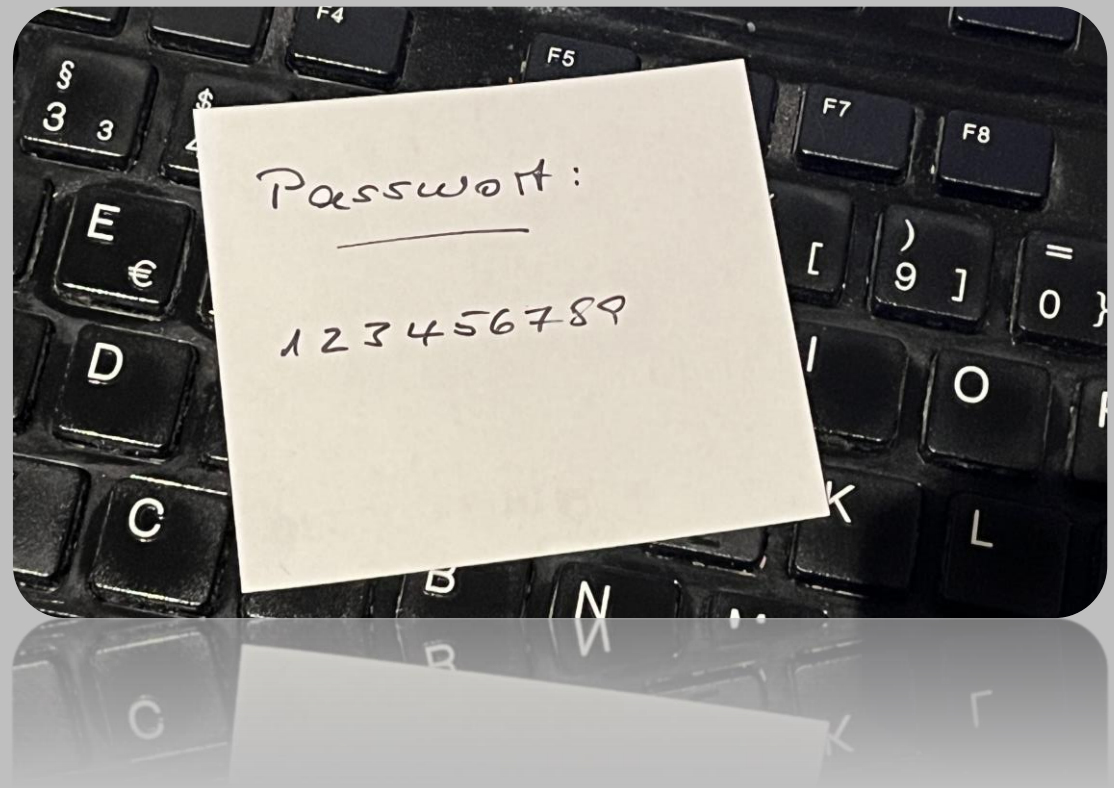
Tipps zum Umgang mit Passwörtern

Wie erstelle ich sichere und dennoch leicht merkbare Passwörter,
und wie kann ich sie verwalten?

© Clemens Braun - Internetcafé 55plus-Südwerk

die beliebtesten Passwörter 2023

1. 123456789
2. 12345678
3. hallo
4. 1234567890
5. 1234567
6. password



Gemeinsamkeiten:
sehr leicht zu merken, aber extrem unsicher

Quelle: Hasso Plattner Institut

die Bedeutung des Passwortes

- Authentifizierung
- Zugriffskontrolle
- Datenschutz
- Netzwerk-Sicherheit
- Geräte-Sicherheit
- Verhinderung von Missbrauch

die Bedeutung des Passwortes im Zeitverlauf

- lange Zeit einzige Sicherheitsebene (1-Wege-Authentifizierung)
- 2-Wege-Authentifizierung
  - zusätzliche Sicherheitsebene
  - SMS-Code, Authentifizierungs-App, biometrische Daten
- Passkey
  - sehr neue Entwicklung
  - funktioniert ohne Passwort
  - hat das Potential, das Passwort überflüssig zu machen

Grundprinzipien sicherer Passwörter

- Länge: mindestens 12, besser 16-20 Zeichen
- Komplexität: Kombination aus Groß- und Kleinbuchstaben, Zahlen & Sonderzeichen
- nicht verwenden:
  - Wörter, die in einem Wörterbuch stehen
  - persönliche Informationen (Namen, Geburtsdatum, Telefonnummer o.ä.)
  - bloße Zahlen- oder Buchstabenfolgen (12345…, abcdef…)
  - Reihe benachbarter Tasten auf der Tastatur (qwertz…)
  - „deutsche“ Zeichen (Umlaute, „ß“)
- Einzigartigkeit: für jedes Konto ein eigenes Passwort

Erstellung leicht merkbarer Passwörter

Akronym-Methode:

- Verwenden Sie die ersten Buchstaben der Worte eines Satzes, den Sie sich leicht merken können:
  - Songzeile
  - erster oder letzter Satz Ihres Lieblingsbuches
  - selbst ausgedachter Satz
- Beispiel:
  - Ich stehe nie vor 6:00 Uhr auf

Erstellung leicht merkbarer Passwörter

Akronym-Methode:

- Verwenden Sie die ersten Buchstaben der Worte eines Satzes, den Sie sich leicht merken können:
  - Songzeile
  - erster oder letzter Satz Ihres Lieblingsbuches
  - selbst ausgedachter Satz
- Beispiele:
  - Ich stehe nie vor 6:00 Uhr auf => Isnv6:00Ua
  - Wir haben 3 Töchter: Eva, Maria und Sophie. => Wh3T:E,MuS
  - Ich gehe mindestens 2 Mal/Woche ins Fitness-Studio => Igm2x/WiF-S

Erstellung leicht merkbarer Passwörter

weitere Methoden:

- Satz-Methode

  Beispiel: „Mein zweites Auto war ein Käfer.“ => Mein2.AutowareinKäfer.

- Leetspeak-Methode:

  Beispiel: „Marie-Luise“ => M@r13-Lu1s3

- Doppelwort-Methode:

  Beispiel: „Apfelsaft“ und „Orangentee“ => Apsa+Orte

Erstellung leicht merkbarer Passwörter

Meine Empfehlung:

Verwenden Sie die Akronym-Technik:

- diese Methode ist die am weitesten verbreitete
- Sie stellt einen guten Kompromiss dar zwischen
  - Sicherheit
  - leichter Merkbarkeit

Aber:

wie ist das dann mit dem Thema „einzigartiges Passwort je Account"?

Erstellung leicht merkbarer Passwörter

Individualisierung Ihrer Passwörter je Account

Beispiel:

für Google: Isnv6:00Ua + Go = Isnv6:00UaGo
oder GoIsnv6:00Ua

Nachteil: ein „Go“ kann als ein Hinweis auf Google verstanden werden

Erstellung leicht merkbarer Passwörter

Individualisierung Ihrer Passwörter je Account

Beispiel:

für Google: lsnv6:00Ua + Go => Ho = lsnv6:00UaHo

oder HoIsnv6:00Ua

Der erste Buchstabe wird durch den im Alphabet folgenden Buchstaben ersetzt.

Erstellung leicht merkbarer Passwörter

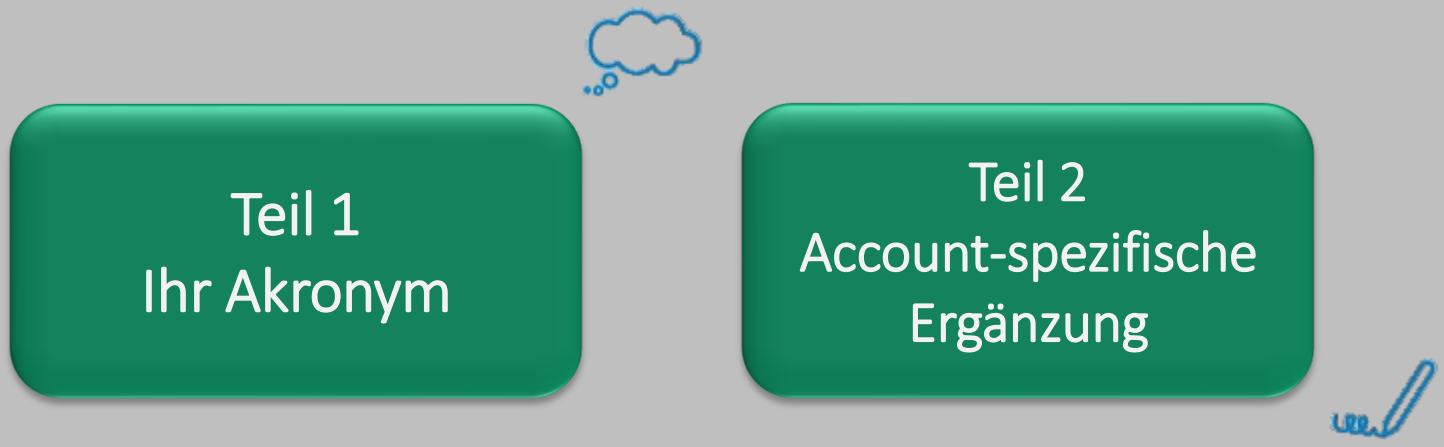
Individualisierung Ihrer Passwörter je Account

Beispiele:

für Google:	Isnv6:00Ua	+	Go => Ho	=	Isnv6:00UaHo
für Apple-ID:	Isnv6:00Ua	+	Ap => Bp	=	Isnv6:00UaBp
für Web.de:	Isnv6:00Ua	+	We => Xe	=	Isnv6:00UaXe

Verwaltung Ihrer Passwörter

das „sichere Passwort-Merkblatt“



Quelle: BSI

Verwaltung Ihrer Passwörter

das „sichere Passwort-Merkblatt“

Account/ Konto	Nutzer-Name/ E-Mail-Adresse	Teil 2 des Passwortes
Google	max@mustermann.de	Ho
Apple	max@mustermann.de	Bp
web.de	max@mustermann.de	Xe

Quelle: BSI

Verwaltung Ihrer Passwörter

verschlüsselte Datei auf Ihrem Notebook oder PC

- Sie benötigen einen Notebook oder PC
- Sie müssen wissen, wie man eine Datei verschlüsselt
- bei Bedarf haben Sie Ihren Notebook oder PC nicht unbedingt dabei

Verwaltung Ihrer Passwörter

Passwort-Manager

- Programm bzw. App zum Speichern und Bereitstellen von Zugangsdaten (Benutzernamen und Passwörter)
- Automatische Eingabe von Benutzername und Passwort in die entsprechenden Eingabefelder
- ist selbst geschützt durch ein Master-Passwort => Sie müssen sich nur dieses eine Master-Passwort merken
- Fingerabdruck bzw. Gesichtserkennung ersetzt i.d.R. die Eingabe des Master-Passwortes

Verwaltung Ihrer Passwörter

Passwort-Manager

- 3 Arten sind zu unterscheiden:
  - in Betriebssystem integriert (z.B. Apple, Samsung)
  - Browser-Erweiterungen (z.B. Firefox, Google Chrome)

    Sicherheitsrisiken => nicht unbedingt empfohlen
  - spezielle Software
    - kostenlose Versionen: meist erheblich eingeschränkt
    - Kauf-Versionen (ca. 3,00 €/Monat)

LastPass ••• | 1Password DASHLANE NordPass

Verwaltung Ihrer Passwörter

Passwort-Manager

- weitere Funktionen:
  - Speicherung der Daten in einer stark verschlüsselten Datenbank
  - Synchronisierung ggf. über mehrere Geräte, teilweise sogar über mehrere Betriebssysteme hinweg
  - Vorschlag von sehr sicheren Passwörtern
  - Sicherheitsanalyse der gespeicherten Passwörter

Verwaltung Ihrer Passwörter

Passwort-Manager für Apple-User

iCloud-Schlüsselbund

- kostenlos
- nahtlose Integration in Apple-Ökosystem
- leicht einzurichten
- starker Datenschutz
- Touch-ID/Face-ID-Unterstützung
- eingeschränkte plattformübergreifende Unterstützung

Verwaltung Ihrer Passwörter

Passwort-Manager für Apple-User

iCloud-Schlüsselbund aktivieren:

- Tippe auf „Einstellungen“ und anschließend auf deinen Namen, und wähle „iCloud“
- Tippe auf „Passwörter und Schlüsselbund“
- Aktiviere den iCloud-Schlüsselbund. Du wirst ggf. nach deinem Code oder Apple-ID-Passwort gefragt

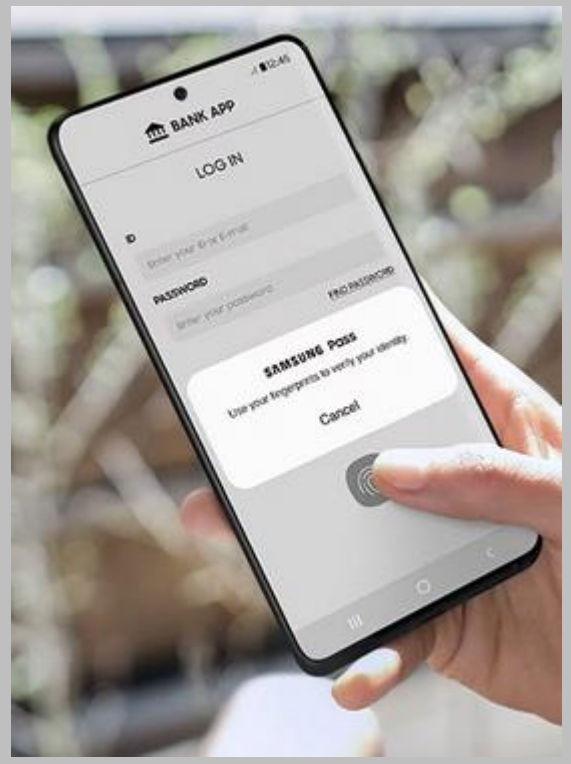
Verwaltung Ihrer Passwörter

Passwort-Manager für Samsung-User

Samsung Pass

- kostenlos
- starker Datenschutz
- Touch ID/Face ID-Unterstützung
- eingeschränkte plattformübergreifende Unterstützung

Eine Anleitung zur Aktivierung finden Sie hier.



regelmäßige Änderung Ihrer Passwörter?

- wurde in der Vergangenheit immer wieder empfohlen
- das BSI hat diese Empfehlung von seiner Seite genommen
- ein sicheres Passwort kann ohne Weiteres jahrelang verwendet werden
- ein Passwort sollte auf jeden Fall geändert werden, wenn es einen Hinweis gibt, dass es tatsächlich in die Hände von unbefugten Dritten gelangt ist

Haben Sie Fragen?

Vielen Dank für Ihre Aufmerksamkeit!