Passwort Sicherheit

1 Inhalt

2 Sichere Passwörter wählen

2.1 No Gos

- Keine Namen einbauen
  - Besonders von Kindern / Verwandten
  - Auch keine Anfangsbuchstaben
- Keine einfachen Zahlenfolgen
  - Bsp. „1234“

2.2 Strategien

1. Satz (Passphrase) ausdenken
   - Bsp.: *In Word müssen Sie Ihre Überschriften nicht manuell nummerieren - das funktioniert auch automatisch.*
2. Erste Buchstaben und Satzzeichen (ohne Leerzeichen) übernehmen (Umlaute umschreiben)
   - *IWmSIUnmn-dfaa.*
3. Je nach Service (Dienst / Firma / Anbieter usw.) präzisieren, gerne auch mit zwei Buchstaben
   - Bsp.:
     - Word: *In Word müssen Sie Ihre Überschriften nicht manuell nummerieren - das funktioniert auch automatisch. → IWmSIUnmn-dfaa.*
     - Google: *In Google müssen Sie Ihre Überschriften nicht manuell nummerieren - das funktioniert auch automatisch. → IGmSIUnmn-dfaa.*
     - Sky Ticket: *In Sky Ticket müssen Sie Ihre Überschriften nicht manuell nummerieren - das funktioniert auch automatisch. → ISTmSIUnmn-dfaa.*
4. Profi Tipp: Jahreszahlen und Monat oder Quartal der Passworterstellung einbauen:
   - *Seit 05 2020 müssen Sie in Word Ihre Überschriften nicht manuell nummerieren - das funktioniert auch automatisch. → IS520mSiWIUnmn-dfaa.*

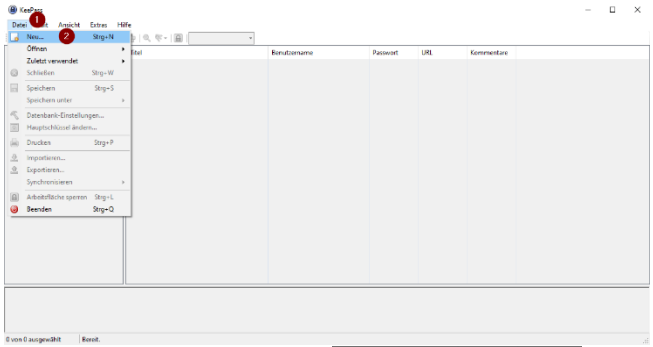
- Wenn nach einer Vorgabe das Passwort alle 3 Monate geändert werden muss, nach drei Monaten:
  - *IS520mSiWIUnmn-dfaa.* → *IS820mSiWIUnmn-dfaa.*

5. Nicht überall das gleiche Passphrase nutzen. Besonders bei Zugängen, die nichts miteinander zu tun haben.
   - Bsp.: berufliche und private Zugänge
   - Oder: Zugang zum Rechner und Zugang zu Diensten, die auf dem Rechner genutzt werden (unterschiedliche Schichten, die häufig hintereinander genutzt werden). Für den Admin sollte nochmal was andere genutzt werden!
   - **Ganz wichtig: KeePass Passwort sollte nirgends anders verwendet werden!**
6. Alternative zu allem oben genannten: Sich von KeePass ein zufälliges Passwort generieren lassen
   - Das macht dann Sinn, wenn:
     - Der Zugang ausschließlich am PC verwendet wird, weil dort KeePass verfügbar ist.
     - Der Zugang für einen Dienst auf dem Handy o.ä. genutzt wird und dort einmal eingetippt wird und dann hinterlegt ist.
7. Allgemein Passwörter / Passphrases regelmäßig ändern.
8. E-Mail ist besonders kritisch, weil man mit Zugang zum Postfach Passwörter für andere Dienste zurücksetzen kann!
9. Keine Konto Passwörter in KeePass speichern!
10. Keine Passwörter im Browser oder sonst wo speichern. Da ist nicht klar, wie gut das Passwort verschlüsselt ist.
11. Bei Passwörtern, die im Handy gespeichert werden o.ä., weil es anders nicht möglich ist, bitte immer ein zufälliges Passwort aus KeePass nutzen oder einen eigenen Passphrase verwenden!

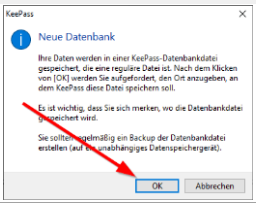
3 KeePass Basics

3.1 Datenbank erstellen

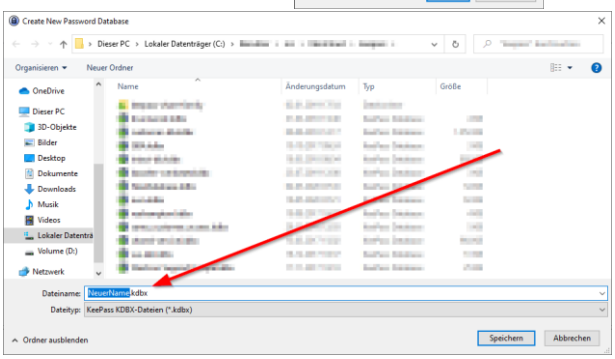
1. Man öffne KeePass.
2. Datenbank anlegen: Datei → Neu



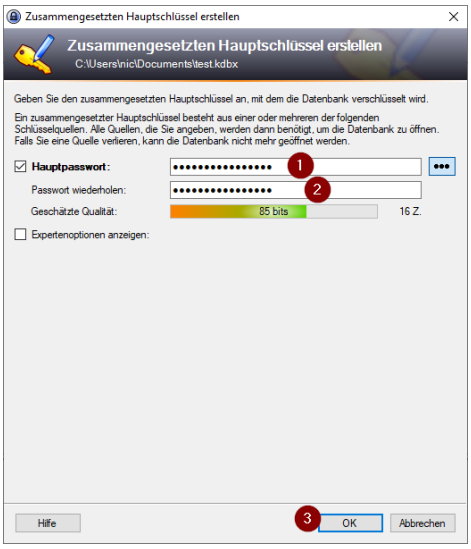
   - Mit OK bestätigen



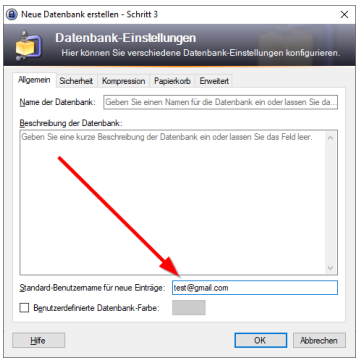
   - Name für die Datenbank wählen



- Hauptpasswort wählen (vgl. 2) und wiederholen. Dies ist das Passwort, um die Datenbank zu entschlüsseln. Man muss es bei jedem Öffnen der Datenbank eingeben.
  → Danach mit OK bestätigen



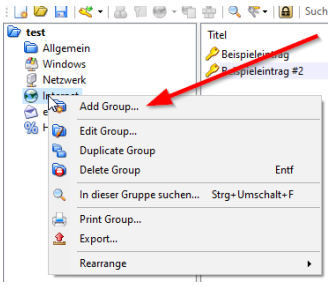
- Die Standardeinstellungen im nächsten Dialog sind ganz ok. Man kann hier noch einen Standard-Benutzernamen (Erster Reiter „Allgemein“) setzen. Dieser wird für neue Einträge in der Datenbank dann immer genutzt, kann aber auch für jeden Eintrag manuell geändert werden. Es macht Sinn, hier die eigene E-Mail Adresse zu nehmen, weil diese häufig als User zu nutzen ist.
- Man kann nun noch ein Notfallblatt ausdrucken. Halte ich für nicht unbedingt erforderlich.

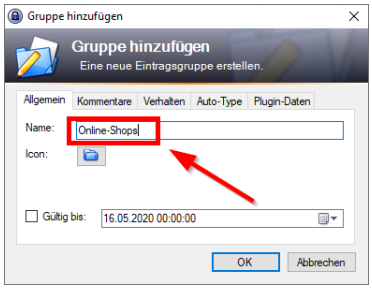


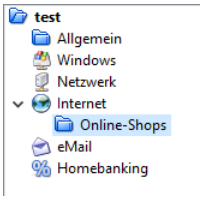
3.2 Mit der KeePass Datenbank umgehen

3.2.1 Ordnerstruktur

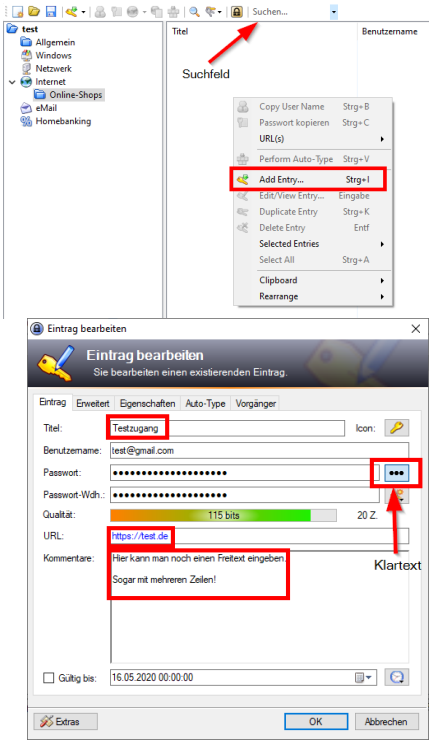
In KeePass gibt es eine Art Verzeichnisstruktur, ähnlich wie im Dokumente Ordner usw. Die einzelnen Ordner lassen sich an der Linken Seite ansteuern. Hier können auch noch Bilder ausgewählt werden und neue Ordner und Unterordner erstellt werden. Im Beispiel wird im Ordner Internet durch einen Rechtsklick darauf ein neuer Unterordner erstellt.







3.2.2 Neuen Eintrag erstellen



In einen Ordner im großen Inhaltsfeld rechts klicken und mit „Add Entry“ einen neuen Eintrag erstellen. Man sollte einen sinnvollen Titel wählen (nach diesen kann auch über das Suchfeld gesucht werden). Wenn eingestellt, ist hier dann bereits der entsprechende Benutzername vorausgefüllt (vgl. 3.1). Es wird auch ein Zufallspasswort generiert. Dies geschieht nach den Standardeinstellungen (20 Zeichen, Groß-, Kleinschreibung und Sonderzeichen sind enthalten).

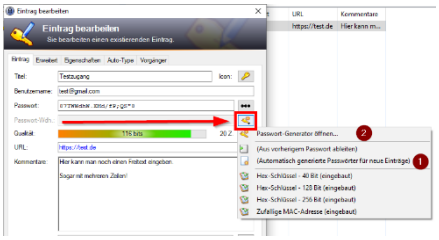
Bei Bedarf Benutzername ändern. Sollten die Passwort Anforderungen komplexer sein (zum Beispiel auch mit Ziffern), kann ein neues generiert werden. Dazu bitte nächster Absatz 3.2.3.1!

Über die drei Punkte kann man sich das Passwort auch im Klartext anzeigen lassen.

Man kann auch noch eine URL (Webseite für den Zugang) oder andere Infos im Kommentare Feld eingeben.

3.2.3 Einträge ändern

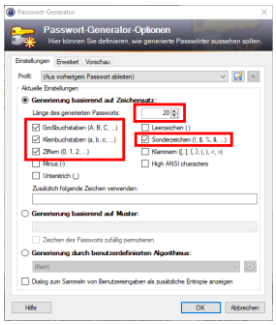
Mit einem Doppelklick auf den Titel (und nur auf den Titel) oder mit einem Rechtsklick auf die ganze Zeile und „Edit/View Entry“ kann man einen Eintrag nachbearbeiten. Dies muss man, wenn man ein neues Passwort abspeichern will (Achtung: Wenn ich ein Passwort ändern will, muss ich das natürlich über die entsprechende Webseite machen, in KeePass sollte das neue dann parallel gespeichert werden! Vgl.)



3.2.3.1 Neues Passwort erstellen / andere Komplexitätseinstellungen wählen

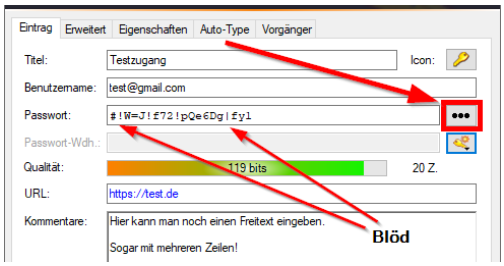
Das Passwortmenu über Schraubenschlüssel Knopf öffnen.

Hier kann man einfach nach den Standardeinstellungen ein neues Zufallspasswort generieren (Automatisch generierte Passwörter für neue Einträge / 1).



Wenn das Passwort andere Anforderungen erfüllen soll (Länge oder andere Zeichentypen), kann man dies auch einstellen. Hierzu „Passwort-Generator öffnen…“. Hier machen die vier Typen Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen Sinn. Mit einem Klick auf OK wird ein neues Passwort erstellt und gleich eingetragen.

Muss man das Passwort auf einem mobilen Gerät (Handy, TV o.ä.) eintippen, möchte man es vielleicht nicht ganz so lang haben. Auch sollte man möglicherweise unübliche Sonderzeichen dann noch nachträglich in einfachere ändern. Hierzu das Passwort im Klartext anzeigen lassen und abändern. Unübliche Sonderzeichen, die schwer auf einer Handy Tastatur zu finden sind, durch ANDERE SONDERZEICHEN wie -,+,!,? ersetzen.



Das Schöne hier ist, dass andere Funktionalitäten, wie beispielsweise Auto-Complete, nicht abgeändert werden müssen. Es wird dann in Zukunft einfach das neue Passwort verwendet.

3.2.3.2 Einfaches Auto-Complete einrichten und nutzen

Mit der Tastenkombination <STRG>-<ALT>-<A> kann man die Autovervollständigung von KeePass nutzen. Diese ist immer für konkrete Fenster mit einem konkreten Titel einzurichten (Im Beispiel heißt das Firefox Fenster einfach „Nextcloud“, es könnte aber auch sowas wie „Web.de – E-Mail – Login“ sein.

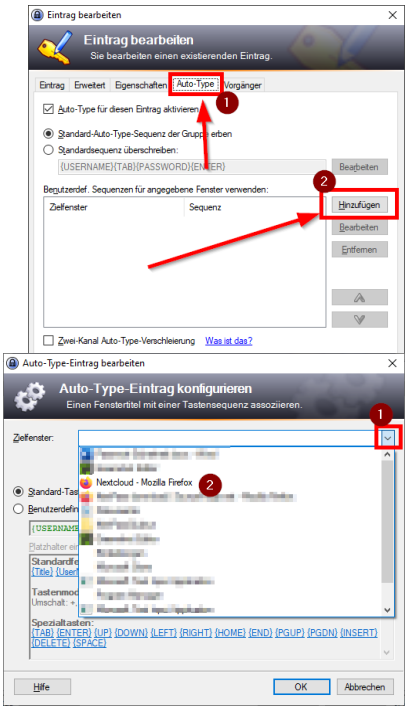
Die Standardeinstellung ist folgende Kombination: <Username> <TAB> <Passwort> <ENTER>

Diese ist für die meisten Webseiten recht gut nutzbar.

Für das Beispiel wurde ein Account auf der Nextcloud eingerichtet und bereits ein KeePass Eintrag angelegt. Für diesen erstellen wir nun eine Auto-Complete Funktion.

1. Man öffne in dem Browser, den man nutzen möchte, die entsprechende Website. Die Funktion ist dann auch nur für diesen Browser und für genau diese Webseite nutzbar. Man kann auch an anderen Stellen eine entsprechende Funktion anlegen, z.B. einem E-Mail Programm.

2. Man öffne die Einstellungen des entsprechenden Zugangs, zum Neuanlegen bitte in 3.2.2 nachlesen.
3. Im Reiter Auto-Type kann man nun eine neue Auto-Complete Regel hinzufügen.
4. Im neuen Fenster wählt man nun über das Dropdown Menu (1) das Zielfenster aus. Bei uns heißt es „Nextcloud – Mozilla Firefox“ (2). Danach beide Fenster mit OK bestätigen.
5. Im Zielfenster kann man nun mit <STRG>-<ALT>-<A>. Sollte es für mehrere Zugänge eine Auto-Complete Funktion für dieses Fenster geben, bekommt man noch eine Liste angezeigt und muss den richtigen Zugang auswählen.
6. Tipp: Es ist auch möglich für einen Zugang mehrere Auto-Complete Funktionen zu definieren, beispielsweise um sich auf der Weboberfläche und im E-Mail Programm mit seinem E-Mail Account anzumelden. Dazu dann einfach eine weitere Funktion hinzufügen (ab Schritt 3).

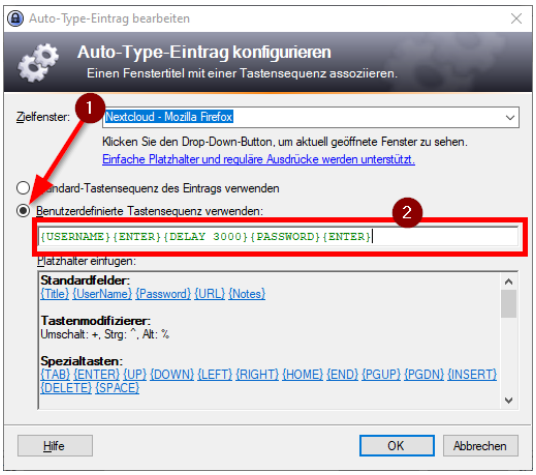


3.2.3.3 Komplexere Auto-Complete Funktion

Manchmal ist es notwendig, dass eine andere Sequenz als der Standard auf einer Webseite eingegeben wird. Dies könnte zum Beispiel sein, dass nach der Eingabe des Usernamens Enter gedrückt werden muss statt Tab. In einem solchen Fall kann es dann auch nötig sein, ein paar Sekunden zu warten mit der Passwort Eingabe, weil sich ggf. eine neue Webseite öffnen muss.

Ein anderer Anwendungsfall wäre, dass nur ein Passwort eingegeben werden muss statt einer Username und Passwort Kombination.

Um dies einzurichten fügen wir wie im vorherigen Kapitel 3.2.3.2 einen neuen Eintrag hinzu und wählen das entsprechende Zielfenster aus (bis Schritt 5) oder bearbeiten einen bereits bestehenden Eintrag.



Das „Auto-Type-Eintrag bearbeiten“ Fenster wird nun aber nicht geschlossen.

Wir wählen hier „Benutzerdefinierte Tastensequenz verwenden:“ aus und definieren diese.

Eine solche Sequenz besteht immer aus den entsprechenden Tasten. Eine Auswahl der Standardtasten findet man in dem Bereich unter der Sequenz. Es ist auch möglich, einzelne Zeichen hinzuzufügen, diese schreibt man dann ohne Klammern hin.

Die beiden Beispiele von eben:

- Nach User Enter und dann 3 Sekunden (3000 ms) warten, bevor das Passwort folgt:
  - `{USERNAME}{ENTER}{DELAY 3000}{PASSWORD}{ENTER}`
- Nur Passwort:
  - `{PASSWORD}{ENTER}`

3.2.4 Allgemeiner Umgang mit KeePass

3.2.4.1 Speichern

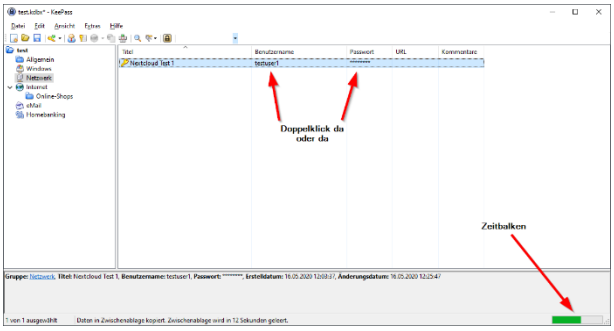
Eure Datenbank liegt in einem Ordner, der regelmäßig synchronisiert wird. Dies passiert allerdings nur, wenn die Datenbankdatei auch gespeichert ist. Dazu gibt es in KeePass ein Diskettensymbol, um zu speichern. Bevor man die Datenbank also auf einem anderen Gerät öffnen will, sollte sie synchronisiert werden, nachdem sie gespeichert wurde.

Achtung: Nach dem Speichern 5 Minuten warten, dass die Synchronisation auch auf beiden Geräten durchgeführt wurde. Dann erst auf dem anderen Gerät KeePass öffnen.

Dies gilt selbstverständlich nur, wenn man Änderungen in der Datenbank vornimmt. Dies kann man an dem Stern im KeePass Fenster erkennen.

3.2.4.2 Benutzername oder Passwort in die Zwischenablage kopieren

Wenn man bei einem bestimmten Eintrag auf den Benutzernamen oder das Passwort doppelklickt, ist dies jeweils für ein paar Sekunden in der Zwischenablage. Solange hat man nun Zeit, mit <STRG>-<V> oder Rechtsklick und Einfügen den Usernamen oder das Passwort an anderem Ort einzufügen. Nach Ablauf der Zeit ist die Zwischenablage aber auch wieder leer. Dies ist eine Sicherheitsfunktion von KeePass. Man kann an dem grünen Balken in KeePass erkennen, wie viel Zeit bereits abgelaufen ist.



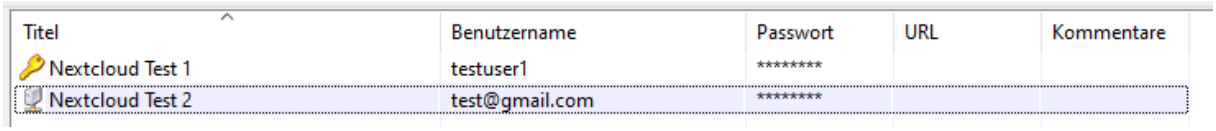
3.2.5 Strategie zum Einrichten eines neuen Accounts

Bei Online Accounts sollte man nach folgendem Schema vorgehen, um ein Zufallspasswort zu nutzen:

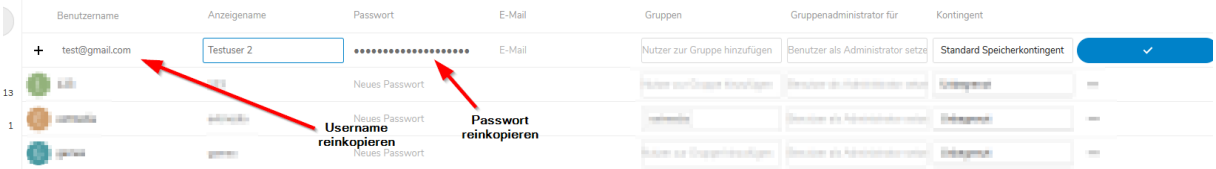
Eintrag in KeePass generieren (dann wird gleich ein Passwort mit generiert), Account über die Webseite anlegen und Passwort dort hineinkopieren (vgl. 3.2.4.2), Auto-Complete einrichten, testen.

Im Beispiel wird ein Nextcloud Account eingerichtet und es wird sich an der Nextcloud angemeldet. Normalerweise nutzt man eine Anmeldeprozedur von Webseiten, wo dann auch Name, Adresse usw. einzugeben sind. Der Benutzername ist häufig die E-Mail Adresse, das wird hier auch versucht.

1. Nach bekanntem Schema wird ein neuer Eintrag in KeePass generiert (vgl. 3.2.2). Dieser heißt im Beispiel „Nextcloud Test 2“.



2. Nun wird im Browser der Account angelegt. Dies ist natürlich je nachdem, wo man sich anmelden will, unterschiedlich. Der Username und das Passwort können wie in 3.2.4.2 beschrieben über die Zwischenablage kopiert werden (Doppelklick und schnell genug sein).



3. Ist der Account angelegt, begeben wir uns auf die Login Seite für den Dienst, um für diese eine Auto-Complete Funktion anzulegen. Dies ist wichtig, weil nur vorhandene Fenster bei

der Auswahl angezeigt werden. In unserem Beispiel kann die Standardsequenz genutzt werden, wir halten uns also an 3.2.3.2.

4. Nun kann der Login auf der Login Seite mit <STRG>-<ALT>-<A> getestet werden.