

## It-sikkerhedskomiteén

### Beskyttelse af børn og unge på online sociale netværkstjenester

Børn og unge har stor glæde af de nye online sociale netværkstjenester, men deres oplevelser på disse tjenester er desværre ikke altid positive. Selv om ulykkelige oplevelser er relativt sjældne, er det ønskeligt at søge at beskytte børn og unge bedst muligt. Der er derfor et behov for at iværksætte tiltag på området. Videnskabsministeren har bedt IT- og Telestyrelsen om at iværksætte en undersøgelse til belysning af problemstillinger og behov vedrørende børn og unges brug af online sociale netværkstjenester, og It-sikkerhedskomiteéns har ligeledes fokus på problemstillingen. Videnskabsministerens opdrag og nærværende oplæg, som er initieret af It-sikkerhedskomiteén, er dog to selvstændige undersøgelser.

It-sikkerhedskomiteén ønsker at opridse de udfordringer, komitéén anser som de centrale indenfor området børn og unge på online sociale netværkstjenester samt at pege på tiltag, der kan imødegå disse udfordringer. It-sikkerhedskomiteén har i den forbindelse afholdt en workshop med oplæg af leverandører af tekniske produkter, der kan bidrage til beskyttelse af børn og unge. Komiteén har derudover afsøgt problemfeltet ved at invitere blandt andet Arto til at give oplæg for komitéén.

#### 1. Børn og unges brug af online sociale netværkstjenester

Online sociale netværkstjenester som Facebook, MySpace, LinkedIn, Arto og Habbo vinder større og større indpas som en integreret del af dagligdagen hos både børn, unge og voksne. Online sociale tjenester kendetegnes ved, at man kan oprette en personlig profil, hvor man blandt andet opretter lister over egne venner og kan se tilsvarende lister hos andre. Brugen af disse tjenester er hastigt voksende. For eksempel er antallet af danskere på Facebook primo oktober 2008 på over 1242900. Arto estimerer, at over 80 procent af alle unge mellem 12 og 20 år har en profil på Arto. Hver dag sendes der mere end 2 millioner beskeder på Arto, og der lægges dagligt mere end 70-80.000 billeder online.

Online sociale netværkstjenester har givet os en mulighed for at pleje og opretholde venskaber og bekendtskaber på en helt anden måde end tidligere. Det skinner igennem hos børn og unge, der er vokset op i den digitale verden. De bruger tjenesterne anderledes end voksne. Børn og unges definition af ”venner” har rykket sig som konsekvens af brugen af tjenester som for eksempel Arto. Begrebet har udvidet sig således, at hvem som helst kan betegnes som en ven. En ven kan være en, man mødte online i går. På de online sociale netværkstjenester kan børn og unge ”skilte” med antallet af online venner og dermed deres popularitet. Her-

1. oktober 2008

It-sikkerhedskomiteéns  
sekretariat

IT- og Telestyrelsen  
Holsteinsgade 63  
2100 København Ø  
Telefon 3545 0000  
Telefax 3545 0010  
E-post itst@itst.dk  
Netsted www.itst.dk  
CVR-nr. 26769388

Side 1/1

ved bliver motivationen for at acceptere fremmede som venner og indgå i dialog med dem også en anden end den, vi som voksne kender.

Børn og unge, der er vokset op med det elektroniske medie, danner også relationerne på anden vis end voksne. For dem er det ikke en selvfølge, at man skal være *fysisk* sammen, for at være sammen. Man kan ligeså godt sidde ved hver sin computer med tilkøbet webcam – det er også at være sammen. Grænsen mellem den fysiske og den digitale identitet udviskes for nutidens børn og unge, hvilket byder på utrolige muligheder, men også mange udfordringer med hensyn til at sikre integriteten af vores børn og unges identitet, offline såvel som online.

### **2. Udfordringer ved børn og unges brug af online sociale netværkstjenester**

Undersøgelser viser, at langt de fleste børn bruger tjenesterne til at kommunikere med de venner, de har i den virkelige verden. Blandt dem, der benytter online sociale tjenester anonymt, gør de fleste dette for at forhøre sig om andres erfaringer med kærlighed og sex og til at eksperimentere med forskellige identiteter. Størstedelen bliver derfor – heldigvis – ikke udsat for ubehagelige oplevelser i forbindelse med deres brug af tjenesterne.

IT- og Telestyrelsen

Side 2/2

Men på grund af børn og unges mønster med hurtigt at acceptere nye venner samt deres høje grad af tillid til andre på nettet, kan der opstå situationer, hvor et barn kan blive udsat for ubehagelige oplevelser. Sådanne oplevelser udspringer for eksempel af det såkaldte ”*grooming*”.

Grooming betegner adfærden hos en voksen, der langsomt og forsigtigt opbygger et tillids- og fortrolighedsforhold til et barn, så barnet føler, at her har det fået en virkelig rar voksenven. Den unikke opmærksomhed og interesse gør, at barnet honorerer den voksne med et loyalt venskab. Børnene beskriver, at de godt ved, at man ikke skal udlevere private oplysninger. Men de betragter den voksne som en personlig og nær ven, en ven, som det for nogle er naturligt at blive ven med i den virkelige verden.

I Danmark har Rigshospitalets team for seksuelt misbrugte børn i perioden 2001-2007 i alt haft ti sager om voksnes misbrug af børn, som er startet som et ”uskyldigt venskab” på en online social netværkstjeneste. Dette svarer til, at det er mindre end to børn årligt, der udsættes for seksuelt misbrug, hvor kontakten er indledt på en online social netværkstjeneste. Udenlandske undersøgelser viser, at kun fem procent af de voksne lyver om deres alder og udgiver sig for at være mindreårige, og kun 21 procent af de voksne lyver om deres seksuelle ønsker i relation til barnet. Endvidere viser undersøgelser, at det som regel ikke er de vel fungerende børn og unge, der er ofre for overgreb. Tendensen følger her det almindelige sociale mønster, hvor det især er socialt udsatte børn fra dårlige kår med svagt bagland, der er i faregruppen for at blive udsat for overgreb.

Sammenholdes fakta fra en række nationale og udenlandske undersøgelser kan det udledes, at der reelt sker meget få grove overgreb på børn og unge som følge af en voksen-barn kontakt indledt på en online sociale netværkstjeneste. De børn, der dog alligevel bliver mål for disse tilnærmelser, er socialt udsatte børn. Endelig afkræftes, at barnet vildledes i alle forhold, der ender i en misbrugssituation.

Tværtimod er den voksne i langt de fleste tilfælde åben og ærlig både omkring sin alder samt omkring sine seksuelle intentioner.

En stor del af udfordringen ved beskyttelse af børn og unge består således i, at voksne ifølge undersøgelserne oftest ikke lyver om hverken alder eller hensigt. Børn, der ønsker at tage kontakt til disse voksne kan vælge ikke at benytte aldersbestemte fora eller blot benytte en udenlandsk tjeneste, der ikke tilbyder denne mulighed. Tillige kan tekniske løsninger for eksempel misbruges ved, at et barn udleverer sin aldersnøgle til en voksen eller, at en forælder misbruger sit barns identitet. En indsats for beskyttelse af børn og unge på online sociale netværkstjenester må derfor primært fokusere på at skabe opmærksomhed på emnet, herunder øge børns og unges viden om konsekvenserne af deres handlinger på online sociale netværkstjenester.

Som supplement til adfærds- og oplysningsmæssige tiltag kan anvendes tekniske løsninger. Et tilbud om en teknisk løsning giver ikke kun udsatte børn, men alle børn et valg – en mulighed for *selv* at gardere sig mod uønsket voksen kontakt.

IT- og Telestyrelsen

Side 3/3

En mulighed er at have en slags aldersbekræftelse eller ”ungdomsbevis” med det formål at søge at begrænse kommunikationen til børn og unge. Der har fra flere sider været peget på muligheden for, at alderen på en given person bekræftes af en betroet tredje part. Dette benævnes også med et teknisk udtryk ”autentifikation”. Dette kan implementeres således, at man kun kan deltage i et chatforum, hvis det kan bekræftes, at man har en given alder. Det kan også bruges på en sådan måde, at man kun kan invitere venner, der er ældre end én selv. På denne måde vanskeliggøres kontakten mellem voksne og børn.

For at belyse de tekniske elementer af en sådan løsning har It-sikkerhedskomiteén holdt en workshop, hvor der var oplæg fra en række leverandører med produkter på området. Komiteén har inviteret leverandører bredt, og tabellen i bilag 1 er blot et udtryk for dem, der havde tid og mulighed for at fremlægge deres løsning for It-sikkerhedskomiteén på workshoppen. Ud fra disse fremlæggelser har It-sikkerhedskomiteén et klart billede af, at det med teknologien i dag er muligt at implementere aldersbekræftelse - ”autentifikation af alder”, og at der endvidere eksisterer en velvilje blandt tjenesteudbydere til at indgå i dialog om en sådan implementering.

Et ungdomsbevis har den fordel, at det ikke indebærer identifikation af barnet eller den unge – tjenesteudbyder får bekræftet, at den pågældende er for eksempel 14 år, men kender ikke barnets navn, adresse, cpr-nummer og så videre. Dette anser It-sikkerhedskomiteén for vigtigt, da egentlig identifikation indebærer problemer i relation til sikringen af barnets eller den unges privatliv.

Ungdomsbeviset har imidlertid den begrænsning, at der iværksættes en løsning, som kun giver mulighed for en delvis beskyttelse af barnet eller den unge. Barnet eller den unge kan vælge andre chatrum, der ikke har implementeret ”ungdomsbevis”. Og chikane kan også finde sted fra personer, der er på alder med barnet eller den unge. Endelig kan det risikere at udelukke mulighed for gode og ønskelige kontakter mellem børn og voksne.

På denne baggrund anbefaler It-sikkerhedskomiteén en dobbelt løsningsmodel.

### 3. It-sikkerhedskomiteéns anbefalinger – dobbelt løsning

It-sikkerhedskomiteén anbefaler,

- at it-kulturen vedrørende de sociale netværkstjenester sættes til debat, og
- at det overvejes at fremme anvendelsen af et ungdomsbevis

#### 3.1. It-kulturen vedrørende sociale netværkstjenester til debat

It-sikkerhedskomiteén foreslår, at der for det første gøres en indsats for at opnå en større bevidsthed om problemet hos børn og unge, hos deres forældre og hos deres lærere. Kun ad denne vej kan man opnå en omfattende grad af beskyttelse. Uanset hvor raffinerede ”tekniske beskyttelsesløsninger” der eventuelt indføres, kan de aldrig fuldstændigt beskytte barnet eller den unge mod uønskede kontakter, da der altid vil være netværkstjenester, som ikke indeholder beskyttelsesmekanismerne. Ydermere er det svært at undgå alle former for misbrug ved en teknisk løsning. Opbygning af viden om risikoen ved at bruge netværkstjenesterne hos barnet eller den unge og deres forældre er vigtig. Tilsvarende er det vigtigt, at børn og unge lærer om fornuftig brug af de sociale netværkstjenester. It-kulturen ved de sociale netværkstjenester skal til debat.

IT- og Telestyrelsen

Side 4/4

#### 3.2. Tekniske muligheder for et ungdomsbevis

Såfremt der fra politisk hold ønskes indført en teknisk løsning, er etablering af et ungdomsbevis en mulighed. Det kan baseres på aldersbekræftelse ved autentifikation. Herved gives alle børn og unge, der bruger online sociale netværkstjenester, et yderligere valg – en mulighed for at gardere sig mod uønsket voksenkontakt. Den tekniske implementering af et ungdomsbevis bør først og fremmest ske under hensynstagen til, at børnenes privatliv bevares. Herved forstås, at børnene skal kunne få deres alder bekræftet (autentifikation af alder). For It-sikkerhedskomiteén er det væsentligt, at børnene og de unge ikke skal kunne identificeres af hverken tjenesteudbyderen (for eksempel Arto) eller af den, der autentificerer alderen (for eksempel CPR-registret eller UNI-C). I tilfælde af mistænkelig opførsel bør et samspil mellem alle sagens parter være nødvendigt for at identificere den pågældende person.

It-sikkerhedskomiteén anbefaler en løsning, hvor børnene gøres opmærksom på, at tjenesterne indhenter en bekræftelse af deres alder. Tjenesten bør således anvende en form for oplysende samtykke, hver gang et barn skal autentificere sig overfor en tjenesteudbyder.

For at sikre børnene bedst muligt, anbefaler It-sikkerhedskomiteén på sigt at undersøge muligheden for, at en teknisk løsning indeholder hardware orienterede tiltag, det vil sige at en software-baseret løsning med login og password kombineret med en fysisk enhed, der beskytter børnene yderligere i deres interaktion på nettet. En sådan fysisk enhed kan benytte sig af biometrisk godkendelse og således gøre det sværere at misbruge enheden, og dermed barnets ungdomsbevis. Men for at komme hurtigt i gang på det eksisterende tekniske fundament, ser It-sikkerhedskomiteén en software løsning som mest nærliggende.

En implementering af en teknisk løsning forudsætter en nærmere beregning af de økonomiske omkostninger, der, som udgangspunkt forventes løftet økonomisk af tjenesteudbyderne. Her foreslår It-sikkerhedskomiteén, at man i videst mulig omfang benytter sig af eksisterende løsninger, der kan minimere de samlede udgifter. En implementering af en teknisk løsning omfatter også en afklaring af principperne for udstedelse af et ungdomsbevis. Det vil sige, hvordan ungdomsbeviset i første omgang skal udstedes til børnene, herunder hvordan man i denne proces sikrer, at ungdomsbeviserne ikke udstedes fejlagtigt. It-sikkerhedskomiteén anser netop denne del af processen som meget væsentlig, idet manglende undersøgelse på dette område kan resultere i en proces, der ikke er hensigtsmæssigt – hverken overfor børnene, overfor sikkerheden, eller overfor de økonomiske perspektiver i løsningen. Endelig forudsætter en teknisk løsning en forhandling med de danske leverandører, der udbyder sociale netværkstjenester.

#### 4. Konference

IT- og Telestyrelsen

Den foreslåede dobbelte indsats vil efter It-sikkerhedskomiteéns opfattelse skabe den bedst mulige beskyttelse af børn og unge i relation til sociale netværkstjenester.

Side 5/5

Som led i It-sikkerhedskomiteéns bidrag til at skabe viden og opmærksomhed omkring online sociale netværkstjenester afholdes den 11. november 2008 en konference "Privatliv på profilen" om borgernes holdninger til og adfærd på online sociale netværkstjenester.

It-sikkerhedskomiteén ønsker med konferencen at tage hul på den brede debat omkring borgernes opførsel og holdninger til privatliv på online sociale tjenester.

Indlæg på konferencen vil blandt andet omhandle:

- Det fundamentale værdigrundlag – frihed, ansvar, omsorg – for hvem?
- Hvem bruger de sociale tjenester – og hvem udbyder dem?
- Skal der mere politisk fokus på spørgsmålet?
- Hvordan opnår vi balance, så vi kan bruge de mange spændende muligheder, de sociale netværkstjenester byder på?
- Hvordan opnår vi brug uden misbrug - og bevarer borgernes sikkerhed, tryghed og tillid til den digitale verden?

**Bilag 1**

Oversigt over løsninger repræsenteret ved leverandører til stede på It-sikkerhedskomiteens workshop 1. august.

	UNI-Login (UNI-G)	Nøgleskabet (EDB- gruppen)	Net-Safe (Netamia)	CertifiedKd (CertifiedKd)	Privacy credential (Priway)	WAYF
<b>Produktstatus</b>	Leverings- klart	Leverings- klart	Prototype	Prototype	Koncept	Leverings- klart
<b>Autentifi- kation</b>	Ja – valgfri	Ja – valgfri	Ja – valgfri	Ja – alder og køn	Ja – Valgfri	Ja - valgfri
<b>Fuld identifikation</b>	Ja	Ja	Valgfri	Nej	Nej	Valgfri
<b>Samtykke</b>	Nej	Nej	Nej	Ja	Ja	Ja
<b>Sporbarhed</b>	Ja	Ja	Ja –valgfri	Ja	Ja –valgfri	Ja – valgfri
<b>Mobiltet</b>	Ja	Ja	Ja	Ja	Ja	Ja
<b>Platforms- uafhængigt</b>	Ja	Ja	Ja	Ja	Ja	Ja
<b>HW/SW baseret</b>	SW	SW	SW	SW	HW	SW

IT- og Telestyrelsen

Side 6/6

**Tabel 1**