Sikker på sociale medier

Har du profiler på sociale medier? Så læs med her.

Har du adgang til klassificeret eller beskyttelsesværdig information? Så kan det være attraktivt for en fremmed efterretningstjeneste at nærme sig dig og din viden, og deres research kan begynde på internettet. Her kan de ofte finde information om dit arbejde, din familiesituation og dine fritidsinteresser – og det kan de bruge imod dig. De kan fx ud fra deres research skræddersy falske e-mails til dig, såkaldt spear phishing, eller de kan forsøge at skabe fysisk kontakt til dig i forbindelse med fx sportsarrangementer, ferier, koncerter og sociale sammenkomster.

Ud fra et sikkerhedsperspektiv er det bedst helt at lade være med at bruge sociale medier. Men der kan være både faglig og personlig værdi ved at være tilstede online. Så har du profiler på sociale medier, er det en god ide at læse og følge disse ti gode råd til bedre sikkerhed på sociale medier:

1. Overvej risiko vs. værdi
Hvilken information har du adgang til? Hvad med personer du kender? Det kan være svært at vurdere, hvor interessant du, og dit netværk, kan være for en fremmed efterretningstjeneste, men jo mere klassificeret og beskyttelsesværdig information, I har adgang til, jo større er risikoen for at blive udset som målperson. Risikoen bør du holde op imod den personlige eller faglige værdi, du har ved at benytte sociale medier. Tag ud fra dette stilling til, i hvor høj grad, du ønsker at være eksponeret på sociale medier.

2. Få dine nærmeste med på den sikre vogn
Din sikkerhedsbevidsthed er ikke nok. Dine nærmestes sikkerhedsbevidsthed er også afgørende. Gennemgå gerne rådene her med dem.

3. Del profilerne op
Ligesom det sikkerhedsmæssigt er en god ide at have en arbejdsmobil og en privat mobil, kan sociale medier også opdeles. Overvej om du skal have flere profiler, så du fx lægger faglige indlæg op på arbejdsprofilen, og billedet fra fødselsdagen op på den private.

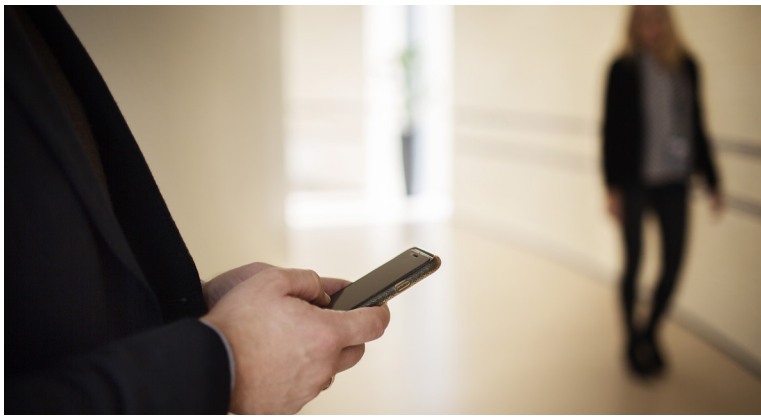
4. Overvej hvad du lægger op til hvem
Skal en fremmed efterretningstjeneste vide, hvilken klub du dyrker sport i, og hvilken skole din datter går på? Overvej hvad du lægger op og til hvem. Brug privatlivsindstillingerne aktivt. Typisk vil der være indhold, som du kan nøjes med at dele med en mere snæver kreds.

5. Brug stærke og forskellige kodeord
Brug stærke kodeord. Et stærkt kodeord består af 15 eller flere tegn, der både indeholder store og små bogstaver samt tal. Brug forskellige kodeord til de forskellige tjenester.

6. Tjek om de allerede har adgang
Brug *haveibeenpwned.com* til at se, om dine loginoplysninger allerede ligger frit tilgængeligt for uvedkommende. Skift i givet fald kodeord.

7. Ryd op
Internettet glemmer aldrig, men hvis du rydder op i, hvad du igennem tiden har lagt op, er det betydeligt sværere at tilgå. Har du gamle profiler liggende, som ikke længere er relevante?

8. Søg på dig selv
Fremmede efterretningstjenester har udvidede muligheder for at finde information på internettet om dig. Men du kan alligevel få en god ide om, hvad der ligger derude, hvis du søger på dig selv. Prøv gerne forskellige søgemaskiner og browsere.



9. Overvej navnet til din profil
Behøver du hedde dit fulde, rigtige navn på de sociale medier? Til private profiler kan du evt. bruge en variation af dit navn, fx initialer – det gør det sværere at finde dig. Opret gerne en ny profil, og slet den gamle.

10. Få gode guides
På *sikkerdigital.dk* er der guides til, hvordan du konkret kan justere, hvem du deler med, hvem der kigger med på din profil, hvem der kan tagge dig, hvad du kan gøre, hvis du er blevet hacket m.m. Et andet godt værktøj er app'en 'Mit Digitale Selvforsvar', hvor du kan holde dig opdateret på de nyeste, digitale trusler. ■