



Passwörter erstellen und verwalten mit KeePass

Unsicheres Passwort!

abc123



G%v97J+A

Sicheres Passwort!



Login

 Username

 Password

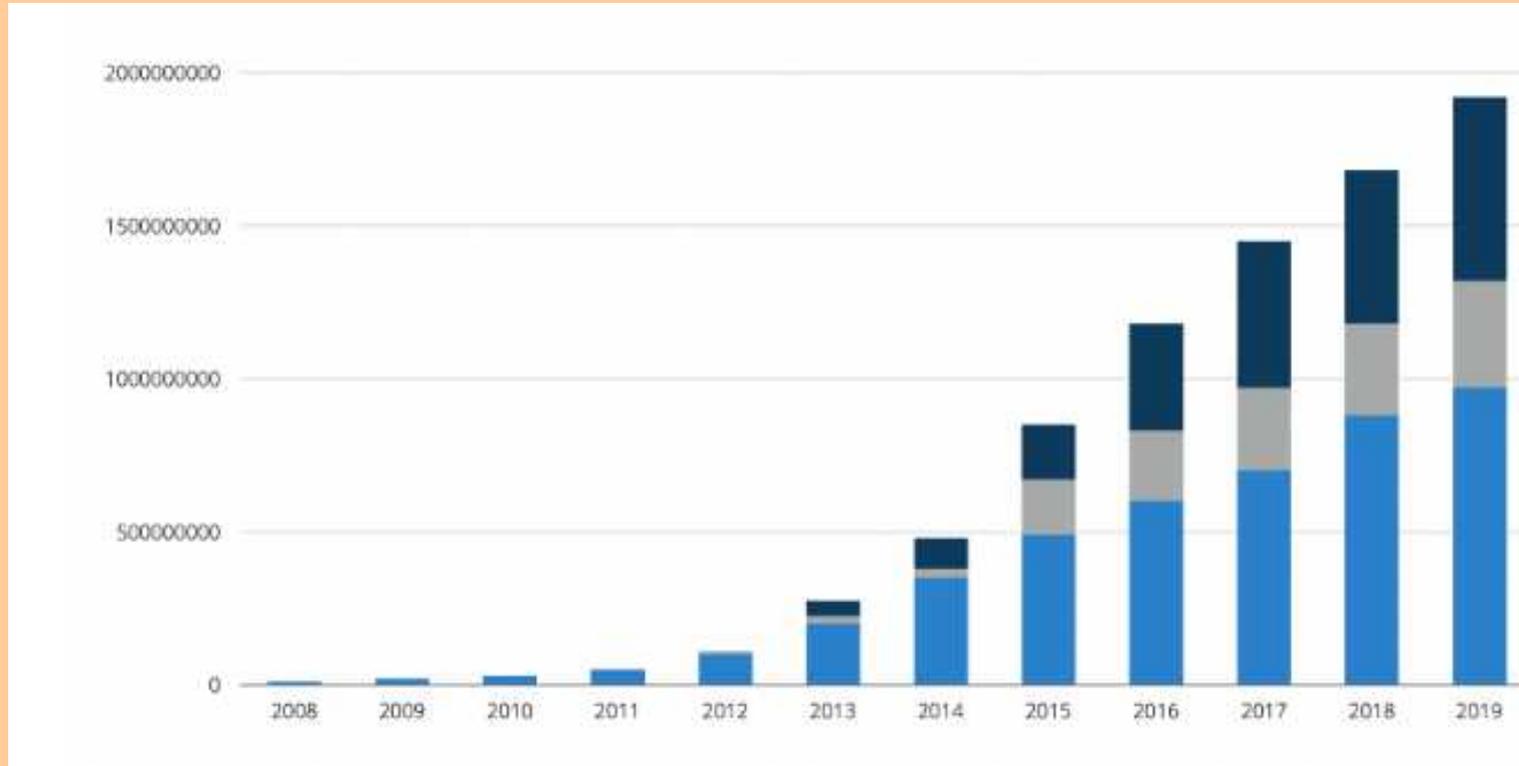
Remember me

[Forgot your password?](#)

LOGIN

Download from
Dreamstime.com
This watermarked comp image is for previewing purposes only.

ID 49685600
© Micha Klootwijk | Dreamstime.com



- | | | |
|---------------------|---------------------|---------------------|
| 1. 123456 | 9. dragon | 17. access |
| 2. password | 10. football | 18. shadow |
| 3. 12345 | 11. 1234567 | 19. master |
| 4. 12345678 | 12. monkey | 20. michael |
| 5. qwerty | 13. letmein | 21. superman |
| 6. 123456789 | 14. abc123 | 22. 696969 |
| 7. 1234 | 15. 111111 | 23. 123123 |
| 8. baseball | 16. mustang | 24. batman |
| | | 25. trustno1 |

Splash Data vom 21.01.2015

Schadprogramme

- Viren, Würmer oder Trojanische Pferde

Phishing

- Gefährliche Umleitung für Ihre Passwörter

Botnetze

- sehr viele PCs – meist mehrere Tausend per Fernsteuerung zusammengeschlossen und zu bestimmten Aktionen missbraucht werden

Spam

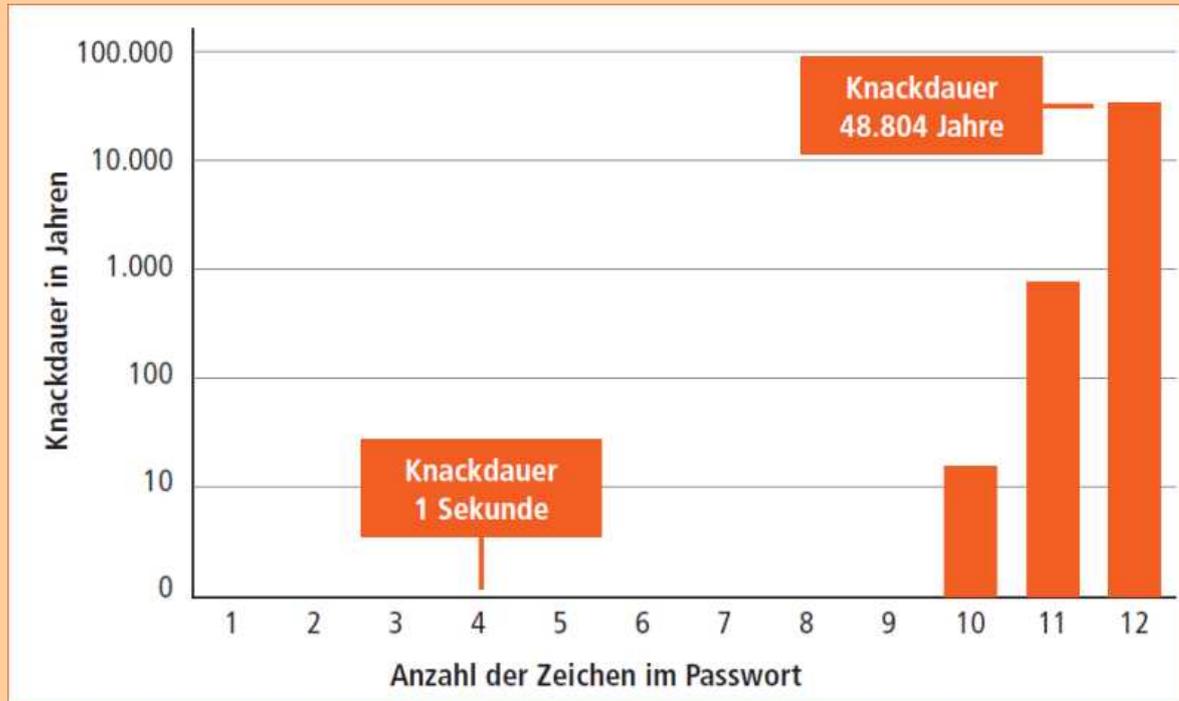
- unerwünschte Werbe-E-Mails, die den Posteingang verstopfen

Auszug aus KeePass – insgesamt über 170 Einträge!



The screenshot shows the KeePass application window. On the left is a tree view of folders, and on the right is a list of password entries. The entries are as follows:

Title	User Name	Password	URL
↑ Deutscher Bundestag		*****	
↑ E-Mail GMX		*****	
↑ E-Mail Google		*****	
↑ E-Mail MICROSOFT Hotmail		*****	
↑ Flight Gear		*****	
↑ KLACK TV		*****	
↑ München Ticket		*****	
↑ PC-ST Webseite		*****	
↑ PC-Stammtisch		*****	
↑ Süddeutsche		*****	
↑ TCE		*****	
↑ TCE ebusy		*****	
↑ TipToy		*****	
↑ Thunderbird		*****	
↑ SKYPE		*****	
↑ ADOBE		*****	
↑ MICROSOFT Konto		*****	
↑ Hermes		*****	
↑ GOOGLE		*****	
↑ Deutsche Herzsstiftung		*****	
↑ Eat Smarter		*****	
↑ Tennispoint		*****	
↑ PhonerLite		*****	
↑ Firefox		*****	
↑ KommEnergie		*****	
• DropBox		*****	



Je länger, desto sicherer: Die Grafik zeigt, wie lange ein Computer benötigt, der bis zwei Milliarden Passwörter pro Sekunde ausprobieren kann, um ein komplexes Passwort zu knacken.

1. Die Akronym-Methode

Willkommen bei FRITZ!Box

Die Benutzeroberfläche der FRITZ!Box ist mit einem Kennwort geschützt. Melden Sie sich mit dem Kennwort der FRITZ!Box an.

Kennwort

Wenn Sie Ihr Kennwort vergessen haben, klicken Sie [hier](#).

Die Akronym-Methode: Der Satz „Was sind doch die rechtschaffenen Leute für Schurken!“ von Émile Zola ergibt das Passwort **WsdDrLfs!**.

2. Die Satz-Methode

Willkommen bei FRITZ!Box

Die Benutzeroberfläche der FRITZ!Box ist mit einem Kennwort geschützt. Melden Sie sich mit dem Kennwort der FRITZ!Box an.

Kennwort

Wenn Sie Ihr Kennwort vergessen haben, klicken Sie [hier](#).

Die Satz-Methode: Der Satz „Mein zweites Auto war ein roter VW Golf“ führt zum extralangen Passwort **Mein2.Autowar1roter VWGolf**



3. Die Doppelwort-Methode

Willkommen bei FRITZ!Box

Die Benutzeroberfläche der FRITZ!Box ist mit einem Kennwort geschützt. Melden Sie sich mit dem Kennwort der FRITZ!Box an.

Kennwort

Wenn Sie Ihr Kennwort vergessen haben, klicken Sie [hier](#).

Die Doppelwort-Methode: Die Namen der beiden Nachbarn Herr Müller und Frau Schneider ergeben das Passwort **HeMue+FrSc**.



KeePass:
ist ein kostenloser Open-Source-Keyverwalter
mit eigenem Passwortgenerator.

keepass.info/download.html



Vorteile:

- + sichere Verschlüsselung
- + Passwörter generieren
- + Master-Passwort oder Key-Disk

Hinweis: Wer der englischen Sprache nicht mächtig ist kann das Programm zusätzlich mit einer deutschen [Sprachdatei](#) erweitern.

Download-Fakten:

CHIP-Bewertung 1092 Nutzerbewertungen
Sehr gut ★★★★★ 4,2

Kompatibel mit Windows 10
und 10 weiteren Systemen. ▼

Sprache: Englisch

Downloadzahl: 672.649

Version: v2.40 - vom 11.09.2018

Kaufpreis: Gratis

Hersteller: Dominik Reichl

Dateigröße: 3,1 MByte

Kategorie: Passwörter & Co

Rang: 3 / 179 bei CHIP

Verwandte Bereiche: Datenbank, Manager, Passwort, Sicherheit

Versionen von KeePass

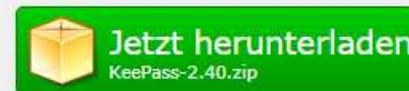
KeePass 2.40

Installer für Windows (2.40):



Laden Sie die obige EXE-Datei herunter, führen Sie sie aus und folgen Sie den Schritten des Installationsprogramms. Sie benötigen lokale Installationsrechte (verwenden Sie die Portable-Version auf der rechten Seite, wenn Sie keine lokalen Installationsrechte haben).

Portable (2.40):



Laden Sie das oben stehende ZIP-Paket herunter und entpacken Sie es an Ihren bevorzugten Ort (USB-Stick). KeePass läuft ohne zusätzliche Installation und speichert keine Einstellungen außerhalb des Anwendungsverzeichnisses.

Unterstützte Betriebssysteme: Windows Vista / 7/8/10 (jeweils 32-Bit und 64-Bit), Mono (Linux, Mac OS X, BSD, ...).

KeePass 1.36

Installer für Windows (1.36):



Laden Sie die obige EXE-Datei herunter, führen Sie sie aus und folgen Sie den Schritten des Installationsprogramms. Sie benötigen lokale Installationsrechte (verwenden Sie die Portable-Version auf der rechten Seite, wenn Sie keine lokalen Installationsrechte haben).



(1.36):



Laden Sie das oben stehende ZIP-Paket herunter und entpacken Sie es an Ihren bevorzugten Ort (USB-Stick). KeePass läuft ohne zusätzliche Installation und speichert keine Einstellungen außerhalb des Anwendungsverzeichnisses.

Unterstützte Betriebssysteme: Windows Vista / 7/8/10 (jeweils 32-Bit und 64-Bit), Wine.

Sie sind unsicher, welche Edition (1.x oder 2.x) Sie wählen sollen? Siehe die [Edition Vergleichstabelle](#) . Siehe auch die [Entwicklungsstatus-FAQ](#) . Verwenden Sie im Zweifelsfall KeePass 2.x.

Vergleich der Versionen von KeePass

Vergleich der KeePass-Edition

KeePass ist in zwei verschiedenen Editionen erhältlich: 1.x und 2.x. Sie unterscheiden sich grundlegend (2.x basiert nicht auf 1.x). Beide Editionen laufen auf Windows auf Mono (Linux, MacOS, BSD usw.).

Siehe auch die [FAQ zum Entwicklungsstatus](#) .

Projekt	KeePass 1.x	KeePass 2.x
Lizenz	Open-Source-Software (GPL)	Open-Source-Software
Kosten	Frei	Frei
Aktive Entwicklung	✓	✓
Installation/Portabilität		
Unterstützte Betriebssysteme	Windows 7, 8, 10, 11, Wine	Windows 7, 8, 10, 11, Linux, MacOS, BSD
Läuft ohne Installation	✓	✓
Läuft vom USB-Stick	✓	✓

<https://keepass.info/compare.html>

Wir überlegen uns ein Masterkennwort, das ...

- Groß und Kleinschreibung beinhaltet ...
- Zahlen und alphanumerische Eingaben enthält ...
- Und zwei Sonderzeichen aufweist!
- z.B. → **!Stammtisch#1234**
- Für jede Anwendung setzen wir den jeweiligen Namen davor
- das ergibt dann **amazon!Stammtisch#1234**

- 37 % aller Nutzer benutzen ein Passwort für alle Anwendungen
- Tabu sind Namen von Familienmitgliedern, Haustieren und Freunden sowie deren Geburtsdaten.
- Vorsicht auch mit Umlauten (ä,ö oder ü)
- Sicherheitsexperten raten zu einem individuellen Passwort für jeden einzelnen Online-Dienst
- Ein gutes Passwort sollte mindestens acht Zeichen lang sein
- Empfehlung des BSI für ein sicheres **Passwort**

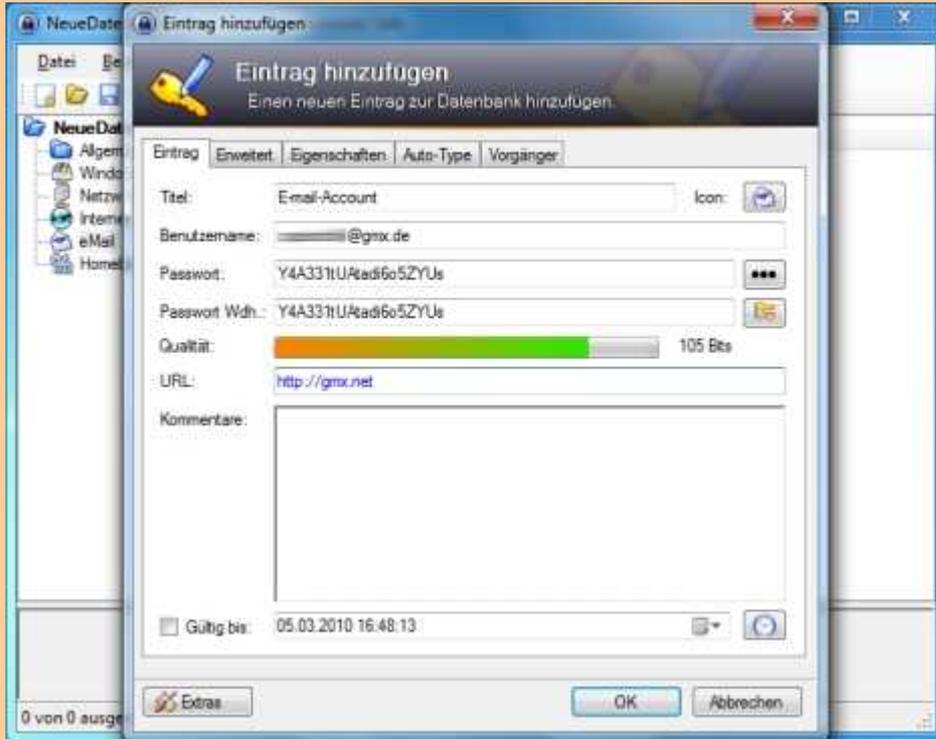


Neue Datenbank erstellen

Im ersten Schritt muss eine neue Datenbank angelegt werden.

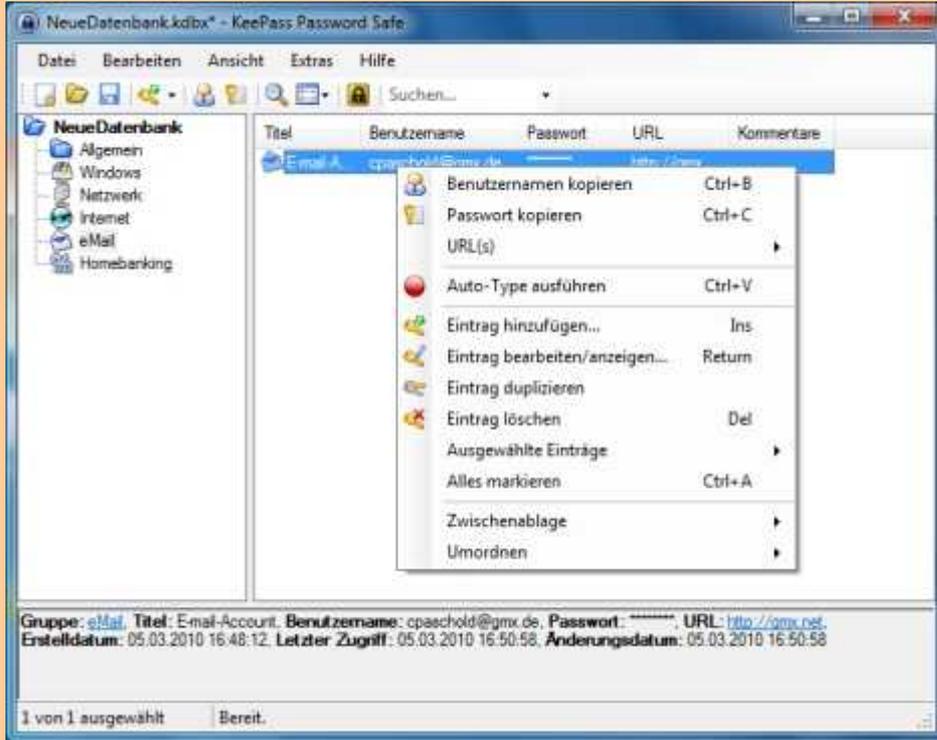
Hierbei vergeben wir das Masterkennwort. Dieses ist äußerst wichtig und darf keinesfalls in falsche Hände geraten. Behalte es am besten für dich.

Anschließend drucken wir das [Notfallblatt](#) aus.



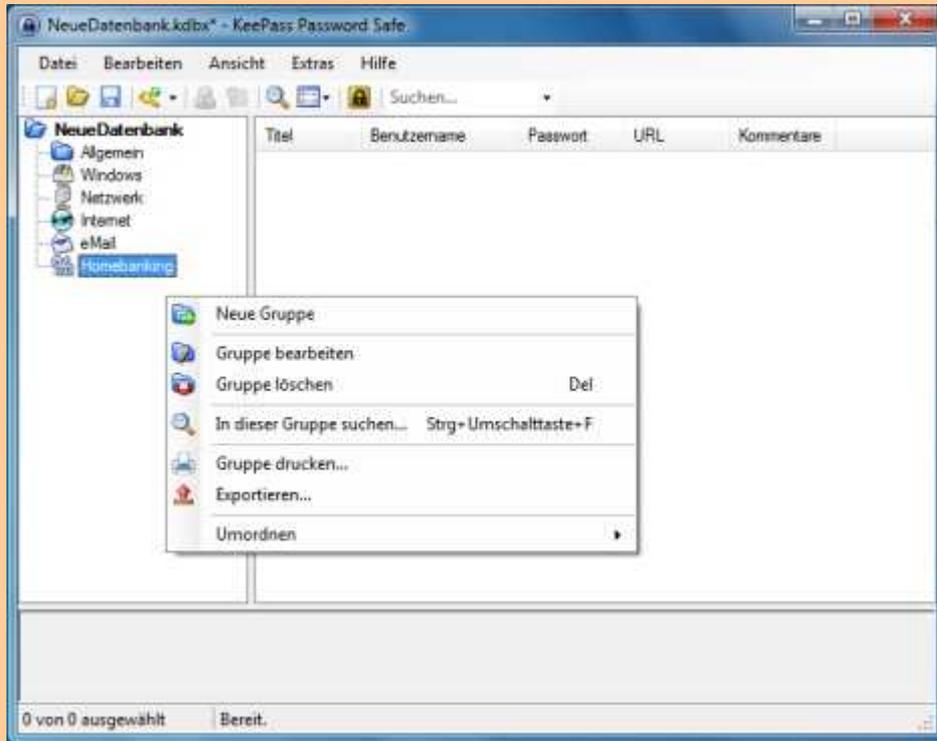
Eintrag hinzufügen

Mit einem Klick auf das Schlüssel-Icon öffnet sich ein neues Fenster, in dem die Daten für einen Zugang angegeben werden



Zugänge schnell nutzen

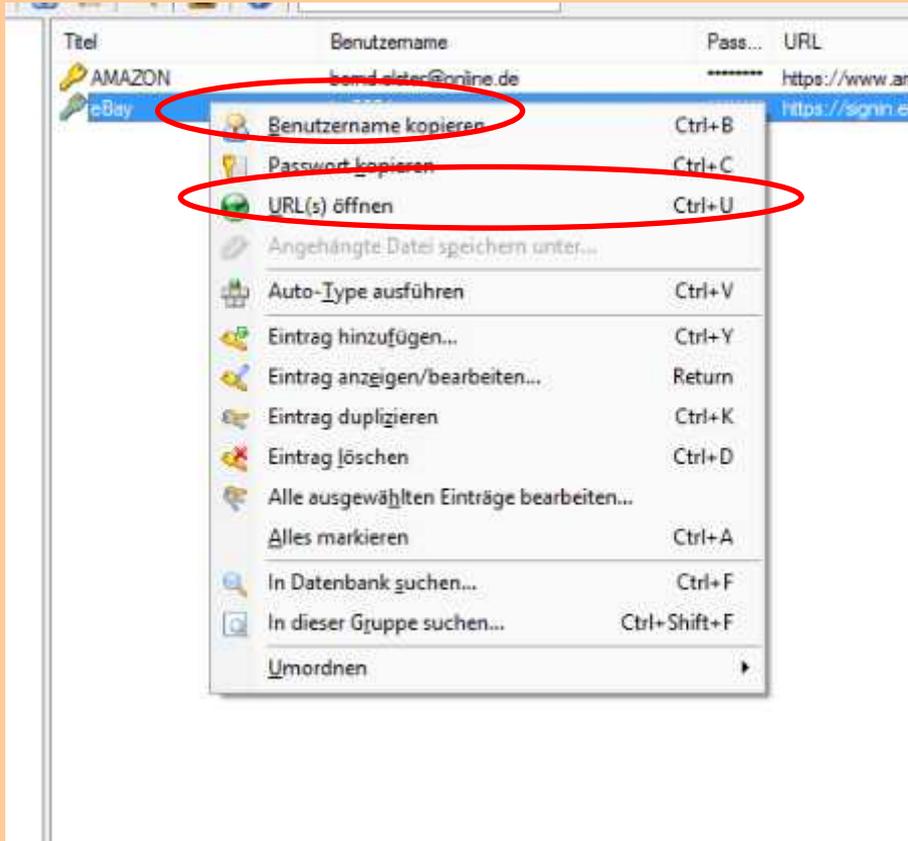
"KeePass" bietet praktische Optionen um den Login so komfortabel wie nur möglich zu gestalten.



Gruppen anlegen

Lege zur besseren Übersicht neue Gruppen an.

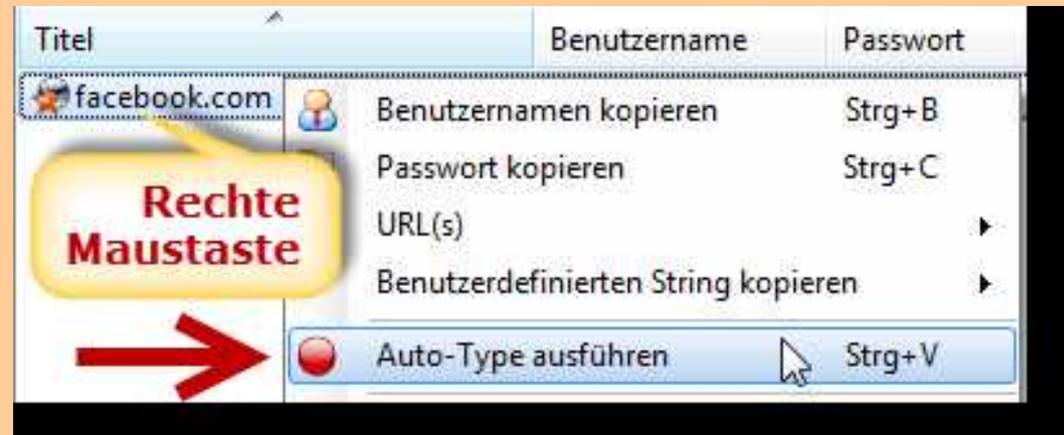
Benenne bestehende Gruppen mit ihrer eigenen Bezeichnung

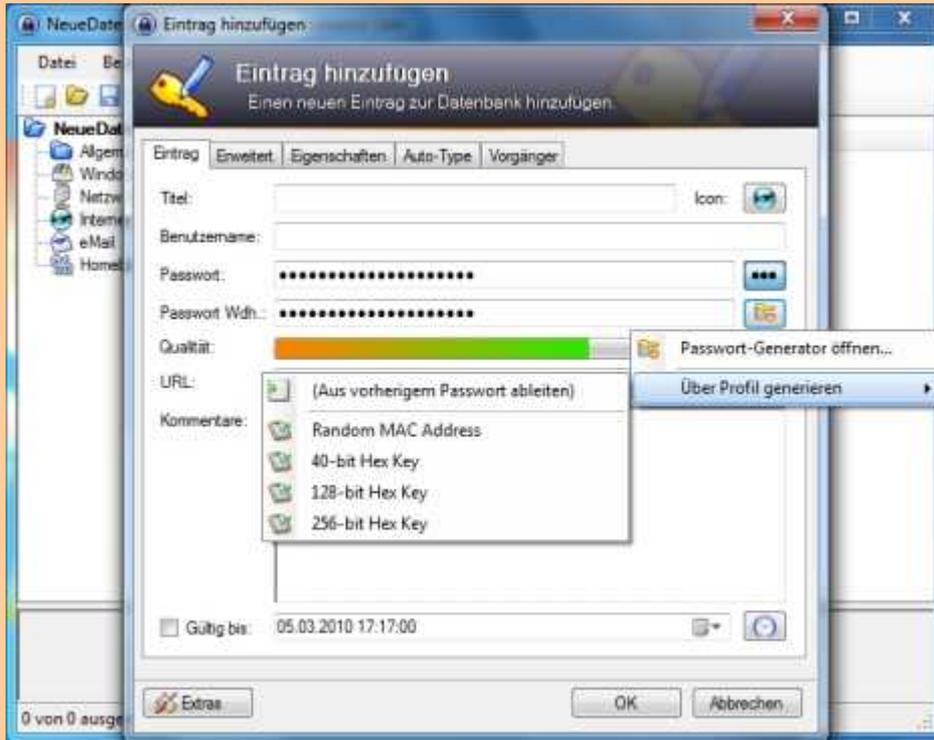


Eingabe mit „Auto-Type“

Die URL öffnen

- Eingabe über die Maus
- oder mit Ctrl+V





Passwort anlegen

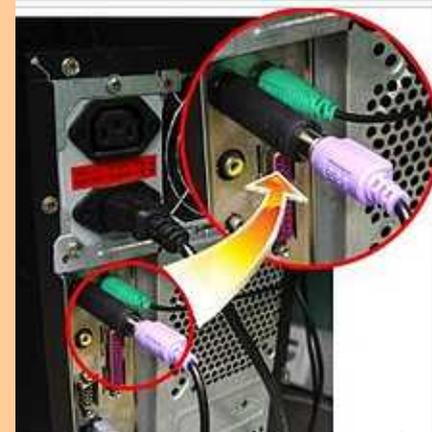
Sichere Passwörter ausdenken fällt schwer. Deswegen bietet "KeePass" einen Passwortgenerator an. Klicke hierfür auf den Schlüssel-Button neben der Eingabezeile für die Passwort Wiederholung

Achtung!

Eines bietet die Auto-Type-Funktion von KeePass aber nicht: den Schutz vor Keyloggern. Diese Schadprogramme überwachen die Tastatureingaben infizierter Rechner und senden die gesammelten Informationen an Ihren Herrn. Da Auto-Type aber nur eine automatisierte Variante der Tastatureingabe darstellt, wird diese Aufzeichnung nicht umgangen



Keylogger-Modul für USB-Tastaturen



ein zwischengesteckter Keylogger auf Hardware-Basis