1. Sicheres Login!

Passwörter wie abcd1234! taugen nichts. Spickzettel unter dem Mousepad und Post-it am Bildschirm sind fahrlässig.

2. Geräte nur ausgeloggt verlassen!

Dazu gibt es praktische Tastenkombinationen.

3. E-Mail-Absender*in unbekannt?

Zweifelhafte Nachrichten nie öffnen. Vor allem deren Anhänge sind tabu. Bei Unsicherheiten den Informatiksupport kontaktieren.

4. Kritische Ereignisse?

Fehlermeldungen und andere unerwartete Programmantworten sowie (fragliche) Anwender*innen-Fehler mit Folgen müssen sofort gemeldet werden.

5. Streng geheim!

Geräte mit Personendaten oder Zugang dazu müssen sehr sorgfältig aufbewahrt und unterwegs ständig überwacht werden. Persönliche Arbeitsnotizen werden sofort nach Eintrag gesetzeskonform vernichtet.

6. Wann findet die nächste Datenschutzübung statt?

Die Risiken im Umgang mit elektronischen Daten sind inzwischen ebenso gross wie die von Bränden, Unfällen oder Naturereignissen. Das erfordert regelmässige Schulungen mit praktischen Übungen. Fragen Sie Ihre Informatik-Abteilung.