

Wie man gespeicherte Passwörter in OS X nachschaauen kann

von Topher Kessler (macissues.com), Übersetzung: KJM



Hat man einmal ein Passwort in eine Webseite eingegeben und es in seinem „Schlüsselbund“ gespeichert, verlässt man sich oft einzig und allein auf das automatische Ausfüllen, um dieses Passwort später erneut einzugeben. Das automatische Ausfüllen ist natürlich bequem, aber führt, wenn man sich allein darauf verlässt, dazu, dass man sein Passwort vergisst oder es nicht einmal kennt.

Wenn man zum Beispiel ein Online-Konto anlegt, kann man Apples automatischen Passwort-Generator nutzen, der ein zufälliges Passwort erzeugt, das automatisch im Schlüsselbund gespeichert wird, aber wenn man zu einem späteren Zeitpunkt auf dieses Konto zugreifen muss, ohne sich direkt des Schlüsselbundes zum automatischen Ausfüllen bedienen zu können, dann hat man möglicherweise keinen blassen Schimmer, wie das Passwort lautet.

Das kann passieren, wenn man ein anderes Gerät benutzt als das, an dem man das Passwort angelegt hat; z. B. an einem öffentlichen System oder an dem eines Freundes. Wenn man in so einem Fall sein Passwort herausfinden will, kann man das am originalen Rechner tun, indem man ein paar schnelle Routinen im Programm Schlüsselbundverwaltung anwendet.

1. Die Schlüsselbundverwaltung öffnen

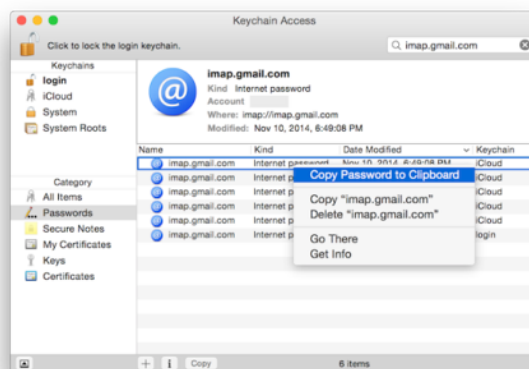
2. Den „Login“-Schlüsselbund auswählen

3. Einen Teil der URL der Website suchen

Dieser letzte Schritt sollte nahezu augenblicklich den entsprechenden Schlüsselbund-Eintrag dieser URL zeigen. Wenn Sie z. B. Ihr Gmail-Passwort suchen, können Sie nach „gmail“ oder „gmail.com“ suchen und den Passwort-Eintrag sehen. Beachten Sie, dass Sie die Benutzernamen dieser Einträge aufgelistet sehen und dass Sie, je nachdem, wie Sie Ihren Schlüsselbund in der Vergangenheit verwaltet haben, u. U. mehrere Einträge für Ihren Benutzernamen zu sehen bekommen. Diese können vom Eintragen des Passworts in Mail oder in anderen Programmen auf Ihrem Mac stammen – zusätzlich zu denen, die Safari zwecks automatischem Ausfüllen speichert.

Um nun das Passwort zu enthüllen, wenn Sie den Eintrag gefunden haben, haben Sie zwei Optionen:

1. Kopieren Sie es, indem Sie einen Rechtsklick auf den Schlüsselbund-Eintrag ausführen und den Befehl wählen „Passwort in die Zwischenablage kopieren“ oder aber **Shift-Command-C** drücken.
2. Enthüllen Sie es, indem Sie einen Doppelklick auf den Eintrag ausführen, um ihn zu öffnen, und dann die Schaltfläche „Passwort anzeigen“ ankreuzen.



Ein Rechtsklick auf einen Schlüsselbund-Eintrag gibt einem die Möglichkeit, das Passwort in die Zwischenablage zu kopieren. Man kann auch den Eintrag doppelklicken, um sein Passwort zu enthüllen. Für beide Optionen benötigt man sein Schlüsselbund-Passwort.

Tut man eins von beiden, wird man aufgefordert, sein Schlüsselbund-Passwort einzugeben (für die meisten Anwender wird das ihr Anmelde-Passwort sein); dann wird das Passwort kopiert oder angezeigt werden. Sie können es sich dann notieren oder anderweitig speichern, um es auf anderen Geräten nutzen zu können.

Anmerkung KJM:

Es ist bei der Passwort-Verwaltung – wie in anderen Sicherheitsbereichen auch – ratsam, eine Doppelstrategie zu benutzen und neben der OS X Schlüsselbundverwaltung auch noch andere Passwort-Software zu benutzen. Im Mac App Store gibt es mittlerweile zahlreiche Apps für diesen Zweck, von kostenlos bis (auf den ersten Blick) recht teuer. Allerdings sollte man beim Thema Sicherheit nicht sparen.

Führende Produkte wie **1Password** bieten u. a. ein Menüleiten-Programm, das den Zugriff auf die Passwörter nicht nur im Browser, sondern auch in anderen Programmen und im Finder ermöglicht, und auch die dazu passende iOS-App, die es ermöglicht, gespeicherte Passwörter per WLAN (also, falls gewünscht, ohne Verwendung der iCloud) zwischen allen verbundenen Geräten abzugleichen.

Zwei-Stufen-Authentifizierung

Bloß nicht den Wiederherstellungsschlüssel verlieren

giga.de/macnews/

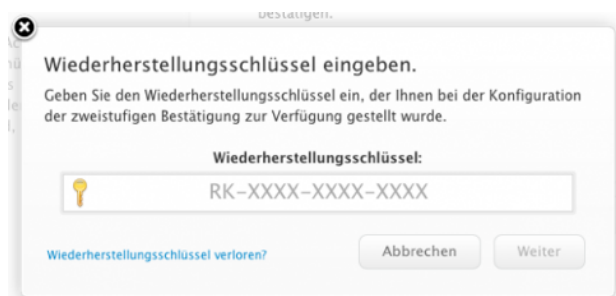
Seit Februar verfügen Apples Benutzerkonten auch hierzulande über eine Zwei-Stufen-Authentifizierung. Dass diese Funktion sehr sicher ist und auch verantwortungsvoll vom Anwender genutzt werden muss zeigt ein neuer Fall aus Neuseeland.

Die zwei-Stufen-Authentifizierung funktioniert grob erklärt nach folgendem Prinzip: Der Nutzer muss etwas wissen (in der Regel ein Passwort) und etwas haben (meist ein Sicherheitstoken, bzw. ein vertrauenswürdige Gerät). Möchte er sich anmelden, wird er zunächst nach dem Passwort gefragt. Ist die Eingabe korrekt, bekommt er beispielsweise einen Code auf sein vertrauenswürdige iPhone geschickt, ruft diesen ab und gibt ihn ein. Fertig ist der Anmeldeprozess.

Hacker aus der Ferne haben somit keine Möglichkeit selbst bei korrekter Passwordeingabe sich einzuloggen. Die Zwei-Stufen-Authentifizierung ist in heutigen Zeiten, in denen fast schon monatlich immer wieder Datensätze mit vielen Nutzerdaten gestohlen werden, sehr empfehlenswert. Doch wie Owen Wilson, ein Journalist des Technikportals [The Next Web](#) am eigenen Leib erfahren musste, muss man mit der Sicherheitsfunktion auch sorgsam umgehen.

Wiederherstellungsschlüssel als zusätzliche Sicherheitsstufe

Denn Apple hat zusätzlich zum Passwort und dem vertrauenswürdigen Gerät auch einen Wiederherstellungsschlüssel eingebaut. Sollte beispielsweise das iPhone mal kaputt gehen oder wir das [Passwort vergessen](#), gibt es immer noch die Möglichkeit sich durch die Eingabe eines 14-stelligen Codes in sein Benutzerkonto einzuloggen. Dieser Code sollte bestenfalls ausgedruckt und an einem sicheren Ort aufbewahrt werden.



Was ist nun also bei Owen Wilson passiert? Ein Krimineller hat versucht, sich in sein Apple-Benutzerkonto

einzuloggen, scheiterte aber an der zwei-Stufen-Authentifizierung. Daraufhin versetzte Apple das Konto in den Recovery Modus. Das hatte zur Folge, dass beim Einloggen nun sofort nach dem Wiederherstellungsschlüssel gefragt wurde. Erst danach sollte das Profil wieder entsperrt werden. Allerdings konnte Wilson den Key nirgends finden.

Auch bei der Apple-Hotline konnte ihm aus Sicherheitsgründen nicht geholfen werden. So steht es auch im entsprechenden [Support-Dokument](#): "If you have permanently lost any two of these items, you will not be able to sign in or regain access to your account. You will need to create a new Apple ID." Auch an der Hotline war der einzige Rat, den man für Wilson hatte, sich ein neues Nutzerkonto anzulegen.

Apple-Support kann im Verlustfall nicht helfen

Nach langem Suchen konnte der Redakteur auf einem alten Backup doch noch einen Screenshot mit dem Wiederherstellungsschlüssel finden und somit wieder Zugriff auf sein Konto erlangen.

Vom Sicherheits-Aspekt betrachtet ist es beruhigend, dass Apples System hier zu greifen scheint und konsequent durchgezogen wird. Allerdings müssen sich die Nutzer auch der Bedeutung ihres Wiederherstellungsschlüssels bewusst sein und dass sie damit sorgsam umgehen sollten. Dann ist die Zwei-Stufen-Authentifizierung wirklich eine gute Sache.

Sollte sich von den Lesern nun jemand unsicher sein, wo sich sein Schlüssel befindet: So lange ihr Passwort und das Gerät habt, könnt ihr euch jederzeit unter [appleid.apple.com](#) einloggen (vorausgesetzt ihr wurdet nicht gehackt oder ähnliches) und euch einen neuen Schlüssel generieren lassen.

Mehr zum Thema:

- [Zwei-Faktor-Authentifizierung: Mehr Sicherheit für eure Accounts](#)
- [Zwei-Faktor-Authentifizierung aktivieren – so geht's](#)
- [Apple erweitert 2-Stufen-Authentifizierung auf iCloud aus](#)



WLAN-Probleme am Mac

Wenn der Rechner sich nicht mit dem WiFi-Netz verbindet

von Sebastian Trepesch (giga.de)

Was können wir tun, wenn sich der Mac nicht mit dem WLAN verbinden möchte? Hier präsentieren wir sechs Lösungsansätze und nennen empfohlene Einstellungen für das Netzwerk.

Schade, dass wir uns so mit WLAN-Problemen herumärgern müssen. Manchmal trägt das Betriebssystem die Schuld. In iOS 8 und OS X 10.10 soll die Technologie, die hinter AirDrop, AirPlay und anderen Funktionen steckt, aktuell Schwierigkeiten bereiten, [fand ein Entwickler heraus](#). Für eine sinnvolle Lösung müssen wir auf ein Update warten; unten nennen wir erste Hilfe.

Hier folgen nun sechs Tipps; wir beginnen mit den am einfachsten umsetzbaren. Manche Lösungsansätze klingen überraschend einfach, können aber trotzdem helfen. Durchprobieren heißt die Devise. Zum Schluss nennen wir noch empfohlene Einstellungen für das WLAN-Netz.

- [Für iOS: WLAN-Probleme: Wenn sich das iPhone nicht mit dem WiFi-Netz verbindet](#)

Sind die WLAN-Probleme wirklich WLAN-Probleme?

Eine Vorüberlegung, bevor wir uns die Lösungsansätze durchgehen: Haben wir wirklich ein Problem mit dem WiFi-Netz, also verbindet sich das MacBook oder der iMac nicht mit dem WLAN? Oder ist der Rechner mit dem heimischen Netz verbunden, und die Internetverbindung zwischen Router und Mobilfunkanbieter funktioniert nicht?

Am schnellsten erkennen wir das über das WLAN-Symbol in der Symbolleiste von OS X Yosemite. So wie

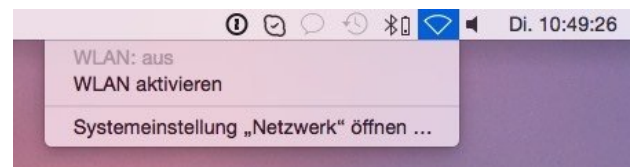
in diesem Bild sieht es aus, wenn der Mac korrekt mit dem Netzwerk verbunden ist.



Wir gehen hier die Lösungen an, wenn die Verbindung zwischen Mac und Router schon nicht mehr läuft. Könnte sie noch nie erstellt werden, kommen unter anderem eine zu große Entfernung oder Störquellen in Frage, sowie falsche Einstellungen – siehe letzte Seite.

1. WLAN des Macs aus- und anschalten

Schalte das WLAN auf dem Mac aus, warte kurz und schalte es wieder an. Gerade wenn viele Geräte mit einem Netzwerk verbunden sind, kann dies Konflikte manchmal schon lösen.



Dieser Vorgang kann (auch auf iPads) helfen, ein WLAN-Netz angezeigt zu bekommen, das vorher nicht zu sehen war. Es darf natürlich nicht auf „unsichtbar“ gestellt sein.

2. Router neu starten

Schalte den Router aus, noch besser: stecke ihn aus. Warte eine halbe Minute, stecke ihn wieder ein und schalte ihn ein. Alle Geräte werden nun neu verbunden – das wirkt oft Wunder. Denn das Problem muss ja nicht unbedingt am Mac liegen, es kann auch der Router der Verursacher sein.

3. Bei WLAN-Problemen AirDrop ausschalten

Wie eingangs beschrieben, bereitet in den aktuellen Betriebssystem-Versionen die Technologie Apple Wireless Direct Link Probleme. Wir können sie ausschalten, dann ist allerdings auch AirDrop und Co nicht mehr möglich. Hierfür muss laut Entwickler Ciabarra im Terminal von OS X Yosemite (zum Beispiel über die Suche aufrufbar) folgender Befehl eingegeben werden:

```
sudo ifconfig awdl0 down
```

Diesen Befehl machen wir mit folgender Zeile wieder rückgängig:

```
sudo ifconfig awdl0 up
```

(Für iPhone: [jailbreaker](#) können auf das Tool WiFried zurückgreifen und wahlweise D2DWiFi/AWDL ein- oder ausschalten.)



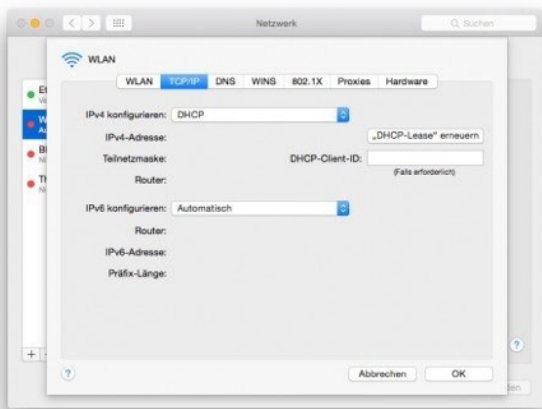
4. Nach Updates für alle beteiligten Geräte suchen

Vielleicht haben die Hersteller ihre Betriebssysteme schon wieder in einer neuen Version aufeinander abgestimmt. Suche nicht nur nach Updates für OS X Yosemite, sondern auch nach einer Aktualisierung für die Netzwerkgeräte – also Router und gegebenenfalls Modem, Verstärker oder ähnliches.

Beispiel: [Fritz!Box-Einstellungen aufrufen und Update installieren, so geht's.](#)

5. Netzwerkeinstellungen erneuern

Hilft das alles nichts, müssen wir einen Schritt weitergehen – und unsere Netzwerkeinstellungen erneuern. Hiermit beseitigen wir eventuelle Konflikte der IP-Adressen in unserem Netz. Rufe die Systemeinstellungen von OS X Yosemite auf und gehe zu Netzwerk -> WLAN -> Weitere Optionen -> TCP/IP. Klicke hier den Button DHCP-Lease erneuern.



Ein anderer Versuch in Netzwerk: Über das + links unten eine neue WLAN-Umgebung einrichten.

6. Router bei WLAN-Problemen zurücksetzen

Das Zurücksetzen des Routers soll einem Nutzerkommentar zufolge schon zur Problemlösung geführt haben. Der Nachteil ist nur leider, dass wir unsere Einstellungen erneut vornehmen müssen. Manch ein Router erlaubt die Speicherung und das Wiederaufspielen der Benutzereingaben. Probieren kann man das – es könnte aber sein, dass dies auch die Ursache für die Verbindungsprobleme wieder herstellt...



Empfohlene Einstellungen für WLAN-Router

Verbindungsprobleme können aus suboptimalen Netzwerkeinstellungen entstehen. Folgende Parameter empfiehlt Apple:

Einen eindeutigen SSID-Namen wählen

Hier ist es bei vielen Routern wichtig, sich vom Standardname zu verabschieden und einen eigenen unverwechselbaren zu erstellen.

MAC-Adresserkennung ausschalten

Geräte, deren MAC-Adressen nicht in den Router-Einstellungen hinterlegt sind, können sich nicht mit dem Netz verbinden. Eine eingeschaltete Adressfilterung ist zwar sicherer. Apple gibt aber zu Bedenken, dass mittels Adressänderung auch so ein unerlaubter Zugriff auf das Netzwerk erfolgen könnte.

Kein unsichtbares Netzwerk

Unsichtbare Netzwerke werden von den Geräten schwieriger gefunden, die Verbindungszeiten können deshalb langsamer und unzuverlässiger sein.

WPA2 als Sicherheitseinstellung

WPA2 Personal (AES) ist aktuell die sicherste Stufe für die Netzwerke, WEP ist überholt – übrigens auch in Sachen Zuverlässigkeit.

Sendermodus in der Standardkonfiguration

Die vorhandenen WLAN-Standards sollten im Router allesamt aktiviert sein, also 802.11a/b/g/n und ac. Damit kann eine möglichst schnelle Verbindung mit dem Rechner vorgenommen werden – oder eine alte, wenn das Gerät das neueste Protokoll noch nicht unterstützt.

Kanal und Kanalbreite

Den Kanal lassen wir unseren Router am besten automatisch wählen, die Einstellung lautet also Auto oder ähnlich. Für die Kanalbreite ist im 2,4-GHz-Netz die Einstellung 20 MHz weniger störanfällig. Bei 5 GHz sollten beide Wahlmöglichkeiten, 20 MHz und 40 MHz, aktiviert sein – sofern verfügbar.

DHCP und NAT

Nur ein DHCP-Server, der die Adressen zuweist, soll im Netzwerk agieren – im Normalfall das Modem. Gleiches gilt für den NAT-Dienst, für die Kommunikation zwischen Internet und unserem Netzwerk. Nur in einem Gerät des Netzwerks darf NAT aktiviert sein.