

# DIGITAL SIKKERHED – METODER OG VÆRKTØJER

## Introduktion

At øge din digitale sikkerhed handler om at anvende effektive metoder og værktøjer for at beskytte dine enheder, data og online aktiviteter. Det kan sammenlignes med at opgradere sikkerhedssystemet i dit hjem med bedre låse, alarmer og overvågning.

### 1. To-faktor Autentificering (2FA)

- Hvad: En sikkerhedsmetode, der kræver to forskellige former for identifikation for at få adgang til en konto.
- Hvorfor: Giver et ekstra lag af sikkerhed, selv hvis dit password bliver kompromitteret.
- Hvordan:
  - Indtast dit normale password.
  - Bekræft din identitet med en anden metode (f.eks. en kode sendt til din telefon eller genereret af en app).

Eksempel: Når du logger ind på din netbank, skal du både bruge dit password og en engangskode sendt til din t

### 2. Anti-malware Software

- Hvad: Programmer designet til at opdage, forhindre og fjerne skadelig software fra dine enheder.
- Hvorfor: Beskytter dine enheder mod virus, spyware, ransomware og andre former for malware.
- Hvordan:
  - Installer et pålideligt anti-malware program (f.eks. Norton, McAfee, Bitdefender).
  - Hold programmet opdateret med de nyeste virusdefinitioner.
  - Kør regelmæssige scanninger af dine enheder.

Eksempel: Dit anti-malware program opdager og blokerer et forsøg på at installere en trojansk hest, der kom med en e-mail-vedhæftning

### 3. Virtual Private Network (VPN)

- Hvad: Et værktøj, der skaber en krypteret tunnel mellem din enhed og internettet.
- Hvorfor: Skjuler din IP-adresse og krypterer din internettrafik, hvilket øger din online privatliv og sikkerhed.
- Hvordan:
  - Vælg en pålidelig VPN-udbyder.
  - Installer VPN-softwaren på dine enheder.
  - Aktivér VPN'en, især når du bruger offentlige Wi-Fi netværk.

Eksempel: Når du bruger en café's Wi-Fi med en VPN aktiveret, kan caféejeren eller andre gæster ikke se eller påvirke din internettrafik.

### 4. Password Managers

- Hvad: Software, der sikkert opbevarer og administrerer dine passwords.
- Hvorfor: Gør det muligt at bruge unikke, komplekse passwords til alle dine konti uden at skulle huske dem.
- Hvordan:
  - Vælg en pålidelig password manager (f.eks. LastPass, 1Password, Bitwarden).
  - Opret et stærkt master-password til din password manager.
  - Lad password manageren generere og gemme unikke passwords for hver af dine konti.

Eksempel: I stedet for at bruge "Password123" overalt, kan du have komplekse passwords som "X9f\$p2Kl@mN7" for hver konto, men du skal kun huske ét master-password.

## Opsummering

Metoder og værktøjer til øget digital sikkerhed inkluderer:

1. To-faktor Autentificering: Tilføjer et ekstra lag af sikkerhed ved login.
2. Antivirus software: Beskytter dine data mod uautoriseret adgang.
3. VPN: Skjuler din online aktivitet og beskytter din data på usikre netværk.
4. Password Managers: Hjælper dig med at bruge og administrere stærke, unikke passwords.

Ved at implementere disse metoder og værktøjer kan du med god samvitighed forbedre din digitale sikkerhed