

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

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?

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/>



The screenshot shows a list of the top 10 breaches of user accounts. Each entry includes a logo, the number of accounts affected, and the name of the service. Some entries have additional icons like a question mark or a flame.

Top 10 breaches	
 myspace	359,420,698 MySpace accounts
 NETEASE www-163-com	234,842,089 NetEase accounts ?
	164,611,595 LinkedIn accounts
	152,445,165 Adobe accounts
	112,005,531 Badoo accounts ?
	93,338,602 VK accounts
	91,436,280 Rambler accounts
	68,648,009 Dropbox accounts
tumblr:	65,469,298 tumblr accounts

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?

Verschleiern auf Papier

ZAHLUNGSANWEISUNG AUFTRAGSBESTÄTIGUNG

AT **ERSTE BANK**

EmpfängerInName/Firma
ÖSTERR. ROTES KREUZ
IBANEmpfängerIn
AT79 2011 1822 3777 3800
BIC (SWIFT-Code) der Empfängerbank
GIBAATWWXXX

Betrag | Cent
EUR | |

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

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		5,90
2	AA - Trekking		109,80
2	Amvel Steigortent		33,80
2	AA Antistoll		31,80
2	360° Flaschen		24,80
			<u>203,10</u>
1	Premies Mug		7,90
*	Flohmarkt-Ware		
			<u>211,-</u>
! Kein Umtausch!			
Verkäufer:		Preise inkl. 20% MwSt.	
15-703821			OMEGA G2S/0
Bei Irrtum oder Umtausch ist dieser Kassenzettel vorzulegen.			

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

3.) Welche Methoden/Hilfsmittel gibt es?

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!”**

Verschleierung im Adressbuch

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

Darf nicht auffällig 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>

SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES	VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES
1. USE ANTIVIRUS SOFTWARE 		1. INSTALL SOFTWARE UPDATES 
2. USE STRONG PASSWORDS 		2. USE UNIQUE PASSWORDS 
3. CHANGE PASSWORDS FREQUENTLY 		3. USE TWO-FACTOR AUTHENTICATION 
4. ONLY VISIT WEBSITES THEY KNOW 		4. USE STRONG PASSWORDS 
5. DON'T SHARE PERSONAL INFORMATION 		5. USE A PASSWORD MANAGER 

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

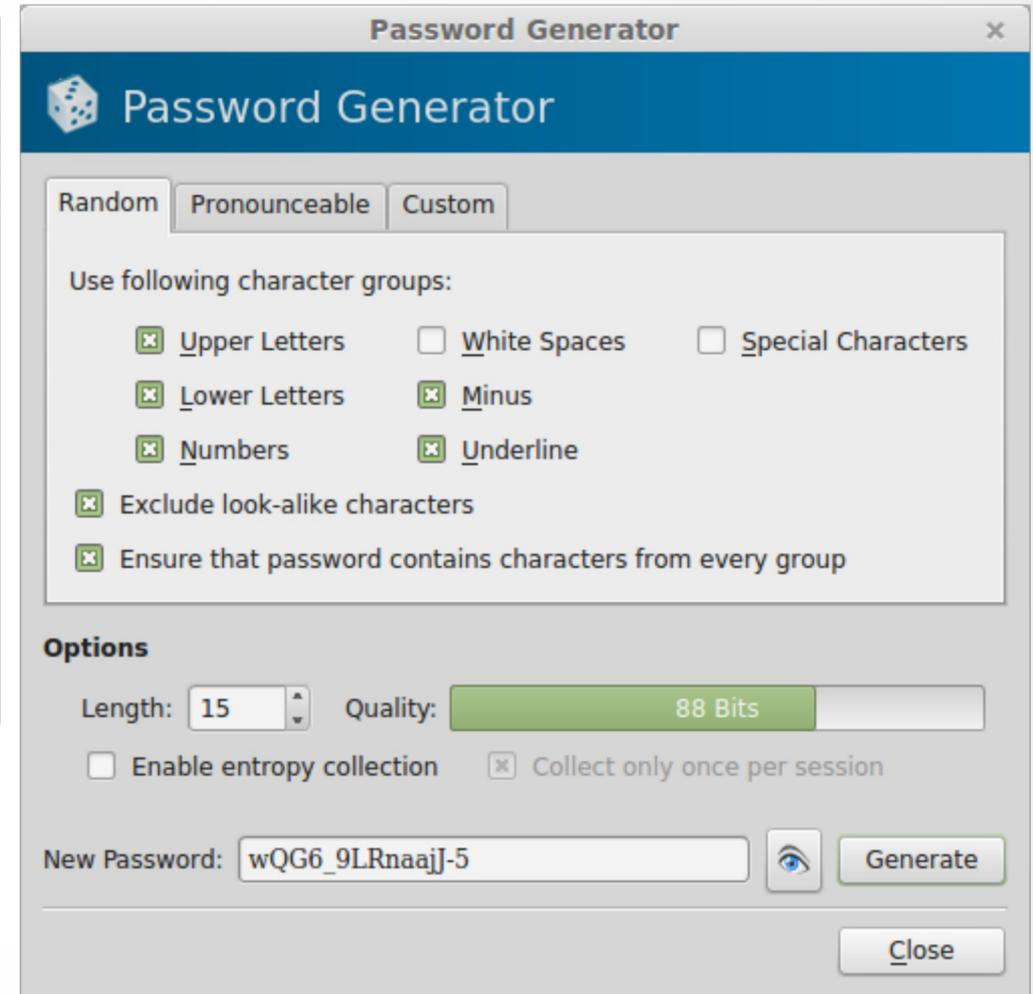
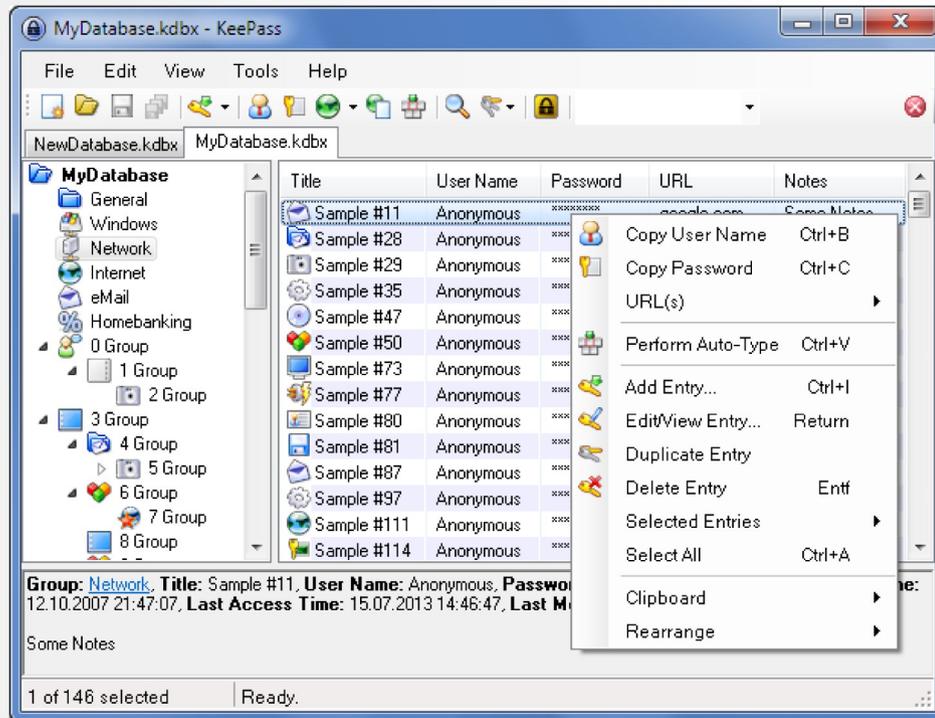


KeePassXC: <https://keepassxc.org>

- Neueste Version für Windows, Linux, MacOS X

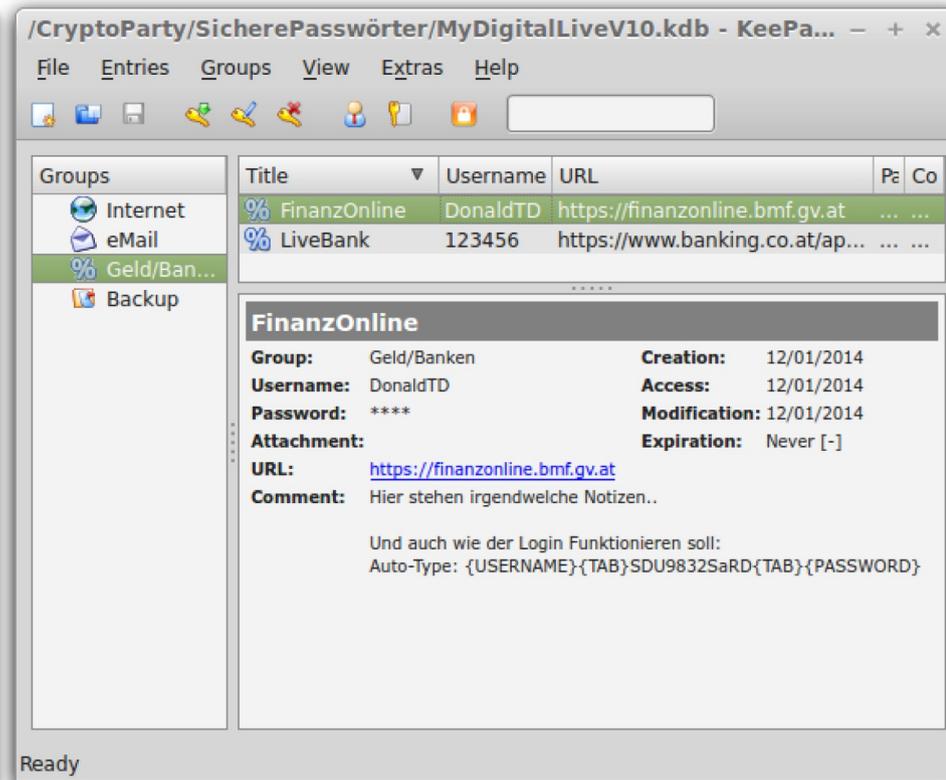
Andere Passwort-Manager bitte recherchieren:
Suchen auf <https://www.heise.de/security/>

Password-Safe: KeePass / KeepassX / Keepass2Android



3.) Welche Methoden/Hilfsmittel gibt es?

Passwort-Safe: KeePass / KeepassX / Keepass2Android



3.) Welche Methoden/Hilfsmittel gibt es?

Schlussworte

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