Bitkom e.V. | Presseinformation

Jeder Vierte nutzt bewusst einfache Passwörter – um sie sich merken zu können

- **Am 1. Februar ist der jährliche „Ändere-dein-Passwort-Tag“**
- **Bitkom gibt 5 Tipps für sichere Passwörter, die länger als ein Jahr halten**

Berlin, 30. Januar 2025 – Ob „geheim“, „123456“ oder Name und Geburtstag des Kindes – beim Umgang mit Passwörtern sind viele immer noch nachlässig, obwohl sie es damit Cyberkriminellen leicht machen, sich Zugang etwa zu Social-Media-Diensten, Online-Shopping oder Bank- und Gesundheitsdaten zu verschaffen. So nutzt rund ein Viertel (23 Prozent) der Internetnutzerinnen und -nutzer häufig bewusst einfache Passwörter, damit sie sich diese leicht merken können. Ein Drittel (33 Prozent) nutzt dasselbe Passwort für verschiedene Dienste. Das sind Ergebnisse einer Umfrage unter 1.021 Internetnutzerinnen und -nutzerin in Deutschland ab 16 Jahren im Auftrag des Digitalverbands Bitkom. „Der Ändere-Dein-Passwort-Tag am 1. Februar ist eine gute Gelegenheit, sich jetzt einen Überblick über die eigenen Kennwörter zu verschaffen und sich von einfachen oder mehrfach genutzten zu verabschieden und sie zu ersetzen“, sagt Bitkom-Sicherheitsexperte Felix Kuhlenkamp. „Aber wer gute Passwörter wählt und sie wo immer möglich mit Zwei-Faktor-Authentifizierung kombiniert oder gleich Passkeys nutzt, der braucht keinen jährlichen Erinnerungs-Tag mehr, um seine Passwörter zu ändern. Das ist dann allenfalls noch nötig, falls es Hinweise auf Datenlecks gibt.“

Anlässlich des Ändere-Dein-Passwort-Tages am 1. Februar gibt Bitkom fünf Tipps für sichere Zugänge:

- **Keine einfachen Passwörter:** Passwörter sollten nicht aus einem leicht zu erratenden persönlichen Begriff, wie dem Namen des Kindes oder des Partners, oder aus einem im Wörterbuch zu findenden einzelnen Wort bestehen. Stattdessen bietet sich eine Kombination aus verschiedenen Worten oder Silben, womöglich mit ungewöhnlicher Groß- und Kleinschreibung an. Je länger das Passwort ist, desto schwieriger ist es, es zu knacken. Sonderzeichen kann man vor allem dann nutzen, wenn man seine Passwörter ohnehin in einem Passwortmanagerspeichert.
- **Keine doppelten Passwörter:** Für jeden Online-Dienst sollte man ein einzigartiges Passwort verwenden. Das reduziert das Risiko, dass bei einem Datenleck Cyberkriminelle Zugriff auf mehrere Konten bekommen, wenn sie gestohlene Zugangsdaten an unterschiedlichen Stellen einsetzen. Vor allem für zentrale Online-Dienste wie etwa den E-Mail-Provider, aber auch für Dienste, bei denen Kontodaten hinterlegt sind, wie etwa beim Online-Shopping, sollte man unbedingt komplexe und einzigartige Passwörter verwenden.
- **Keine Zettel und einfache Textdateien:** Niemand kann sich Dutzende von Zugangsdaten merken. Passwörter aufzuschreiben und auf dem Büro-Schreibtisch liegenzulassen ist aber ebenso wenig eine gute Idee wie Passwortlisten in einer einfachen Textdatei auf dem Computer zu speichern. Stattdessen bieten sich Passwortmanager an. Das sind Programme für den PC oder als App für das Smartphone, in denen Zugangsdaten sicher verschlüsselt abgelegt werden können. Der Vorteil: Man muss sich nur ein – möglichst gutes – Passwort für den Passwortmanager merken oder kann diesen auf dem Smartphone zum Beispiel auch per Fingerabdruck „aufschließen“.
- **Doppelt hält besser:** Wo immer möglich sollte die sogenannte Zwei-Faktor-Authentifizierung eingerichtet werden, denn selbst das stärkste Passwort lässt sich knacken. Bei der Zwei-Faktor-Authentifizierung reichen Nutzername und Passwort alleine nicht für den Zugang, sondern man muss aus einer speziellen App auf dem Smartphone noch einen Zahlencode ablesen und diesen zusätzlich eingeben. Das bedeutet, dass sich Angreifer nicht nur das Passwort verschaffen müssen, sondern auch Zugang zum Smartphone brauchen, wodurch die Sicherheit erhöht wird. Manchmal wird der zweite Faktor – also der Zahlencode – auch per SMS oder andere

Kurznachricht verschickt oder per Mail.

- **Noch mehr Sicherheit – ganz ohne Passwort:** Passkeys sind eine moderne und besonders sichere Alternative zum klassischen Passwort. Anstatt wie bisher das Kennwort einzugeben, wird bei einem Passkey bei der ersten Registrierung ein Schlüsselpaar generiert, bei dem ein Teil (der private Schlüssel) sicher auf dem Gerät bleibt und der andere (der öffentliche Schlüssel) an den Online-Dienst übermittelt wird. Der Vorteil: Der private Schlüssel – der wie früher das Passwort der Ausweis für die eigene Identität ist – muss nie übertragen werden und kann so auch nicht so einfach gestohlen und missbraucht werden. Die Schlüssel selbst sind eine lange Zahlenkolonne, die der Nutzer aber gar nicht kennen muss, stattdessen wird für die Identifikation auf dem eigenen Gerät bequem der Fingerabdruck, die Gesichtserkennung oder eine PIN verwendet.

Kontakt

Andreas Streim
Pressesprecher
Telefon: +49 30 27576-112
E-Mail: a.streim@bitkom.org
Download Pressefoto

Felix Kuhlenkamp
Bereichsleiter Sicherheitspolitik
Download Pressefoto
Nachricht senden

Hinweis zur Methodik

Grundlage der Angaben ist eine Umfrage, die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat. Dabei wurden 1.115 Personen in Deutschland ab 16 Jahren telefonisch befragt, darunter 1.021 Internetnutzerinnen und Internetnutzer . Die Befragung fand im Zeitraum von KW 49 2024 bis KW 02 2025 statt. Die Gesamtumfrage. Die Gesamtumfrage ist repräsentativ. Die Fragestellung lautete „Welche der folgenden Aussagen treffen auf Sie zu bzw. nicht zu?“

Link zur Presseinformation auf der Webseite:
https://www.bitkom.org/Presse/Presseinformation/Jeder-Vierte-nutzt-einfache-Passwoerter