Sichere Passwörter – das Wichtigste auf einen Blick

1 Drei Konten, die eigene, starke Passwörter verlangen

Mindestens diese drei Konten bekommen je ein eigenes, langes Passwort, das Sie nirgendwo sonst verwenden:

- **E-Mail** (wer Ihre E-Mails lesen kann, kann alle anderen Passwörter zurücksetzen)
- **Apple- oder Google-Konto** (das Konto Ihres Handys)
  - **Google-Passwort ändern:** Geben Sie in die Adresszeile Ihres Browser die `myaccount.google.com/security` ein. Dort finden Sie unter „Sicherheit und Anmeldung“ den Punkt „Passwort“.
  - **Apple-Passwort ändern**: „Einstellungen“ → oben auf Ihren Namen tippen → „Anmeldung & Sicherheit“ → „Passwort ändern“.
- **Bank**

So entsteht ein langes Passwort:

- **Weg A, vier bis fünf Wörter:** Wählen Sie zufällige Wörter, die nichts miteinander zu tun haben, und ergänzen diese mit Zahlen, zum Beispiel `Gartenzaun4-Mond0-Kaffee1-Fahrrad2`.
- **Weg B, ein Merksatz:** Nehmen Sie die ersten drei Buchstaben des Anbieters und dann die Anfangsbuchstaben und Satzzeichen eines Satzes. Beispiel:

Merksatz	**Passwort**
Amazon = 1 Anbieter, für den ich ein besonders sicheres Passwort verwende!	`Ama=1A,fdiebsPv!`

Der Satz bleibt gleich, nur die ersten drei Buchstaben wechseln je nach Webseite. Beispiel: Für Kleinanzeigen wird daraus `Kle=1A,fdiebsPv!`

BITTE NICHT DIE BEISPIELE VON DIESEM BLATT VERWENDEN!

2 Passwörter sicher aufbewahren

Niemand muss sich alle Passwörter merken. Beide Wege sind gut:

- **Notizbuch zu Hause:** Ein Heft nur für Passwörter, an einem festen Platz in der Wohnung. Nicht im Portemonnaie und nicht als Notiz im Handy.
- **Passwortmanager:** Ihr Handy bzw. Computer kann Passwörter sicher speichern und selbst starke Passwörter vorschlagen. Auf dem iPhone heißt die App „Passwörter“, auf Android-Handys „Google Passwortmanager“. Beide sind schon installiert.

So verwenden Sie die Passwörter auf Handy und Computer

- **Mit dem Notizbuch:** Sie tippen das Passwort beim Anmelden ab. Das funktioniert immer.
- **Mit dem Passwortmanager auf dem Handy:**
  - Neues Passwort: Wenn Sie ein Passwort anlegen oder ändern, schlägt das Handy ein starkes Passwort vor. Tippen Sie auf den Vorschlag, das Handy speichert es.
  - Anmelden: Das Handy bietet das gespeicherte Passwort an. Sie bestätigen mit Fingerabdruck, Gesicht oder dem Code Ihres Handys.
  - Nachsehen: Alle gespeicherten Passwörter finden Sie in der App „Passwörter“ (iPhone) oder im „Google Passwortmanager“ (Android).
- **Mit dem Passwortmanager auf dem Computer:** Die Passwörter vom Handy erscheinen auch dort, wenn Sie auf beiden Geräten mit demselben Konto angemeldet sind.

Ihr Handy	Ihr Computer	So geht es
iPhone	iMac oder MacBook	Am Mac mit demselben Apple-Konto anmelden. Die App „Passwörter“ gibt es auch auf dem Mac, und der Browser Safari füllt Passwörter automatisch aus.
iPhone	Windows-PC	Das Programm „iCloud für Windows“ installieren und mit dem Apple-Konto anmelden. Es bringt „iCloud-Passwörter“ für Chrome und Edge mit.
Android-Handy	Windows-PC, iMac oder MacBook, Linux	Den Browser Chrome verwenden und dort mit demselben Google-Konto anmelden. Chrome füllt die Passwörter automatisch aus.

Wichtig: Das Passwort für Ihr Apple- oder Google-Konto gehört trotzdem ins Notizbuch. Ohne dieses Passwort kommen Sie an die gespeicherten Passwörter nicht mehr heran, wenn Sie Ihr Handy verlieren.

3 Ein zweiter Schutz

Sie kennen das von der Bank: Zum Einloggen muss man zusätzlich zum Passwort ein zweites Merkmal eingeben, z.B. auf dem Smartphone mit Fingerabdruck bestätigen. Im Internet heißt das „**Zwei-Faktor-Authentifizierung**“, kurz 2FA, oder „Bestätigung in zwei Schritten“. Selbst wenn Ihr Passwort mal gestohlen oder erraten wurde, die Zwei-Faktor-Authentifizierung schützt Sie.

Auch für Ihr E-Mail-Konto: Schalten Sie in den Einstellungen Ihres E-Mail-Kontos unter „Sicherheit“ die Bestätigung in zwei Schritten ein und wählen Sie den Code per SMS. Wenn sich jemand auf einem fremden Gerät in Ihr E-Mail-Konto will, braucht er dann zusätzlich den Code, der jedoch nur auf Ihrem Handy ankommt.

Für Geübte: Statt der SMS gibt es eigene Apps, die solche Codes erzeugen (Authenticator-Apps). Sie sind noch sicherer, aber etwas aufwendiger einzurichten.

Und was ist mit Passkeys?

Passkeys sind die moderne Passwort-Alternative. (Die Stiftung Warentest erklärt das online sehr gut. Suchen Sie unter www.test.de nach dem Stichwort *Passkey*.) Sie lassen sich im Erbfall – Stichwort „Digitales Erbe“ – aber schwerer weitergeben als Ihre Passwort-Sammlung.

Die wichtigste Regel

Codes und Passwörter gibt man niemals weiter. Nicht am Telefon, nicht per SMS, nicht per Mail, nicht per WhatsApp. Auch nicht an die „Bank“, die „Polizei“ oder den „Enkel“. Nur Betrüger fragen danach.

Das nehme ich mir vor

☐ Eigenes, langes Passwort für mein E-Mail-Konto
☐ Eigenes, langes Passwort für mein Apple- oder Google-Konto
☐ Eigenes, langes Passwort für meine Bank
☐ Passwörter ins Notizbuch oder in den Passwortmanager eingetragen

TIPP: Wenn Sie unabhängig von Google und Apple Ihre Passwörter digital verwalten wollen, installieren Sie einen Passwort-Manager wie **Proton Pass**. Dieser bietet einen kostenlosen Free-Tarif.