macOS Big Sur 11.2.1 und Updates für Catalina sowie Mojave

Quelle: fen (mactechnews.de)

Soeben tauchte in der Software-Aktualisierung ein weiteres Systemupdate auf. Es handelt sich aber um eine kleinere Aktualisierung, wie die Versionsnummer "11.2.1" bereits suggeriert. Eine Woche nach der Veröffentlichung von macOS 11.2 schob Apple nämlich ein Bugfix-Update nach, welches sich nur an bestimmte Hardware richtet. In der Beschreibung heißt es, macOS 11.2.1 sei für das MacBook Pro der Modellreihen 2016 und 2017 bestimmt – also das erste MacBook Pro mit Touch Bar sowie dessen Nachfolger. Die Release Notes gehen auch auf die Verbesserungen ein und geben an, macOS 11.2.1 nehme sich eines Fehlers an, der das Aufladen der Akkus verhindern konnte.

Weitere Details nennt Apple nicht. Wenn Cupertino Formulierungen wie "einige" anstatt "in sehr seltenen Fällen" verwendet, handelt es sich normalerweise um einen etwas häufiger auftretenden Fehler. Der kurze Abstand zwischen macOS 11.2 und 11.2.1 deutet zudem an, dass es sich wohl um ein Problem handelte, das mit dem letzten größeren Update ins System wanderte. Laden und installieren lässt sich das 2,4 bis 3,5 GB riesige Systemupdate wie üblich via Software-Aktualisierung in den Systemeinstellungen.

Zu sehen ist die neue Version auch auf Geräten, die gemäß Updatebeschreibung gar nicht betroffen sein sollten. Der Grund dafür ist aber einfach: Ein Support-Dokument schlüsselt auf, dass macOS 11.2.1 auch Sicherheitsverbesserungen beinhaltet: . Neben macOS 11.2.1 stehen zudem das macOS Catalina 10.15.7 "Supplemental Update" und das macOS Mojave 10.14.6 "Security Update 2021-002" zur Verfügung.

Auswirkungen des Lade-Fehlers

Einigen Stimmen in den offiziellen Supportforen zufolge manifestierte sich der Fehler darin, dass der Ladestecker zwar angebracht wurde, betroffene Geräte allerdings nicht dem Laden begannen. Andere Nutzer berichteten, dass die Akkuanzeige plötzlich bei null Prozent stand und sich das MacBook Pro daraufhin deaktivierte. Mit dem Stecker verbunden waren es aber plötzlich wieder 100 Prozent und alles lief tadellos. Es ist ebenfalls unbekannt, ob theoretisch jedes MacBook Pro der Baujahre 2016 und 2017 darunter leiden konnte oder ob es sich nur um bestimmte Chargen handelte.

Ende des „sudo“-Bugs: Updates schließen schwere Sicherheitslücken

Quelle: bk (mactechnews.de)

Acht Tage nach der Veröffentlichung von macOS 11.2 legte Apple noch einmal nach – und stellt aktuell Version 11.2.1 sowie Sicherheitsupdates für Catalina und Mojave zur Verfügung. Die Updates geben bei betroffenen Baureihen des MacBook Pro Hinweis auf einen fehlerhaften Akku – Betroffene können diesen kostenlos bei Apple austauschen lassen (siehe). Alle gestern bereitgestellten Aktualisierungen nehmen sich zudem der Beseitigung eines schwerwiegenden Exploits an – und beheben Bugs bei Intel-Grafiktreibern.

„sudo“-Bug ausgemerzt

Mit dem „sudo“-Befehl lassen sich Prozesse mit den Rechten anderer Benutzer starten. Treten hier Sicherheitslücken auf, kann das gravierende Folgen nach sich ziehen: Angreifern wäre es möglich, sich Root-Zugang zu verschaffen und sich damit Zugriff über einen fremden Rechner zu verschaffen. Somit ließen sich die Daten anderer abgreifen. Dabei handelt es sich um keine Möglichkeit, die bloß in der Theorie besteht: Wie vor etwa einer Woche bekannt wurde (siehe), ist macOS von dieser Schwachstelle betroffen. Mit den gestern veröffentlichten Updates gehört der Exploit aber der Vergangenheit an: Wie Apple in einem Support-Dokument erläutert, kommt nun die neue „sudo“-Version 1.9.5p2 zum Einsatz. Somit müssen sich Inhaber von Macs, die zumindest mit macOS Mojave kompatibel sind, keine Gedanken mehr über Angriffe dieser Art machen.

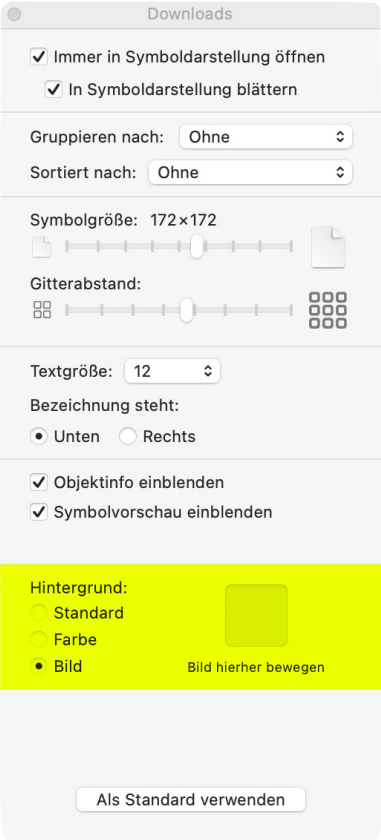
Weitere Fehler behoben

Apples Beschreibung der Sicherheitsupdates gibt aber auch Aufschluss über weitere Bugs, die von macOS 11.2.1 sowie dem Supplemental Update für 10.15.7 adressiert werden: Dabei geht es um Fehler von Intel-Grafiktreibern, bei denen Anwendungen unter Umständen beliebigen Code mit Kernel-Berechtigungen auszuführen vermochten. Das Problem scheint sich lediglich auf Big Sur und Catalina zu beschränken – bei Mojave wurde nach Auskunft Apples „nur“ die „sudo“-Lücke geschlossen. Sämtliche Sicherheitsupdates lassen sich über den Punkt „Softwareupdate“ in den Systemeinstellungen des Macs herunterladen und installieren.

Eigener Hintergrund für Finder-Fenster

Quelle: Chris (ifun.de)

Hand aufs Herz: Wer von den langjährigen Mac-Nutzern unter euch wusste, dass man Finder-Fenstern eigene Hintergrundfarben oder Bilder zuweisen kann? Die Option besteht zwar schon seit Jahren, ist allerdings kaum bekannt und findet im privaten Bereich auch nur selten Anwendung. App-Anbieter nutzen die Möglichkeit dagegen gerne, um beispielsweise bei ihren Datei-Images ein Bild mit Installationsanweisungen zu hinterlegen.

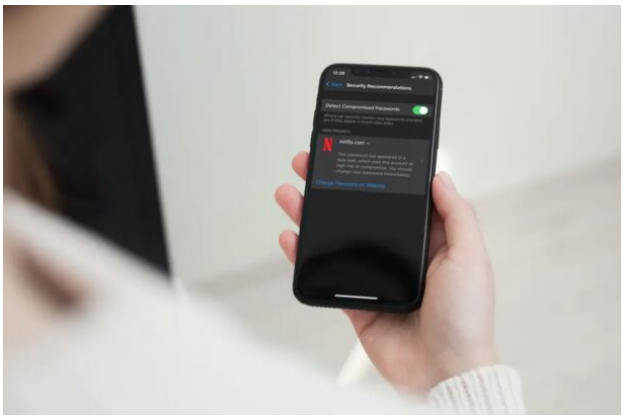


Ein Grund für den seltenen Einsatz der Funktion dürfte sein, dass sich der Hintergrund von Finder-Fenstern nur im verändern lässt, wenn die Option „**Ansicht als Symbole**“ ausgewählt ist. Über das Finder-Menü „Darstellung“ oder das Tastenkürzel Befehl+J könnt ihr die Darstellungsoptionen für das aktuell ausgewählte Finder-Fenster aufrufen. Im unteren Bereich des Einstellungsfensters seht ihr dann die für den Hintergrund verfügbaren Optionen. Als Alternative zur Standard-Darstellung kann man hier eine eigene Farbe oder ein eigenes Bild zuweisen.

Im aktuellen Handbuch von macOS Big Sur erklärt Apple die Möglichkeiten zum Anpassen des Fensterhintergrunds im Bereich „Ändern von Anzeigeoptionen im Finder auf dem Mac“. Ergänzende Informationen zum ändern der Symbole für Dateien oder Ordner findet ihr hier, dort könnt ihr nachlesen, wie ihr hier statt der Systemvorgaben eigene Bilder und Farben verwendet.

Überprüfung auf kompromittierte oder geleakte Passwörter auf iPhone & iPad mit Sicherheitsempfehlungen

Quelle: osxdaily.com, Übersetzung KJM und DeepL



Haben Sie sich jemals gefragt, ob die Passwörter zu einem Ihrer Online-Konten durch eine Datenpanne kompromittiert worden sind? Da sind Sie sicher nicht der Einzige, aber jetzt können Sie ganz einfach direkt von Ihrem iPhone und iPad aus überprüfen, ob die Sicherheit Ihrer Passwörter verletzt wurde.

In den neuesten Versionen von iOS und iPadOS (14 und später) hat Apple eine Sicherheitsfunktion namens "Sicherheitsempfehlungen" hinzugefügt, die Sicherheitswarnungen für die im iCloud-Schlüsselbund gespeicherten Passwörter liefern würde. Wenn eines oder mehrere Ihrer Konten ein Passwort verwenden, das leicht zu erraten ist, eine Sequenz wie 123 verwendet oder ein Passwort, das zuvor aufgrund einer Datenverletzung im Internet geleakt wurde, werden Sie gewarnt und aufgefordert, das Passwort für diese Konten zu ändern.

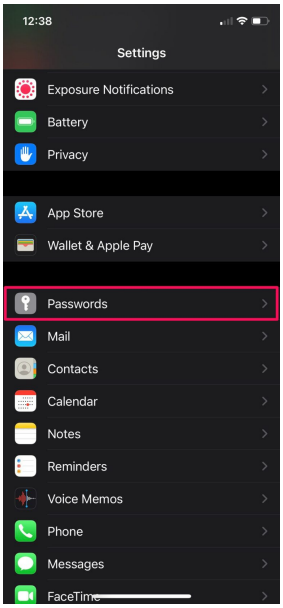
Möchten Sie sicherstellen, dass keines der von Ihnen verwendeten Passwörter ein Sicherheitsrisiko darstellt? In diesem Artikel erfahren Sie, wie Sie die Kennwort-Sicherheitsempfehlungen auf Ihrem iPhone und iPad überprüfen können.

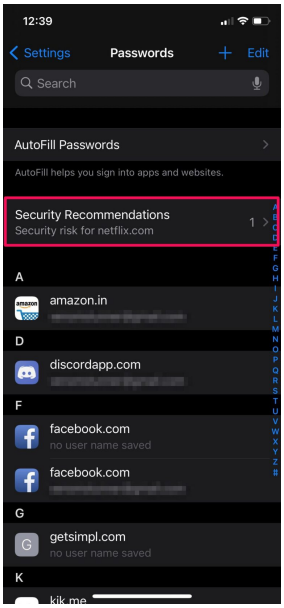
Wie man Passwort-Sicherheitsempfehlungen auf iPhone & iPad überprüft

Da dies eine Funktion ist, die zusammen mit modernen Versionen von iOS und iPadOS eingeführt wurde, stellen Sie sicher, dass auf Ihrem Gerät iOS 14/iPadOS 14 oder höher läuft, bevor Sie mit dem Verfahren fortfahren. Angenommen, Sie verwenden eine moderne Systemsoftware-Version, dann ist hier alles, was Sie als nächstes tun müssen:

Gehen Sie auf dem Startbildschirm Ihres iPhones oder iPads zu „Einstellungen“.

Scrollen Sie im Einstellungsmenü nach unten und tippen Sie auf "Passwörter".

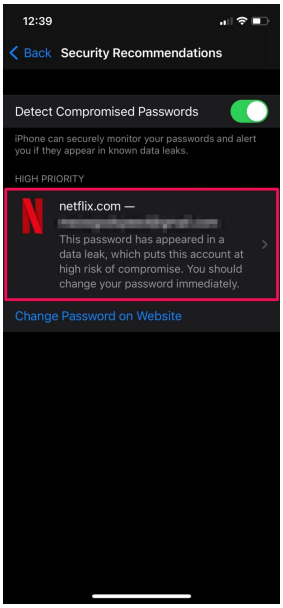


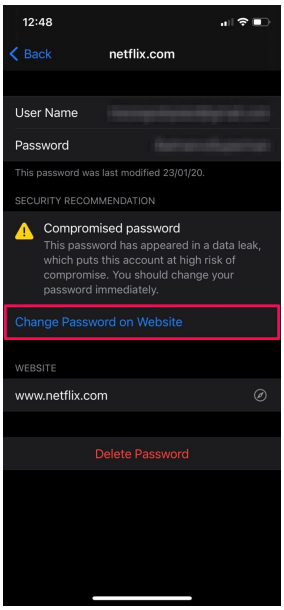


Als Nächstes werden Sie je nach Gerät aufgefordert, sich mit Face ID oder Touch ID zu authentifizieren, bevor Sie die iCloud-Schlüsselbunddaten einsehen können.

Tippen Sie dann hier auf "Sicherheitsempfehlungen", die sich direkt oberhalb der Liste der Passwörter befinden.

Wenn eines Ihrer Konten ein Passwort verwendet, das schwach oder leicht zu erraten ist oder in einem Datenleck auftauchte, wird es hier angezeigt. Tippen Sie auf das Konto, um weitere Details anzuzeigen.





Sie werden aufgefordert, das kompromittierte Passwort zu ändern. Tippen Sie auf "Passwort auf Website ändern", um damit fortzufahren.

Wenn Sie durch die Liste blättern, sehen Sie vielleicht einen Hinweis wie "Dieses Kennwort ist in einer Datenverletzung aufgetaucht, wodurch dieses Konto einem hohen Risiko der Kompromittierung ausgesetzt ist", und wenn das der Fall ist, ist das ein guter Indikator, um Kennwörter zu ändern, die mit diesem Konto verbunden sind oder anderswo wiederverwendet werden.

In der Annahme, dass Sie den Anweisungen gefolgt sind, haben Sie nun gelernt, wie Sie Sicherheitsempfehlungen in Bezug auf Ihre Online-Konten, die im iCloud-Schlüsselbund gespeichert sind, überprüfen können. Das war ziemlich einfach, oder?

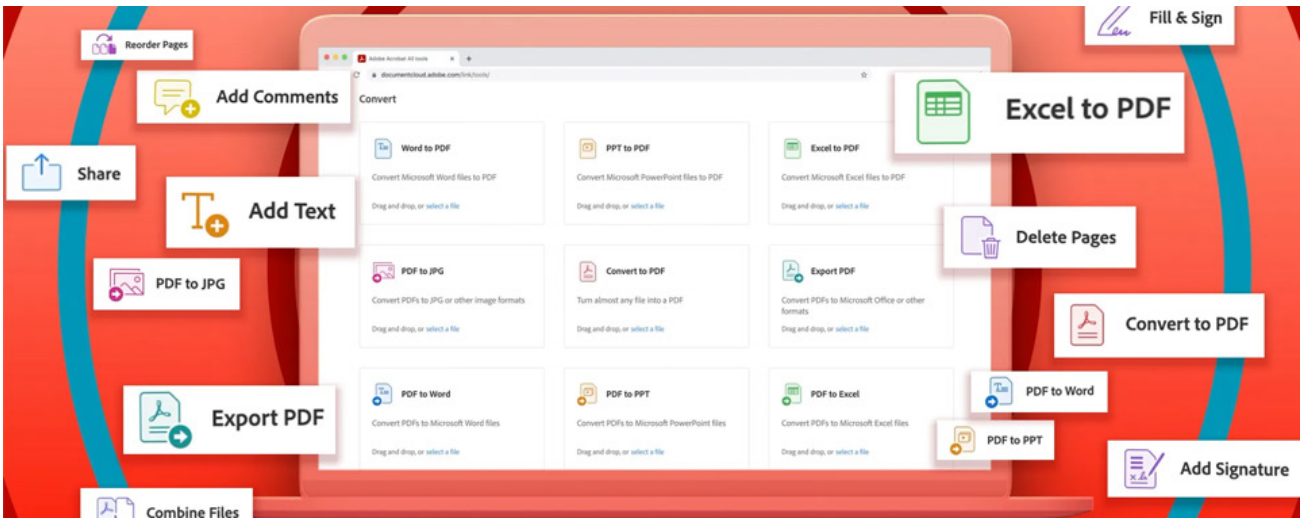
Dank dieser Funktion können Sie ganz einfach sicherstellen, dass keines der Passwörter, die Sie verwenden, schwach ist oder durch eine Datenverletzung gefährdet wurde. Dies hilft, Sicherheitsrisiken zu minimieren, die mit Online-Konten verbunden sind, besonders wenn Sie Passwörter zwischen Diensten teilen (was im Allgemeinen von Sicherheitsexperten nicht empfohlen wird, aber viele Benutzer tun es trotzdem aus Bequemlichkeit).

Wenn Sie sich fragen, wie diese Funktion funktioniert und welche Auswirkungen sie auf die Privatsphäre hat, so sagt Apple: "Safari verwendet starke kryptografische Techniken, um regelmäßig Ableitungen Ihrer Kennwörter mit einer Liste von verletzten Kennwörtern auf eine sichere und private Weise zu überprüfen, die Ihre Kennwortinformationen nicht preisgibt - auch nicht an Apple."

Vergessen Sie nicht, dass Sie Passwörter und Logins auch manuell zu Keychain auf iPhone und iPad hinzufügen können, wenn Sie möchten, dass sie von dieser Funktion überprüft werden.

Darüber hinaus hat Apple mit aktuellen iOS- und iPadOS-Versionen einige große Verbesserungen für die Privatsphäre vorgenommen. Dank Funktionen wie "Ungefährer Standort", "Beschränkter Zugriff auf Fotos", "Datenschutzbericht" und "Aufzeichnungsindikatoren" haben Nutzer nun die vollständige Kontrolle darüber, auf welche Daten Drittanbieter-Apps und Entwickler von ihren iPhones und iPads zugreifen können. Weitere datenschutzspezifische Tipps und Tricks finden Sie hier, wenn Sie das Thema interessiert.

Wir hoffen, Sie konnten die Sicherheitsempfehlungen nutzen, um schwache oder durchgesickerte Passwörter zu überprüfen und zu aktualisieren.

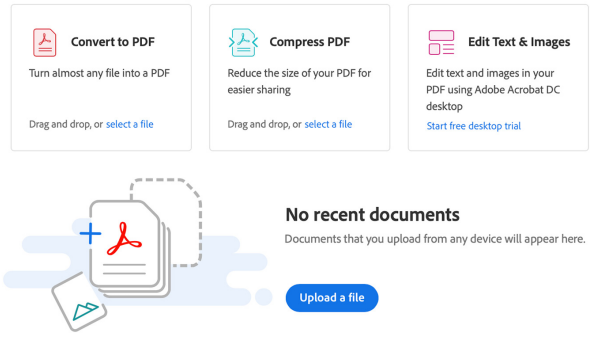


Adobe stellt Acrobat-Funktionen online bereit

Quelle: Chris (ifun.de)

Mit **Acrobat Web** bietet Adobe ausgewählte Funktionen seiner PDF-Bearbeitungssoftware kostenlos über ein Web-Interface an. Einzige Voraussetzung ist die Anmeldung mit einem kostenlosen Benutzerkonto, denn sonst sind die Möglichkeiten stark eingeschränkt und in der Regel auf eine Transaktion limitiert.

Wer sich mit einer Adobe ID angemeldet hat, kann Acrobat Web ohne Einschränkungen dazu verwenden, um PDFs auszufüllen, zu unterzeichnen oder um Kommentare zu ergänzen. Dateien können dafür einfach per Drag-and-Drop ins Browserfenster gezogen werden.



Über diese Basisfunktionen hinaus können angemeldete Nutzer die zusätzlich zur Verfügung stehenden Profi-Werkzeuge wie das Konvertieren oder Komprimieren von Dateien mit Einschränkungen verwenden, hier ist die Anwendung in der Regel auf eine Datei alle 24 Stunden begrenzt. Adobe-Nutzer mit einem Acrobat-DC-Abo haben uneingeschränkten Zugriff auf den gesamten Funktionsumfang.

Funktioniert das eingebettete Video nicht? Hier klicken.