Kaffetørst? Offentlige nettverk.

Det er vi av og til – og da er det bra å ha en kafeteria eller kaffebar i nærheten. Det tenkte også en av våre medlemmer da han var på ferie i Spania engang. Så inn på første og beste kafé der varen ble rekvirert. Mens man sitter der og nyter sin kaffe, cafe solo, så finner han ut at det var gratis Wifi i lokalet, og da er det tid for å lese nytt fra hjemlandet og å lese og sende noen e-poster. Så det gjorde han. Wifi-en var helt gratis og det var ingen pålogging nødvendig – han kom rett inn på nett. Dette finner du mange steder også her i landet: kafeer, restauranter, hoteller, barer osv har dette. Og noen e-poster ble lest og sendt av mannen.

Så hendte det noe: venner og kontakter i e-postsystemet hans fikk så plutselig alle en e-post fra den stakkars mannen der det sto at han var i Bulgaria, hadde mistet lommeboken sin og måtte få tilsendt noen penger til en konto så han kom seg hjem igjen. Det hørtes kanskje rimelig ut. Vi kan jo komme i en slik situasjon noen og enhver – bare at dette var ren svindel!

Mens han jobbet med e-postene sine på kafeen, så var det en av de andre i lokalet som hadde logget seg inn på samme Wifi kanalen (som var helt uten pålogging) og brutt seg inn i mannens e-postsystem. Altså greid å lytte til påloggingen hans, og så sendt ut alle disse beskjedene fra hans e-post konto. Ikke bra! Og han var heldig som ikke hadde logget seg inn på mer følsomme nettsteder!

Så moralen må være:

Offentlige, eller halv-offentlige Wifi punkter skal man være forsiktige med dersom de er uten INDIVIDUELL passord-pålogging, det vil si: der passordet er individuelt for hver bruker. Mange steder er bra ved at man får sitt helt eget passord på en lapp eller liknende. Men for de som ikke har dette så vær varsom. Aviser kan leses – og andre websider, men ikke der hvor du må logge deg inn så som e-post, Facebook og liknende. Men her finnes det en metode som er mye sikrere: 2FA (two-factor authentication eller to-trinns pålogging).Litt mer kronglete, men, som sagt, langt sikrere. I korthet går det ut på, vanligvis, at du logger deg inn som vanlig med brukernavn og passord, men i tillegg må du sette inn en kode også. Og denne koden får du tilsendt, fort som lynet, som en sms til telefonen din. Koden blir forskjellig hver gang du logger deg på – så hvis noen kopierer deg så kan de ikke bruke samme koden du brukte. Og de får heller ikke tak i en ny kode for da må de jo ha mobilen din. Det blir tilsvarende som et system som du kanskje bruker på nettbanken din, altså med kodebrikke. Men forskjellen er at det nå er mobilen din som er brikken.

Jeg sa «mye sikrere» - og det er sånn det er. Det er mange luringer der ute så ikke noe system blir 100%, garantert, men dette 2FA systemet er veldig bra og det beste vi har så langt. Alle de ulike tilbyderne har litt ulike måter å sette opp dette systemet på, så det er vanskelig å gi en oppskrift her. Facebook, Outlook, Gmail osv. er alle litt forskjellige, men alle tilbyr systemet – om man graver litt.

Så generelt bør vi være litt forsiktige når vi har med innlogginger på nettet å gjøre. Mener absolutt ikke å skremme, men litt sunn skepsis kommer man langt med!

Så har vi dette passord-despotiet! Her er det mange ulike synspunkter og overbevisninger ute og går: «Aldri bruk det samme passordet på mer enn ett sted!», «Jeg bruker det samme passordet overalt. Kan ikke gå rundt å huske på alle de forskjellige!» osv. Nå finnes det noen programmer man kan bruke på nett for å lagre alle passordene sine på et sikkert sted. Noen er gratis og noen er abonnementsbasert.

- Her finner du noen av dem:

http://uk.pcmag.com/password-managers-products/4296/guide/the-best-password-managers-of-2018

Jeg må innrømme at jeg sløver selv litt med å ha forskjellige passord overalt, **men:** alt som har med mine penger å gjøre, nettbank, vipps etc., - der er jeg flink og gjenbruker ikke disse kodene eller passordene noe sted.

Det er et godt tips!

Tore Langemyr Larsen, Seniornett Norge