Informationssammlung über IT-Sicherheit für den privaten Bereich.

- **Mobile Datenträger**
  - Mobile Datenträger sind z.B.: Notebooks, PDA´s, Mobiltelefone, Speicherkarten, USB-Speichermedien, externe Festplatten, DVD,…
  - Der Verlust mobiler Datenträger stellt oft ein erhebliches Sicherheitsrisiko dar.
  - Die Datenmenge die dabei verloren gehen kann, sei am Beispiel eines 8 GB-USB-Sticks dargestellt: auf solch einem Datenträger finden etwa 80000 Word-Dokumente von durchschnittlicher Größe (etwa 100kB) platz.
  - Materieller und finanzieller Schaden meist vernachlässigbar, aber der unwiederbringliche Datenverlust ist es oft nicht.
- **Schutz**:
  - Autorun/Autoplay-Funktion deaktivieren (Schutz vor häufigen Schadprogrammen die mittels portabler Datenträger übertragen werden können.)
  - Transportsicherung (nach Möglichkeit am Körper tragen und nicht unbeaufsichtigt lassen.
  - Überblick bewahren: Datenbestand so gering wie möglich halten, nicht benötigte Daten löschen.
  - Schutzmechanismen verwenden: Verschlüsselung verwenden
  - Einsatz planen: Äußere Einflüsse (Hitze, Nässe,…)
  - Vor dem Verbinden mit Netzwerken prüfen, ob diese Vertrauenswürdig sind. (Daten könnten kopiert oder manipuliert werden.)
- **Mobiltelefone**
  - Mobiltelefone sicher verwahren, am besten immer am Körper tragen.
  - PIN-Code-Abfrage auf jeden Fall aktivieren
  - Tastensperre mit Code-Funktion verwenden
  - Bei **SMS** grundsätzlich keine eingebetteten URL öffnen.
  - Bei **MMS** Datenempfang von fremden Personen grundsätzlich ablehnen.
  - Updates von einem „sicheren“ Arbeitsplatzrechner ausführen. Vorher Datensicherung!
  - Vor der Installation von Apps, diese genau prüfen.
  - Internet auf Mobiltelefonen nur bei entsprechender Sicherheitssoftware verwenden.
  - **E-Mails**:
    - Sollten nur dann heruntergeladen werden, wenn sie aus vertrauenswürdiger Quelle stammt. Dateianhänge nach Möglichkeit nicht herunterladen, wenn dies unvermeidbar ist, dann sollte das nur bei vorhanden sein von Sicherheitssoftware, getan werden.
  - **Bluetooth**:
    - Bluetooth-Funktion nur bei einem tatsächlichen Bedarf aktivieren.
    - Sichtbarkeit des Telefons unterbinden
    - Bluetoothname sollte keine Rückschlüsse auf den Besitzer oder den Betreiber zulassen.
    - Keine automatischen Datenübertragungen und Pairingvorgänge zulassen.
  - **Infrarotübertragung**:

- Nur zum unmittelbaren Datenaustausch aktivieren.

- **WAP**:
  - Drittanbieterberechtigungssperre aktivieren
- **GPS**:
  - Nur bei Bedarf verwenden. Spart außerdem Strom.
- Sonstige Schnittstellen sollten ebenfalls nur bei Bedarf aktiviert werden.