Infoveranstaltung Piraten Rüsselsheim – Meine Daten/Sicherheit im World Wide Web

- Social Networks (MeinVZ, Facebook, WKW)
  - Grundsätzlich sind alle angegeben Daten öffentlich
  - Einschränkungen auf Portalen möglich (Wer kann Daten einsehen → Öffentlich [auch von außerhalb], innerhalb des Portals, nur Freunde, Niemand?!)
  - Arbeitgeber nutzen Portale um Bewerber im Vorfeld zu prüfen
  - Mitschüler/Mitarbeiter können Daten gegen eine nutzen (komprimierende Fotos, Aussagen in Foren/Gästebüchern)
  - Sparsam mit seinen Daten umgehen, so wenig wie möglich reale Daten angeben → Synonym verwenden
  - Profileinsicht einschränken
  - Gesundes Misstrauen an den Tag legen
  - Nicht jeden als „Freund" akzeptieren um Zugriff auf Profil zu ermöglichen
  - Keine Daten von anderen Menschen preisgeben, wenn sie es nicht wollen (z.B. Facebook-Sync mit Postfach oder Handy)
  - Folgen: Spam, Abweisungen bei Bewerbungen, Mobbing, Erpressung, Jugendsünden (Maxime: Was einmal im Netz ist, bleibt im Netz!)
  - Man sollte sich so darstellen wie es vertretbar ist und man die eventuellen Folgen abschätzen kann
- Google (Googlemail, etc. → Verknüpfungen)
  - Welche Dienste stellt Google, wie sind sie miteinander verknüpft?
- Cookies (Rückverfolgung über Cookies)
  - Was sind Cookies, wozu werden sie genutzt, wozu können sie auch genutzt werden?
- Kreditkartendaten (Welchen Webshops kann ich trauen, Was sollte man beachten)
  - Vertrauenswürdigkeit der Webshops im Vorfeld prüfen
  - Regelmäßig Kreditkartenumsätze prüfen (wöchentlich) und bei Auffälligkeiten sofort reagieren
  - Auch hier generell sparsam sein (Unternehmen verlieren gerne auch mal die Kundendaten inkl. Bankdaten)
- Trojaner/Viren (Keylogger, Botnetze, Datenverlust, Datenabzweigung)
  - Wie kommen Schadprogramme auf meinen PC
  - Was machen sie?
  - Woran erkenne ich sie, wie kann ich verhindern, dass sie auf meinem System landen?)
- Sicherung des eigenen Routers (WPA2 Verschlüsselung, MAC Filter, Firewall, Port Forwarding etc.)
  - Provider liefern Router mit unsicheren Werkseinstellungen (entweder keinerlei Sicherheit eingestellt oder aber bekannte Standardeinstellungen)
  - Was muss man konfigurieren um sich abzusichern?
  - Was kann passieren wenn die Einstellungen unsicher sind?
- Richtige Browserwahl
  - Browserauswahl vorstellen (Vorteile, Nachteile, etc.
- Updates des Betriebssystems, Updates sämtlicher Software, Software-Firewalleinstellungen
  - Warum man immer up to date sein sollte
- Mailsystem → Spam, hoax mails
- Phishing, Social Enginnering
- Sichere Passwörter (zur Erinnerung in Tools wie Pins 2.0)