Berichte über Data Breaches häufen sich. Das ist besonders peinlich, wenn in Server von Passwort-Programmen eingebrochen wurde. Da wundert es nicht, dass viele User die Sicherheit der Passwort-Onlinespeicherung grundsätzlich bezweifeln.

Zwei Artikel aus dem 1Password-Blog erklären, wie 1Password Ihre sensiblen Daten schützt und warum ein Angriff auf 1Password keine Bedrohung für die in Ihren Tresoren gespeicherten Informationen darstellen würde.

Wie 1Password Ihre Daten schützt, selbst im Falle eines Angriffs

von Pedro Canahuati, blog.1password.com • Übersetzung: KJM

Da Datenschutzverletzungen immer häufiger vorkommen und beängstigende Schlagzeilen in den Nachrichten erscheinen, fühlen Sie sich vielleicht etwas unwohl. Hier die gute Nachricht: Wenn Sie Nutzer von 1Password sind, müssen Sie nichts tun und haben keinen Grund zur Sorge.

Wir werden weiter unten erklären, warum, aber wenn Sie es eilig haben, können Sie sich hiermit beruhigen:

- Wenn Sie 1Password verwenden, sind Ihre Informationen sicher. 1Password verschlüsselt Ihre Tresordaten auf eine grundlegend andere Weise als andere Passwortmanager. Unsere Dual-Key-Verschlüsselung stellt sicher, dass ein Einbruch in die Systeme von 1Password keine Bedrohung für die in Ihren Tresoren gespeicherten sensiblen Informationen darstellen würde.
- 1Password verschlüsselt wichtige Metadaten, um Ihre Privatsphäre zu schützen. Zusätzlich zu den Inhalten Ihrer Tresore verschlüsseln wir auch die Namen der Tresore und die gespeicherten Website-URLs. Ohne sie hätte jemand, der Ihre verschlüsselten Tresordaten abruft, keine Möglichkeit zu erraten, was sich darin befindet — er wüsste nicht, ob er einen Tresor mit Kreditkarten oder Cookie-Rezepten knacken würde.
- Sie brauchen uns nicht beim Wort zu nehmen. Wir investieren viel, um gute Bürger der Sicherheitsgemeinschaft zu sein, ziehen externe Forscher für regelmäßige Überprüfungen heran und bieten das branchenweit größte Bug Bounty an, um Schwachstellen zu entdecken und zu beheben, bevor sie Sie betreffen können.

Lesen Sie weiter, um zu erfahren, wie wir 1Password so entwickelt haben, dass Ihre Tresordaten für Angreifer praktisch unbrauchbar sind, selbst wenn sie sie irgendwie in die Hände bekämen.

Was würde ein Einbruch in 1Password für Ihre Passwörter bedeuten?

Bei 1Password gab es noch nie einen Einbruch. Sollte es aber einmal dazu kommen, würde eine Verletzung unserer Systeme Ihre sensiblen persönlichen Tresordaten nicht in Gefahr bringen.

Als wir die Sicherheitsarchitektur von 1Password entwickelt haben, mussten wir die Möglichkeit in Betracht ziehen, dass unsere Server eines Tages kompromittiert werden könnten. Wenn gut ausgerüstete, entschlossene Angreifer es auf Passwortmanager abgesehen haben, tun sie das, weil sie glauben, dass der Preis den Aufwand wert ist. Warum sollte man die Daten einer einzelnen Person kompromittieren, wenn man potenziell Millionen von Kopfgeldern kassieren kann?

1Password ist so aufgebaut, dass, wenn Angreifer in unsere Systeme eindringen, alle Tresordaten, die sie erlangen, für sie praktisch nutzlos wären, selbst wenn sie alle Rechenleistung der Welt zur Verfügung hätten, um zu versuchen, sie zu knacken.

Wie ist das möglich? 

Was macht 1Password anders?

Ein Passwort-Manager ist wie ein Bankschließfach: ein sicheres Behältnis, in dem Dinge aufbewahrt werden, das in einer befestigten Bank außerhalb des Unternehmens aufbewahrt und mit einem Schlüssel (dem Passwort Ihres Kontos) verschlossen wird.

Wenn sich jemand Zugang zu dieser Bank verschafft, kann er das Fach stehlen und versuchen, das Schloss zu knacken. Dann ist es nur noch eine Frage der Zeit, bis sie das Passwort knacken … und oft ist das viel schneller, als wir denken.

Deshalb ist bei 1Password eine Kombination aus zwei Schlüsseln erforderlich, um Ihr Schließfach zu öffnen, die 1Password niemals zu Gesicht bekommt (geschweige denn besitzt).

1. Der erste Schlüssel ist Ihr Kontopasswort — das ist das Passwort, das Sie wählen und das einzige, das Sie sich merken müssen, um Zugang zu Ihrem Tresor zu erhalten.
2. Der zweite Schlüssel, der nur bei 1Password vorhanden ist, wird als Secret Key (Geheimschlüssel) bezeichnet. Es ist ein maschinell erzeugter 128-Bit-Code, der mathematisch nicht zu knacken ist.

Andere Passwortmanager verlassen sich nur auf den ersten Schlüssel, um Ihre Daten zu schützen. Das Problem ist, dass diese Schlüssel oft viel leichter zu erraten sind, weil man sie sich merken können muss. 1Password fügt den nicht zu erratenden geheimen Schlüssel hinzu, um die Verschlüsselung zu verstärken und sicherzustellen, dass es keine praktische Möglichkeit gibt, Ihre Tresordaten zu knacken.

Im täglichen Gebrauch müssen Sie nicht über den geheimen Schlüssel nachdenken, da die 1Password-Apps dies für Sie übernehmen. So erhalten Sie alle Sicherheitsvorteile der Zwei-Schlüssel-Verschlüsselung und behalten gleichzeitig den Komfort eines einzigen Passworts, das Sie sich merken müssen, um Ihre Tresore zu entsperren.

Wenn Kriminelle jemals eine Kopie Ihrer Tresordaten erlangen würden, bräuchten sie sowohl das Kontopasswort (das nur Sie kennen) als auch den geheimen Schlüssel (den nur Sie haben), um sie zu kombinieren und Ihre Daten zu entsperren. Ohne beide Schlüssel ist es praktisch unmöglich, Ihre Daten zu entschlüsseln. Der Versuch, das kombinierte Verschlüsselungsschema dieses Dual-Key-Ansatzes zu knacken — selbst unter Verwendung aller heutigen Computer auf der Erde - würde konservativ betrachtet ein Mehrfaches des bekannten Alters des Universums erfordern.

Ein Overkill? Das glauben wir nicht. Es ist das Mindeste, was wir tun können, um unser Versprechen zu erfüllen, dass Ihre Daten niemals in die falschen Hände geraten.

Bleiben Sie skeptisch!

Wir sind davon überzeugt, dass unser Sicherheitsmodell den besten Schutz bietet, den Sie bekommen können, aber wir möchten, dass Sie sich genauso sicher fühlen.

Deshalb veröffentlichen wir ein detailliertes Sicherheits-Whitepaper (Download), das einen ausführlichen Blick auf unseren Ansatz wirft, einschließlich zusätzlicher Aspekte, die einzigartig für 1Password sind, wie das Secure Remote Password (SRP) Protokoll.

Aber selbst das ist noch nicht genug. Die Dinge ändern sich in der Sicherheitsbranche schnell, und deshalb investieren wir ständig in unsere Bemühungen, dem Spiel immer einen Schritt voraus zu sein. Je mehr wir unsere Arbeitsweise hinterfragen und verbessern können, desto mehr Transparenz und Sicherheit können wir Ihnen bieten, wenn Sie Ihre Optionen abwägen.

So haben wir zum Beispiel kürzlich die Prämien für Sicherheitsforscher erhöht. Diese externen Experten helfen uns, potenzielle Schwachstellen in unseren Systemen zu erkennen, damit wir sie beheben können, bevor sie sich auf die Kunden auswirken.

Unser mit 1 Million Dollar dotiertes Bug-Bounty-Programm ist inzwischen das größte im Bereich der Passwort-Manager. Zusammen mit anderen laufenden Bemühungen wie unserem Sicherheits-Audit-Programm von Drittanbietern sorgt es dafür, dass Sie immer über vertrauenswürdige, aktuelle Informationen verfügen, die Sie zur Bewertung unserer Ansprüche nutzen können.

Mit anderen Worten: Wenn wir sagen, dass wir Ihre Daten schützen, müssen Sie sich nicht auf unser Wort verlassen.

Sind Sie bereit, loszulegen?

Letztendlich muss man sich Vertrauen verdienen. Wir könnten Sie bitten, uns einfach zu vertrauen, aber das tun wir nicht.

Wir möchten, dass Sie skeptisch bleiben, und wir freuen uns, wenn Sie uns die schwierigen Fragen stellen, wie alles funktioniert. Unser Team ist immer bereit, Ihnen zu helfen.

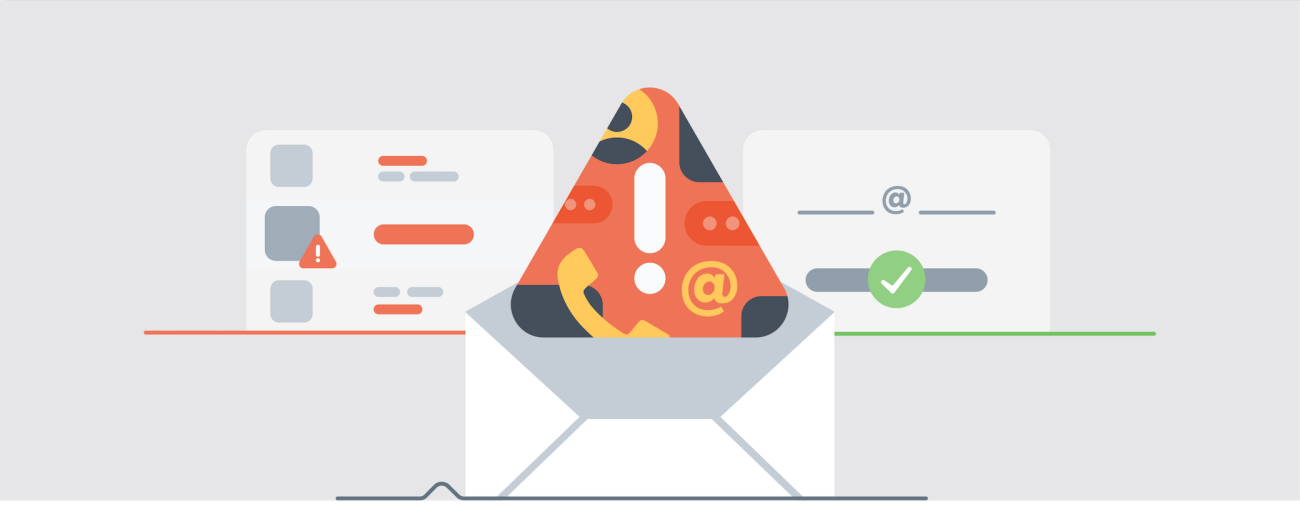
Was auch immer Sie tun, geben Sie sich nicht mit „gut genug“ zufrieden — wir tun das ganz sicher nicht. Denn wenn es um den Schutz Ihrer wertvollsten Informationen geht, ist „gut genug“ nicht gut genug.

Sind Sie bereit, 1Password auszuprobieren?

Melden Sie sich noch heute bei 1Password an und Sie erhalten die ersten 14 Tage kostenlos. Los geht's.

Braucht Ihr Unternehmen Hilfe bei der Umstellung?

Unsere Einführungs- und Kundenerfolgsteams stehen bereit, um Ihnen zu helfen, schnell zu reagieren und Ihre Mitarbeiter zu schützen. Sprechen Sie mit uns.



Die Daten, die Sie in 1Password speichern, werden durch mehrere Schutzschichten geschützt, aber reicht das aus, um Cyberangriffe wie das Ausfüllen von Anmeldeinformationen abzuwehren?

Wie 1Password Ihre Kontodaten vor Cyberangriffen schützt

von Marius Masalar, blog.1password.com • Übers.: KJM

Kaum etwas ist beängstigender, als eine E-Mail zu erhalten, in der jemand versucht, sich in eines Ihrer Konten einzuloggen. Das gilt umso mehr, wenn es sich dabei um das Konto Ihres Passwortmanagers handelt.

Die gute Nachricht ist, dass Sie durch das Verwenden von 1Password bereits gegen die häufigste Art von Cyberangriffen geschützt sind, der diese E-Mails auslöst: Credential Stuffing.

Was genau ist Credential Stuffing?

Bei modernen Cyberangriffen wird nur selten tatsächlich gehackt. Es ist einfacher und effektiver geworden, einfach Anmeldedaten zu verwenden, die bei Datenverletzungen gestohlen wurden, ohne Zeit damit zu verschwenden, einzelne Passwörter zu knacken. Hacker verwenden spezielle Software, um mit diesen gestohlenen Anmeldedaten massenhaft Anmeldeversuche bei beliebten Webdiensten zu unternehmen. Diese Art des Angriffs wird als *Credential Stuffing* bezeichnet.

Inzwischen haben wir alle gelernt, dass Datenschutzverletzungen im Internet zum Alltag gehören. Im Jahr 2021 waren sie im Vergleich zu 2020 um mindestens 17 % häufiger, was bedeutet, dass viel mehr gestohlene oder durchgesickerte Anmeldeinformationen zur Verfügung stehen, die böswillige Akteure für ihre Versuche nutzen können.

Die Angreifer machen sich die Tatsache zunutze, dass viele Menschen ihre Passwörter für mehrere Konten wiederverwenden. Wenn ein Kennwort von einem relativ unwichtigen Konto — z.B. von Ihrer Lieblingsseite für den Austausch von Katzenfotos — durch einen Datendurchbruch in die Hände von Angreifern gelangt, können diese versuchen, dieselbe Kombination aus Benutzername und Kennwort für den Zugriff auf Ihre Konten in sozialen Medien, Ihre Arbeitssoftware und sogar Ihr Online-Banking zu verwenden.

Möchten Sie online sicher bleiben? Erstellen Sie einen einzigartigen Benutzernamen mit dem kostenlosen Benutzernamen-Generator von 1Password!

Im Allgemeinen sind Angriffe zum Ausfüllen von Anmeldeinformationen wie Spam-E-Mails: Sie werden in großem Umfang durchgeführt, führen aber selten zu Ergebnissen. Einigen Schätzungen zufolge führt Credential Stuffing nur in 2 % der Fälle zu einem erfolgreichen Kontozugriff. Aber wenn man bedenkt, dass eine einzige Datenpanne 1 Million Benutzer-Anmeldedaten enthalten kann, bedeutet das immer noch 20.000 gefährdete Konten.

Wie 1Password Ihre Daten schützt

Ein erfolgreicher Angriff zum Ausfüllen von Anmeldeinformationen beruht auf zwei Dingen:

1. Zugang zu gestohlenen oder durchgesickerten Anmeldeinformationen aus einer Datenschutzverletzung
2. Die Wiederverwendung von Passwörtern auf mehreren Websites

Als Einzelpersonen können wir nicht viel tun, um zu verhindern, dass unsere Anmeldeinformationen durchsickern oder gestohlen werden, wenn ein von uns genutzter Dienst von einer Datenschutzverletzung betroffen ist.

Glücklicherweise können wir den zweiten Punkt leicht angehen, indem wir 1Password verwenden, um starke, eindeutige Passwörter für jedes von uns verwendete Konto zu erstellen. Selbst wenn ein Angreifer mit gestohlenen Zugangsdaten auf ein Konto zugreift, kann er dasselbe Kennwort nicht verwenden, um auf andere Konten zuzugreifen — weil Sie es nur an einer Stelle verwendet haben.

Natürlich bleibt immer noch die Frage nach Ihrem 1Password-Konto selbst: Was passiert, wenn jemand Ihr Kontopasswort errät oder erhält? Das Sicherheitsmodell von 1Password ist so konzipiert, dass es sich nicht auf einen einzigen Fehlerpunkt stützt, daher lautet die kurze Antwort: nichts.

Und so funktioniert es.

Drei Dinge sind erforderlich, um Ihre Daten zu entschlüsseln:

1. Ihr Kontopasswort (der Künstler, der früher als „Master Password“ bekannt war)
2. Ein zusätzlicher Verschlüsselungsbestandteil, der so genannte geheime Schlüssel
3. Die verschlüsselten Tresordaten selbst

Nur Sie kennen Ihr Kontopasswort, und Ihr geheimer Schlüssel wird bei der Einrichtung lokal generiert. Die beiden werden auf Ihrem Gerät kombiniert, um Ihre Tresordaten zu verschlüsseln, und werden nie an 1Password gesendet.

Nur die verschlüsselten Tresordaten befinden sich auf unseren Servern, sodass weder 1Password noch ein Angreifer, der Ihr Kontopasswort errät oder stiehlt, auf Ihre Tresordaten zugreifen kann.

Wenn Sie sich bei Ihrem 1Password-Konto anmelden, werden Ihre Informationen zusätzlich durch ein einzigartiges Kommunikationssystem geschützt, das sicherstellt, dass weder Ihr Kontopasswort noch Ihr geheimer Schlüssel jemals über das Netzwerk gesendet werden.

Der Industriestandard Transport Layer Security (TLS) bietet eine erste Verteidigungslinie, aber wir haben sie mit einem benutzerdefinierten Protokoll, bekannt als Secure Remote Password (SRP), verstärkt. Mit SRP schützt ein weiterer, auf dem Gerät generierter Verschlüsselungsschlüssel Ihre Daten bei der Übertragung, selbst wenn es jemandem gelingt, TLS zu entschlüsseln.

Außerdem ist dieser Verschlüsselungsschlüssel für jede Sitzung unterschiedlich, sodass ein Angreifer, dem es gelingt, eine Authentifizierungssitzung aufzuzeichnen, diese Informationen nicht für einen Einbruchsversuch verwenden kann.

SRP beweist dem Server auch, dass die 1Password-App ein Geheimnis hat, das nur mit dem richtigen Kontopasswort und dem geheimen Schlüssel abgeleitet werden kann. Ebenso beweist es der 1Password-App, dass der Server den richtigen Verifizierer hat, was garantiert, dass die Verbindung mit dem echten 1Password-Server besteht und nicht mit einem Betrüger.

Indem Sie 1Password verwenden, gehen Sie bereits über die Grenzen hinaus, um sich zu schützen.

Was kann ich sonst noch tun?

Seien Sie proaktiv in Bezug auf Ihre Online-Sicherheit, indem Sie diese einfachen Richtlinien im Kopf behalten:

1. Verwenden Sie immer 1Password, um starke, eindeutige Passwörter für jedes Konto zu erstellen
2. Stellen Sie sicher, dass Ihr Kontopasswort für 1Password.com ausgeklügelt und einprägsam ist und nicht für andere Dinge verwendet wird.
3. Schließen Sie alte Konten, die Sie nicht mehr benötigen; mit weniger Konten ist die Wahrscheinlichkeit geringer, dass Sie von einer Datenverletzung betroffen sind.

1Password bietet auch zusätzliche Funktionen für diejenigen, die ihre Geheimnisse noch besser schützen möchten:

1. Richten Sie die Zwei-Faktor-Authentifizierung für alle Konten und Websites ein, die sie unterstützen. Dies stellt eine zusätzliche Verteidigungsebene dar, die Sie retten kann, falls es jemandem gelingt, Ihr Passwort für diese Konten zu erhalten, sei es durch eine Datenverletzung oder eine andere Methode.
2. Lassen Sie Watchtower als Ihren persönlichen Sicherheitswächter agieren, der Ihnen hilft, schwache oder wiederverwendete Passwörter zu identifizieren und optional Ihr Konto auf Anmeldeinformationen zu überwachen, die in eine Datenverletzung verwickelt waren. Wenn eines Ihrer Konten von einer Sicherheitsverletzung betroffen ist, erhalten Sie eine Benachrichtigung, so dass Sie diese Passwörter zurücksetzen können, bevor jemand die Möglichkeit hat, sie zu missbrauchen. Sie können Watchtower auch verwenden, um zu sehen, für welche Websites Sie die Zwei-Faktor-Authentifizierung noch nicht aktiviert haben.

Online sicher zu sein, muss nicht kompliziert oder verwirrend sein. Mit 1Password profitieren Sie von besserer Sicherheit, ohne sich selbst darum kümmern zu müssen.

Probleme mit dem Wiederherstellungsmodus und wie man sie löst

von Howard Oakley, eclecticlight.co • Übersetzung: KJM

Normalerweise versuchen wir, einen Mac im Wiederherstellungsmodus zu starten, wenn es ein Problem gibt. Aber was können wir tun, wenn der Wiederherstellungsmodus selbst ein Problem darstellt?

Wiederherstellungsmodus nicht aktivierbar

Intel Macs können den Wiederherstellungsmodus und andere Startmodi nur dann aufrufen, wenn eine funktionierende Tastatur angeschlossen ist. Wenn Sie eine kabellose Tastatur verwenden und Ihr Mac in keinem dieser Modi starten kann, verwenden Sie entweder eine kabelgebundene USB-Tastatur oder schließen Sie die kabellose Tastatur über das Ladekabel an Ihren Mac an, wodurch sie zu einer USB-Tastatur wird.

Wenn die normale Wiederherstellung fehlschlägt, können Sie es mit der Internet- oder Remote-Version versuchen, indem Sie mit gedrückter Tastenkombination Befehl-Option-R starten. Dies ist bekanntermaßen langsam, da zunächst ein Disk-Image des Wiederherstellungssystems heruntergeladen werden muss, bevor es ausgeführt werden kann.

Macs mit Apple-Prozessoren verwenden die Einschalttaste, um den Wiederherstellungsmodus und andere Startmodi aufzurufen. Dazu müssen Sie einfach die Einschalttaste gedrückt halten, bis auf dem Display angezeigt wird, dass die Optionen geladen werden. Sollte dies nicht der Fall sein, versuchen Sie die unten beschriebene Fallback-Wiederherstellung. Dies mag zunächst schwierig erscheinen, ist aber in Wirklichkeit viel einfacher. Allerdings gibt es keine Internet- oder Fernwiederherstellung.

Probleme mit der Tastatur oder der Sprache

Oben rechts auf jedem Bildschirm im Wiederherstellungsmodus befindet sich ein Tastaturmenü, in dem Sie Ihr bevorzugtes Layout auswählen können.

Mit den Apple Silicon Macs können Sie auch Bluetooth-Eingabegeräte, einschließlich Tastatur, Maus und Trackpad, koppeln oder reparieren. Der Zugriff darauf erfolgt über den anfänglichen Optionsbildschirm, sobald die Wiederherstellung geladen ist. Um Geräte zu koppeln, drücken Sie die Einschalttaste dreimal in etwas weniger als drei Sekunden. Wenn Sie zu schnell drücken oder mehr als eine Sekunde zwischen den einzelnen Tastendrücken verstreichen lassen, funktioniert dies möglicherweise nicht. Wenn Sie es richtig gemacht haben, sollte der Bluetooth-Einrichtungsassistent Ihnen helfen, das gewünschte Gerät zu koppeln.

Probleme mit dem Netzwerk

Wenn das Hauptfenster der Wiederherstellungsoptionen geladen ist, sollten Sie oben rechts auf dem Bildschirm ein Wi-Fi-Symbol sehen. Wenn dort kein vernünftiges Signal angezeigt wird, verwenden Sie dieses Menü, um das richtige Netzwerk zu verbinden.

Hardware-Diagnose durchführen

Auf Intel Macs müssen Sie die Diagnose mit den Tasten D oder Option-D starten. Mit der Taste D wird die Diagnose von Ihrem Mac aus gestartet, während Option-D der Ausweg ist, wenn das nicht funktioniert, da ein Diskettenabbild von Apples Servern heruntergeladen und dann gestartet wird.

Apple-Silicon-Macs verwenden hier, und nur hier, einen Tastenbefehl, der allerdings nicht während des Starts gehalten wird. Um Diagnostics aufzurufen, halten Sie auf dem ersten Optionsbildschirm der Wiederherstellung die Befehlstaste-D gedrückt, bis Sie die Meldung erhalten, dass Diagnostics geladen wird, und wählen Sie dann Ihre Sprache. Wenn das nicht funktioniert, werden Sie aufgefordert, über das Diagnosemenü einen Neustart durchzuführen und es erneut zu versuchen. Wenn das nicht klappt, starten Sie die Fallback Recovery und versuchen Sie es dort.

Fallback-Wiederherstellung

Anstatt einen Internet-Wiederherstellungsmodus anzubieten, verfügen Apple-Silicon-Macs in der Regel über eine lokale Fallback-Wiederherstellung. Diese wird normalerweise in einer versteckten Partition/Container auf der internen SSD des Macs installiert. Um in diesen Modus zu gelangen, müssen Sie zweimal schnell hintereinander die Einschalttaste drücken und beim zweiten Mal die Taste gedrückt halten, bis Sie sehen, dass die Optionen geladen werden.

Die Fallback-Wiederherstellung ist in jeder Hinsicht mit der normalen Wiederherstellung identisch, mit einer Ausnahme: Das Startup Security Utility kann in den meisten Fällen nicht verwendet werden, um die Boot-Sicherheit zu ändern.

Wiederherstellung im DFU-Modus

Apple-Silicon-Macs haben eine letzte und ultimative Ausweichmöglichkeit: Im schlimmsten Fall können Sie den Mac im DFU-Modus starten, ihn mit einem anderen Mac verbinden, auf dem Apple Configurator 2 läuft, und von dort aus seine Firmware und Software vollständig wiederherstellen. Der Mac befindet sich dann in einem neuwertigen Zustand, so als ob er gerade erst ausgepackt worden wäre. Alle Benutzerdaten werden bei diesem Vorgang gelöscht. Sie müssen also von Ihrer letzten Sicherungskopie migrieren, wenn Sie Ihren wiederhergestellten Mac in Betrieb genommen und personalisiert haben. Dieser Vorgang wird in der Hilfe für Configurator ausführlich beschrieben und erfordert ein USB-C-Kabel (nicht Thunderbolt), um die beiden Macs zu verbinden. Wenn Sie sich damit überfordert fühlen, sollten Apple Stores und autorisierte Service Provider in der Lage sein, dies zu tun, während Sie warten.

Support-Artikel

Intel: Ein A bis Z der Tasten und Tastaturen: Starten und Anmelden und Apple

Apple Silicon: Ein illustrierter Leitfaden zur Wiederherstellung auf Apple-Silizium-Macs und Apple

Ein AirTag im Gepäck kann Lösungen für Notlagen finden.

Die besten Tipps für Reisen mit AirTags

Artikel, Bilder, Screenshots von D. Griffin Jones/cultofmac.com
Übersetzung: KJM

Reisen ist viel einfacher, wenn man mit AirTags den Überblick über sein Gepäck behalten kann. In letzter Zeit gab es immer wieder Nachrichten darüber: Fluggesellschaften haben Gepäckstücke von Fluggästen verloren und Menschen haben sie wiedergefunden, weil sie die Voraussicht hatten, ein AirTag in das Gepäck zu stecken. So können Sie sicherstellen, dass Sie Ihr Gepäck während der gesamten Reise bei sich haben und es bei der Gepäckausgabe am Zielort schnell wiederfinden.

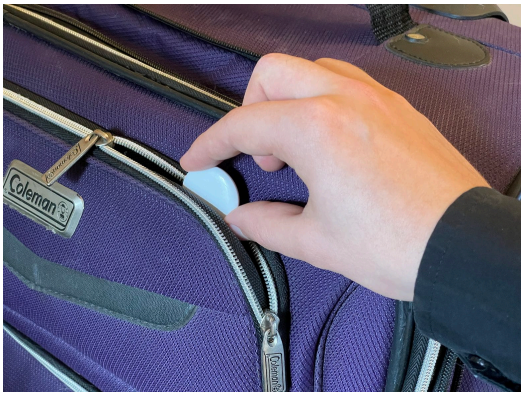
Wie man mit AirTags reist

AirTags kosten ca. 29 $ für ein Stück oder 99 $ für ein Vierpack. Holen Sie sich eines und stecken Sie es in Ihre Tasche (oder kaufen Sie ein Vierpack, wenn die ganze Familie verreist) und beherzigen Sie diesen Rat:

Lassen Sie ihn nicht irgendwo sichtbar liegen.

Vielleicht locken Sie einige Schlüsselanhänger an, die das glänzende weiß-silberne Medaillon perfekt zur Geltung bringen, aber davon rate ich ab. Wenn ein verärgerter Angestellter der Fluggesellschaft sieht, dass Ihr Gepäck einen AirTag hat, besteht die Möglichkeit, dass er ihn entfernt.

Ein Gepäckstück mit einem AirTag auf der Außenseite kann genauso gut gar keinen AirTag haben.



Stecken Sie ihn einfach in die Außentasche Ihres Gepäcks, und schon ist alles in Ordnung.

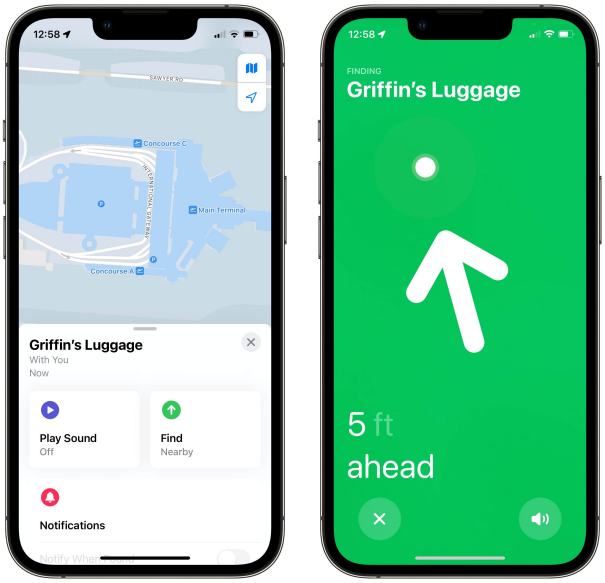
Verstecken Sie Ihren AirTag darin. Nicht so tief, dass er Probleme haben könnte, eine Verbindung zu finden — wenn Sie eine Außentasche haben, die auf der Oberfläche liegt, stecken Sie ihn am besten dort hinein.

Oder verwenden Sie eine der AirTag-Tarnkappen, die Sie im Cult of Mac Store finden.

Finden Sie Ihr Gepäck in der Gepäckausgabe

Sie müssen nicht auf ein Unglück warten, um auf Ihre Kosten zu kommen. Sie können Ihr aufgegebenes Gepäck während der gesamten Reise verfolgen, damit Sie sich keine Sorgen machen müssen.

Meine Frau und ich hatten einmal einen Anschlussflug, bei dem wir in wenigen Minuten eine halbe Meile durch den Dulles International Airport rennen mussten (ich verdiene meinen Lebensunterhalt mit dem Schreiben über Computer; ich bin nicht zum Laufen geschaffen). Wir haben es geschafft, aber wir waren besorgt, dass unser Gepäck es nicht geschafft hatte. Als wir in Deutschland landeten, beruhigte es unsere Nerven, zu wissen, dass unsere Koffer noch bei uns waren.

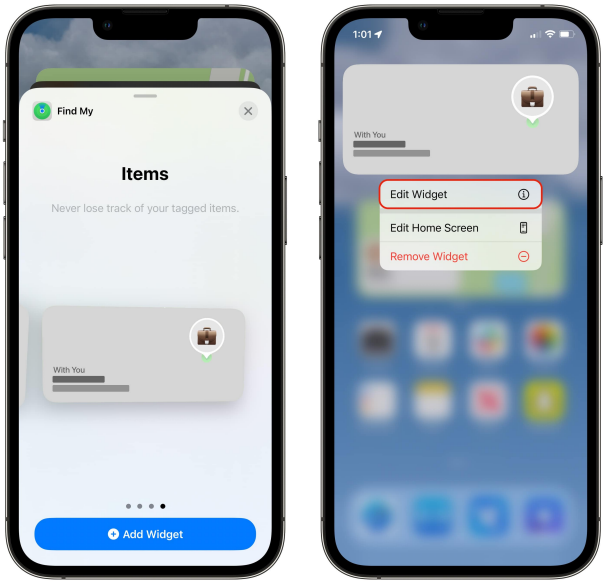


Mit der Find My App ist es leicht, sein Gepäck in einem großen Flughafen zu finden. Screenshot: D. Griffin Jones/Cult of Mac

Und wenn Sie die letzte Etappe Ihrer Reise antreten, müssen Sie vielleicht nicht ewig warten, um Ihr Gepäck in der Gepäckausgabe zu finden. Öffnen Sie einfach die App „Wo ist“, tippen Sie auf der Registerkarte „Gegenstände“ auf Ihr Gepäckstück und tippen Sie auf „Suchen“, um genau zu sehen, wo es sich in dem unvermeidlichen Meer von ähnlich aussehenden Koffern befindet. So können Sie sich von der Masse absetzen und wissen genau, wann Ihr Gepäckstück kommt.

Ein Widget für den Startbildschirm hinzufügen

Wenn Sie sich auf einer langen Reise mit mehreren Etappen befinden (und Sie der nervöse Typ sind), werden Sie die App "Mein Gepäck suchen" möglicherweise sehr oft öffnen. Es gibt einen schnelleren Weg - fügen Sie Ihrem Telefon ein Find My-Widget hinzu.



Fügen Sie ein Widget zu Ihrem Startbildschirm hinzu, damit Sie Ihre Sachen schnell im Blick haben können.

Tippen Sie dazu zunächst auf Ihren Homescreen und halten Sie ihn gedrückt, um ihn zu bearbeiten (oder wischen Sie nach links, wenn Sie keinen Platz haben). Tippen Sie auf das +-Symbol oben links und scrollen Sie nach unten, um ein Find My-Widget hinzuzufügen. Scrollen Sie weiter, um ein Artikel-Widget hinzuzufügen, und tippen Sie auf Widget hinzufügen.

Wenn du mehrere AirTags hast, solltest du sicherstellen, dass du den richtigen verfolgst. Tippen Sie auf das Widget, während Sie sich noch im Bearbeitungsmodus befinden (oder tippen und halten Sie und wählen Sie Widget bearbeiten), und wählen Sie den Artikel aus, den Sie verfolgen möchten.