkonten mit den entsprechenden Zugängen erstellen und an einem sicheren Ort verwahren.
- ✓ Sensible Daten (Zugangsdaten, Passwörter) bei einer vertrauenswürdigen Person oder einem Notar hinterlegen.
- ✓ Die Daten dabei regelmäßig aktualisieren.
- ✓ Detailliert beschreiben, wie der digitale Nachlass verwaltet werden soll. Die Löschung der Benutzerkonten kann im Testament aufgenommen werden.
- ✓ Vollmacht erstellen, in der Sie festlegen, was nach dem Tod mit Ihren Benutzerkonten und- profilen, Abonnements, digitalen Gesundheitsdaten usw. passieren soll.

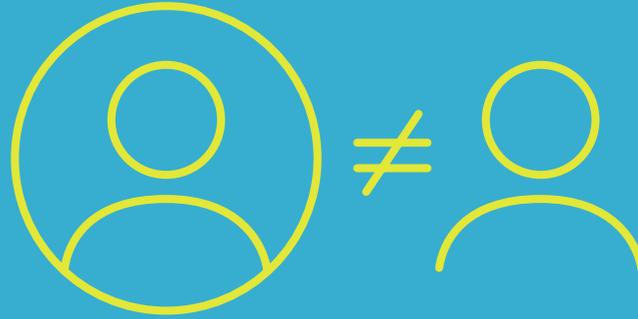


Mehr Tipps und weiterführende Links erhalten Sie auf unseren Webseiten. Einfach QR-Code mit Ihrem Smartphone oder Tablet abfotografieren und mehr erfahren.

sicher-im-netz.de/das-digitale-ich-digitaler-nachlass

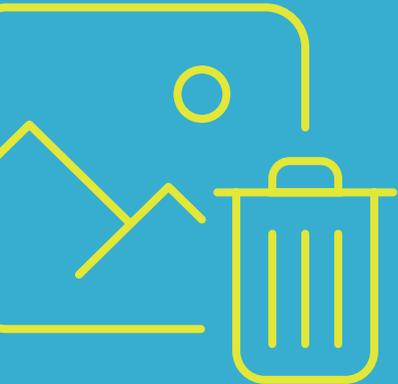
43%

der Befragten geben an, dass ihre Social-Media-Profile nicht ihr authentisches Selbst wiedergeben.



21%

gehen davon aus, dass ihre Social-Media-Konten nach ihrem Tod dauerhaft gelöscht werden.

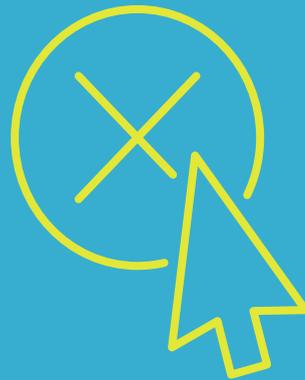


82%

der Befragten würden die eine oder andere Spur aus ihrer Internetpräsenz im Jahr 2021 dauerhaft löschen wollen.

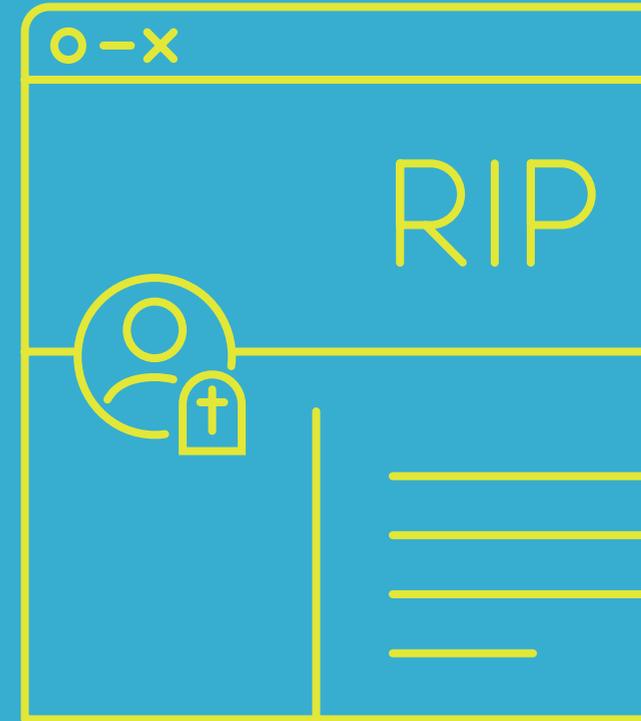
75%

der Befragten glauben, sie hätten die volle Kontrolle darüber, was sie aus ihrer Online-Präsenz löschen.



18%

möchten, dass ihre Social-Media-Präsenzen als Gedenkstätte erhalten bleiben.



Q.: Kaspersky-Studie „Das Recht auf Vergessen werden“ (2022)
<https://kas.pr/6zqf>

Was ist ... die DsiN-Ratgeberreihe?

Die DsiN-Ratgeberreihe erklärt einfach und verständlich die wichtigsten Begriffe rund um Sicherheit im Internet – von Algorithmus bis Zwei-Faktor-Authentisierung. Mit unseren DsiN-Tipps erhalten Sie praktische Handlungsempfehlungen für souveränes Surfen im Alltag. In weiterführenden Links finden Sie umfassende Informationen zu den jeweiligen Themen sowie Kontakte zu Beratungs- und Hilfsangeboten. So hilft die DsiN-Ratgeberreihe, das Internet für Sie, Ihre Familie und andere Menschen in Ihrem Umfeld sicherer zu machen.

Weitere Themen der DsiN-Ratgeberreihe:

- Belästigung im Netz – kompetent kontern
- Online einkaufen und bezahlen – sicher shoppen



Mehr Tipps und weiterführende Links erhalten Sie auf unseren Webseiten. Einfach QR-Code mit Ihrem Smartphone oder Tablet abfotografieren und mehr erfahren.

sicher-im-netz.de/ratgeberreihe

Immer auf dem Laufenden bleiben bei Digitalthemen und die eigenen Kompetenzen verbessern und zertifizieren lassen: mit den DiFü-News und dem DsiN-Digitalführerschein.

[difü.de](https://difue.de)

DAS DIGITALE ICH – SELBSTBESTIMMT SURFEN

Über DsiN

DsiN engagiert sich für Schutz, Sicherheit und Vertrauen in der digitalen Welt bei Verbraucher:Innen und im Mittelstand. Getragen von Unternehmen, Verbänden und zivilgesellschaftlichen Organisationen betreibt DsiN zahlreiche Projekte und Initiativen für digitale Souveränität und Selbstbestimmung im privaten und beruflichen Alltag. DsiN wurde im IT-Gipfel der Bundesregierung gegründet und fördert digitale Aufklärungsarbeit über Bildungs- und Dialogprojekte.

Mehr Infos finden Sie hier:



sicher-im-netz.de

Impressum

DsiN-Ratgeberreihe
Ausgabe 3: Das digitale Ich

Verantwortlich (V.i.S.d.P.):
Dr. Michael Littger

Redaktion:
Anne Schilling (Leitung)
Katharina Rychlik
Isabelle Rosière

Gestaltung:
KRAUT & KONFETTI, Berlin

Deutschland sicher im Netz e.V.
Albrechtstr. 10 c
10117 Berlin

Telefon +49 (0) 30 767 581-500
info@sicher-im-netz.de

In Zusammenarbeit mit

[bitkom](https://bitkom.org) [schufa](https://www.schufa.de)

