Installation af eduroam

Vejledning til DeIC-ansatte og personer, der har konto hos DeIC.

Du skal køre et installationsprogram for at få adgang til Eduroam. Det sørger for at bringe de rette sikkerhedsindstillinger på plads.

Sådan henter og kører du installationsprogrammet:

1. Gå ind på websiden http://cat.eduroam.org
2. Tryk på den store knap med teksten "eduroam user: download your eduroam installer".
   Fra listen over 'Home institutions' vælger du DeIC.
   En række knapper giver nu valg mellem platforme/operativsystem.

Android: Der behøves en app + xml-profil fra CAT.

Se separat Android-vejledning.

3. Vælg den platform og det operativsystem, du bruger, og klik på knappen. Afhængig af platformen er der tale om et exe-program, et script eller en profil/beskrivelse.
4. Kør programmet.

Under installationen skal du indtaste *brugernavn* og *kodeord.* Dit brugernavn er på formen: **`ini@deic.dk`**, hvor **`ini`** er dine initialer. Som ny bruger får du oplyst kodeordet mundtligt eller på sms. Som etableret bruger kender du kodeordet, eller du kan få sat et nyt ved henvendelse til eduroam@deic.dk.

Ved installationen bliver CA-rodcertifikatet "DeIC Staff eduroam Root" installeret på din enhed. På Mac og iPhone/iOS bliver du bedt om at godkende dette.

Sådan fungerer sikkerheden i eduroam

Når du forbinder dig til et trådløst netværk på et andet sted end din egen institution, bliver dit brugernavn og password sendt videre til din institution. Hvis den genkender oplysningerne, får det lokale netværk besked om, at du må bruge det.

Kommunikationen er krypteret for at forhindre, at andre kan se dit password. Krypteringen sker ved hjælp af et såkaldt servercertifikat fra serveren på din institution.

Hvis en it-kriminel vil aflytte din kommunikation, kan vedkommende sende et falsk certifikat til din computer/smartphone. Hvis det sker, vil du blive spurgt, om du vil godkende dette certifikat. Det skal du altid svare nej til – også selvom certifikatet har et navn, der ser troværdigt ud.

Under installationen er din enhed sat op til at genkende certifikatet fra din egen institution. Hvis den ikke genkender et certifikat, er det tegn på, at der er noget galt.

Hvis du alligevel svarer ja, risikerer du, at din kommunikation bliver aflyttet. Dermed kan uvedkommende læse dine mails og chat-beskeder, se de billeder du tager og få fat i dine passwords.