Was sind eigentlich Passkeys?



Vielleicht ist auch Ihnen beim Anmelden auf einer Internetseite in letzter Zeit einmal die Frage begegnet: „Möchten Sie einen Passkey erstellen?“ Hinter diesem Begriff steckt eine neue Möglichkeit, sich bei einem Benutzerkonto anzumelden. Immer mehr Internetseiten bieten Passkeys (auch Hauptschlüssel genannt) an, daher möchten wir dieser neuen Funktion nun auch einen ausführlichen Beitrag widmen. Dafür haben wir auch wieder ganze neue Filme für Sie erstellt, in denen wir zeigen, wie man einen Passkey anlegt und wie er funktioniert.

Empfehlen Sie die Nutzung und Erläuterung von Passkey an Freunde und Bekannte:
Diesen Artikel per E-Mail weiterleiten, Diesen Artikel an einen WhatsApp-Kontakt senden,
Diesen Artikel weiterempfehlen und Link in die Zwischenablage kopieren

Was ist ein Passkey?
Ein Passkey ist eine Art digitaler Schlüssel. Er öffnet Ihnen den Zugang zu einem bestimmten Benutzerkonto, zum Beispiel bei Amazon, Google oder Apple. Anders als bei einem Passwort müssen Sie sich diesen Schlüssel aber weder selbst ausdenken noch auswendig lernen oder eintippen. Ihr Gerät beziehungsweise ein Passwortmanager bewahrt den Passkey für Sie auf.
Bisher geben Sie beim Anmelden auf einer Internetseite Ihr Passwort ein. Haben Sie für diese Seite auch einen Passkey eingerichtet, können Sie die Anmeldung stattdessen beispielsweise mit Ihrem Fingerabdruck bestätigen. Je nach Gerät funktioniert das auch mit der Gesichtserkennung oder mit der PIN, mit der Sie Ihr Gerät entsperren.
Ihr Fingerabdruck ist in diesem Beispiel nicht der Passkey. Er erlaubt Ihrem Gerät lediglich, den gespeicherten digitalen Schlüssel abzurufen und zu verwenden. Ihr Fingerabdruck, die Daten der Gesichtserkennung oder Ihre Geräte-PIN werden auch nicht an die Internetseite weitergegeben.
Wichtig ist außerdem: Ein Passkey ist kein Universalschlüssel. Wie bei Passwörtern auch, richten sie ihn immer nur für das jeweilige Benutzerkonto ein. Für Ihr Amazon-Konto verwenden Sie also einen anderen Passkey als für Ihr Google-Konto oder Ihren GMX-Zugang. Die Verwaltung übernimmt Ihr Gerät oder Ihr Passwortmanager.

Was bringt ein Passkey im Alltag?
Der offensichtlichste Vorteil eines Passkeys ist natürlich die bequemere Anmeldung: Sie müssen Ihr Passwort nicht mehr heraussuchen und eintippen. Stattdessen bestätigen Sie die Anmeldung beispielsweise mit Ihrem Fingerabdruck, der Gesichtserkennung oder Ihrer Geräte-PIN.
Ein Passkey bietet außerdem einen wichtigen Schutz vor Betrug. Kriminelle bauen häufig Internetseiten nach, die der echten Anmeldeseite einer bekannten Seite täuschend ähnlich sehen. Wer dort sein Passwort eingibt, übermittelt es an die Betrüger. Ein Passkey funktioniert nur bei dem Anbieter, für den er eingerichtet wurde. Auf einer gefälschten Internetseite kann er nicht zur Anmeldung verwendet werden. Damit schützt er vor einer häufigen Methode des Passwortdiebstahls.
Auch das Erraten eines Passworts fällt bei dieser Anmeldemethode weg: Ein Passkey wird automatisch erzeugt und ist kein selbst gewähltes Wort wie ein Name oder ein Geburtsdatum.

Ersetzt der Passkey mein Passwort?
Nein, normalerweise müssen Sie Ihr bisheriges Passwort nicht aufgeben, wenn Sie einen Passkey einrichten. Der Passkey kommt einfach als weitere Anmeldemöglichkeit hinzu. Ihr bestehendes Passwort wird dadurch nicht geändert oder gelöscht. Man kann es sich also wie einen zusätzlichen Zugang vorstellen: Sie können den Passkey verwenden, haben aber weiterhin die Möglichkeit, sich stattdessen mit Ihrem Passwort anzumelden. Je nach Anbieter finden Sie diese Möglichkeit auf der Anmeldeseite unter Bezeichnungen wie „Andere Anmeldeoptionen“ oder „Andere Möglichkeit wählen“.
Das ist beispielsweise hilfreich, wenn Sie an einem anderen Computer sitzen und Ihr Passkey gerade nicht verfügbar ist. Bewahren Sie Ihr bisheriges Passwort deshalb weiterhin sicher auf, auch wenn Sie künftig meistens den Passkey verwenden. Sie müssen sich nicht sofort für eine der beiden Möglichkeiten entscheiden, sondern können die neue Anmeldung zunächst in Ruhe ausprobieren.

Wo wird der Passkey gespeichert?
Einen Passkey müssen Sie sich nicht merken oder aufschreiben, er wird für Sie gespeichert. Dabei gibt es zwei grundlegende Möglichkeiten: nur auf einem bestimmten Gerät oder in einem Passwortspeicher, der mehrere Geräte miteinander verbindet.
Möglichkeit 1: Nur auf einem Gerät
Der Passkey wird beispielsweise direkt auf Ihrem Windows-Computer gespeichert. Sie können ihn dort verwenden und die Anmeldung mit Ihrer Geräte-PIN, Ihrem Fingerabdruck oder der Gesichtserkennung bestätigen. Auf einem anderen Computer ist dieser Passkey dann nicht

automatisch vorhanden. Geht das ursprüngliche Gerät verloren oder kaputt, steht Ihnen auch der dort gespeicherte Passkey nicht mehr zur Verfügung. Deshalb ist es wichtig, eine weitere Anmeldemöglichkeit zu behalten, beispielsweise Ihr bisheriges Passwort.
Das Gerät, auf dem der Passkey gespeichert wird, kann auch ein sogenannter Sicherheitsschlüssel sein. Ein Sicherheitsschlüssel ist ein kleines Gerät, das oft wie ein USB-Stick aussieht. Wenn die Internetseite diese Möglichkeit anbietet, können Sie Ihren Passkey direkt darauf speichern. Dafür brauchen Sie aber solch einen speziellen Sicherheitsschlüssel, ein gewöhnlicher USB-Stick eignet sich dafür nicht.
Zum Anmelden stecken Sie den Sicherheitsschlüssel in den USB-Anschluss. Der Vorteil: Sie können denselben Sicherheitsschlüssel auch an einem anderen geeigneten Computer verwenden. Der Passkey bleibt auf dem Schlüssel, den Sie mitnehmen.

Möglichkeit 2: In einem Passwortspeicher mit Cloud-Anbindung

Der Passkey wird in einem Passwortmanager gespeichert, der ihn über das Internet verschlüsselt mit Ihren anderen Geräten abgleicht. Beispiele dafür sind der iCloud-Schlüsselbund von Apple und der Google Passwortmanager. Speichern Sie einen Passkey beispielsweise auf Ihrem iPhone im iCloud-Schlüsselbund, kann er dadurch auch auf Ihrem iPad oder Mac verfügbar sein. Voraussetzung ist, dass die Geräte mit demselben Apple Account verbunden sind und der Abgleich eingeschaltet ist. Das Gleiche gilt für den Google Passwortmanager im Chrome-Browser. Der Vorteil: Sie müssen den Passkey nicht auf jedem Ihrer Geräte neu einrichten. Er steht allerdings nicht automatisch auf jedem beliebigen Gerät zur Verfügung.
Bei der Einrichtung wird Ihnen ein Speicherort vorgeschlagen. Je nach Gerät und Browser können Sie über eine Schaltfläche wie „Weitere Optionen“ oder „Anders speichern“ einen anderen Speicherort auswählen. Welche Möglichkeiten erscheinen, hängt davon ab, welches Gerät und welchen Passwortmanager Sie verwenden.
Achten Sie deshalb beim Einrichten darauf, wo der Passkey gespeichert werden soll, bevor Sie bestätigen. Nur weil Sie die Einrichtung am Computer beginnen, muss der Passkey nicht ausschließlich auf diesem Computer gespeichert werden. Unsere Filme zeigen dies.

Filmische Anleitung: Passkey erstellen

In den folgenden Filmen zeigen wir Ihnen, wie Sie einen Passkey für Ihr Google-Konto, Ihr Microsoft-Konto und Ihr GMX-Konto einrichten. Das sind drei Beispiele, stellvertretend für zahlreiche andere Anbieter. Immer mehr Internetseiten bieten nach und nach die Anmeldung mit einem Passkey an. Häufig wird Ihnen das Einrichten eines Passkeys schon vorgeschlagen, wenn Sie sich wie gewohnt mit Ihrem Passwort anmelden. Sie können diesen Vorschlag auch zunächst überspringen. Wenn die Internetseite Passkeys unterstützt, können Sie das in der Regel auch später noch einrichten. Die passende Option finden Sie meist in den Einstellungen Ihres Benutzerkontos, etwa unter „Sicherheit“ oder „Anmeldung“.

Passkey für Google-Konto anlegen

Video-Player: https://levato.de/wp-content/video/passwoerter/passkey_google.mp4?_=1 8:30 Min.

Passkey für Microsoft Konto anlegen

Video-Player: https://levato.de/wp-content/video/passwoerter/passkey_microsoft.mp4?_=2 5:07 Min.

Passkey für GMX anlegen

Video-Player: https://levato.de/wp-content/video/passwoerter/passkey_gmx.mp4?_=3 5:16 Min.

Das Wichtigste zusammengefasst

1. Ein Passkey ist ein digitaler Schlüssel für ein bestimmtes Benutzerkonto.
Damit können Sie sich anmelden, ohne das Passwort für dieses Konto einzutippen. Sie bestätigen die Anmeldung zum Beispiel mit Ihrem Fingerabdruck, per Gesichtserkennung oder mit Ihrer Geräte-PIN.
2. Passkeys schützen vor gefälschten Anmeldeseiten.
Der digitale Schlüssel funktioniert nur bei der Internetseite oder App, für die er eingerichtet wurde.
3. Der Speicherort entscheidet, auf welchen Geräten der Passkey verfügbar ist.
Er kann auf einem einzelnen Gerät, in einem Passwortmanager mit Abgleich auf mehreren Geräten oder auf einem tragbaren Sicherheitsschlüssel gespeichert werden.
4. Ihr bisheriges Passwort bleibt normalerweise weiterhin gültig.
Das Einrichten eines Passkeys löscht das Passwort nicht automatisch. Bewahren Sie es weiterhin sicher auf, solange Sie es zur Anmeldung verwenden können.

Quelle: https://levato.de/was-sind-eigentlich-passkeys/