

Passwörter & Datenschutz

Sicher. Clever. Gemeinsam digital

Orientierung für Familien, Schulen und Lehrkräfte.



Passwörter, die wirklich schützen

- Für jedes Konto ein eigenes Passwort verwenden - keine Wiederverwendung.
- Je länger, desto besser: mindesten 8 Zeichen, Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen.
- Keine Namen, Geburtstage, logische Wörter oder einfache Muster wie 123456 oder qwertz.
- Wenn möglich Zwei-Faktor-Authentifizierung (2FA) aktivieren; Passkeys nutzen, wenn sie angeboten werden.
- Passwörter und BestätigungsCodes niemals per Chat, E-Mail oder Telefon weitergeben!

Hat sich was geändert?
Sofort aktualisieren!

Zugangsdaten dokumentieren

- Zugangsdaten aufschreiben: oft ist schon nach kurzer Zeit unklar, mit welcher E-Mail-Adresse oder welchem Benutzernamen ein Konto angelegt wurde.
- Passwortmanager oder ein festes Zugangsdaten-Heft nutzen: Dienst, Login-E-Mail bzw. Benutzername, Passwort und Wiederherstellungsdaten notieren.
- Neue E-Mail-Adresse oder Telefonnummern sofort ergänzen; ein Notizheft sicher zuhause verwahren.

Datenschutz: weniger ist mehr

- Vor jeder Anwendung fragen: Welche Angaben sind WIRKLICH notwendig?
- Profile möglichst privat einstellen; Standort und Kontakte nur freigeben, wenn die Funktion sie wirklich braucht.
- Adresse, Schule, Telefonnummer, Geb.datum und tägliche Routinen nicht unnötig öffentlich teilen.
- Fotos/Videos anderer Personen nicht ohne Zustimmung veröffentlichen oder weiterleiten.
- Bei unbekannten Links oder Formularen niemals Zugangsdaten eingeben.

Virenschutz & Gerätesicherheit

- Virenschutz und Firewall - sofern sinnvoll - installieren und regelmäßig updaten (oft im System schon integriert).
- Betriebssystem regelmäßig Updates installieren (automatischer Update).
- Browser und Apps möglichst zeitnah updaten, damit bekannte Sicherheitslücken geschlossen werden können.
- Unbekannte Links, Anhänge oder Downloads nie unüberlegt öffnen!
- Vorsicht auch bei Spielen, kostenlosen Downloads oder Nachrichten - diese enthalten oft Schadprogramme.

Wenn etwas schiefgeht

2FA - zweifach sicher!

- Passwort vergessen? Nur die offizielle Funktion des Dienstes zur Wiederherstellung nutzen.
- Verdacht auf Diebstahl oder Datenleck: Passwort sofort ändern - auch überall dort, wo es nochmals verwendet wurde.
- 2FA prüfen und aktivieren, unbekannte Geräte bzw. Sitzungen abmelden und Passwörter erneuern.
- Das E-Mail-Konto besonders schützen: Darüber lassen sich oft andere Konten zurücksetzen.
- Bei Kindern sollten Eltern die wichtigsten Accounts, Login-Adressen und Wiederherstellungswege mit im Blick haben und sich die Zugangsdaten auf jeden Fall auch notieren.
- Machen Sie regelmäßig Backups Ihrer Daten - für den Fall der Fälle geht Ihnen dann nichts verloren.

Mit wenigen einfachen Einstellungen und klaren Regeln begleiten Sie Ihr Kind wirksam auf seinem Weg durch die digitale Welt. Wir helfen Ihnen dabei.

www.computermäuseverein.de