# Sicheres Passwort

**Im Onlinebreich wird es immer wichtiger, wirklich sichere Passwörter zu nutzen - Kennt ein Angreifer das Passwort, kann er nicht nur im digitalen sondern auch im realen Leben erheblichen Schaden anrichten!!**

Anforderungen an ein sicheres Passwort:

- ✓ **schnell + einprägsam**
- ✓ **fast gleich und doch deutliche Unterschiede**
- ✓ **nie ein Passwort für mehrere Accounts**
- ✓ **Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen und mindestens 10 Zeichen - je länger, desto besser**
- ✓ **niemals für andere sichtbar auf Zettel schreiben**
- ✓ **kein Speichern des Passwortes im Browser**
- ✓ **keine persönliche Daten enthalten**
- ✓ **nicht im Wörterbuch zu finden sein**

---

## Methode „Eselsbrücke“

Eselsbrücken sowie persönliche Erlebnisse lassen sich leicht merken und daraus ein sicheres Passwort kreieren - die Anfangszeichen ergebn mein Passwort:

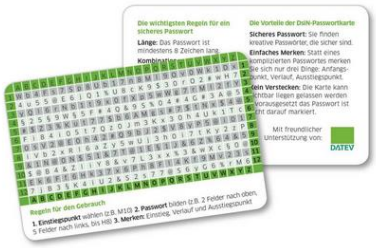
**M**ein **H**und **N**ero **i**st **15** **J**ahre **a**lt **g**eworden **u**nd **2013** **g**estorben

Gehe ich im Anschluss hin und modelliere noch besondere Zeichen am Anfang und Ende hinzu und berücksichtige zudem jenen Account, für den ich das Passwort erstelle, könnte es folgender Maßen ausschauen:

**@MHNi15Jagu2013g-A (Amazon)**
**@MHNi15Jagu2013g-G (Google)**
**@MHNi15Jagu2013g-O (Osnatel)**
**@MHNi15Jagu2013g-G (GMX)**
**@MHNi15Jagu2013g-T (Telekom)**

Ergebnis:
ein sicheres Passwort, obendrein fast identisch (leicht zu merken) und doch unterschiedlich (trotzdem sicher), weil sich der letzte Groß-Buchstabe jeweils an den Account orientiert, dem ich mich gerade anmelden möchte.

## Methode „DsiN-Passwortkarte“



Näheres hier
https://www.sicher-im-netz.de/dsin-passwortkarte-1

Weiteres hier per Video:
https://www.youtube.com/watch?v=9ur7NcDFrN4

---

# Passwort mit Passkey

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/passkeys-anmelden-ohne-passwort.html?nn=1107468

Hinweis: Selbständiger Umgang für SeniorenInnen ohne digitale Erfahrung eher schwierig.
Probleme bei Verlust des Gerätes:

Was, wenn mein Gerät verloren oder gestohlen wird?

Falls das Gerät, auf dem Ihre Passkeys hinterlegt sind, verloren gegangen ist oder gestohlen wurde, können Sie Ihre Zugänge dann wiederherstellen, wenn Sie entweder lokale Backups angelegt haben oder wenn Ihre Passkeys in einer Cloud synchronisiert werden. Sollten Sie keine Sicherheitskopien Ihrer Passkeys besitzen, bieten einige Dienste weitere Möglichkeiten, Ihre Identität nachzuweisen und so beispielsweise einen neuen Passkey für Ihren Zugang zu erstellen. In seltenen Fällen kann es aber vorkommen, dass Sie sich nach dem Verlust Ihres Geräts nicht mehr einloggen können. Dann müssen Sie den Anbieter kontaktieren und den Account wiederherstellen.

## Methode „Keymanager“

Passwörter verwalten mit dem Passwort-Manager

Näheres hier
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html

Die Sicherheit des erstellten Passwortes kann auf folgender Website getestet werden

Passwort Check: Wie sicher ist mein Passwort? | EXPERTE.de