EKSEMPEL PÅ USIKKERHEDEN VED NEMID

Så let kan kriminelle frarøve dig dine NemID oplysninger

Ingeniøren bragte i deres medlemsblad den 4. november 2011 en række detaljerede artikler om usikkerheden ved NemID.
Artiklerne beskriver, hvor let det er at franarre oplysninger fra de danske NemID brugerne, og de påpeger i, at myndighederne bør anerkende den store sikkerhedsbrist, der truer ved anvendelse af NemID.

Ifølge Ingeniøren er opskriften på, at narre NemID-oplysninger fra tillidsfulde borgere bekymrende simpel, og dette bevises i en testopstilling, hvor Ingeniøren igennem 5 simple trin demonstrerer, hvor let det kan gøres. Vi skal for en god ordens skyld gøre opmærksom på, at sådan adfærd er kriminel og dette skal på ingen måde anses for at være en opfordring til at følge opskriften.

5 simple trin gør det muligt, at narre NemID brugere

- Den It-kriminelle har to skærme. Den ene skærm viser brugerens login-oplysninger, mens den anden viser en side med et rigtigt NemID vindue, så den It-kriminelle umiddelbart kan indtaste oplysningerne.
- Den It-kriminelle laver en falsk hjemmeside, som brugeren bliver lokket ind på. Hjemmesiden er en tro kopi af f.eks. en banks hjemmeside, og det er derfor svært for forbrugeren at opdage, at hjemmesiden er falsk.
- Når brugeren forsøger at logge ind på den falske hjemmeside bliver oplysningerne synlige på den it-kriminelles skærm.
- Den it-kriminelle indtaster brugerens brugernavn og adgangskode på den rigtige hjemmeside. Derefter tager den it-kriminelle en kopi af vinduet med nøglekortet, og sender det til den falske hjemmeside, så brugeren kan se den.
- Dernæst indtaster brugeren sandsynligvis sin nøglekode og den it-kriminelle kan herefter logge ind på den rigtige hjemmeside. Brugeren bliver i stedet mødt med en almindelig fejlbesked, såsom ”Det er for øjeblikket ikke muligt at kommunikere med serveren, prøv venligst senere”.

Se eventuelt en video:
http://www.version2.dk/artikel/video-saadan-kan-nemid-hackes-32396