Sichere Passwörter ganz einfach

CRYPTOPARTY

https://cryptoparty.at/graz

Dieser Vortrag und alle Links zu den Tools unter obigem Link

Vortrag vom 6.6.2017

Inhalt:

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

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

Besser: 2-Faktor-Authentifizierung, wenn möglich nicht per SMS

Wieso nicht "Mutzi2011" 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
  - Geldforderung um wieder Zugriff zu erlangen
  - Username bei allen üblichen Diensten ist die Mailadresse
  - "Passwort-Vergessen"-Funktion liefert neues Passwort an die Mailadresse

Test der eigenen Mail-Adresse:
https://haveibeenpwned.com/

Kapitel 1) Warum sind gute Passwörter wichtig?

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

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

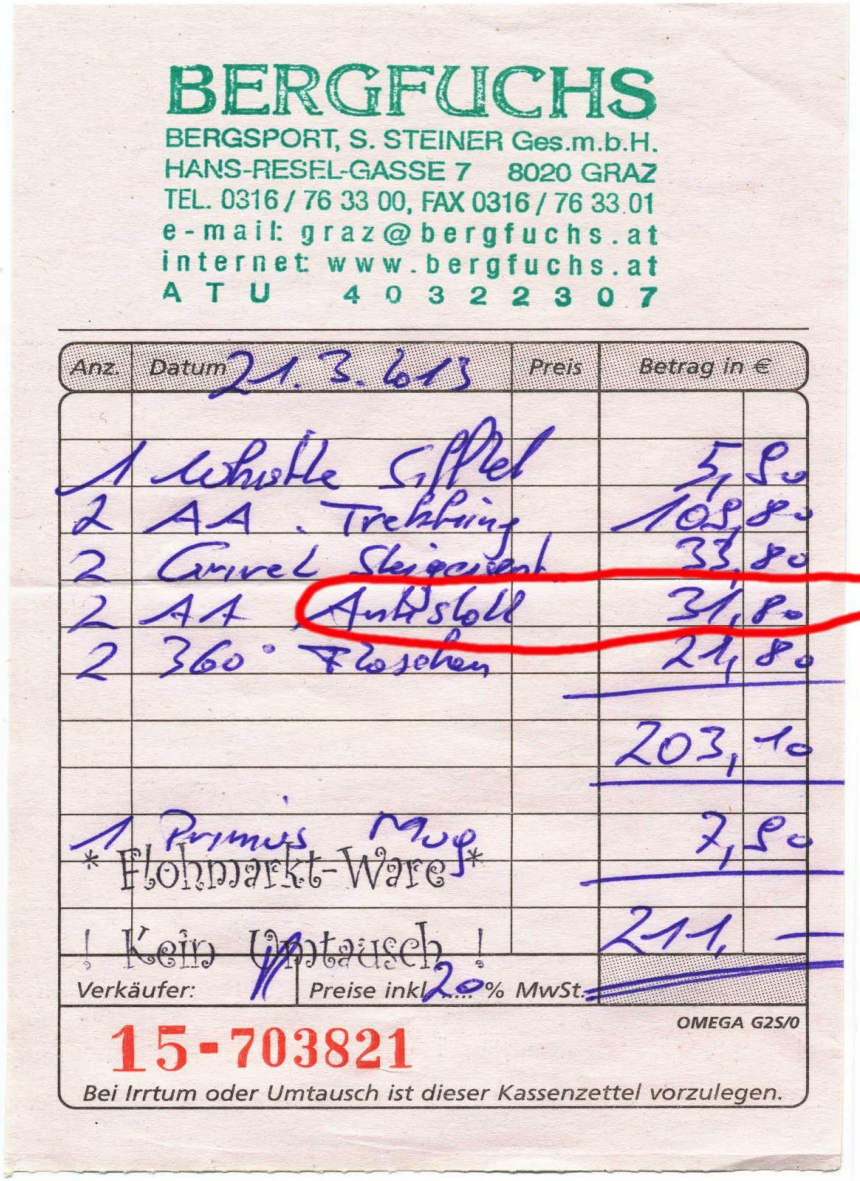
Passwörter auf Papier aufschreiben?

- ✚ 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

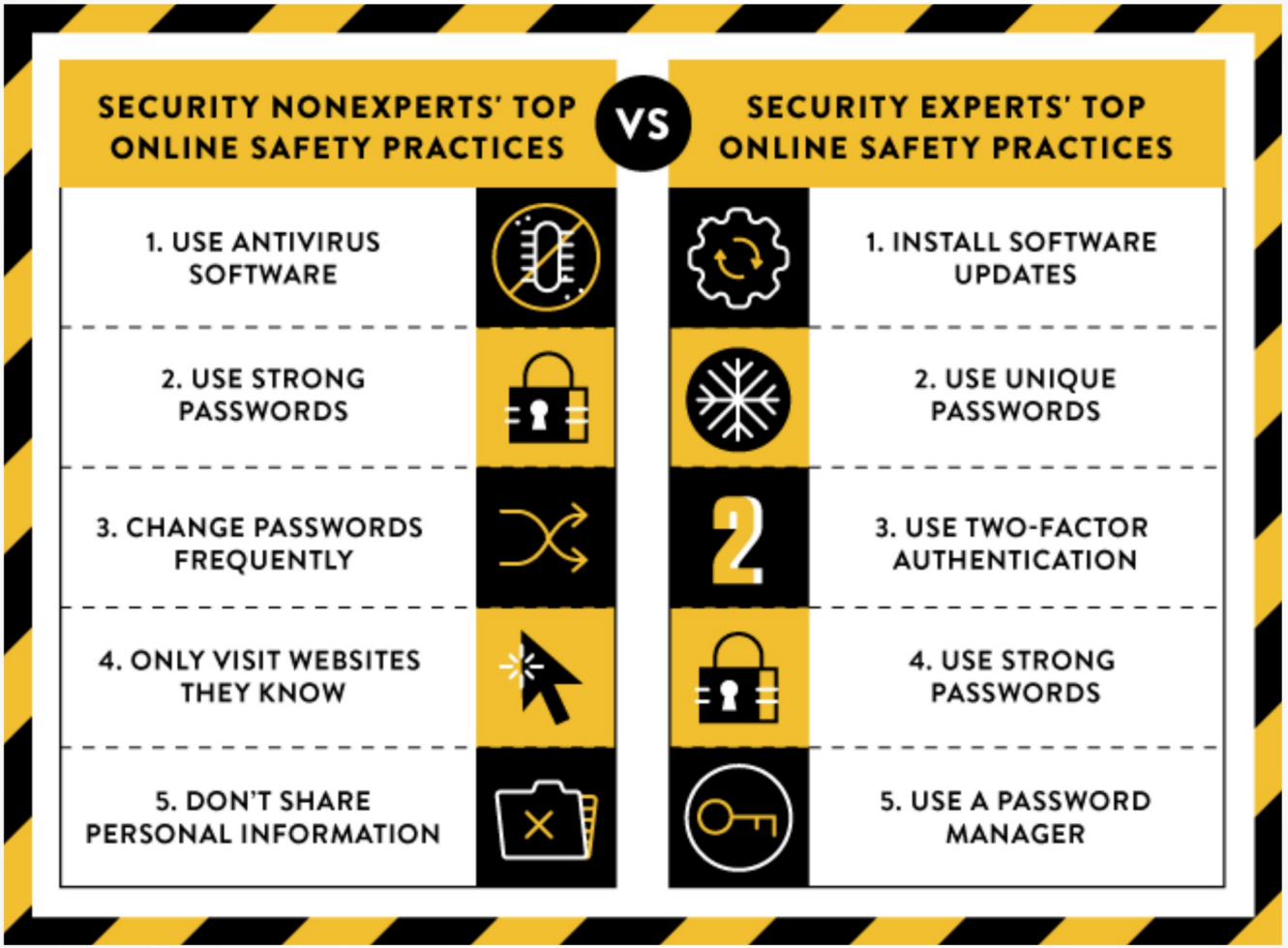
  Darf nicht aufällig sein!

Passwort-Safe: KeePass[XC]

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

Umfrage zu IT-Security: <Link>



Kapitel 1) Warum sind gute Passwörter wichtig?

Passwort-Safe: KeePass[XC]

KeePass: http://keepass.info

- Original für Windows, Version V2.xx hat mehr Features

KeePassX: https://www.keepassx.org/

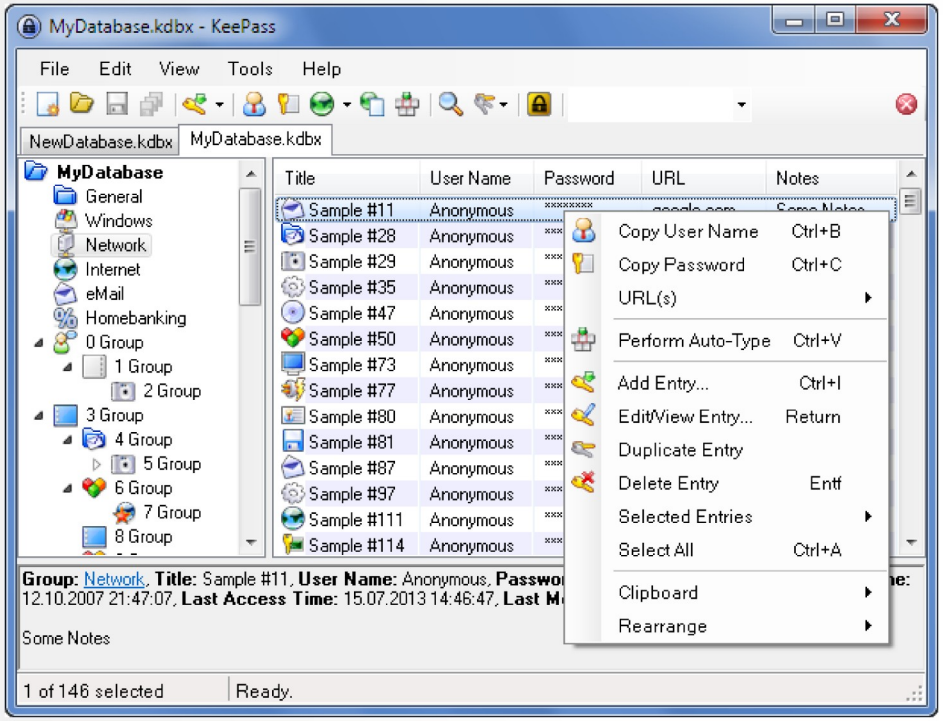
- Für Linux, MacOS X

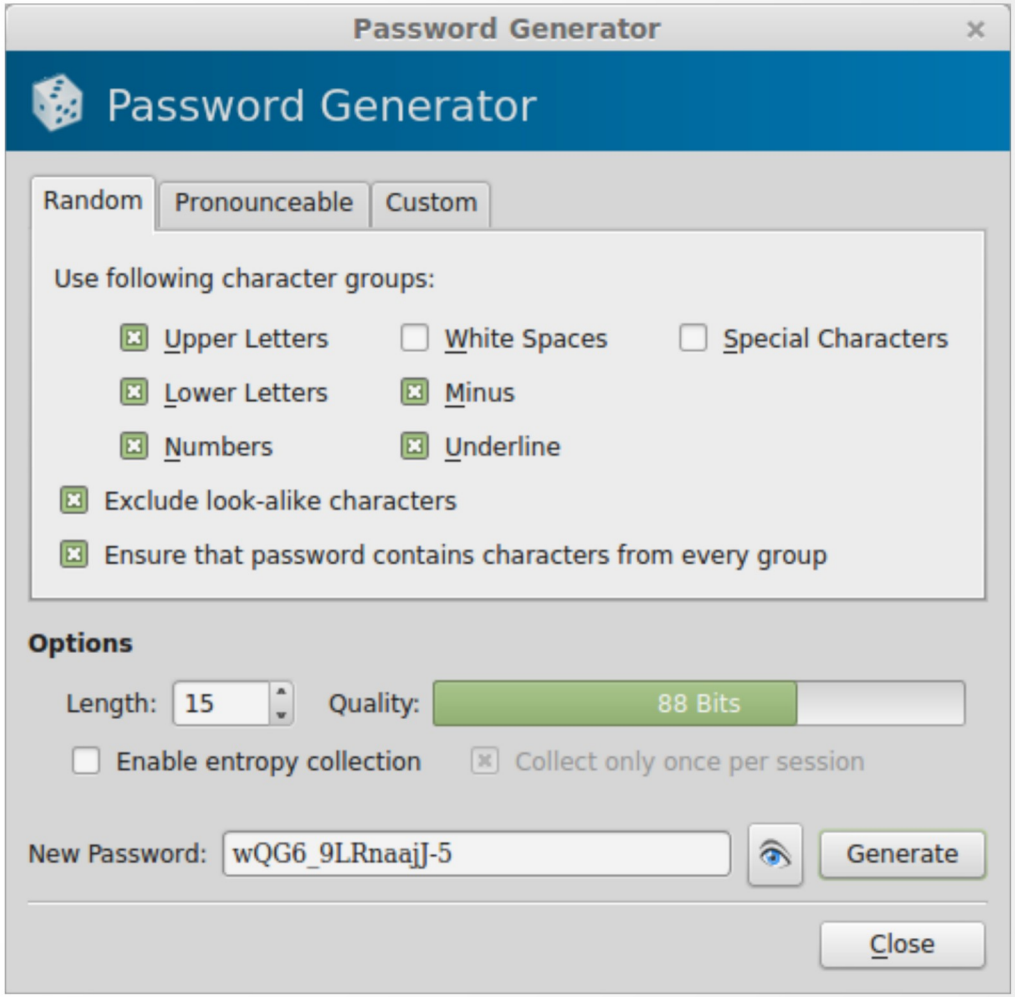
KeePassXC: https://keepassxc.org

- Neueste Version für Windows, Linux, MacOS X

Andere Passwort-Manager bitte recherchieren:
Suchen auf https://www.heise.de/security/

Passwort-Safe: KeePass / KeepassX / Keepass2Android

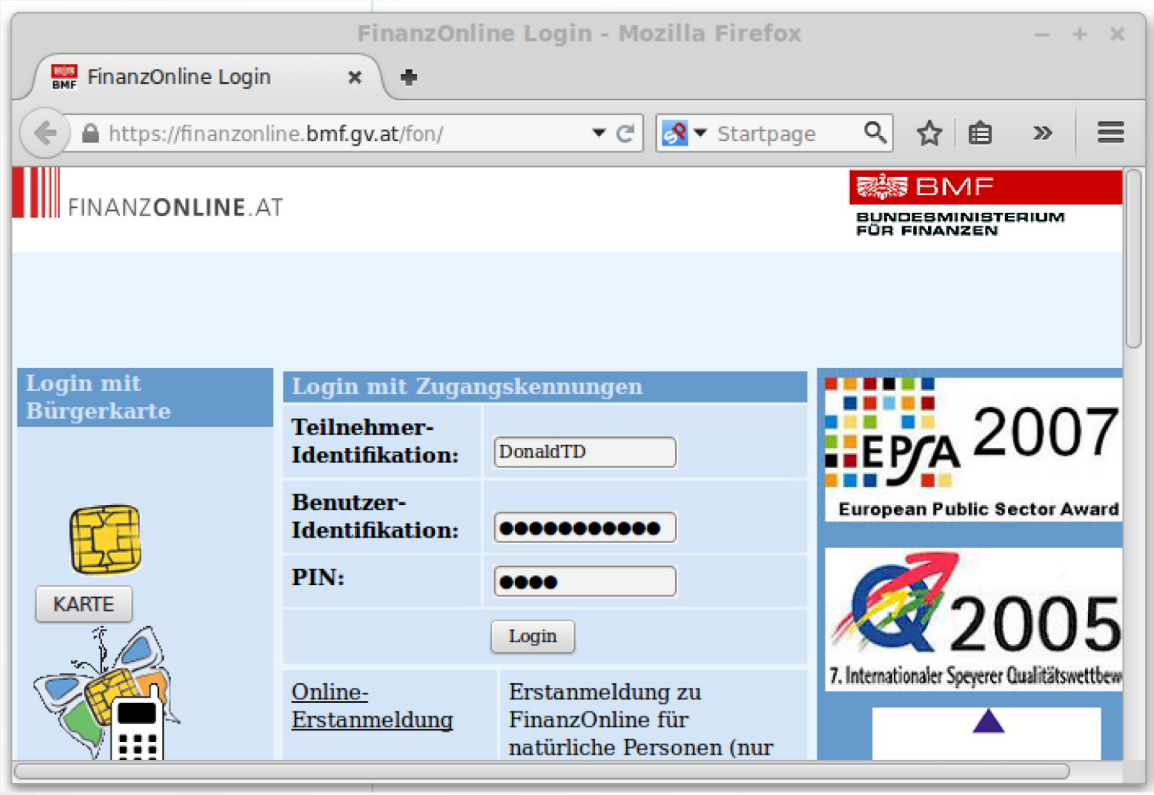


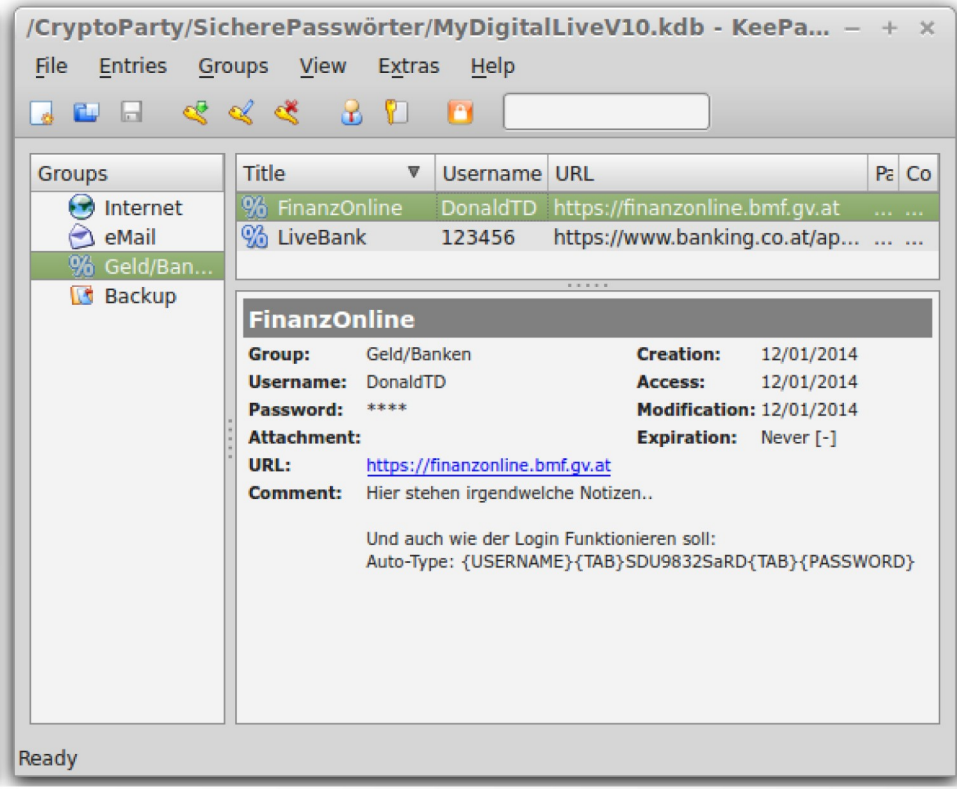


3.) Welche Methoden/Hilfsmittel gibt es?

CRYPTOPARTY
https://cryptoparty.at/graz

Passwort-Safe: KeePass / KeepassX / Keepass2Android





3.) Welche Methoden/Hilfsmittel gibt es?

CRYPTOPARTY
https://cryptoparty.at/graz

Schlussworte

- Ein Passwort niemals zweimal verwenden!
- Immer alle Rechner/Smartphones aktualisieren!
- Backup! Backup! Backup!

CRYPTOPARTY
https://cryptoparty.at/graz