30.01.2025

Passwort ändern: einmal richtig und dann nie wieder!

Mit den richtigen Maßnahmen bleiben Online-Konten dauerhaft geschützt

Lange wurde empfohlen, Passwörter regelmäßig zu ändern, um Konten vor unberechtigten Zugriffen zu schützen. Viele Verbraucher:innen haben dadurch ihre Passwörter mit der Zeit aber eher geschwächt, um sie sich bei der Vielzahl an Passwörtern leichter merken zu können. „Es ist besser einmal ein starkes Passwort zu wählen statt ständig wechselnde schwache Passwörter zu nutzen“, sagt Ayten Öksüz, Datenschutzexpertin bei der Verbraucherzentrale NRW. Daher sei auch der "Ändere Dein Passwort"-Tag am 1. Februar in seinem ursprünglichen Sinne überholt. Die Expertin rät: „Wer noch keine starken Passwörter nutzt oder ein und dasselbe Passwort für mehrere Accounts verwendet, sollte seine Passwörter jetzt einmal ändern. Dann können die Passwörter im besten Fall dauerhaft im Einsatz bleiben. Noch wichtiger wäre es aber, gerade sensible Accounts zusätzlich mit der 2-Faktor-Authentisierung zu sichern.” Mit den folgenden Tipps können Verbraucher:innen ihre Online-Accounts effektiv schützen:

- **Wie sieht ein starkes Passwort aus?**
  Grundsätzlich gilt: Je länger, desto besser. Ein starkes Passwort sollte mindestens acht (besser zwölf) Zeichen lang sein – dann aber auch aus vier verschiedenen Zeichenarten bestehen, also Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (z.B. § $ % & ! ?). Ein langes Passwort, das mindestens 25 Zeichen oder länger ist, kann hingegen auch aus nur zwei Zeichenarten bestehen. Je sensibler ein Zugang ist (etwa beim Online-Banking), umso mehr Sorgfalt ist bei der Auswahl eines starken Passworts nötig. Besonders wichtig: Für jedes Konto sollte ein eigenes Passwort gewählt werden. Wer einmal ein starkes Passwort erstellt hat, kann es so dauerhaft für das entsprechende Konto nutzen. Es müsste nur in den Fällen, in denen das Passwort in die falschen Hände geraten sein könnte, geändert werden, zum Beispiel wenn ein Datenleck bekannt wird oder das Gerät mit Schadsoftware infiziert wurde.
- **Wie funktioniert die 2-Faktor-Authentisierung?**
  Da selbst das stärkste Passwort nicht unknackbar ist und bei einem Datenleck oder erfolgreichem Phishing-Angriff schnell in falsche Hände geraten kann, bieten Passwörter allein nicht den

Verbraucherzentrale
Nordrhein-Westfalen e.V.
Verbraucherarbeit im Kreis
mobil & digital

Tel. (0211) 54 2222 11
service@verbraucherzentrale.nrw
www.verbraucherzentrale.nrw/kleve

bestmöglichen Account-Schutz. Es empfiehlt sich, Online-Accounts mit einer Zwei-Faktor-Authentisierung (2FA) zusätzlich zu schützen, wenn Anbieter diese Möglichkeit bereitstellen. Diese fungiert wie ein zweites Sicherheitsschloss. Bei der 2FA wird die Identität, nicht nur mit dem Passwort, sondern mit einem zweiten Faktor bestätigt. Damit wird es Kriminellen erschwert, auf Daten zuzugreifen, selbst wenn ihnen das Passwort bekannt ist. Bei diesem zweiten Faktor kann es sich beispielsweise um einen Bestätigungscode per E-Mail, eine SMS-TAN oder ein Einmal-Passwort handeln. Mittlerweile sind auch biometrische Verfahren sehr verbreitet, beispielsweise Gesichts- oder Fingerabdruckscans über das Smartphone.

- **Wie kann ich Passwörter sicher aufbewahren?**
  Verbraucher:innen nutzen heutzutage so viele Online-Dienste, dass die einzelnen Passwörter unmöglich im Gedächtnis behalten werden können. Eine gute Hilfe können daher Passwort-Manager sein. Darin lassen sich starke Passwörter erstellen, verwalten und verschlüsselt speichern. Nutzer:innen müssen sich dann nur noch das zentrale Passwort für den Zugang zu ihren Passwort-Manager merken, das natürlich ganz besonders stark sein sollte.
- **Gibt es eine Alternative zu Passwörtern?**
  Seit einigen Jahren gibt es das Passkey-Verfahren, das die Anmeldung bei Online-Diensten ganz ohne Passwörter ermöglicht. Damit besteht auch nicht mehr die Gefahr, dass Kriminelle Passwörter zum Beispiel bei einem Phishing-Angriff oder Datenleck abgreifen können. Passkeys sind lange, zufällig generierte Zeichenketten, offen und herstellerunabhängig. Sie werden von einem sogenannten Authenticator erstellt und dort auch gespeichert, sobald man sich bei einem Online-Dienst, der dieses Verfahren unterstützt, registriert. Gleichzeitig wird ein zum jeweiligen Passkey (auch privater Schlüssel genannt) passender öffentlicher Schlüssel erzeugt und beim Anbieter hinterlegt. Der Authenticator kann zum Beispiel ein FIDO2-Stick sein (ein spezielles Gerät ähnlich wie ein USB-Stick), ein Computerprogramm oder eine Smartphone-App. Bei der nächsten Anmeldung wird dann im Hintergrund durch das Zusammenspiel mehrerer Komponenten die Identität des Nutzers oder der Nutzerin bestätigt. Nutzer:innen selbst müssen beim Login in den Online-Account dann kein Passwort mehr eingeben, sondern nur noch den Zugriff auf die Passkeys im Authenticator bestätigen, per Fingerabdruck, Gesichtsscan oder durch die Eingabe einer PIN. Falls Kriminelle beispielsweise durch einen Datenleck beim Anbieter Zugriff auf die dort gespeicherten öffentlichen Schlüssel bekommen, können sie damit nichts anfangen. Denn diese funktionieren nur in Kombination mit dem jeweils passenden privaten Schlüssel, dem Passkey.

Weiterführende Infos und Links:

- Mehr Infos zu starken Passwörtern unter:
  https://www.verbraucherzentrale.nrw/node/11672
- So funktioniert die 2-Faktor-Authentisierung:
  https://www.verbraucherzentrale.nrw/node/85173
- So funktionieren Passkeys:
  https://www.verbraucherzentrale.nrw/node/94842