

# Sichere Passwörter ganz einfach

**CRYPTOPARTY**  
**<https://cryptoparty.at/graz>**

Dieser Vortrag und alle Links zu den Tools unter obigem Link

Vortrag für ÖH-Uni/Graz

This work is licensed under a Creative Commons Attribution 4.0 International License.

# Inhalt:

- 1) Warum sind gute Passwörter wichtig?
- 2) Was soll man alles Berücksichtigen?
- 3) Welche Methoden/Hilfsmittel gibt es?
- 4) Ein praktisches Beispiel

# 1.) Warum sind gute Passwörter wichtig?

Passwörter gewähren Zugriff zu einem System,  
einem Diensteanbieter:

- Um sich zu Authentifizieren
- Um Daten vor unbefugten Zugriff zu schützen

# Wieso nicht "Mutzi85" für alles?

- Leicht von Personen und besonders leicht von Computern zu erraten
- Panne/Veröffentlichung kann einem selbst passieren (Handy verloren)
- Panne/Veröffentlichung kann dem Diensteanbieter passieren (Datenbank gehackt)

# Was passiert so in RealLife

- iCloud-Account-Foto Panne
- Google-Account wird gehackt
  - man muss zahlen damit man wieder Zugriff auf seine Mails erhält
  - Username bei allen üblichen Diensten ist die Mailadresse
  - "Passwort-Vergessen"-Funktion liefert neues Passwort an die Mailadresse

## 2.) Was gilt es zu beachten?

### Sehr hohe Anforderungen an Passwörter nötig:

- !! Für jeden Account ein eigenes Passwort !!
- Mindestens 14 Zeichen
  - (Länge ist wichtiger als Sonderzeichen)
- Zahlen und Sonderzeichen müssen enthalten sein
  - (Nicht nur am Anfang oder Ende!)
- !! Für jeden Account ein eigenes Passwort !!

→ kaum zu merken

- Sicherheitsfrage wenn Passwort vergessen:
  - Mädchenname der Mutter?
    - war der nicht : "ads03qj\_\sd'asd45" ?
- Sicherheits-E-Mail-Adresse, wenn Passwort vergessen:
  - Separate Mailadresse!
  - Eigenes besonders sicheres Passwort.
- Speichern der Passwörter im Browser?
  - Chrome/Firefox: Unbedingt Masterpasswort setzen!
  - InternetExplorer: Getrennt für jeden User

2.) Was gilt es zu beachten?

# Bankgeschäfte mit dem Smartphone?

Es gibt Handy-Trojaner die SMS abfangen/ändern können.

- Konzept SMS-Tan funktioniert nur wenn es zwei unterschiedliche Geräte sind!
  - Zweites Handy (kein Smartphone) oder iTans auf Papier verwenden



# Passwörter auf Papier aufschreiben?

- + Sicher vor Trojanern!
- Unsicher vor zukünftiger Ex-FreundIn
- Backup bei Verlust/Feuer?

In die Brieftasche?

→ wenn dann verschleiert!

2.) Was gilt es zu beachten?

# Regelmäßig Passwörter ändern?

## Wird eher überbewertet:

- Wenn Hacker Zugriff auf einen Account haben, tritt der Schaden eher gleich ein.
- Falls es ein Account "geteilt" wird macht das Sinn, weil dann regelmäßig die Gruppe an Personen hinterfragt wird.
  - Wirklich wichtige darf man ruhig alle paar Jahre ändern.

### 3.) Welche Methoden/Hilfsmittel gibt es?

- Im Kopf: Wie merkt man sich gute Passwörter?

Ein Satz ist leichter zu merken:

Das Merken von Passwörtern ist mühsam,  
darum verwende ich einen Passwort-Save!

→ **“DmvPim,dvieP-S!”**

# Verschleiern auf Papier

ZAHLUNGSANWEISUNG  
AUFTRAGSBESTÄTIGUNG

EmpfängerInName/Firma  
ÖSTERR. ROTES KREUZ  
IBANEmpfängerIn  
AT79 2011 1822 3777 3800  
BIC(SWIFT-Code) der Empfängerbank  
GIBAATWWXXX  
EUR Betrag Cent  
Zahlungsreferenz  
230040419206  
IBANKontoinhaberIn/AuftraggeberIn  
Verwendungszweck  
18 Rotkreuz-Lose +  
2 Gratis-Lose  
Hinweis auf Steuerabsetzbarkeit  
Ihrer Spende auf der Rückseite!  
ACHTUNG: Letzter Einzahltag:  
22. Dez. 2014

AT ERSTE BANK

EmpfängerInName/Firma  
ÖSTERREICHISCHES RO  
IBANEmpfängerIn  
AT79 2011 1822 3777  
BIC(SWIFT-Code) der Empfängerbank  
GIBAATWWXXX  
230040419206 Bedrucken d  
Verwendungszweck wird bei ausgefüllter  
18 Rotkreuz-Lose à  
Bei Telebanking-Überweisungen bitte in  
IBANKontoinhaberIn/AuftraggeberIn  
KontoinhaberIn/AuftraggeberInName/

Unterschrift Zeich

**EÖIABGEZ2IV12HIA2**

Deutsches Museum

Dr. Max Schneider  
Foto + Film  
Leitung

Museumsinsel 1, 80538 München  
Telefon (089) 21 79-2 49 · Telefax (089) 21 9 3 24 7  
e-mail: mp@deutsches-museum.de

**BERGFUCHS**  
BERGSPORT, S. STEINER Ges.m.b.H.  
HANS-RESEL-GASSE 7 8020 GRAZ  
TEL. 0316 / 76 33 00, FAX 0316 / 76 33 01  
e-mail: graz@bergfuchs.at  
internet: www.bergfuchs.at  
A T U 4 0 3 2 2 3 0 7

Anz.	Datum	Preis	Betrag in €
	21.3.2013		
1	Whistle Gipfel		5,50
2	AA - Trekking		108,80
2	Amvel Steigortent		33,80
2	AA Antistoll		31,80
2	360° Flaschen		24,80
			<u>203,70</u>
1	Premies Mug		7,50
	* Flohmarkt-Ware *		
			<u>211,-</u>
! Kein Umtausch!			
Verkäufer:		Preise inkl. 20% MwSt.	
<b>15-703821</b>			OMEGA G2S/0
Bei Irrtum oder Umtausch ist dieser Kassenzettel vorzulegen.			

**CRYPTOPARTY**  
<https://cryptoparty.at/graz>

3.) Welche Methoden/Hilfsmittel gibt es?

# Verschleierung im Adressbuch

- PIN's: Telefonnummern aus Adressbuch:
- z.B. letzte Stellen der Faxnummer oder Durchwahl

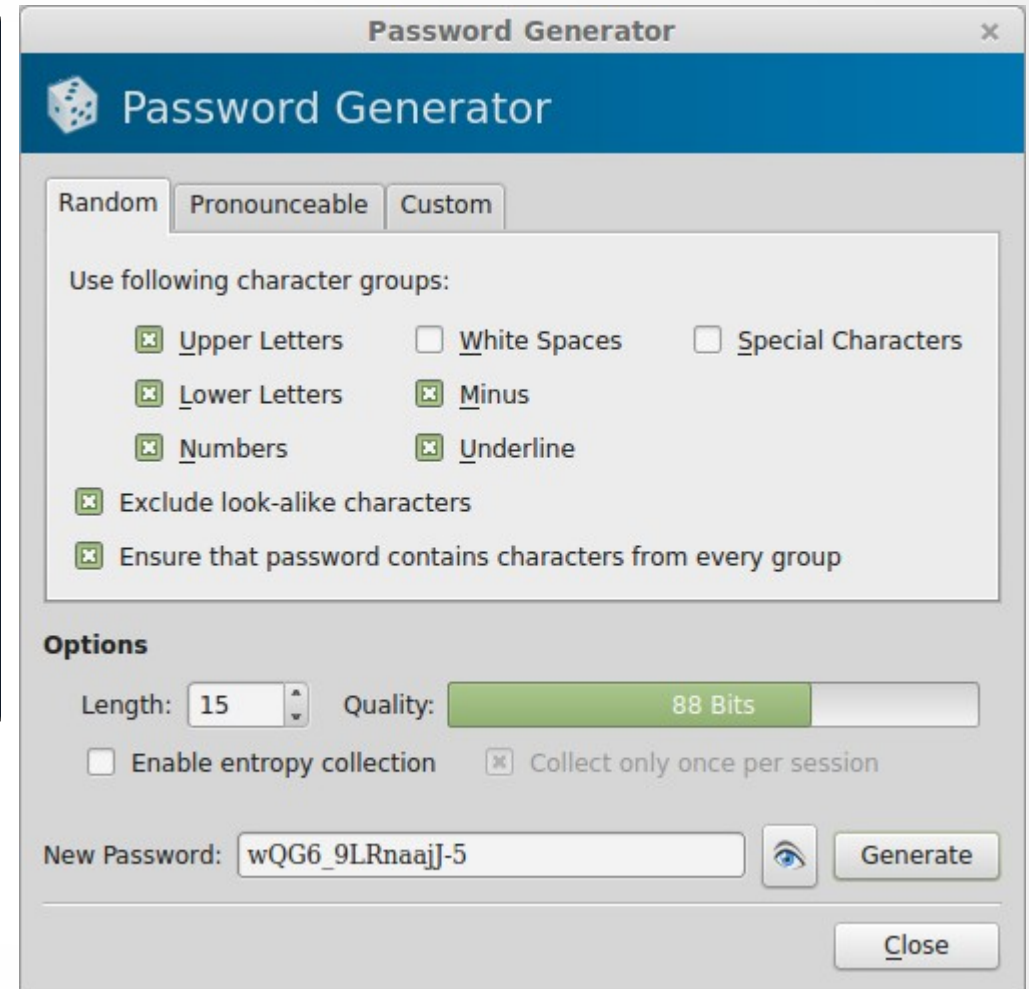
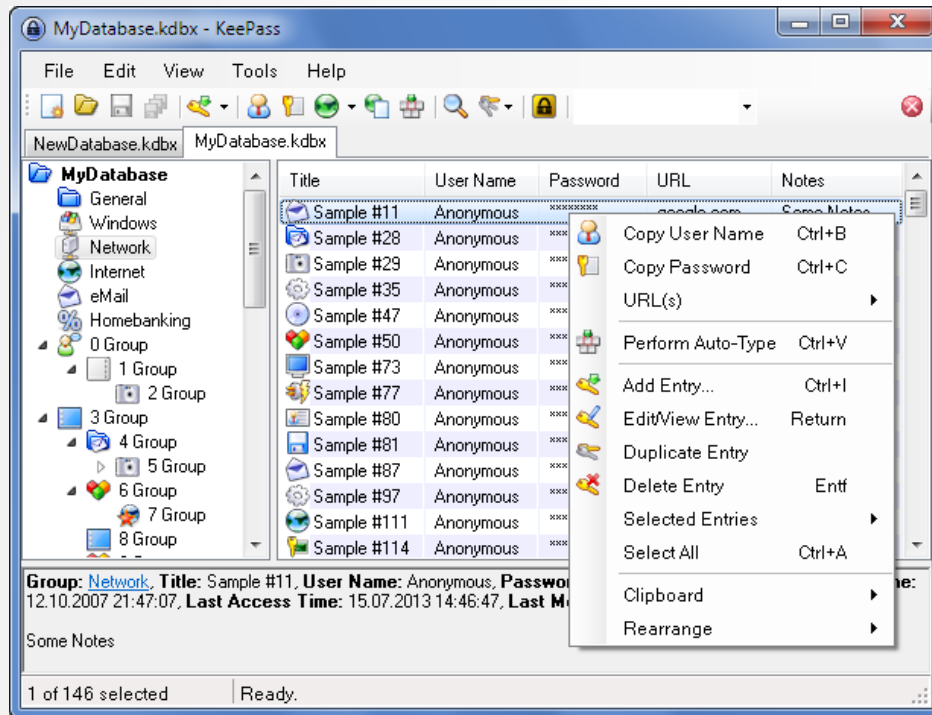
**Darf nicht auffällig sein!**

# Passwort-Safe: KeePass

## Vorteile:

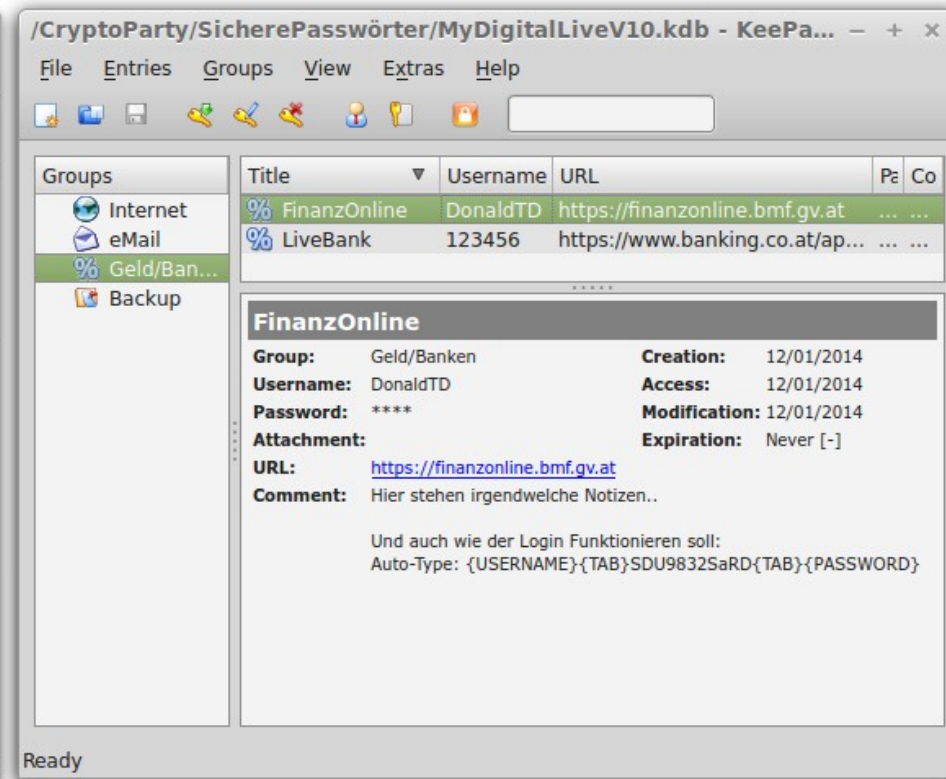
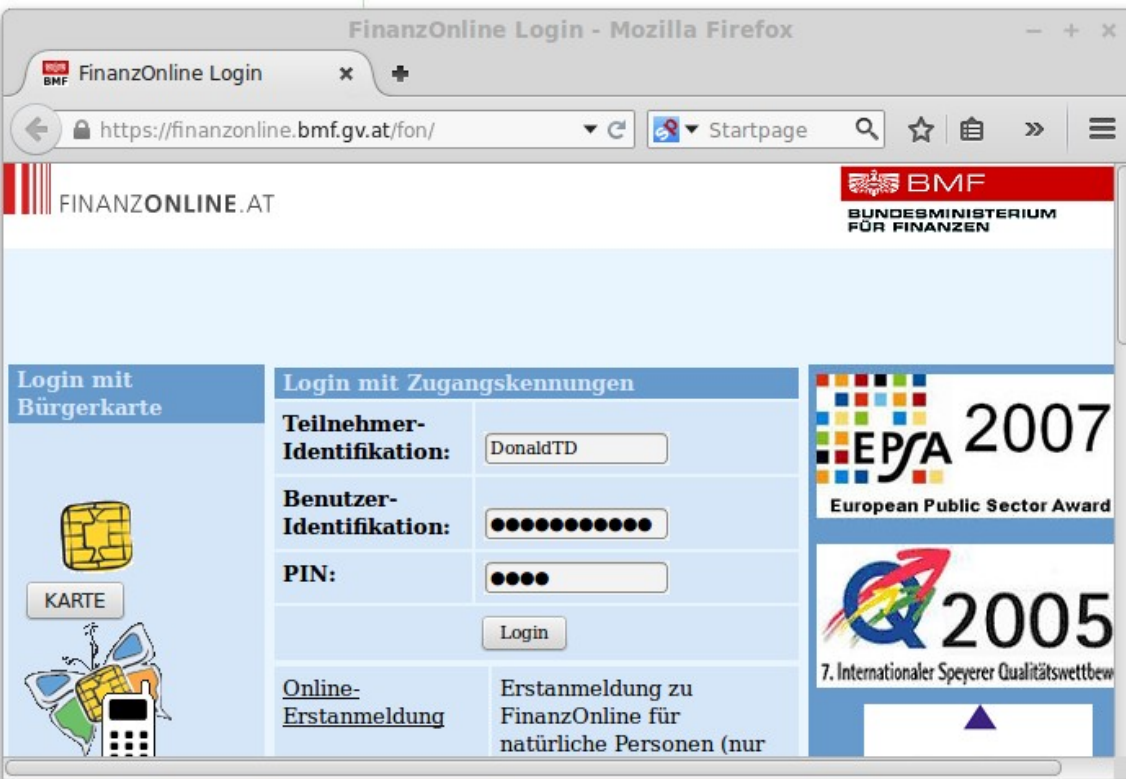
- Passwortgenerator integriert
- Leicht für jede Seite ein eigenes Passwort erstellbar
- AutoType ersetzt Copy&Paste
- Kann Lesezeichen/Bookmarks ersetzen
- Hohe Sicherheit da OpenSource-Produkt (+Gratis verwendbar)
- Verfügbar für PC: Windows/Linux/MacOSX  
Smartphones: Android, iPhone, WindowsPhone

# Password-Safe: KeePass / KeepassX / Keepass2Android



3.) Welche Methoden/Hilfsmittel gibt es?

# Passwort-Safe: KeePass / KeepassX / Keepass2Android

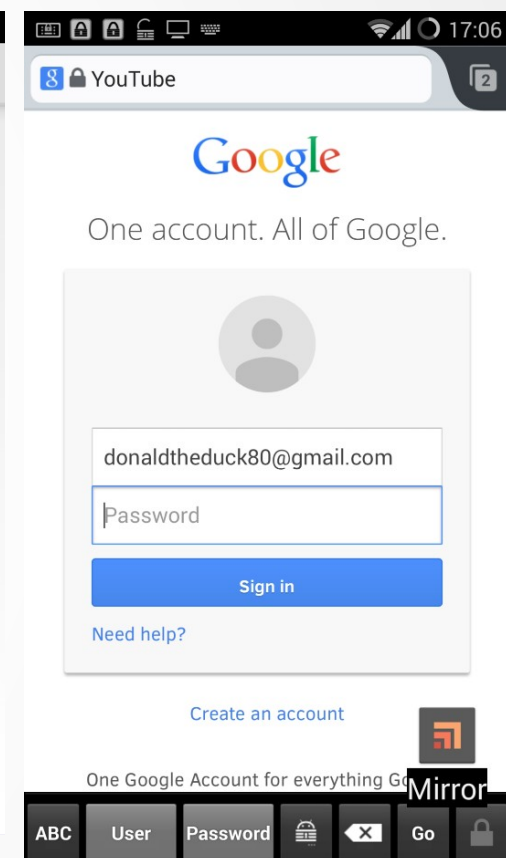
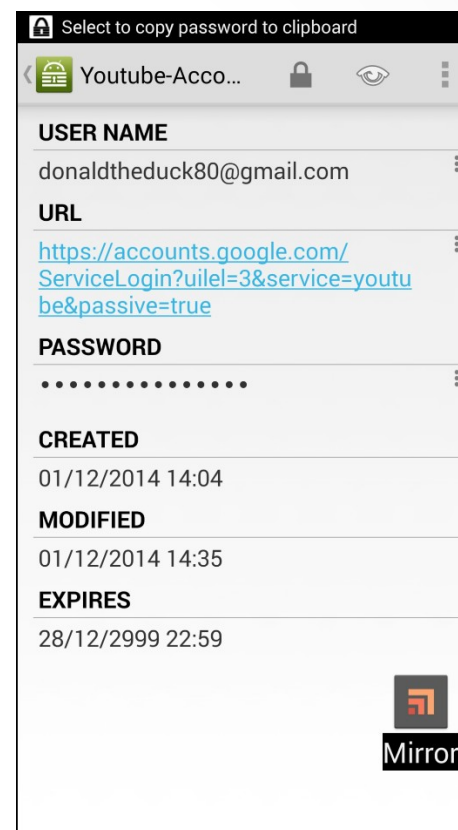
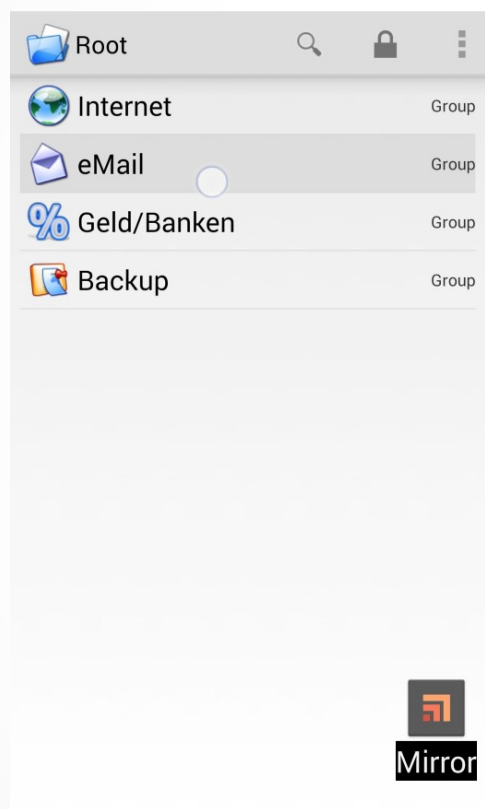
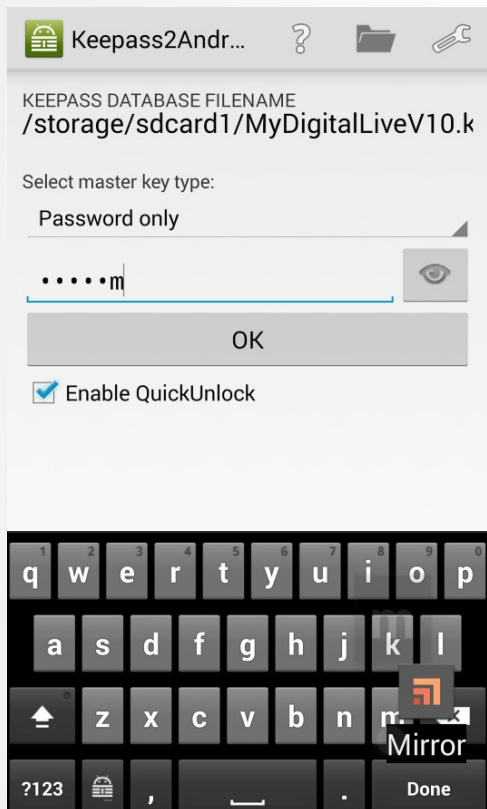


3.) Welche Methoden/Hilfsmittel gibt es?



# Keepass2Android

Youtube-Video: [http://youtu.be/R\\_3lCwuMaVQ](http://youtu.be/R_3lCwuMaVQ)



3.) Welche Methoden/Hilfsmittel gibt es?

# Passwort-Safe: Keepass2Android

TODO: VideoLink von Keepass2AndroidLive.mp4 (auf Youtube)  
Vorzeigen

## Vorzeigen:

- Öffnen von verschlüsselter Passwort-Datei
- Suche
- Öffnen des Links
- AutoType einmal herzeigen
- Funktionsweise AutoType: Keyboard vernsteuern, Excel
- Custom-AutoType
- Neuen Eintrag erstellen: Passwortmanager

3.) Welche Methoden/Hilfsmittel gibt es?

# 4.) Ein praktisches Beispiel

## Annahme Hardware:

- PC zu Hause (Windows)
- Android-Smartphone (nicht gerooted, nicht verschlüsselt)
- MAC-Laptop (privat)
- PC im Büro (Windows)

## Annahme Anwendungsfälle:

- Für jeden Account ein eigenes Passwort
- Onlineshopping am Handy soll möglich sein
- Alle-Kreditkartendaten für den Urlaub mitnehmen
- Bankgeschäfte nur am Heim-PC
- Backup-Strategie: Schutz vor Diebstahl, Wohnungsbrand
- Synchronisations-Strategie

- 1.) Neue Email-Adresse zulegen für Passwort-Resets
- 2.) Zwei Keepass-Dateien am Heim-PC anlegen

HeimPC.kbd:

- Computer-Passwörter
- Handy-PIN, Handy-Original-PIN, PUK
- Finanzonline
- Onlinebanking
- Kreditkartennummer
- Kreditkarten-Rückseiten-Nummer
- Kreditkarten 3-D-Secure-Code
- Kreditkarten-Geldautomat-Pin

Smartphone.kbd:

- Ebay
- Amazon
- E-Mail (Nicht die Passwort-Reset-Mail-Adresse!)
- Facebook
- Twitter

keine Kreditkarteninfos!

keine Onlinebankinginfos!

- beide auf auf USB-Stick speichern und bei den Bankunterlagen verwahren.
- beide auf 2.USB-Stick speichern und einem Vertrauten geben.  
(Auch praktisch in Notfällen).

4.) Ein praktisches Beispiel

→ Smartphone.kbd auf Smartphone, Firmen-PC und Mac-Laptop kopieren

### Synchronisation:

- Wenn am Smartphone.kbd neuer Eintrag: Mail an sich selber schicken (nur Account-Name) und am Heim-PC später aktualisieren.
- Wieder Backups erstellen und verteilen

### In die Geldtasche:

- Kreditkarte (3 stelliger Code steht auf Rückseite)
- Pseudo-Visiettenkarte: Kreditkarten-Geldautomat-Pin
- Kreditkarten 3-D-Secure-Code: verschleiert als Quercodes auf altem Erlagschein
- Passwort für Smartphone.kbd als Quercodes auf Rechnung.

→ beide auf USB-Stick speichern und bei den Bankunterlagen verwahren.

→ beide auf 2.USB-Stick speichern und einem Vertrauten geben.

(Auch praktisch in Notfällen).

## 4.) Ein praktisches Beispiel

# Schlussworte

Sensible Daten gehören nicht in die Cloud!

Cloud ersetzt kein persönliches Backup!