KeePass

– Passwörter sicher im Team koordinieren

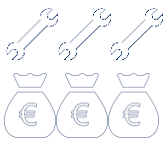
Durch die zunehmende Digitalisierung brauchen wir auch immer öfter Passwörter, um unsere diversen Zugänge zu schützen. Insbesondere wenn es um geteilte Accounts geht, ist die Koordination im Team manchmal schwierig.

Wir haben den Passwortmanager KeePass für dich getestet. Mit dem Tool kannst du sichere Passwörter erstellen und speichern. Diese werden in einer verschlüsselten Datei hinterlegt. Du musst dir somit nur noch ein Master-Passwort merken, das für KeePass. Die Datei kannst du in einem Ordner ablegen, auf den mehrere Mitarbeitende Zugriff haben, wenn ihr euch Zugänge teilt. Aus Sicherheitsgründen empfehlen wir allerdings, Zugänge nur zu teilen, wenn es unbedingt notwendig ist. Nach Möglichkeit sollten Zugänge immer nur für eine Person gelten. Die Datei mit deinen individuellen Passwörtern legst du am besten in einem privaten Ordner ab.

Bitte beachte, dass der korrekte Umgang mit Passwörtern auch zur Einhaltung der Datenschutzgrundverordnung wichtig ist. So müssen Anwendungen, in denen personenbezogene Daten erfasst werden, gegen unbefugten Zugriff geschützt werden. Passwortsicherheit ist dazu unerlässlich. Bitte achte beim Umgang mit Passwörtern immer auf den korrekten Umgang mit den rechtlichen Rahmenbedingungen der Datenschutzgrundverordnung.

Arbeitsaufwand Umsetzung

Finanzieller Aufwand



vhs Bayerischer Volkshochschulverband e.V.

Janina Schubert | Projektmanagerin
E-Mail: janina.schubert@ansbach.de
Telefon: 0981 977 82 31 - 314

vhs Digitalverbund Customer Journey

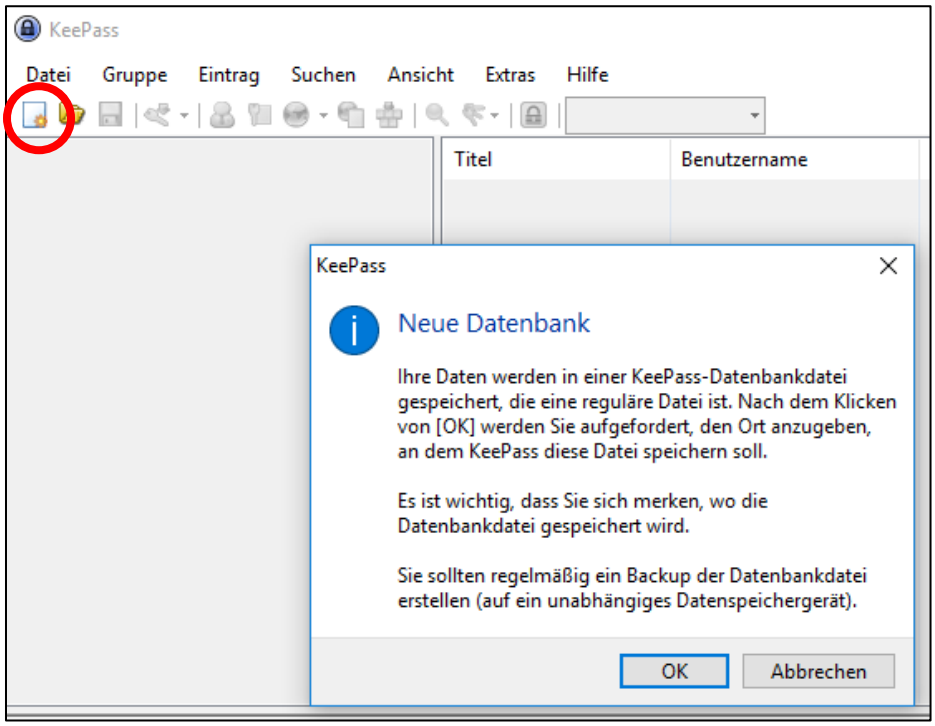
Passwörter sicher koordinieren

1. Öffne die KeePass-Anwendung.

Wenn diese noch nicht installiert ist, kannst du sie dir kostenfrei online herunterladen. Hier geht's zum Download. Du findest die App auch unter dem Namen „KeePassXC“ im Microsoft Store.

2. Lege eine neue Datenbank an.

Unter der Registerkarte „Datei“ kannst du eine neue Datenbank erstellen. Klingt kompliziert? Keine Sorge: Es geht letztlich nur um eine Liste von Websites oder Anwendungen und den zugehörigen Zugangsdaten. Klicke auf „OK“.



3. Wähle einen Namen und einen Speicherort.

Es öffnet sich die normale Ordner-Struktur. Du kannst nun den Ort suchen, an dem du die Passwort-Datei ablegen möchtest und einen Namen vergeben.

4. Erstelle ein Hauptpasswort.

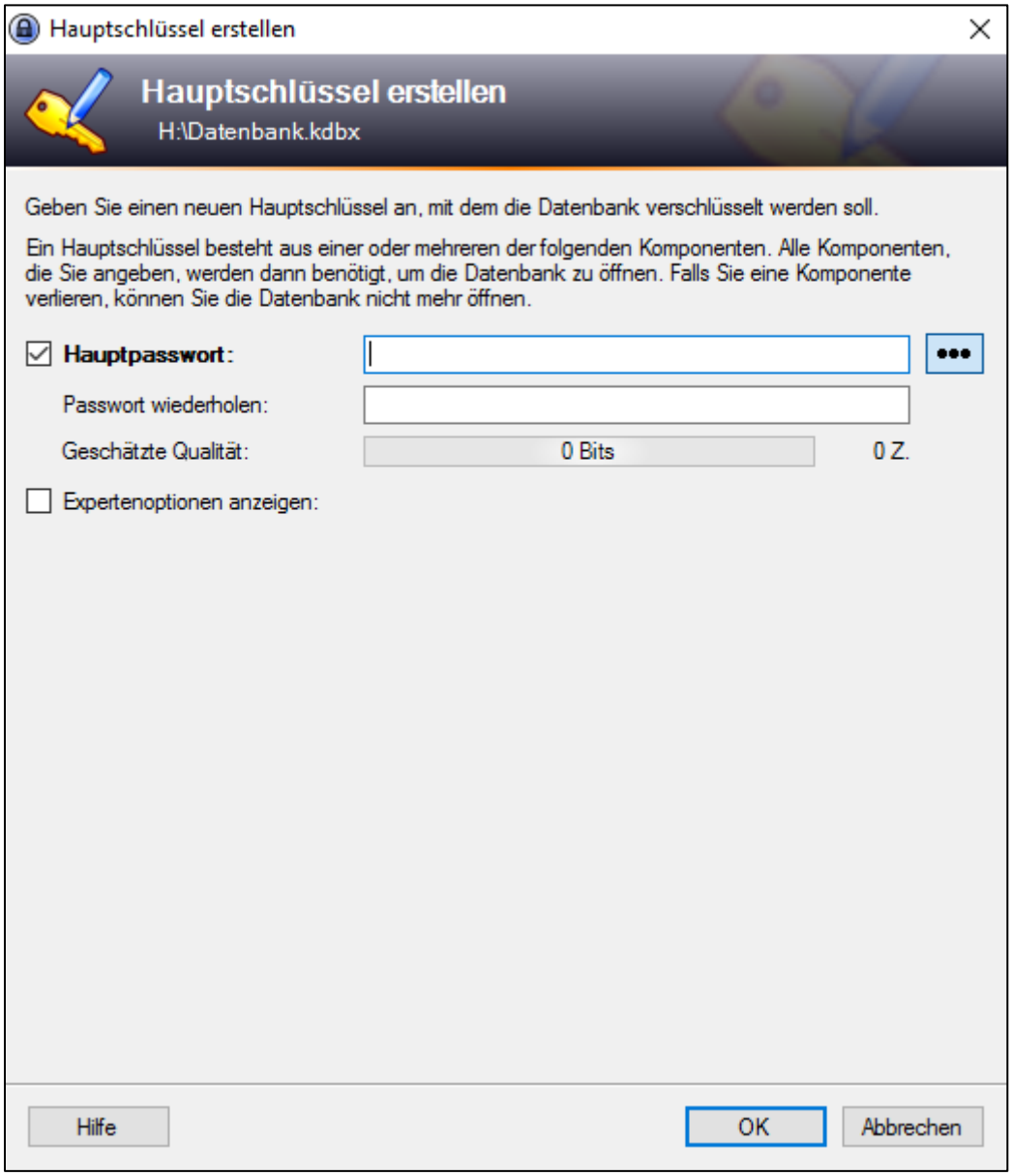
Der nächste Schritt ist sehr wichtig. Du musst dich nun für einen Hauptschlüssel entscheiden. Dieses muss allen Sicherheitskriterien entsprechen und schützt alle deine weiteren Passwörter.

Über die drei Punkte neben dem Feld kannst du dir automatisch ein Passwort generieren lassen oder du entwickelst es selbst. Beachte, dass es möglichst lang

sein sollte und aus einer Kombination aus Buchstaben, Sonderzeichen und Zahlen besteht. Wenn du dir selbst ein Passwort auszudenkst, solltest du ganze Wörter vermeiden.

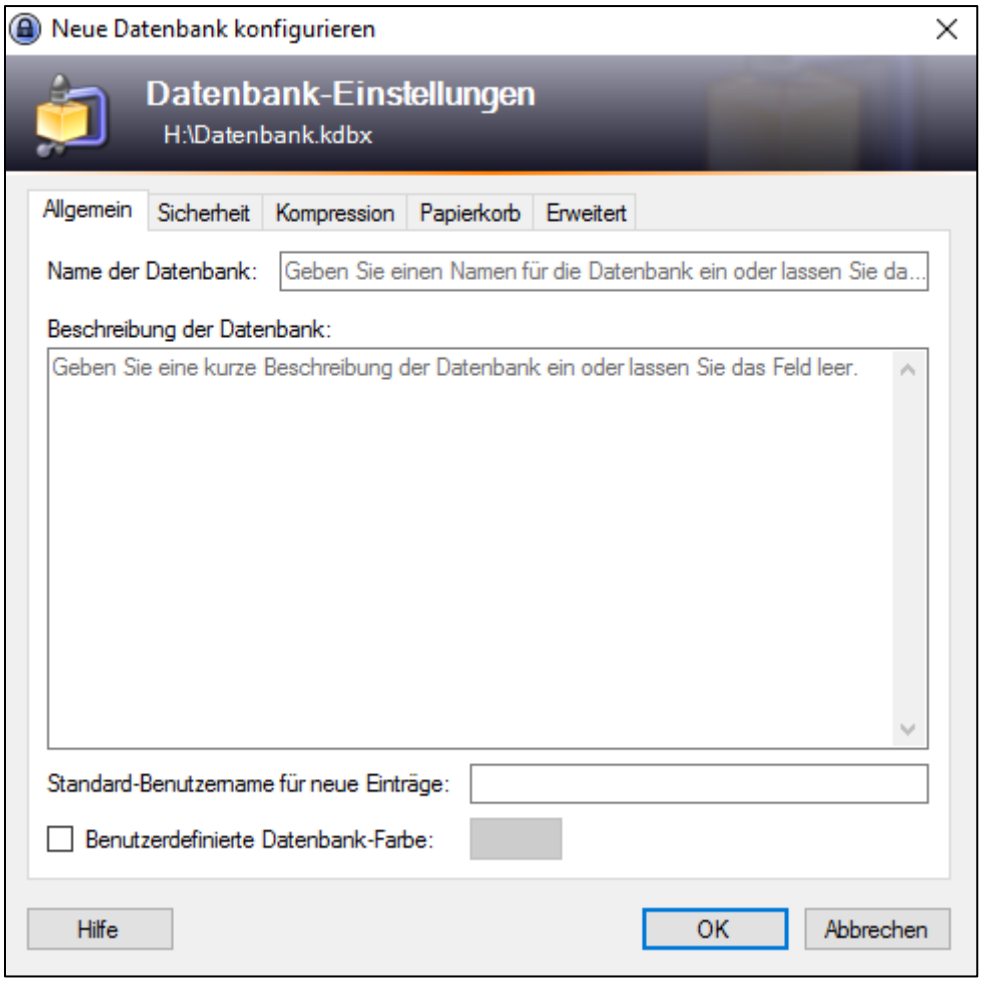
Tipp: Nimm eine Zeile aus deinem Lieblingssong und reihe die Anfangsbuchstaben in Groß- und Kleinschreibung aneinander. Jetzt noch mit ein paar Sonderzeichen und Zahlen garnieren, und du hast ein ziemlich starkes Passwort, das du dir auch merken kannst.

Anschließend kannst du dich entscheiden, das Passwort zu drucken und in einem Safe zu hinterlegen.

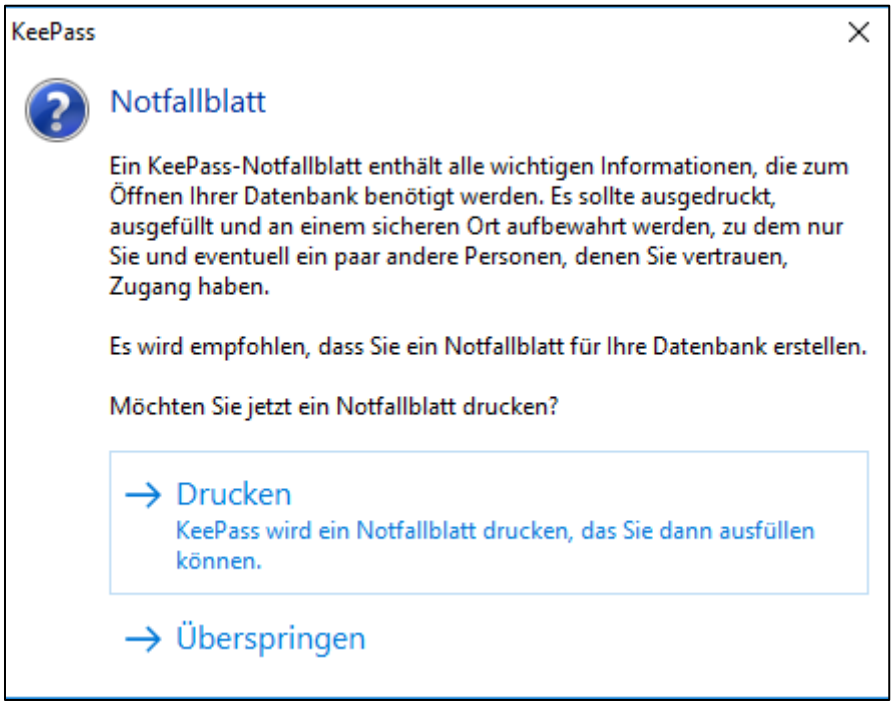


5. Prüfe die Datenbank-Einstellungen.

Im nächsten Schritt siehst du die Einstellungen deiner Datenbank und kannst den Namen bzw. die Beschreibung präzisieren.

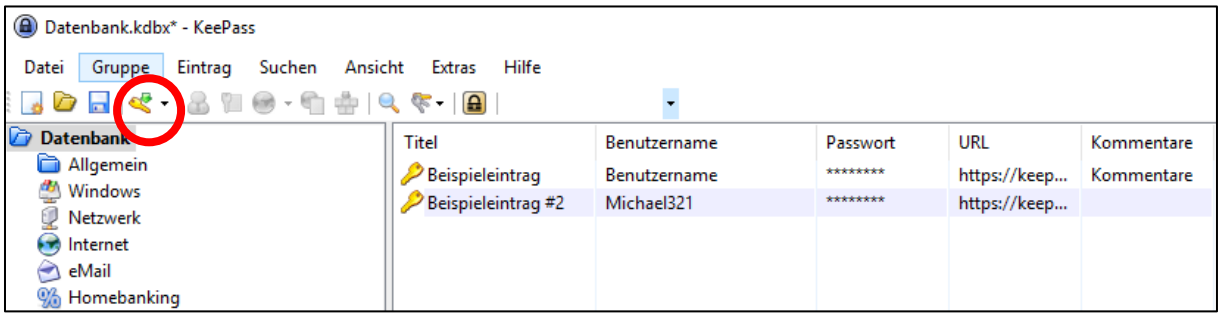


Nach einem Klick auf „OK“ erhältst du die Option, ein Notfallblatt mit allen Informationen zu drucken. Überlege gut, ob du die Informationen zu deiner Datenbank auswendig weißt oder drucken möchtest. Bewahre die Infos sicher auf, wenn du sie druckst.



6. Pflege deine Passwörter in die Datenbank ein.

Nun befindest du dich in deiner Datenbank. Dir werden zwei Beispiele angezeigt. Du kannst nun aber auch selbst neue Passwörter hinterlegen, indem du auf das Schlüssel-Symbol klickst.

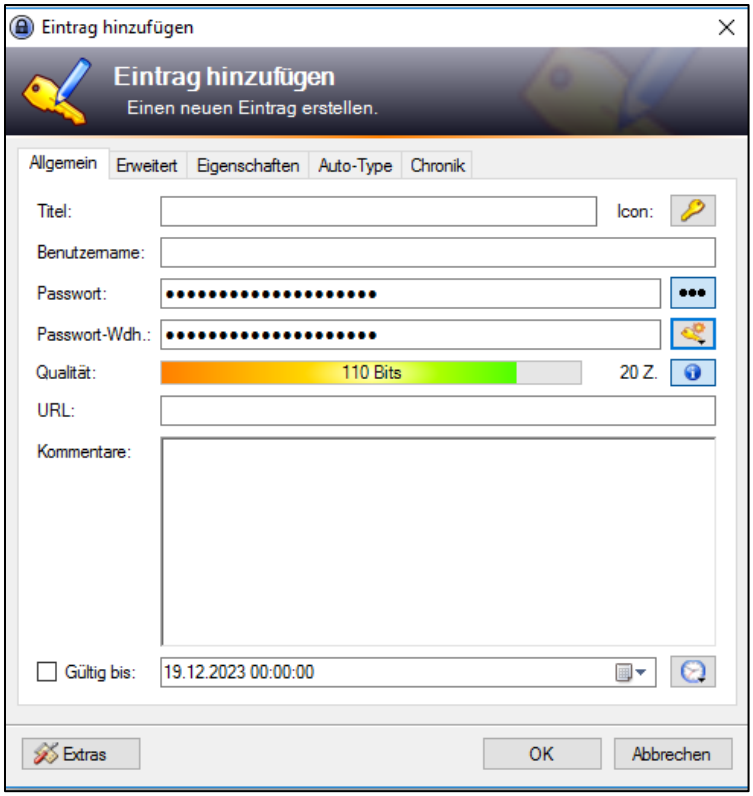


7. Lege das erste Passwort an.

Wähle hierfür einen eindeutigen Titel. Im Idealfall orientierst du dich bei Websiten an der Überschrift, die in der Registerkarte deines Browsers angezeigt wird. So kannst du später den Login ganz einfach über eine Tastenkombination ausfüllen lassen. KeePass ordnet die Daten durch den Titel richtig zu.

Hinterlege zudem deinen Benutzernamen. Bei vielen Portalen ist das deine E-Mail-Adresse. Du kannst nun wahlweise ein eigenes Passwort eintragen oder ein neues generieren. Dies machst du über das untere Schlüsselsymbol. Dort kannst du über den Passwort-Generator auch dessen Länge festlegen.

Über die drei Punkte neben dem Passwort kannst du es dir anzeigen lassen. Gib abschließend unten die dazugehörige Website (URL) an und bestätige mit „OK“.

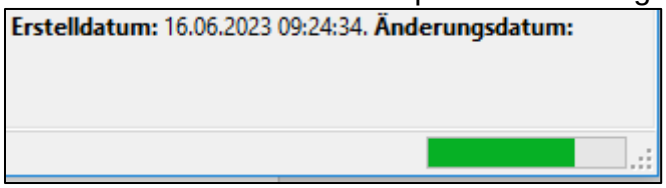


8. Nutze deine Passwörter.

Ab sofort musst du zu Beginn deines Arbeitstages nur mit dem Hauptpasswort deine KeePass-Datei öffnen. Du kannst deine Passwörter wahlweise durch einen Doppelklick auf das Passwort in der Übersicht kopieren oder durch die Tastenkombination Strg + Alt + A die Daten automatisch in der jeweiligen Website ausfüllen lassen.

Der Vorteil: Kopierst du das Passwort, bleibt es nur wenige Sekunden im Zwischenspeicher. Befindest du dich bspw. mit geteiltem Bildschirm in einer online-Konferenz, kann es dir somit nicht passieren, dass du zu einem späteren Moment aus Versehen dein Passwort einfügst.

Du siehst unten rechts im KeePass einen Balken. Dieser zeigt dir an, wenn dein Passwort noch im Zwischenspeicher hinterlegt ist:



Exkurs: Mehrere Team-Mitglieder arbeiten parallel

Manchmal arbeiten mehrere im Team parallel in der gleichen KeePass-Datei. Wenn du dann ein Passwort anlegst, wirst du nach einer Synchronisierung des Ordners gefragt, sobald du KeePass schließen möchtest. Bitte bestätige die Speicherung. So werden alle Daten immer für alle Mitglieder aktualisiert hinterlegt.