SICHERHEIT IM INTERNET

Durch **Sicherheitslücken** im System von Computern oder mobilen Endgeräten können Angriffe auf diese Geräte, sogenannte Cyber-Angriffe, erfolgen und Fremde ...

- ... Patente abgreifen
- ... sensible Daten (z. B. Passwörter und Bankdaten) klauen
- ... Nutzende mit der Veröffentlichung persönlicher Daten erpressen

Schutz vor Hacker-Angriffen

- Installation eines aktuellen Virenscanners auf Computern, Smartphones, Tablets etc.
- sichere Passwörter für alle Konten errichten
  - » Passwort mit mindestens 13 Zeichen aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen erstellen
  - » Namen, Hobbies und einfache Zahlenfolgen als Passwort vermeiden
  - » pro Konto und Internetseite jeweils unterschiedliche Passwörter verwenden
  - » Passwörter an einem sicheren Ort aufbewahren und niemals an Fremde weitergeben
  - » Passwortgeneratoren nutzen
- Plausibilitätsüberprüfung
  - » vor jeder Passwort- und Dateneingabe sollte die Plausibilität von Seite oder Absender_in überprüft werden
  - » bei Bestellungen im Internet sollten Onlineshops auf ihre Seriosität hin kontrolliert werden
- Einrichtung einer verschlüsstelten WLAN-Verbindung
  - » Auswahl eines neutralen Namens für das Netzwerk
  - » sicheres Passwort als WPA-Schlüssel erstellen

Andere Personen schützen

- persönliche Aufklärung über Gefahren im Internet
- Vermittlung eines verantwortungsbewussten Umgangs mit dem Internet

Was bedeutet das für die Praxis?

- WLAN-Netzwerk der Arbeitsstätte schützen
- Menschen mit sogenannter geistiger Behinderung über Sicherheitsrisiken im Internet aufklären
- sichere Passwörter verwenden