BLM
Bayerische Landeszentrale für neue Medien

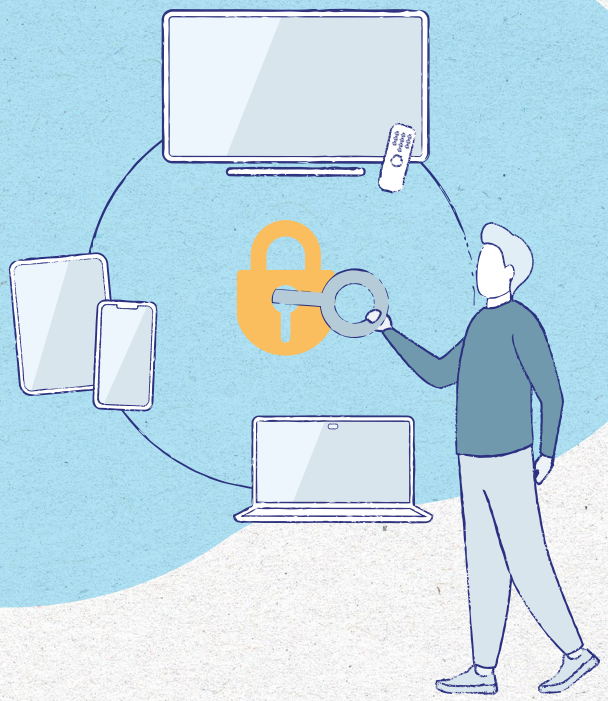
Kompetenz stärken.
Vertrauen schaffen.

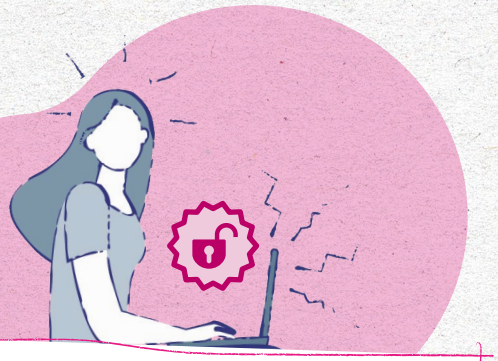
Tipps zum sicheren Passwort

Unsere Haus- und Autotüren zu verschließen ist für uns selbstverständlich. So kann nichts entwendet werden. Warum sollten wir wichtige und sensible Informationen online nicht genauso schützen? Online-Banking-PINs, Fotos der Familie oder die Kontaktdaten unserer Lieben sind auch wichtig.

Deshalb lohnt es sich, Sicherheitsvorkehrungen zu treffen. Dazu gehören sichere Passwörter. In diesem Flyer geben wir Tipps dazu, wie man Passwörter sicher gestaltet und wie man mit ihnen umgeht.

Dr. Thorsten Schmiege
Präsident der Bayerischen Landeszentrale für neue Medien (BLM)





Absolute Sicherheit …

… gibt es nicht. Aber mit den Strategien aus diesem Flyer können Sie Ihre Daten gut schützen. Selbstdatenschutz ist wichtig, weil Ihre persönlichen Informationen in den falschen Händen zu

- Identitätsdiebstahl,
- finanziellen Verlusten und
- anderen schwerwiegenden Problemen

führen können.

Indem Sie Ihre Daten schützen, bewahren Sie Ihre Privatsphäre und verhindern, dass Unbefugte Zugriff auf Ihre sensiblen und wichtigen Informationen erhalten.

IMPRESSUM

Herausgeberin
Bayerische Landeszentrale für neue Medien (BLM)
Heinrich-Lübke-Str. 27
81737 München
info@blm.de

Verantwortlich
Kerstin Prange, BLM

Redaktion
Dr. Kristina Hopf, Mara Gibis, BLM

Autoren der Ausgangsbroschüre
Dr. Olaf Selg, Dr. Daniel Hajok, AKJM

Gestaltung
Theresa Fischer

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

Tipps zum sicheren Passwort

Starke Passwörter ...

... **helfen,** Ihre Identität und persönlichen Daten zu schützen.

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

... **bewahren** Sie vor finanziellen Schäden durch Online-Betrug.

... **schützen** Sie vor unangemessenen oder peinlichen Inhalten, die z.B. andere in Ihrem Namen posten könnten.

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

Besonders wenn Sie mit Apps oder mittels Online-Banking zahlen oder oft Social Media und Online-Dienste nutzen, sollten Sie auf starke Passwörter achten. So machen Sie es Hackern schwerer, Ihre Konten zu knacken.

So wird's sicher!

Dies sind wichtige Merkmale, die ein sicheres Passwort ausmachen:

Länge: Je mehr Zeichen, umso sicherer!

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

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

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

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

Nützliches Tool: Der Passwortmanager

Vorteile

- Einfache Verwaltung komplexer Passwörter
- Erhöhte Sicherheit durch Verschlüsselung
- Zeitersparnis durch automatisches Generieren von Passwörtern
- Sie müssen sich nur ein Passwort – das Master-Passwort – merken.

Nachteile

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

Tipps zum Master-Passwort

- Verwenden Sie als Master-Passwort ein sicheres Passwort, das die wichtigen Merkmale erfüllt (siehe Kasten links in Pink).
- Um es sich gut merken zu können, können Sie sich auch einen längeren Satz inkl. Satzzeichen, Groß- und Kleinschreibung sowie einer Zahl ausdenken, z.B.: Gibtesum12UhrMittagessen? Dann verwenden Sie nur die Anfangsbuchstaben daraus als Master-Passwort: Geu12UM?
- So können Sie 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 Sie per SMS oder App erhalten.
- Die **biometrische Entsperrung** (z.B. per Fingerabdruck) am Handy sorgt dafür, dass Sie weniger oft Ihr Passwort eingeben müssen.

Zusätzliche Tipps:

- **Verdecken Sie Ihre Eingabe bei Bankautomaten und Handy-Entsperrung** – damit niemand Ihre PIN sieht.
- **Überprüfen Sie regelmäßig Ihre Konten** auf verdächtige Aktivitäten und ändern Sie Ihre Passwörter sofort, wenn Sie einen Verdacht haben.
- **Behalten Sie Ihre Passwörter stets für sich.**
- Halten Sie Ihr Betriebssystem und alle Apps **auf dem neuesten Stand**, um Sicherheitslücken zu schließen.
- Nutzen Sie **kein öffentliches WLAN** oder nur in Verbindung mit einem **VPN** für sensible Aktivitäten (z.B. Online-Banking), da diese oft unsicher sind.

Weitere Informationen:

Sicher online unterwegs

BLM-Materialien

www.blm.de