Tipps zum sicheren Passwort

Starke Passwörter …

… **helfen**, deine Identität und persönlichen Daten zu schützen.

… **verhindern** den ungewollten Zugriff auf deine privaten Nachrichten, Fotos und Dateien.

… **bewahren** dich vor finanziellen Schäden durch Online-Betrug.

… **schützen** dich vor unangemessenen oder peinlichen Inhalten, die z.B. andere in deinem Namen posten könnten.

Starke Passwörter sind der Schlüssel zum Schutz deiner persönlichen Daten und Online-Konten.

Besonders wenn du mit Apps oder mittels Online-Banking zahlst oder oft Social Media und Online-Dienste nutzt, solltest du auf starke Passwörter achten. So machst du es Hackern schwerer, deine Konten zu knacken.

So wird's sicher!

Dies sind wichtige Merkmale, die ein sicheres Passwort ausmachen:

Länge: Je mehr Zeichen, umso sicherer!

Kombination: Wähle eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.

Einzigartigkeit: Verwende möglichst kein Passwort mehrfach – v.a. bei sensiblen Aktivitäten (z.B. Online-Banking) und bei unterschiedlichen E-Mail-Konten.

Unvorhersehbarkeit: Vermeide einfache Muster, gebräuchliche Wörter oder persönliche Informationen wie Geburtsdaten.

Komplexität statt regelmäßige Aktualisierung: Wähle ein komplexes, langes Passwort statt regelmäßig leicht zu merkende Passwörter zu ändern.

Druckprodukt mit finanziellem Klimabeitrag
ClimatePartner.com/15064-2009-1001

Nützliches Tool: Der Passwortmanager

Vorteile

- Einfache Verwaltung komplexer Passwörter
- Erhöhte Sicherheit durch Verschlüsselung
- Zeitersparnis durch automatisches Generieren von Passwörtern
- Du musst dir nur ein Passwort – das Master-Passwort – merken.

Nachteile

- Abhängigkeit vom Master-Passwort
- Sicherheitsrisiken bei Cloud-Diensten – besser: Programm nutzen, das man am PC installiert.

Tipps zum Master-Passwort

- Verwende als Master-Passwort ein sicheres Passwort, das die wichtigen Merkmale erfüllt (siehe Kasten links in Pink).
- Um es dir gut merken zu können, kannst du dir auch einen längeren Satz inkl. Satzzeichen, Groß- und Kleinschreibung sowie einer Zahl ausdenken, z.B.: Gibtesum12UhrMittagessen? Dann verwendest du nur die Anfangsbuchstaben daraus als Master-Passwort: Geu12UM?
- So kannst du es auch bei anderen Passwörtern machen.

Zusätzliche Sicherheit:

- Nutzung biometrischer Sperre auf dem Smartphone (z.B. Fingerabdruck)
- 2-Faktor-Authentifizierung aktivieren
- Regelmäßige Backups: Gespeicherte Passwörter regelmäßig offline sichern, um deren Verlust bei Verlust des Master-Passworts zu vermeiden.

Extra sicher – so geht's!

- Die **Zwei-Faktor-Authentifizierung** (2FA) ermöglicht einen zusätzlichen Sicherheitsschritt: Zusätzlich nach dem Passwort wird ein Code verlangt, den du per SMS oder App erhältst.
- Die **biometrische Entsperrung** (z.B. per Fingerabdruck) am Handy lässt dich weniger oft dein Passwort öffentlich eingeben.

Zusätzliche Tipps:

- **Verdecke deine Eingabe bei Bankautomaten und Handy-Entsperrung** – damit niemand deine PIN sieht.
- **Überprüfe regelmäßig deine Konten** auf verdächtige Aktivitäten und ändere deine Passwörter sofort, wenn du einen Verdacht hast.
- **Behalte deine Passwörter stets für dich.**
- Halte dein Betriebssystem und alle Apps **auf dem neuesten Stand**, um Sicherheitslücken zu schließen.
- Nutze **kein öffentliches WLAN** oder nur in Verbindung mit einem **VPN** für sensible Aktivitäten (z.B. Online-Banking), da diese oft unsicher sind.

BLM
Bayerische Landeszentrale für neue Medien
Heinrich-Lübke-Str. 27 | 81737 München
www.blm.de

Weitere Informationen:

Sicher online unterwegs

BLM-Materialien