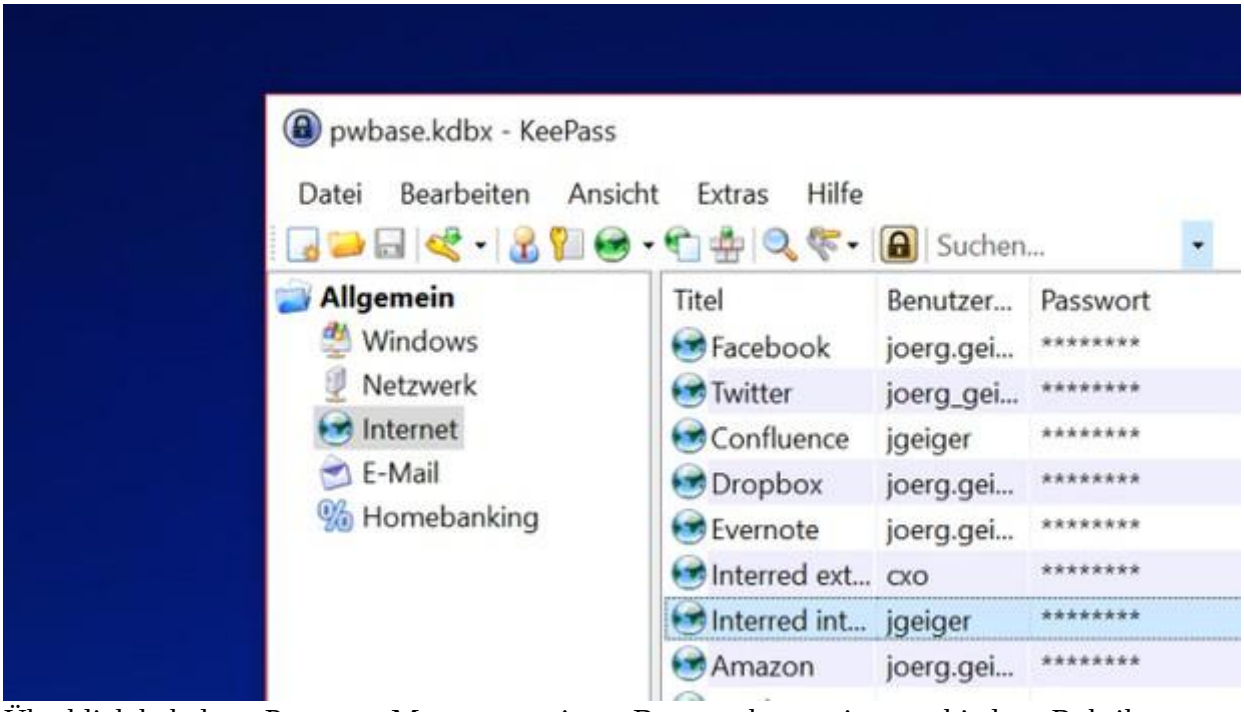
KeePass_Das wichtigste Security-Tool der Welt gibt es kostenlos

Sichere Passwörter mit KeePass

Endlich sichere Passwörter: Das geht ganz einfach mit KeePass
Ob Firewall, Antivirus oder Verschlüsselung: Windows 10 verfügt über eine Vielzahl von Sicherheitstools. Was allerdings bislang fehlt, ist eine Lösung für sichere Passwörter. Unsere Top-Empfehlung: der kostenlose Passwort-Manager KeePass, den es jetzt in einer neuen Version gibt.
Passwörter sind eines der größten Risikos für Nutzer im Internet. Wir müssen uns zu viele von ihnen merken, was in den meisten Fällen dazu führt, dass man entweder verschiedene einfache Passwörter verwendet oder sich auf wenige sehr sichere konzentriert. Beide Strategien bergen ein hohes Risiko. Besser ist es, jedem Benutzerkonto ein eigenes sehr sicheres Passwort zu spendieren. Dafür braucht es aber eine Merkhilfe.
Natürlich können Sie auch Ihrem Browser Passwörter anvertrauen, wir raten aber zu einem anderen Ansatz. Tools wie KeePass packen Passwörter in eine verschlüsselte Datei und versiegeln den Zugriff mit einem Masterpasswort. Sie müssen sich selbst also nur noch ein starkes Passwort merken. Der große Vorteil: So können Sie für jeden Dienst ein eigenes, sehr sicheres Passwort verwenden.
Anders als bei anderen Passwort-Managern laden Sie Ihre Passwörter beim Open-Source-Tool KeePass nicht auf fremde Server. Somit sind Sie die einzige Person, die Kontrolle über Ihre Passwörter hat. Nun hat das Tool ein Update auf **Version 2.44** erhalten. Darin wurden verschiedene Neuerungen an der Benutzeroberfläche sowie in den diversen Integrationen hinzugefügt. Den vollständigen Changelog finden Sie auf der Seite des Herstellers.

Download: KeePass **Zum Download**



Überblick behalten: Passwort-Manager sortieren Benutzerkonten in verschiedene Rubriken ein.

Installieren Sie sich KeePass und legen Sie beim ersten Start eine neue Passwort-Datenbank an. Das Programm gibt Ihnen gleich verschiedene Rubriken wie Internet, E-Mail oder Homebanking vor. Sie können aber auch eigene Gruppen anlegen, etwa Arbeit oder Streaming und so Passwörter passend sortieren. Wenn Sie bei einem Dienst ein neues Benutzerkonto anlegen, erstellen Sie auch gleichzeitig einen neuen Eintrag in KeePass.

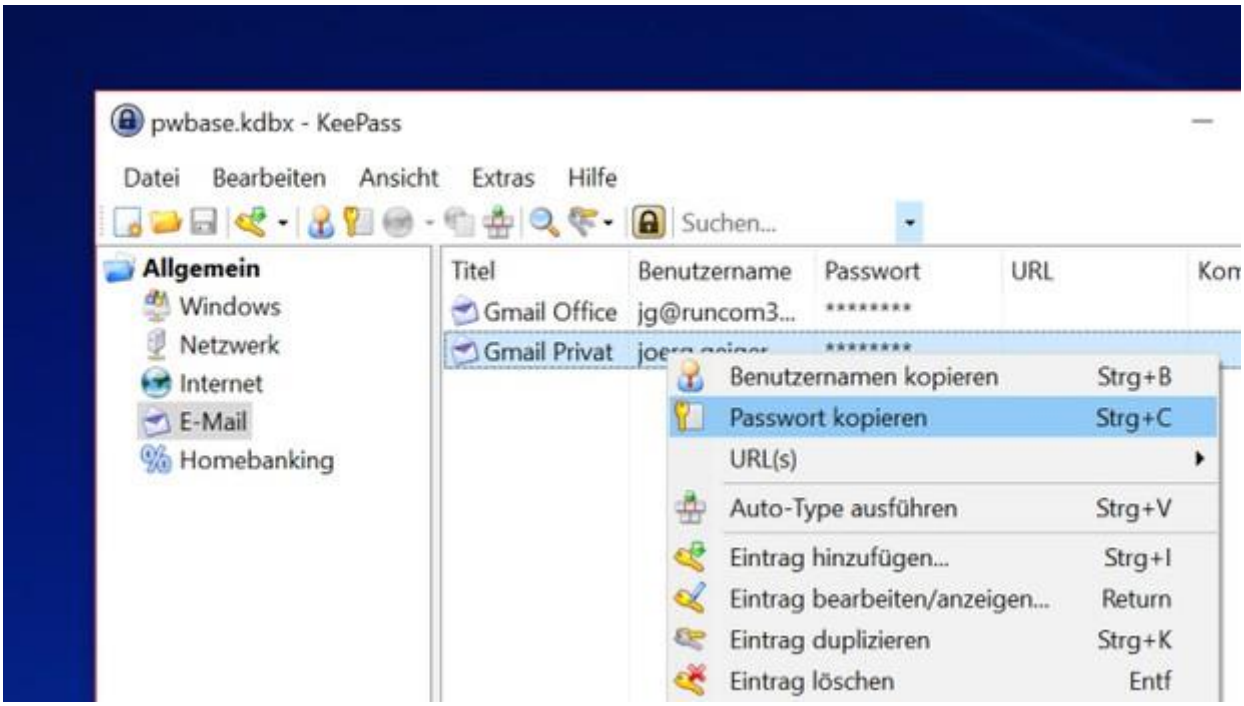
Die besten Passwort-Manager im CHIP Test

Sichere Passwörter erzeugen lassen

Passwörter erzeugen lassen: KeePass generiert auf Wunsch sichere Passwörter.

Fangen Sie aber jetzt nicht an, den Passwort-Manager mit "123abc" oder "test456" zu füttern. Nutzen Sie unbedingt den eingebauten Passwort-Generator. Er erzeugt garantiert sichere Passwörter und KeePass merkt sich diese für Sie. So können Sie zum Beispiel für Ihr Mail-Konto ein Passwort mit 25 Stellen festlegen, inklusive Sonderzeichen, Ziffern und Groß-Kleinschreibung.

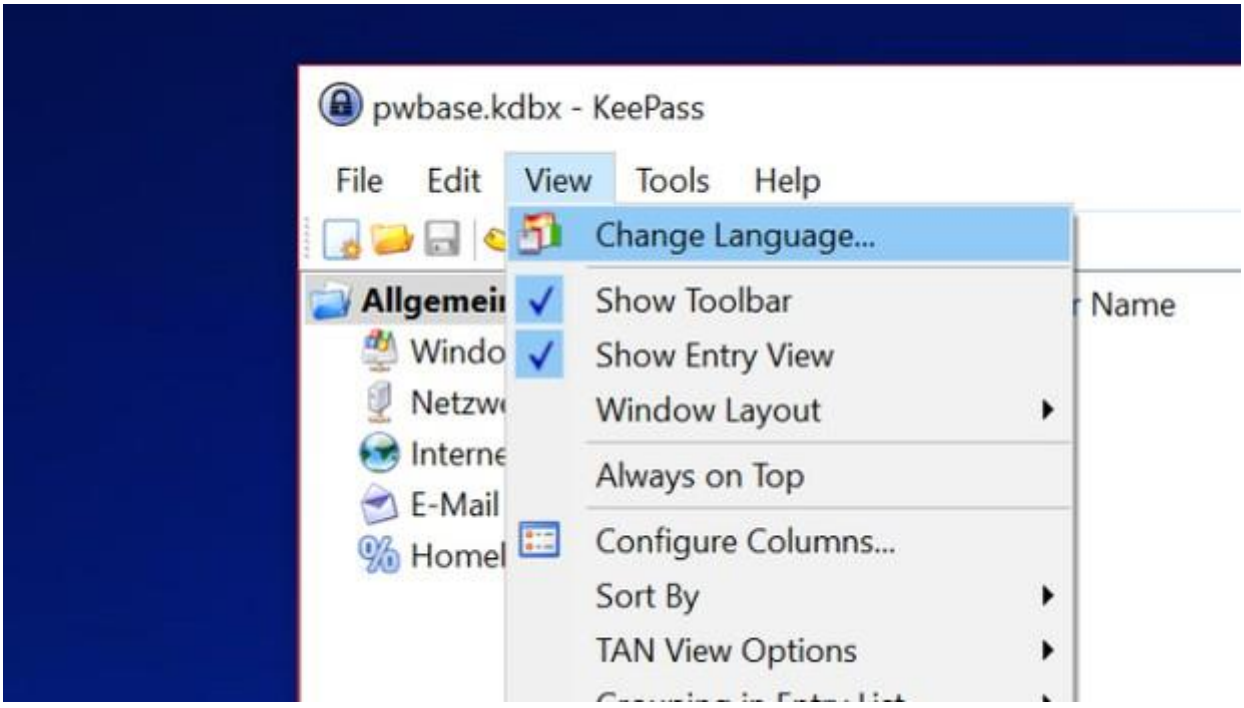
Passwörter schnell nutzen



Schneller Zugriff: Per Copy and Paste holen Sie Passwörter schnell aus der Datenbank.

In der Praxis macht es dann aber keinen Sinn, Passwort-Ungetüme abzutippen. Um sich jetzt schnell bei einem Dienst anzumelden, steuern Sie in KeePass den passenden Eintrag an und wählen aus dem Kontextmenü "Copy Password" aus bzw. "Passwort kopieren" beim Einsatz der deutschen Sprachdatei (siehe unten). Für wenige Sekunden bleibt dann das Passwort in der Zwischenablage und Sie können es in den Browser kopieren. Sie können in KeePass übrigens auch Login-Namen hinterlegen und diese auf die gleiche Weise in den Browser kopieren.

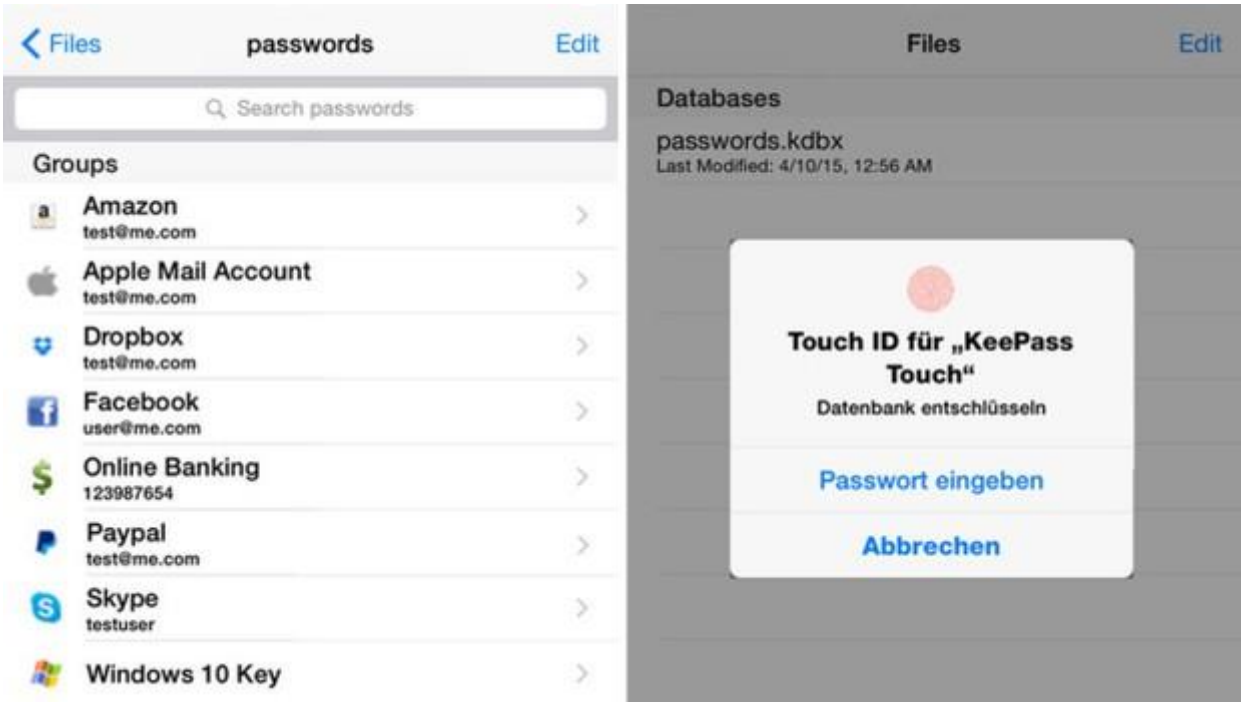
Deutsche Oberfläche nachrüsten



Deutsche Oberfläche: Wen das englische Menü stört, kann es per Sprachdatie ändern.

Wer Probleme mit der englischen Oberfläche hat, kann sich eine deutsche Sprachdatei nachinstallieren und dann die Sprache bequem über das Menü umstellen. Dazu kopieren Sie die Sprachdatei in den gleichen Ordner, in dem auch die EXE-Datei von KeePass liegt. Starten Sie danach den Passwort-Manager neu und wählen Sie über "View" den Punkt "Change Language" aus. Dann klicken Sie auf "German" und bestätigen den Neustart von KeePass.

KeePass jenseits von Windows



KeePass überall: Auch für Smartphones und Macs gibt es passende Tools für KeePass-Datenbanken.

Eiin Vorteil von KeePass ist auch, dass die Datenbanken auch jenseits von Windows genutzt werden können. Sie können zum Beispiel KeePassX auf macOS nutzen, KeePassDroid unter Android und KeePass Touch auf iOS. Damit haben Sie Ihre Passwörter überall dabei. Die Benutzung ist auch jenseits von Windows ähnlich: Sie entsperren in einem Schritt die Passwort-Datenbank mit dem Masterpasswort und können dann auf Ihre gespeicherten Passwörter zugreifen.

Sie müssen nur eine Sache beachten: Hüten Sie die Passwort-Datenbank wie Ihren Augapfel und halten Sie immer mindestens ein Backups dieser Datei einsatzbereit.

Sichere Passwörter sind Pflicht

Ist ein Passwort-Manager die beste Option? Nein, Sicherheitslücken in der Software, zerschossene Datenbanken und auch Ihr Masterpasswort könnte geknackt werden. Die beste Option wäre, wenn Sie sich für jeden Zugang ein eigenes komplexes Passwort merken könnten. Doch das klappt in der Praxis einfach nicht. Stattdessen dominieren zwei Strategien, entweder hantiert man mit einfachen Passwörtern oder man hat ein oder zwei richtig gute und verwendet die über verschiedene Dienste hinweg. Beide Strategien bergen ein hohes Risiko. Ein Passwort-Manager ist die beste Option für die meisten Nutzer.