Aftenposten
Lørdag 15. desember 2018

Svindlere lurer deg på gratis nett

Ingrid Emilie Thoresen Bakker

– Svindlere kan få tilgang til sensitiv informasjon når du er koblet på gratis nettverk, sier sikkerhetsekspert.

Se for deg at du sitter på et hotell som heter Radisson. Du skal koble deg opp på internett og ser to nettverk med disse navnene: «Radisson WiFi» og «Radisson Free Wifi».

Ett av nettverkene krever betaling, og ett er gratis.

Hvilket logger du deg på?

Mest sannsynlig hadde du valgt det kostnadsfrie nettverket.

Mer enn åtte av ti har nemlig benyttet seg av gratis internettkobling på hoteller, kafeer og flyplasser. Det viser en fersk undersøkelse fra Nordea.

– Jeg er ikke overrasket over disse tallene, men det er samtidig litt bekymringsfullt. Flere bør forstå risikoen knyttet til trådløse nettverk, sier Roar Thon, fagdirektør for sikkerhetskultur ved Nasjonal sikkerhetsmyndighet (NSM).

– Gjør deg sårbar for svindel

Mange av de gratis nettverkene man finner på blant annet kafeer, hoteller og flyplasser, kan gi tilgang til usikrede nett uten kryptering.

Likevel kobler en stor del av den norske befolkningen seg opp på slike nettverk, viser en fersk undersøkelse utført for Nordea.

– Når man surfer på et nett som ikke er kryptert, gjør du deg sårbar for blant annet svindel, sier Elin Reitan fra Nordea.

Usikrede og ukrypterte nett gjør det nemlig mulig for en svindler å hente ut sensitiv informasjon om andre som er koblet til samme nettverk – hvis vedkommende vet hva han eller hun driver med.

Kriminelle vil gjerne ha tilgang til dine personopplysninger og passord.

> Der hvor det finnes flere nettverk med lignende navn, kan det tenkes at noen forsøker å lure deg

Roar Thon, Nasjonal sikkerhetsmyndighet

Kan ligge en kriminell hensikt bak

Når så mange andre kobler seg på gratis internettkoblinger, er det lett å tenke at dette er ganske ufarlig. *Men er det egentlig det?*

– Når vi kobler oss på åpne, trådløse nettverk, vet vi ikke hvem som eier det og hva den bakenforliggende hensikten er, forklarer Thon.

Ofte er hensikten å gi kunden internettilgang, men i noen tilfeller kan det også ligge en kriminell hensikt bak, påpeker han.

Svindlere kan nemlig sette opp et falsk, trådløst nettverk med navnet til kafeen du sitter på – og lure deg til å koble deg på.

Det gir svindleren muligheten til å se passordet du taster, innhold i meldinger og e-poster. Og ikke minst, innloggingskode i nettbanken.

– En hacker kan få deg til å tro at du kobler deg på banken din fordi vedkommende har gitt deg en forfalsket side som oppfører seg nøyaktig som banken din. Da gir du blant annet fra deg personnummer og personlig passord til svindleren, forklarer Thon.

– Men hvordan kan man vite at nettverket man kobler seg på, er trygt?

– Der hvor det finnes flere nettverk med lignende navn, kan det tenkes at noen forsøker å lure deg. Da kan det være lurt å spørre kafeen, flyplassen eller hotellet du er på, om hvilket nettverk som er deres, sier Thon.

Inngangsport til ID-tyveri

Han anbefaler, så langt det er mulig, å unngå å logge seg på nettsteder og tjenester som krever passord mens man er tilkoblet et gratis trådløst nettverk.

– Det finnes en viss risiko for at hackere kan tukle med enheten du bruker når du kobler deg på trådløse nettverk, sier Thon.

Dette er en av inngangsportene til identitetstyveri for svindlerne, mener han.

– De kan fange opp påloggingsinformasjon på alt fra Facebook til e-post. Denne informasjonen kan misbrukes i forskjellige settinger. Det er bare fantasien som setter stopper for kjeltringene hvis de først får tak i informasjonen, sier Thon.

– Bruk mer mobildata

Han innrømmer at han selv innimellom kobler seg på ukjente trådløse nettverk.

– Men jeg er kritisk til hva jeg gjør når jeg koblet på et slikt nettverk. Hvis jeg sitter på en flyplass, er det kanskje uproblematisk å lese aviser på nett. Men jeg gjør aldri finansielle transaksjoner.

Hans klare råd er å bruke mer 4G.

– For å spare penger benytter vi oss ofte av gratis nett. Men likevel bør man bruke mer mobildata. Det er sikrere å surfe på 4G enn å bruke kaffebarens trådløse nett som vi i realiteten ikke vet noe om, sier Thon.

– Les aldri e-posten din på et gratis nettverk

Gisle Hannemyr, universitetslektor ved Universitetet i Oslo, jobber blant annet med personvern, datasikkerhet og informasjonssikkerhet.

Han innrømmer at også han er blant dem som kobler seg på gratis nettverk.

Men selv er han god til å ta forholdsregler. Det oppfordrer han også andre til å være.

– Logg deg aldri inn et sted hvor du er nødt til å taste inn et passord eller å oppgi personlige opplysninger mens du er koblet til et gratis nettverk. Vær særlig forsiktig hvis du har dårlig passord-disiplin og bruker det samme passordet flere steder. Det kan gi svindleren adgang til andre tjenester.

Les heller aldri e-posten din når du er tilkoblet et slikt nettverk, råder han.

– Logger du deg inn på e-posten din, kan svindleren også lese e-postene dine. Her kan det finnes mye snacks som vedkommende kan bruke i et identitetstyveri. Her kan han finne ut hva hunden din, ektefellen og barna dine heter, og lure andre folk til å tro at de er deg.