

Passwortwechsel: So schützen sich die Südwestpfälzer besser!

Erfahren Sie, wie Südwestpfälzer heute am „Ändere-dein-Passwort“-Tag ihre digitalen Konten schützen und sichern können.

Zweibrücken, Deutschland - Am 1. Februar jedes Jahr findet der bundesweite „Ändere-dein-Passwort“-Tag statt, dessen Ziel es ist, die Sicherheit im Umgang mit Passwörtern zu erhöhen. Während viele Nutzer trotz dieser Initiativen dazu neigen, ihre Passwörter regelmäßig zu wechseln, raten Fachleute von dieser Praxis ab. So wird insbesondere vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen, Passwörter nicht routinemäßig zu ändern, da dies oft zu schwächeren Passwörtern führen kann. Stattdessen sollte der Fokus darauf liegen, Online-Konten so abzusichern, dass Passwörter möglichst nie mehr verändert werden müssen, wie **Rheinpfalz** berichtet.

In der heutigen digitalen Welt sind Passwörter ein zentraler Bestandteil unseres Lebens, die jedoch immer wieder Ziel von Angriffen werden. Laut einer Umfrage berichteten 53 % der Nutzer von Datenschutzverletzungen aufgrund schlecht verwalteter Benutzernamen und Passwörter. Angesichts der steigenden Zahl an Cyberangriffen und Datenlecks ist es unerlässlich, rechtzeitig Vorkehrungen zu treffen. Hierzu raten Experten, verschiedene Methoden zur Sicherung von Konten zu nutzen.

Empfohlene Methoden zur Passwortsicherung

Zu den sichersten Methoden gehören:

- **Zwei-Faktor-Schutz (2FA):** Diese Technik ergänzt das Passwort durch ein zusätzliches Element, wie einen Zahlencode oder 2FA-Stick. Dies erhöht die Sicherheit, da Angreifer sowohl das Passwort als auch Zugriff auf das Gerät benötigen.
- **Passkeys:** Diese passwortlose Authentifizierungsmethode nutzt biometrische Daten, wie Fingerabdrücke oder Gesichtserkennung, um den Zugang zu ermöglichen.
- **Passwortmanager:** Diese Programme helfen Nutzern, komplexe Passwörter zu erstellen und sicher zu speichern. Dabei sollte jedoch das Risiko des Verlusts des Masterpassworts oder Datenlecks bei Anbietern nicht unterschätzt werden.
- **Starke Passwörter:** Experten empfehlen Passwörter, die mindestens acht Zeichen umfassen und eine Mischung aus Groß- und Kleinbuchstaben, Zahlen sowie Sonderzeichen enthalten.

Zusätzlich sollten Nutzer besondere Sicherheitsmaßnahmen wie die Absicherung ihrer E-Mail-Konten in Betracht ziehen, da diese oft für Passwortzurücksetzungen genutzt werden. Das Ökosystem der Passwortsicherheit ist entsprechend komplex, und viele Nutzer machen die Erfahrung, dass die Verwaltung schwierig ist. Laut einer Umfrage empfinden 80 % der Befragten die Passwortverwaltung als herausfordernd. Dies belegt, wie wichtig es ist, sich mit den Tools und Methoden zur Sicherung der eigenen Daten auseinanderzusetzen, wie auf **Swiss Cyber Institute** dargestellt wird.

Aktuelle Herausforderungen im Alltag

Die Realität zeigt, dass viele Nutzer nach einem Sicherheitsvorfall dazu neigen, ihre Passwörter zu ändern. Laut einer Umfrage haben 76 % der Privatpersonen und 65 % der IT-Fachleute ihre Passwörter nach einem Angriff geändert.

Dennoch verwenden 36 % der Nutzer dasselbe Passwort für mehrere Konten, was die Sicherheit erheblich gefährdet. Zu den häufigsten Herausforderungen in der Passwortsicherheit zählen Phishing-Angriffe, die 90 % der Befragten im Jahr 2021 erlebten, sowie Brute-Force-Angriffe, die 24 % der Sicherheitsexperten in den letzten zwei Jahren berichtet wurden.

Um die Risiken zu reduzieren und die цифровую безопасность zu erhöhen, ist es entscheidend, ein Bewusstsein für die eigene Passwortsicherheit zu entwickeln und technologische Fortschritte gezielt zu nutzen. Der dialog über Maßnahmen zur Verbesserung der Passwortsicherheit bleibt unerlässlich, um die Nutzer auf die Herausforderungen in der digitalen Welt vorzubereiten.

Details	
Ort	Zweibrücken, Deutschland
Quellen	• www.rheinpfalz.de • www.test.de • swisscyberinstitute.com

Besuchen Sie uns auf: n-ag.de