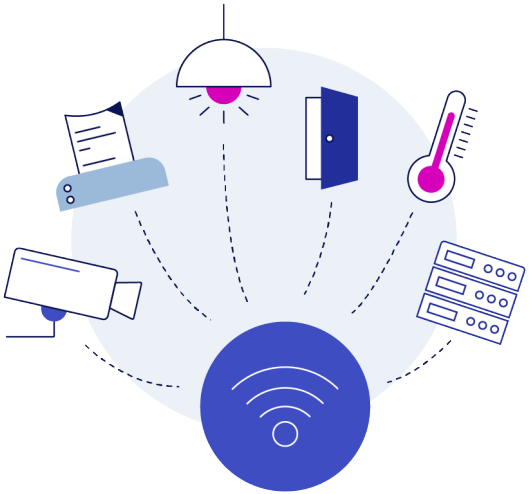
Har du sikret din smart-enhed mod hackere?

Dine smart-enheder er forbundet til internettet og omverdenen, derfor er de sårbare overfor hackerangreb. Hvis ikke enhederne er sikret, kan hackere få adgang til dine enheders funktioner og data, samt det netværk de er forbundet til.

1. **Skift adgangskode og brugernavn på enheden**
   Mange smart-enheder har standard adgangskoder og brugernavne, der kan være kendt af hackere. Det giver dem let adgang til enheden og det øvrige netværk.

2. **Slå automatisk opdatering til i enhedens indstillinger**
   Manglende opdateringer kan efterlade sikkerhedshuller, som giver hackere adgang til enheden og dermed resten af dit netværk.

3. **Slå enhedens internetadgang fra, når du ikke bruger det**
   Når enheden er forbundet til internettet, kan det potentielt give adgang til hackere.



FORBRUGERRÅDET tænk

sikker digital DK

DANSK ERHVERV

Rådet for Digital Sikkerhed

Hvad er en smart-enhed?

Betegnelsen ”smart-enhed” også kaldet ”Internet of Things” (IoT) bruges om hverdagsobjekter som fx lyskilder, køleskabe og kameraer, der er koblet til internettet og kan styres centralt (fx fra telefonen). De kan kommunikere automatisk med hinanden og med omverdenen.

Derfor skal din nye enhed sikres

Det er vigtigt, at du er opmærksom på sikkerheden, når du får nye smart-enheder og -gadgets. Alle dine smart-enheder, der er koblet på dit netværk, har forbindelse til internettet. I den forbindelse er de sårbare overfor digitale svindlere, der kan udnytte enhederne til at få adgang til dit øvrige netværk og enhedens funktioner og data.

Læs mere om digital sikkerhed i smart-enheder på sikkerdigital.dk

FORBRUGERRÅDET tænk

sikker digital DK

DANSK ERHVERV

Rådet for Digital Sikkerhed