ONLINE-BANKING

ZEITGEMÄSS ZAHLEN

DsiN-Schirmherrschaft:

Bundesministerium des Innern und für Heimat

DsiN Deutschland sicher im Netz

#

#Passwort
#PIN
#ZweiFaktorAuthentifizierung
#TAN
#Phishing
#3DSecureVerfahren
#MobileBanking

Onlinebanking – zeitgemäß zahlen

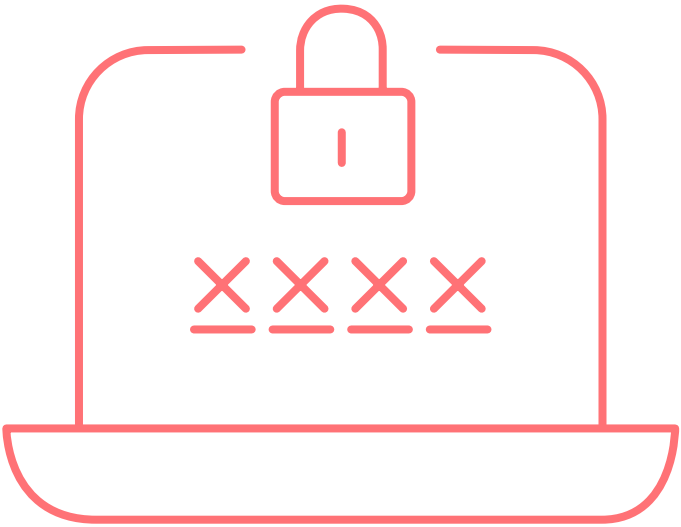
Über die letzten Jahre hat sich unser Konsumverhalten stark verändert – nicht zuletzt bedingt durch die Corona-Pandemie. Der Einkauf im Internet und auf Online-Marktplätzen gehört inzwischen zum Alltag, ebenso das digitale Bezahlen an der Ladenkasse per Karte oder Smartphone. Viele Banken bieten mittlerweile Onlinebanking an. Zudem gibt es mobile Banken, die sich auf digitales Banking spezialisieren. Dennoch sind einige Verbraucher:innen weiterhin skeptisch gegenüber Onlinebanking und haben Bedenken hinsichtlich Sicherheits- und Datenschutzmaßnahmen. Worauf Sie achten müssen und wie Sie Onlinebanking sicher nutzen, verrät Ihnen dieser DsiN-Ratgeber.

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

sicher-im-netz.de/onlinebanking

Was ist …
ein Passwort / eine PIN?

- … beides ermöglicht in Kombination mit einem Benutzernamen bzw. Anmeldenamen den Zugang zu Ihrem Onlinebanking-Konto.
- … durch die Kombination von Zahlen, Sonderzeichen, Klein- und Großbuchstaben wird Ihr Passwort sicherer.
- … Passwörter werden an einen Server übertragen und können bei der Übertragung abgefangen oder von einem Server gestohlen werden.
- … häufig wird daher eine PIN (persönliche Identifikationsnummer) beim Onlinebanking verwendet. Diese wird lokal auf dem Gerät gespeichert und weder übertragen noch auf dem Server gespeichert.
- … Geldinstitute senden häufig eine PIN aus Sicherheitsgründen per Post an Ihre Anschrift.



DsiN-Tipps

- ✓ Wählen Sie für jeden Dienst ein eigenes Passwort, das aus Buchstaben, Zahlen und Sonderzeichen besteht.
- ✓ Namen, Geburtsdaten und weitere von Dritten einfach nachvollziehbare Informationen sind bei der Passwortvergabe nicht zu empfehlen.
- ✓ Wenn Sie Ihre Zugangsdaten auf Papier notieren, verwahren Sie diese verschlossen und sicher auf.
- ✓ Nutzen Sie unsere DsiN-Passwort-Karte. Diese erleichtert das Merken und Erstellen von komplexen Passwörtern.
- ✓ Verzichten Sie auf digitale Geräte von Dritten, um sich in Ihrem Onlinebanking-Konto anzumelden.
- ✓ Sicheres Übertragen der Daten wird z. B. durch das Schlosssymbol in der Browserzeile und durch die Bezeichnung https:// gewährleistet.

Mehr Tipps, weiterführende Links und die kostenfreie Bestellung einer DsiN-Passwortkarte erhalten Sie auf unseren Webseiten von sicher-im-netz.de. Einfach QR-Code mit Ihrem Smartphone oder Tablet abfotografieren und mehr erfahren.

sicher-im-netz.de/onlinebanking-passwort-pin

Was ist …
Zwei-Faktor-Authentifizierung (2FA)?

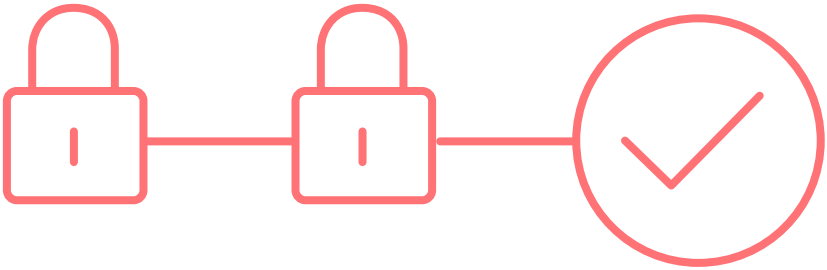
… dient zur zusätzlichen Identifikation nach einer Passworteingabe und ermöglicht einen sicheren Ablauf bei mobilem Banking.

… schützt doppelt vor fremdem Zugriff: Gelangt Ihr Passwort oder Ihre PIN in falsche Hände, sind Ihre sensiblen Daten dennoch gut gesichert, da ein zweiter Faktor zur Authentifizierung notwendig ist.

… wird bei einem Anmeldevorgang oder bei einer Online-Transaktion (z. B. einer Online-Überweisung) eingesetzt.

… als zweiter Faktor zu einem Passwort oder einer PIN kommt häufig das TAN-Verfahren zum Einsatz.
→ siehe Seite 6 / 7

… andere zweite Faktoren können auch biometrische Merkmale in Form des Fingerabdrucks sein.



DsiN-Tipps

- ✓ Wichtig ist, dass die Faktoren dabei aus verschiedenen Kategorien stammen, also eine Kombination aus Wissen (z. B. Passwort, PIN), Besitz (z. B. Chipkarte, TAN-Generator) oder Biometrie (z. B. Fingerabdruck).
- ✓ Wenden Sie eine Zwei-Faktor-Authentifizierung an, sobald ein Online-Dienst dies ermöglicht.
- ✓ Speichern Sie die Notfall Nummer Ihrer Bank in Ihrem Mobiltelefon um bei unbefugten Zugriff die Karte und das Konto möglichst schnell sperren zu können.

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

sicher-im-netz.de/onlinebanking-zwei-faktor-authentifizierung

Was ist …
eine TAN?

… wird auch als Zwei-Faktor-Authentifizierung (2FA) oder doppelte Authentifizierung bezeichnet.
→ siehe Seite 4

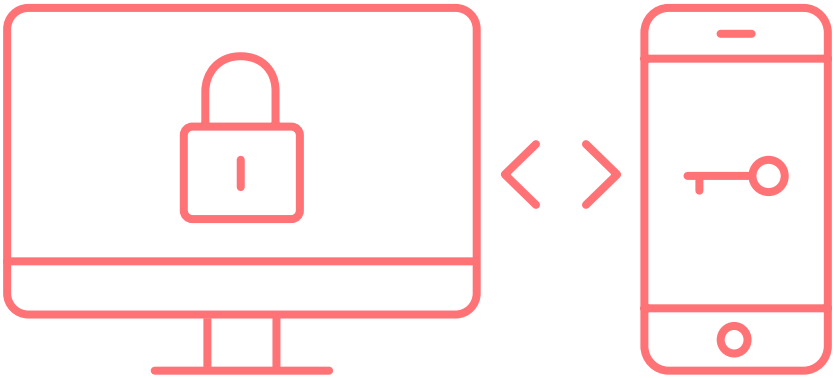
… eine TAN (**T**rans**A**ktions**N**ummer) wird häufig als zweiter Faktor zur Authentifizierung genutzt, z. B. für das Einrichten eines Dauerauftrags oder einer Überweisung.

… ist nur einmal gültig sowie aus Sicherheitsgründen nur einige Minuten nutzbar.

… ersetzt die physische Unterschrift des Auftraggebers bzw. Kontoinhabers in der Bank und ermöglicht so ein sicheres Onlinebanking.

… erschwert Identitätsdiebstähle oder Phishing-Angriffe.

… kann auf verschiedenen Wegen generiert werden. Je nach Bankzugehörigkeit stehen unterschiedliche Verfahren zur Verfügung: pushTan, photoTan, chipTan.



DsiN-Tipps

- ✓ Erfragen Sie die möglichen TAN-Verfahren bei Ihrer Bank.
- ✓ Entscheidend ist, dass niemand die TAN auf dem Weg von der Bank zu Ihnen und zurück auslesen oder missbrauchen kann.
- ✓ Als weniger sicher gilt das smsTAN-Verfahren. Die zur Authentifizierung verschickten SMS-Nachrichten können unter Umständen von Kriminellen abgefangen oder umgeleitet werden. Das zuständige Bundesamt BSI empfiehlt, auf dieses Verfahren zu verzichten.

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

sicher-im-netz.de/onlinebanking-tan-verfahren

Was ist …
Phishing?

… bezeichnet kriminelle Aktivitäten im Internet, bei denen Verbraucher:innen gezielt getäuscht und betrogen werden.

… Hacker:innen setzen gezielt auf die detailgetreue Nachahmung von E-Mails und Webseiten von bekannten Anbietern – z.B. Banken. Sie erhalten eine gefälschte E-Mail, die Links zu gefälschten Webseiten oder Pop-Up-Fenstern beinhaltet. Dort werden Sie unter einem Vorwand dazu aufgefordert, Zugangsdaten einzugeben.

… gestohlene Daten von Opfern werden von Kriminellen häufig zum Abschließen von kostenpflichtigen Abos, Buchungen von Reisen oder Käufen im Internet genutzt.

DsiN-Tipps

- ✓ Banken fordern niemals sensible Daten per E-Mail, Telefon oder SMS an.
- ✓ Phishing-Mails fallen oft mit ungewöhnlichen Rechtschreibfehlern oder verdrehten Formulierungen auf.
- ✓ Wenn Sie an der Echtheit einer E-Mail zweifeln, reagieren Sie nicht auf die E-Mail, sondern kontaktieren Sie Ihre Bank persönlich oder per Telefon, um die Anfrage zu überprüfen.
- ✓ Unseriöse Nachrichten sind oft allgemein formuliert und enthalten meist keine persönliche Anrede.

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

sicher-im-netz.de/onlinebanking-phishing

91 %

der Onlinebanking-Nutzenden halten Online-banking für sicher [1]

36,6 %

halten Onlinebanking für gefährlich [2]

56,4 %

tätigen Bankgeschäfte online [2]

58,5 %

achten auf verschlüsselte Datenverbindung beim Onlinebanking & Online-shopping [2]

76 %

der 16 bis 29-Jährigen nutzen Smartphone-Banking [1]

64 %

greifen auf Mobile-Banking zurück [3]

1 Q.: Bitkom-Studie (2021), Digital Finance- wie die Digitalisierung die Finanzbranche verändert: https://www.bitkom.org/sites/default/files/2021-06/bitkom-prasentation-digital-finance-09-06-2021_final_.pdf

2 Q.: DsiN-Sicherheitsindex (2022), Studie von Deutschland sicher im Netz e.V. zur digitalen Sicherheitslage von Verbraucher: https://www.sicher-im-netz.de/file/13898/download?token=xQQauU9G

3 Q.: Statista-Studie, Anteil der Nutzer von Online-Banking in Deutschland bis (2021): https://l.dsin.de/5c

Was ist …
ein 3D-Secure-Verfahren?

… ein von internationalen Kreditkartenunternehmen entwickeltes Authentifizierungsverfahren, das Kund:innen im Online-Handel ermöglicht, sich zu identifizieren um eine mit der Karte verbundene Zahlung freizugeben.

… kann auch außerhalb von Zahlungen zur Authentifizierung eines Karteninhabers genutzt werden, z. B. zur Identitätsverifizierung beim Hinzufügen neuer Karten in einer Bezahl-App.

… erfordert zur Nutzung eine einmalige Registrierung bei der Bank.

… bietet zusätzliche Sicherheit beim Onlineshopping mit Kreditkarte.

… wird eine Zahlung nicht mit 3D-Secure abgesichert, kann diese wie bisher unter alleiniger Angabe von PIN, Name des Karteninhabers, Gültigkeitsdatum und CVC freigegeben werden.

… Kund:innen können nicht beeinflussen, ob Zahlungen mit oder ohne 3D-Secure authentifiziert werden. Dies entscheiden die Banken selbst.

DsiN-Tipps

- ✓ Bei Zahlung per Kreditkarte sollten Sie darauf achten, dass die Kreditkartendaten nur verschlüsselt übermittelt werden. Dies erkennen Sie, wenn die Adresszeile im Browser mit **https** beginnt.
- ✓ Erkundigen Sie sich bei Ihrer Bank, ob das 3D-Secure-Verfahren angeboten wird und lassen Sie sich dafür registrieren.
- ✓ Bei Banktransaktionen von unterwegs besser mobile Daten als ein öffentliches WLAN oder einen Hotspot nutzen. Bei der Nutzung eines WLANs von unterwegs raten wir zu einer zusätzlichen Nutzung eines VPN (Virtuelles Privates Netzwerk).
- ✓ Abbuchungen über betrügerische Kreditkartentransaktionen können innerhalb von acht Wochen zurückgefordert werden. Checken Sie regelmäßig Ihre Kreditkartenabrechnungen!

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

sicher-im-netz.de/onlinebanking-3D-secure-verfahren

Was ist …
Mobile Banking?

… ermöglicht das mobile Abwickeln von Bankgeschäften.

… Banken bieten Onlinebanking-Anwendungen für das Smartphone (Banking-Apps) an, die es ermöglichen, Bankgeschäfte und Überweisungen mit mobilen Geräten wie Smartphones oder Tablets auszuführen.

… zusätzlich gibt es Banken, die sich auf Mobile Banking und digitale Finanzdienstleistungen spezialisieren, sogenannte Digitalbanken. Diese sind genauso sicher wie traditionelle Banken.

… das Eröffnen oder Freischalten von Onlinebanking-Diensten ist häufig schnell erledigt und kann online oder in einer Filiale beantragt werden.

… die genutzten Daten für Mobile Banking unterliegen dem Datenschutz (DSGVO) und sind durch Verschlüsselungen, PIN, TAN Codes und Zwei-Faktor-Authentifizierung gesichert.
→ siehe Seiten 2 bis 7

… 64 Prozent der Nutzer:innen greifen bei der Abwicklung von Bankgeschäften auf Mobile Banking zurück.
→ siehe Seite 10 bis 11

DsiN-Tipps

- ✓ Halten Sie das Betriebssystem Ihres Smartphones auf dem aktuellen Stand. Machen Sie regelmäßige Updates.
- ✓ Installieren Sie die Banking-App nur von vertrauenswürdigen Quellen, wie z. B. in Ihrem bekannten App-Store und achten Sie darauf, dass Sie immer die aktuelle Version der App installiert haben.
- ✓ Bevor Sie die App schließen, nutzen Sie den Button **Logout** oder **Abmelden**.
- ✓ Nutzen Sie die Sperrfunktion Ihres mobilen Gerätes.
- ✓ Führen Sie mobile Transaktionen möglichst nicht über ein öffentlich zugängliches WLAN aus.
- ✓ Bluetooth, NFC und WLAN nur bei Gebrauch aktivieren, um es Angreifern zu erschweren eine Verbindung zum Endgerät aufzubauen.

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

sicher-im-netz.de/onlinebanking-mobilebanking

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

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 4: Onlinebanking – zeitgemäß zahlen

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

Redaktion:
Katharina Rychlik (Leitung)
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: N26

SICHER-IM-NETZ.DE/RATGEBERREIHE