Passwortmanager

Passwortmanager sind Programme, die alle deine Passwörter, im besten Fall auch mit den zugehörigen Benutzernamen, speichert und durch ein "Masterpasswort" verschlüsselt.

- Generell
- Keepass

Generell

> Passwortmanager sind Programme, die alle deine Passwörter, im besten Fall auch mit den zugehörigen Benutzernamen, speichert und durch ein "Masterpasswort" verschlüsselt.

Eventuell kennst du dieses Prinzip schon, wenn du z.B. auf dem Handy oder in deinem Browser auf "Passwort speichern" geklickt hast. Das Problem daran ist, dass diese Datenbanken, besonders auf deinem Handy und bei Google Chrome von Google sind und dadurch nur durch dein Google-Mail-Account Passwort gesichert sind. Zusätzlich besteht bei Unternehmen die Gefahr, dass diese mit Sicherheitsbehörden zusammenarbeiten. Eine weitere Gefahr besteht darin, dass diese Datenbank online ist und so eine weitere Angriffsmöglichkeit bietet.

Im besten Foll sollte dein Passwortmanager also:

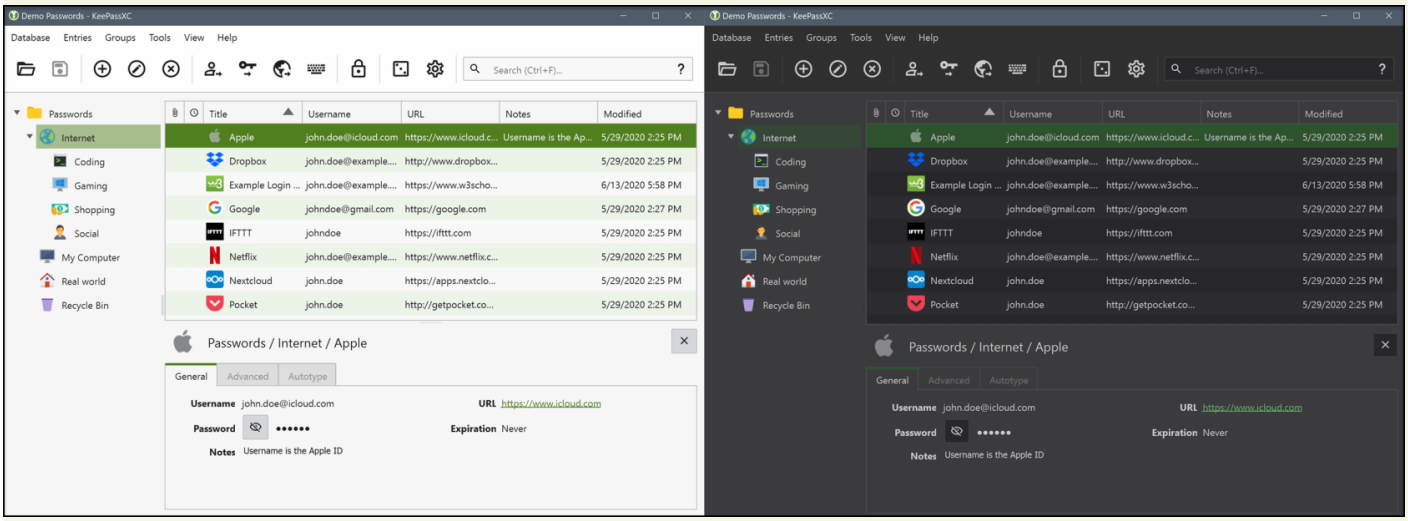
- offline/lokal
- unabhängig
- und Quelloffen sein

Keepass

> Im folgenden stellen wir das KeePass Ökosystem vor. Alle folgenden Programme verwenden die .kdbx-Endung für Passwort-Datenbanken und sind deshalb kompatibel miteinander, ihr könnt also die gleiche Datenbank auf allen Geräten nutzen. Dafür müsst ihr sie synchronisieren, wie das geht zeigen wir auch am Ende.

Zur offiziellen KeePass-Dokumentation

KeepassXC (Mac, Windows, Linux)



1. Verwende ein sichere Haupt-Passphrase für deinen Passwortmanager (mind. 20 Zeichen)
   - Nutze das Diceware Verfahren: https://diceware.dmuth.org/
   - Oder schnapp dir ein Buch aus dem Regal und nimm Wörter von zufälligen Seiten
2. Generiere neue zufällige Passwörter für Accounts mit unsicheren Passwörten mit dem Passwortmanager oder pflege sie ein.
3. **Erstelle unbedingt ein Backup deiner Datenbank (z.B. in deiner Nextcloud)!**

Browserintegration

> Auf dem PC lassen sich auch Browserintegrationen einstellen, d.h. du musst die Passwörter nicht immer herauskopieren, sondern sie werden nach dem Entsperren der Datenbank einfach eingefügt.

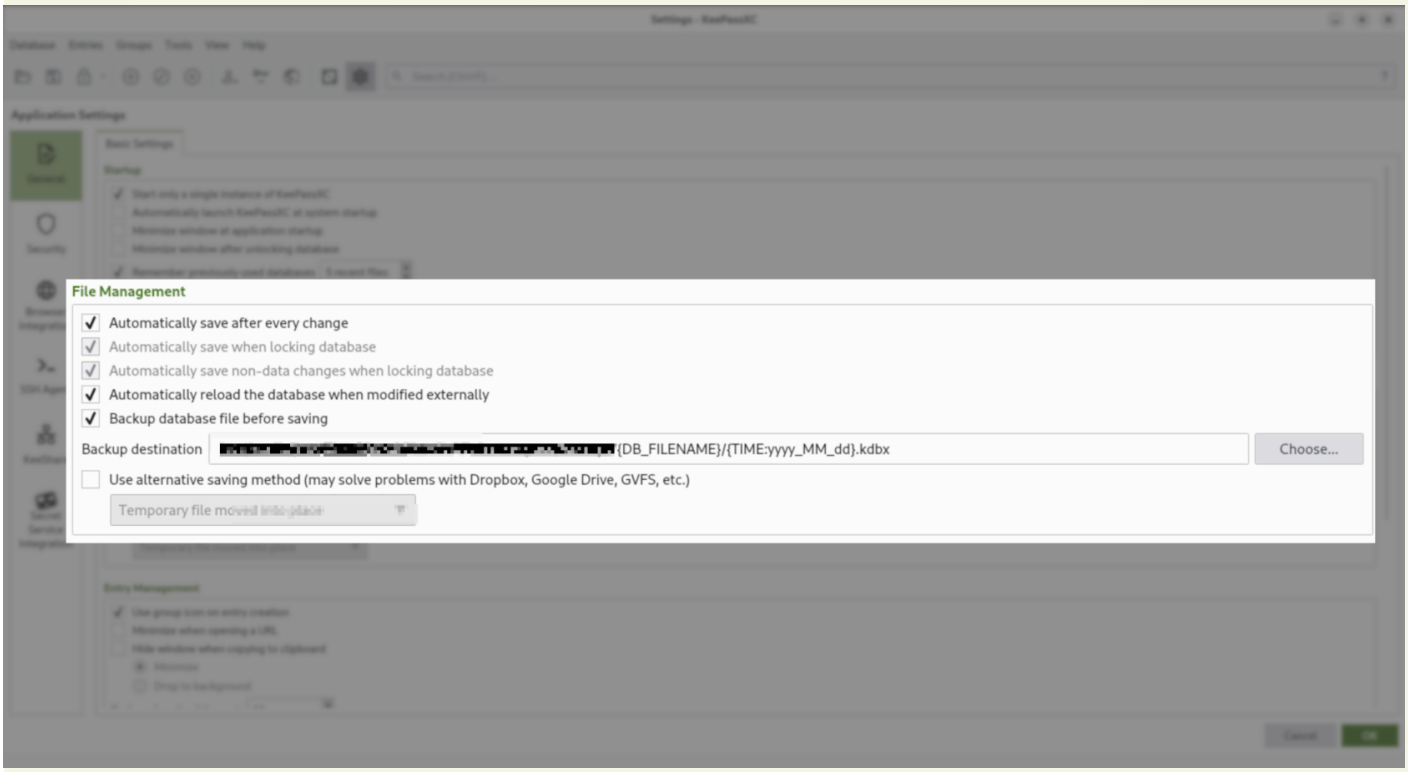
Automatische Backups bei jeder Änderungen

>

> Auf dem PC lassen könnt ihr mit KeePassXC automatisch Backups nach jeder Änderung erstellen.

Die Aktivierung dieses Feature lässt euch sicher gehen, dass ihr Zugnang zu älteren Versionen eurer KeePass Datei habt. Und zudem habt ihr, wenn ihr die Haupt-Keepass-Datei verliert, ein Backup (wenn auch nicht eine aktuelle Version).

In den Datenbankeinstellungen unter der Kategorie "General" könnt ihr "Backup database file before saving" aktivieren und dann einen Pfad festlegen, wo diese Back-ups gespeichert werden. Verwendet in der Benennung eurer Datei auf jeden Fall die verschiedenen Platzhalter für z.B. den Dateinamen und den Tag der Speicherung (Ansonsten werden alte Versionen bei jeden Backup überschrieben!) Seht dafür das Beispielbild:



KeePassDX (Android)

ToDo

KeePassium (iOS)

ToDo

KeePass via Nextcloud synchronisieren

> Für diese Variante benötigst du eine funktionierende Nextcloud-Synchronisation!

Desktop

Öffne die Datenbank direkt aus deinem WebDav-Ordner mit KeePassXC - sie sollte dann dort in der KeePass-History erscheinen und du kannst sie dann immer direkt dort auswählen

Android

> Es könnte sein, dass es mittlerweile auch direkt funktioniert wenn man die .kdbx-Datei aus der Nextcloud-App öffnet.
> Wir testen das weiter und updaten das dann hier.

1. Öffne deine Nextcloud App und synchronisiere die KeePass-Datenbank (indem du draufklickst) - mit dieser Variante kannst du die Datenbank auch öffnen, aber nur einmalig.
2. Öffne deinen Dateimanager > Interner Speicher > Android > media > com.nextcloud.client > user@cloud.example.com und suche die KeePass-Datei in deiner Ordner-Struktur > klicke darauf > Öffnen mit KeePassDX
3. Die Datenbank sollte jetzt in deiner keePass-History erscheinen und von dort immer wieder zu öffnen sein.