Auf einen Kaffee mit…

Sicheren Passwörtern

Passwörter sicher vergeben, speichern & teilen

Jens Jacobsen, benutzerfreun.de

Version 1.0, April 2014

Für wen das ist

Die E-Book-Reihe *Auf einen Kaffee mit…* der benutzerfreun.de widmet sich je einem aktuellen Thema. Und das so prägnant, dass Sie nicht länger als eine Kaffeepause brauchen, um es zu lesen.
Wir alle kennen das: Wir sollten uns unbedingt über Thema A informieren. Wenn wir ein bisschen Zeit haben, widmen wir uns endlich Thema B. Und das dicke Buch zu Thema C, was seit Wochen auf unserem Schreibtisch liegt und uns ein schlechtes Gewissen macht, das lesen wir auch bald.
Auf einen Kaffee mit… können Sie ***jetzt*** lesen. Viel Spaß dabei wünscht Ihnen
Jens Jacobsen

PS: Haben Sie Fragen? Anregungen? Jederzeit gern auf www.benutzerfreun.de/auf-einen-kaffee!

Das Kreuz mit den Passwörtern

Ohne Passwörter kommt heute niemand mehr aus. Kein Geldautomat rückt Bargeld heraus, kein Webdienst gewährt Zutritt, wenn man nicht eine mehr oder weniger lange Kombination von Ziffern oder Buchstaben eintippt.

Man braucht dutzende von Passwörtern für all die vielen Geräte und Dienste, die man im täglichen Leben nutzt. Und nachdem unser Hirn nicht dafür geschaffen ist, sich komplexe Abfolgen von nichtssagenden Zeichen zu merken, haben wir alle ein Problem.

Die zwei häufigsten Lösungsstrategien für dieses Problem sind im Alltag:

1. Immer das gleiche Passwort verwenden.
2. Die Passwörter aufschreiben.

Beide Strategien führen zur Katastrophe. Es ist nur eine Frage der Zeit.

18 Millionen gestohlene E-Mail-Adressen samt Passwörtern haben deutsche Ermittler im April 2014 bei Kriminellen entdeckt. Diese wurden vor allem genutzt, um Spam zu verschicken – was die Verbrecher noch damit angestellt haben, wird sich nie restlos aufklären lassen.

Berühmte Opfer

Viele große Firmen wurden Opfer eines Hacks – Sony ebenso wie z. B. LinkedIn oder Adobe, der Hersteller der Software Photoshop. Bei Sony kamen 2011 die Passwörter und Kreditkartendaten von 77 Millionen Nutzern abhanden, bei LinkedIn wurden 2012 6,5 Millionen Passwörter gestohlen und bei Adobe waren es 153 Millionen E-Mail-Passwort-Kombinationen im Jahr 2013.

Was tun?

Am sichersten sind Passwörter in Ihrem Kopf. Nachdem aber nicht jeder ein Gedächtnisgroßmeister ist, schreiben sich fast alle ihre Passwörter irgendwo auf. Die Post-its am Monitor sind die zweitschlechteste Variante. Gefährlicher ist nur noch eine Textdatei "Meine Passwörter.txt" – ein gefundenes Fressen, sollte sich jemand Zugang zu Ihrem Rechner verschaffen, sei es durch Einbruch in Ihre Wohnung oder durch einen Virus.

Aber auch der häufig genutzte Zettel im Geldbeutel hat den Nachteil, dass bei dessen Verlust viel mehr als Ihr Bares in Gefahr ist.

Die Lösung mit einem Passwort, das für jeden Dienst genutzt wird, ist nur so lange sicher, wie es keine Probleme gibt. Aber die gibt es immer wieder – siehe "Berühmte Opfer". Oft sind die bei solchen spektakulären Hacks entwendeten Passwörter zwar noch verschlüsselt, aber viele dieser Passwörter sind innerhalb von Minuten oder Tagen geknackt.

1.	1911938	123456
2.	446162	123456789
3.	345834	password
4.	211659	adobe123
5.	201580	12345678
6.	130832	qwerty
7.	124253	1234567
8.	113884	111111
9.	83411	photoshop
10.	82694	123123

Die zehn häufigsten Passwörter, die bei Adobe gestohlen wurden.

Nachdem die Datendiebe auch wissen, dass viele immer das gleiche Passwort nutzen, probieren sie die erbeuteten Passwörter gleich bei anderen Diensten aus und bekommen so regelmäßig Zugriff auf E-Mail-Konten, Einkauf-Sites, ja sogar auf Bankkonten.

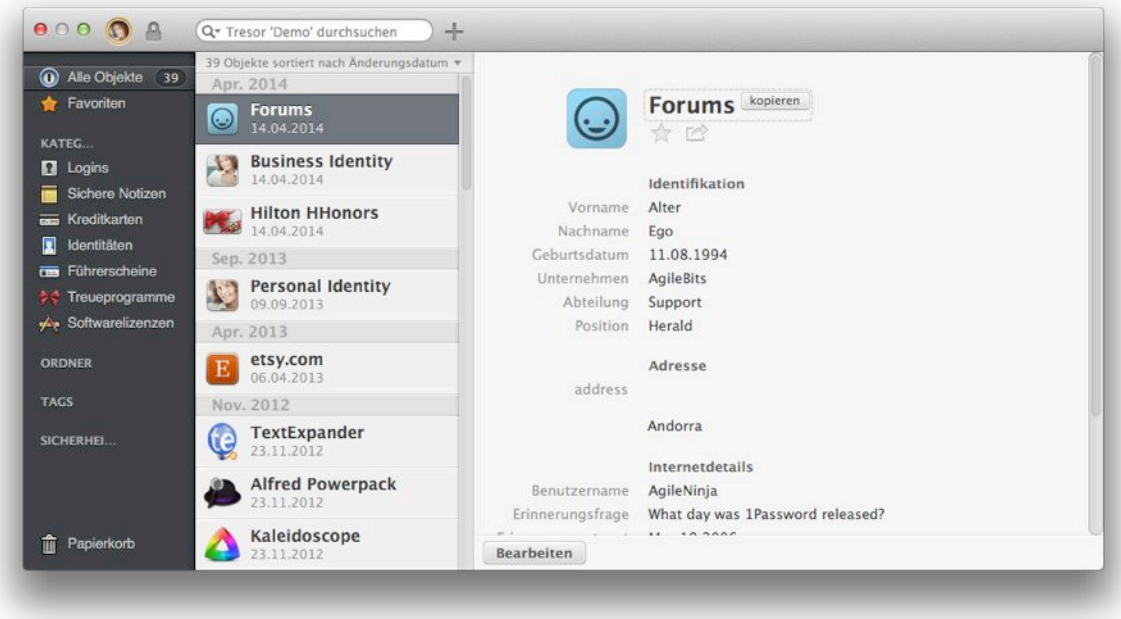
Fazit: Verwenden Sie **nie das gleiche Passwort für verschiedene Dienste**!

Passwort-Merken/-Speichern

Eine bessere Lösung des Problems sind Passwort-Manager. Also Programme, die alle Ihre Passwörter speichern, geschützt mit einem Master-Passwort. Das reduziert die Gedächtnisstrapazen, weil Sie nur noch ein einziges Passwort behalten müssen. Tun Sie sich dann aber den Gefallen und machen Sie dieses eine Passwort so sicher wie möglich (siehe weiter unten bei *Passwort-Wahl*).

Und ein weiterer Vorteil von guten Passwort-Managern: Diese nehmen Ihnen die Arbeit ab, Passwort und Nutzername auf jeder Website eingeben zu müssen. Sie suchen nur die Site aus einer Liste aus, und das Programm meldet sich (bzw. Sie) automatisch dort an.

Die ganze Bequemlichkeit hat natürlich ihren Preis: fangen Sie sich ein Schadprogramm ein, das zum Beispiel ihre Tastatureingaben aufzeichnet und weiterleitet, dann hat dessen Urheber Zugriff auf alle Ihre Zugangsdaten. Leider ist es beim Thema Sicherheit immer so: Sie können nur wählen, mit welchen Unzulänglichkeiten Sie am besten leben (und schlafen) können.



Der Passwort-Manager 1Password

Achtung: Vertrauen Sie Ihre Passwörter nie unverschlüsselt einem Unternehmen an. Es gibt ein paar Programme/Dienste, die legen Ihre Passwörter auf einem eigenen Server ab. Das bedeutet, Sie müssen darauf vertrauen, dass das Unternehmen sorgfältig arbeitet. Selbst wenn es nur das Beste will, aber einen Fehler macht, gelangen Ihre Daten in die falschen Hände. Die unten empfohlenen Dienste/Programme verschlüsseln Ihre Passwörter auf Ihrem Rechner, bevor Sie diese übertragen.

KeePass

Ein bewährter Passwort-Manager ist KeePass. Das ist ein open-source-Projekt. Das heißt, das Programm ist nicht nur kostenlos, sondern jeder kann sich theoretisch davon überzeugen, dass der Quellcode in Ordnung ist. Bisher gab es bei KeePass noch nie Probleme, und auch die Hacker haben sich an dem Programm bisher die Zähne ausgebissen. Ein Restrisiko bleibt aber immer, wenn Sie Ihre Passwörter einem Programm anvertrauen.

Als Nutzer installieren Sie das Programm auf Ihrem Rechner (Windows, Mac oder Linux). Dieses legt eine verschlüsselte Datenbank an, die auf einem beliebigen Cloud-Server liegen kann (Dropbox, Skydrive, WebDAV…). Auf diese Datenbank greifen Sie dann mit einem KeePass-Client zu.

Profitipp für noch mehr Sicherheit:
Man kann zusätzlich auf jedem lokalen Rechner noch eine Schlüsseldatei ablegen, die beim Öffnen der KeePass-Datei überprüft wird. Sollte die Password-Datei auf Dropbox abhandenkommen, kann der Dieb damit nichts anfangen, selbst wenn er sie entschlüsseln könnte. Denn er braucht zusätzlich zum Passwort für die Datei auch noch diese Schlüsseldatei, um an die Passwörter zu kommen.

Versionen für Desktop-Betriebsysteme
Die offizielle Seite des Projekts: http://keepass.info

iOS-Versionen
MiniKeePass (kostenlos) MiniKeePass im App-Store
iKeePass (ca. 1€) iKeePass im App-Store
KyPass (ca. 3€) KyPass im App-Store

Windows Phone-Version
7Pass (ca. 1€) http://7pass.wordpress.com

Android-Version
KeePassDroid (kostenlos) KeePassDroid im Google Play Store
Keepass2Android (kostenlos) Keepass2Android im Google Play Store

1 Password

Besonders unter Mac- und iOS-Nutzern erfreut sich das Programm *1 Password* einiger Beliebtheit. Inzwischen gibt es auch Versionen für Windows und Android. Dieser Passwort-Manager arbeitet nach dem gleichen Prinzip wie KeePass, auch hier können Sie die verschlüsselte Datenbank auf einem beliebigen Cloud-Speicher ablegen. Das Programm selbst ist allerdings kommerziell (ca. 40€ für die Desktop-Version, für iOS und Android 16€).

Die Programme wirken etwas polierter und bequemer als KeePass, sicherer ist aber eine open-source-Lösung.

Mehr Infos: https://agilebits.com/onepassword

LastPass

Immer wieder liest man auch Gutes von LastPass. Dieser Kennwort-Manager hat sogar eine praktische Funktion zum Teilen von Passwörtern. Damit müssen Sie Passwörter nicht mehr unsicher per Mail verschicken. Man kann damit Passwörter sogar verleihen: Sie können ein

Passwort so teilen, das der andere Ihr Passwort gar nicht sieht. Um die Passwörter zu empfangen, muss sich der Empfänger allerdings (kostenlos) registrieren.

Die Site wirkt auf mich persönlich etwas unbeholfen gestaltet und seltsam getextet - das fördert das Vertrauen bei mir nicht.

Mehr Infos: https://lastpass.com/

Passwörter teilen

Am besten ist: Teilen Sie Ihre Passwörter gar nicht. Kommt das nicht in Frage, dann gibt es folgende Möglichkeiten, mit absteigender Sicherheit:

1. Persönlich
2. Per Telefon
3. Per Brief (mit Einschreiben, Vermerk "persönlich")
4. Per SMS
5. Per speziellem Online-Dienst
6. Auf mehreren Kanälen (den ersten Teil per Skype, den nächsten per Chat o. Ä.)
7. In mehreren Mails (nicht empfehlenswert)

Besser als Passwörter per Mail zu verschicken ist z. B. One Time Secret. Bei diesem kostenlosen Dienst geben Sie das Passwort ein und verschicken dann den Link zu dieser Seite. Dieser Link zeigt das Passwort an und löscht es sofort. Das heißt, auch wer später z.B. die Mail findet, kann an das Passwort nicht mehr heran.

Einen Blick wert ist auch der Online-Dienst Passpack, den habe ich selbst aber nicht getestet.

Passwort-Wahl

Wie sieht ein gutes Passwort aus? Was sollten Sie beachten, wenn Sie ein Passwort vergeben?

Das sichere Grundpasswort

Überlegen Sie sich einen Standard-Satz, den Sie sich leicht merken können. Etwa:

```
Mein Passwort ist wirklich sicher, vor allem im Mai.
```

Von diesem Satz nehmen Sie die Anfangsbuchstaben und das Satzzeichen:

```
MPiws,vaiM.
```

Lang

Je länger ein Passwort, desto sicherer ist es. Generell gilt für Passwörter das Gleiche wie für Haustüren: Perfekte Sicherheit gibt es nicht. Man kommt überall rein, es ist nur eine Frage des Aufwands.

Und bei Passwörtern bedeutet das: Je mehr und je schnellere Computer (bzw. Rechenkerne) ein Hacker einsetzt, desto schneller hat er Ihr Passwort geknackt. Eine absolute Empfehlung für die Länge kann man schwer geben. Klar ist aber, dass es unter acht Zeichen Länge fahrlässig wird.

Welches Passwort ist sicherer: `Rz8hx8&h$j` oder `E1s`.....? Antwort: Das Zweite, obwohl es leichter zu merken ist. Denn es ist viel länger. Schwer zu glauben, daher lesen Sie am besten selbst nach über das Konzept des "Password Padding" (nur englisch): Passwort-Test

Um Ihr Passwort noch sicherer zu machen, "padden" Sie es. Padding bedeutet ausstopfen/auspolstern. Sie verpacken Ihr Passwort in eine Zeichenkette, die Sie sich leicht merken können.

Zum Beispiel `+++++++++MPiws,vaiM.+++++++++`. Nehmen Sie nicht das Plus, sondern ein Zeichen, das Sie sich selbst ausgesucht haben – oder, noch besser, eine Zeichenkombination wie +–+.

Besonders

Passwortknacker probieren heute nicht mehr einfach nur stupide ein Passwort nach dem anderen. Sie beginnen mit denen, die am häufigsten verwendet werden. Dann testen sie verschiedene Varianten davon, die typisch sind. Dank der Massen geklauter Passwörter der letzten Monate weiß man recht gut, wie Menschen Passwörter vergeben. Aussprechbare Silben sind zum Beispiel viel häufiger als nicht aussprechbare. Vierstellige Zahlen zwischen 1950 und 2013 sind sehr häufig – da haben viele Menschen Geburtstag, sie haben in diesem Jahr geheiratet oder ihre Kinder wurden geboren. Deshalb ist etwa `HaMaDa1977Fa` auf den ersten Blick ein gutes Passwort. Aber leider ist es so schematisch aufgebaut, dass es sehr schnell gehackt ist. Auch bekannte Zeichenfolgen wie :-), `<3` oder `lol` finden sich in jedem Lexikon für Passwortknacker. Fast alles, was Menschen sich leicht merken können ist als Passwort leider schlecht geeignet.

Kompliziert

Ein gutes Passwort ist also kompliziert. Das heißt, es ist nicht nur lang, sondern auch zufällig und es enthält keine typischen Muster.

Derzeit hat ein Passwort, das mit dem üblichen Aufwand nicht geknackt werden kann, folgende Eigenschaften:

- mindestens 9 Stellen
- Groß- und Kleinbuchstaben
- mindestens ein Sonderzeichen wie -;&@ etc.

Wenn es ganz sicher sein soll, sollte Ihr Passwort **vollkommen zufällig** sein. Damit Sie bei der Erstellung nicht doch unbewusst logische Muster erzeugen, etwa indem Sie Buchstaben nehmen, die auf der Tastatur näher beieinander liegen, nutzen Sie am besten einen Passwortgenerator, wie er in viele Passwort-Manager eingebaut ist (siehe oben).

Ein Passwort ist nur einmal gut
Ein Passwort sollte nicht nur für Sie einmalig sein (weshalb `passwort` das allerschlechteste Passwort ist, das nutzen immer noch erstaunlich viele Menschen). Weil auch noch so gute Passwörter immer in falsche Hände gelangen können, sollte jedes Passwort auch nur *an genau einer Stelle* eingesetzt werden. Wer auf sein Hirn setzt und sich seine Passwörter alle merkt: Verwenden Sie zum Beispiel ein Grundpasswort und hängen Sie daran für jeden Dienst einen Anhang. Also zum Beispiel für Xing:

```
grundpasswort-xin38g
```

`grundpasswort` ist dabei Ihr Basispasswort, das Sie immer verwenden. Und die `38` ist dafür da, weil das Anhängsel `xing` allein zu leicht zu erraten wäre. Und um es noch schwerer zu machen, hängen Sie es nicht ans Ende, sondern an den vorletzten Buchstaben. Noch besser ist, die Buchstaben des Dienstes im Passwort zu verteilen:

```
gxriunngdpasswort-38
```

Haben Sie es erkannt? Jeder zweite Buchstabe ist der des Dienstes:

```
gXrIuNnGdpasswort-38
```

Wem das zu aufwendig ist, der greift vielleicht doch lieber zu einem der oben empfohlenen Passwort-Manager.

> *Im Zweifel lieber nicht so geheim*
> Wenn Sie wie beschrieben mit Grundpasswörtern arbeiten: sparen Sie sich Ihr Grundpasswort für die wichtigen Dienste auf. Bei Foren oder Diensten, bei denen Sie nicht mit Ihrem Klarnamen auftreten und bei denen Sie keine wichtigen Daten speichern, geben Sie lieber ein Passwort an, das Sie sich leicht merken können und das schnell eingetippt ist. Wenn der Dienst-Betreiber absichtlich oder unabsichtlich Schindluder damit treibt, gerät Ihr wertvolles Grundpasswort nicht in falsche Hände. Auch wenn es bei jedem Dienst etwas anders aussieht: hat ein Passwortknacker zwei, drei Varianten Ihres Passworts und die Namen der dazugehörigen Dienste, kann er Ihr Grundpasswort erraten.

Wer macht denn sowas?

Vielleicht fragen Sie sich, warum wir diesen großen Aufwand überhaupt betreiben müssen. Wer klaut schon Ihre persönlichen Passwörter?

Es gibt Hacker, die haben es auf Sie persönlich abgesehen. Doch das ist sehr selten, denn die meisten Menschen sind weder so reich noch so einflussreich, dass es sich lohnt, sie direkt anzugehen. Die meisten Hacker suchen einfach nur nach der leichtesten Beute. Dabei ist es ihnen egal, wer ihr Opfer ist.

Ihr Ziel ist oft eher sportlich: sie wollen zeigen, was sie können. Dass sie dabei großen Schaden anrichten, nehmen sie in Kauf. Manche hacken auch zum Geldverdienen. Gestohlene Passwörter lassen sich auf dem Schwarzmarkt über einschlägige Foren leicht verkaufen.

Man darf sich den typischen Passwort-Dieb nicht als bösartiges Genie aus einem Agentenfilm vorstellen. Denn es braucht nicht viel Können. Wer schon mal eine Windows-Installation selbst gemacht hat, kann auch Passwörter knacken. Man lädt sich ein paar kostenlose Programme herunter, liest in einigen Foren und hat innerhalb eines Tages die ersten Erfolge. Wer das nicht glauben kann, dem empfehle ich den Artikel des Journalisten Nate Anderson, in dem er beschreibt, wie er ohne Vorwissen in nur einem Arbeitstag gelernt hat, wie man das Passwort-Knacken lernt: How I became a password cracker

Sicherheitsrisiko Sicherheitsfragen

Vorsicht ist bei den "Sicherheitsfragen" von Webdiensten geboten. (Zum Beispiel "Wie ist der Mädchenname Ihrer Mutter?"). Erstens sind solche Antworten mit der Hilfe von Google, Facebook, Xing oder mit ein, zwei Anrufen bei nichts ahnenden Freunden oder Verwandten problemlos herauszubekommen. Außerdem: Gelangen diese Antworten durch einen Server-Hack in falsche Hände, können die Diebe die Antworten auch bei anderen Diensten nutzen, um Ihre E-Mail-Adresse auf ihre eigene zu ändern. Daher empfiehlt es sich, absichtlich falsche Antworten zu geben. (Die Sie aber natürlich nicht vergessen sollten…)

Sicherheitsplus Zwei-Stufen-Authentifizierung

Wo immer möglich nutzen Sie bei Webdiensten die so genannte Zwei-Stufen-Authentifizierung (two-factor-authentification). Diese bieten zum Beispiel Google, Twitter oder Apple. Haben Sie die Zwei-Stufen-Authentifizierung aktiviert und melden Sie sich von einem Gerät aus an, das sie bisher noch nicht dafür verwendet haben, dann müssen Sie eine zweite Sicherheitsüberprüfung machen. Normalerweise bekommen Sie eine SMS mit einem Code, den Sie dann eingeben müssen.

> *Warum sind Banken-Sites sicher?*
> Banken-Sites sperren einen Nutzer normalerweise, wenn für diesen dreimal das falsche Passwort eingegeben wurde. Um wieder zugreifen zu können, muss man sich über einen anderen Kanal authentifizieren, etwa per Telefon. Einen Link zum Zurücksetzen des Passworts gibt es nicht. Das könnten andere Sites genauso machen, würde aber die Benutzerfreundlichkeit deutlich reduzieren und die Supportkosten deutlich erhöhen.

Fazit

Die besten Passwörter sind vollkommen zufällig. Nachdem wir uns solche am schlechtesten merken können, müssen wir Kompromisse machen.

Lösung eins: Nutzen Sie einen Passwortmanager, vergeben Sie mit dessen Hilfe vollkommen zufällige Passwörter und merken Sie sich ein sehr gutes Passwort für den Zugriff auf den Passwortmanager.

Lösung zwei: Vergeben Sie so lange Passwörter wie möglich. Damit Sie sich das irgendwie merken können, nutzen Sie „Padding“: Polstern Sie das eigentliche Passwort mit einer möglichst langen Kette gleicher Zeichen.

Fragen? Anregungen? Kritik? Jederzeit gern auf www.benutzerfreun.de/auf-einen-kaffee!

Vielen Dank an die sehr hilfreichen Korrekturleser: Matthias Gidda, Heiko Müller, Ficus Elastica und Hampa Brügger. Ihre Tipps haben geholfen, dieses E-Book deutlich zu verbessern.

© Jens Jacobsen 2014. Alle Rechte vorbehalten.
Bitte dieses E-Book nicht direkt weitergeben. Sehr gern können Sie aber den Link zum kostenlosen Download weitergeben: www.benutzerfreun.de/auf-einen-kaffee