

Tools für mehr Datensicherheit

Je mehr Geräte, desto mehr Daten werden gesammelt

Unser Alltag ist erfüllt von digitalen Helfern. Seien es Smartphone, Tablet, Notebook oder stationärer PC. Nichts geht mehr ohne und überall werden Unmengen von Daten gespeichert, gelöscht, verschoben und verwaltet. Im Laufe der Zeit sammelt sich so auf unseren Computern ein gigantischer Datenberg an. Dieser besteht aus sensiblen persönlichen Daten, zum Beispiel Zugangsdaten und Passwörtern, genauso wie aus individuell wichtigen Dateien wie Dokumenten, Bildern, oder gespeicherten MP3s. Entsprechend wichtig ist es, diese Daten einerseits natürlich vor Fremdzugriff zu schützen, andererseits aber auch im Falle eines Rechnerausfalls optimal abgesichert zu haben, um möglichst wenig Datenverlust zu riskieren.

Diese kostenlosen Sicherheitstools machen aus deinem PC eine Datenfestung:

- [Partition Wizard Free](#)
- [Secure Eraser](#)
- [Avira Free Antivirus](#)
- [KeePass 2](#)
- [Clonezilla Live](#)

Mit diesen Programmen kannst du dein System optimal gegen Schadsoftware schützen. Kinderleicht und übersichtlich strukturieren und alle nicht mehr benötigten Daten sicher und einfach löschen.

• Partition Wizard Free

Ordnung ist das halbe Leben – auch bei deinen Daten

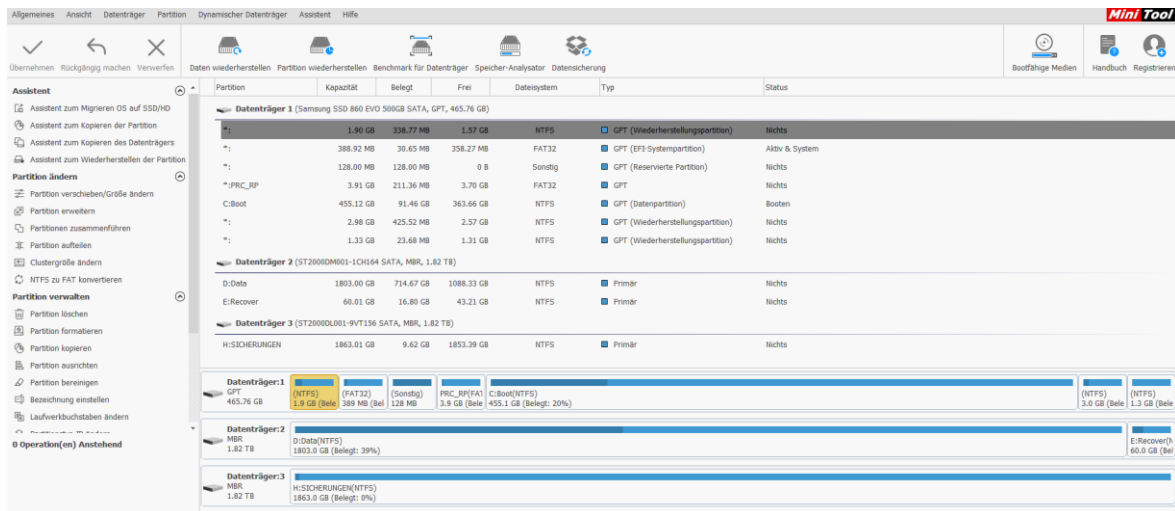
Bevor du ans Thema Datensicherheit und -sicherung denkst, solltest du deine Daten ordentlich strukturieren. So hast du jederzeit die perfekte Übersicht, wo welche Dateien gespeichert sind, was du noch benötigst oder was du getrost löschen kannst. Somit entsteht erst gar nicht so viel „Datenmüll“, um den du dir später Gedanken machen müsstest. Am besten fängst du damit natürlich gleich nach dem Kauf deines Computers oder Notebooks an, solange noch nicht viele Daten auf dem Gerät sind. So hast du am allerwenigsten Aufwand. Aber auch, wenn der PC schon etwas älter ist, ist es problemlos möglich, die Daten im Nachhinein noch zu ordnen.

Was ist Partitionieren überhaupt und warum ist das sinnvoll?

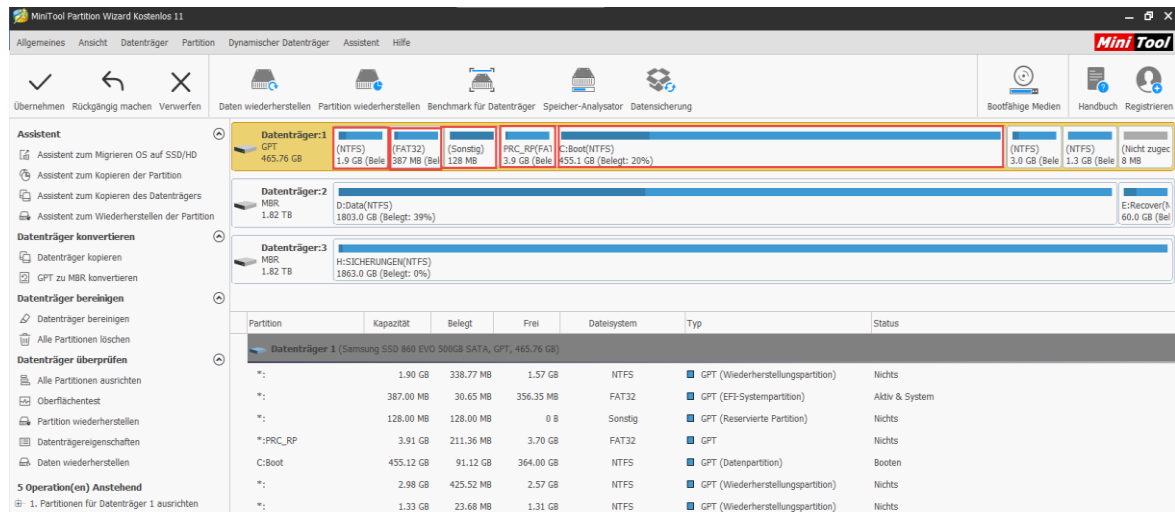
Weitaus eleganter und nebenbei auch noch sicherer, als einfach nur unzählige Unterordner auf dem gleichen Laufwerk anzulegen, ist dabei die sogenannte Partitionierung deiner Festplatte(n). Damit täuschst du deinem Computer mehrere separate Festplatten vor, wo sich in Wirklichkeit nur eine einzige Festplatte befindet. Der Vorteil daran ist, dass dein Computer diese einzelnen vorgetäuschten Festplatten genauso behandelt, als seien es tatsächlich mehrere physisch getrennte und damit

voneinander völlig unabhängige Festplatten. Ist dann irgendwann einmal eine komplette Neuinstallation von Windows nötig, so kannst du die entsprechende Partition ganz einfach komplett löschen und Windows neu installieren. Alle anderen Daten auf den anderen Partitionen werden nicht angetastet.

Sehr übersichtlich: Die Benutzeroberfläche:



8 Partitionen auf 1 Festplatte:



Auch für Anfänger verständlich und intuitiv bedienbar

Das Programm ist sehr schlicht aufgebaut und die Funktionen sind auf das Wesentliche beschränkt. Dafür ist es absolut einfach in der Bedienung und somit auch für den Laien ohne viel Aufwand verständlich.

Alle Funktionen mit wenigen Klicks ausführbar

Partition Wizard Free punktet vor allem dadurch, dass alle Aktionen mit nur wenigen Mausklicks ausführbar sind. So kannst du Partitionen erstellen oder löschen, verschieben, vergrößern oder verkleinern, alles via Schieberegler und wenigen Mausklicks. Unterläuft dir dabei ein Fehler, kannst du mit einem einfachen Klick auf „Rückgängig machen“ alles widerrufen und nochmal von vorne beginnen. Bist du mit dem Ergebnis zufrieden, so genügt abermals ein Klick auf „Übernehmen“ und alle eingestellten Änderungen werden durchgeführt.

[Hier geht's zum direkten Download von Mini Tool](#)

• Secure Eraser

Einfaches löschen ist noch lange nicht endgültig

Natürlich müssen Dateien auch hin und wieder einmal gelöscht werden. Spätestens, wenn der alte Rechner oder die Festplatte entsorgt oder verkauft werden soll, stellt sich die Frage nach der sicheren Löschung aller persönlichen Dateien und Daten. Wenn du dabei jedoch der Meinung bist, ein einfaches Drücken der „Entf“-Taste oder ein Klick auf den Löschen-Button wäre ausreichend, so ist dies ein fataler Irrtum. Hierbei werden die betreffenden Segmente auf der Festplatte nämlich keineswegs wirklich gelöscht, sondern lediglich als „wieder beschreibbar“ markiert, während die Daten in der eigentlichen Form nach wie vor unverändert vorliegen und ausgelesen werden können. Dieser Zustand hält so lange an, bis wieder neue Daten auf eben diese Segmente geschrieben werden. Selbst das Formatieren der kompletten Festplatte ändert nichts an dieser Tatsache.

Überschreiben mit Zufallszahlen

Willst du deine Festplatte nicht physisch zerstören, d.h. in winzig kleine Stückchen schreddern, so ist die einzige Möglichkeit, deine persönlichen Daten wirklich sicher und endgültig zu löschen, das Überschreiben mit Zufallswerten. Dies erledigt das Programm Secure Eraser für dich, welches für die private Nutzung ebenfalls völlig kostenlos ist.

Kinderleichte Bedienung

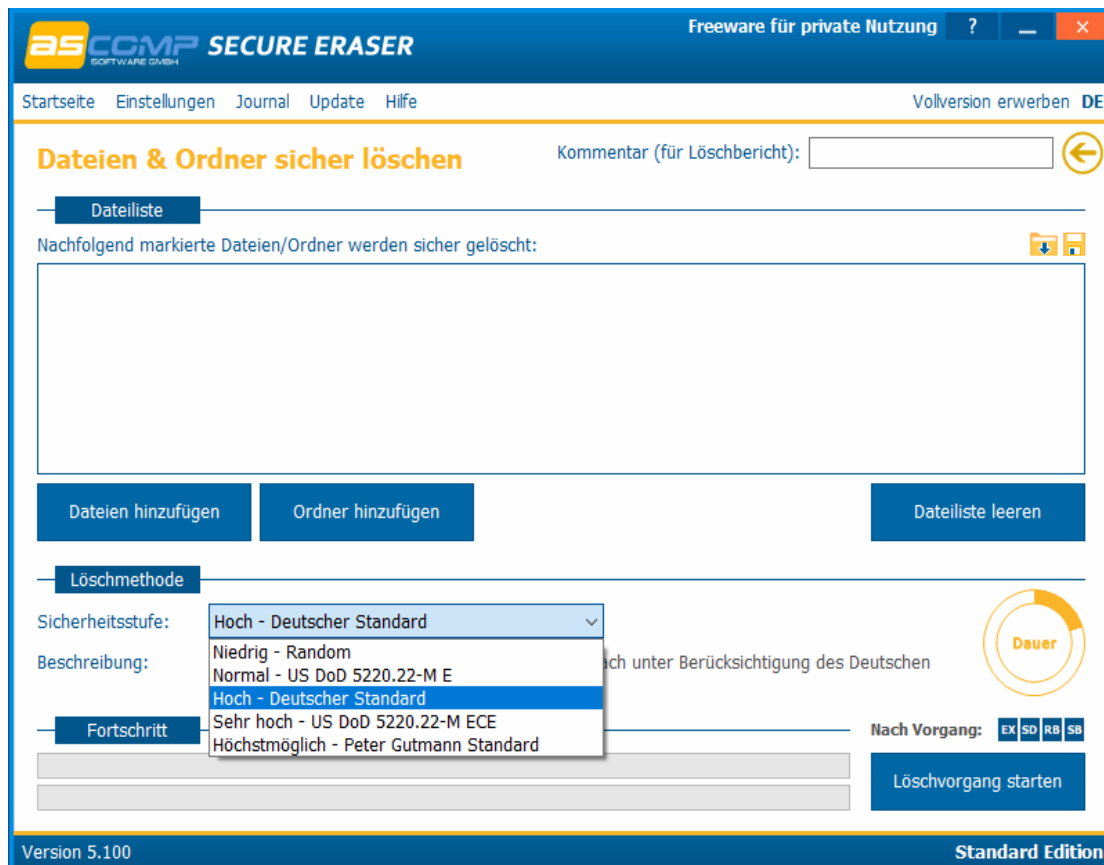
Zum Programm selbst gibt's nicht allzu viel zu sagen. Die Bedienung ist absolut kinderleicht und erklärt sich von selbst. Nach dem Programmstart stehen folgende 5 Optionen zur Verfügung:

- Dateien und Ordner sicher löschen
- Festplatte / Partition sicher löschen
- Freien Speicher sicher löschen
- Registry säubern
- Festplatte bereinigen



Während du beim ersten Punkt einzelne Dateien oder Ordner zum sicheren Löschen auswählen kannst, wird bei Punkt 2 der Inhalt einer ganzen Festplatte bzw. Partition eliminiert. Hast du bereits Daten über die normale Löschfunktion von Windows gelöscht und Secure Eraser erst nachträglich installiert, so empfiehlt sich als erster Schritt einmal denn dritte Punkt auszuführen. Hierüber kannst du sämtlichen freien Speicherplatz noch einmal bzw. dieses Mal wirklich sicher löschen. Ebenfalls empfehlenswert sind Nummer 4 und 5, womit du deine Windows-Registry von unnötigen nicht mehr genutzten Einträgen, sowie deine Festplatte von temporären Dateien, Cookies und dergleichen befreien kannst.

5 Löschmethoden stehen zur Auswahl



Bei jedem der oben genannten Punkte hast du die Wahl zwischen 5 amtlich anerkannten Standards zur Datenlöschung.

- Niedrig-Random (einmaliges Überschreiben)
- Normal-US DoD 5220.22-M e (dreifaches Überschreiben)
- Hoch-Deutscher Standard (siebenfaches Überschreiben)
- Sehr hoch-US DoD 5220.22-M ECE (siebenfaches Überschreiben)
- Höchstmöglich-Peter Gutmann Standard

Je höher der Standard, desto gründlicher die Löschung, aber auch der Zeitbedarf. So kann die Löschung einer kompletten Festplatte nach dem Peter-Gutmann-Standard durchaus mehr als 10 Stunden benötigen. In der Regel ist für moderne Datenträger mit mehr als 80 GB Speicherplatz jedoch ein 1-3maliges Überschreiben ausreichend, um wirklich alle Daten zu eliminieren. Hier kann bedingt durch die dichte Speicherarchitektur danach nicht einmal mehr mit einem Magnet-Elektronenmikroskop auf die gespeicherten Daten zugegriffen werden. Nur bei älteren und kleineren Festplatten sind die höheren Standards noch nötig, da die Daten hier deutlich weniger dicht geschrieben werden.

[Hier geht's zum direkten Download von asCOMP](#)

• Avira Free Antivirus

Deine Festplatte ist nun übersichtlich partitioniert und alle Dateien, die du nicht mehr brauchst sind datensicher gelöscht. Jetzt gilt es, deinen Rechner vor Fremdzugriffen und Schadsoftware zu schützen.

Seit Jahren bewährt

Das Programm Avira Free Antivirus belegt seit Jahren regelmäßig die Top-Plätze der kostenlosen Virenprogramme. Und dies mit Recht. Es ist einfach zu benutzen und schützt effektiv gegen die allermeisten Bedrohungen. Zusätzlich sorgen regelmäßige Updates selbstverständlich dafür, dass die Virendefinitionen immer auf dem aktuellsten Stand der Dinge sind und bleiben.

Basis-Version reicht vollkommen aus

Bereits die Basis-Version von Aviras Virenscanner ist mehr als ausreichend für den Schutz deines Computers gegen jegliche Schadsoftware. Der Vollständigkeit halber sei erwähnt, dass alternativ dazu auch die Free Security Suite heruntergeladen werden kann, die als Zusatzfunktionen noch mit Browserschutz, Phantom-VPN, Tuning-Tools, Software-Updater, Passwortmanager, sowie SafeSearchPlus zu glänzen versucht. Diese Funktionen lassen sich unserer Meinung nach aber durch separate Programme weitaus besser sicherstellen.



The advertisement banner for Avira Free Security Suite features a gradient background from orange to yellow. At the top center is the Avira logo. To the right, a red box contains the text 'AVIRA ANTIVIRUS EDITION 2019'. The main title 'Avira Free Security Suite' is prominently displayed in the center. Below it, a subtitle reads 'Free Antivirus und unsere besten kostenlosen Sicherheitstools in einem Paket.' Three product boxes are shown: 'FREE ANTIVIRUS', 'FREE SECURITY SUITE', and 'AVIRA PRIME'. Each box has a corresponding download or purchase button and a list of features.

FREE ANTIVIRUS	FREE SECURITY SUITE	AVIRA PRIME
Kostenlos herunterladen	Kostenlos herunterladen	Jetzt kaufen 9,95 €/Monat
• Basisschutz • Vielfach preisgekrönt	• Free Antivirus • VPN, Software Updater u.v.m. • Kostenloses Komplettpaket	• 30-tägige Geld-zurück-Garantie • Alle <u>Premiumprodukte</u> • Monatlich kündbar

Funktion vollautomatisch

Einmal heruntergeladen, erfüllt das Programm auch schon völlig selbstständig seinen Zweck. Es muss nichts mehr konfiguriert oder eingerichtet werden. Das Programm platziert sich automatisch in der Taskleiste von Windows und kennzeichnet ab sofort durch einen aufgespannten roten Regenschirm die Überwachung des Computers. Startet man das Programm manuell via Desktop-Icon, so kann man sein System auch manuell nach Schadsoftware durchforsten lassen, andernfalls wird die Suche in gewissen Zeitabständen vollautomatisch gestartet.



[Hier geht's zum direkten Download von Avira](#)

• KeePass 2

Passwörter anlegen, aber richtig

Im Zeitalter der Digitalisierung hat man unzählige verschiedene Accounts. Angefangen bei diversen Shoppingportalen im Internet, über diverse Social-Media Konten, bis hin zum Zugang aufs Onlinebanking seiner Hausbank. Folgt man den allgemeinen Datenschutz-Empfehlungen, so sollte jeder einzelne Account mit einem unterschiedlichen Benutzernamen und Passwort gesichert sein. Zudem sollten die Passwörter mindestens 10-stellig und eine Mischung aus Groß- und Kleinschreibung, Ziffern und Sonderzeichen enthalten.

Passwörter nie unverschlüsselt auf dem Rechner abspeichern

Da sich diese Unzahl an Passwörtern und Benutzernamen kein normaler Mensch merken kann, werden die Passwörter auf einem Notizzettel, oder noch schlimmer in einer Datei auf dem Computer gespeichert. Eigentlich eine ganz praktische Sache, aber leider auch für jeden, der sich Zugang zu deinem Rechner verschafft und diese Datei findet.

Eine Datenbank mit modernster Verschlüsselung

Das kleine Sicherheitstool KeePass 2 punktet durch seine Transparenz: Das Open-Source-Programm liegt im Quellcode offen, sodass Experten sicherstellen, dass keine Hintertüren enthalten sind. Es handelt sich um eine verschlüsselte Datenbank, in der alle Zugangsdaten und entsprechenden Kennwörter übersichtlich sortiert abgespeichert werden können. Die Verschlüsselung erfolgt dabei nach modernsten Standards und wird über ein Master-Passwort abgesichert.

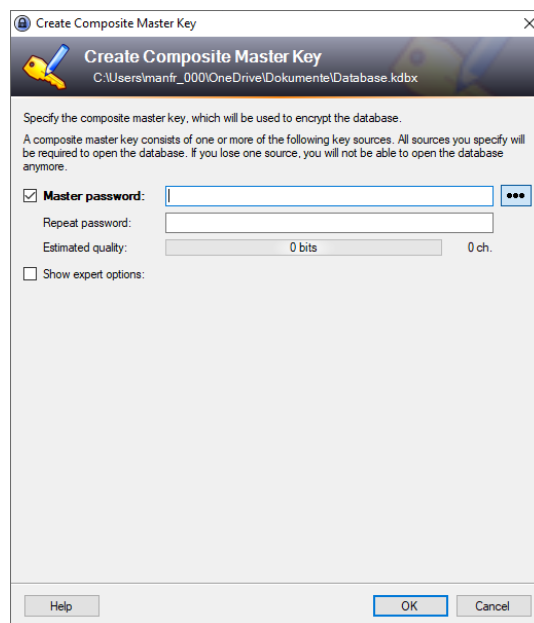
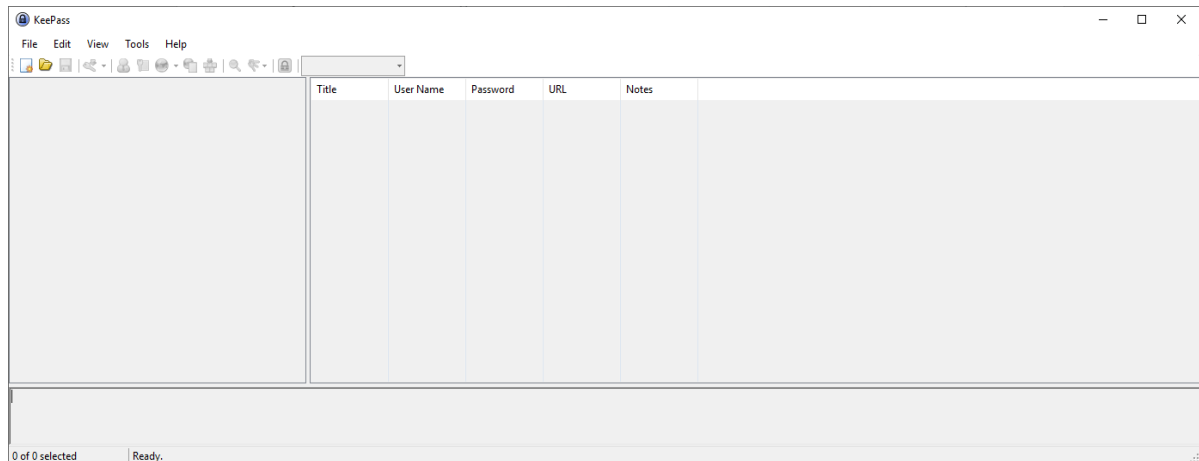
Der Vorteil: Du brauchst dir zukünftig nur noch dein Master-Passwort merken und hast sofort Zugriff auf alle deine anderen gespeicherten Passwörter.

KeePass 2 wird nach dem Download nur in englischer Sprache installiert. Wenn du damit zu Recht kommst, super. Falls nicht, findest du unter dem folgenden Link ein kleines Tutorial, wie du die Sprache auf Deutsch ändern kannst.

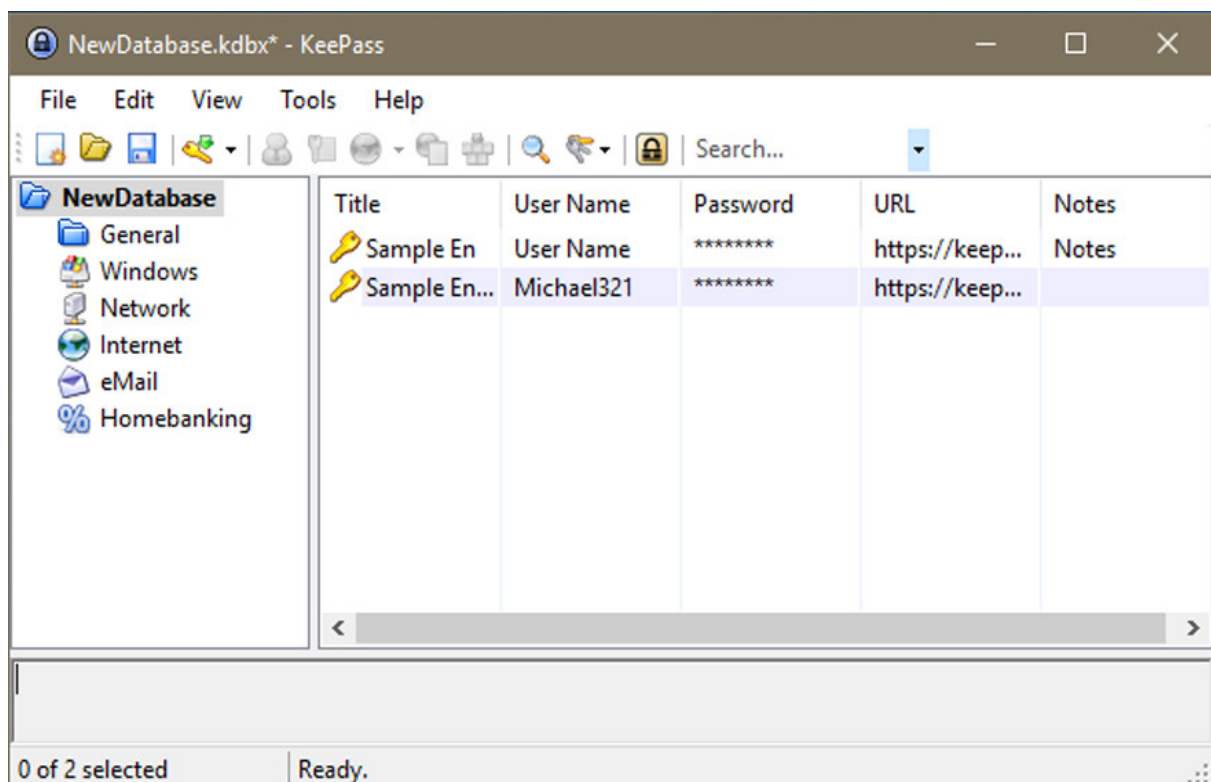
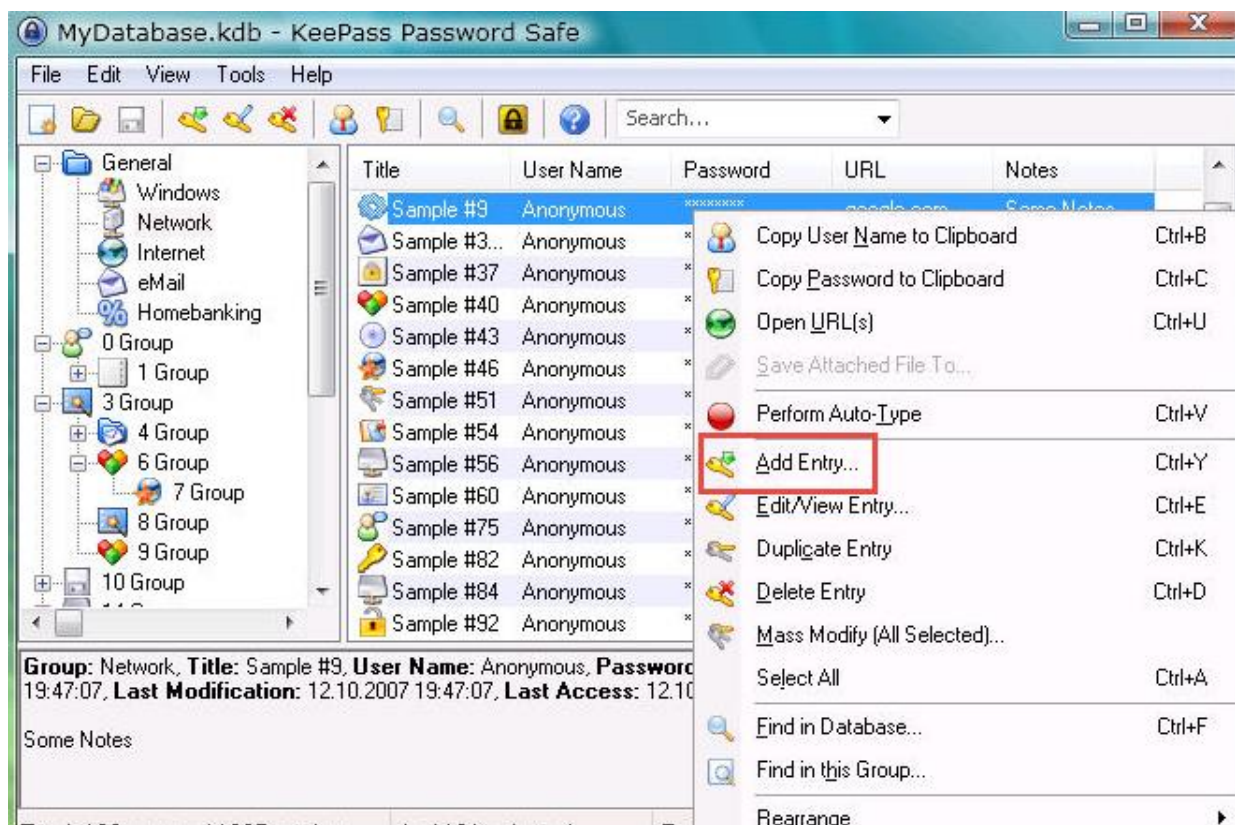
[\[Tutorial\] KeePass 2 Passwortmanager Sprache auf Deutsch ändern](#)

Einfache Bedienung, maximale Sicherheit

Nach Klick auf „File“ und „New“ sowie der Auswahl des Speicherortes der Datenbank und des Masterpassworts, können nach Belieben neue Passwörter angelegt werden.



Dies geschieht per einfachem Rechtsklick in das Fenster sowie Linksklick auf „Add Entry...“. Siehe Bild unten. Ebenfalls per Rechtsklick auf einen bestehenden Eintrag kannst du anschließend sowohl deinen Benutzernamen als auch dein Passwort in den Zwischenspeicher übertragen. In der gewünschten Anwendung kann dies dann wie üblich per „Strg+V“ wieder eingefügt werden. Dies schützt neben der Verschlüsselung zusätzlich auch durch das Abgreifen der Passwörter während der Eingabe durch sogenannte „Tasten-Protokollierer“ (Keylogger).



[Hier geht's zum direkten Download von KeePass 2](#)

• Clonezilla Live

Nun ist deine Festplatte also perfekt strukturiert, übersichtlich geordnet, datensicher und von allem unnötigen Ballast befreit, vor Fremdzugriffen und Malware geschützt und

mit einer verschlüsselten Datenbank für alle Passwörter versehen. Was noch fehlt ist ein Programm zur einfachen Wiederherstellung, falls es doch einmal zum Schlimmsten – nämlich dem totalen Systemcrash - kommt. Diese Funktion bietet das Programm Clonezilla Live.

Komplette Images einfach und schnell erstellt

Mit diesem kleinen Helferlein lassen sich komplette Images eines Datenträgers oder einer Partition erstellen. Ein Image ist ein 1:1-Abbild des kompletten Datenträgerinhalts inklusive aller Dateien sowie der Datenträgerstruktur.

Systemstart per CD erforderlich

Clonezilla Live braucht nicht installiert zu werden, sondern wird von einer autarken CD oder einem bootfähigen USB-Stick „live“ gestartet. Über eine textbasierte Menüführung kannst du eine Festplatte oder einzelne Partitionen kopieren und später wiederherstellen. Das Partitions- oder Festplattenabbild wird als Datei auf einem anderen Datenträger (Festplatte, USB-Stick, DVD) gespeichert. Unterstützt werden interne und externe Festplatten sowie der Netzwerkzugriff auf Speichermedien, zum Beispiel mittels NFS-, SSH- oder Samba-Servern.

Platzsparende Images

Clonezilla speichert beim Kopiervorgang nur die belegten Teile einer Partition oder Festplatte, so dass die Images weit weniger Platz beanspruchen als die Ursprungspartition. Es unterstützt beim Erstellen von Imagedateien und Backups die gängigen Dateisysteme wie ext2, ext3, reiserfs, xfs, jfs, FAT und NTFS.

[Hier geht's zum direkten Download von Clonezilla Live](#)

Geschafft!

Nun ist dein Computer ordentlich strukturiert und datensicher ausgerüstet. Wir hoffen, wir konnten mit diesen Programmen deinen Computer etwas sicherer machen!