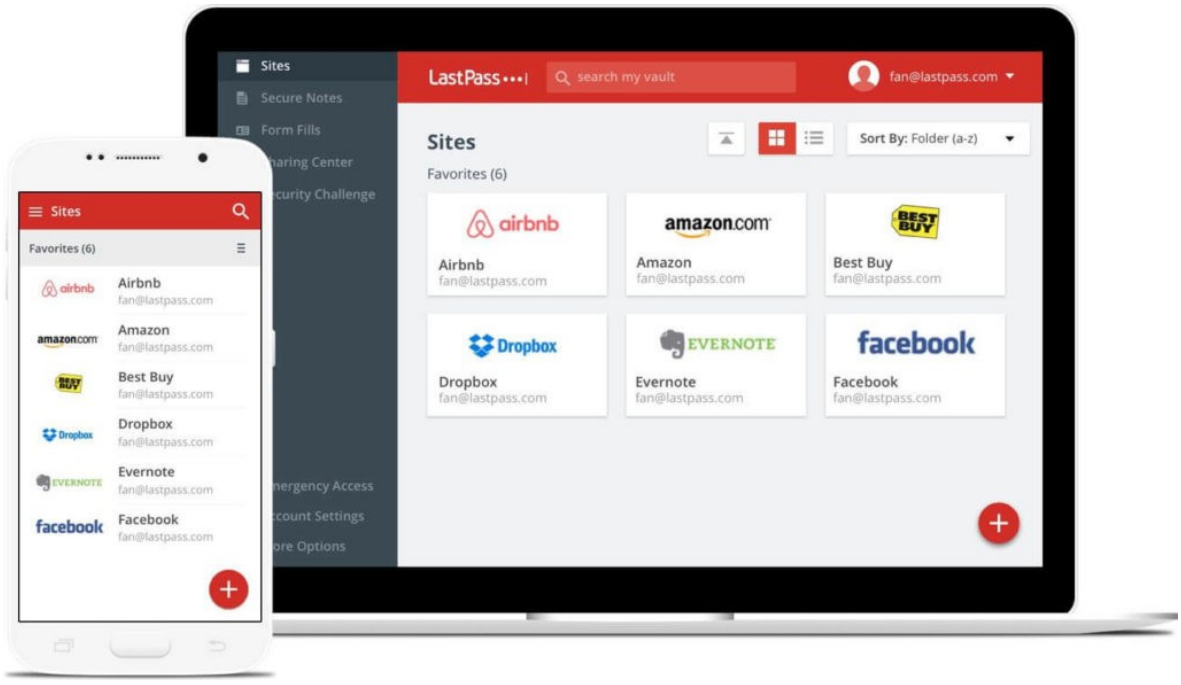
Wie ich alle meine Passwörter unter Linux mit FOSS verwalte

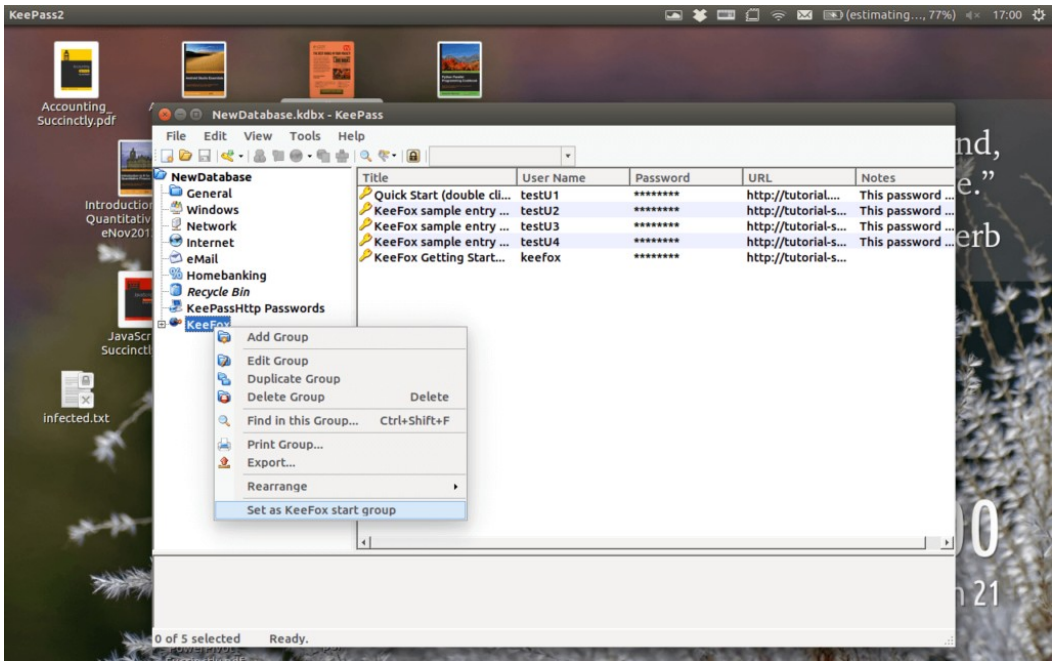
Für die letzten Jahren habe ich LastPass verwendet, um meine Passwörter zu verwalten. Das ist eine proprietäre Freemium-App, in der alle deine Passwörter hinter einem Hauptpasswort gespeichert werden. Solange du dich an das Master-Passwort erinnerst, kannst du alle gespeicherten Passwörter entsperren. Diese App hat eine Browsererweiterung, die es für dich sehr einfach macht, da sie automatisch Webseiten ausfüllt und die einzige Sache, die du tun musst ist, nur auf ein Symbol zu klicken. LastPass fügt die Anmeldeinformationen ein und du wirst sofort angemeldet. Super einfach. Wenn du dich jemals auf einer neuen Website registrierst, erkennt das LastPass und fragt dich, ob du die neuen Anmeldeinformationen speichern willst. Es hat sogar einen Passwortgenerator für die Generierung sicherer Passwörter. Da ich ihn verwende, sehen meine Passwörter in etwa so aus: 3V $% ervwEWFCGw4 _?=Ky – Ich muss sie mir nicht merken, LastPass wird das tun. Mit solchen extrem sicheren Passwörtern kannst du sicher sein, dass sie so gut wie nicht zu hacken sind.

Seit ich LastPass verwende habe ich tausende von Anmeldeinformationen „gesammelt“ und dort gespeichert. Ich kenne also ein einziges Master-Passwort und für hunderte von Webseiten weiß ich nicht ein einziges Passwort.



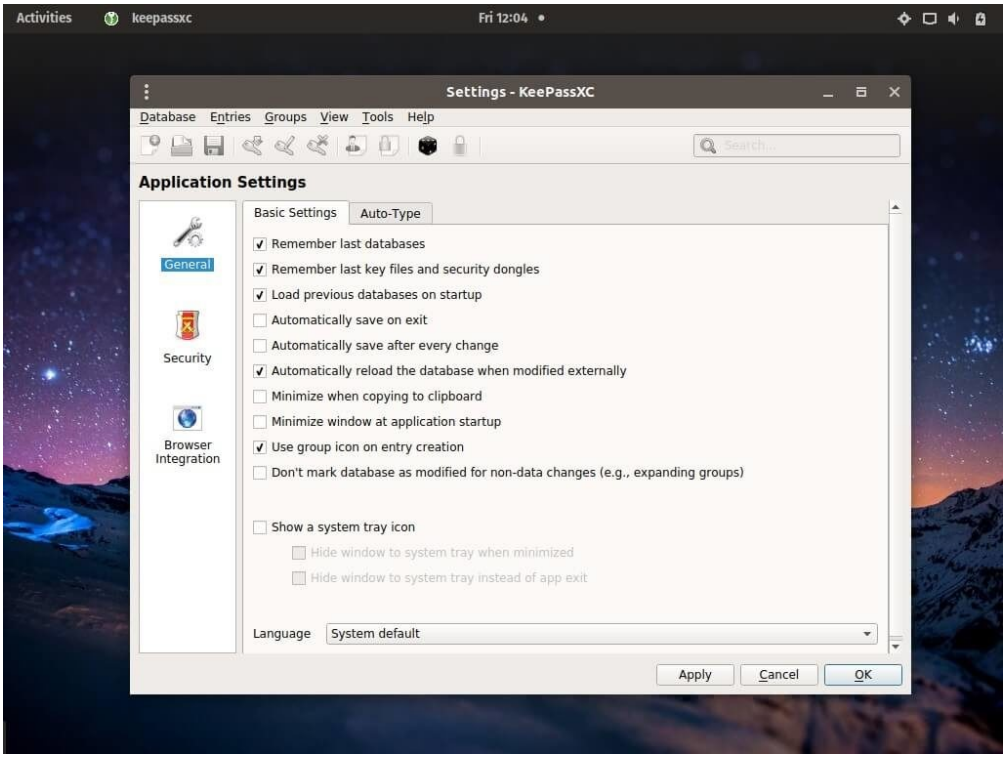
LastPass ist eine proprietäre Software. Du weißt also nie genau, was sie mit deinen Daten machen oder ob sie in der Lage sind, sie zu schützen. Außerdem fehlen der kostenlosen Version einige seiner Premium-Funktionen. Darüber hinaus sammelt LastPass wie die meisten „kostenlosen“ Dienste aus verschiedenen Gründen deine Daten (Quelle).

Aber dann habe ich mich entschieden, damit komplett auf Open Source zu wechseln. Und ich habe KeePass gefunden. Dies ist wahrscheinlich der bekannteste und robusteste Open-Source-Passwortmanager. Aber seine Benutzeroberfläche ist scheiße. Es sieht aus, als ob es vor 20 Jahren entworfen wurde.



Kein Screenshot von meinem Computer.

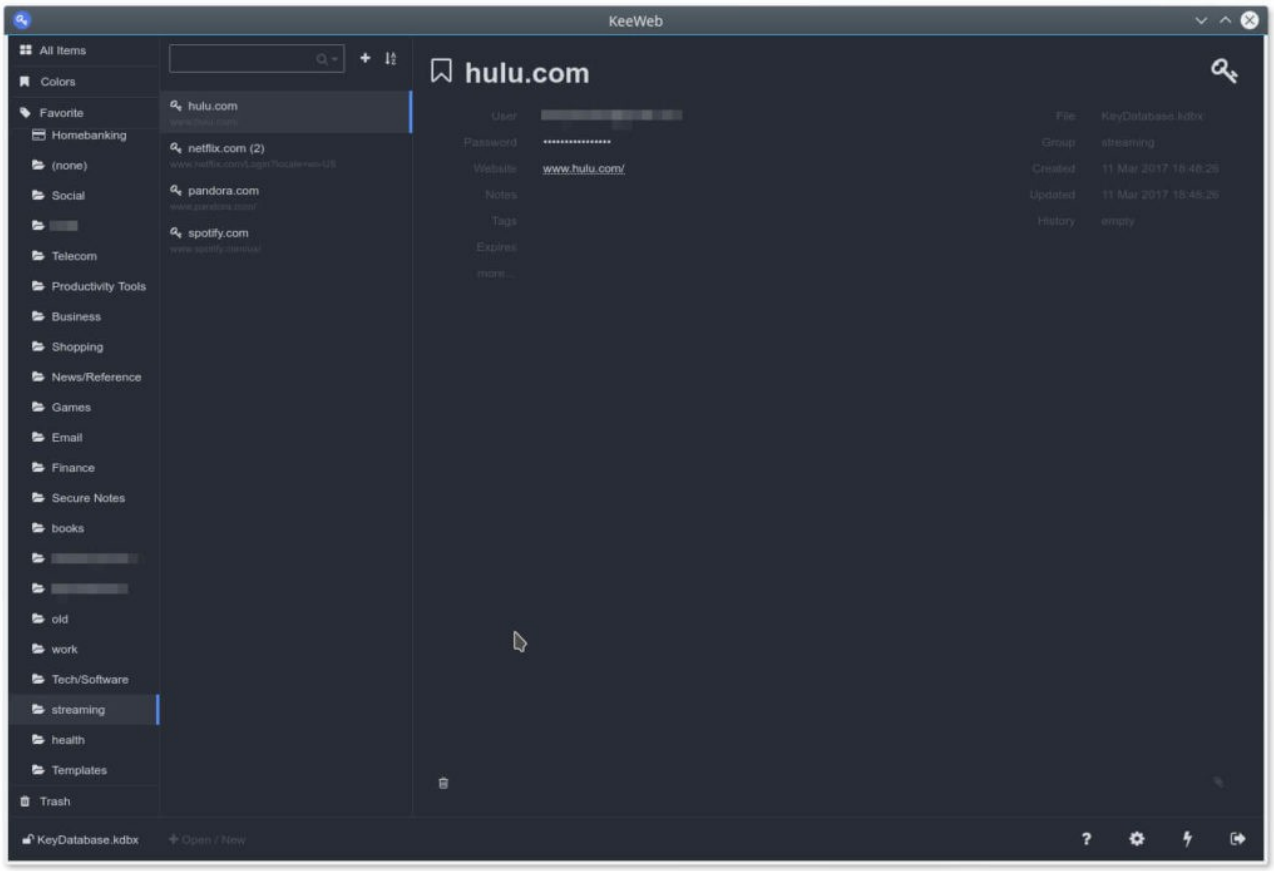
Da es jedoch ein Open Source-Projekt ist, mutiert es in verschiedene Formen. Ich habe dann eine schöne Mutation namens KeePassXC gefunden – schöner aussehend und für Linux angepasst.



Kein Screenshot von meinem Computer.

Ich installierte es. Dann ging ich zu meinem LastPass-Konto (Website) – Weitere Optionen – Erweitert – Exportieren. Ich habe meine Passwörter exportiert – sie werden als Klartext angezeigt. Kopiere diesen Text in einen Texteditor, speichere ihn als CSV-Datei (.csv) und stell sicher, dass du die Kodierung vor dem Speichern als UNICODE (UTF-16) auswählst. Jetzt hatte ich mein gesamten Passwörter als CSV-Datei. Geh zu KeePassXC, importiere CSV und wähle ein Hauptpasswort aus – kann das gleiche, wie das LastPass-Passwort sein. Nun kommt der wichtige Teil: Stell sicher, dass du die Tabellen richtig auswählst, sodass der Benutzername-Tab mit den LastPass-Benutzernamen, der Passwort-Tab mit den LastPass-Passwörtern usw. gefüllt ist. Du wirst feststellen, dass es sehr einfach ist – du musst nur ein paar Dinge auswählen. Das ist alles. Jetzt habe ich meine Passwörter in KeePassXC importiert. Und jetzt lösche die verdammte CSV-Datei :D. Es ist unnötig eine solche Datei mit allen Passwörtern auf dem eigenen Computer oder an einem anderen Ort aufzubewahren.

Aber ich war nicht glücklich, ich brauche einen besseren KeePass-Mutanten und eine bessere Integration mit Chromium. KeeWeb! – großartige Benutzeroberfläche und super einfach zu bedienen. In Bezug auf die Benutzeroberfläche hast du mehrere Themes: dunkel, hell etc..



Kein Screenshot von meinem Computer.

Hab´s heruntergeladen und installiert. Bin zurück zu KeePassXC (dem halb-hässlichen) und hab die Datenbank als .kdbx-Datei gespeichert. Ich hab KeeWeb geöffnet und sie importiert. Migration abgeschlossen! Meine LastPass-Datenbank wurde in KeeWeb importiert. Im Grunde genommen habe ich KeePassXC nur verwendet, um die LastPass CSV-Datei korrekt in eine ordentliche KeePass-Datenbank (Datei) zu konvertieren.

Jetzt konnte ich mit den KeeWeb-Einstellungen herumspielen, z. B. „Zwischenablage nach dem Kopieren löschen“, oder wann die App gesperrt werden soll etc.. Aber ich wollte sie auch in Chromium integrieren, weil das der Punkt ist. Um das zu tun, geh zu den Einstellungen, dann zu den Plugins und such nach dem Plugin „keewebhttp“. Installiere es. *Anmerkung: Bei Firefox brauchst du das nicht – du brauchst nur die Erweiterung “KeePassXC-Browser”. Du findest sie, wenn du bei den Add-ons nach “KeePassXC-Browser” suchst.*

Nun installiere ich eine Browsererweiterung namens chromeIPass. Das ist auch Open Source. Das ist es. Wenn du auf die Erweiterung klickst, wirst du aufgefordert, eine Verbindung zu KeeWeb herzustellen. Verbinde es und du bist fertig.

Jetzt habe ich meine LastPass-Datenbank in das KeePass-Format konvertiert, über KeeWeb (der schöne Mutant) verwaltet und über ChromeIPass mit meinem Chromium verbunden.

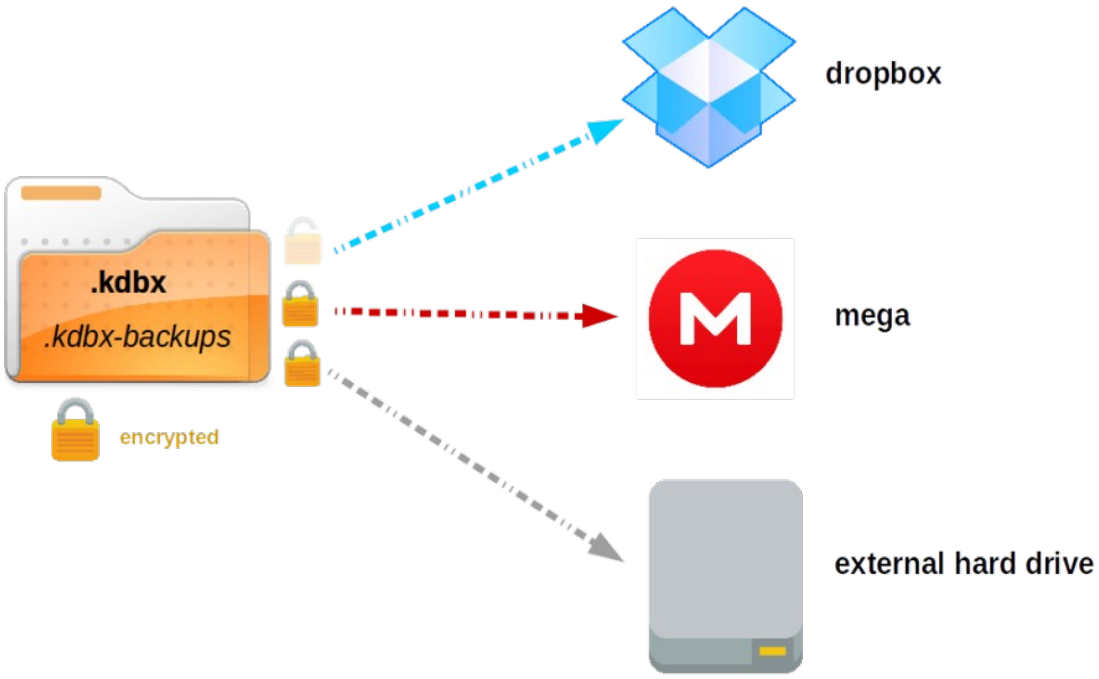
Solange KeeWeb auf deinem System geöffnet ist und du angemeldet bist, funktioniert die Browsererweiterung genau wie LastPass. Sie erkennt Webseiten und Anmeldeformulare automatisch und füllt die Anmeldungen für dich aus. Super cool! Du kannst KeeWeb so einrichten, dass es niemals geschlossen wird.

Aber jetzt kommt das Großartige 😀 – bereit?

Vielleicht denkst du: Warum all dieses Getue? Warum von LastPass zu diesem wechseln, nur weil es Open Source ist? Nun, weil es verdammt geschickt ist und ich sage dir warum. Das einzige, was KeePass (das Original) benötigt, ist diese .kdbx-Datenbank. Diese Datei enthält alle deine Passwörter und Anmeldeinformationen. Diese Datei wird mit deinem Master-Passwort verschlüsselt. Du kannst diese Datei an eine beliebige Stelle verschieben. Lass sie auf deinem Computer, damit du weißt, dass alle deine Passwörter dir gehören und nur von dir und nicht von einem Drittanbieter gehostet werden. Niemand kann diese Datei öffnen, außer dir (mit dem Master-Passwort). Und du kannst coole Sachen damit machen – diese Datenbank funktioniert mit jeder KeePass-Fork (Mutant). Du magst KeeWeb nicht? Kein Problem, wechsel zum originalen und funktionsreicheren KeePass. Die von mir installierte Chromium-Erweiterung funktioniert auch mit allen KeePass-Mutanten.

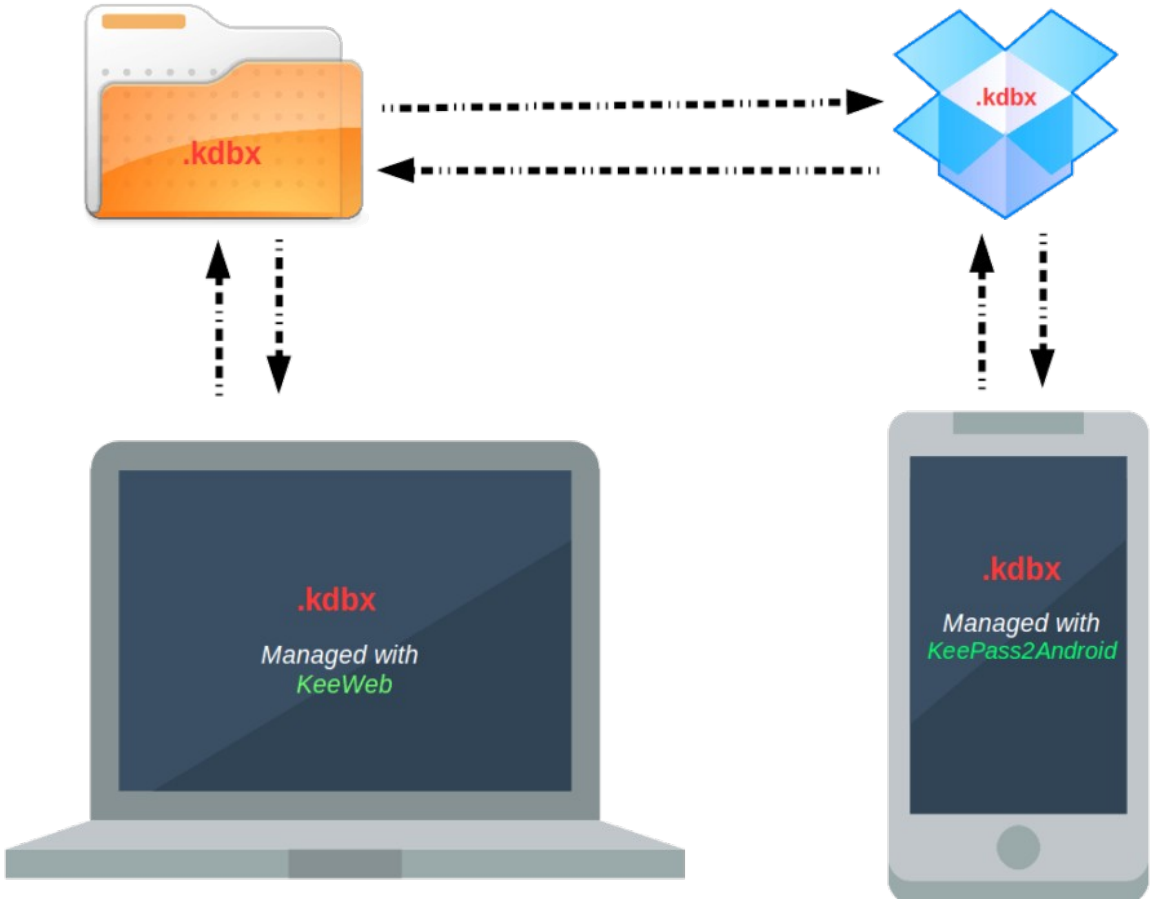
Und das habe ich mit meiner .kdbx-Datenbank (meinen Passwörtern) gemacht: Ich habe sie als einfache Datei auf meinem Computer gespeichert. Jetzt gibt es für KeeWeb eine Backupoption, und ich habe mich dafür entschieden, jedes Mal, wenn ich die Datenbank ändere (ein neues Kennwort hinzufüge, etwas ändere etc.), Backups (Sicherungskopien) auf meinem Computer zu erstellen. Ich habe also meine .kdbx-Datei + Sicherungskopien davon in einem Ordner auf meinem Computer. Sie sind schon verschlüsselt. Ich mache aber auch täglich verschlüsselte Sicherungen meiner Ubuntu-Systemdateien auf einer externen Festplatte. Daher werden die .kdbx-Datei und ihre Backups neben meinen anderen Betriebssystemdateien auch täglich auf meiner externen Festplatte gesichert. **Nicht genug!** :D. Jetzt synchronisiere ich diesen Ordner mit meiner rohen .kdbx-Datei und deren Backups zu meiner Dropbox und Mega.

Ok, lass uns zusammenfassen. Ich habe auf meinem Computer einen Ordner, in dem sich die .kdbx-Datei und ihre Backups befinden. Dieser Ordner wird mit Dropbox und Mega + auf meiner externen Festplatte gesichert.



Warum das alles? Zum einen aus Sicherheitsgründen (das ist das externe Festplatten-Backup, das ich mache und die Mega-Synchronisierung), und zum anderen, sobald die .kdbx-Datei auf Dropbox gespeichert ist, kann ich sie auf meinem Handy verwenden – du kannst Google Drive oder WebDAV auch dafür verwenden, aber Dropbox war für mich die einfachste Lösung. **So geht das:**

Lass uns jetzt den Passwort-Manager KeeWeb mit dem Smartphone synchronisieren. Installiere das Open Source Keepass2Android auf deinem Smartphone. Klick dann auf “Datei öffnen” und wähle Dropbox aus. Wähle jetzt die .kdbx-Datei aus, die du mit deiner Dropbox synchronisiert hast. Gib das Master-Passwort ein und melde dich an. Erledigt! Jetzt verwenden deine App auf deinem Desktop (KeeWeb) und deine App auf deinem Smartphone (Keepass2Android) genau die gleiche Passwortdatenbank und diese Datenbank wird an mehreren Orten synchronisiert und gesichert. Wenn du etwas in deiner Desktop-App änderst (wie z. B. einen neuen Benutzernamen hinzufügen oder ein Kennwort ändern), dann werden die Änderungen auf deinem Telefon angezeigt, da sie an Dropbox gesendet werden. Und andersherum. Sehr nice! Und natürlich kannst du Keepass2Android mit deinem Fingerabdruck entsperren, sodass du nie das Datenbankpasswort eingeben musst. Du kannst die Einstellungen auch an deine Bedürfnisse anpassen.



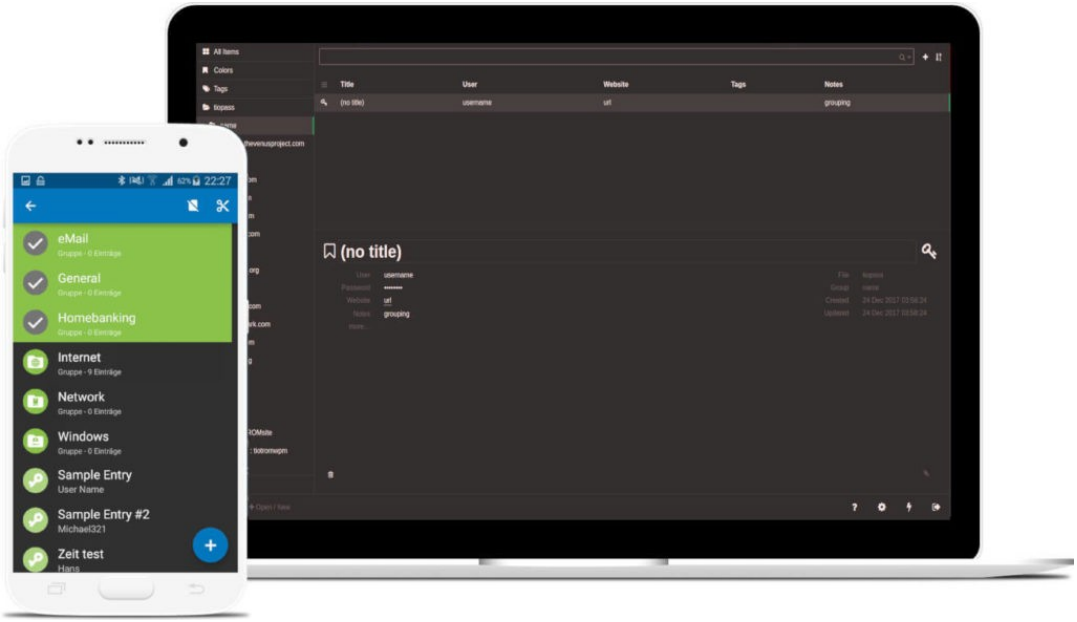
Lass mich das betonen: Jetzt sind alle meine Passwörter in einer Datei mit einem Master-Passwort gespeichert, das nur ich kenne. Das Passwort ist stark genug. Diese Datei kann mit vielen kostenlosen und Open-Source-Apps freigeschaltet und verwaltet werden, sodass sie deine Daten nicht erfassen oder etwas falsch machen. Diese Datei wird ebenfalls wie verrückt an mehreren Orten gesichert und synchronisiert, sodass ich sie von jedem beliebigen Gerät aus verwenden kann.

Ich habe volle 100% Kontrolle über meine Passwörter/Konten. Auch wenn ich die Datei auf Dropbox legen musste, um sie problemlos mit dem Smartphone synchronisieren zu können, ist die Datei bereits verschlüsselt, sodass Dropbox oder andere Personen nicht lesen können, was darin enthalten ist.

Du denkst vielleicht, dass die Verwendung von KeeWeb oder der Wechsel von LastPass zu Keeweb ein bisschen kompliziert ist. Aber das ist es auf gar keinen Fall, wenn du den Vorteil der vollständigen Kontrolle über deine Kennwörter und Kontenanmeldedaten bedenkst. Sobald du die .kdbx-Datei (die Datenbank) erstellt hast, kannst du sie mit verschiedenen Apps (online oder offline) auf jedem Gerät beliebig verwenden. ☺

Sag mir, dass das nicht verdammt cool ist!

So konvertierte LastPass für mich in FOSS.



Kurz gesagt, du brauchst KeeWeb und KeePass2Android.

Dieser Artikel stammt von Tio und ich habe ihn ins Deutsche übersetzt, weil ich ihn spannend, relevant und interessant finde. Hier ist das Original.