



Om trådlösa nät



Om trådlösa nät

Trådlösa nät för uppkoppling mot Internet är vanliga både i bostäder och på stan – till exempel på kaféer, hotell och flygplatser. I den här broschyren beskriver vi hur du kan höja säkerheten när du använder din dator eller mobiltelefon i trådlösa nät och svarar på följande frågor:

- **Vad är ett trådlöst nät?**
- **Vad är bluetooth?**
- **Vad ska jag alltid tänka på vad gäller säkerheten?**
- **Vad ska jag tänka på vad gäller säkerheten för trådlösa nät och bluetooth?**
- **Vad gör jag om det blir problem?**
- **Var kan jag få mer information?**

Den här broschyren innehåller inte information om mobilt Internet. Det kan du läsa om i broschyren som heter Om bredband.

Vad är ett trådlöst nät?

För att skapa ett lokalt trådlöst nät används oftast en enhet som innehåller både ett bredbandsmodem och en sändare/mottagare för trådlös kommunikation – en trådlös router. Ibland är bredbandsmodemet och den trådlösa routern två separata enheter som har kopplats ihop med en nätverkskabel.

Tack vare den trådlösa routern kan datorn kommunicera med Internet via

radiovågor. Det innebär att du kan använda Internet var du vill inom räckvidden för det trådlösa nätet, exempelvis vid köksbordet eller i tv-soffan. Räckvidden inomhus är vanligtvis 20-100 meter. Trådlösa nät kallas ibland för WLAN och Wi-Fi.

Privata trådlösa nät

Privata lokala trådlösa nät finns i hem och på arbetsplatser och är inte tillgängliga för alla. Ordet ”lokala” innebär att det är nät som bara täcker ett begränsat område. Vi kommer härnäst att kalla dessa nät för privata trådlösa nät.

Den som använder ett privat trådlöst nät har ofta möjlighet att påverka säkerheten genom att ställa in det på olika sätt.

Publika trådlösa nät

Publika lokala trådlösa nät finns på offentliga platser som hotell, restauranger, tågstationer och i centrala delar av städer. I resten av broschyren kallar vi dessa nät för publika trådlösa nät. Den här typen av nät kallas ibland för hotspots.

Publika trådlösa nät är tillgängliga för alla – gratis eller mot betalning. Den som använder sådana nät har ofta inga möjligheter att påverka säkerheten i själva nätet.

Vad är bluetooth?

Bluetooth är en teknik som ofta finns inbyggd i datorer och mobiltelefoner. Ibland används benämningen blåttand på svenska. Tekniken används för att trådlöst överföra information över korta avstånd, normalt ett tiotal meter, till och från exempelvis mobiltelefoner, datorer, tangentbord, skrivare, headset och mikrofoner. Till exempel kan bluetooth användas för att ansluta ett trådlöst headset till mobiltelefonen eller för att överföra filer mellan två mobiltelefoner.

Vad ska jag alltid tänka på vad gäller säkerheten?

Trådlös kommunikation är vanligtvis säker, men när du kopplar upp dig mot Internet med en dator eller en mobiltelefon finns det alltid en risk att du utsätts för virus eller andra skadligheter. Vi rekommenderar därför att du följer våra råd nedan. Läs även de råd som gäller för den teknik du använder när du kommunicerar – de finns i nästa avsnitt.

Slå på din mentala brandvägg

När du kommunicerar – använd sunt förnuft. Hur känslig är informationen som du ska sända? Det kan till exempel handla om kreditkortsnummer, användarnamn eller lösenord. Finns det risk att någon kan se vad du läser och skriver? Vad kan konsekvensen bli? Behöver du hantera informationen här och nu? Vilka alternativ har du?

Se din mobiltelefon som en dator

Använd samma sunda förnuft när du använder din mobiltelefon som när du sitter vid datorn. Klicka inte på länkar, öppna inte filer och acceptera inte saker som du inte vet vad det är eller om de kommer från en okänd avsändare.

Skydda och säkerhetskopiera din information

Du kan tappa bort din dator eller din mobiltelefon och de kan bli stulna. Skydda dig genom att aktivera en personlig kod (PIN-kod) för inloggning och använd starka lösenord. Ta regelbundet säkerhetskopior av viktig information, till exempel fotografier och adressbok.

Uppdatera dina program

Håll operativsystem, webbläsare och andra program i din dator och mobiltelefon uppdaterade. Du kan ställa in de flesta av dina program så att de hämtar uppdateringar automatiskt. Använd antivirusprogram och brandvägg på din dator.

Se till att din kommunikation är säker

Om du hanterar information som är känslig, till exempel personuppgifter, kreditkortsnummer, inloggningsuppgifter eller liknande – se till att din kommunikation är säker och välj krypterade tjänster. Om adressen till webbsidan börjar med ”https” så är kommunikationen krypterad, vilket innebär att informationen inte skickas i klartext.

-
- På PTS webbplats, www.pts.se/internetsakerhet, finns en kort film som informerar om hur du kan kommunicera trådlöst på ett säkert sätt.
 - Med webbtjänsten Testa lösenord, testalosenord.pts.se, kan du lära dig hur lösenord bör konstrueras för att bli starka och svåra att knäcka.
 - Med webbtjänsten Testa datorn, testadatorn.pts.se, kan du testa om din dator har några säkerhetshål.
-

Vad ska jag tänka på vad gäller säkerheten för trådlösa nät och bluetooth?

När du ska ansluta till privata trådlösa nät, publika trådlösa nät och bluetooth finns det några saker du bör tänka på för att höja säkerheten.

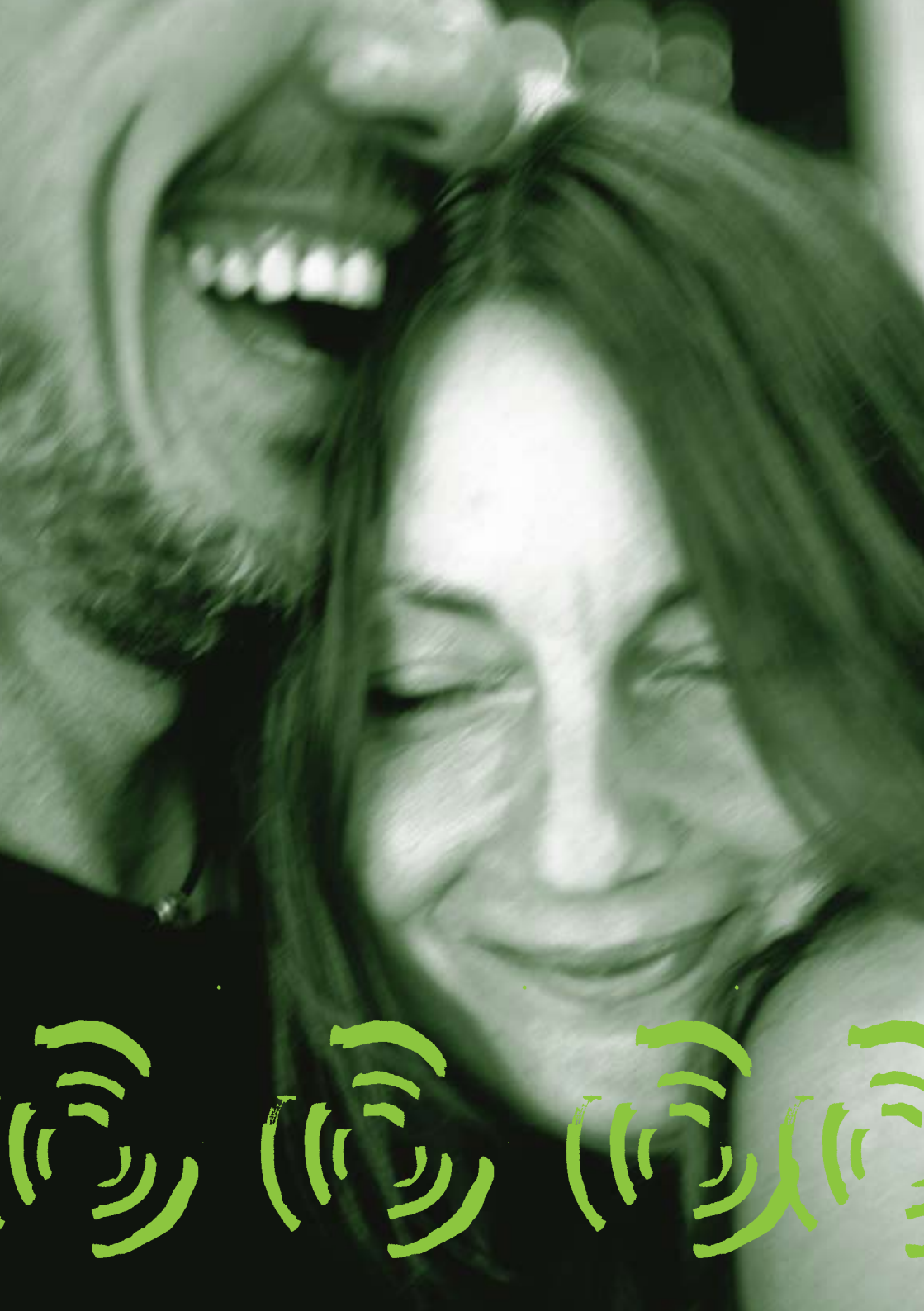
Privata trådlösa nät

Här finns råd till dig som har ett trådlöst nät hemma. De tre råden består i att du ändrar olika säkerhetsinställningar i din trådlösa router.

Slå på krypteringen

Slå på den inbyggda krypteringen i din trådlösa router för att förhindra att någon obehörig använder ditt nät. Använd så stark kryptering som möjligt. Det finns vanligtvis tre olika krypteringsmetoder. WPA2 är den starkaste krypteringen, följt av WPA. WEP är den svagaste krypteringen och är ganska lätt att knäcka, men den är bättre än att inte använda någon kryptering alls.





Byt användarnamn och lösenord

Ofta har en tillverkare samma användarnamn och lösenord till alla trådlösa routrar av samma modell. Den här informationen är därför lätt att hitta på Internet. För att försvåra intrång bör du byta användarnamn och lösenord. Använd ett starkt lösenord. Stäng även av möjligheten att ändra inställningar trådlöst eller via Internet. Då kan du bara ändra inställningarna via kabel.

Byt namn på nätet och stäng av utsändning av namnet

Som grundinställning sänder alla trådlösa nät ut sitt namn, vilket ofta är namnet på tillverkaren eller tjänsteleverantören. För att försvåra intrång bör du byta namn på nätet. Du bör även stänga av utsändning av namnet på nätet.

-
- På PTS webbplats, www.pts.se/internetsakerhet, finns en kort film som demonstrerar hur du ställer in din trådlösa router på rätt sätt.
 - Med webbtjänsten Testa lösenord, testalosenord.pts.se, kan du lära dig hur lösenord bör konstrueras för att bli starka och svåra att knäcka.
-

Publika trådlösa nät

Här får du råd om du vill ansluta till ett publikt trådlöst nät.

Använd bara trådlösa nät du litar på

Använd bara trådlösa nät som erbjuds av någon du känner till och litar på. Ta reda på hur säkert nätet är. Om du är osäker på vilket nät du bör använda, fråga på stället där du vill ansluta till Internet. Detta är särskilt viktigt om du ska överföra känslig information.

Kommunicera inte omedvetet med omvärlden

Stäng av funktionen för trådlös nätanslutning på datorn när du inte behöver trådlös anslutning. Då riskerar du inte att koppla upp dig mot ett nät av misstag. Du kan också slå av funktionen som gör att datorn automatiskt ansluter till nät som du tidigare har använt. Genom att manuellt godkänna vilka nät som datorn ska ansluta till, får du bättre kontroll och säkerhet.

Bluetooth

Här får du råd om du vill använda bluetooth.

Låt din mobil och dator bara vara synlig när det behövs

I de flesta mobiltelefoner och datorer finns det tre inställningar för bluetooth
1. av, 2. på men dold för andra, 3. på och synlig för andra.

Stäng av bluetooth när du inte använder det. När bluetooth är på – använd funktionen som gör att bluetooth inte syns för andra. Låt bara bluetooth vara påslaget och synligt när du behöver det.

Acceptera bara filer och anslutningar från någon du litar på

Acceptera bara filer och anslutningar via bluetooth som kommer från någon du litar på. Får du frågan att acceptera något från en okänd och som du inte förväntat dig, acceptera inte utan att ta reda på vad det är och vem som har skickat det. Det finns en risk att du kan få skadliga program installerade på din dator eller mobiltelefon.

Var försiktig när du ansluter

Var försiktig när du vill ansluta med bluetooth. Ska du göra det på en allmän plats – var säker på att du ansluter till rätt mobiltelefon eller dator, det kan finnas flera med samma namn. Om du av misstag ansluter till fel enhet riskerar du att andra kan ta del av din information.

-
- På PTS webbplats, www.pts.se/internetsakerhet, finns en kort film som informerar om hur du kan använda bluetooth på ett säkert sätt.
-

Vad gör jag om det blir problem?

Om du får problem med att följa råden, börja med att titta i instruktionsboken för din dator, din mobiltelefon eller din trådlösa router. Där finns värdefull information om hur du ställer in enheterna för att de ska fungera så säkert som möjligt.

Leverantörer och tillverkare av datorer, mobiltelefoner och trådlösa routrar erbjuder ofta support till dem som har köpt deras produkter. Om du har problem med ditt trådlösa nät och har fått utrustningen från din Internetleverantör, kan du även kontakta din Internetleverantör. Det finns även andra företag som hjälper privatpersoner att installera trådlösa nät.

Om du vill ha mer detaljerade råd kan du läsa PTS rapport Säkerhet i trådlösa nät – råd till dig som användare, som den här broschyren bygger på. Den finns på PTS webbplats, www.pts.se.

Var kan jag få mer information?

Den här informationen kommer från kommunikationsmyndigheten PTS. Mer information, frågor och svar, tips och råd för tele- och IT-konsumenter finns på PTS speciella konsumentwebbplats, www.pts.se/konsument. Besök även gärna vår webbplats för Internetsäkerhet, www.pts.se/internetsakerhet.

Det finns även broschyrer om mobiltelefoni, fast telefoni och bredband. Allt informationsmaterial från PTS är gratis och kan beställas från www.pts.se, info@pts.se eller via telefon 08-678 55 00.

Informationen i broschyren finns även i lättläst version på www.pts.se. Om du vill ha informationen i ett alternativt format, exempelvis i punktskrift, kontakta PTS via e-post info@pts.se eller via telefon 08-678 55 00.



Post- och telestyrelsen Box 5398 102 49 Stockholm
Växel: 08-678 55 00 pts@pts.se www.pts.se