Passwörter sicher gestalten

Ein **sicheres Passwort** schützt vor unbefugtem Zugriff auf sensible Daten und Geräte. Sichere Passwörter sind lang (mind. 8-12 Zeichen) und komplex (Mix aus Klein- und Großbuchstaben, Sonderzeichen und Zahlen). Echte Wörter, gängige Zahlen- oder Buchstabenfolgen und persönliche Daten sind ungeeignet.

Aus einem Satz wird aus Anfangsbuchstaben, Zahlen und Sonderzeichen ein Passwort gebildet. „Montag ist vier Stunden Training – aber nur für Mitglieder!“ wird zum Passwort **Mi4ST-anfM!**

Passwörter sollten nie mehrfach verwendet werden. Damit man sich nicht für jedes Konto ein Passwort merken muss, gibt es **Passwort-Manager**, die Passwörter generieren und automatisch ausfüllen. Einige Geräten haben diese Funktion integriert, es gibt aber auch externe Programme.

Weitere hilfreiche Tools zur digitalen Sicherheit finden sich im Infopool von digital verein(t): **www.digital-vereint.de/infopool/**

digital verein(t) bietet zudem Workshops, eine Beratungssprechstunde und Handbücher zu Sicherheit im Netz und vielen weiteren Themen an. **www.digital-vereint.de**

@digitalvereint

@digitalvereint

Herausgeber: Landesarbeitsgemeinschaft der Freiwilligenagenturen/ -Zentren/ Koordinierungszentren Bürgerschaftlichen Engagements Bayern e.V. (lagfa bayern e.V.), Projekt digital verein(t)
Projektpartner: Deutschland sicher im Netz e.V. (DsiN)
1. Auflage 2024, Redaktion: Melissa Elbl, Leonore Lukschy

Gefördert durch

Bayerisches Staatsministerium für Digitales

Ein Projekt von

lagfa bayern

In Zusammenarbeit mit

DsiN Deutschland sicher im Netz

digital verein(t)

digital verein(t) – online, aber sicher!
Grundlagen für Engagierte, Ehrenamt und Vereine

Sicher im Netz:
Passwörter, Suchmaschinen und WLAN

Eine sichere Verbindung ins Internet

Jedes WLAN sollte mit **WPA3** und einem **Passwort** verschlüsselt sein. Ein **Gäste-WLAN-Zugang** bietet sich bei größeren Veranstaltungen an, damit nur bestimmte Personen Zugriff auf das Heimnetzwerk haben.

Sensible Daten, z. B. bei Bank Log-ins, sollten nur verschlüsselt **(https)** und nicht über öffentliche Verbindungen wie das BayernWLAN verschickt werden. Wenn kein gesichertes WLAN verfügbar ist, sollte man lieber auf mobile Daten umsteigen oder einen **VPN** (Virtual Private Network) Client nutzen.

Webbrowser und Programme sollten nur von **vertrauenswürdigen Quellen** wie offiziellen App Stores oder dem Anbieter der Software heruntergeladen werden. Bei Links, die über Messengerdienste oder SMS zugeschickt werden, ist Vorsicht geboten.

Computer und Daten schützen

Regelmäßige Updates von Betriebssystemen, wie Computer, Router oder Drucker, und Softwares schließen entstandene Sicherheitslücken. Am besten richtet man automatische Updates ein.

Eine Firewall ist bei den meisten Geräten schon vorinstalliert. Ein **Anti-Viren-Programm** schützt vor schädlicher Software aus dem Internet – sogenannter Malware. Dabei werden nicht nur Webseiten, sondern auch E-Mails und ihre Anhänge untersucht.

Ein **Adblocker** verhindert, dass Werbung Dritter in Form von Bannern oder Pop-Ups auf einer Webseite angezeigt wird. Er verhindert auch das Anzeigen von Bildern oder Videos, die oft automatisch auf potenziell schädliche Seiten weiterleiten.

Datenschutz

Der beste Schutz von Daten ist, sie nur sparsam im Internet preiszugeben. Daher sollten der **Verlauf** und **Cache-Speicher** des Browsers regelmäßig gelöscht oder der **Inkognito-Modus** verwendet werden. Bei manchen Anbietern kann man die E-Mail-Adresse bei der Nutzung von Onlinediensten verbergen. So bleibt diese privat.

Einige Browser haben integrierte Tools, wie eine Tor-Unterstützung, einen VPN-Client oder bieten die Option mehrere Profile anzulegen, die dabei helfen, anonym und sicher zu surfen.

Ein **Tracking-Blocker** verhindert, dass seitenübergreifend Daten über die Internetnutzung einer einzelnen Person gesammelt werden. Blocker lassen sich als Add-ons oder Plug-ins in den Browser integrieren.

Ob am Computer oder Smartphone: Man sollte immer kritisch überprüfen, welche **Zugriffsrechte** Apps und Programme auf Geräte und Daten haben. Zugriffe, die nicht für die Funktionalität der App erforderlich sind, sollten abgelehnt werden.

Sicher genug?

Zusätzlichen Schutz im Netz bieten auch **Zwei-Faktor-Authentifizierung** und **Ende-zu-Ende-verschlüsselte** Online-Kommunikation. Natürlich gibt es noch mehr Maßnahmen, um sich im Netz abzusichern.