# Sikkerhed i trådløse netværk

IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

IT- og Telestyrelsen
Holsteinsgade 63
2100 Kbh. Ø

Telefon 3545 0000
Telefax 3545 0010
E-post: itst@itst.dk
www.itst.dk

Rådet for it-sikkerhed
www.raadetforitsikkerhed.dk

# Beskyt dit trådløse netværk

Der findes ingen netværk, der er 100% sikre. Du kan dog foretage en række tiltag for at sikre dit netværk. Jo bedre du sikrer dit netværk, jo dyrere og mere tidskrævende bliver det for uvedkommende at skaffe sig adgang.
Du opnår altså, at det slet ikke kan betale sig for uvedkommende at skaffe sig adgang.
Ved at følge rådene i denne vejledning er det således muligt at opnå et rimeligt sikkerheds-niveau i dit trådløse netværk.

## Hvorfor skal jeg særligt beskytte mit trådløse netværk?

**Når netværket bruger radiobølger i stedet for kabler betyder det,**

**at uvedkommende nemmere kan få adgang til dine informationer**

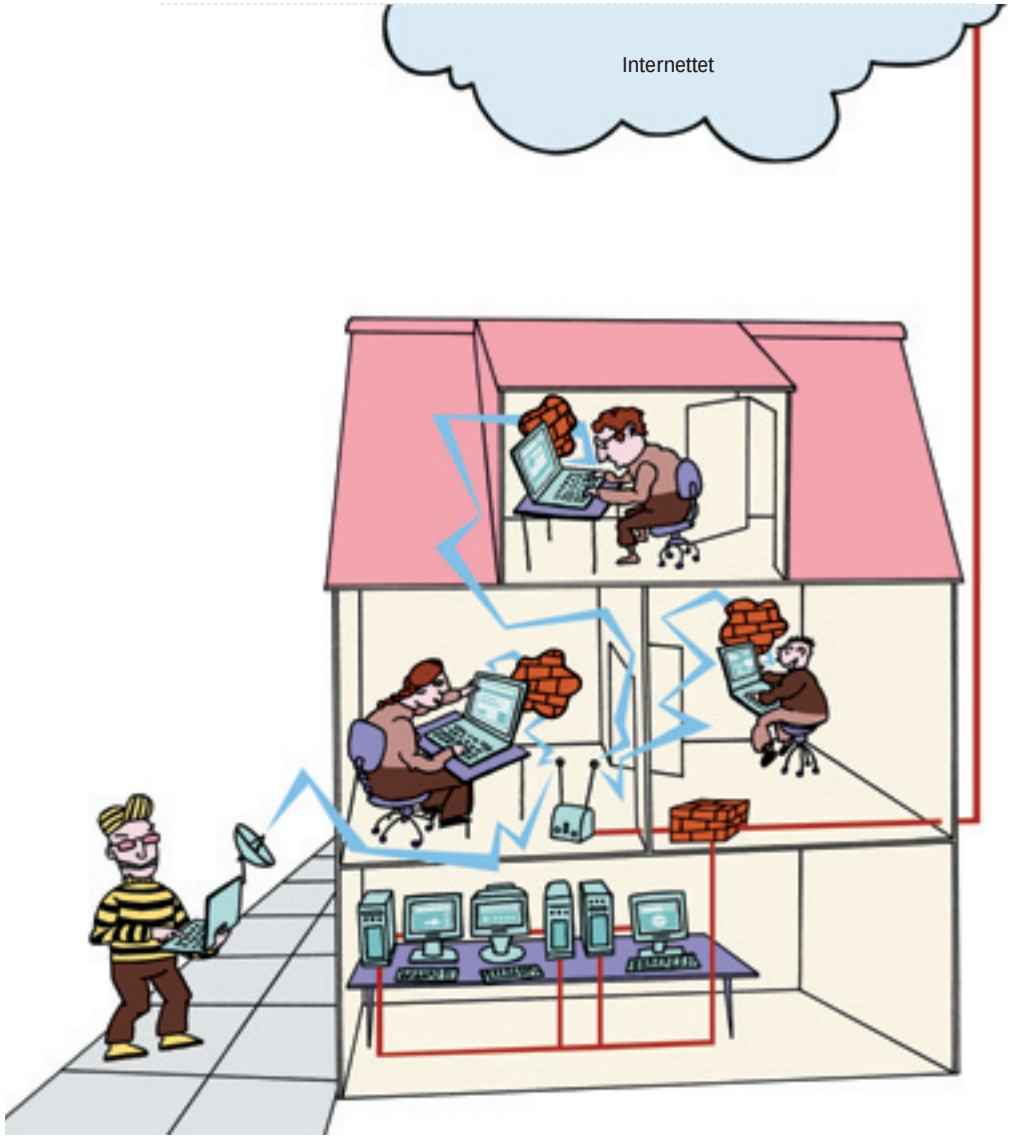
Et trådløst netværk - også kaldet WLAN - er et datanetværk, der bruger radiobølger til at sende og modtage data, hvor traditionelle datanetværk bruger kabler. Et trådløst netværk er derfor smart at bruge til bærbare computere, som ofte skal have adgang til netværket fra forskellige steder. Men det kan også være praktisk at undgå at skulle trække datakabler til faste PC'er.

Radiobølgerne fra et trådløst netværk i en bygning stopper imidlertid ikke ved bygningens mure, men fortsætter uden for. Enhver, der befinder sig uden for, kan derfor med ganske enkelt udstyr som en bærbar pc og en antenne modtage radiobølger fra dit trådløse netværk.

Med et særligt hackerprogram, som kan hentes på internettet, kan uvedkommende både se dine data og evt. ændre eller stjæle dem.

## Radiobølger kan aflyttes

Et trådløst netværk uden beskyttelse er meget usikkert. Uvedkommende kan uden videre aflytte og bruge dit trådløse netværk og ændre i din computer og dit trådløse netværk. De kan også bruge din computer til såkaldt 'bouncing'. Det betyder, at de kan bruge din computer til at foretage angreb på andre computere. Disse angreb vil kunne spores tilbage til dig!



# Lås dørene til dit trådløse netværk

## Hvordan kan jeg beskytte mit trådløse netværk?

For at modvirke at uvedkommende følger med i din kommunikation, er der en række forholdsregler, som du bør tage for at sikre dit trådløse netværk.

### Slå broadcastmeddelelser fra i dit trådløse netværk - hvis det er muligt

Mange hackerprogrammer finder et trådløst netværk ved at lede efter såkaldte broadcastmeddelelser, der sendes fra trådløse netværk. Broadcastmeddelelser er signaler fra det trådløse netværks basisstation, der udsender meddelelser om navnet på basisstationen (også kaldet SSID), datahastigheden i dit trådløse netværk, og om udvekslede data er krypterede eller ej. Hvis disse oplysninger opsnappes, kan hackere nemt og hurtigt koble sig på det trådløse netværk. Det er for det meste muligt at slå broadcastmeddelelser fra i det trådløse netværk. Herved gør du det sværere for hackere at finde og tilslutte sig dit netværk. Du og andre brugere skal så selv taste SSID og datahastighed ind i de PC'er, der skal have adgang til netværket.



<

### Husk at ændre standard password

Når du får dit trådløse netværk fra forhandleren, er det forsynet med et standard password. Det skal beskytte mod utilsigtede ændringer af opsætningen. Har du ikke ændret standard passwordet, har hackeren let ved at få direkte adgang til dit netværk. Ofte kender hackere nemlig de gængse standard passwords i trådløse netværk. I din virksomhed bør du overveje at ændre password'et regelmæssigt.

### Husk at ændre SSID

SSID er et navn på din basisstation. Hvis en ny bruger vil kobles på et trådløst netværk, skal han/hun bruge dets SSID for at få adgang.
I et åbent trådløst netværk sendes SSID'en i en broadcastmeddelelse. Herved kan nye brugere læse navnet på basisstationen. Leverandøren af dit trådløse netværk har givet det en standard SSID. Hackere kender alle standard SSID'er, så hvis du ikke ændrer din SSID, kan de let gætte sig til navnet og få adgang til netværket.
Du skal derfor vælge et SSID, der ikke er for nemt at gætte. Det bør ikke indeholde navn eller adresse på din virksomhed.

Selvom du følger ovennævnte sikkerheds-foranstaltninger, og derved gør det sværere for hackere at finde dit trådløse netværk, vil radiosignalerne stadig kunne modtages af andre. Derfor bør du ikke sende informationer, så de umiddelbart kan læses.

## Husk at slå kryptering til

## Husk at skifte krypteringsnøgle med jævne mellemrum

Du kan gøre dine data ulæselige for uvedkommende ved at kryptere dem. Data kan så kun læses ved at bruge den rigtige krypteringsnøgle - et langt ord eller tal. Når du køber et trådløst netværk, følger der normalt en kryptering med, som hedder WEP. Du skal selv aktivere WEP, og du bør altid sørge for at skifte den medfølgende krypteringsnøgle til en anden.
Desuden bør du skifte krypteringsnøglen med jævne mellemrum.



**Hvad med persondata og trådløse netværk?**

Hvis du håndterer personfølsomme data i dit trådløse netværk til erhvervsmæssig brug eller tænker på at gøre det i fremtiden, er der en række krav, du skal opfylde.
Hvordan du skal håndtere personfølsomme data er beskrevet i Persondataloven, som administreres af Datatilsynet (www.datatilsynet.dk). Datatilsynet forlanger bl.a., at der anvendes stærk kryptering, når der sendes personfølsomme data over åbne netværk. Hvad der er 'stærk kryptering' er afhængigt af teknologiudviklingen på det givne tidspunkt. WEP kryptering anses pt. ikke for at være sikker nok til at kunne betegnes som stærk kryptering.

## Overvej at bruge en stærkere kryptering

Ihærdige hackere kan godt bryde WEP kryptering og dermed læse data, du sender over dit trådløse netværk. Det kan derfor være nødvendigt med en stærkere kryptering for at holde dine data private.
Nogle leverandører tilbyder nu en ny krypteringsstandard (WPA). WPA er en mere sikker krypteringsform, men standarden er endnu ikke endelig godkendt.
Du kan allerede i dag benytte krypteringer som SSL (Secure Sockets Layer) eller IPSec.
Se www.webopedia.com. for nærmere information om stærk kryptering.

<

**Hvilken sikkerhed, du bør vælge, afhænger af værdien af de data, som du vil beskytte.**

### Overvej en firewall

En firewall er et program eller en hardwareenhed, der filtrerer og overvåger datastrømmen mellem flere netværk eller mellem en computer og et netværk. Internettet er usikkert, og forbindelsen hertil bør derfor filtreres med en firewall.
Et trådløst netværk er mindst lige så usikkert som internettet. Det anbefales derfor, at alle pc'er med adgang til det trådløse netværk beskyttes med en personlig firewall.
Hvis du både har trådløst og kablet netværk, bør disse også adskilles med en firewall.
Se tegning på side 5.

### Overvej at anvende MAC adresse filtrering

WLANkortet i din PC har et unikt identifikationsnummer, en såkaldt MAC adresse.
Ved kun at tillade specifikt angivne MAC adresser adgang til netværket afskæres alle andre fra at få adgang.
Dette giver en god sikkerhed mod hackere.
De MAC adresser, der skal have adgang til det trådløse netværk indkodes i det trådløse netværks basisstation.



# Sikkerheden i trådløse netværk

**Hvad med sikkerheden i fælles trådløse netværk eller trådløse netværk på offentlige steder?**

En række boligforeninger har valgt at deles om et trådløst netværk. På den måde undgår de en dyr og besværlig kabling af de tilsluttede boliger.

Du kan også finde trådløse netværk på offentlige steder i såkaldte 'hot spots'. Her tilbydes kunder i f.eks. lufthavne, hoteller, konferencecentre, caféer eller lignende trådløs internetadgang. Servicen kan enten være gratis eller den stilles til rådighed mod betaling.
Der kan være store forskelle på, hvor meget du betaler for at bruge et WLAN på offentlige steder.

Når du bruger et offentligt trådløst netværk, har du ingen indflydelse på sikkerhedsniveauet på netværket. På caféen eller hotellet er sikkerheden afhængig af, hvad ejeren af det trådløse netværk har indstillet netværket til. At tilslutte sig et offentligt trådløst netværk bør ikke betragtes som mere sikkert end at tilslutte sig internettet.
Du bør derfor anvende samme sikkerhedstiltag, som når du tilslutter dig internettet, f.eks. personlig firewall og antivirus beskyttelse på din PC.
Dernæst anbefales det at bruge kryptering, hvis du skal sende fortrolige data over det trådløse netværk.

## Hvad skal du ellers være klar over ?

Når du anskaffer et trådløst netværk og har foretaget de sikkerhedsmæssige tilpasninger, er der også andre forhold, du bør være opmærksom på:

**Forstyrrelser**

Det trådløse netværk, du normalt kan købe i dag, bruger frekvenser, der også bruges af mange andre forskellige typer apparater, bl.a. husholdningsudstyr og andet udstyr til datakommunikation. Sådant udstyr kan forstyrre dit trådløse netværk, hvis de to typer udstyr anvendes samtidig. Normalt er forstyrrelserne af kort varighed. Placer dit trådløse netværk så langt fra det forstyrrende udstyr som muligt.

**CE-mærke**

Dit trådløse netværk skal være CE-mærket. Leverandøren lover med CE-mærket, at dit trådløse netværk sender med den tilladte styrke og bruger de frekvenser, der er afsat til trådløst netværk. CE-mærket garanterer dog ikke mod forstyrrelser.

**Yderligere information**

For at få hjælp til hvordan du skal indstille dit trådløse netværk, så det sikres bedst muligt, skal du kontakte din leverandør. Der kan være forskel fra det ene WLAN-produkt til det andet, men din leverandør kan fortælle dig, hvordan lige præcis dit WLAN indstilles bedst muligt.



Nogle leverandører tilbyder også VPN, som kan hjælpe til at forbedre sikkerheden i dit trådløse netværk. Spørg din leverandør, hvad de kan tilbyde.

På internationalt plan arbejdes der på at gøre WLAN mere sikkert. WPA standarden er et resultat heraf.
IT- og Telestyrelsen følger med i udviklingen. Vi bringer således nyt på vores hjemmeside, når der er nye løsninger på markedet, eller når vi bliver bekendt med nye trusler mod trådløse netværk.

Hos IT- og Telestyrelsen vil du også kunne få andre råd om it-sikkerhed. Nyheder og nye vejledninger om it-sikkerhed offentliggøres løbende på

**www.itst.dk**

## Ordliste

| | |
|---|---|
| **Basisstation** | Basisstationen kaldes ofte for et 'access point' (AP) i manualer og salgsmateriale. Afstanden mellem din PC og AP skal typisk være mindre end 50 - 100 meter, for at du kan få forbindelse. |
| **Broadcast-meddelelse** | Oplysning fra et trådløst netværk om navn på basisstationen (SSID), datahastighed og kryptering. Nogle vejledninger bruger andre betegnelser som 'broadcast associations'. Spørg din forhandler, hvis du er i tvivl. |
| **Firewall** | En firewall er et program eller en hardware enhed, som regulerer og overvåger adgangen til og fra netværk, f.eks. internettet. |
| **Hacker** | Person, der uden tilladelse forsøger at trænge ind i et fremmed computernet. |
| **Kryptering** | At gøre data ulæselige ved at forvrænge dem. |
| **SSID** | Service Set Identifier (navnet på en basisstation) |
| **VPN** | Virtuelt Privat Net - en datatransmissionstjeneste, der inde i et andet net laver en virtuel datatunnel fra punkt til punkt for de tilsluttede brugere. |
| **WEP** | Wired Equivalent Privacy er den krypteringsprotokol, der bruges i de mest almindelige trådløse netværk. |
| **WLAN** | Wireless Local Area Network er en engelsk betegnelse for trådløse lokalnetværk. |
| **WPA** | Wi-Fi Protected Access - ny krypteringsstandard, der anvender dynamiske nøgler |



## Tjekliste

**Hvad du kan gøre for at øge sikkerheden i brugen af trådløse netværk**

- [ ] Slå broadcastmeddelelser fra
- [ ] Ændre standard password
- [ ] Ændre SSID
- [ ] Brug kryptering - skift WEP nøgler med mellemrum
- [ ] Overvej at installere en firewall
- [ ] Brug filtrering på MAC adresser, hvis det er muligt
- [ ] Brug stærk kryptering, hvis du behandler følsomme personoplysninger i dit WLAN. Undersøg Persondatalovens bestemmelser herom
- [ ] Er dit WLAN CE-mærket?

**Skal du installere et trådløst netværk - hjemme eller i virksomheden?**

**Har du allerede et trådløst netværk?**

**Har du tænkt du på datasikkerheden i dit trådløse netværk?**

Pjecen henvender sig til private og mindre virksomheder, der ønsker en trådløs internetforbindelse, ønsker at koble flere pc'er sammen i et netværk uden brug af kabler eller ønsker at udvide et datanet med et trådløst netværk.

## Sikkerhed - hvilke krav skal du stille?

Indenfor de sidste par år er trådløse netværk - også kaldet WLAN - blevet meget populære både på arbejdspladsen og i hjemmet. Samtidig har der været fokus på datasikkerheden i trådløse netværk. For signaler fra trådløse netværk kan nå helt ud på gaden, hvor uvedkommende med ganske enkelt udstyr kan opfange informationer fra netværket.
I værste fald kan uvedkommende få kontrol over din computer og eventuelt ødelægge data.

Ved at følge rådene i denne vejledning er det således muligt at opnå et rimeligt sikkerhedsniveau i dit trådløse netværk.

**IT- og Telestyrelsen**
www.itst.dk

**Rådet for it-sikkerhed**
www.raadetforitsikkerhed.dk