Verschlüsseln - Warum?

Alexander Skiba - Cryptoparty #1 - spektral, Graz

Aktueller Stand?

Szenario 1

- WLAN, Studentenheim
  - Mail auf unverschlüsseltem Server
  - Kann per Software mitgelesen werden
- Problem: Credentials, Cookies

Szenario 2

- WLAN, Studentenheim, die zweite
  - Unterhaltung über Chat
    - Kann mitgelesen werden - und Unterhaltung gefälscht!
  - Problem: Privatsphäre

Du denkst du bist sicher?

- 3G: abgefangen
- WLAN: teils schwach oder gar nicht verschlüsselt
- Ethernet: Angreifer vielleicht bereits im Netz
- Passwörter: zu oft zu schwach oder notiert

Abhilfe

- Verschlüsselung
  - Mail → Lukas' Vortrag
  - Chat → Informationen bei mir
  - Passwörter → zufällig erstellt (Keypass, 1Password)

Einstieg

- Twitter: @ghostlyrics (Alexander Skiba)
- Hashtag der Veranstaltung: #cpg1