

Deutsche Bank schaltet sichere Online-Funktionen ab - So handeln Sie jetzt!

Die Deutsche Bank schaltet am 30. Juni 2025 wichtige Online-Banking-Funktionen ab. Kunden müssen Daten rechtzeitig sichern.



Ruhr, Deutschland - Am 30. Juni 2025 wird die Deutsche Bank zwei ihrer Online-Banking-Funktionen, den Persönlichen Safe und den Passwort-Safe, einstellen. Dies geschieht aufgrund der „sehr geringen Nachfrage“ nach diesen Speicherdiensten, wie **Ruhr24 berichtet**. Kunden sind aufgefordert, ihre wichtigen Dokumente und Passwörter bis zu diesem Stichtag herunterzuladen und auf eigenen Geräten zu sichern, da nach dem 30. Juni 2025 kein Zugriff mehr auf die gespeicherten Daten möglich sein wird.

Der Persönliche Safe diente als verschlüsselter Cloud-Speicher für bankbezogene und private Dokumente. Der Passwort-Safe war ein digitaler Tresor für Zugangsdaten und bot Funktionen

zur Passwortverwaltung und -generierung. Kunden, die diese Dienste genutzt haben, müssen sich nun alternative Lösungen suchen. Empfohlen werden andere Cloud-Dienste mit Verschlüsselung zur Speicherung von Dokumenten sowie spezialisierte Passwort-Manager für die Verwaltung ihrer Zugangsdaten.

Wichtige Schritte für Kunden

Kunden sollten ihre Passwörter und Dokumente proaktiv sichern, bevor die Dienste endgültig abgeschaltet werden. Eine Möglichkeit, um Passwörter einfach zu sichern, erklärt die Deutsche Bank in ihrer Hilfe zur Nutzung des Passwort-Safes: Kunden können sich in ihren eSafe einloggen, die Option „Importieren“ auswählen und ihre Passworteinträge entsprechend anpassen. Eine Vorschautabelle hilft dabei, die richtigen Attraktionen zu überprüfen, bevor sie importiert werden.

Die Notwendigkeit, auf sichere Passwortverwaltungen umzusteigen, wird auch von Experten betont. Laut **Hanseatic Bank** bieten Passwort-Manager die Möglichkeit, Passwörter sicher zu erstellen, zu speichern und zu verwalten. Nutzer müssen sich lediglich ein Master-Passwort merken, um Zugang zu allen anderen Passwörtern zu erhalten. Dies ist um ein Vielfaches sicherer als die Speicherung von Passwörtern im Webbrowser, die als unsicher gilt.

Alternativen zur Passwortverwaltung

Bei der Auswahl eines Passwort-Managers sollten Nutzer auf sichere Datenverschlüsselung, wie AES-256, und die Zero-Knowledge-Policy achten, um ihre Daten bestmöglich zu schützen. Auch zusätzliche Sicherheitsmerkmale, wie die Zwei-Faktor-Authentifizierung, können dabei helfen, den Schutz zu erhöhen. Offline-Passwort-Manager speichern Daten lokal, während cloudbasierte Lösungen den Zugriff von verschiedenen Geräten ermöglichen, aber auch Risiken in Bezug auf Hacks

bergen.

Mit der bevorstehenden Abschaltung der Funktionen der Deutschen Bank, müssen Kunden also aktiv werden. Eine sorgfältige Planung und der Einsatz sicherer Technologien werden entscheidend sein, um den Verlust ihrer Daten zu verhindern und die Sicherheit ihrer Online-Konten zu gewährleisten. Es ist empfehlenswert, frühzeitig die notwendigen Schritte zu unternehmen und sich über alternative Auffüllungen zu informieren.

Details	
Vorfall	Information
Ursache	sehr geringe Nachfrage
Ort	Ruhr, Deutschland
Quellen	<ul style="list-style-type: none">• www.ruhr24.de• www.deutsche-bank.de• www.hanseaticbank.de

Besuchen Sie uns auf: n-ag.net