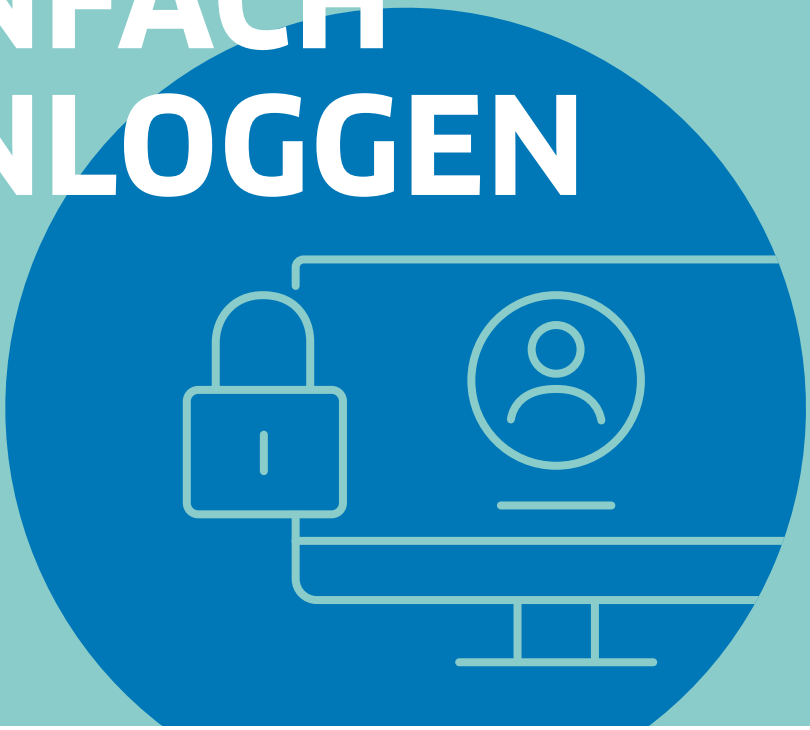
BENUTZER-KONTEN SICHERN

EINFACH EINLOGGEN



DsiN-Schirmherrschaft:

Bundesministerium des Innern und für Heimat

DsiN Deutschland sicher im Netz

#

#Login
#Passwortmüdigkeit
#Datenverlust
#Phishing
#Authentifizierungsmethoden
#Passwortmanager
#Sicherheitsschlüssel
(Security Key)

Benutzerkonten sichern – einfach einloggen

Unser Leben wird von Tag zu Tag digitaler. Täglich bewegen wir uns online in der digitalen Welt. Bei der Arbeit, mit unserem E-Mail-Konto, beim Online-Shopping, in der Nutzung von Social Media, Streaming Diensten oder Finanzdienstleistern. Bei all diesen Anwendungen, die wir nutzen, steht eine Funktion im Zentrum: Die einwandfreie Identifikation über einen Login („Anmeldung“), gebunden an ein Nutzerkonto. Häufig wird es mit dem englischen Begriff Account bezeichnet. Diese sind durch Login-Daten für uns zugänglich. In unserem Alltag nutzen wir diese Accounts geschäftlich oder privat für unterschiedlichste Zwecke. Sie sind unser Zugang zum digitalen Leben. Denn einmal eingeloggt, können wir im Netz kommunizieren und agieren. Worauf Sie achten müssen, um Ihre Logins sicher zu verwalten und welche Gefahren es gibt, erfahren Sie in diesem DsiN-Ratgeber.

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/benutzerkonten-sichern-einfach-einloggen

Was ist …
ein Login?

… als Login wird der Vorgang bezeichnet, sich in einem Computersystem oder einer Internetseite anzumelden (einzuloggen).

… besteht aus Anmeldedaten, die sich aus einem Benutzernamen und einem Passwort zusammensetzen.

… zusätzlich gibt es die Zwei-Faktor-Authentifizierung (2FA) und die Multi-Faktor-Authentifizierung (MFA), diese bieten eine ergänzende Absicherung Ihrer Logindaten
→ siehe Seite 14 / 15

… es dient dazu, die Nutzer:innen zu identifizieren und zu authentifizieren.

… kann missbräuchlich verwendet werden, um die eigene Identität zu stehlen und ist deshalb besonders schutzbedürftig.

DsiN-Tipps

- ✓ Verschiedene Account-Passwort-Kombinationen: Für sichere Zugänge ist es wichtig, die Kombination aus Accountnamen und unterschiedlichen Passwörtern zu verändern. Es empfiehlt sich deshalb verschiedene Passwörter einzusetzen und auch eine Variation von Accountnamen zu verwenden.
- ✓ Beim Login sensibler Vorgänge wie z. B. Onlinebanking auf eine sichere Verbindung achten: In der Adresszeile im Internetbrowser muss „https“ statt „http“ stehen. Durch das Schlosssymbol in der Adresszeile weist Sie der Internetbrowser zusätzlich auf eine verschlüsselte und damit sichere Verbindung hin.
- ✓ Wenden Sie eine Zwei-Faktor-Authentifizierung (2FA) oder eine Multi-Faktor-Authenitfizierung (MFA) an, sobald ein Online-Dienst dies ermöglicht.
  → siehe Seite 14 / 15
- ✓ Nutzen Sie dazu einen Passwortmanager. Dieser speichert mehrere Login-Dateien verschlüsselt ab und erspart das Merken oder Aufschreiben komplexer Zugänge.

Mehr Tipps und weiterführende Links erhalten Sie auf unserer Webseite DsiN.de. Einfach QR-Code mit Ihrem Smartphone oder Tablet abfotografieren und mehr erfahren.

sicher-im-netz.de/benutzerkonten-sichern-login

Was ist …
Passwortmüdigkeit?

… mit der Zeit häufen sich eine Vielzahl von unterschiedlichen Benutzerkonten und Logindaten an. Dabei kann schnell der Überblick verloren gehen.

… um die eigenen Passwörter nicht ständig zu vergessen, nutzen viele Menschen oft dasselbe Passwort für alle Anwendungen.

… viele Verbraucher:innen sind sich der Gefahrenlage zwar bewusst, aber durch Bequemlichkeit bleiben sie bei einfachen Passwörtern oder nutzen dasselbe Passwort für unterschiedliche Konten.

… ist ein Passwort einmal bekannt, ist es für Hacker:innen leicht, dieses bei anderen Diensten auszuprobieren. Auf diese Weise erhalten Kriminelle den Zugang zu vielen Logins der Betroffenen.

DsiN-Tipps

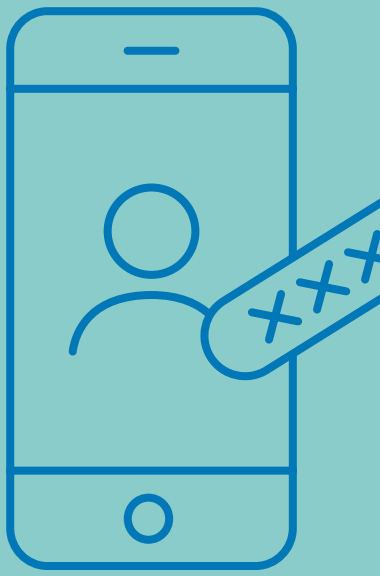
- ✓ Starke Passwörter mit Buchstaben, Zahlen und Sonderzeichen nutzen. Die Kombination kann leicht durch einen Passwort-Generator zufällig erstellt werden.
- ✓ Keine Passwörter wählen, die sich aus öffentlich zugänglichen Informationen erschließen lassen oder sehr allgemeine Wörter beinhalten z. B. „Liebe“, „Passwort“ etc.
- ✓ Zur Erstellung und Verwaltung von Login-Daten einen sicheren Passwortmanager verwenden.
- ✓ Alternativ darauf achten, dass Sie sich das Passwort merken können, z. B. mit einer Merksatzregel, bei der die jeweiligen Anfangsbuchstaben der Wörter eines Satzes aneinandergereiht werden.
- ✓ Nutzen Sie unsere DsiN-Passwortkarte: Diese erleichtert das Erstellen und Merken von komplexen Passwörtern.
- ✓ Ganz auf passwortlose Lösungen umstellen, um der Passwortmüdigkeit zu entgehen.
  → siehe Seite 14 / 15

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/benutzerkonten-sichern-passwortmuedigkeit

90 %

aller Verstöße im Internet sind auf gestohlene Anmelde-daten zurückzuführen.[1]



53,6 %

glauben, dass sie sich sowieso nicht gegen Datenmissbrauch schützen können.[2]

54,7 %

sehen die Verantwortung der Sicherheit von personenbezogenen Daten bei den Betreibern von Online-Diensten.[3]

10,6 %

waren bereits vom Ausspähen ihrer Zugangsdaten zu einem Onlineshop betroffen.[2]

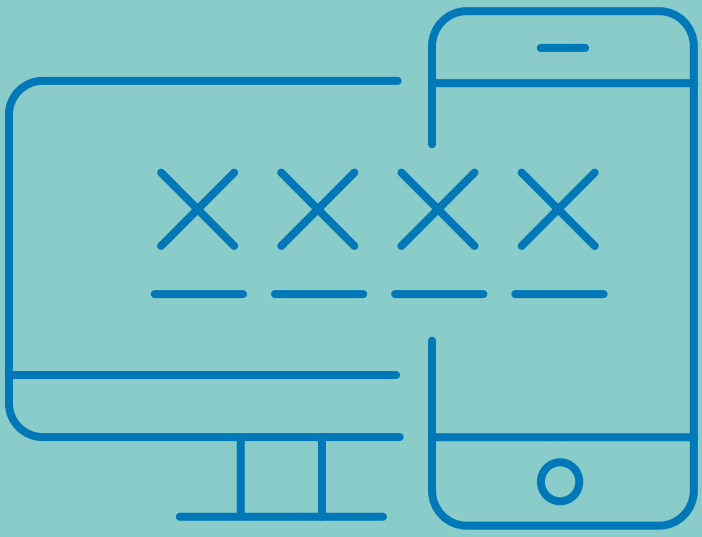
1 Q.: Blogartikel von Yubico zu den Ergebnissen der ersten Umfrage zum Stand der globalen Unternehmensauthentifizierung 2022: https://l.dsin.de/98

2 Q.: DsiN-Sicherheitsindex (2022): https://l.dsin.de/9a

3 Q.: DsiN-Sicherheitsindex (2021): https://l.dsin.de/9b

54 %

der Nutzer:innen geben an, Passwörter in mehreren Anwendungen wieder-zuverwenden.[4]



Schaden in den Jahren 2020/21 in Deutschland durch Cyber-Angriffe.[5]

Das meistgenutzte Passwort.[6]

35,3 %

finden Bequemlichkeit im Umgang wichtiger als Sicherheit und Datenschutz.[7]

4 Q.: “EMEA Remote Work Research Report 2021”, Yubico, 2021: https://l.dsin.de/9c
5 Q.: 220 Milliarden Euro Schaden durch Ransomware und andere Cyber-Angriffe | heise online: https://l.dsin.de/9d
6 Q.: Hasso-Plattner-Institut: https://l.dsin.de/9e
7 Q.: DsiN-Sicherheitsindex (2022): https://l.dsin.de/9f

Was ist …
Datenverlust?

- … bezeichnet das unvorhergesehene Verlorengehen von digitalen Daten.
- … Gründe hierfür können sein: menschliche Fehler, Virenbefall, Hacker:innenangriffe, Datendiebstahl oder technische Fehler.
- … das E-Mail-Konto bildet oftmals das Zentrum unserer digitalen Identität. Denn viele Dienste und Logins sind mit unserer E-Mail-Adresse verknüpft.
- … betroffen sind oft Shopping-Accounts mit sensiblen Bankdaten und Informationen zum Einkaufsverhalten, Bewerbungsunterlagen, Zeugnisse und Zertifikate, Abrechnungen, Kontoauszüge usw. Eine Kette des kompletten Kontrollverlustes kann so in Gang gesetzt werden.

DsiN-Tipps

- ✓ Speichern Sie Ihre Daten mit Hilfe von Back-Ups: Schützen Sie wichtige Daten offline auf Ihren lokalen Geräten, wie z. B. auf externen Festplatten oder USB-Sticks. Nutzen Sie sichere und verschlüsselte Cloud-Dienste. Besonders wichtig ist dies bei mobilen Geräten, die schnell verloren gehen können.
- ✓ Je wichtiger die Daten, desto mehr Sicherungen: Welche Daten sind Ihnen besonders wichtig? Diese sollten Sie im Zweifel mehrfach sichern und an unterschiedlichen Orten aufbewahren.
- ✓ Bleiben Sie über sicherheitsrelevante Vorfälle auf dem Laufenden: die SiBa-App (Sicherheitsbarometer) informiert über Bedrohungen im digitalen Alltag und gibt Tipps und Links, was im Falle eines Angriffs zu tun ist. Kostenlos zum Download im Google Playstore oder im Apple App Store.

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/benutzerkonten-sichern-datenverlust

Was ist …
Phishing?

- … Phishing („Passwort + Fishing“) bezeichnet den Versuch, dem Opfer gezielt Informationen wie z. B. Nutzerdaten zu entlocken oder zur Ausführung einer schädlichen Aktion zu bewegen. In der Folge werden dann z. B. Kontoplünderung oder Identitätsdiebstahl begangen oder auch eine Schadsoftware installiert.
- … erfolgt über schadhafte Anhänge oder Links in E-Mails, SMS und Chatnachrichten oder Telefonanrufe. Diese können sich je nach Aufwand an eine große Masse richten oder ganz gezielt eine bestimmte Person adressieren.
- … Social Engineering bezeichnet die Manipulation, Lügen und Irreführung von Internet-Opfern, um an Daten zu gelangen und wird oftmals unter Einsatz von Phishing durchgeführt.
- … bei einem Ransomware-Angriff handelt es sich auch um eine Phishing-Methode, bei der sich durch Anklicken eines unsicheren Links eine Schadsoftware installiert, die alle Daten auf einem IT-System verschlüsselt und erst gegen Zahlung eines Lösegeldes (engl. Ransom) entschlüsselt.
- … das Ziel von Phishing-Angriffen ist es, dass gestohlene Daten weiterverkauft oder häufig zum Abschließen von kostenpflichtigen Abos, Buchungen von Reisen oder Käufen im Internet genutzt werden.

DsiN-Tipps

- ✓ Ignorieren Sie verdächtige Mails, SMS oder Anrufe und öffnen Sie keine Anhänge oder Links.
- ✓ Phishing-Mails fallen oft mit ungewöhnlichen Rechtschreibfehlern, veraltetem Design oder verdrehten Formulierungen auf und sind häufig allgemein formuliert ohne persönliche Anrede.
- ✓ Aber Achtung: die Angriffsmethoden werden immer professioneller. Auch korrekte Angaben über Ihre Identität, Anschrift sowie Kreditkarteninformationen können betrügerisch sein. Bei Unverständnis oder Unstimmigkeiten nicht klicken oder den Vorgang fortsetzen, sondern umgehend nachforschen.
- ✓ Kontaktieren Sie den Anbieter (Bank etc.) eines Dienstes beispielsweise per Telefon, um die Anfrage zu überprüfen.

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

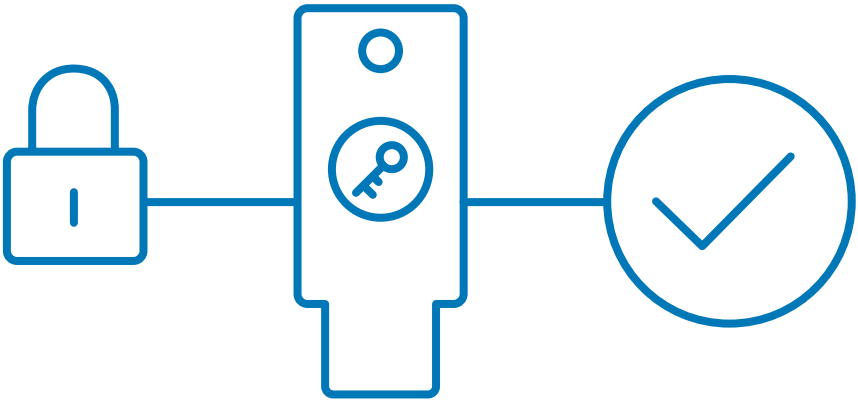
sicher-im-netz.de/benutzerkonten-sichern-phishing

Was sind …
Authentifizierungsmethoden?

… Authentifizierung ist die Bestätigung bzw. Beglaubigung Ihrer digitalen Identität, um digitale Prozesse freizuschalten, wie z. B. eine Banküberweisung oder bei einem Anmeldevorgang.

… Zwei-Faktor-Authentifizierung (2FA) oder auch Multi-Faktor-Authentifizierung (MFA) sind die gängigsten Methoden, um zusätzlich oder anstelle eines Passworts Ihre Online-Identität zu bestätigen. Der zweite Faktor wird mit Hilfe des Handys über biometrische Merkmale wie Fingerabdruck, Gesichtserkennung, Iris-Scan oder über einen physischen Sicherheitsschlüssel mit USB-Anschluss (Security Key) oder Smartcard erzeugt.

… der Trend geht zur Anmeldung ganz ohne Passwörter: Der sogenannte FIDO2-Standard ermöglicht es, passwortlos, mit einem physischen Sicherheitsschlüssel, einer Smartcard oder künftig auch integriert im Smartphone, eine Identitätsüberprüfung mit nachfolgender Anmeldung zu tätigen. → siehe Seite 18 / 19



DsiN-Tipps

- ✓ Voraussetzung für eine Zwei-Faktor-Authentifizierung (2FA) bzw. Multi-Faktor Authentifizierung (MFA) ist es, dass die Faktoren aus verschiedenen Kategorien stammen, also eine Kombination aus Wissen (z. B. Passwort, PIN), Besitz (z. B. Smartcard, TAN-Generator) oder Biometrie (z. B. Gesichtserkennung, Iris-Scan oder Fingerabdruck).
- ✓ Informieren Sie sich, ob Ihr Online-Dienst 2FA bzw. MFA unterstützt und nutzen Sie diese nach Möglichkeit.
- ✓ 2FA und MFA ermöglichen es Ihnen grundsätzlich auch bei Systemen, die nur schwache Passwörter unterstützen, vollständig geschützt zu sein.

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/benutzerkonten-sichern-authentifizierungsmethoden

Was ist …
ein Passwortmanager?

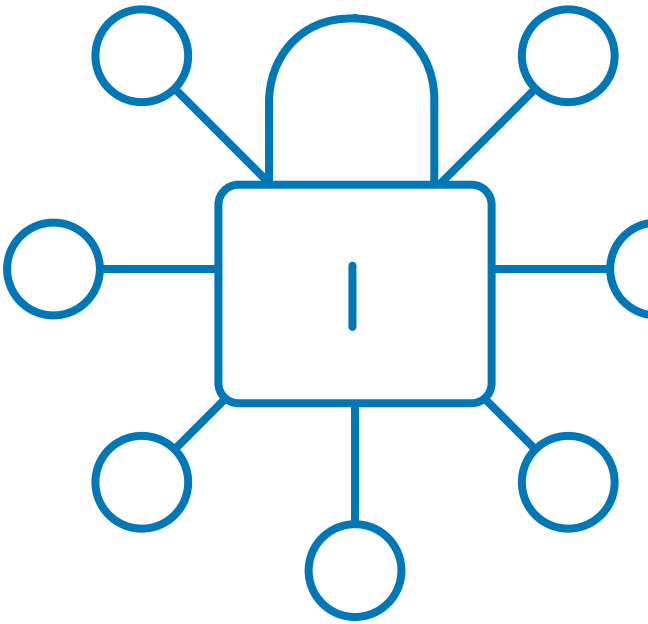
… ein Programm, mit dessen Hilfe Sie Passwörter erstellen, an einem sicheren Ort hinterlegen und schützen können.

… es wird zusätzlich mit einem Master-Passwort verschlüsselt.

… ist sowohl für alle handelsüblichen stationären Computer, Laptops und Mobiltelefone verfügbar.

… Vorteil eines Passwortmanagers ist, dass sich mit seiner Hilfe auch komplexe und damit sicherere Passwörter speichern lassen.

… alle Passwörter sind somit an einem Ort gespeichert und durch die komplexe Sicherheitsarchitektur der Anbieter von Passwortmanagern sehr gut geschützt.



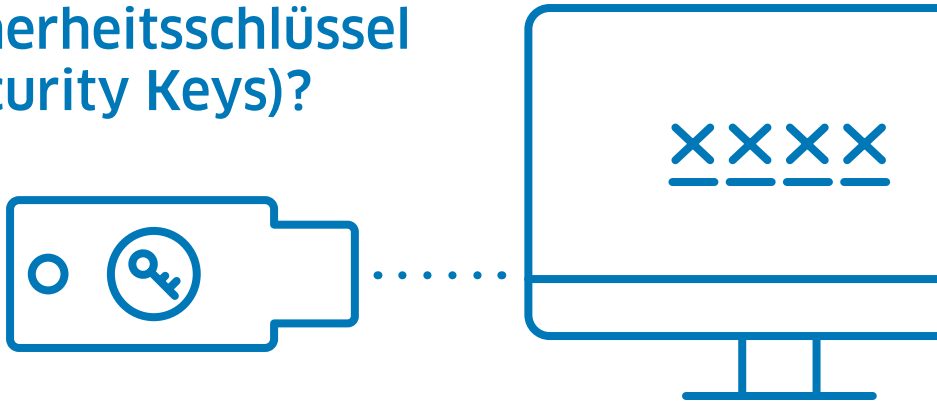
DsiN-Tipps

- ✓ Bei geteilten Accounts unter Freunden, im Büro oder der Familien ersparen Sie sich das unsichere Mitteilen eines Passworts per Messenger oder Handzettel.
- ✓ Auf Plattformen, welche 2FA nicht anbieten, kann durch den Passwortmanager die Sicherheit erhöht werden.
- ✓ Eine entscheidende Sicherheitsoption, die auch von vielen Passwortmanagern unterstützt wird, ist die Multi-Faktor-Authentifizierung (MFA) durch Security Keys wie z. B. YubiKey. → siehe Seite 18 / 19
- ✓ Geschützte, komplexe Passwörter müssen seltener ausgetauscht werden. Wir empfehlen den alljährlichen Sicheren-Login-Tag am 1. Februar zu nutzen, um einmal die Sicherheit Ihrer Accounts zu überprüfen und unsere DsiN-Tipps anzuwenden.
- ✓ Nutzen Sie die DsiN-Passwortkarte für das Master-Passwort für Ihren Passwortmanager.

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/benutzerkonten-sichern-passwortmanager

Was sind …
Sicherheitsschlüssel (Security Keys)?



… sind eine der sichersten Methoden, die Zugänge für Ihre Accounts und Logins zu schützen.

… lassen sich über einen USB-Anschluss mit dem Computer verbinden. Über die Methode NFC (Near Field Communication) wird der Sicherheitsschlüssel manuell durch Heranhalten an PC, Laptop, Mobiltelefon oder Tablet angewendet.

… wie gewohnt, werden die Anmeldedaten über den Browser eingegeben. Das System fragt nach einem weiteren Faktor, in diesem Fall kann der Sicherheitsschlüssel verwendet werden. Durch die manuelle Verbindung mit dem Security Key authentifizieren Sie sich.

… durch diesen Prozess können Hacker:innen selbst mit einem erbeuteten Passwort nicht auf die 2FA bzw. MFA geschützten Accounts zugreifen, da der persönliche Sicherheitsschlüssel fehlt. So bleiben die Daten sicher, auch bei ausgereiften Phishing-Methoden.

… Sicherheitsschlüssel brauchen keine Internetverbindung oder Empfang und funktionieren ohne eigene Energiequelle bzw. Batterie. Die Security Keys können nicht von Unberechtigten entschlüsselt werden.

DsiN-Tipps

- ✓ Informieren Sie sich, welcher Sicherheitsschlüssel für Ihren Gebrauch geeignet ist. Die meisten bieten bereits Verschlüsselungen für die gängigen Plattform-Dienste, E-Mail-Provider, Zahlungs-Apps oder auch sozialen Medien an.
- ✓ Achten Sie darauf, welchen Anschluss Ihr Gerät hat. Während die meisten PCs etwa USB Typ A nutzen (breit und nur einseitig nutzbar), sind neuere Laptops und Tablets mit USB Typ C ausgestattet (schmaler und beidseitig nutzbar) oder kontaktlos über NFC.
- ✓ Bewahren Sie den Sicherheitsschlüssel an einem sicheren Ort auf.
- ✓ Wir empfehlen dort, wo es möglich ist, die Nutzung eines Sicherheitsschlüssels, da diese eine höhere Sicherheit vor Phishing-Angriffen bieten.

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/benutzerkonten-sichern-sicherheitsschluessel

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
- → Das Digitale Ich – selbstbestimmt surfen
- → Onlinebanking – zeitgemäß zahlen

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

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 5: Benutzerkonten sichern – einfach einloggen

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

Redaktion:
Katharina Rychlik (Leitung)
Anna-Leona Bösl

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: yubico

SICHER-IM-NETZ.DE/RATGEBERREIHE