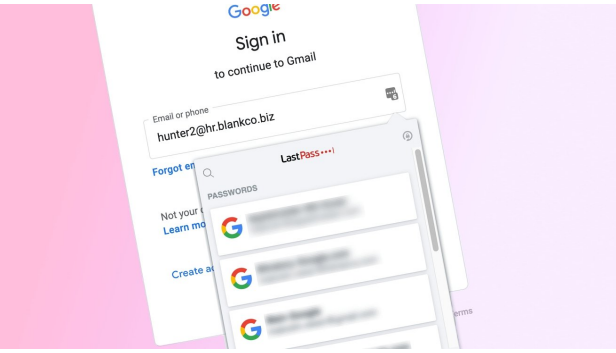
Schlüsselbund, LastPass, 1Password, Dashlane, Nordpass: Bewahren Sie Ihre Passwörter sicher auf

von Malcolm Owen, appleinsider.com ; Übersetzung KJM



Verwenden Sie nicht mehr dasselbe Passwort für alle Ihre Konten, sondern sichern Sie Ihr Online-Leben richtig ab, indem Sie einen Passwort-Manager verwenden. Hier finden Sie einige der besten für Ihren digitalen Schutz.

Praktisch alles, was Sie online tun, erfordert irgendeine Form von Konto und eine Kombination aus Benutzernamen und Passwort. Als grundlegendste Form der Authentifizierung werden Benutzername und Kennwort als Konzept sofort verstanden, können aber auch extrem unsicher und schwierig zu verwenden sein.

Dies gilt insbesondere dann, wenn eine Person Dutzende oder Hunderte von Konten hat, bei denen sie sich jederzeit anmelden können muss. Bei einer größeren Anzahl von Konten wird die Sicherheit zu einem größeren Problem.

Das größte Problem ist, wenn Benutzer versuchen, dasselbe Kennwort für mehrere Konten zu verwenden, damit sie sich nicht viele verschiedene Anmeldedaten merken müssen. Diese zeitsparende Idee ist auch sehr unsicher, da ein Angreifer, der die Kontodaten für einen Dienst oder eine App kennt, auf andere Konten zugreifen kann, die dieselben Informationen verwenden.

Die Lösung für dieses Problem besteht darin, für jedes Konto ein anderes Kennwort zu verwenden, was sofort verhindert, dass jemand die Daten eines Kontos für den Zugriff auf ein anderes verwendet. Dies führt jedoch zu einem weiteren Problem, da Sie sich plötzlich mehrere Kontopasswörter merken und merken müssen, anstatt nur eines zu verwenden.

Selbst wenn Sie sich nicht dafür entschieden haben, verschiedene Passwörter zu verwenden, könnten Sie durch Kontensysteme, die die Verwendung von Zahlen, Buchstaben, Groß- und Kleinbuchstaben, Sonderzeichen oder anderen Regeln vorschreiben, dazu gezwungen sein.

Dieses Problem könnte durch die Verwendung eines Textdokuments oder eines physischen Notizbuchs zum Aufschreiben der Kennwörter behoben werden, aber auch dies ist extrem unsicher.

Im Laufe der Jahre hat sich eine ganze Industrie entwickelt, um das Passwortproblem zu lösen. Passwort-Schließfächer oder Passwort-Manager bieten die Möglichkeit, eine große Anzahl von eindeutigen Passwörtern zu verwalten, so dass der Benutzer sich nur noch dasjenige merken muss, das er für den Zugang zu diesem Passwort-Schließfach verwendet.

Viele Dienste verfügen über Funktionen, die ihren Nutzern das Leben erleichtern, wie die Generierung von Passwörtern und die automatische Eingabe, die für ein sicheres Passwort sorgen, ohne dass der Nutzer es sich merken muss. Außerdem gibt es Funktionen wie Zwei-Faktor-Authentifizierungssysteme für zusätzliche Sicherheit.

Entscheidend ist jedoch, dass alle Manager die Kennwörter sicher online speichern können, so dass sie von jedem Gerät aus zugänglich sind und auch automatisch über verschiedene Plattformen hinweg aktualisiert werden können.

Natürlich bieten viele gängige Webbrowser integrierte Passwortverwaltungsfunktionen, was sinnvoll ist, da Sie sich damit wahrscheinlich bei Websites anmelden werden, aber das ist nicht unbedingt die beste Lösung. Oft haben Sie das Problem, dass Ihre Passwörter im Browser gespeichert und zwischen Geräten synchronisiert werden, auf denen der Browser ebenfalls installiert ist, aber Sie können diese gespeicherten Passwörter nicht einfach in anderen Browsern oder außerhalb von Browsern verwenden.

Im Folgenden finden Sie einige der großen Namen im Bereich der Kennwortsperren, ihre Angebote und die Kosten, die sie verursachen, damit Sie Ihre Konten sicher halten können.

Apples Schlüsselbund: Kostenlos und verfügbar

Die meisten Nutzer von Apple-Geräten kennen wahrscheinlich den Schlüsselbund als das Passwort-Schließfachsystem des Unternehmens. Jeder, der schon einmal ein iPhone, ein iPad oder einen Mac besessen hat, wird irgendwann einmal mit dem Schlüsselbund in Berührung gekommen sein.

Der Schlüsselbund wird verwendet, um Benutzernamen und Passwörter für Apps und Dienste zu verwalten, die dann auf dem Gerät gespeichert werden und später abrufbar sind. Dank Apples Voraussicht bei der Entwicklung von iOS ist diese Funktion am deutlichsten zu erkennen, wenn Sie mit Passworteingabe-Bildschirmen in einer App zu tun haben. iOS bietet Ihnen an, Daten aus dem Schlüsselbund automatisch einzugeben.

Der Schlüsselbund speichert nicht nur Passwörter, sondern kann auch für andere Daten wie Kreditkartennummern und PINs von Bankkonten verwendet werden. All diese Daten können von iOS angeboten werden, damit sie automatisch und so unauffällig wie möglich in Textfelder eingegeben werden.

Außerdem gibt es eine Synchronisierungskomponente, bei der iCloud Keychain automatisch Passwörter aus Apples iCloud an Ihr Gerät sendet und abruft. Alle Passwörter sind durch eine Ende-zu-Ende-Verschlüsselung geschützt, aber Apple hat den Dienst auch um die Möglichkeit erweitert, nach Passwortverletzungen zu suchen, Benutzer zu warnen, wenn sie Passwörter wiederholt in verschiedenen Konten verwenden, und sogar Zwei-Faktor-Authentifizierungsschlüssel einzubauen.

Als kostenloses Tool, das in iOS und macOS integriert ist und von einem der wohl datenschutzfreundlichsten großen Tech-Unternehmen der Welt unterstützt wird, ist dies etwas, was Nutzer vor anderen Alternativen ausprobieren sollten. Allerdings hat es auch seine Grenzen.

Der große Minuspunkt für den Schlüsselbund ist, dass er unglaublich Apple-zentriert ist. Angenommen, Sie arbeiten innerhalb des Apple-Ökosystems. In diesem Fall haben Sie kein Problem damit, den Schlüsselbund ständig zu verwenden, sogar um Anmeldedaten über die Einstellungen-App in iOS oder die Systemeinstellungen für macOS zu aktualisieren.

Das gilt aber nicht, wenn Sie dieselben Anmeldedaten auf verschiedenen Plattformen verwenden müssen. Unter Windows können Sie über eine Chrome-Erweiterung auf den iCloud-Schlüsselbund zugreifen, aber Plattformen wie Android haben das Nachsehen.

Wer auf mehreren Plattformen arbeitet, sollte vielleicht einen der vielen anderen Passwortmanager auf dem Markt ausprobieren.

LastPass: Einfach zu verwendender Schutz

Mit seinem rot-schwarzen Farbschema ist LastPass eines der bekanntesten Passwortmanagement-Tools. Das System speichert Anmeldeinformationen in seinem Passwort-Tresor, der mit Hilfe einer großen Auswahl an Apps und Browser-Erweiterungen zwischen Geräten synchronisiert wird.

Die Unterstützung ist umfangreich, einschließlich Apps für iOS und macOS zur Verwaltung des Tresors, Apps für Windows und Android, Erweiterungen für viele beliebte Browser und sogar einige für Linux. Das bedeutet, dass Sie Anmeldedaten auf jedem gängigen Gerät, das Sie verwenden möchten, hinzufügen, bearbeiten oder verwalten können.

Mit denselben Tools können Sie auch andere Informationen speichern, z. B. Wi-Fi-Passwörter, Kreditkartendetails und weitere Daten, die alle hinter einem einzigen Passwort stehen. Die Daten werden auf der Geräteebene gespeichert und entschlüsselt, ohne dass LastPass das Master-Passwort oder die Schlüssel für das Konto selbst erhält.

Im Dezember 2021 gab es jedoch Berichte, dass einige Nutzer feststellen mussten, dass ihre Master-Passwörter kompromittiert worden waren. LastPass behauptete, dass die Nutzer Warnungen über Zugriffsversuche auf Konten durch „Credential Stuffing“ und andere Techniken erhalten haben und dass es aufgrund der fehlenden Kenntnis des Master-Passworts des Nutzers nicht die Quelle der Lecks war.

Um den Nutzern noch mehr zu helfen, gibt es außerdem integrierte Kennwortgeneratoren, eine Überwachung von Datenschutzverletzungen im Dark Web, die die Nutzer betreffen könnten, und eine sichere Freigabe von Anmeldedaten für Familienmitglieder und Kollegen. All dies befindet sich in einem leicht zu navigierenden und benutzerfreundlichen System, das auf verschiedenen Plattformen sehr ähnlich funktioniert.

Der einzige Nachteil von LastPass ist, dass das kostenlose Angebot ein wenig unübersichtlich ist. Die kostenlose Version bietet die wichtigsten Vorteile des Dienstes, ist aber nur auf einen Gerätetyp beschränkt: Computer oder Mobiltelefon, wobei die Benutzer aufgefordert werden, für die Premium-Version zu zahlen, damit sie auf beiden Gerätetypen funktioniert.

Eine kostenlose 30-tägige Testversion von Premium ist ebenfalls verfügbar.

Der Premium-Service von LastPass kostet 3 US-Dollar pro Monat bei jährlicher Abrechnung, 4 US-Dollar pro Monat, wenn Sie sich für die Familien-Option entscheiden, die sechs Passwort-Tresore, ein Dashboard für Familienmanager und gemeinsam nutzbare Ordner umfasst. Es sind auch Business-Pläne verfügbar.

1Password: Ideal für Reisende

Der Name ist zweifelsohne ein Hinweis darauf, was 1Password seinen Nutzern bietet: Sichern Sie Ihre Konten mit eindeutigen Passwörtern, aber Sie müssen sich nur eines merken. Wenn 1Password aufgerufen wird, füllt es automatisch Anmeldebildschirme und Formulare auf Websites für den Benutzer aus und verwendet dabei dieselben Anmeldedaten auf allen seinen Geräten.

Der Dienst nutzt Apps auf vielen verschiedenen Plattformen und Browsererweiterungen, und es gibt sogar eine Befehlszeilenschnittstelle für diejenigen, die lieber im Terminal arbeiten.

Die macOS-Version der App wurde im Mai 2022 auf Version 8 aktualisiert, die ein neues Aussehen und überarbeitete Arbeitsabläufe mit sich bringt, um das Erlebnis für die Nutzer zu optimieren.

Alle Passwörter werden mit einer AES-256-Bit-Verschlüsselung auf den Servern des Unternehmens gespeichert, wobei ein Master-Passwort und ein geheimer Schlüssel für die Verschlüsselung verwendet, aber nicht an das Unternehmen selbst gesendet werden. Die Verwendung von Secure Remote Password hilft auch bei der Authentifizierung von Anmeldedaten, ohne dass diese überhaupt über das Internet gesendet werden.

Darüber hinaus gibt es Warnmeldungen bei Sicherheitsverletzungen, Phishing-Schutz und Dateneingabe nur dann, wenn der Benutzer die App dazu auffordert. Um zu verhindern, dass böswillige Akteure die Zwischenablage eines Geräts zum Kopieren von Daten missbrauchen, werden Informationen, die geheim bleiben sollen, in regelmäßigen Abständen aus dem temporären Datenspeicher entfernt.

Ungewöhnlicherweise gibt es auch einen Reisemodus, der beim Überschreiten von Grenzen in Situationen verwendet wird, in denen Beamte möglicherweise auf Ihre Hardware zugreifen möchten. Die in **1Password** gespeicherten sensiblen Daten werden gelöscht, können aber nach Verlassen des Sicherheitskontrollpunkts mit einem Klick wiederhergestellt werden.

Zu den weiteren Funktionen gehören die sichere Freigabe von Anmeldeinformationen, die Speicherung verschiedener Datenelemente, ein 365-Tage-Elementverlauf zum Wiederherstellen gelöschter Kennwörter und die Zwei-Faktor-Authentifizierung. Mit Version 8 für macOS wurde ein Schnellzugriffsbereich für den schnellen Zugriff auf Dienste und Passwörter sowie ein Watchtower-Tool zur Berechnung der Passwortstärke und zur Erkennung gefährdeter Passwörter durch geräteinterne Verarbeitung eingeführt.

Außerdem wurde Universal Autofill eingeführt, mit dem Sie Kontofelder von praktisch überall in macOS mit einer einfachen Tastenkombination ausfüllen können.

Nach einer 14-tägigen Testphase kostet das Einzelkonto von 1Password 2,99 US-Dollar pro Monat, die jährlich abgerechnet werden, und steigt auf 4,99 US-Dollar monatlich für die Familienversion. Dieser Plan funktioniert mit bis zu fünf Familienmitgliedern und bietet die gemeinsame Nutzung von Passwörtern und Kreditkarten, die Verwaltung der Daten, die jedes Familienmitglied nutzen kann, und die Möglichkeit, gesperrte Konten von Familienmitgliedern wiederherzustellen.

Ergänzung: Lizenz-Inhaber von 1Password 7 erhalten 50% Rabatt auf die ersten drei Jahre des 1Password8 - Abos.

Dashlane: Browserbasierte Sicherheit

Dashlane, ein langjähriges Mitglied des Passwortverwaltungsmarktes, bietet die gleichen Funktionen wie seine anderen Top-Konkurrenten. Dashlane speichert Passwörter, Zahlungsdaten und persönliche Informationen in seinem digitalen Schließfach, das in seinem Cloud-Speicherdienst aufbewahrt wird.

Darüber hinaus gibt es personalisierte Sicherheitswarnungen, einschließlich der Überwachung von bis zu fünf E-Mail-Adressen im Dark Web, eine Kennwortprüfung, um zu sehen, wie Sie schwache oder immer wiederkehrende Kennwörter verwenden, und einen Kennwortgenerator. Für den Fall, dass ein Passwort aktualisiert werden muss, weil es unsicher ist, gibt es einen automatischen Passwortwechsler, der diese Aufgabe für viele Websites übernehmen kann.

Neben Passwörtern und wichtigen Details gibt es eine Funktion für sichere Notizen, mit der Sie hochsensible Informationen in Dashlane speichern können, die Sie auch sicher mit anderen teilen können. Dashlane verwendet eine „patentierte US-Sicherheitsarchitektur mit Null-Wissen“, um sicherzustellen, dass nur die Benutzer Zugriff auf ihre Daten haben, und das ist etwas, von dem Dashlane behauptet, dass es „noch nie verletzt wurde“.

Um die Sicherheit zu erhöhen, enthalten die kostenpflichtigen Tarife auch ein VPN, das privates Surfen ermöglicht, wenn Nutzer einen öffentlichen Wi-Fi-Hotspot nutzen.

Dashlane unterscheidet sich von den anderen Anbietern durch die Abkehr von dedizierten Desktop-Apps zugunsten einer browserbasierten Schnittstelle. Mobile Apps und Browser-Erweiterungen sind nach wie vor verfügbar, aber der Wegfall der Desktop-Verwaltungs-Apps könnte für einige ein Problem darstellen.

Dashlane kostet 6,49 US-Dollar pro Monat bzw. 4,99 US-Dollar pro Monat bei jährlicher Abrechnung, wobei auch ein Familientarif für 8,99 US-Dollar pro Monat bzw. 7,49 US-Dollar pro Monat bei jährlicher Abrechnung erhältlich ist. Das Familienabonnement gilt für bis zu sechs Premium-Konten, mit Dark-Web-Überwachung für fünf E-Mail-Adressens pro Benutzer sowie allen anderen Vorteilen.

Es ist eine kostenlose Option verfügbar, die Speicherplatz für bis zu 50 Passwörter, Funktionen zur Überprüfung und Erstellung von Passwörtern sowie personalisierte Sicherheitswarnungen bietet. In der kostenlosen Version sind Elemente wie VPN, Überwachung des Dark Web und automatischer Passwortwechsler nicht enthalten, und sie kann auch nur auf einem Gerät verwendet werden.

Man könnte jedoch leicht argumentieren, dass der kostenlose Plan einen Vorgeschmack auf den Premium-Plan bietet und für Benutzer mit einfacheren Anforderungen an die Passwortverwaltung geeignet ist.

NordPass: Jünger, aber mit Stammbaum

NordPass, ein Schwesterdienst von NordVPN, ist ein neueres Angebot desselben Unternehmens. Wie die anderen bietet es eine sichere Möglichkeit, eindeutige Passwörter, Notizen, Kreditkarten und andere persönliche Informationen zu erstellen und aufzubewahren, die über die gesamte Gerätesammlung eines Benutzers synchronisiert werden können.

Ebenso gibt es eine große Auswahl an Apps und Browser-Erweiterungen, so dass es ohne große Schwierigkeiten auf mehreren Plattformen verwendet werden kann. Außerdem gibt es die üblichen Schutzfunktionen wie die Freigabe von Anmeldeinformationen, die Überwachung des Passwortstatus und die Überprüfung von Datenlecks auf Kontodetails.

Als neuestes Mitglied bietet **NordPass** jedoch auch einige Funktionen, die sich von den anderen Anbietern unterscheiden. So gibt es zwar die typische Freigabefunktion, aber der Notfallzugang ermöglicht Familienmitgliedern oder engen Freunden in bestimmten Situationen den Zugriff auf den Tresor des Benutzers.

Und dann ist da noch die Sicherheit: NordPass verwendet die XChaCha20-Verschlüsselung, einen neueren Verschlüsselungsalgorithmus, der als Ersatz für AES-256 gehandelt wird. NordPass wurde auch von Cure53, einem Unternehmen, das Penetrationstests durchführt, geprüft und erhielt einen ausgezeichneten Bericht.

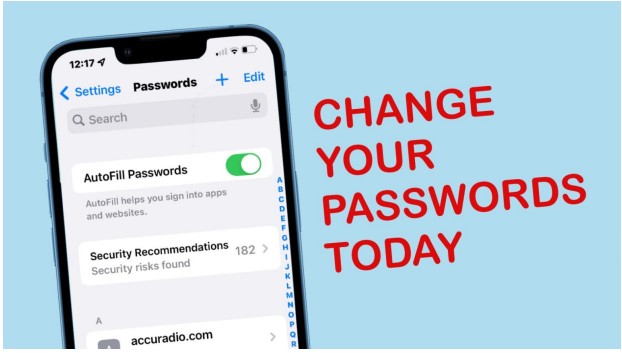
Die Multi-Faktor-Authentifizierung ist auch in NordPass vorhanden, obwohl Sie einen One-Time-Passwort-Generator, ein Bluetooth-Gerät oder einen USB-Stick hinzufügen können, um eine zusätzliche Token-basierte Sicherheitsebene zu einem Konto hinzuzufügen. Eine Funktion für vertrauenswürdige Kontakte ermöglicht es Benutzern, manuell zu bestätigen, dass sie eine verschlüsselte Verbindung mit einer anderen Person herstellen möchten, so dass die gemeinsame Nutzung von Passwörtern vor Man-in-the-Middle-Angriffen geschützt bleibt.

NordPass kostet 4,99 US-Dollar pro Monat für den Premium-Plan, 2,99 US-Dollar pro Monat bei jährlicher Abrechnung oder 2,49 US-Dollar pro Monat für den Zweijahresplan. Der Family Plan kostet 7,99 Dollar monatlich, 5,99 Dollar pro Monat für die Jahresversion und unterstützt bis zu sechs Benutzerkonten.

Eine kostenlose Version ist mit einer 30-tägigen Premium-Testversion erhältlich, die sich auf die Funktionen vertrauenswürdige Kontakte, Freigabe, Notfallzugriff, Kennwortschutz und Scannen von Datenlecks auswirkt.

Wie man von Hackern gestohlene Passwörter findet und ersetzt

von Ed Hardy, cultofmac.com ; Übersetzung KJM



Wenn Hacker die Passwörter stehlen, mit denen Sie sich auf Websites anmelden, kann Ihr Apple-Gerät Sie warnen und Ihnen helfen, sie zu ändern. Bild: Cult of Mac

Es ist gut möglich, dass die laxen Sicherheitsvorkehrungen eines Unternehmens bereits dazu geführt haben, dass Hacker Ihr Passwort für die Website des Unternehmens gestohlen haben. Und das könnte bei einer ganzen Reihe von Unternehmen passiert sein. Zum Glück können Sie mit Ihren Apple Geräten ganz einfach herausfinden, welche Ihrer Kennwörter an die Öffentlichkeit gelangt sind, damit Sie sie ändern können.

Heute, am 5. Mi 2022, ist Welt-Passwort-Tag. Nehmen Sie das zum Anlass, diese Probleme jetzt zu lösen.

Der iCloud-Schlüsselbund hilft, mit der Unmenge an Passwörtern umzugehen

Sie haben wahrscheinlich Hunderte von Websites und Programmen, die durch Kennwörter geschützt sind. Ich habe so viele, dass ich sie gar nicht mehr zählen kann — ich habe bei 100 aufgehört zu zählen, und ich war immer noch ganz oben auf der Liste.

Apple macht es Ihnen mit dem iCloud Schlüsselbund leicht, diese zu speichern und zu verwenden. Damit merkt sich Ihr iPhone, Mac usw. die Passwörter für Sie und fügt sie automatisch in Websites und Apps ein. Alles, was Sie tun müssen, ist Ihre Identität mit Face ID oder Touch ID zu verifizieren.

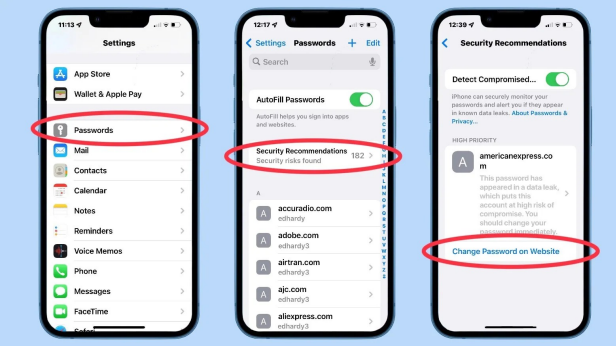
Das macht es leicht, sichere Passwörter zu verwenden und sie regelmäßig zu ändern, weil Sie sie sich nie merken müssen. Ihr Computer merkt sie sich für Sie.

Wenn Sie Ihre Passwörter nie ändern, besteht die Gefahr, dass ein Krimineller Ihr Passwort ausnutzt, um z. B. eine Reihe von Produkten bei Amazon zu kaufen. Oder einfach Ihre Bankkonten zu leeren.

Wie man unsichere Kennwörter findet

Ihr Apple-Gerät speichert sie nicht nur einfach, sondern warnt Sie auch, wenn Passwörter im iCloud-Schlüsselbund in ein Datenleck geraten sind. Welche das sind, lässt sich leicht herausfinden.

Diese Funktion ist auf iPhone, iPad und Mac verfügbar. In meinem Beispiel verwende ich das iPhone, aber die Funktion ist auch auf anderen Geräten verfügbar. Und Sie müssen den iCloud-Schlüsselbund verwenden, aber das ist etwas, was Apple Ihnen dringend empfiehlt, wenn Sie ein neues Gerät einrichten.



Gehen Sie in den Einstellungen zum Abschnitt "Passwörter", sehen Sie sich die Sicherheitsempfehlungen an und ändern Sie dann das Passwort auf der Website. Bild: Ed Hardy/Cult of Mac

Gehen Sie zu Einstellungen > Passwörter. Um diesen Bereich zu öffnen, müssen Sie natürlich Face ID oder Touch ID verwenden.

Suchen Sie nach dem Abschnitt Sicherheitsempfehlungen. Daneben steht wahrscheinlich eine Zahl. Sie gibt an, wie viele Sicherheitsprobleme Keychain in Ihrer Passwortliste gefunden hat. Sie werden feststellen, dass ich 182 habe - ich muss meinen eigenen Rat befolgen und einige Passwörter aktualisieren.

Tippen Sie auf Sicherheitsempfehlungen, um eine Liste der Websites und Anwendungen zu öffnen, bei denen Ihre Passwörter Probleme aufweisen. Für jedes Kennwort wird der Grund angegeben, wobei „dieses Kennwort wurde in einem Datenleck gefunden“ der häufigste Grund ist.

Sie haben die Möglichkeit, auf jede Website zu tippen, um eine ausführlichere Beschreibung der Sicherheitsprobleme zu erhalten. Dies kann auch eine Schelte für die Wiederverwendung von Passwörtern beinhalten.

Für jedes Passwort erhalten Sie die Möglichkeit, das Passwort auf der Website zu ändern.

Ein Beispiel für das Ändern eines Google-Passworts über iCloud Keychain

Um Ihnen ein Beispiel dafür zu geben, wie einfach dies ist, ändere ich das Kennwort für einen meiner Google-Accounts, wenn ich in den Einstellungen unter Kennwörter nachsehe.

Während ich mir die Liste der Sicherheitsempfehlungen ansehe, klicke ich auf „Kennwort auf Website ändern“, wodurch sich der Google-Anmeldebildschirm öffnet. Bevor ich das Kennwort ändern kann, muss ich mich natürlich bei dem Google-Konto anmelden. Das ist kein Problem, da der iCloud-Schlüsselbund den Benutzernamen und das aktuelle Passwort gespeichert hat.

Google möchte, dass ich die Zwei-Faktor-Authentifizierung durchführe und schickt mir einen Code. Ich gebe ihn ein und der Bildschirm zur Eingabe eines neuen Passworts öffnet sich.

Das einzige Problem bei diesem Vorgang ist, dass der Browser nicht weiß, dass ich ein neues Passwort erstellen möchte, und daher nicht automatisch ein starkes Passwort vorschlägt. Ich muss mir selbst eines ausdenken und es dann zweimal eingeben.

Keychain fragt dann, ob ich das neue Kennwort speichern soll. Ich sage, dass ich es speichern soll.

Und das war's dann. Das Verfahren ist bei anderen Websites sehr ähnlich. Sie können auch einfach den iCloud-Schlüsselbund als Warnung nehmen und zu Ihrem Lieblings-Webbrowser wechseln, die Website aufrufen und das Kennwort dort aktualisieren.

Tun Sie es einfach. Sie werden froh sein, dass Sie es getan haben.

Ich verstehe, dass das Ändern von Passwörtern ziemlich lästig ist. Schließlich bin ich der Typ mit den 182 Sicherheitswarnungen. Aber das ist es wert.

Jeder Tag, an dem Sie feststellen, dass jemand eines Ihrer durchgesickerten Passwörter verwendet hat, um Ihnen Geld zu stehlen, ist ein schlechter Tag. Das Ändern Ihrer Passwörter trägt viel dazu bei, dies zu verhindern.

Wie man macOS Monterey auf nicht unterstützten Macs installiert, um Sicherheitsverbesserungen zu erreichen

von Joshua Long, intego.com ; Übersetzung KJM

Aus Sicherheitssicht ist die Verwendung der neuesten Version von macOS, dem Mac-Betriebssystem, unerlässlich, insbesondere wenn Sie sich vor aktiv ausgenutzten Schwachstellen schützen möchten.

Wenn Ihr Mac jedoch mehrere Jahre alt ist, ist leider damit zu rechnen, dass die aktuelle Version von macOS nicht auf Ihrem Mac ausgeführt wird; Apple stellt die Unterstützung für Mac-Modelle ein, die es als vintage oder veraltet erklärt.

Wenn Sie die neueste Version von macOS verwenden möchten, Apple Ihren Mac aber nicht mehr unterstützt, ist die beste Option (in Bezug auf Geschwindigkeit, Systemstabilität und die gesamte Palette der Apple-Funktionen), einfach einen neuen Mac zu kaufen. Natürlich kann es sich nicht unbedingt jeder leisten, dies zu tun.

Aber was wäre, wenn es eine Möglichkeit gäbe, die neueste und sicherste Version von macOS viel länger auszuführen, als Apple bereit ist, Ihr Mac-Modell zu unterstützen?

Es gibt Hoffnung für ältere Macs

Es gibt in der Tat Hoffnung für die Benutzer vieler alter Mac-Modelle. Mit etwas Aufwand können Sie ein quellverfügbares Dienstprogramm eines Drittanbieters verwenden, das es Ihnen ermöglicht, die neueste macOS-Version auf deutlich älterer Hardware auszuführen, mit (meist) recht minimalen Vorbehalten.

Laut Apple sind dies die unterstützten Modelle für macOS Monterey (macOS 12.x):

MacBook (Anfang 2016 oder neuer)
MacBook Air (Anfang 2015 oder neuer)
MacBook Pro (Anfang 2015 oder neuer)
iMac (Ende 2015 oder neuer)
iMac Pro (2017)
Mac mini (Ende 2014 oder neuer)
Mac Pro (Ende 2013 oder neuer)
Mac Studio (2022)

Die Liste der Macs, auf denen macOS Monterey inoffiziell ausgeführt werden kann, sieht jedoch eher so aus:

MacBook (Anfang 2008 oder neuer)
MacBook Air (Ende 2008 oder neuer)
MacBook Pro (Anfang 2008 oder neuer)
iMac (Mitte 2007, nach dem Upgrade der CPU)*
iMac (Anfang 2008 oder neuer)
iMac Pro (2017)
Mac mini (Anfang 2009 oder neuer)
Mac Pro (Anfang 2008 oder neuer)
Mac Studio (2022)
Xserve (Anfang 2008 oder neuer)

*Mit einem Prozessor-Upgrade (nicht für schwache Nerven) kann die inoffizielle Liste sogar den iMac Mitte 2007 enthalten - einen Computer, der jetzt etwa 15 Jahre alt ist.

Josh Long (the JoshMeister)

@theJoshMeister

Older Macs deserve #security updates, too.

Over the weekend, I installed #macOS Monterey on my 15-year-old iMac, thanks to OpenCore Legacy Patcher. It works great!

(The chipset misidentifies my upgraded 2.6 GHz CPU as 700 MHz. Most ≥2008 Macs don't require new hardware!)

11:47 PM · Apr 19, 2022

Die inoffizielle Liste sieht beeindruckend aus, nicht wahr? Vielleicht scheint das zu gut, um wahr zu sein, und um fair zu sein, gibt es einige bekannte Probleme mit bestimmten Modellen (siehe Liste der von OpenCore Legacy Patcher unterstützten Modelle für Details).

Sie fragen sich vielleicht, wie so etwas überhaupt funktionieren kann. Teilweise verwendet es eine ähnliche Methodik wie sogenannte „Hackintosh"-Computer, bei denen zusätzliche Apple-Treiber aus früheren Versionen des Betriebssystems enthalten sind, damit die aktuelle Version von macOS mit einer breiteren Palette von Hardware funktioniert.

Apple möchte möglicherweise keine Anstrengungen unternehmen, um das neueste macOS auf Ihrer alten Mac-Hardware am Laufen zu halten. (Dies macht natürlich Sinn, besonders wenn man bedenkt, dass Apple mit dem Verkauf neuer Macs Geld verdient und nicht direkt von den kostenlosen macOS-Upgrades profitiert.) Aber zum Glück sind Bastler bereit, viele Stunden damit zu verbringen, um neue macOS-Versionen auf älteren Macs ohne Unterstützung von Apple funktionieren zu lassen.

Vorbereitung auf das Patchen

Wenn Sie macOS Monterey ausführen möchten, dies aber nicht können, da Ihr Mac nicht offiziell unterstützt wird, gehen Sie wie folgt vor:

1. Gehen Sie zuerst zu Ihrem Apple-Menü und wählen Sie „Über diesen Mac“. Schreiben Sie auf, was neben „Modell“ steht (wenn es aufgeführt ist). Klicken Sie dann auf „Systembericht..." (oder „Weitere Informationen...“). Im angezeigten Hardware-Übersichtsfenster wird ein „Model Identifier“ aufgeführt; notieren Sie sich diesen auch.
2. Nachdem Sie nun Ihr Mac-Modell identifiziert haben, müssen Sie als nächstes überprüfen, ob OpenCore Legacy Patcher mit Ihrem Mac funktioniert, indem Sie die Liste der unterstützten Modelle überprüfen.
3. Sichern Sie alle Ihre Daten. Verwenden Sie Apples Time Machine und/oder Intego Personal Backup, folgen Sie einer "3-2-1"-Backup-Strategie und stellen Sie sicher, dass Ihre Backups wirklich funktionieren.
4. Schnappen Sie sich ein USB-Flash-Laufwerk (oder eine andere externe USB/FireWire/Thunderbolt-Festplatte), die gelöscht werden kann und 16 GB oder größer ist. (Wählen Sie im Idealen ein schnelles externes Laufwerk. Dies spart Zeit, wenn Sie das macOS-Installationsprogramm auf das Laufwerk kopieren und Ihren Mac während der Installation davon booten.)
5. Laden Sie die neueste Version von OpenCore Legacy Patcher von dieser Website herunter. Achten Sie darauf, die „GUI-Offline“-Version zu wählen.
6. Wenn Sie normalerweise eine drahtlose Bluetooth-Tastatur und/oder -Maus verwenden, ist es besser, stattdessen eine kabelgebundene USB-Tastatur und -Maus für diesen Prozess zu verwenden. (Wenn Sie ein MacBook aktualisieren, sind die integrierte Tastatur und das Trackpad in den meisten Fällen in Ordnung.)

Nebenbei finden Sie viele der Schritte aus diesem Handbuch (und ein paar zusätzliche Details) auf der OpenCore Legacy Patcher-Website. Aber ich werde die Reise mit Ihnen mit meinem iMac (20", Mitte 2007, mit einer aktualisierten CPU) unternehmen und basierend auf meiner Erfahrung einige hilfreiche Tipps hinzufügen. Meins ist das älteste unterstützte (äh, nicht unterstützte) Modell, und es ist acht Jahre älter als das minimale iMac-Modell, das Apple noch unterstützt. (Beachten Sie, dass ich von einer gepatchten Version von Catalina aus aktualisiere, aber die folgenden Schritte sind — unabhängig davon — gleich. Der Screenshot unten stammt tatsächlich von einem anderen Mac mit OS X El Capitan 10.11.6, was zufällig die endgültige macOS-Version ist, die Apple auch auf meinem iMac unterstützt hat.)

Obwohl Hardware-Upgrades normalerweise nicht erforderlich sind, möchten Sie Ihren Mac möglicherweise auf die maximale Menge an RAM aktualisieren und Ihre Festplatte durch ein Solid-State-Laufwerk (SSD) ersetzen, vorausgesetzt, Ihr Mac-Modell ist benutzer-erweiterbar und Sie sind mit solchen Upgrades vertraut. Dadurch läuft Ihre Maschine viel reibungsloser.

Ich brauche nicht zu betonen, dass Intego keinen technischen Support leisten kann, wenn etwas schief geht. Machen Sie auf eigene Gefahr weiter.

Jetzt, da Sie alles bereit haben, fangen wir an!

So installieren Sie macOS Monterey auf einem eigentlich nicht unterstützten Mac

Nachdem Sie alle Ihre Vorbereitungsarbeiten aus dem vorherigen Abschnitt abgeschlossen haben, können Sie nun dieser Schritt-für-Schritt-Anleitung zur Installation von macOS Monterey auf Ihrem nicht unterstützten Mac folgen.

1. Schließen Sie Ihr USB-Flash-Laufwerk oder Ihre externe Festplatte an. (Sie werden dies für spätere Schritte benötigen.)

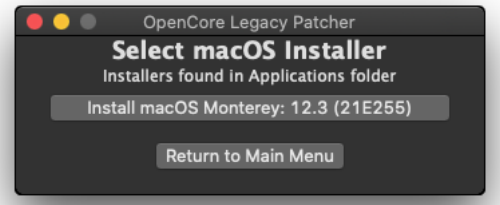
2.Öffnen Sie die App "OpenCore-Patcher" (die GUI-Offline-Version, die Sie in Schritt 5 Ihrer Vorbereitung heruntergeladen haben). Klicken Sie auf "Öffnen", wenn Sie dazu aufgefordert werden.

3. Klicken Sie im Hauptfenster der App auf die Schaltfläche „macOS-Installationsprogramm erstellen“.

4. Es erscheint ein neues Fenster, das viele macOS-Versionen auflistet. Klicken Sie auf die neueste Nicht-Beta-Version, die am Ende der Liste erscheinen sollte.

5. Die von Ihnen ausgewählte macOS-Version beginnt mit dem Herunterladen. Wenn der Download abgeschlossen ist, werden Sie möglicherweise aufgefordert, den Benutzernamen und das Passwort eines Administrators „to add InstallAssistant“ für den nächsten Schritt einzugeben (dies kopiert die App „macOS Monterey installieren“ in Ihren Anwendungsordner).

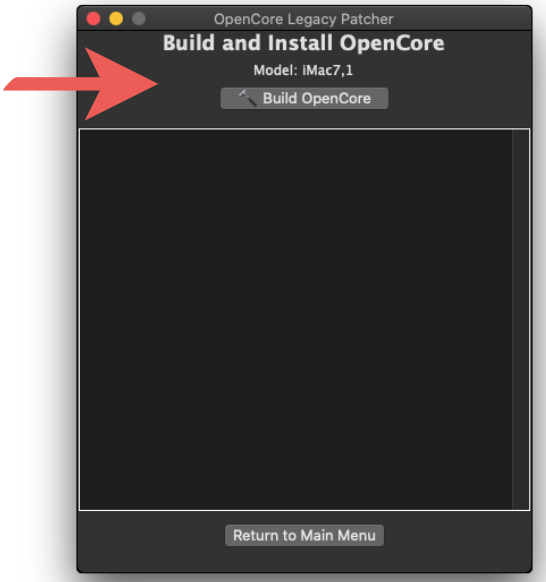
6. Klicken Sie anschließend auf die Schaltfläche „Flash Installer“. Sie werden dann aufgefordert, die App „macOS Monterey installieren“ auszuwählen, die Sie im vorherigen Schritt heruntergeladen haben. (Wenn Sie mehrere Optionen haben, wählen Sie die neueste Version von Monterey in der Liste.)



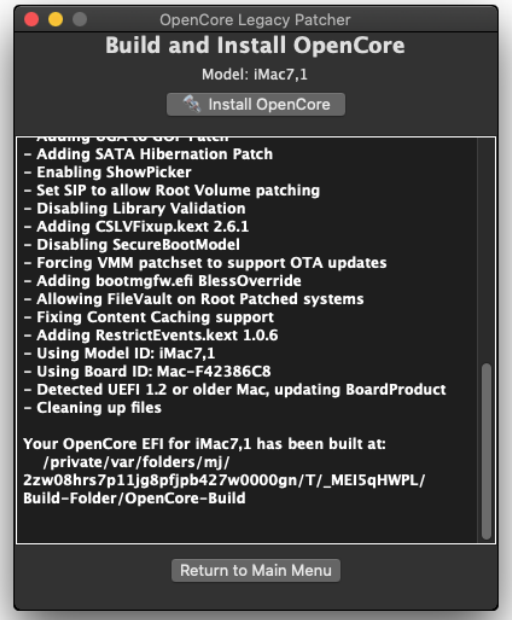
7. Sie werden dann aufgefordert, Ihr USB-Flash-Laufwerk oder Ihre externe Festplatte auszuwählen. (Wenn Sie mehrere Optionen zur Auswahl haben, wählen Sie sorgfältig aus; im nächsten Schritt wird das Laufwerk vollständig gelöscht.) Vielleicht möchten Sie die Festplattendetails aufschreiben; Sie müssen die gleiche Festplatte später erneut auswählen.

8. Auch hier werden Sie möglicherweise aufgefordert, den Benutzernamen und das Passwort eines Administrators einzugeben, da „OCLP-Helper Änderungen vornehmen möchte“ (OCLP ist die Abkürzung für OpenCore Legacy Patcher; dieser Schritt ermöglicht die Formatierung Ihres externen Laufwerks). Wie auf dem Bildschirm „Installationsprogramm erstellen“ erläutert, kann das Kopieren von Daten auf Ihr externes Laufwerk möglicherweise sehr lange dauern; dieser Schritt dauerte auf meinem iMac 2007 fast 90 Minuten.

9. Sobald dieser Vorgang abgeschlossen ist, erhalten Sie ein Dialogfeld „Erfolg“ und können dann auf die Schaltfläche „Zurück zum Hauptmenü“ klicken.
10. Klicken Sie im Fenster „Hauptmenü“ auf die Schaltfläche "OpenCore erstellen und installieren“. Ein neues Fenster wird angezeigt; klicken Sie auf die Schaltfläche „OpenCore erstellen“, um fortzufahren.

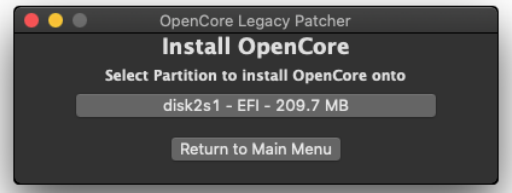


11. Sobald der Text aufhört zu scrollen, ändert sich die Schaltfläche „OpenCore erstellen“ in „OpenCore installieren“; klicken Sie auf „OpenCore installieren“.



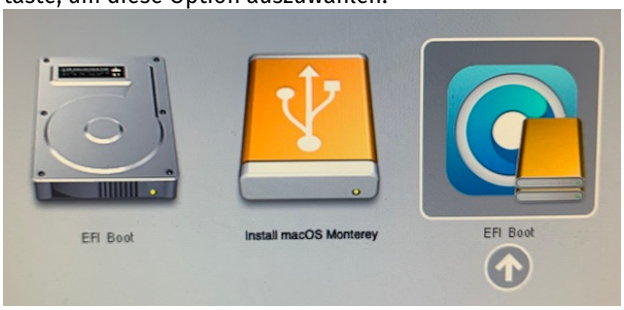
12. Klicken Sie im Fenster „OpenCore installieren“ auf die Schaltfläche für dieselbe Festplatte, die Sie in Schritt 7 oben ausgewählt haben (d.h. Ihr externes Laufwerk).

13. Als nächstes müssen Sie die Partition auswählen. Es sollte nur eine Schaltfläche in dieser Liste geben (in der Mitte wird wahrscheinlich „EFI“ stehen). Klicken Sie auf diese Schaltfläche, um fortzufahren.

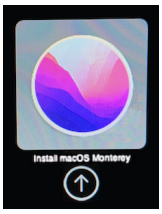


14. Auch hier werden Sie möglicherweise aufgefordert, den Benutzernamen und das Passwort eines Administrators einzugeben, da „OpenCore Legacy Patcher Administratorrechte benötigt, um Ihr EFI zu mounten“. Dies ist notwendig, um das externe Laufwerk für die nächsten Schritte vorzubereiten.
15. Augenblicke später sehen Sie ein wenig Text, der auf „OpenCore-Übertragung abgeschlossen“ endet. Ihr Mac ist jetzt bereit, macOS Monterey zu installieren.

16. Jetzt ist es an der Zeit, das neue Betriebssystem auf Ihrem Mac zu installieren! Lesen Sie diesen gesamten Schritt sorgfältig durch, bevor Sie fortfahren; Sie müssen bereit sein, schnell Tasten auf der Tastatur zu drücken.
    Klicken Sie auf das Apple-Menü, wählen Sie dann „Neu starten…“ und klicken Sie erneut auf Neustart, wenn Sie bereit sind. Halten Sie sofort die Wahltaste auf Ihrer Tastatur gedrückt (oder „Alt“, wenn Sie eine USB-Tastatur eines Drittanbieters verwenden). Sobald Sie mehrere Laufwerksoptionen sehen, halten Sie die Option/Alt-Taste gedrückt und wählen Sie mit den Pfeiltasten die Option „EFI Boot“ mit dem blau-weißen OpenCore-Logo. Drücken Sie die Eingabetaste oder die Eingabetaste, um diese Option auszuwählen.



    Als nächstes verwenden Sie die Pfeiltasten und die Eingabetaste, um die Option „macOS Monterey installieren“auszuwählen.

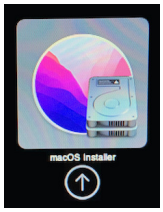


    Ihr Mac startet von der Installationsdiskette. Abhängig vom Alter und der Geschwindigkeit Ihres Mac und Ihres externen Laufwerks kann dies einige Minuten dauern.

17. Sobald Ihr Mac mit dem Booten fertig ist, sollten Sie die folgenden Optionen sehen: Wiederherstellen von Time Machine, Installieren von macOS Monterey, Safari und Festplattendienstprogramm.

    Wählen Sie „macOS Monterey installieren“ und lassen Sie das Installationsprogramm wie gewohnt laufen. Stellen Sie sicher, dass Sie in dem Bereich, in dem Sie aufgefordert werden, eine Festplatte auszuwählen, das interne Laufwerk Ihres Mac auswählen (z. B. „Macintosh HD“).

18. Nach einer Weile wird Ihr Mac wahrscheinlich von selbst neu starten. Wenn Sie zu dem in Schritt 17 gezeigten Bildschirm zurückkehren, klicken Sie einfach auf das Apple-Menü und wählen Sie Neu starten und halten Sie sofort die Option erneut gedrückt. Wählen Sie erneut „EFI Boot“, aber dieses Mal müssen Sie die Option „macOS Installer“ mit dem überlagerten internen Festplattensymbol (Bild unten) wählen. Auf diese Weise kann die Installation des Betriebssystems abgeschlossen werden.



19. Wenn die Installation von macOS Monterey abgeschlossen ist, bleiben nur noch ein paar Schritte übrig. Zuerst sollten Sie Ihr internes Laufwerk richtig einrichten, um sicherzustellen, dass Sie das angeschlossene externe Laufwerk nicht mehr benötigen. Öffnen Sie dazu die OpenCore-Patcher-App (die, die Sie in Schritt 2 verwendet haben). Wiederholen Sie im Hauptmenü (wie in Schritt 3 dargestellt) die Schritte 10 und 11 erneut, um OpenCore zu erstellen und mit der Installation zu beginnen.

20. Obwohl Sie in Schritt 12 Ihr externes Laufwerk ausgewählt haben, wählen Sie dieses Mal stattdessen Ihr internes Laufwerk aus (was höchstwahrscheinlich disk0 ist, aber je nach Mac variieren kann).

21. Wie Schritt 13 sollte es nur eine Option geben, die in der Mitte „EFI“ sagt; klicken Sie auf diese Schaltfläche.

22. Wie in Schritt 14 werden Sie aufgefordert, den Benutzernamen und das Passwort eines Administrators einzugeben, da „OpenCore Legacy Patcher Administratorrechte benötigt, um Ihr EFI zu mounten“. Dies ist not-

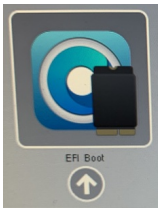
wendig, um das interne Laufwerk auf den Start vorzubereiten, ohne dass das externe Laufwerk angeschlossen ist.

23. Sobald Sie ein Fenster ähnlich wie Schritt 15 sehen, sehen Sie wieder ein bisschen Text, der mit „OpenCore-Übertragung abgeschlossen“ endet. Klicken Sie auf „Zurück zum Hauptmenü“, um sich auf den nächsten Schritt vorzubereiten.

24. Klicken Sie im Hauptmenü auf die Schaltfläche „Post Install Root Patch“. (Dies wird Ihnen helfen, alle zusätzlichen Korrekturen zu installieren, die möglicherweise erforderlich sind, damit Monterey mit der Legacy-Hardware Ihres Mac funktioniert.) Klicken Sie dann auf die Schaltfläche „Root Patching starten“.

25. Wenn Sie die Eingabeaufforderung „Relaunch als Root?“ erhalten, klicken Sie auf „Ja“. Auch hier werden Sie aufgefordert, den Benutzernamen und das Passwort eines Administrators einzugeben, da „OpenCore Legacy Patcher Administratorrechte benötigt, um als Administrator neu gestartet zu werden“. Die App wird im Hauptmenü neu gestartet, an diesem Punkt sollten Sie Schritt 24 wiederholen. Fahren Sie dann mit Schritt 26 fort.

26. Sobald es heißt: „Patching abgeschlossen“, sehen Sie auch die Meldung: „Bitte starten Sie den Computer neu, damit Patches wirksam werden“. Ziehen Sie vor dem Neustart Ihre externe (z.B. USB) Laufwerkssymbol vom Desktop in den Papierkorb, um es auszuwerfen, und trennen Sie dann physisch das externe Laufwerk von Ihrem Mac. Klicken Sie dann auf das Apple-Menü, klicken Sie auf „Neu starten...“ und klicken Sie dann auf Neustart. Halten Sie die Option/Alt noch einmal gedrückt und wählen Sie die EFI-Startoption des internen Laufwerks aus.



Sie sind fertig! Auf Ihrem von Apple nicht unterstützten Mac läuft jetzt macOS Monterey!

Installieren von macOS-Updates (kleine und große)

Wenn es das nächste Mal ein kleineres macOS-Update gibt, d.h. eine neue Version von Monterey, ist Folgendes zu tun, um sicherzustellen, dass alles reibungslos läuft:

1. Sichern Sie wichtige Dateien von Ihrem Computer. (Siehe Schritt 3 im Abschnitt „Vorbereitung auf das Patchen“ dieses Artikels für Tipps.) Sie sollten dies trotzdem tun, unabhängig davon, ob Sie einen Mac verwenden, der unterstützt wird oder nicht.
2. Führen Sie die OpenCore-Patcher-App aus, um nach Updates zu suchen. Wenn es Sie darüber informiert, dass ein Update verfügbar ist, laden Sie die GUI-Offline-Version herunter.
3. Sie sollten nun in der Lage sein, das macOS Monterey-Update wie gewohnt zu installieren (über das Menü Apple-> Systemeinstellungen... > Software-Update).
4. Nach dem Neustart von macOS müssen Sie den Root Patch nach der Installation (Schritte 24 und 25 oben) neu installieren und dann Ihren Mac erneut starten.

Bevor Sie ein Upgrade auf eine wichtige neue macOS-Version in Betracht ziehen (z. B. macOS 13, die wahrscheinlich am 6. Juni 2022 angekündigt und im Herbst 2022 veröffentlicht wird), müssen Sie zuerst warten, bis OCLP kompatibel ist. Höchstwahrscheinlich ist ein Update auf OCLP erforderlich, bevor Sie sicher auf die nächste Hauptversion von macOS aktualisieren können.

Wenn die Installation erfolgreich war und Sie begeistert sind, das neueste Betriebssystem auf Ihrer alten Mac-Hardware ausführen zu können, sollten Sie erwägen, Hardware an die OpenCore Legacy Patcher-Entwickler zu spenden, um ihnen zu helfen, Updates schneller auf einer größeren Auswahl älterer Macs zu testen.

Zusätzliche Tipps

Nun, da Sie macOS Monterey auf einem nicht unterstützten Mac-Modell verwenden, sind hier ein paar weitere Dinge, die Sie vielleicht wissen möchten:

- Sichern Sie Ihre wichtigen Dateien oft. Sie führen macOS nicht nur ohne Unterstützung aus, sondern Ihre Hardware ist auch ziemlich alt, so dass ein erhöhtes Risiko von Datenverlust besteht. Um Ihre Dokumente sicher aufzubewahren, können Sie Apples Time Machine und/oder Intego Personal Backup verwenden, eine "3-2-1"-Backup-Strategie verwenden und sicherstellen, dass Ihre Backups wirklich funktionieren.
- Halten Sie das externe Laufwerk griffbereit, das Sie für die Installation von Monterey verwendet haben. Sie benötigen es für die Installation zukünftiger wichtiger macOS-Updates wie macOS 13 (vorausgesetzt natürlich, dass Ihr Mac — inoffiziell — damit kompatibel ist).
- Eine weitere Möglichkeit, sich über OpenCore Legacy Patcher-Software-Updates auf dem Laufenden zu halten, besteht darin, Mr. Macintosh auf YouTube zu folgen. Er veröffentlicht ein Video für jedes neue OCLP-Update und macOS-Update. Wenn Sie also Bedenken bezüglich des Prozesses haben oder sicher sein möchten, dass es vor dem Update keine "Gotchas" gibt, ist dies eine gute Möglichkeit, sich auf dem Laufenden zu halten.

Willkommen in der Legacy-Patching-Community!

Herzlichen Glückwunsch! Ihr älterer Mac kann nun mit den neuesten Sicherheitsupdates Schritt halten. Obwohl Firmware-Updates nicht enthalten sind (diese sind modellspezifisch und Apple veröffentlicht sie nur für unterstützte Macs), ist Ihr macOS dennoch viel sicherer als mit der alten Version von Mac OS X, die Sie zuvor ausgeführt haben.

Jedes Mal, wenn ein neues macOS veröffentlicht wird, freue ich mich auf den nächsten macOS Patcher, da er unsere geliebten — und immer noch mehr als leistungsfähigen — alten Macs nun eine Weile länger einsatzfähig hält.

Über Joshua Long

Joshua Long (@theJoshMeister), Chief Security Analyst der Firma Intego, ist ein renommierter Sicherheitsforscher, Schriftsteller und öffentlicher Redner. Josh hat einen Master-Abschluss in IT mit dem Konzentration auf Internetsicherheit und hat Doktorarbeiten in Informationssicherheit absolviert. Apple hat Josh öffentlich dafür anerkannt, dass er eine Apple-ID-Authentifizierungsschwachstelle entdeckt hat. Josh betreibt seit mehr als 20 Jahren Cybersicherheitsforschung, die oft von großen Nachrichtenagenturen weltweit vorgestellt wurde. Suchen Sie nach weiteren Artikeln von Josh unter security.thejoshmeister.com und folgen Sie ihm auf Twitter.

Alle Beiträge von Joshua Long anzeigen →