Passwort-Verwaltung am Smartphone

Die Umstellung vieler Serviceleistungen auf Online-Dienste bringt eine neue Herausforderung mit sich: unterschiedliche Passwörter müssen erstellt und im Gedächtnis behalten werden. Dieses Infoblatt bietet eine Übersicht über Möglichkeiten, Passwörter am Smartphone zu verwalten, zu speichern und einzusehen.

Automatischer Passwort Manager über Google Konto, Internet Browser

- Passwörter verwalten und Passwort-Optionen über **Google Konto:** „Google Konto verwalten" (kleines rundes Symbol, rechts oben) – „mein Konto" – „Sicherheit" – „Passwortmanager" – Einstellung (kleines Zahnrad) –
    - Speichern von Passwörtern anbieten (Android und Chrome) aktivieren
    - Automatische Anmeldung
    - Passwörter exportieren

  Saferinternet: Schritt für Schritt Anleitung

- Passwörter verwalten und Passwort-Optionen über **Google Chrome:**

  Automatisches Speichern aktivieren:
  Chrome App öffnen – Dreipunkt Menü, rechts oben, öffnen – „Einstellungen" – „Passwörter" – „Automatisch anmelden" aktivieren

  Passwörter ansehen/löschen/exportieren:
  Chrome App öffnen – Dreipunkt Menü öffnen, rechts oben – „Einstellungen" – „Passwörter"

    - Ansehen: unter Passwörter (blaue Schrift) finden sich alle Webseiten, wo Passwörter bereits gespeichert sind. Mit Klick auf die Webseite sind Nutzername und Passwort einsehbar (Klick auf das Augensymbol).
    - Löschen: Klick auf den Papierkorb.
    - Exportieren: Dreipunkt Menü öffnen, rechts oben – Passwörter exportieren.

  Anmelden mit gespeichertem Passwort:
    - Chrome füllt das Anmeldefeld automatisch aus.

- Bei mehr als einem gespeicherten Nutzernamen und Passwort: Chrome listet die gespeicherten Nutzernamen auf und es benötigt eine Auswahl des_der Nutzer_in.
- Auswahl des Schlüsselsymbols und Auswahl des Passworts.

Anleitung: Passwort verwalten in Google Chrome

- Passwörter speichern in den **Browsern Google Chrome, Microsoft Edge, Mozilla Firefox, Internet Explorer, Opera**

  https://praxistipps.chip.de/kennwoerter-speichern-so-gehts-in-allen-browsern_94093

Passwort Manager

Passwort-Manager vereinfachen die Verwaltung von unterschiedlichen Passwörtern und sind meist als App erhältlich. Mit einem Master-Passwort werden alle gespeicherten Passwörter geschützt. Der Blogbeitrag von privacytutor informiert umfassend über weitere Vorteile von Passwort-Manager. Die Tabelle enthält eine Auswahl an kostenlosen und deutschsprachigen Apps:

- **KeePass**

Grundfunktion	• Kostenfrei, Open-Source
Leistung	• Nicht Cloud-basiert: Die PW werden in einer Datei abgespeichert (Datei-Endung .kdbx), diese wird gut verschlüsselt und kann überall gespeichert werden. • Synchronisation mit anderen Geräten. • **QuickUnlock:** mit den letzten drei Zeichen des Master-PW kann die Datenbank entsperrt werden. Diese Funktion kann für einen bestimmten Zeitraum aktiviert werden, endet aber automatisch, wenn die App beendet wird bzw. nach einer falschen Eingabe. • Entsperren mit Fingerdruck • Individueller Passwortgenerator
Nachteil	• Passwörter werden am Gerät gespeichert und nicht in einer Cloud. → Gerät sollte nicht verloren gehen.
Tool-Link	• https://keepass.info/
Weitere Details:	https://www.datenschutz.org/keepass/ Mobilsicher: Ratgeber und Schritt für Schritt Anleitung

- **Dashlane**

Grundfunktion	• cloud-basiert
Leistung	• Tutorial zu Beginn • Hinterlegung eines Notfallkontakts, um Master-Passwort wiederherzustellen • intuitive und benutzerfreundliche Bedienung • Speicherung von Bankkonten und Adressen möglich
Nachteil	• Kostenfreie Version: Nutzung nur auf einem Gerät (keine automatische Synchronisierung zwischen mehreren Geräten) und max. 50 PW
Tool-Link	https://www.dashlane.com/de
Weitere Details:	https://www.experte.de/passwort-manager/dashlane

- **Lastpass**

Grundfunktion	• cloud-basiert
Leistung	• Bei Anmeldung per Mail und Bestätigung des Standorts freischalten • Einfache Bedienung • Passwort Generator • Sicherheitstest • Zuweisung eines Notfallkontakts • Master-Passwort kann wiederhergestellt werden • Speichern von Notizen, Zahlungsmethoden möglich • Ver- und Entschlüsselung auf Geräte-Ebene
Nachteil	• Desktop App nur für Mac • Sehr viele englische Phrasen
Tool-Link	https://www.lastpass.com/de/
Weitere Details:	https://www.experte.de/passwort-manager/lastpass

- **Bitwarden**

Grundfunktion	• cloud-basiert
Leistung	• Mobile App für Windows, Android, iOS • Hohe Benutzungsfreundlichkeit • Ordnerstruktur • Einfache Suchfunktion • Kostenlose Synchronisation für alle Geräte • Open Source • Speichern von Kreditkarte, Adressen, Notizen möglich
Nachteil	• Lokaler Betrieb mit eigenem Server • Geringere Verlässlichkeit bei Auto-Fill Funktion bei der mobilen Version • Support nur auf Englisch
Tool-Link	https://bitwarden.com/#organizations
Weitere Details:	https://www.chip.de/downloads/Bitwarden-Passwort-Manager_135079747.html https://www.experte.de/passwort-manager/bitwarden