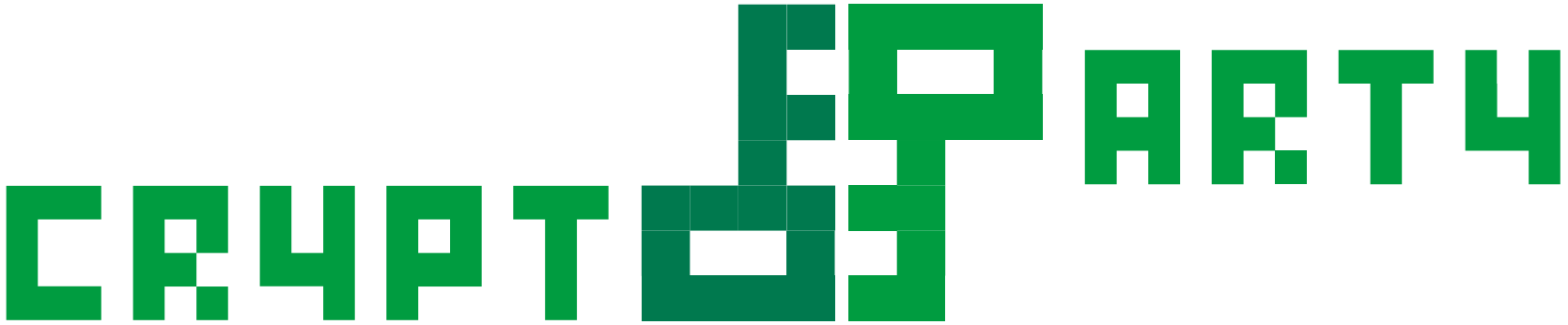
Sichere Passwörter ganz einfach



https://cryptoparty.at/graz

Dieser Vortrag und alle Links zu den Tools unter obigem Link

Vortrag für URANIA/Graz

Inhalt:

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

CRYPTOPARTY
https://cryptoparty.at/graz

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 funtkioniert nur wenn es zwei unterschiedliche Geräte sind!

  → Zweites Handy (kein Smartphone) oder iTans auf Papier verwenden

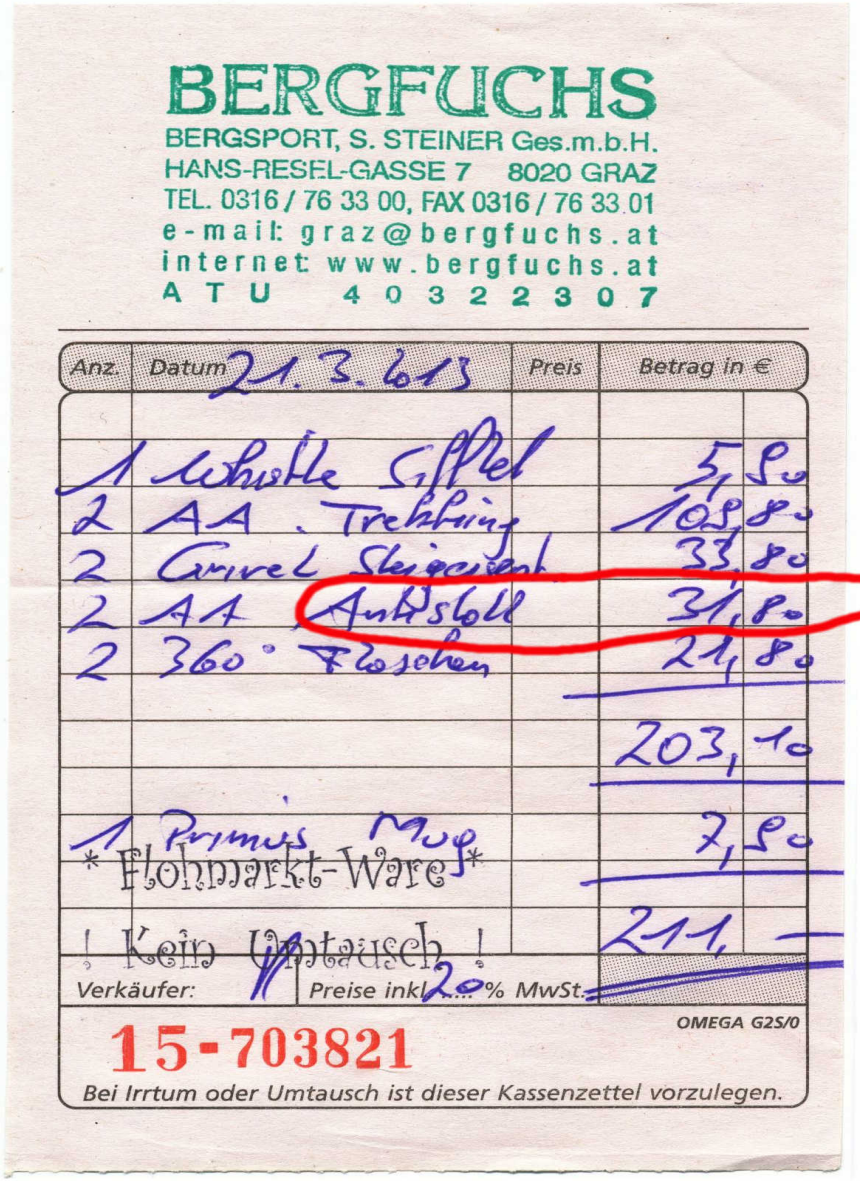
Passwörter auf Papier aufschreiben?

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

In die Brieftasche?

→ wenn dann verschleiert!

Verschleiern auf Papier



3.) Welche Methoden/Hilfsmittel gibt es?

CRYPTOPARTY
https://cryptoparty.at/graz

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.

2.) Was gilt es zu beachten?

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!**“

Verschleierung im Adressbuch

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

  Darf nicht aufällig sein!

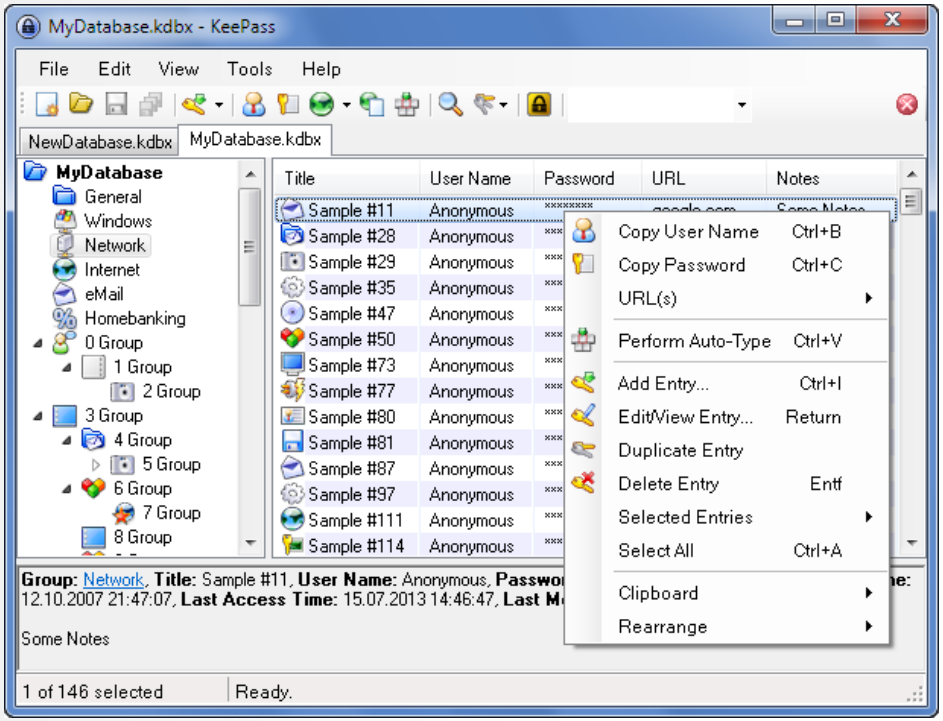
Passwort-Safe: KeePass

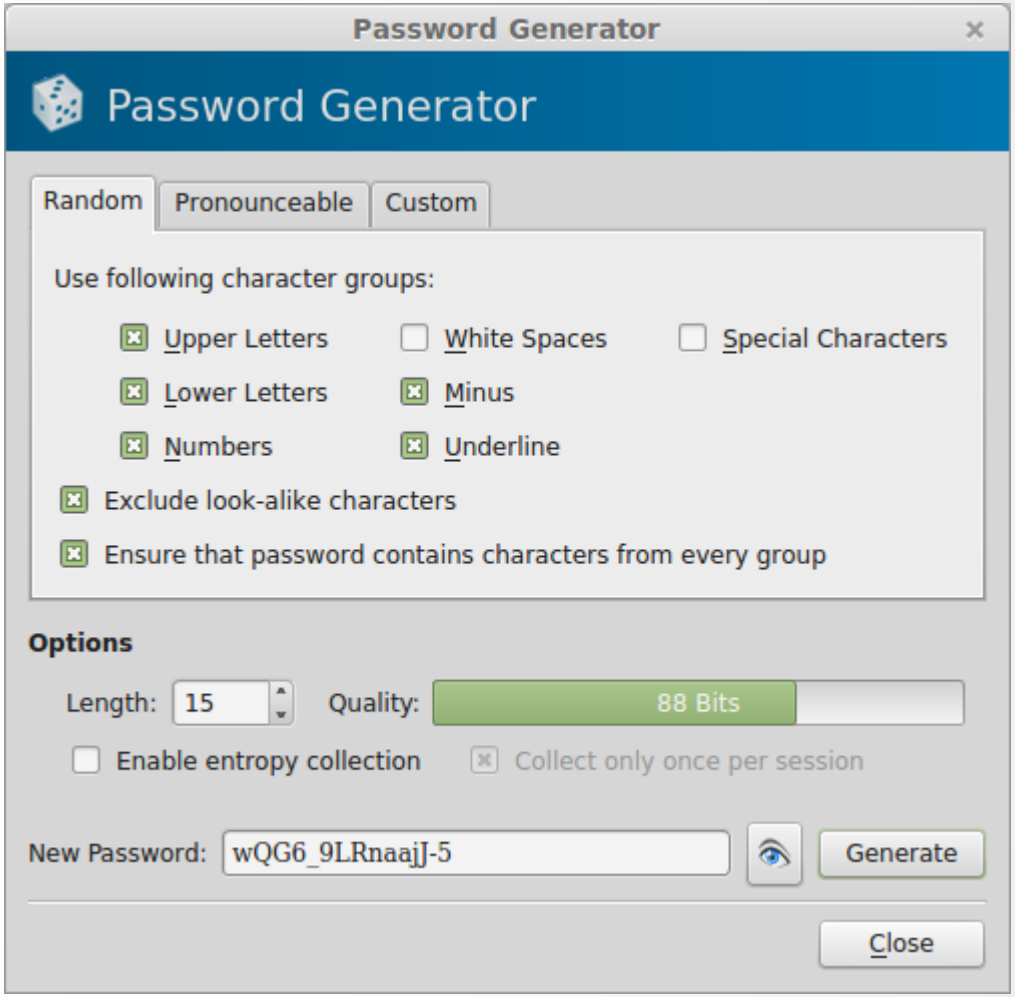
Vorteile:

- 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

Passwort-Safe: KeePass / KeepassX / Keepass2Android

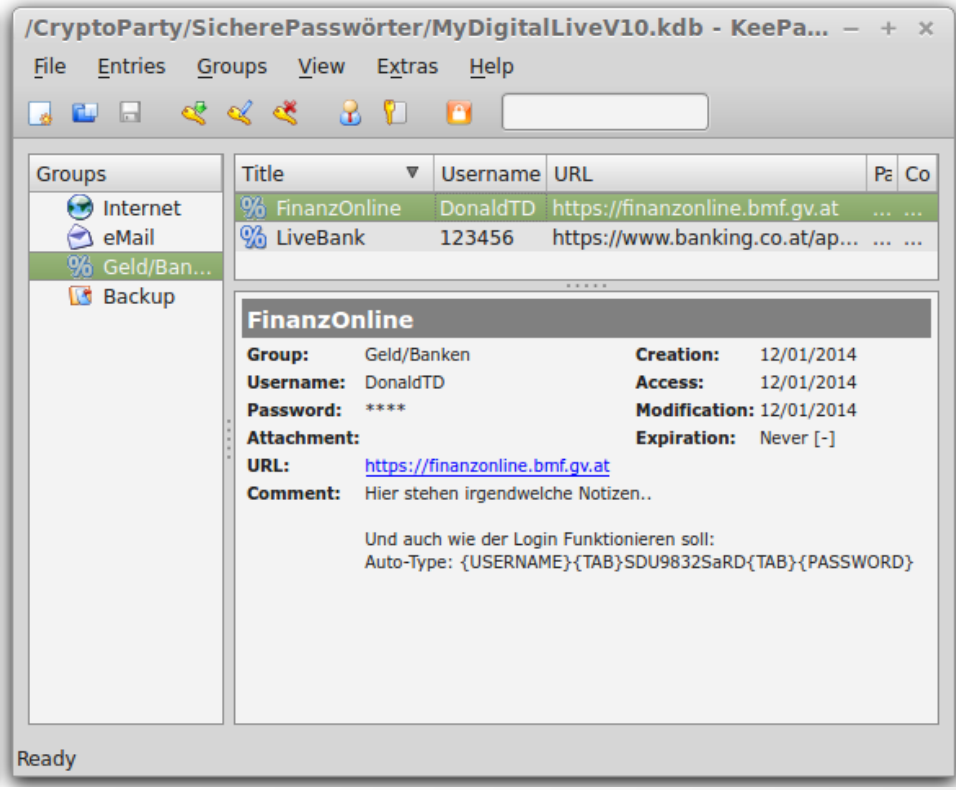




3.) Welche Methoden/Hilfsmittel gibt es?

CRYPTOPARTY
https://cryptoparty.at/graz

Passwort-Safe: KeePass / KeepassX / Keepass2Android

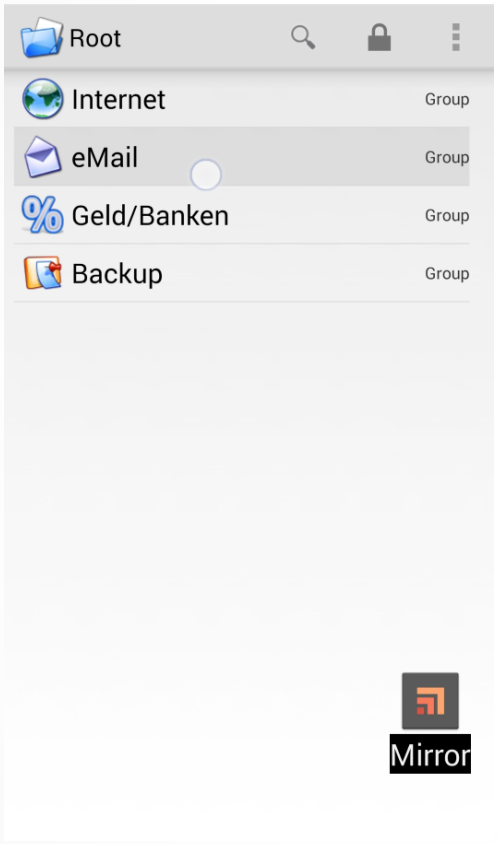


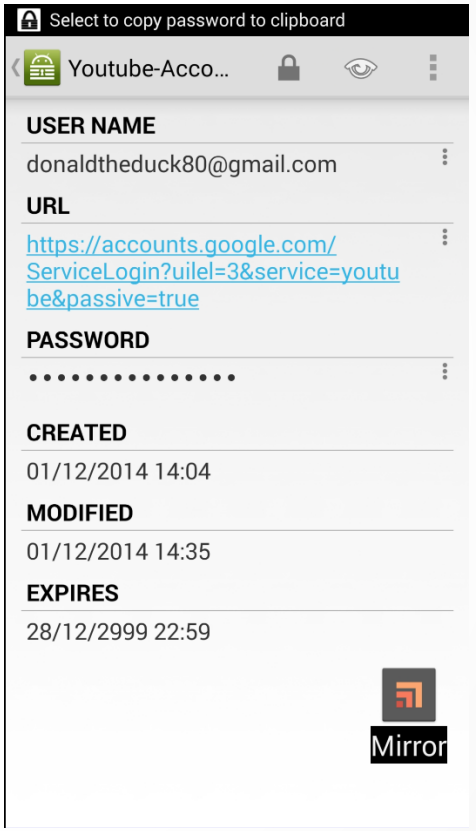
3.) Welche Methoden/Hilfsmittel gibt es?

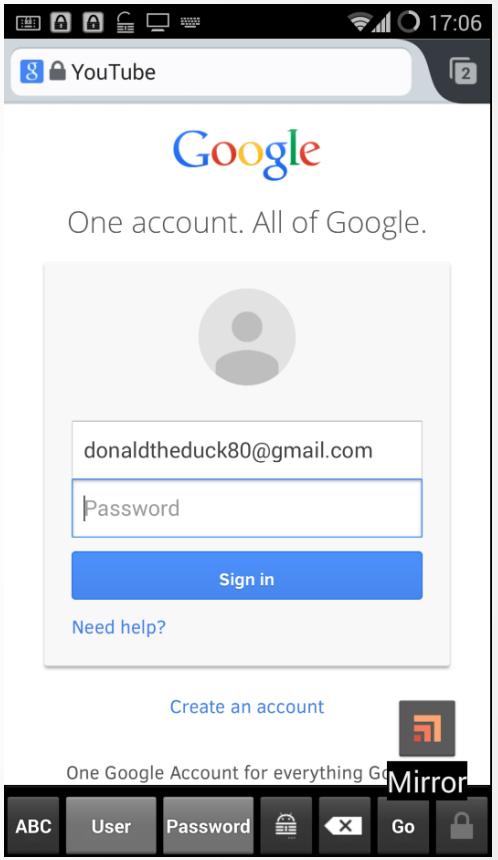
CRYPTOPARTY
https://cryptoparty.at/graz

Keepass2Android

Youtube-Video: http://youtu.be/R_3lCwuMaVQ







3.) Welche Methoden/Hilfsmittel gibt es?

CRYPTOPARTY
https://cryptoparty.at/graz

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

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
- Syncronisations-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 Quercode auf altem Erlagschein
- Passwort für Smartphone.kbd als Quercode auf Rechnung.

→ 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).

Schlussworte

Sensible Daten gehören nicht in die Cloud!

Cloud ersetzt kein persönliches Backup!