



Brug internettet - men med omtanke



Brug internettet - men med omtanke

Internettet er for forsvarrets ansatte, som for alle andre danskere, en integreret del af hverdagen. Især for udsendte, opleves internettet som et oplagt kommunikationsmiddel til at holde kontakt til familie, venner og kolleger.

Det er internettet også på mange måder – men det skal bruges med omtanke.

Forsvarschefen sagde på Forsvarets Kommunikationskonference i februar 2009:

”De ansatte skriver ting, som kan bruges imod dem og risikerer derfor at gøre sig selv eller deres familier til et mål for trusler.”

Denne folder skal medvirke til at øge din sikkerhedsbevidsthed, når du bruger internettet. Brug af mobiltelefon er beskrevet i folderen ”Hold kontakten - men med omtanke”.

Brug af internettet

Alt, hvad du lægger på internettet, kan potentielt læses af hvem som helst. Derfor er det vigtigt, at du er sikkerhedsbevidst og tager nogle forholdsregler, når du bruger internettet. Hjemmesider, der er beskyttet af password, og e-mails kan 'aflyttes' på samme måde som mobiltelefoner og fastnettelefoner. Passwordet er derfor ingen garanti, men en forbedring af sikkerhed.

Brug din sunde fornuft, når du bruger internettet. Omtal ikke ting som f.eks. operationer, telefonnumre og navne, der kan bringe din egen, dine pårørendes eller din enheds sikkerhed i fare. Tænk altid på operationssikkerhed. Informationer, der umiddelbart kan synes banale som ”I morgen tager vi på patrulje i Geresk”, eller ”Vi kommer tilbage den 12.”, er i de forkerte hænder vigtig information, der i værste fald kan bringe patruljen i fare.

Tænk også på, hvilke billeder du lægger på nettet. Et billede siger mere end 1.000 ord, og derfor kan et billede afsløre detaljer. Der er flere eksempler på, at udsendte i bedste mening har lagt billeder på nettet eller suppleret mails med billeder, der har afsløret detaljer fra lejren. Billeder der i de forkerte hænder kan bringe sikkerheden i fare.

For at minimere risici er det vigtigt, at du er bevidst om, hvad du skriver, og hvilke billeder du lægger på nettet.

Hvorfor denne forsigtighed? Af fire grunde:

1. For at beskytte dig selv

Når du benytter internettet, udsætter du dig selv for en række risici. Din computer kan blive inficeret af virus, du kan blive udsat for angreb, bl.a. på din web-bank, og du kan risikere at gøre dig selv til mål for chikane og terror, hvis du kan sættes i forbindelse med forsvaret.

2. For at beskytte dine pårørende

Dine pårørende risikerer at blive mål for chikane og terror, hvis det kan spores, at de har forbindelse til ansatte i forsvaret.

3. For at beskytte operationssikkerheden i missionsområderne

Der har været flere eksempler på beskrivelser af procedurer og omtale af kommende operationer bl.a. på blogs og på Facebook. Sådanne omtaler kan ødelægge kommende operationer samt bringe dit og dine kollegers liv i fare.

4. For at beskytte forsvarrets installationer

Personer eller organisationer, der planlægger aktioner mod forsvaret, som f.eks. våbentyveri, hærværk eller andet, vil kunne udnytte detaljeret information, som de kan finde på internettet, i deres planlægning.

Hvad kan du gøre for at optimere sikkerheden?

Det allervigtigste er at bruge internettet med omtanke!

Når du skriver e-mails, skal du være opmærksom på, at der er en potentiel risiko for, at disse kan læses af andre end den ønskede modtager. Husk derfor, at internettet kun er til uklassificeret kommunikation, og undlad at omtale klassificerede emner såsom operationer, missioner, enheder etc., og undlad at vedhæfte billeder, der kompromitterer sikkerheden.

Hvis du har en hjemmeside eller en blog, skal du ligeledes være opmærksom på, hvad du lægger ud og hele tiden huske, at internettet kun må anvendes til uklassificerede emner. Du kan forbedre sikkerheden ved at begrænse adgangen til hjemmesiden med et kodeord, som du kun oplyser de personer, som du ønsker skal læse med.

Hvis du har en profil på Facebook, LinkedIn, Myspace eller lignende, skal du overveje, hvad du oplyser om dig selv. Du skal bl.a. undgå at give oplysninger om de operationer, du deltager i. Hvis nogen ønsker at chikanere eller terrorisere danske soldater, vil Facebook være et godt udgangspunkt for at finde frem til udsendte. Hvis du undlader at oplyse om dit tilhørsforhold til forsvaret på dine profiler, minimerer du risikoen for, at du eller dine pårørende bliver chikaneret.

Har du en profil på dating.dk, scor.dk etc., skal du være opmærksom på, at der kan være nogen, der ønsker at skabe kontakt til dig, udelukkende fordi du har adgang til klassificerede oplysninger. Undgå derfor at oplyse, at du er ansat i forsvaret i disse fora.

Når du skriver, bliver dit budskab ikke bedre af, at du skriver dit fulde navn.

Gode råd

- Husk, at oplysninger på internettet er søgbare for alle.
- Begræns de personlige informationer, du lægger ud om dig selv. Brug f.eks. ikke dit fulde navn.
- Når du 'møder' andre på nettet, så vær naturligt skeptisk.
- En 'ven' på nettet er ikke nødvendigvis din ven. I værste fald kan det være en falsk profil, som fjenden har oprettet for at lokke informationer ud af dig.
- Læg ikke oplysninger på nettet om andre uden deres tilladelse.
- Undgå at lægge oplysninger på nettet, der kan vise dine relationer til forsvaret og især til specifikke enheder, personer, våbensystemer, tekniske systemer, missioner og operationer.
- Undgå at lægge billeder på nettet, som viser personer, materiel og indretning af kaserner, lejre og baser i Danmark og udlandet.
- Giv ikke andre adgang til din mailadresse, brugernavn eller password.
- Kontroller det domæne, du har tænkt dig at lægge oplysninger på. Læs deres politik for håndtering af personlige oplysninger, og især hvordan de evt. deler denne information og med hvilken hensigt.
- Anvend de sikkerhedsindstillinger, der er tilgængelige, og sørg for, at det kun er dig selv, der giver andre adgang til oplysninger om dig.
- Hold din PC ajour med et opdateret antivirusprogram. Som ansat i forsvaret kan du gratis downloade et antivirusprogram fra McAfee på FIIN fra FKIT hjemmeside, under "Sikkerheds-info".
- Læs også folderne "Hold kontakten – men med omtanke" og "Undgå spionage – for din sikkerheds skyld", som du kan få på dit tjenestested, eller som kan rekvireres ved Forsvarets Efterretningstjeneste.

Hvad skal pårørende gøre, hvis de bliver chikaneret?

Pårørende skal kontakte forsvaret.

For udsendte fra Hæren

Hærens Operative Kommando, tlf. 99 62 49 70, lok. 7900

For udsendte fra Søværnet

Søværnets Operative Kommando, tlf. 89 43 30 99

For udsendte fra Flyvevåbnet

Flyvertaktisk Kommando, tlf. 99 62 49 50

Telefonerne er åbne hele døgnet

Anmeldelsen går videre til Forsvarets Efterretningstjeneste, som videregiver til Politiet. Politiet forestår efterforskningen med støtte fra forsvaret.



FE

Forsvarets Efterretningstjeneste
- Den Militære Sikkerhedsafdeling
Kastellet 30
2100 København Ø
Tlf. +45 33 32 55 66
www.fe-ddis.dk
email: fe@fe-mail.dk