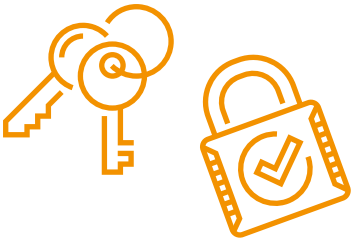

Passwörter

Die Schlüssel für Ihr digitales Zuhause.

Unsere privaten Bereiche schützen wir durch Schloss und Schlüssel. Wir versperren unsere Wohnungstür, das Auto und sichern das Fahrrad.

Ähnlich wie ein Schlüssel für Ihre Wohnungstür, schützen sichere Passwörter Ihr digitales Eigentum und Ihre Privatsphäre.

Das Benutzerkonto

In der digitalen Welt werden Zugangsberechtigungen z.B. für E-Mail, Online-Banking, Online-Shopping und Soziale Netzwerke durch ein Benutzerkonto (**Account**) geregelt. Um Zutritt zu bekommen, müssen im Anmeldevorgang (**Login**) der Benutzername und das Passwort (**Kennwort**) bekanntgegeben werden.

Die 10 schlechtesten Passwörter

1. 123456
2. passwort
3. abc123
4. qwertz
5. iloveyou
6. hello
7. football
8. welcome
9. 111111
10. hallo123

Genauso wie es leicht zu knackende Schlösser gibt, gibt es auch unsichere Passwörter. Daher sollten Sie bei der Vergabe einige Sicherheitshinweise beachten.

Tipps zur Erstellung eines guten Passwortes

+ Wählen Sie ein möglichst langes Passwort (wenn möglich mehr als zehn Zeichen).
+ Verwenden Sie Groß- und Kleinbuchstaben.
+ Variieren Sie Buchstaben, Zahlen und **Sonderzeichen**.
+ Erstellen Sie ein kryptisches Passwort.

- Vermeiden Sie Wiederholungen oder **Tastaturmuster**.
- Verwenden Sie keine einfachen Buchstaben- oder Zahlenfolgen wie „1234“ oder „abcd“.
- Verwenden Sie keine Namen, egal ob von Tieren, Menschen, Städten oder Dingen.
- Verwenden Sie keine Postleitzahlen, Telefonnummern oder Geburtstage (auch nicht in abgeänderter Form).

Bundesministerium Arbeit, Soziales, Gesundheit und Konsumentenschutz
oiat
digitaleseniorInnen

Fett gedruckte Begriffe siehe letzte Seite.

Passwörter

Tipps

Das ist im Umgang mit Passwörtern zu beachten

- Nutzen Sie für jedes Online-Konto ein anderes Passwort.
- Nutzen Sie einen **Passwort-Manager** für die Verwendung unterschiedlicher Passwörter.
- Ändern Sie Passwörter regelmäßig.
- Achten Sie bei der Eingabe des Passwortes darauf, dass Ihnen niemand über die Schulter sieht.
- Speichern Sie Ihre Passwörter nicht auf einem Klebezettel am Monitor oder unverschlüsselt auf der Festplatte des Computers.

Das kryptische Passwort

Besonders schwer zu knacken sind kryptische Passwörter.

Denken Sie sich einen für Sie einprägsamen Satz aus. Verwenden Sie die Anfangsbuchstaben.	*MFssO16idG* ***M****ein* ***F****ahrrad* ***s****teht* ***s****eit* ***O****ktober 20****16*** ***i****n* ***d****er* ***G****arage.*
Erzeugen Sie einen Satz, der keinen Sinn ergibt, ersetzen Sie Umlaute und fügen Sie Sonderzeichen hinzu.	*Elefantenregen*flUEstern§W€ihnachten!*
Überlegen Sie sich einen Satz, der nur für Sie eine Bedeutung hat.	*IchbinnochnieineinemrotenFerarrigefahren.*

Fett gedruckte Begriffe siehe letzte Seite.

Bundesministerium Arbeit, Soziales, Gesundheit und Konsumentenschutz
oiat
digitaleseniorInnen

Passwörter

Passwort-Manager

Passwort-Manager

Ein Passwort-Manager kann Ihnen helfen, Passwörter zu erzeugen und zu verwalten. Ihre Passwörter werden in einer zentralen Datenbank gespeichert, die mit einem Master-Passwort gesichert ist. Dieses ist zugleich das einzige, das Sie sich merken müssen. Das ist in etwa so, als würden Sie Ihre Schlüsselsammlung in einen gut gesicherten Safe legen, zu dem nur Sie Zutritt haben.

Zwei-Faktor-Authentifizierung

Im Optimalfall erhöht der Anbieter den Schutz des Passwort-Managers durch eine **Zwei-Faktor-Authentifizierung**. Das ist ein zusätzlicher Schritt bei der Anmeldung. Beispielsweise benötigen Sie neben Ihrem Benutzernamen und dem Passwort die Eingabe eines Einmal-Codes, der per SMS an Ihr Mobiltelefon gesendet wird.

Es gibt kostenlose und kostenpflichtige Passwort-Manager.

TIPP:
Nutzen Sie vor Abo-Abschluss die Demoversionen bzw. Testphasen unterschiedlicher Passwort-Manager.

Sicher ist sicher?!

Denken Sie daran, dass nur Sie Zugang zu Ihren passwortgeschützten Online-Aktivitäten haben und sorgen Sie vor, was im Falle Ihres Todes mit Ihrem **digitalen Nachlass** passieren soll und wer Zugriff darauf haben darf. Eine Möglichkeit besteht in der Nennung eines Notfallkontaktes im Passwort-Manager.

Fett gedruckte Begriffe siehe letzte Seite.

Bundesministerium Arbeit, Soziales, Gesundheit und Konsumentenschutz
oiat
digitaleseniorInnen

Passwörter

Begriffserklärungen

Account: oder auch User Account, engl. für Benutzerkonto. Über das Benutzerkonto werden die Zugangsberechtigungen zu einem geschützten Bereich geregelt.

Login: Anmeldung zu einem passwortgeschützten Bereich. In der Regel erfolgt dies unter Angabe eines Benutzernamens und Passwortes. Der Vorgang wird auch als Einloggen bezeichnet.

Kennwort: anderes Wort für Passwort, manchmal auch mit PWD abgekürzt (engl. Password).

Passwort-Manager: ist ein Programm mit dem Sie alle Ihre Zugangsdaten (Onlinekonten, Username und Kennwort) verwalten, speichern und in der Regel auch sichere Passwörter per Zufallsgenerator generieren lassen können. Das Programm wird mit einem starken Haupt-kennwort, dem Master-Passwort gesichert. Passwort-Manager werden auch Passwort-Safe oder Kennwort-Tresor genannt.

Passwortgenerator: erstellt Passwörter nach definierten Kriterien (Länge, Verwendung von Sonderzeichen, etc.).

Sonderzeichen: sind Schriftzeichen, die weder Buchstaben noch Ziffern sind. (§, &, ?, €, @, ...).

Tastaturmuster: sind Tastenkombinationen, die einem Muster auf der Tastatur folgen (qwertz).

Zwei-Faktor-Authentifizierung: dient zur Feststellung der Identität durch zwei Komponenten, wie z.B. Bankomatkarte und Pin (=Zahlenkombination), oder Login-Daten (Benutzername und Passwort) und zusätzlicher Einmal-Code per SMS.

Digitaler Nachlass: als digitaler Nachlass werden alle Daten bezeichnet, die nach dem Tod einer Person im Internet weiter bestehen. Dazu zählen E-Mail-Konten, Online-Zugänge, Profile in Sozialen Netzwerken, Blogs, Webseiten, usw.

Links Passwort Manager

LastPass – https://www.lastpass.com/de

Dashlane – https://www.dashlane.com/de

Enpass – https://www.enpass.io/

Bundesministerium Arbeit, Soziales, Gesundheit und Konsumentenschutz
oiat
digitaleseniorInnen