



Faktablad

Säkerhet i publika trådlösa nätverk

Publika trådlösa nätverk, så kallade hotspots, är nätverk som är vanliga på offentliga platser för att ansluta till exempel en dator trådlöst med WLAN-teknik till Internet.

Sådana nät är sårbara eftersom informationen överförs med radiovågor och oftast i klartext, utan kryptering. Det innebär att informationen enkelt kan fångas upp med radioutrustning. I det här faktabladet ger Post- och telestyrelsen, PTS, råd som höjer säkerheten vid användning av publika trådlösa nätverk.

Utgå från att all kommunikation sker oskyddad och använd en säker förbindelse när du hanterar känslig information

När du använder ett offentligt trådlöst nätverk är det extra viktigt att använda en säker förbindelse när du hanterar känslig information.

En säker förbindelse är en krypterad förbindelse mellan två kommunicerande ändpunkter. En sådan kan uppnås med hjälp av en https-förbindelse (Hyper Text Transfer Protocol Secure) i din webbläsare eller en VPN-lösning (Virtual Private Network).

Https-förbindelsen erbjuds ofta för nätbanktjänster för att kunna utföra säkra transaktioner eller för e-tjänster som hanterar dina kreditkortsuppgifter. Om webbadressen börjar med https, i stället för http, är förbindelsen säker. Https symboliseras med ett hängglås i många webbläsare.

En VPN-lösning är ofta tillgänglig för företagsanvändare för att kunna ansluta sig säkert till ett företags interna nätverk.

Om Post- och telestyrelsen

- Post- och telestyrelsen, PTS, är den myndighet som bevakar områdena elektronisk kommunikation och post. Begreppet elektronisk kommunikation inkluderar telekommunikationer, IT och radio.
- PTS arbetar med fyra övergripande områden: konsument- och konkurrensfrågor, effektivt resursutnyttjande och säker kommunikation.
- PTS vision är att alla i Sverige ska ha tillgång till effektiva, prisvärda och säkra kommunikationstjänster.



Var uppmärksam på falska publika trådlösa nätverk

Var uppmärksam på falska nätverk som kan användas för avlyssning vid uppkopplingen till Internet. Det finns de som erbjuder publika trådlösa nätverk utan inloggning över en https-förbindelse för att det ska vara enkelt att ansluta. Om du upptäcker samma eller liknande namn på flera publika trådlösa nät, på en och samma plats, exempelvis på ett café eller tågstation, anslut inte till något om du inte vet exakt vad nätet ska heta. Om det finns en https-förbindelse och webbadressen till den som erbjuder tjänsten är korrekt, har du en säker förbindelse mellan din dator och inloggningsservern. Då är tjänsten säker att använda.

Om du är osäker på vilka publika trådlösa nätverk som ska finnas tillgängliga och vad de heter, fråga då innehavaren av det trådlösa nätet, alternativt innehavaren av cafét, hotellet eller motsvarande.

Använd ett uppdaterat operativsystem, brandvägg och antivirusprogram

Du bör alltid ha ett uppdaterat operativsystem, brandvägg och antivirusprogram. Du bör också alltid använda starka lösenord för inloggning till olika tjänster. Så skapar du ett starkt lösenord:

- Blanda små och stora bokstäver, siffror och specialtecken
- Använd minst åtta tecken
- Använd inga kända ord, namn eller nummer
- Använd ingen information som kan kopplas till dig

Tänk på sociala faktorer

Slutligen, var uppmärksam på sociala faktorer som att någon försöker läsa över din axel, till exempel vid inloggning till e-tjänster. Skapa en användarprofil på din dator som innebär att du måste logga in på datorn med lösenord om den inte har använts aktivt på en kortare period. Lämna inte datorn obevakad.

Mer information

För ytterligare information, se rapporten ”Säkerhet i lokala trådlösa nät – råd till användare för ökad säkerhet” (PTS-ER-2007:16) och broschyren ”Om trådlösa nätverk”, som tar upp säkerhet i trådlösa nätverk i hemmet. Både rapporten och broschyren går att ladda ner på www.pts.se.

Läs gärna mer om Internetsäkerhet på www.pts.se/internetsakerhet.