

Passwörter

Erstellen von sicheren PW

Verwalten von PW

rh 2018/2019

Erstellen von sicheren PW

Die größten PW-Sünden

- Kein PW über längere Zeit verwenden
- Keine Namen, Adressen, Geburtstage, Zahlenfolgen
- Nie das gleiche PW auf mehreren Internet-Seiten verwenden
- Keine Automatikfunktion verwenden
- Keine PW-Eingabe auf unbekanntem Systemen oder Seiten
- Keine PW-Eingabe auf Seiten über einen erhaltenen Link
- Nicht über ‚Offenes WLAN‘ auf Konto mit PW zugreifen.

Quelle: Computerwelt

Passwörter erstellen

- **Möglichst viele Zeichen**
- **Buchstaben, Zahlen, Sonderzeichen**

Passwörter erstellen (Beispiel)

Anfangsbuchstaben in einem Satz/Vers

- **AdWgHuiNgF**
- **Auf dem Wase graset Hase und im Neckar gambled Fisch**

Verwalten von Passwörtern

Einen PW-Safe verwenden

Hier werden PW verschlüsselt gespeichert

Verschlüsselt mit Master-PW

Verwalten von Passwörtern

Was ist verschlüsseln?

Daten so verändern, dass Sie nicht erkannt werden

Beispiel einfachste Verschlüsselung:

Was ist: QD-Usfgg ?

→: PC-Treff

Buchstaben nur um 1 nach rechts verschoben

Verwalten von Passwörtern

Für Master-PW möglichst viele Zeichen und Zahlen verwenden

**Auch Sonderzeichen wie & \$? % @ und
Gross- und Kleinschreibung**

**Hiermit werden Passwörter wieder in Klartext angezeigt
(entschlüsselt)**

Die größten Passwort-Sünden: Was Sie niemals tun sollten!

- Verwenden Sie nie das gleiche Passwort über einen längeren Zeitraum:** Auch wenn es zunächst mühsam erscheint - wechseln sie Ihre Passworte gerade bei Online-Accounts regelmäßig. Wenigstens alle sechs Monate, besser alle drei Monate oder immer dann, wenn Sie sich auf einer Seite einloggen, die sie schon lange nicht mehr verwendet haben!
- Verwenden Sie nie Passworte, die Namen (ganz gleich ob aus der Familie oder von Haustieren), Geburtstage, Adressen oder andere persönliche Informationen beinhalten:** Solche persönlichen Informationen sollten auch teilweise nicht in Ihren Passwörtern zu finden sein. Das gilt auch für alle Worte, die sie in einem Lexikon finden können und für Zahlen- oder Buchstabenwiederholungen wie **222** oder Folgen wie **ABCD** und **qwertz**.
- Verwenden Sie nie das gleiche Passwort auf mehreren Internet-Seiten:** Ist eine derartige Seite kompromittiert, sind gleich alle Ihre Accounts gefährdet.
- Verwenden Sie grundsätzlich keine "Automatik-Funktionen":** Erlauben sie keiner Webseite, dass Sie Ihren Namen und Ihr Passwort speichert ("remember me"). Vermeiden Sie es ebenfalls, dass sich Ihr System beim Start automatisch bei den diversen Online-Konten wie etwa Web-Mail anmeldet.
- Keine Passwort-Eingabe auf "unbekannten" Systemen und Seiten:** Geben Sie ihre Passworte nicht auf Systemen ein, deren Sicherheitseinstellungen Sie nicht kontrollieren: Das gilt für den PC im Internet-Café ebenso wie für das System eines Kollegen oder Freundes!
- Keine Passwort-Eingabe auf Webseiten, die Sie über einen Link in einer E-Mail erhalten haben:** Die Gefahr ist zu groß, dass es sie hier um eine [Phishing-Mail](#) handelt. Geben Sie die URL von Bank- und Shop-Webseiten immer direkt in ihrem Browser ein und wechseln dann dort zu der entsprechenden Eingabe!
- Niemals über ein offenes WLAN auf einen Account mit einem Passwort zugreifen:** Wenn Sie sich in einem offenen WLAN oder einem ähnlich unsicheren Netzwerk befinden, sollten Sie Passwörter ausschließlich auf Seiten eingeben, die [HTTPS](#)-Verschlüsselung (Hypertext Transfer Protocol Secure) verwenden oder noch besser nur via [VPN](#) (Virtual Private Network) auf die entsprechenden Accounts zugreifen.

Quelle: Computerwelt

Verwalten von Passwörtern

Mit ‚KeePass‘
 Freeware, AES-Verschlüsselung, 256 bit

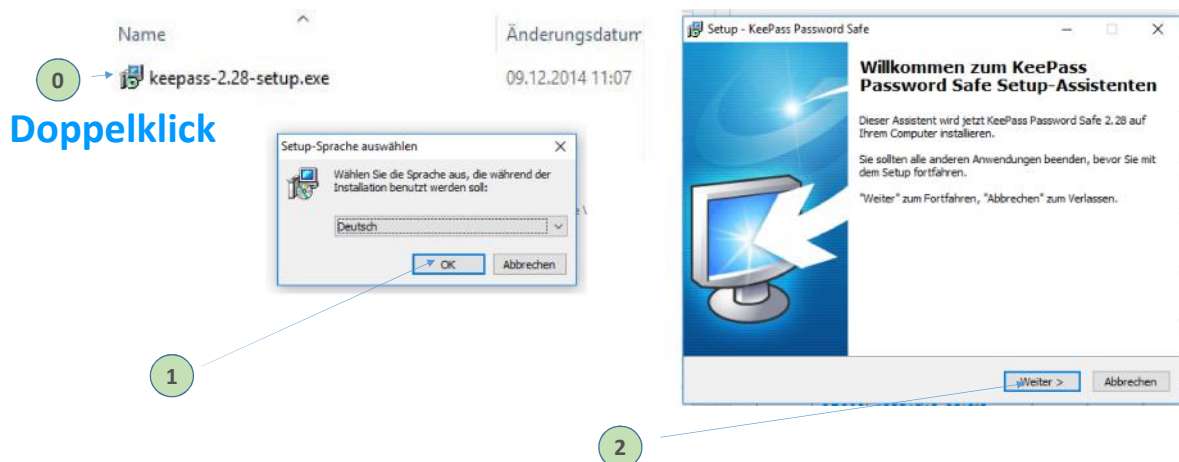
KeePass Installation

0 → keepass-2.28-setup.exe

Doppelklick

1

2



Setup - KeePass Password Safe

Willkommen zum KeePass Password Safe Setup-Assistenten

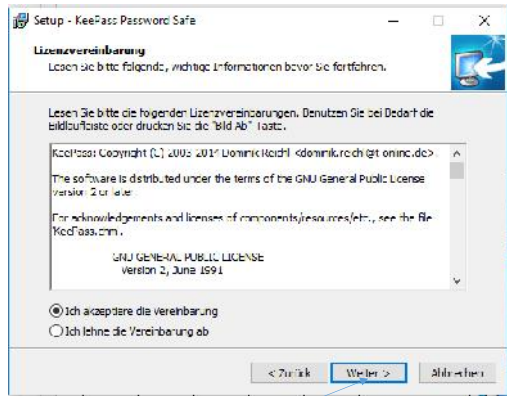
Dieser Assistent wird jetzt KeePass Password Safe 2.28 auf Ihrem Computer installieren.

Sie sollten alle anderen Anwendungen beenden, bevor Sie mit dem Setup fortfahren.

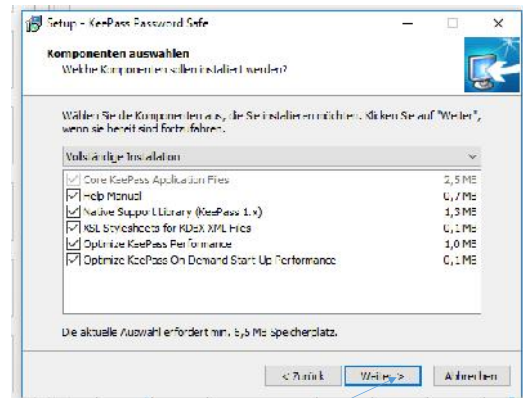
"Weiter" zum Fortfahren, "Abbrechen" zum Verlassen.

Weiter > Abbrechen

KeePass Installation

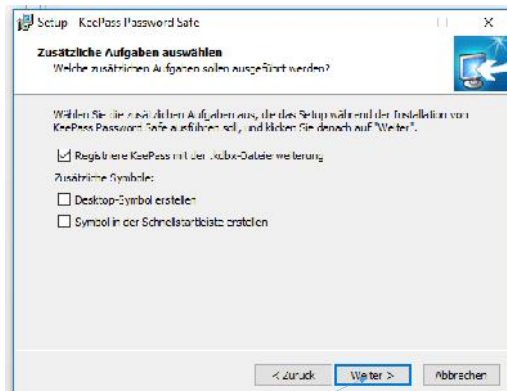


3

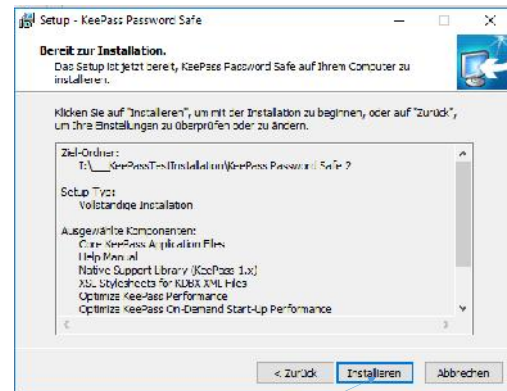


4

KeePass Installation



5



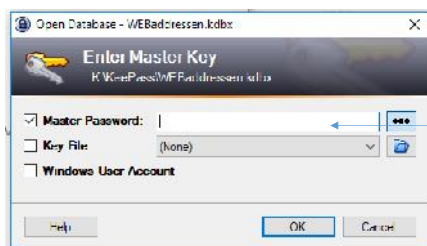
6

KeePass Installation



7

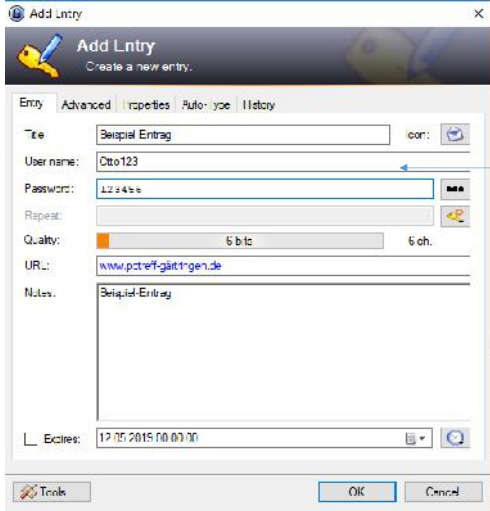
KeePass Installation



8

Master PW eingeben und merken !!

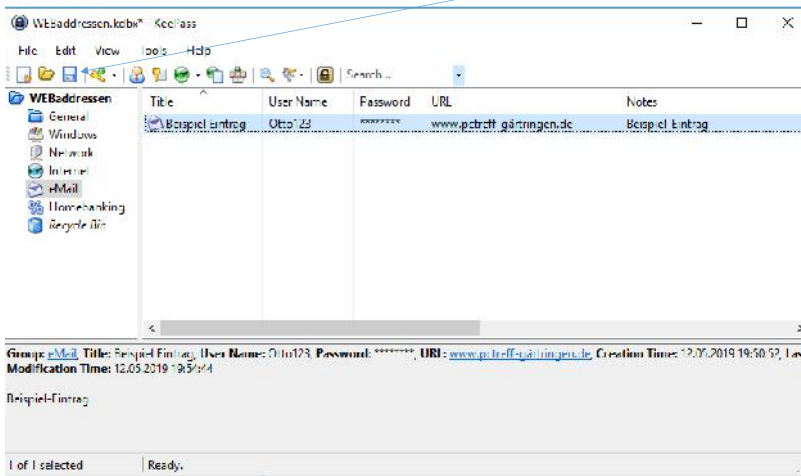
KeePass Installation



9

Eingabe

KeePass Installation



11

Speichern

10

Erster Eintrag

Title	User Name	Password	URL	Notes
Beispiel-Entrag	Oto123	*****	www.pctreff-gaertingen.de	Beispiel-Entrag

Group: eMail, Title: Beispiel-Entrag, User Name: Oto123, Password: *****, URL: www.pctreff-gaertingen.de, Creation Time: 12.05.2019 19:50:52, Last Modification Time: 12.05.2019 19:52:54

Beispiel-Entrag

1 of 1 selected | Ready.