

Selbstdatenschutz!

Tipps zum sicheren Passwort





Der Handel mit persönlichen Daten ist ein Milliardengeschäft – leider auch für Cyberkriminelle: Der Diebstahl digitaler Identitäten ist enorm angestiegen. Daher sind sichere Passwörter zum Schutz von persönlichen, sensiblen oder gar intimen

Informationen im Netz wichtiger denn je. Dennoch lauteten nach einer Untersuchung des Hasso-Plattner-Instituts (HPI) im Jahr 2021 die meistgenutzten Passwörter in Deutschland „123456“ und „password“. Während jeder Mensch im analogen Leben die Haustüre abschließt, gehen viele Nutzerinnen und Nutzer online mit ihrem Schlüssel – dem Passwort –

sorglos um und lassen auf diese Weise ihre Datentüre weit offenstehen.

Mit dem Heft „Selbstdatenschutz! Tipps zum sicheren Passwort“ geben wir Ihnen alltagstaugliche Tipps und Tricks bei der Wahl der richtigen Passwörter für ihre Accounts an die Hand.

Ich wünsche Ihnen einen hilfreichen Erkenntnisgewinn für die Wahl Ihrer nächsten Passwörter.

Dr. Thorsten Schmiege

Präsident der Bayerischen Landeszentrale für neue Medien (BLM)

Warum sind Passwörter so wichtig?

Beispiel 1 „Konto gehackt?“

Sie haben nicht viel eingekauft und trotzdem leert sich Ihr Bankkonto? Konto- und Kreditkarten-Daten können durch Leichtsinnsinn oder gezielte Hacker-Angriffe in falsche Hände geraten. Dann werden z.B. Zahlungen umgeleitet oder Bestellungen auf Kosten anderer Leute getätigt.

Verwenden Sie sichere Passwörter und schauen Sie genau hin, bevor Sie Ihre Konto- und Kreditkarten-Daten im Internet verwenden und überprüfen Sie Ihre Kontoauszüge.

Beispiel 2 „Smartphone geklaut!“

Datendiebstahl passiert nicht nur online. Daten können auch abgerufen werden bei Gerätediebstahl oder bei Abwesenheit (etwa am Arbeitsplatz).

Schützen Sie sich mit sicheren Passwörtern vor teuren Handyrechnungen oder Bestellungen auf Ihre Kosten.

Passwörter und Zugangssperren sind leicht eingerichtet und schnell geändert.



Warum brauchen wir sichere Passwörter?

Ob bei der Smartphone-Nutzung, beim Online-Banking, beim E-Mailen oder beim Shoppen im Netz man benötigt immer ein Passwort.

Häufig verwenden wir als Passwort eine Zahlenfolge oder einen Eigennamen ergänzt mit einer Zahl oder einem Ausrufezeichen. Viel zu häufig nutzen wir dasselbe Passwort für verschiedene Accounts, um uns das Passwort leichter merken zu können. Das ist verständlich aber auch leichtsinnig.



Die Daten, die mit Passwörtern geschützt werden, sind Bank- und Kontodaten, Fotos auf dem Handy, Kalenderdaten und vieles mehr. Diese zu schützen, ist wichtig.

Selbstdatenschutz ist hier das Schlagwort: Jeder sollte sich selbst um den Schutz seiner Daten kümmern und sie mit sicheren Passwörtern vor unbefugter Nutzung durch Dritte schützen.

Absolute Sicherheit gibt es nicht!

Kein Passwort kann absolute Sicherheit bieten. Zu vielfältig sind die immer neuen Möglichkeiten des missbräuchlichen digitalen Datenzugriffs.

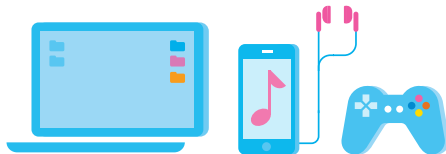
Durch einen **optimierten Selbstdatenschutz** können jedoch Risiken verringert werden. Voraussetzung ist ein Bewusstsein dafür, in welcher Form Gefahren im analogen sowie im digitalen Alltag lauern.

Ein Post-it mit dem Passwort an den PC zu kleben, ist unvorsichtig.



Welchen Gefahren bei der Passwort-Eingabe sind wir ausgesetzt?

- Einfache und beliebte Passwörter wie „123456“ oder „Hallo“ können leicht **erraten** werden.
- Immer das gleiche Passwort bei verschiedenen Diensten zu verwenden, kann den Zugang zu umfangreichen sensiblen Daten **erleichtern**.
- Der **Blick über die Schulter** („Shoulder-Surfing“) kann zum Ausspähen des Passwortes z.B. bei der Eingabe am Bankautomat oder beim Kartenlesegerät im Supermarkt führen.
- Das „Abfischen“ („**Phishing**“) von Passwörtern erfolgt über vermeintlich bekannte, aber lediglich nachgebildete Webseiten.



- **Keylogger** können bei der Eingabe eines Passwortes die Anschläge auf der Tastatur oder dem Bildschirm registrieren.
- Mit der **Brute-Force-Methode** werden Millionen Passwort-Kombinationen in kürzester Zeit digital ausprobiert.
- Mit **Wörterbuch-Angriffen** werden bestimmte Passwort-Listen automatisiert nach bestimmten Vorlieben abgearbeitet (z.B. Listen für Tierliebhaber, Mediziner, Filmfans).

Was ist beim Online-Banking zu beachten?

- EC- und Kreditkarten-PIN **nie ungeschützt** aufbewahren oder speichern, keinesfalls an Dritte weitergeben und bei der Eingabe am Automaten oder Kartenterminal **immer verdecken**.



- Nutzen Sie fürs Online-Banking nur die **eigenen Endgeräte** und das **eigene Netzwerk** (bei WLAN eine WAP2-verschlüsselte Verbindung).

- Beachten Sie bei der Wahl der PIN für den Zugang zum Online-Banking die Anforderungen an ein **sicheres Passwort**.
- Geben Sie die Web-Adresse per Hand ein (Vorsicht **Phishing**-Seiten: kein Aufruf der Bankseiten über Suchmaschinen). Achten Sie auf eine verschlüsselte Datenübertragung „**https://**“ bzw. „**Schloss Symbol**“.



Beispiel „https“ und „Schloss-Symbol“ im Mozilla Firefox-Browser

8

Welche Zugangssperren für digitale Geräte sind möglich?

Schließen Sie nicht nur die Haustüre ab, sondern versehen Sie auch alle digitalen Geräte mit einer Zugangssperre.



Boot-Sperre

ist aktiv vor dem Hochfahren des Geräts.
Sicherung durch PIN, Passwort oder Fingerabdruck-Scanner

Display-Sperre bzw. Sperrbildschirm

ist aktiv nach dem Hochfahren und nach Inaktivität des Geräts.
Sicherung durch PIN, Passwort oder Fingerabdruck-Scanner oder Tastatur-Muster

PIN-Schutz der SIM-Karte

ist aktiv bei Ausschalten des Geräts oder bei Entwenden der SIM-Karte aus dem Gerät.
Sicherung durch PIN

Welche Sicherheitsstufen bieten die Zugangssperren?

Es gibt verschiedene Sicherheitsstufen bei Zugangssperren, je nachdem welche Zugangshindernisse eingerichtet werden.



Geringe bis mittlere Sicherheit

Unterschrift auf dem Display des Handys,
Muster auf dem Bildschirm streichen

Mittlere Sicherheit

Geheimzahl, PIN (Persönliche Identifikationsnummer), oft nur vierstellige Zahlenkombination

Höhere Sicherheit

Passwort/Kennwort: Buchstaben-, Zahlen- und Zeichenkombinationen, höhere Sicherheit bei Beachtung der Regeln für ein sicheres Passwort

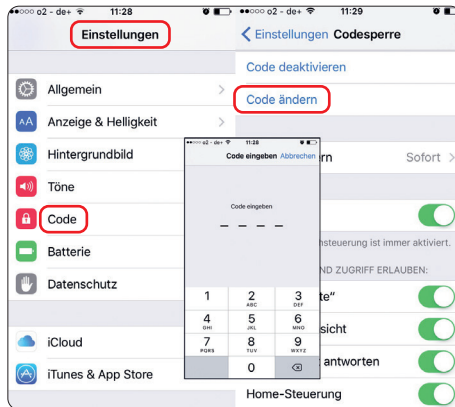
Wie richtet man technische Zugangssperren für mobile Geräte ein?

Um zu verhindern, dass Fremde Zugriff auf mobile Geräte erlangen können, sollten Zugangssperren eingerichtet werden.

Beispiel: Smartphone mit iOS Betriebssystem

Über den Button „**Einstellungen**“ kann unter der Kategorie „**Code**“ ein Zahlencode als technische Zugangssperre für den Bildschirm eingegeben werden.

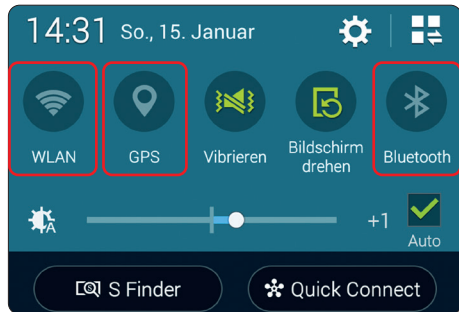
In der Broschüre „**Selbstdatenschutz! – Tipps, Tricks und Klicks**“, abrufbar unter www.blm.de, findet sich ein Beispiel zum Einrichten einer Display-Sperre bzw. eines Sperrbildschirms mit Android Betriebssystem.



Technische Zugangssperre
im iOS Betriebssystem verwalten

Was ist bei Verlust mobiler Geräte zu unternehmen?

- Aktivierte **Bluetooth-Funktion** oder **Ortungsdienste** (Mobilfunk oder GPS) zum Auffinden, Sperren oder Löschen des mobilen Geräts im näheren Umkreis nutzen
Achtung: Die Bluetooth-Funktion und die Ortungsdienste sollten in der Regel aus Gründen des Selbst Datenschutzes **deaktiviert** sein, wenn sie nicht genutzt werden
- **Passwörter** schnell **ändern**
- **SIM-Karte** über den Mobilfunkanbieter **sperren**
- **Polizei** unter Angabe der Seriennummer des mobilen Geräts über Verlust **informieren** (die Seriennummer findet sich auf der Verpackung, Kaufbeleg, Produktgehäuse oder teilweise in synchronisierten Programmen).



WLAN, GPS und Bluetooth deaktiviert;
kann durch Antippen aktiviert werden

Wie sichert man den Zugang zu E-Mail-Programmen?

Beispiel: E-Mail-Programm GMX

Klicken Sie auf „**Start**“ und auf „**Mein Account**“.
Auf der linken Seite auf „**Sicherheit**“ und anschließend unter „**Passwort**“ auf „**Passwort ändern**“ klicken.

Gefahren bei ungenügend gesicherten E-Mail-Programmen:

- unbefugter Zugriff auf geschäftliche und private Korrespondenz
- Identitätsdiebstahl
- Versand von Viren an vorhandene Kontakte über E-Mail-Programme

The screenshot shows the GMX Kundencenter interface. At the top right, there are three icons: a home icon labeled 'Start', an envelope icon labeled 'E-Mail', and a person icon labeled 'Adressbuch'. The 'Start' icon is circled in red. On the left side, there is a navigation menu with the following items: 'GMX Mein Account' (circled in red), 'Persönliche Daten', 'Sicherheit' (circled in red and highlighted with a blue bar), 'Meine Verträge', 'Vertrag kündigen', 'Vertrag widerrufen', 'Meine Zahlungsdaten', 'Meine Rechnungen', 'Meine Dokumente', 'Tarifwechsel & Produkte', 'Privatsphäre', 'Account löschen', and 'Hilfe & Kontakt'. The main content area is titled 'Sicherheit' and contains a 'Passwort' section with the text 'Zuletzt geändert:'. Below this, there is a 'Passwort ändern' button circled in red. At the bottom of the main content area, there is an 'E-Mail-Kontaktadresse' section with the text 'Wenn Sie Ihr Passwort vergessen zurücksetzen.'

Sicherheitseinstellungen im E-Mail-Programm GMX verwalten

Tricks zur Gestaltung starker Passwörter

Tricks, um sich sichere Passwörter leichter zu merken (Tricks können auch kombiniert werden):

Trick 1: Anfangsbuchstaben eines Satzes verwenden (Satz-Methode)

Beispiel: Aus einem Zitat aus Goethes Faust
 „**M**ein **s**chönes **F**räulein, **d**arf **i**ch **w**agen,
Meinen **A**rm **u**nd **G**eleit **I**hr **a**nzutragen?“
 wird: **MsF,diw,MAuGla?**

Trick 2: Buchstaben durch Zeichen und Zahlen ersetzen (Zeichen-Methode)

Beispiel: Aus Spaghettisauce wird mit
 s = ?; a = 3 und t = !: **?p3ghe!!i?3uce**

Trick 3: Buchstaben eines Satzes durch benachbarte Buchstaben auf der Tastatur ersetzen (Vertippt-Methode):

Jeden dritten Buchstaben nach rechts oben vertippen.

Beispiel: Aus Pferdeanhänger wird:
ßfe5deWnh+ng4r

Trick 4: Wörter aneinanderreihen (Wortketten-Methode)

Beispiel: **TanzZAHN&LiftSeehund**

Trick 5: Wörter aus verschiedenen Sprachen mischen (Fremdsprachen-Methode)

Beispiel: **sugercubesMERCIE!lachenlaudere**

Tipps zur Erstellung und zum Umgang mit sicheren Passwörtern

- Je länger das Passwort, umso sicherer: mindestens 10 Zeichen (WLAN-Passwort mindestens 20 Zeichen)
- Unvorhersehbare Kombinationen: Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
- Keine Eigennamen, Geburtsdaten, Tastaturabfolgen, ABC- und Zahlenreihen verwenden
- Nicht in unbekanntem Umgebungen einloggen (z.B. offene Netzwerke, Internet-Cafés)
- Passwort regelmäßig wechseln und nicht erneut alte Passwörter nutzen
- Passwörter nicht auf den Geräten oder im Browser speichern
- Passwörter nicht an andere weitergeben
- Zum Einkaufen über das Internet für Kundenkonto ein sicheres Passwort verwenden
- E-Mail-Postfach besonders schützen
- Pro Dienst/Account unterschiedliche Passwörter wählen



Impressum

Herausgeber

Bayerische Landeszentrale
für neue Medien (BLM)

Verantwortlich

Verena Weigand

Konzeption/Redaktion

Dr. Kristina Hopf

Autoren

Dr. Olaf Selg, Dr. Daniel Hajok
Arbeitsgemeinschaft Kindheit,
Jugend und neue Medien
(AKJM, www.akjm.de, info@akjm.de)

Layout/Illustration

Mellon Design GmbH

Copyright

Bayerische Landeszentrale
für neue Medien (BLM)

Stand 2017, geänderte Auflage 2022

Weiterführende Informationen

Broschüre „Selbstdatenschutz! – Tipps, Tricks und Klicks“



Abrufbar unter

www.blm.de



Überreicht von:

Stiftung 
Medienpädagogik
 Bayern

Bayerische Landeszentrale für neue Medien • Rechtsfähige Anstalt des öffentlichen Rechts
Heinrich-Lübke-Straße 27 • 81737 München • Tel. +49 (0)89 63808-278 • Fax +49 (0)89 63808-290
blm@blm.de • www.blm.de