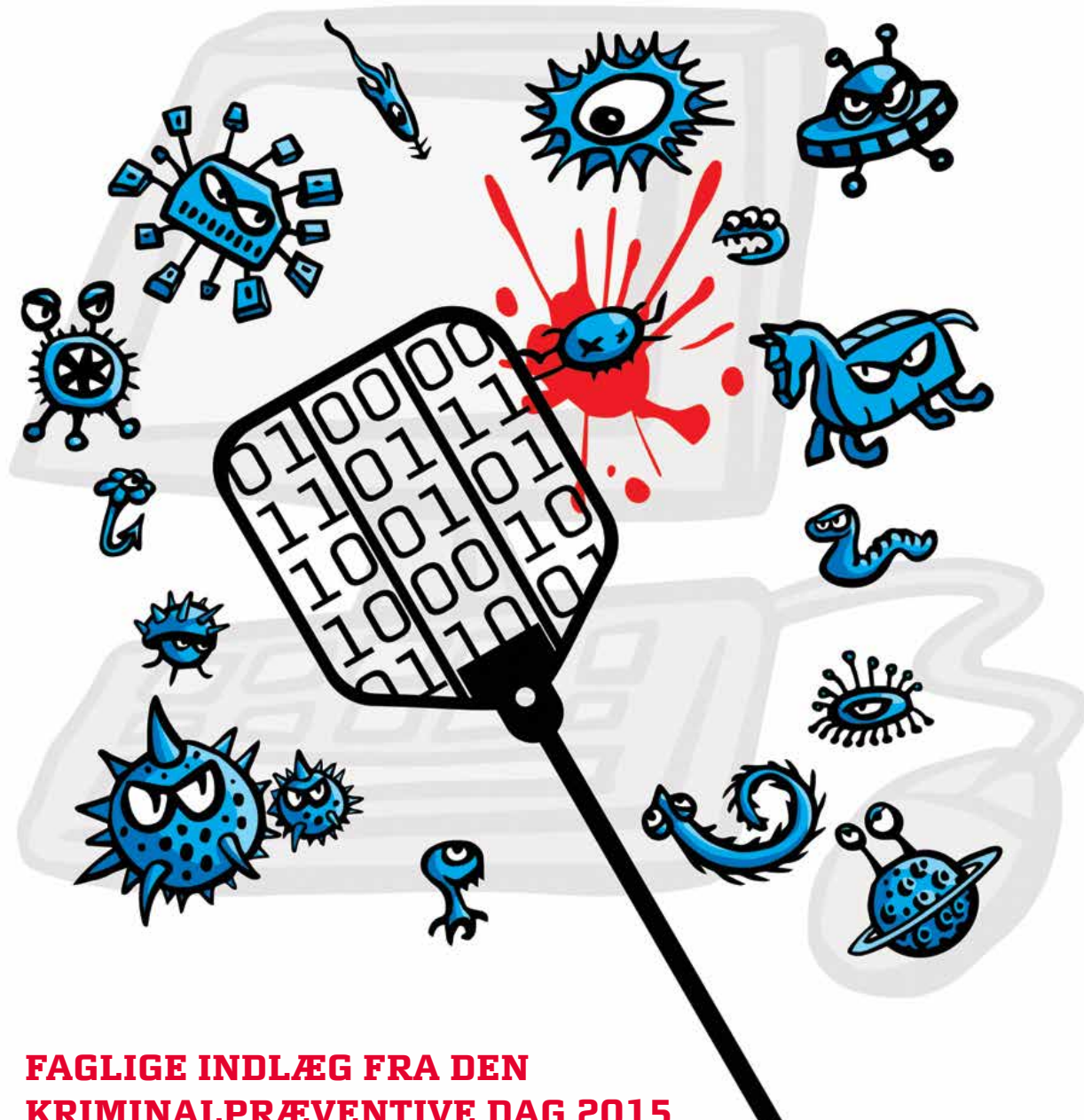


ANGREB OG OVERGREB I CYBERSPACE

- HVORDAN FOREBYGGER VI DET?



FAGLIGE INDLÆG FRA DEN
KRIMINALPRÆVENTIVE DAG 2015



DET KRIMINAL
PRÆVENTIVE RÅD

TrygFonden

Det Kriminalpræventive Råd

Ejby Industrivej 125 - 135

2600 Glostrup

45 15 36 50

dkr@dkr.dk

dkr.dk

Ansvarshavende redaktør: Anna Karina Nickelsen

Tekst: Journalist Henrik Jensen, Hos Journalisterne

Foto: s. 5: © Colorbox

Øvrige fotos: © Michael Bo Rasmussen

Vignetter og forsidegrafik: © Lars Bjørstrup

DKR nr.: 14-422-0098

ISBN: 978-87-92966-28-5

Juni 2015

Kopiering tilladt med kildeangivelse.





INDHOLD

PÅ FORKANT MED UDVIKLINGEN,	5
Interview med Linda Nielsen, formand for DKR	
DEL 1: IT-KRIMINALITET MOD BORGERNE	
Internetkriminalitet rammer årligt 150.000 danskere	6
Om undersøgelsen "Internetkriminalitet 2014" af Peter Kruize	
Svindelmails bruger kendte salgsteknikker	8
Prof. dr. Peter Fischer om nigeriabreve mm.	
Personlige data på nettet er guld værd	11
Journalist og forfatter Pernille Tranberg om Digitalt selvforsvar	
DEL 2: BØRN OG UNGE PÅ INTERNETTET	
Børn har brug for voksne i den digitale verden	12
Lektor Gitte Stald om undersøgelsen EU kids online	
Unge møder mere ekstremistisk indhold på nettet	14
Socialstyrelsen om radikaliserings via nettet	
Tonen er grov i digital mobning	17
Lektor Jette Kofoed om mobning på sociale medier	
Det værste er tonen på nettet	18
Elever fra 8. klasser om unge og sociale medier	
DEL 3: ORGANISERET CYBERCRIME	
Organiseret kriminalitet på nettet udfordrer politiet	20
Vicepolitiinspektør Tormod Husted, NEC om politiets efterforskning af cybercrime	
Dansk politi styrker indsatsen mod cybercrime	22
Centerchef Kim Aarenstrup om Det Nationale Cybercrime Center	
Hacker-begrebet spænder vidt	25
Tidligere hacker Raoul Chiesa om forskellige hackerprofiler	
IT-VÆRKTØJ HJÆLPER UDSATTE BØRN	
Om politiets nye it-redskab, Socialsøg	27



PÅ FORKANT MED UDVIKLINGEN

IT-KRIMINALITET VAR TEMAET PÅ DEN KRIMINALPRÆVENTIVE DAG 2015. FORMAND FOR DET KRIMINALPRÆVENTIVE RÅD LINDA NIELSEN HÅBER, AT DAGEN HAR VÆRET MED TIL AT SÆTTE CYBERCRIME PÅ DAGORDENEN, INDEN PROBLEMET FOR ALVOR VOKSER SIG STORT I DANMARK.

”Det er helt sikkert, at it-kriminalitet vil blive en stigende udfordring i de kommende år. I forhold til den kriminalitetsforebyggende indsats står vi på dørtærsklen til en ny virkelighed, som vi ved kommer,” siger Linda Nielsen.

Den Kriminalpræventive Dag, der blev holdt den 23. april i Aalborg Kongres & Kultur Center, var arrangeret af Det Kriminalpræventive Råd i samarbejde med TrykFonden.

Mere end 600 deltagere fra landets politikredse, kommuner og mange andre, der er involveret i kriminalpræventivt arbejde, var mødt op for at blive klogere på, hvordan man kan forebygge it-kriminalitet.

”Endnu er kriminalitet og bedrageri på nettet ikke et stort problem i Danmark, men det kan det nemt blive i fremtiden. Når vi har sat cyberkriminalitet på dagsordenen med den kriminalpræventive dag, så er det også for at prøve at tage problemet alvorligt, inden det vokser sig stort,” siger Linda Nielsen.

MANGLER VIDEN OG OVERBLIK

Dagen igennem blev der præsenteret ny viden om, hvordan it-kriminaliteten udvikler sig både i Danmark og interna-

tionalt. Der var workshops og oplæg fra eksperter blandt andet om, hvad myndighederne gør for at bekæmpe cybercrime, og hvordan børn og unge håndterer de mange nye udfordringer i den digitale verden.

Ifølge Linda Nielsen er der ikke tilstrækkelig viden om, hvordan it-kriminalitet udvikler sig i Danmark.

”Vi savner overblik, når det handler om it-kriminalitet. Det er et område, hvor der endnu ikke eksisterer en masse grundlæggende viden, som vi kan tage udgangspunkt i, når det handler om forebyggelse,” siger hun.

Det Kriminalpræventive Råd har valgt, at cyberkriminalitet skal være et af rådets strategiske indsatsområder i de kommende år, og Linda Nielsen ser dagen i Aalborg som en god begyndelse for den kriminalpræventive indsats i forhold til it-kriminalitet.

”Den Kriminalpræventive Dag er en god måde til at skabe en fælles dagsorden sammen med de øvrige aktører på det kriminalpræventive område, så der kommer til at ske noget i den virkelige verden. Jeg håber, at vi kan bruge dagen i Aalborg som afsæt til, at vi får sat mere fokus på forebyggelsen af it-kriminalitet i Danmark,” siger hun.



INTERNETKRIMINALITET RAMMER ÅRLIGT 150.000 DANSKERE



IDENTITETSTYVERI, BEDRAGERI, AFPRESNING OG CHIKANE. SIDSTE ÅR BLEV 150.000 DANSKERE UDSAT FOR EN ELLER ANDEN FORM FOR INTERNETKRIMINALITET. DET VISER EN NY RAPPORT OM INTERNETRELATERET KRIMINALITET I DANMARK FRA DET KRIMINALPRÆVENTIVE RÅD.

"Tallet er faktisk lidt lavere, end jeg havde forventet. Det er en lille positiv overraskelse, at antallet af danskere, der har været ude for internetkriminalitet i 2014, trods alt ikke er højere," siger kriminolog på Københavns Universitet Peter Kruize, der har foretaget undersøgelsen for Det Kriminalpræventive Råd.

Ifølge undersøgelsen var det cirka 3,6 procent af danskere i alderen 16-74 år, der var ofre for internetkriminalitet i 2014. Et fald i forhold til 2013, hvor det var 4,0 procent. Forskellen er dog så lille, at den ikke er statistisk signifikant. "Jeg havde forventet en stigning, så selvom der kun er tale om et mindre fald, mener jeg alligevel, at det er positivt," siger Peter Kruize.

MINDRE FUPHANDEL

Undersøgelsens resultater dækker over modsatrettede tendenser og udviklinger i de forskellige former for internetkriminalitet i Danmark.

Fra 2013 til 2014 har der fx været en markant nedgang i antallet af sager, hvor danskere er blevet bedraget i forbindelse med handel på internettet. Det kan blandt andet dreje sig om falske webbutikker eller handel med privatpersoner, hvor man aldrig modtager den vare, man har betalt for.

Ifølge undersøgelsen var der i 2014 cirka 22.500 danskere, der blev ofre for

bedrageri i forbindelse med internethandel - et kraftigt fald fra 2013, hvor cirka 110.000 danskere blev udsat for internethandelsbedrageri.

Omvendt viser undersøgelsen en stigning i ofre for betalingskortmisbrug fra under 30.000 i 2013 til cirka 75.000 i 2014. Når danskere bliver udsat for betalingskortmisbrug, sker det ofte efter, at de er blevet franarret deres betalingskortoplysninger i forbindelse med nethandel.

BRUG FOR FOREBYGGELSE

Der foregår stadig langt mere kriminalitet og tyveri i den fysiske verden sammenlignet med den digitale verden. Hvor det ifølge undersøgelsen var cirka 3,6 procent af danskerne, som i løbet af de seneste år var ofre for it-kriminalitet, var det til sammenligning 11 procent af danskerne i samme aldersgruppe, der i 2013 var udsat for tyveri i den fysiske verden.

"Det er positivt, at risikoen for at blive udsat for grimme ting på nettet ikke er så stor. Selvom det godt kan bekymre, at undersøgelsen viser en kæmpe stigning i misbrug af betalingskort, men det er heldigvis også det område, hvor borgerne er allerbedst beskyttet," siger konsulent Anders Young Rasmussen fra Det Kriminalpræventive Råd.

Ifølge reglerne for betalingskort er det således i sidste ende ikke borgeren,

der sidder med det økonomiske tab, men typisk banken, hvis betalingskortoplysningerne er blevet opsnappet af fx en hacker på internettet.

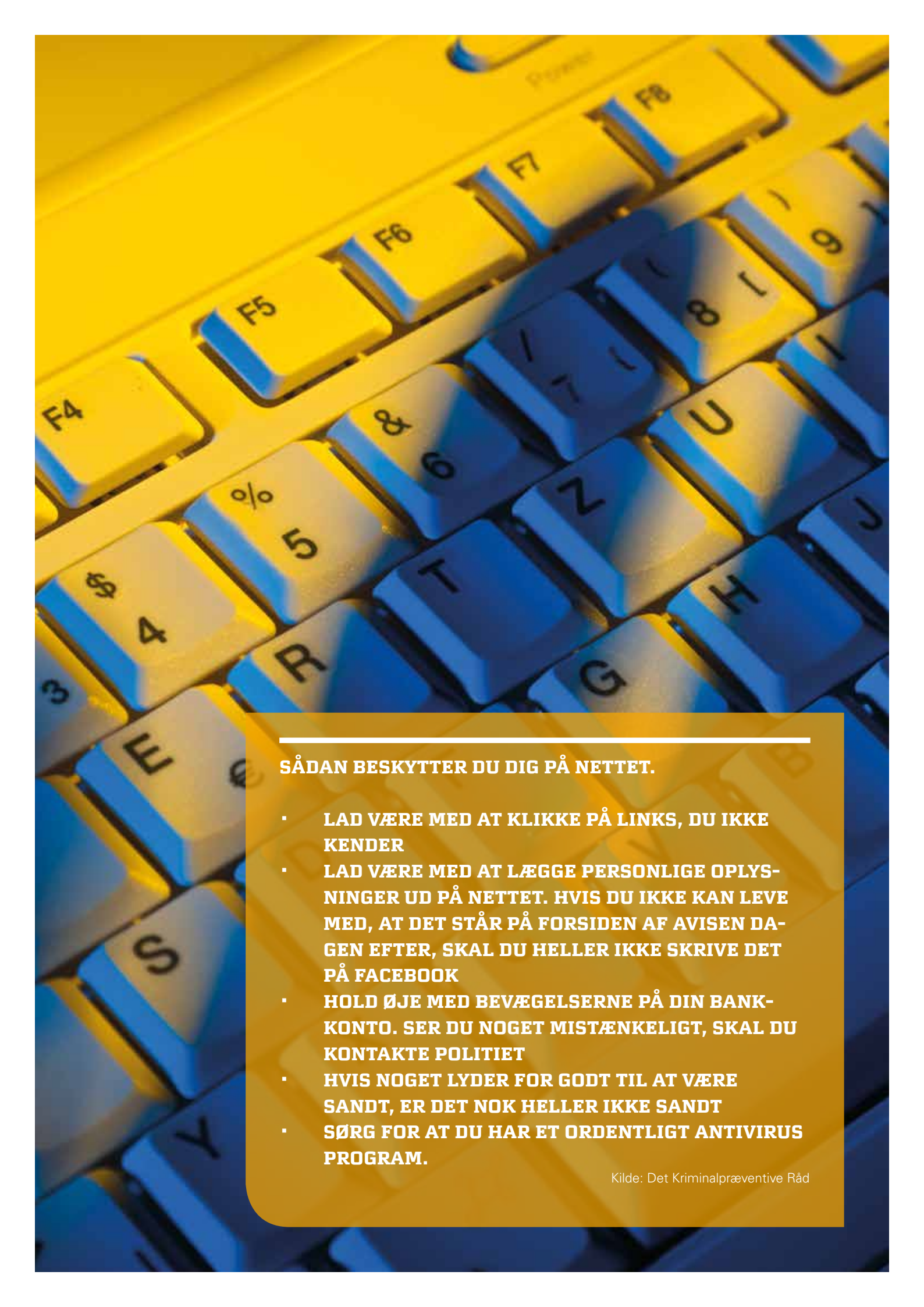
Som forbruger kan man gøre flere ting for at forebygge, at man bliver udsat for kriminalitet på nettet.

"Der er behov for, at borgerne bliver klædt bedre på til at undgå at komme i situationer, hvor deres betalingskort bliver misbrugt. Og at virksomhederne bliver bedre til at sikre sig selv og deres kunder i forbindelse med internethandel," siger Anders Young Rasmussen.

Klik for at høre indlæg her:



UNDERSØGELSEN "INTERNETKRIMINALITET 2014 – IDENTITETSTYVERI, BEDRAGERI, AFPRESNING OG CHIKANE I CYBERSPACE" ER FORETAGET AF KRIMINOLOG PÅ KØBENHAVNS UNIVERSITET PETER KRUIZE FOR DET KRIMINALPRÆVENTIVE RÅD. UNDERSØGELSEN BLEV OFFENTLIGGJORT PÅ DEN KRIMINALPRÆVENTIVE DAG 2015.



SÅDAN BESKYTTER DU DIG PÅ NETTET.

- **LAD VÆRE MED AT KLIKE PÅ LINKS, DU IKKE KENDER**
- **LAD VÆRE MED AT LÆGGE PERSONLIGE OPLYSNINGER UD PÅ NETTET. HVIS DU IKKE KAN LEVE MED, AT DET STÅR PÅ FORSIDEN AF AVISEN DAGEN EFTER, SKAL DU HELLER IKKE SKRIVE DET PÅ FACEBOOK**
- **HOLD ØJE MED BEVÆGELSERNE PÅ DIN BANKKONTO. SER DU NOGET MISTÆNKELIGT, SKAL DU KONTAKTE POLITIET**
- **HVIS NOGET LYDER FOR GODT TIL AT VÆRE SANDT, ER DET NOK HELLER IKKE SANDT**
- **SØRG FOR AT DU HAR ET ORDENTLIGT ANTIVIRUS PROGRAM.**

Kilde: Det Kriminalpræventive Råd



SVINDELMAILS BRUGER KENDTE SALGSTEKNIKKER

VI KENDER DEM ALLE SAMMEN. DE FALSKE SPAMMAILS, DER ØNSKER TILLYKKE MED DEN STORE LOTTERIGE VINST ELLER TILBYDER ET "BUSINESS PROPOSAL", DER LYDER FOR GODT TIL AT VÆRE SANDT.

De såkaldte nigeriabreve har eksisteret i mere end et kvart århundrede. Som regel er de skrevet på dårligt dansk eller engelsk og bliver ofte fanget i mailprogrammernes spamfiltre. Men de bliver ved med at komme, for selvom brevene for de fleste virker nemme at gennemskue, er der alligevel altid nogle få, der lader sig narre af de masseudsendte svindelmails.

"Bagmændene bag svindelmails'ene ved præcist, hvad de gør, og hvordan de udnytter de psykologiske faktorer, der kan lokke folk i fælden. Brevene indeholder fristende tilbud, som gør det svært for nogle at handle rationelt," siger prof.dr. Peter Fischer fra Psykologisk Institut på Regensburg Universitet i Tyskland.

FRA MANGE LANDE

Nigeriabreve er en fællesbetegnelse for svindel, der hovedsageligt foregår via mail. Metoden blev første gang kendt i Europa i 1987, hvor virksomheder be-

gyndte at modtage breve, der gav sig ud for at være afsendt af nigerianske embedsmænd. I dag kommer brevene ikke kun fra Nigeria, men også fra for eksempel Uganda, Irak, Holland og USA.

Udover falske gevinstmeddelelser fra lotterier og tilbud om lukrative forretningsaftaler kan brevene også tilbyde mirakelkure imod alvorlige sygdomme. Eller de kommer fra en person, der angiveligt har en masse penge stående på sin bankkonto, og som vil betale sig til hjælp med at få et stort pengebeløb ført ud af sit hjemland.

Målet med nigeriabrevene er at få modtagerne til at indbetale et mindre beløb, oplyse sine bankoplysninger eller klikke på et virusinficeret link.

KENDTE SALGSTEKNIKKER

Peter Fischer har i flere forskningsprojekter undersøgt metoderne i nigeriabrevene og forsøgt at finde frem til, hvorfor nogle modtagere af brevene lader sig bondefange.

"I virkeligheden benytter brevene sig af helt traditionelle og kendte markedsførings- og salgsteknikker. De forsøger at få modtageren til at handle irrationelt ved at udnytte menneskelige motivationsfaktorer som grådighed, anerkendelse eller spænding," siger Peter Fischer.

Desuden forsøger brevene at fremstå autoritære og giver ofte en kort frist til at tænke sig om, da man som regel skal svare øjeblikkeligt for ikke at miste chancen for den store gevinst.

TRE TYPER OFRE

Peter Fischer har interviewet en lang række personer, der er blevet narret af nigeriabreve, og placerer dem i tre grupper.

Personer, som i bakspejlet ikke kan forstå, at de kunne være så godtroende.

Personer, som stædigt fastholder, at de ikke havde nogen rimelig mulighed for at gennemskue svindlen.

Og så er der også personer, der fra starten var stort set klar over, at de blev snydt, men alligevel vurderede, at det var en kalkuleret risiko, der var værd at løbe.

"Desto større gevinst, desto større risiko er folk villige til at løbe, når det gælder svindelmails. Det er meget naturligt. Mennesker er født med en positiv illusionsevne, der gør, at vi let kommer til at overvurdere vores egne evner, og det gør os til mulige naive ofre for disse svindelnumre," siger Peter Fischer.

Klik for at høre indlæg her:





PROF.DR. PETER FISCHER FRA PSYKOLOGISK INSTITUT PÅ REGENSBURG UNIVERSITET I TYSKLAND HAR I FLE-RE FORSKNINGSPROJEKTER UNDERSØGT SVINDEL-METODERNE I NIGERIABREVEN. HAN VAR BLANDT OPLÆGSHOLDERNE PÅ DEN KRIMINALPRÆVENTIVE DAG 2015.



Don't Give Data To A Stranger

ber: Dataejendomme Big Data



PERNILLE TRANBERG ER SELVSTÆNDIG FORFATTER OG JOURNALIST I FIRMAET, DIGITAL IDENTITET, DER RÅDGIVER OM AT BESKYTTE OG KONTROLLERE PERSONDATA OG TRIMME SIT DIGITALE OMDØMME. DESUDEN UDVIKLER HUN PRIVACYKOM-PASSET.DK FOR ERHVERVSSTYRELSEN, DER SKAL HJÆLPE DANSKE VIRKSOMHEDER I GANG MED BIG DATA PÅ EN ANSVARLIG MÅDE. LÆS MERE PÅ [HTTP://DIGITAL-IDENTITET.DK](http://digital-identitet.dk). PERNILLE TRANBERG VAR BLANDT OP-LÆGSHOLDERNE PÅ DEN KRIMINALPRÆVENTIVE DAG 2015.



PERSONLIGE DATA PÅ NETTET ER GULD VÆRD



VORES PERSONLIGE DATA ER NUTIDENS OLIE ELLER GULD. PROBLEMET ER, AT VI IKKE VED, HVILKEN PRIS VI BETALER, NÅR VI LADER OPLYSNINGER OM VORES LIV FLYDE PÅ NETTET. DERFOR ER DER GOD GRUND TIL DIGITALT SELVFORSVAR.

I virkelighedens verden er det de færreste af os, der vil videregive oplysninger til fremmede om vores kontakters telefonnumre, indholdet i vores sms'er eller hvor vi har været den seneste uge. Men i den digitale verden tillader vi det. Vi lader fx Facebook og Google følge med i stort set alt, hvad vi foretager os på nettet, og vi installerer gratis app's og giver til gengæld grønt lys til, at vi bliver kigget over skulderen.

"Vores persondata bliver i stor stil indsamlet og videresolgt, men vi aner ikke, hvordan vores oplysninger bliver brugt, eller hvordan en gammel Facebook-opdatering fortolkes i en nutidig sammenhæng. Derfor er det en god idé at forsøge at beskytte og trimme sin digitale identitet," siger Pernille Tranberg, der er konsulent i privacy på nettet.

Virksomheder indsamler og videresælger data om vores interesser, smag, religion, alder, politiske overbevisning, helbred, seksuelle orientering, venner osv. Oplysningerne bliver blandt andet brugt til at målrette reklamer til os alle vegne på nettet.

"Det kan virke temmelig uskyldigt, at vi på nettet bliver forfulgt af en reklame for et par støvler eller en skiferie. Men indsamlingen af vores data bliver også i stigende grad brugt til at give individualiserede priser. Har du rige forældre, en høj indkomst eller er du meget afhængig af et bestemt produkt, vil det afspejle sig i den pris, som du bliver tilbudt," siger Pernille Tranberg.

VI BLIVER GENNEMSIGTIGE

Vores adfærd på nettet betyder ikke kun noget for, hvad vi skal betale for forskellige produkter, eller hvilke reklamer vi bliver mødt af. Det kan ifølge

Pernille Tranberg også få betydning for, om vi kan få et job, en uddannelse eller en kæreste.

"Forskere har bevist, at hvis man kan få adgang til en ansøgers facebookprofil, så er det langt bedre end at hyre en erhvervspsykolog til at hjælpe med at vælge den rette kandidat til et job. Vi googler jo alle hinanden, og et forkert tweet eller like kan få store konsekvenser for vores liv," siger hun.

Pernille Tranberg mener ikke kun, at udviklingen har konsekvenser for os som individer – det har også store konsekvenser for hele vores samfund, at vi bliver mere gennemsigtige som mennesker:

"I et demokrati, er det staten og virksomhederne, der skal være åbne og gennemsigtige, mens individer skal beskyttes. Men lige nu sker der det stik modsatte. Vi er som borgere hele tiden offentlige og fortæller alt om os selv, mens stater og virksomheder bliver mere og mere lukkede."

DIGITALT SELVFORSVAR

Pernille Tranberg har selv taget sine forholdsregler på nettet, hvor hun udøver det, hun kalder digitalt selvforsvar. Hun optræder fx under falsk navn og identitet på Facebook, blokerer for cookies og bruger søgemaskiner og app's, som ikke sporer hende. Til gengæld optræder hun under eget navn på Twitter, LinkedIn og i alle professionelle sammenhænge.

"Det er en menneskeret at være anonym – også i den digitale verden. Retten til at bestemme over vores eget liv og vores egne data er utroligt vigtigt i et demokrati," siger hun.

Klik for at høre indlæg her:



Meget tyder på, at der også er en modreaktion i gang. Forbrugerne bliver mere og mere skeptiske og utrygge ved at blive kigget over skulderen, og det betyder, at virksomheder, som forstået at kapitalisere på data uden at smide respekten for kundernes privatliv over bord, vinder kampen om fremtidens digitale marked.

"Flere og flere digitale produkter bliver designet, så standardindstillingerne er, at du er privat, og flere virksomheder markedsfører sig på, at de er private og ikke videresælger dine data. Retten til at bestemme over vores egne data bliver et konkurrenceparameter i fremtiden, men vi risikerer ligesom med økologi, at det kun er noget de rige og veluddannede får råd til," siger Pernille Tranberg

TIPS

Her er en række konkrete tips, og du kan læse mere i Pernille Tranbergs bog, License2share på: <http://license2share.dk/startpage.com>
Søgemaskiner der ikke sporer dig:
duckduckgo.com
qwant.com

Effektive programmer til blokering af cookies:
disconnect.me

Blokering af reklamer:
adblockplus.org

Sikker e-mail som ikke opsamler dine data:
neomailbox.com
countermail.com

Sikker app til chat:
wickr

Få et godt falsk navn:
fakenamegenerator.com



BØRN HAR BRUG FOR VOKSNE I DEN DIGITALE VERDEN

BØRN OG UNGE HAR BRUG FOR STØTTE OG VEJLEDNING FRA DERES FORÆLDRE, NÅR DE BRUGER DE DIGITALE MEDIER. MEN NOGET TYDER PÅ, AT DANSKE FORÆLDRE I DAG ER KNAPT SÅ GODE SOM TIDLIGERE TIL AT TALE MED DERES BØRN OM DERES OPLEVELSER PÅ INTERNETTET.

"Der er en tendens til, at færre forældre i Danmark taler med deres børn om, hvordan de bruger de digitale medier. Antallet af forældre, der aktivt støtter deres børn og giver dem gode råd i forhold til internettet og digitale medier, er faldet i de senere år, og det er lidt bekymrende," siger Gitte Stald, som er lektor på it-Universitetet i København. Som medieforsker er hun den danske repræsentant i to store europæiske forskningsprojekter, EU Kids Online og Net Children Go Mobile, der begge har undersøgt europæiske børn og unges brug af digitale medier. Projekterne sluttede med udgangen af 2014

FÆRRE FORÆLDRE STØTTER

EU Kids Online, blev gennemført i 2010 i 33 europæiske lande, mens Net Children Go Mobile blev gennemført i 2013-14 i syv europæiske lande. Når man sammenligner resultaterne fra de to projekter, viser det sig, at den såkaldte forældremediering i Danmark er faldende.

Hvor det i 2010 var 67 procent af alle danske forældre, der aktivt guidede deres børn og talte med dem om mulig-

heder, risici og opførsel på internettet, var det i 2014 faldet til 60 procent. "Det er ikke noget voldsomt fald, men det er trods alt en negativ udvikling i forhold til de fleste andre lande i Europa, hvor forældremedieringen stiger," siger Gitte Stald, der dog understreger, at det er hendes erfaring, at de fleste danske forældre aktivt interesserer sig for deres børns færden i den digitale verden. "Men det er også virkelig vigtigt, at forældre og andre voksne, der har med børn og unge at gøre, er på banen i forhold til unges brug af de digitale medier. Forældre skal tage det samme ansvar for deres børn i den online verden, som de gør i den offline verden," siger hun.

BØRN HAR BRUG FOR VÆRDIER

Gitte Stald peger på, at nogle forældre oplever, at det er svært at følge med i, hvad deres børn laver på internettet. Men hun understreger, at det er vigtigt, at børnene ikke bliver overladt til sig selv på de digitale medier.

"Børn og unge kan godt være kompetente på nogle områder, men helt generelt har de stadigvæk meget brug for, at de voksne giver dem nogle værdier og normer, som gælder, uanset om tingene foregår online eller offline," siger hun.

Det kan godt være, at voksne ikke kender alle de sidste applikationer, og heller ikke tænker på computere og it på samme måde, som de unge gør.

"Men vi ved jo godt, hvordan man skal opføre sig overfor vennerne, og hvordan man skal være forsigtig med at møde fremmede, når man ikke er på de digitale medier. Alt det gælder også

i den digitale verden, og der har børn og unge brug for støtte og vejledning fra deres forældre," siger Gitte Stald.

VEJLEDNING VIRKER

Danmark er sammen med de øvrige skandinaviske lande og Holland de lande i Europa, hvor børn og unge har mest adgang til digitale medieplatforme og digitalt indhold.

Af samme grund er danske børn og unge ifølge de europæiske undersøgelser også blandt dem, der er mest udsatte i forhold til risikoadfærd på nettet i form af fx digital mobning, seksuelle billeder, skræmmende indhold og kontakt med ukendte personer.

Fra 2010 til 2014 er der ifølge EU Kids Online sket en klar stigning i antallet af danske børn og unge, der møder de forskellige typer af negative oplevelser på nettet. Ifølge Gitte Stald er danske børn dog også blandt de bedste til at håndtere risikoadfærd på en god måde.

Undersøgelserne viser, at især de yngre danske børn gerne vil have vejledning og gode råd fra forældre og andre voksne, og det virker:

"Vi kan se ud fra undersøgelserne, at børn får færre negative oplevelser i forbindelse med risici på de digitale medier, når forældrene er gode til at tale med dem om deres oplevelser og dermed gøre dem bedre til at håndtere de forskellige situationer, de kan komme ud for på nettet," siger Gitte Stald.

Klik for at høre indlæg her:





GITTE STALD ER LEKTOR OG MEDIEFORSKER PÅ IT-UNIVERSITETET I KØBENHAVN. HUN ER MED TIL AT LAVE TO STORE EUROPÆISKE UNDERSØGELSER EU KIDS ONLINE OG NET CHILDREN GO MOBILE SAMT EN RÆKKE DANSKE UNDERSØGELSER AF UNGE DANSKERES BRUG AF DIGITALE OG MOBILE MEDIER. GITTE STALD VAR BLANDT OPLÆGSHOLDERNE PÅ DEN KRIMINALPRÆVENTIVE DAG 2015.



UNGE MØDER MERE EKSTREMISTISK INDHOLD PÅ NETTET

INTERNETTET SPILLER EN STADIG STØRRE ROLLE FOR MILITANTE TERRORGRUPPER OG EKSTREMISTER, SOM UDNYTTET INTERNETTET TIL AT SPREDE DERES BUDSKABER. NETTET BUGNER MED VIDEOER OG PROPAGANDAMATERIALE, OG DET ER BLEVET LETERE FOR UNGE OG ANDRE AT STØDE IND I EKSTREMISTISK MATERIALE, NÅR DE FÆRDES PÅ INTERNETTET.

”Det ekstremistiske indhold spredt sig i højere og højere grad på fx Facebook og YouTube. I modsætning til tidligere, hvor det ekstremistiske indhold typisk var at finde på lukkede fora, kan man i dag ofte finde det på almindelige mainstream sociale medier, hvor alle færdes,” siger souschef Michael Karlsen fra Socialstyrelsen. Han er faglig leder for det område i styrelsen, der beskæftiger sig med forebyggelse af ekstremisme.

SPILLER PÅ FØLELSERNE

Materialet der spredes på nettet, kan både være militant islamistisk propagandamateriale i form af relativt professionelt lavede videoer. De sidste par år har der floreret en del materiale, som blandt andet har til formål at få unge til at rejse til Syrien for at kæmpe for Islamisk Stat eller Al-Nusra.

Det ekstremistiske indhold på internettet kan også komme fra andre grupper i form af for eksempel stærkt racistiske holdninger og udsagn.

”YouTube-videoerne søger at opildne til krig eller drab ud fra et ekstremt enkelt verdensbillede. De bruger vold-

somme billeder, dramatisk musik og andre virkemidler, der spiller på følelserne hos dem, som ser filmene. Videoerne er ofte lavet, så de går lige til grænsen for, hvad man må videregive på de sociale medier,” siger Michael Karlsen.

RADIKALISERER IKKE ALENE

Selvom det er god grund til at være på vagt over for den stigende mængde af propagandamateriale på internettet, så understøtter Michael Karlsen, at det er vigtigt ikke at overvurdere effekten af det ekstremistiske indhold.

”Det er selvfølgelig problematisk, at flere unge i al almindelighed kan komme i berøring med materialet. Men forskningen viser, at det ikke bare er sådan, at unge sidder i deres lejligheder og bliver radikaliseret alene ved at kigge på videoer på nettet,” siger han: ”Man plejer at kunne sige, at en radikaliseringsproces kan blive accelereret af det, du finder på nettet. De unge kan blive hærdede i deres overbevisninger, og det kan også være alvorligt. Men man går ikke ud og sprænger en bombe på grund af en video på internettet.”

ET NYT UNDERVISNINGSMODUL

Efter terrorangrebene i Paris i januar vedtog regeringen at opruste terrorbekæmpelsen med en række initiativer. Et af initiativerne handler om at ruste børn og unge til bedre at kunne forstå og modstå de ekstremistiske holdninger, som de møder på internettet.

Konkret skal der laves et undervisningsmodul, der kan bruges i folkeskolen og på ungdomsuddannelserne, og som skal være med til at styrke elevernes kritiske stillingtagen til det, de møder på nettet.

”Undersøgelserne viser, at der er overraskende mange unge, som tror, at alt på internettet er sandt. Når det drejer sig om forebyggelse, er der behov for, at vi styrker de unges kildekritik og deres evner til at gennemskue ekstremistisk materiale,” siger Michael Karlsen. Det er Socialstyrelsen, der har ansvaret for at udarbejde undervisningsmodulet, som efter planen er klar til brug i skolerne i 2016.

Klik for at høre indlæg her:



A close-up, profile photograph of a young man with short, dark brown hair, looking towards the left. He is wearing a light blue collared shirt. The background is a solid, muted teal color. The lighting is soft, highlighting the contours of his face.

SOCIALSTYRELSEN ER ANSVARLIG FOR DET SOCIALT FOREBYGGENDE FOKUS PÅ EKSTREMISME OG RADIKALISERING I DANMARK. SOUSCHEF I SOCIALSTYRELSEN MICHAEL KARLSEN ER FAGLIG LEDER FOR DET OMRÅDE I STYRELSEN, DER BESKÆFTIGELSER MED FOREBYGGELSE AF EKSTREMISME. HAN VAR BLANDT OPLÆGSHOLDERNE PÅ DEN KRIMINALPRÆVENTIVE DAG 2015.



JETTE KOFOED ER LEKTOR I SOCIALPSYKOLOGI VED INSTITUT FOR UDDANNELSE OG PÆDAGOGIK PÅ AARHUS UNIVERSITET. HENDES FORSKNINGSFELT ER DIGITAL MOBNING OG BØRN OG UNGES INKLUSIONS- OG EKS-KLUSIONSPROCESSER I SKOLEN. JETTE KO-FOED VAR BLANDT OPLÆGSHOLDERNE PÅ DEN KRIMINALPRÆVENTIVE DAG 2015.

TONEN ER GROV I DIGITAL MOBNING

KENDETEGNENE VED DEN DIGITALE MOBNING ER, AT DEN IKKE ER TIL AT SLIPPE VÆK FRA, AT HELE VERDEN KAN FØLGE MED, OG DET KAN VÆRE SVÆRT AT VIDE, HVEM ELLER HVOR MANGE DER STÅR BAG.

"Fuck dig din luder. Du skulle dø. Skrid hjem til Istedgade. Verden ville være bedre uden dig."

I digital mobning er tonen grov, og både de direkte involverede og alle omkring situationen får følelserne i kog. Men digital mobning minder også på mange måder om den mobning, der foregår ansigt til ansigt:

"Al mobning handler om ekstrem eksklusion fra fællesskabet over længere tid, men der er nogle særlige aspekter ved digital mobning, som gør det komplekst på nogle andre måder," siger Jette Kofoed, der er lektor ved Institut for Uddannelse og Pædagogik på Aarhus Universitet og har digital mobning som sit forskningsfelt.

Et særligt kendetegn ved den digitale mobning er, at mobberne har mulighed for at være anonyme.

"Når du bliver mobbet i skolegården ved du, hvem der står bag. Men på nettet har alle – afhængig af platformen – mulighed for at skjule deres identitet. Det betyder, at du ikke altid ved, hvem der står bag mobningen. Du kan heller ikke vide, om afsenderen er én enkelt person eller en hel flok, der sidder sammen og skriver," siger Jette Kofoed. Hun fortæller, at når de digitale platforme gør det muligt at være anonym, bliver mobningen ofte destruktiv på nogle særlige måder.

HELE VERDEN FØLGER MED

Et andet kendetegn ved digital mobning er, at du ikke kan gemme dig for den. Du kan godt slukke din mobil eller computer, men beskederne venter på dig, når du tænder igen.

"Det er umuligt at slippe væk fra den digitale mobning. Samtidig foregår rig-

tig meget af børn og unges sociale liv på nettet, og derfor er det svært bare helt at melde fra og ikke være en del af det," siger Jette Kofoed.

Derudover er det særlige ved mobning på nettet, at den bliver eksponeret for den uendelige offentlighed. Det står ikke bare på væggen på din egen skole. Det er potentielt hele verden, der kan se, at nogle synes, du er en smatso.

"Digital mobning er forbundet med en stor grad af uvished. Ikke kun for den, som det går direkte ud over, men også for alle omkring det, for man ved ikke, om man er det næste offer," siger Jette Kofoed som mener, at det også er værd at holde øje med den tavse digitale mobning. Den handler om dem, der ikke er en del af cirkulationen. Dem som ikke modtager beskeder, som aldrig bliver tagget i et billede eller får likes fra de andre.

ALLE HAR NOGET PÅ SPIL

En af hendes vigtigste pointer er, at mobbesagerne påvirker hele fællesskabet, og at der ofte ikke kun er en enkelt udøver og et enkelt offer indblandet. Alle har noget på spil, og mobningen er udtryk for, at det er kulturen i hele klassen eller skolen, som den er gået med.

"Derfor er det vigtigt, at de voksne ikke kun leder efter en udøver og et offer, men at de har et bredere perspektiv. Digital mobning er meget komplekst, og den der er offeret den ene dag, kan være udøveren den næste, og den der så på i tavshed, kan pludselig blive næste offer," siger hun.

Det er svært at sige noget præcist om, hvor udbredt digital mobning er, for det afhænger af spørgemetoder og svarmuligheder i de forskellige undersøgelser.

Nogle undersøgelser af mobning blandt børn og unge viser, at 3 procent har været udsat for digital mobning, mens andre er helt oppe på 21 procent.

"Men hvis man som jeg mener, at det er hele fællesskabet, der bliver ramt, så er 3 procent også et højt tal, for så er det 3 procent af alle klasser, der har været involveret i digital mobning," siger Jette Kofoed.

Hun oplever, at mobning har fået meget opmærksomhed de senere år, men at der også er stor rådvildhed om, hvad man kan stille op, og mange diskussioner om, hvorvidt det er skolens eller forældrenes ansvar at gøre noget ved det.

"Til forældrene er mit råd, at de skal kende deres børns liv. Og selvfølgelig har man som forældre et ansvar for at lære sine børn om etik, og hvordan man behandler hinanden. Men da meget af mobningen foregår med afsæt i skolen og klassen, så vil jeg mene, at en stor del af ansvaret hører til i skolen," siger hun:

"Når jeg kommer ud på skolerne, siger lærerne og skolelederne som regel, at her er der ingen mobning, mens børnene siger, at der er mobning. Det er bekymrende, og derfor er jeg sikker på, at der kan gøres mere."

Klik for at høre indlæg her:



DET VÆRSTE ER TONEN PÅ NETTET

FALSKE FACEBOOK-PROFILER, HENVENDELSER FRA FREMMEDE VOKSNE OG VIDEOER MED UPASSENDT INDHOLD ER EN DEL AF DE UNGES HVERDAG PÅ NETTET. MEN IFØLGE DE UNGE ER DET STØRSTE PROBLEM ALLIGEVEL DEN TONE SOM DE BRUGER, NÅR DE SKRIVER TIL HINANDEN PÅ NETTET.

"Tonen i de beskeder, som vi sender til hinanden, er det værste ved de sociale medier. Man tør heller ikke rigtig at konfrontere folk ansigt til ansigt med det, som de har skrevet på nettet, og så får man aldrig snakket ud om det," siger Nicklas Meldgaard fra 8. klasse på Filstedvejens Skole i Aalborg.

Det Kriminalpræventive Råd havde arrangeret workshops om de sociale medier for fire 8. klasser fra Aalborg som optakt til årets Kriminalpræventive Dag. Klasserne deltog også på selve dagen, og 12 udvalgte elever var på scenen, hvor de fortalte resten af salen om deres oplevelser på nettet.

"Når man ikke kan se folk og aflæse deres kropssprog, ved man jo ikke altid, om de laver sjov, når de skriver i en hård tone. Andre gange er afsenderen anonym, og så har det ingen konsekvenser for dem, som skriver noget grimt," siger Tim Vittrup fra Filstedvejens Skole.

FALSK FACEBOOK-PROFIL

Stort set alle de unge i panelet havde oplevet at blive kontaktet af fremmede voksne.

"Som regel handler det om, at de vil have os med til nogle sexlege eller vil sende nøgenbilleder til os. Men jeg blokerer dem bare," siger Mille Glerup fra Filstedvejens Skole. Hendes kammerater håndterer henvendelserne på samme måde.

Til gengæld var det en meget dårlig oplevelse for hende, da hun opdagede, at nogen eller nogle havde oprettet en falsk profil på Facebook, hvor hendes profilbillede blev brugt.

"Jeg fandt ud af, at personen bag profilen skrev til forskellige drenge og inviterede dem til at have sex. Det var rigtig ubehageligt. Jeg har en mistanke om, hvem der stod bag, men jeg ved det ikke med sikkerhed, så jeg har aldrig fået talt det igennem med vedkommende," siger hun.

Men de sociale medier byder også på andre grænseoverskridende oplevelser:

"Jeg trykker nogle gange på et link til en video på Facebook, som viser noget, jeg slet ikke har lyst til at se. Det kan være nogle seksuelle ting eller høje skrig, som kan få mit headset til

at brænde sammen. Det er vildt irriterende, og jeg har da set ting, som jeg ville ønske, jeg ikke havde set," siger Tim Vittrup.

INTERESSEREDE VOKSNE

Hverken Nicklas Meldgaard eller Tim Vittrup fortæller deres forældre om, hvad de laver på nettet. Det samme gælder stort set alle deres klassekammerater.

"Jeg synes ikke rigtigt, at det er relevant for mine forældre, hvad jeg laver på for eksempel Facebook. Det er mine private sager," siger Tim Vittrup, men både han og Nicklas Meldgaard oplever, at deres forældre spørger og interesserer sig for deres liv på nettet. Mille Glerup fortæller til gengæld sin mor rigtig meget om det, som hun oplever på de sociale medier, men ikke alt:

"Mindre episoder fortæller jeg ikke noget om, for så kan min mor godt blive overbeskyttende, og så ender det bare med, at noget som egentlig var en lille ting, bliver gjort til noget stort," siger hun.





**DET KRIMINALPRÆVENTIVE RÅD INVITEREDE SOM OPTAKT TIL DEN KRIMI-
NALPRÆVENTIVE DAG 2015 FIRE NORDJYSKE 8. KLASSE TIL WORKSHOPS
OM SOCIALE MEDIER. DE FIRE KLASSE DELTOG OGSÅ I SELVE DAGEN, OG 12
UDVALGTE ELEVER FORTALTE RESTEN AF SALEN OM DERES ERFARINGER
MED DE SOCIALE MEDIER. TIM VITTRUP, NICKLAS MELDGAARD OG MILLE
GLERUP FRA FILSTEDVEJENS SKOLE VAR BLANDT PANELDELTAGERNE.**

ORGANISERET KRIMINALITET PÅ NETTET UDFORDRER POLITIET

INTERNETTET BLIVER I STIGENDE GRAD BRUGT SOM ET REDSKAB I FORBINDELSE MED INTERNATIONAL ORGANISERET KRIMINALITET. DET STILLER STORRE KRAV TIL, HVORDAN POLITIET AFDÆKKER OG EFTERFORSKER DEN ORGANISEREDE KRIMINALITET.

"Internettet bliver i dag brugt af de kriminelle som et moderne koblen. Et redskab til at begå deres kriminelle gerninger. Det ser vi ikke mindst i forbindelse med den organiserede kriminalitet," siger vicepolitiinspektør Tormod Husted fra Rigspolitiets Nationale Efterforskningscenter (NEC), der beskæftiger sig med grænseoverskridende og organiseret kriminalitet.

Efterforskningscentret har særligt fokus på komplicerede og tunge kriminalitetsområder som rocker- og bandekriminalitet, menneskehandel, omrejsende kriminelle bander, narkokriminalitet og handel med illegale våben.

"Vi oplever, at den organiserede kriminalitet bliver mere og mere it-baseret, og de kriminelles kreativitet i forhold til at bruge internettet er virkelig stor," siger Tormod Husted.

NARKOTIKA OG LEJEMORD

Han forklarer, at NEC's fokus ikke drejer sig om it-kriminalitet og hacking, men om sager hvor internettet bliver brugt i forbindelse med forskellige former for "almindelig" organiseret kriminalitet:

"Det er kendte typer af kriminalitet som fx handel med stoffer, der nu også foregår via Facebook. Vi ser også

menneskesmugling og menneskehandel, som bliver faciliteret via nettet. Internettet er på mange måder blevet et understøttende element til den kriminalitet, vi kender i forvejen," siger Tormod Husted.

Det har i flere år været kendt, at der på internettet eksisterer illegale paralleluniverser, hvor kriminelle ved hjælp af krypteret kommunikation kan bevæge sig rundt på hjemmesider, som sælger alt fra danske pas til lejemord.

Et eksempel er det sorte internetmarked, Silk Road, der blev lukket af FBI i 2013, hvor man anonymt kunne købe narkotika, børneporno og illegale våben. Og betale med bitcoins eller andre virtuelle betalingsmidler, som er forholdsvis svære at spore.

"Det er en rigtig stor udfordring i forbindelse med organiseret kriminalitet, at man kan sidde i Danmark via en server i en anden verdensdel og købe og sælge ulovlige effekter i et lukket internetsystem," siger Tormod Husted, og peger på, at det internationale politisamarbejde bliver stadig mere vigtigt i bekæmpelsen af organiseret kriminalitet. Han påpeger dog samtidig, at det bestemt ikke er risikofrit at sidde ved sin computer og købe ulovlige effekter via nettet. Politiet er meget opmærksomme på denne handel med ulovlige varer, og sammen med både Skat og internationale samarbejdspartener bliver der løbende afsløret og strafforfulgt kriminelle, der har købt fx narko, doping og våben via internettet.

MERE PINKODEAFLURING

I Danmark er NEC udpeget til at være "single point of contact" for dansk politi. Det betyder, at hvis udenlandsk politi skal have kontakt til dansk politi, eller hvis dansk politi skal have kontakt med udenlandsk politi, så går det altid gennem NEC.

"Vi har rigtig meget samarbejde med politiet i andre lande, når det drejer sig om organiseret kriminalitet på nettet. Det kan være svært at fange bagmænd, der sidder i udlandet, og derfor gør vi i NEC meget ud af at styrke det internationale samarbejde," siger han.

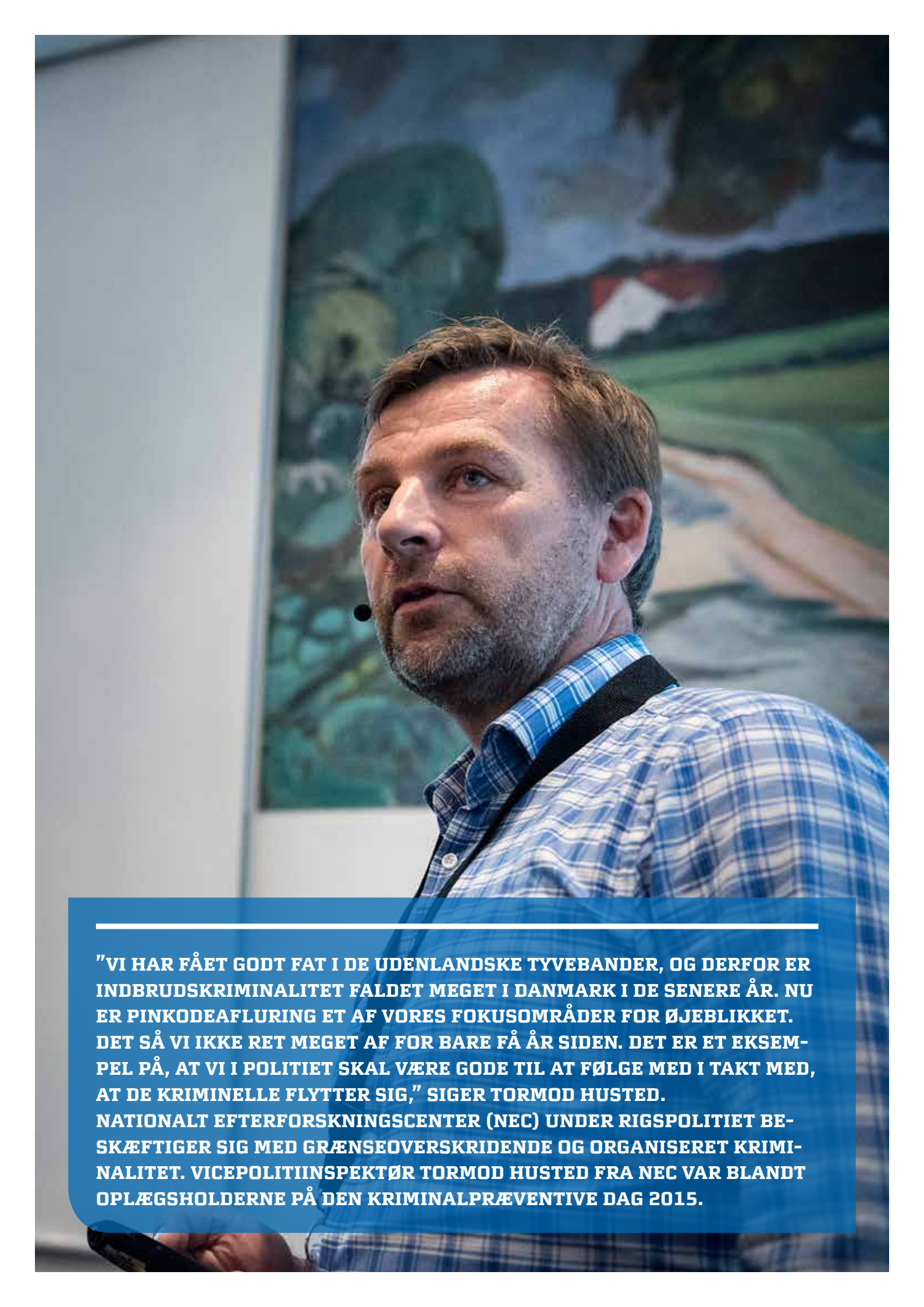
Samtidigt med, at den organiserede og internationale kriminalitet er blevet mere it-baseret, er de kriminelle blevet langt mere dynamiske og opportunistiske sammenlignet med tidligere.

"De kriminelle binder sig ikke længere til et bestemt forretningsområde. Hvis vi kaster grus i maskineriet i forbindelse med deres kriminalitet, så er de hurtige til at kaste sig over nye former for kriminalitet," siger Tormod Husted.

For eksempel har dansk politi i de senere år haft god succes med at bekæmpe udenlandske tyvebander, der rejste til Danmark for at lave indbrudskriminalitet. Til gengæld er der nu mange omrejsende kriminelle, der i stedet beskæftiger sig med pinkodeafluring.

Klik for at høre indlæg her:





"VI HAR FÅET GODT FAT I DE UDENLANDSKE TYVEBANDER, OG DERFOR ER INDBRUDSKRIMINALITET FALDET MEGET I DANMARK I DE SENERE ÅR. NU ER PINKODEAFLURING ET AF VORES FOKUSOMRÅDER FOR ØJEBLIKKET. DET SÅ VI IKKE RET MEGET AF FOR BARE FÅ ÅR SIDEN. DET ER ET EKSEMPEL PÅ, AT VI I POLITIET SKAL VÆRE GODE TIL AT FØLGE MED I TAKT MED, AT DE KRIMINELLE FLYTTER SIG," SIGER TORMOD HUSTED. NATIONALT EFTERFORSKNINGSCENTER (NEC) UNDER RIGSPOLITIET BESKÆFTIGER SIG MED GRÆNSEOVERSKRIDENDE OG ORGANISERET KRIMINALITET. VICEPOLITIINSPEKTØR TORMOD HUSTED FRA NEC VAR BLANDT OPLÆGSHOLDERNE PÅ DEN KRIMINALPRÆVENTIVE DAG 2015.

DANSK POLITI STYRKER IND- SATSEN MOD CYBERCRIME



DANSK POLITI SKAL VÆRE BEDRE TIL AT AFSLØRE HACKERE OG OPKLARE IT-KRIMINALITET. DET ER MÅLET MED RIGSPOLITIETS NYE CENTER FOR CYBER-KRIMINALITET, SOM ÅBNEDE I MAJ SIDSTE ÅR. NC3 HEDDER CENTRET, DER SKAL VÆRE POLITIETS KRAFTCENTER, NÅR DET GÆLDER ALLE FORMER FOR IT-KRIMINALITET.

”Vi skal være førende inden for bekæmpelse af cybercrime i Europa,” lyder den ambitiøse målsætning fra centerchef Kim Aarenstrup fra NC3.

Centeret blev etableret ved at samle i alt 70 medarbejdere fra Rigspolitiets Nationale it-efterforskningssektion og Politiets Aflytningscenter i den nye enhed. Siden er der blevet tilført yderligere ressourcer til NC3, som i løbet af 2015 vil nærme sig en medarbejderstab på 100 it- og politifolk, som udelukkende arbejder med at bekæmpe it-kriminalitet.

”Uanset om det handler om organiseret kriminalitet på nettet, distribution af børneporno eller hackerangreb mod firmaer og myndigheder, så skal politiet i fremtiden kunne matche udfordringerne,” siger Kim Aarenstrup.

IT-KRIMINALITETEN STIGER

Meget tyder på, at der er et behov for at styrke indsatsen mod cybercrime. Mens kriminaliteten som helhed falder på langt de fleste områder, stiger it-kriminalitet i Danmark. Ifølge tal fra Rigspolitiet steg antallet af it-sager, der

drejede sig om hacking eller databedrageri med flere hundrede procent fra 2012 til 2014.

”Hvis man spørger, om politiet hidtil har været dygtige nok, når det drejer sig om it-kriminalitet, så er det korte svar nej. Men det bliver vi, og vi er godt på vej med oprettelsen af NC3,” siger Kim Aarenstrup.

Han fortæller, at NC3 i alle politikredse er i gang med at ansætte it-ingeniører, der skal hjælpe med de tekniske kompetencer i forbindelse med efterforskning af it-kriminalitet rundt omkring i landet.

”Det er et kompetenceløft, der virkelig kommer til at skabe nye muligheder for politiet over hele Danmark,” siger han.

SKAL VÆRE FREMME I SKOENE

Udviklingen i den grænseoverskridende cyberkriminalitet går stærk og det nytter ikke, at politiet teknologisk set halter efter de kriminelle.

Selvom de it-kriminelle er dygtige, så er de ikke overmennesker. Ligesom i

den fysiske verden, hvor forbryderne efterlader sig fingeraftryk og DNA-spor, afsætter de it-kriminelle digitale spor, som kan afsløre dem.

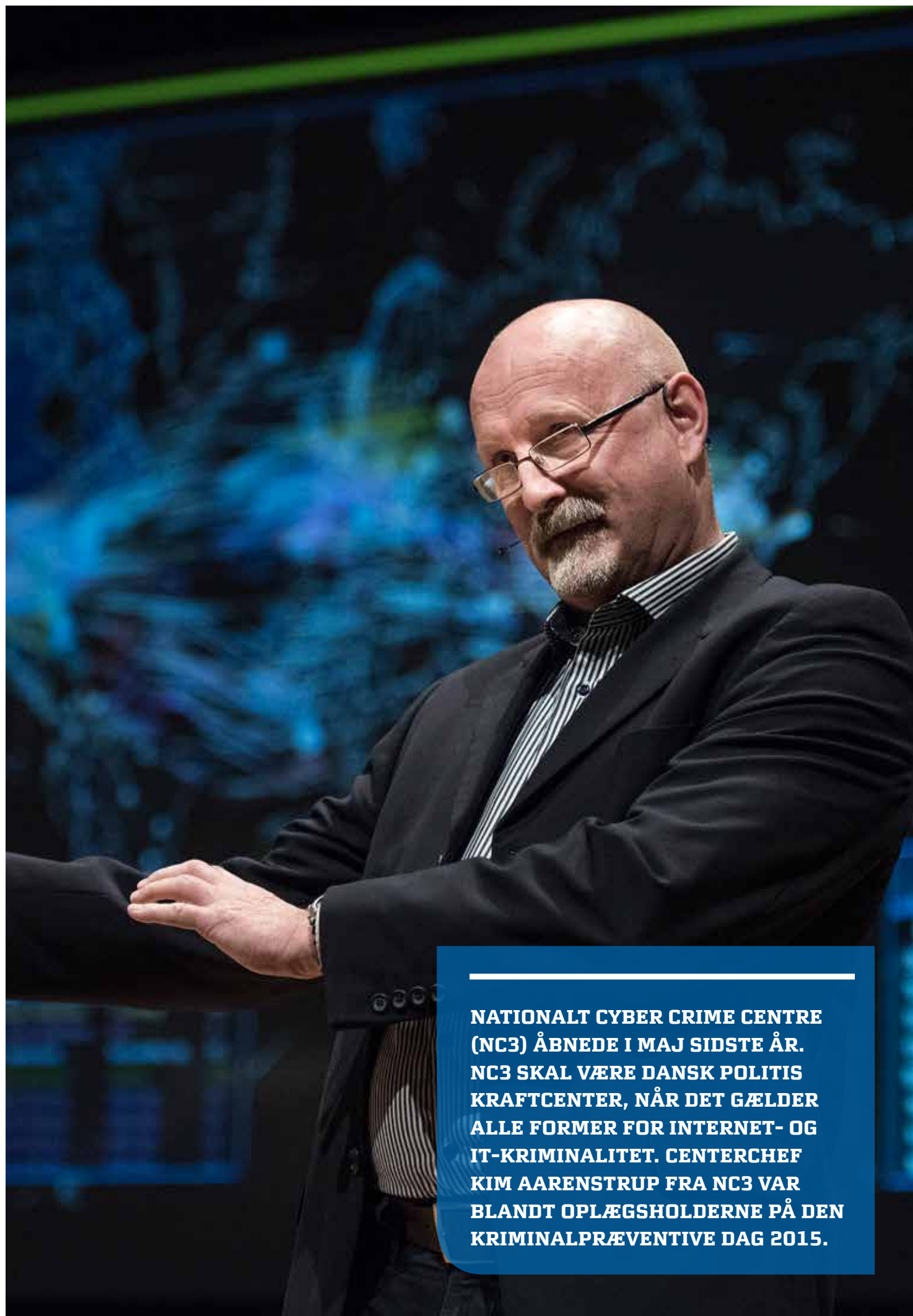
”Det stiller dog krav til, at vi i politiet er helt fremme i skoene, både når det drejer sig om it-kompetencer, teknologisk udstyr og kapacitet,” siger Kim Aarenstrup.

Det vil stadig være de enkelte politikredse, der er ansvarlige for efterforskningen af de fleste konkrete sager om it-kriminalitet, men fremover vil NC3 kunne bistå med ekspertviden og specialiseret udstyr.

Desuden skal NC3 lave analyser af kriminalitetsudviklingen, samarbejde med udenlandske partnere og sætte den nationale strategi på cybercrime-området. En anden opgave bliver at gennemføre uddannelse i politikredsene og levere efterforskningsoplæg på de mest komplicerede områder.

Klik for at høre indlæg her:





NATIONALT CYBER CRIME CENTRE (NC3) ÅBNEDE I MAJ SIDSTE ÅR. NC3 SKAL VÆRE DANSK POLITIS KRAFTCENTER, NÅR DET GÆLDER ALLE FORMER FOR INTERNET- OG IT-KRIMINALITET. CENTERCHEF KIM AARENSTRUP FRA NC3 VAR BLANDT OPLÆGSHOLDERNE PÅ DEN KRIMINALPRÆVENTIVE DAG 2015.

A portrait of Raoul Chiesa, a middle-aged man with a beard and a headset microphone, wearing a suit and tie. He is looking slightly to the side with a serious expression. The background is dark and out of focus.

ITALIENSKE RAOUL CHIESA VAR SELV HACKER FRA 1986 TIL 1995. HAN BETEGNER SIG SELV SOM EN SÅKALDT 'ETISK HACKER', DER ALDRIG SKADEDE DE SYSTEMER, SOM HAN BRØD IND I, MEN I STEDET INFORMEREDE ADMINISTRATORERNE OM DE SIKKERHEDSBRISTER, HAN FANDT. I 1996 VALGTE HAN AT BLIVE PROFESSIONEL SIKKERHEDSKONSULENT. HAN ER BL.A. RÅDGIVER FOR UNICRI, SOM ER FN'S TVÆRREGIONALE RESEARCH-INSTITUT FOR KRIMINALITET OG LOVGIVNING OG ER FORFATTER TIL BOGEN: PROFILING HACKERS. RAOUL CHIESA VAR BLANDT OPLÆGSHOLDERNE PÅ DEN KRIMINALPRÆVENTIVE DAG 2015.



HACKER-BEGREBET SPÆNDER VIDT

NUTIDENS HACKERE ER IKKE BARE DIGITALE DRENGERØVE, MEN SOFISTIKEREDE OG ORGANISEREDE KRIMINELLE, DER HAR GJORT INTERNETKRIMINALITET TIL EN MILLIARDDOLLAR INDUSTRI.

"Vores stereotype billede af hackere som teenagere, der sidder foran skærmen om natten iført kasket og omgivet af coladåser, holder ikke. Nutidens it-kriminelle er alt fra sofistikerede hackere til udspekulerede forbrydere," siger Raoul Chiesa, der selv er tidligere hacker og nu arbejder med it-sikkerhed. Han er bl.a. rådgiver for UNICRI, som er FN's tværregionale researchinstitut for kriminalitet og lovgivning.

I FN har han fx arbejdet med Hackers Profiling Project (HPP), der på baggrund af spørgeskemaundersøgelser og observationer skitserer de forskellige typer af hackere og deres kriminelle profiler.

"Begrebet hacker bliver brugt om alle former for it-kriminelle, og det gør det svært for virksomheder og andre at vide, hvem det egentlig er, de skal være bange for. Vores filosofi er, at vi skal forstå, hvem hackerne er for at kunne bekæmpe dem. Derfor følger vi hackerne og deres udvikling tæt," siger Raoul Chiesa.

SORTE OG HVIDE HATTE

Oprindeligt blev udtrykket 'hackere' forbundet med noget positivt, da det opstod tilbage i 1970'erne, hvor hackerne var drevet af nysgerrighed og higen efter viden. Med filmen 'Wargames' fra 1983 blev det pludselig moderne at være hacker og flere kom til.

Men dengang var det alligevel forholdsvis simpelt at danne sig et billede af, hvem hackerne var.

Der var de gode hackere (de hvide hatte), som var optaget af etikken bag hacking og fx samarbejdede med myndighederne omkring sikkerhedsbrud, og så var der de dårlige hackere (de

sorte hatte), der var amoralske og kun brød ind i sikkerhedssystemer for egen vindings skyld, mens politisk aktivisme var drivkraften for andre.

"Hackerne blev hurtigt bevidste om, at når man har information, så har man magten. Man kan fx bruge informationerne til afpresning, hævn, til at snyde penge ud af folk eller til at opnå konkurrencefordele. I dag har de organiserede kriminelle grupper taget over, og de er ikke optaget af kunsten ved hacking eller dens etik og historie. De er først og fremmest drevet af profit og politik," siger Raoul Chiesa.

MILLIARDDOLLARINDUSTRI

Internetkriminalitet er hurtigt blevet mere rentabel og mindre risikofyldt end traditionel kriminalitet og overgår nu narkotikahandlen som den største kriminelle pengemaskine.

"Det er en milliarddollarindustri, og internettet fungerer som magnet for alle former for kriminelle. De er tiltrukket af

de store summer af penge og den lave risiko for at blive opdaget. Dertil kræver det ikke store investeringer at udnytte nettet til kriminelle aktiviteter, og man kan nemt finde redskaberne online til, hvordan man gør," siger Raoul.

De kriminelle aktiviteter på nettet spænder lige fra bedrageri, identitetstyveri, afpresning, falske hjemmesider og angreb på offentlige og private virksomheders computersystemer til cyberkrigsførelse, hvor en nationalstat trænger ind på en anden nationalstats computernetværk for fx spionere eller skabe skade.

"Mange hackere anser ikke sig selv som rigtige kriminelle, fordi de bruger et tastatur og ikke er fysisk voldelige. Deres tankegang er, at hvis folk er dumme nok til at lade sig narre, så er det deres eget problem," siger Raoul Chiesa.

Klik for at høre indlæg her:





NORDJYLLANDS POLITI HAR SAMMEN MED RIGSPOLITIET UDVIKLET "SOCIALSØG", DER ER ET IT-VÆRKTØJ, SOM KAN SPOTTE UDSATTE FAMILIER MED BØRN TIDLIGERE END HIDTIL. "SOCIALSØG" BLEV PRÆSENTERET PÅ DEN KRIMINALPRÆVENTIVE DAG 2015.

IT-VÆRKTØJ HJÆLPER UDSATTE BØRN

ET NYT IT-SYSTEM KAN VÆRE MED TIL AT REDDE FLERE UDSATTE BØRN FRA OMSORGSSVIGT OG KRÆNKELSER. VÆRKTØJET SOM NORDJYLLANDS POLITI HAR VÆRET MED TIL AT UDVIKLE, SKAL EFTER PLANEN INDFØRES I LANDETS ØVRIGE POLITIKREDSE.

Undersøgelser viser, at personer, der begår en seksual- eller en mishandlingsforbrydelse mod et barn, ofte tidligere har været i kontakt med politiet. Det er baggrunden for, at Nordjyllands Politi sammen med Rigspolitiet har udviklet "Socialsøg" - et it-værktøj, der kan opdage udsatte familier med børn tidligere end hidtil.

"Det handler om at få identificeret familier, der er på vej i en social deroute på et tidligt tidspunkt, så de kan få hjælp, inden det for alvor går galt," siger politiassistent og kriminolog Knud Rasmussen fra Nordjyllands Politi, der er leder af projektet med "Socialsøg"

TÆNDER EN RØD LAMPE

Programmet fungerer på den måde, at det samkører data fra politiets registre for på et tidligt tidspunkt at spotte forhold, der kan føre til svigt af børn.

Det sker ved, at udvalgte oplysninger fra politiets døgnrapporter om blandt andet misbrug af alkohol og stoffer, husspektakler og trusler trækkes ud, så politiets sagsbehandlere kan kæde disse oplysninger sammen med lignende aktuelle sager.

"Vi har mange data liggende i vores systemer fra, når folk har været i kontakt med politiet. Det kan man som enkeltperson ikke overskue, men systemet kan kæde de forskellige risikofaktorer sammen og tænde en rød lampe, når der er en indikation på, at en familie har brug for hjælp," siger Knud Rasmussen.

Desuden ligger det i grundtanken bag Socialsøg, at hvis myndighederne griber tidligere ind, så bliver færre børn i sidste ende udsat for en alvorlig forbrydelse.

"Socialsøg er et eksempel på, hvordan moderne teknologi kan bruges til at forbedre udsatte børns vilkår," siger han.

GODE ERFARINGER

Siden Nordjyllands Politi begyndte at bruge it-værktøjet i 2013 er antallet af socialrapporter, som politiet sender videre til de nordjyske kommuner, steget kraftigt.

Før Socialsøg blev taget i brug skrev politiet i Nordjylland mellem 50 og 90 indberetninger til de sociale myndigheder om året. Alene i løbet af de første fire måneder af 2015 skrev Nordjyllands Politi 226 socialrapporter, som

blev sendt videre til sagsbehandlerne i kommunerne.

Herefter er det kommunernes opgave at tage stilling til, hvordan der skal følges op på politiets socialrapporter, og ifølge Knud Rasmussen er erfaringerne gode.

"Tilbagemeldingerne fra kommunerne er, at de nu på et tidligt tidspunkt får identificeret flere familier, der kan have behov for hjælp og støtte. Også familier, de ikke kendte til i forvejen," siger han.

Klik for at høre indlæg her:



