DKR
DET KRIMINAL PRÆVENTIVE RÅD

NÅR FORBRYDELSER BLIVER DIGITALE

En antologi om IT-kriminalitet og adfærd på internettet

KOLOFON:

Det Kriminalpræventive Råd
Ejby Industrivej 125-135
2600 Glostrup
Tlf. 45 15 36 50

Grafisk tilrettelæggelse: Advice
Tryk: Mercoprint
Oplag: 1.000
DKR nr. 15-401-0377
ISBN: 978-87-92966-34-6

Kopiering tilladt med kildeangivelse
Udgivelsen er gratis tilgængelig på www.dkr.dk

Marts 2016

FORORD

IT-kriminalitet er et område, der fylder stadig mere i bevidstheden hos både borgere, offentlige myndigheder og virksomheder. For hvordan er det lige, man beskytter sig mod noget, der for mange virker meget teknisk, og hvordan ved man, at man har gjort nok for at undgå at blive udsat? Og hvad med ansvaret – hvem har egentlig ansvaret for, at det er sikkert at færdes på internettet? Er det borgeren selv, der ved en fejl kommer til at logge på en falsk netbanksside? Er det de erhvervsvirksomheder, der udbyder digitale services, eller er det politikerne, der igennem regulering og håndhævelse skal bekæmpe kriminalitet på internettet?

Svaret er ikke entydigt, og i realiteten er ansvaret ofte delt mellem mange forskellige aktører. Sandheden er nemlig, at vi hver især – det være sig som privatperson, virksomhed eller myndighed – kan gøre noget for at beskytte os selv, vores virksomhed, vores kunder eller borgerne i samfundet.

Ingen kan dog løfte opgaven alene, og udfordringen kalder derfor på koordination, vidensindsamling, videndeling og oplysning. Det er i relation til de sidste to af disse punkter, at denne antologi spiller ind ved at give en bred indføring i IT-kriminalitet og relaterede problematikker på internettet samt oplyse om, hvad man kan gøre for at forebygge at blive udsat.

Antologien er tiltænkt alle, der godt kunne tænke sig at vide mere om området, og hvordan man kan beskytte sig. Men antologien er i lige så høj grad tiltænkt personer, der i kraft af deres arbejde har en eller anden form for berøring enten med kriminalitet og uetisk adfærd på internettet eller med befolkningsgrupper, der er i særlig risiko for at blive udsat for eksempelvis bedrageri, identitetstyveri, mobning osv. på internettet.

Intentionen er, at antologien både skal kunne læses af personer uden noget forudgående kendskab til området og af fagpersoner, for hvem IT-kriminalitet ikke er et nyt fænomen. Vi håber, at antologien lever op til dette og også vil vække din interesse, uanset hvor du befinder dig i dette spektrum.

Antologien er kun blevet en realitet, fordi en lang række af væsentlige bidragsydere har udvist en enorm velvilje og lyst til at bidrage. Vi skylder derfor en kæmpe tak til Rigspolitiets Nationale Cyber Crime Center, Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste, Professor Dr. Peter Fischer, e-mærket, Raoul Chiesa, Børnerådet, SSP København, Red Barnet, Rådet for Digital Sikkerhed, Professor Lars Bo Langsted, Christian Wernberg-Tougaard og Professor Vincent F. Hendricks.

Udgivelsen skriver sig ind i Det Kriminalpræventive Råds igangværende arbejde med at sætte fokus på IT-kriminalitet og ikke mindst, hvordan IT-kriminalitet kan forebygges. Når vi taler om kriminalitet på internettet er det dog også vigtigt, at vi ikke bliver bekymrede i en grad, der overstiger problemets reelle omfang og den enkeltes risiko for at blive udsat. Vi håber derfor, at antologien giver læseren en fornemmelse af, at der faktisk er noget, man kan gøre for at beskytte sig selv og andre mod kriminalitet på internettet, og at der samtidig er mange gode kræfter i gang med at forebygge og bekæmpe denne kriminalitetsform – også på et mere overordnet niveau.

Med disse let optimistiske ord er der nu kun tilbage at sige – rigtig god læselyst!

Henrik Dam

Formand, Det kriminalpræventive Råd.

Redaktionen bestod af forebyggelseschef Henriette Korf, DKR, analytiker Anna Vibe Onsberg Hansen, DKR, konsulent Anders Young Rasmussen, DKR og senior advisor Merete Arentoft, Advice.

INDLEDNING

MAN KAN NÆSTEN IKKE OVERVURDERE BETYDNINGEN AF DEN DIGITALE UDVIKLING, HVOR SÆRLIGT INTERNETTET HAR VÆRET EN DRIVENDE KRAFT. INTERNETTET OG COMPUTERE HAR SKABT ET HAV AF NYE MULIGHEDER, SOM VI ALLE NYDER GODT AF.

Uheldigvis har kriminelle også været gode til at udnytte disse muligheder til at begå meget alvorlige kriminalitetsformer samtidig med, at man også ser dagligdags forbrydelser begået af helt "almindelige" danskere. IT-kriminalitet eller cyber crime dækker derfor både over hackere med store tekniske evner, som er i stand til at stjæle enorme pengebeløb fra banker, til den frustrerede borger, der sender trusselsmails til politikere.

Spændvidden i kriminalitetsformerne kan gøre det svært at få et overblik over, hvad begrebet IT-kriminalitet egentlig betyder. Ofte dækker begrebet både over de meget tekniske former for kriminalitet, men ligeså ofte består "cyberdelen" alene af, at internettet udnyttes til at komme i kontakt med potentielle ofre på en let, billig og anonym måde.

Selvom IT-kriminalitet dækker over mange forskellige typer af forbrydelser, så gælder det på internettet som i den "analoge" verden, at man ofte kan beskytte sig selv ved at tage nogle fornuftige forholdsregler. Vi låser døren til vores hjem, er opmærksomme på lommetyve og er skeptiske, når noget lyder for godt til at være sandt. De fleste af os undgår derfor at blive udsat for kriminalitet i den fysiske verden ved en kombination af tekniske hjælpemidler og fornuftig adfærd. Det samme gælder, når man skal undgå kriminalitet på internettet. Og selvom IT-kriminalitet kan være meget teknisk at udføre, så behøver det at beskytte sig mod det ikke nødvendigvis at være det.

Det er dog ikke altid lige let at gennemskue, hvad "fornuftig adfærd" på nettet er. Ambitionen med denne udgivelse er derfor både at give et overblik over begrebet IT-kriminalitet samt give håndgribelige råd til, hvordan man kan beskytte sig selv. Disse råd kan både bruges af privatpersoner og af fagpersoner til at videreformidle til andre, eksempelvis til ens elever, hvis man arbejder som lærer, eller til medarbejdere og kollegaer, der eksempelvis har kontakt til særligt udsatte grupper i samfundet.

Som for mange andre former for kriminalitet gælder det også for IT-kriminalitet, at man ikke bør lade sin bekymring for at blive offer begrænse sig i sin hverdag, da risikoen for at blive udsat heldigvis er relativt begrænset, og da man som privatperson langt hen af vejen er godt beskyttet i forhold til at få dækket eventuelle økonomiske tab.

FOREBYGGELSE AF IT-KRIMINALITET

Det Kriminalpræventive Råd arbejder med at forebygge kriminalitet bredt set og har de senere år haft et særligt fokus på kriminalitet begået på eller via internettet.

Forebyggelse af kriminalitet er en mangefacetteret proces, der både indebærer tidlige og brede indsatser samt mere målrettede indsatser mod udsatte personer eller grupper. En udbredt tilgang til kriminalitetsforebyggelse er at se kriminelle handlinger som et resultat af tilstedeværelsen af tre elementer: 1) en motiveret gerningsperson, 2) et muligt offer/mål og 3) et egnet gerningssted. Logikken bag denne tredeling er, at hvis blot ét af disse tre elementer tages ud, så vil den kriminelle handling ikke ske.

Mange internetforbrydelser er kendetegnet ved at være anonyme og udført uden, at offer og gerningsperson har været i fysisk kontakt med hinanden. Dertil kommer, at IT-forbrydelser ikke sjældent er grænseoverskridende, hvilket betyder, at der i disse tilfælde stort set ikke er begrænsninger på, hvor mange potentielle ofre en gerningsperson kan forsøge at nå ud til. Gerningsmændene er derfor ofte meget motiverede, den økonomiske gevinst er stor og risikoen for at blive opdaget og straffet begrænset. Dette indebærer, at mange af de sociale indsatser, som er målrettet gerningsmænd ved traditionel kriminalitet, ofte ikke er anvendelige, når det kommer til IT-kriminalitet. Det er derfor særligt det andet og det tredje element, der er relevant, når kriminalitet på internettet skal forebygges. De bedste måder at fore-

bygge IT-kriminalitet på er derfor ofte ved at reducere mulighederne for gerningsmændene, eksempelvis igennem:

- Tiltag, der øger robustheden hos borgere og andre typer af ofre, eksempelvis via udbredelse af brugbare råd til at beskytte sig selv
- Tiltag, der øger den nødvendige arbejdsindsats for at begå en kriminel handling
- Tiltag, der reducerer gevinsterne ved en kriminel handling
- Tiltag, der øger gerningsmandens risiko for at blive opdaget, mens den kriminelle handling begås.

Forebyggelse af IT-kriminalitet handler med andre ord særligt om at undgå, at folk bliver ofre for svindelmails, falske internetbutikker med mere, men også om at gøre det vanskeligt og risikabelt for kriminelle eksempelvis at bryde ind i IT-systemer. Heldigvis er dette langt hen af vejen områder, man både som privatperson og som virksomhed eller myndighed kan arbejde med – dels ved at kende farerne og de gode råd til at undgå dem, og dels ved hjælp af tekniske løsninger så som antivirusprogrammer og løbende opdatering af programmer.

Antologien er et godt sted at begynde, hvis man vil skærpe sin opmærksomhed på forebyggelse af IT-kriminalitet eller bare gerne vil vide mere om emnet. Det gælder uanset, om man eksempelvis er ude efter at få et indblik i farerne på internettet eller vil have gode råd til, hvordan man kan styre udenom fupbutikker, identitetstyve og andre bedragere i det digitale univers. Antologien giver også inspiration til, hvordan man som virksomhed designer en fornuftig IT-sikkerhedsstrategi, og hvordan man som forælder, lærer eller pædagog kan håndtere udfordringerne med børn og unges digitale liv.

LÆSEVEJLEDNING

Antologien er opdelt i seks kapitler med hvert sit tema. Artiklerne varierer mellem det meget konkrete for eksempel, hvordan man kan "spotte en fupbutik" på internettet, til de mere beskrivende og begrebsforklarende artikler såsom Red Barnets artikel om såkaldt grooming på internettet.

KAPITEL 1 giver en indføring i, hvad IT-kriminalitet er for en størrelse, hvilke former for IT-kriminalitet der findes, og hvad forskellige myndigheder gør for at løse problemet med kriminalitet på internettet.

KAPITEL 2 stiller skarpt på den del af kriminaliteten på internettet, der typisk rammer private personer, og som oftest har til formål at franarre penge fra offeret. Der er typisk tale om identitetstyveri, betalingskortmisbrug, svindelmails, afpresning og fupbutikker på internettet.

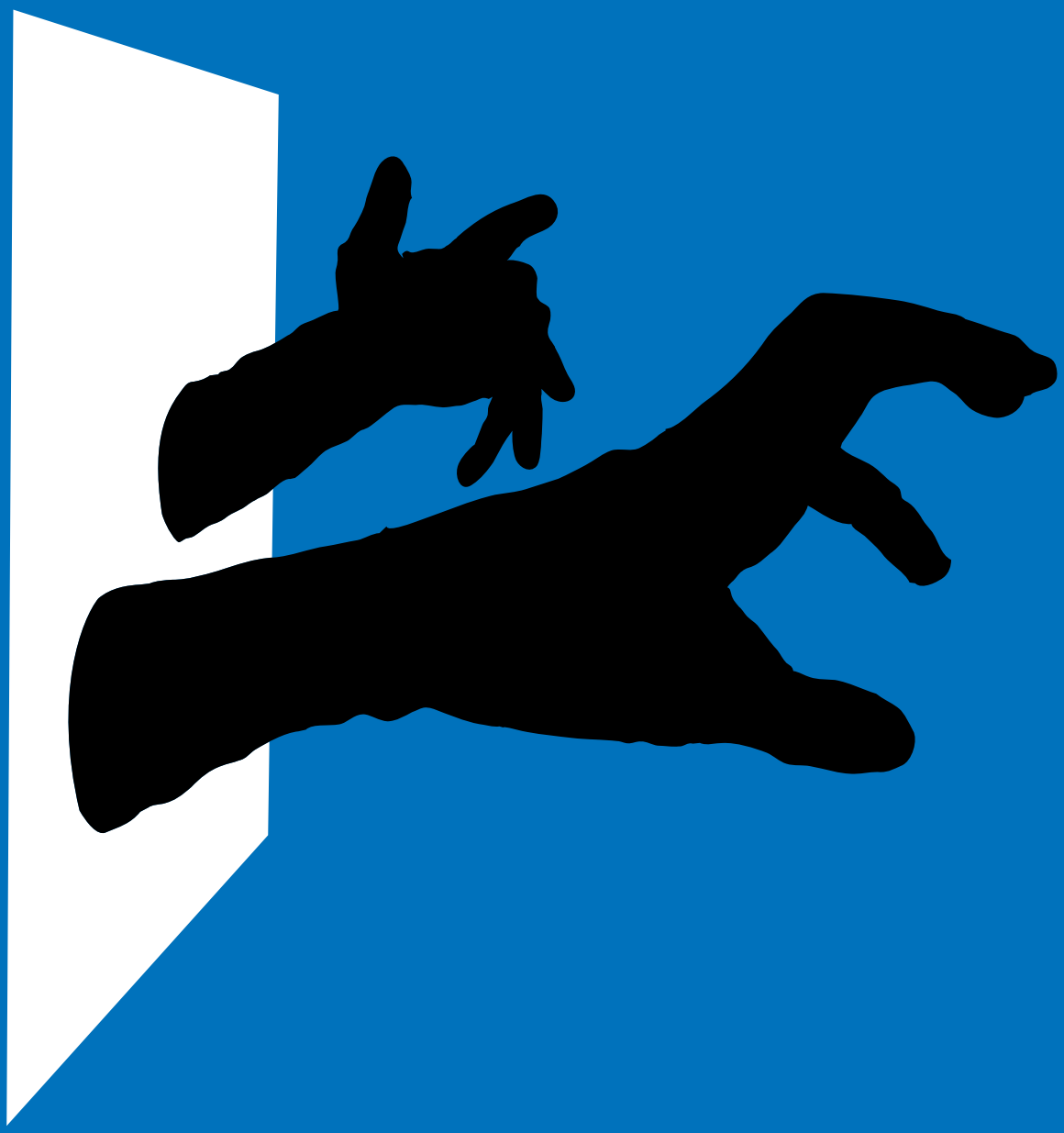
KAPITEL 3 sætter fokus på hacking og giver et indblik i de forskellige former for hackerforbrydelser, der begås, og hvilke forskellige typer af hackere, der findes. Kapitlet har et særligt fokus på cyberspionage, og hvad man som virksomhed eller myndighed kan gøre for at beskytte sig mod hackerangreb og spionage.

KAPITEL 4 retter fokus på børn og unges adfærd på internettet, og kapitlet belyser både alvorlig kriminalitet rettet mod børn og unge og mere uhensigtsmæssig adfærd på internettet, så som mobning, der, skønt det ikke er kriminelt, ikke desto mindre kan være meget krænkende og alvorligt.

KAPITEL 5 handler om, hvordan vi sikrer vores digitale privatliv og sætter fokus på nogle af de problematikker, der er med privatlivsbeskyttelse i takt med at mere og mere af vores adfærd foregår på internettet.

Endelig slutter **KAPITEL 6** antologien af med en ordbog med forklaringer af de vigtigste begreber i relation til IT-kriminalitet samt en række gode råd til, hvordan man beskytter sig i hverdagen, hvad man som forældre kan gøre for at beskytte sine børn, og hvad man særligt som barn eller ung skal være opmærksom på, når man færdes på internettet.

INDHOLDSFORTEGNELSE



Kapitel 1

DIGITALE FORBRYDELSER

HVAD ER IT-KRIMINALITET?

DE FLESTE HAR NOK EN IDÉ OM, HVAD BEGREBET IT-KRIMINALITET, ELLER CYBERCRIME, BETYDER. SKAL MAN BESKÆFTIGE SIG MERE INDGÅENDE MED OMRÅDET, OG SÆRLIGT FRA ET FOREBYGGELSESPERSPEKTIV, KAN DET DOG VÆRE HENSIGTSMÆSSIGT AT INDDELE BEGREBET I FLERE KATEGORIER. IT-KRIMINALITET KAN NEMLIG VÆRE ALT FRA SIMPELT BEDRAGERI TIL EN MEGET MERE TEKNISK AVANCERET FORM FOR KRIMINALITET, LIGESOM IT-KRIMINALITET KAN HAVE BETYDNING FOR ALLE – PRIVATE BORGERE SÅVEL SOM MYNDIGHEDER OG VIRKSOMHEDER.

TRE TYPER AF IT-KRIMINALITET

IT-kriminalitet er en paraplybetegnelse for en lang række kriminelle aktiviteter, hvis fællesnævner er, at computerbaseret teknologi – i særdeleshed internettet - udgør et centralt element for udførelsen af den kriminelle handling.

Der er imidlertid stor forskel på, om forbrydelsen sker ved, at kriminelle blot anvender internettet til at komme i kontakt med potentielle ofre, for eksempel ved at tage kontakt over Facebook, eller om gerningspersonen er en professionel hacker, som skaffer sig adgang til virksomheders computersystemer for at stjæle forretningshemmeligheder. IT-kriminalitet kan derfor have mange ansigter og foregå på mange forskellige måder.

Overordnet set kan IT-kriminalitet opdeles i tre kategorier, der afhænger af, hvilken rolle computeren spiller i forhold til forbrydelsen. Er det computeren og dens indhold, som er målet for forbrydelsen? Er computeren et middel til at komme i kontakt med et potentielt offer eller et middel til at hente og dele ulovligt indhold?

Begrebet computer-integritetsforbrydelser anvendes om forbrydelser, hvor det er selve computeren, der angribes. Ofte med henblik på uretmæssigt at få adgang til oplysninger eller at ødelægge eller ændre IT-systemer. Denne form for kriminalitet bliver ofte omtalt som hacking og er en relativt ny type af forbrydelse, som er opstået i takt med den teknologiske udvikling.

Begrebet computer-assisterede forbrydelser henviser til mere traditionelle former for kriminalitet, hvor computerbaseret teknologi spiller en assisterende rolle for gennemførelsen af forbrydelserne. Mens computer-integritetsforbrydelser retter sig mod selve computeren, retter computer-assisterede forbrydelser sig hovedsagligt mod personer. Eksempler på forbrydelser assisteret af internetteknologi tæller blandt andet svindelbreve sendt over e-mail (såkaldt phishing), bedrageri i forbindelse med internethandel og identitetstyveri, hvor kriminelle udnytter internettet til at komme i kontakt med potentielle ofre på en let, billig og anonym måde.

Begrebet computer-indholdsforbrydelser vedrører ulovligt indhold i materiale, der lægges ud på eller overføres via internettet. Eksempler på ulovligt indhold kan være børneporno, voldeligt materiale og racistisk eller andet "hate crime"-materiale. Denne type af kriminalitet eksisterer i sin grundform i den fysiske verden, men får en ny dimension, når kriminelle udnytter mulighederne ved internettet til at distribuere det ulovlige materiale. I den forstand er computer-indholdsforbrydelser også en form for computer-assisterede forbrydelser, der kan ramme private personer, som det for eksempel er tilfældet ved børneporno.

Denne opdeling af IT-forbrydelser kan være hensigtsmæssig, fordi den er retningsgivende i forhold til, hvordan de pågældende forbrydelser bedst håndteres. Forebyggelse af IT-kriminalitet handler ofte om enten at øge sikkerheden ved tekniske løsninger eller ved at gøre brugere opmærksomme på risikosituationer og give vejledning om sikker internetadfærd.

NÅR KRIMINALITET SKER ONLINE

Traditionelle former for kriminalitet, såsom tyveri, bedrageri og pædofili har ændret form som følge af digitaliseringen. Samtidig er rækkevidden af kriminaliteten øget eller har fået en mere ekstrem karakter.

Selvom mange IT-forbrydelser derfor i deres substans ligner kendte former for kriminalitet, tilføjer computerbaseret teknologi altså en ny og væsentlig dimension til den kriminelle handling.

Internettet gør det eksempelvis muligt med få midler at sende bedragerimails (Nigeriabreve eller phishing-mails) ud til millioner af mennesker, og selvom det er et mindretal, der bider på, så giver det digitale aspekt mulighed for at opskalere bedragerierne i en størrelsesorden, som er vanskelig at genfinde i den fysiske verden.

Tilsvarende kan internettet gøre kendte former for kriminalitet mere ekstreme, for eksempel ved at give nye værktøjer til pædofile grupper i form af chatrum, digital distribuering af børneporno og så videre. Hertil kommer, at IT-kriminalitet ofte er grænseoverskridende i sin natur, hvorfor det i praksis ofte kun er de mest alvorlige forbrydelser, som bliver efterforsket, fordi retsforfølgning på tværs af landegrænser er yderst ressourcekrævende. Dette skal også sammenholdes med, at internettet gør det let for gerningsmænd at operere anonymt.

Relationen mellem offer og gerningsmand er også væsentligt anderledes ved IT-kriminalitet end ved kriminalitet i den fysiske verden, fordi kriminaliteten på nettet ofte er skjult og upersonlig. Krænkelseselementet ved IT-forbrydelser er derfor ofte ubetydelige sammenlignet med overgreb i den fysiske verden. Der findes selvfølgelig eksempler, hvor det er en gråzone, om det er tale om en offline eller online krænkelse, eksempelvis grooming (krænkelser af børn på nettet). I mange

TYPER AF IT-KRIMINALITET

COMPUTER-INTEGRITETS-FORBRYDELSER

Forbrydelser direkte rettet mod IT-systemer.

Selvstændig form for kriminalitet. Ofte rettet mod virksomheder eller myndigheder, men kan også være rettet mod private borgere. Typisk økonomisk, politisk, ideologisk eller privat formål.

EKSEMPLER:

HACKING | DDOS-ANGREB | TROJANSKE HESTE | VIRA | ORME

COMPUTER-ASSISTEREDE FORBRYDELSER

Forbrydelser, hvor computerbaseret teknologi anvendes som centralt redskab til at begå kriminalitet.

Kendte/traditionelle former for kriminalitet, der faciliteres af internettet. Ofte rettet mod private borgere, hvor formålet ofte er økonomisk vinding.

EKSEMPLER:

IDENTITETSTYVERI | BETALINGSKORTMISBRUG | NETHANDELSBEDRAGERI | PHISHING | NIGERIABREVE | DATINGBEDRAGERI

COMPUTER-INDHOLDS-FORBRYDELSER

Forbrydelser, der knytter sig til ulovligt indhold af filer mm., som deles via internettet.

Kriminalitet, der får et nyt format, når ulovligt materiale kan distribueres og formidles online. Besiddelse og deling af materialet kan for eksempel være motiveret af ideologiske overbevisninger eller egennyttige interesser/ præferencer.

EKSEMPLER:

OPBEVARING OG DELING AF BØRNEPORNOGRAFISK MATERIALE | RACISTISK/EKSTREMISTISK MATERIALE

tilfælde er ofrene dog enten ikke vidende om, at de har været udsat for en IT-forbrydelse eller anser ikke forbrydelsen som en egentlig krænkelse. Eksempelvis modtager mange næsten på daglig basis e-mails, som formelt set er bedrageriforsøg. Disse henvendelser er irriterende, men de færreste anser det som en krænkelse, der bør politianmeldes. Det samme gør sig gældende med betalingskortmisbrug, hvor mange nøjes med at kontakte deres bank.

MYNDIGHEDER OG VIRKSOMHEDER

Hvor borgere primært skal bekymre sig om ikke at blive snydt på internettet, og hvor de fleste problemer kan undgås ved sikker internetadfærd, så er sikkerhedsudfordringerne langt mere komplekse for myndigheder og virksomheder, og de potentielle skadevirkninger er her enorme.

IT-kriminalitet, som rammer borgere, har ofte mere eller mindre tilfældig karakter, og i mange tilfælde vil det ikke være den ramte borger, der står med et eventuelt økonomisk tab. I modsætning hertil er hackerangreb mod virksomheder og myndigheder langt mere målrettede og kan i visse situationer ligefrem være udført af statslige eller statsstøttede aktører. Både hyppigheden og konsekvenserne er blevet mere markante for de organisationer og virksomheder, som bliver ramt. Og det er ikke kun store og kendte virksomheder, der er udsatte, men også små og mellemstore organisationer bliver jævnligt udsat for angreb.

Myndigheder og virksomheder skal desuden ikke kun beskytte sig mod almindelige svindelmails, men skal også forholde sig til en række forskellige sikkerhedsudfordringer. Hvordan beskyttes eksempelvis stats- og forretningshemmeligheder, vital infrastruktur såsom vand, varme, el og betalingssystemer, private oplysninger om borgere, kunder og kerneforretningen?

Der findes talrige eksempler på, at både myndigheder og virksomheder har været udsat for hackerangreb, som har medført enorme økonomiske tab, og derudover også har medført tab af tillid til de ramte organisationer. Samtidig kan hackerangreb hos virksomheder også betyde kompromittering af private kunders personlige oplysninger for eksempel betalingskortoplysninger eller andre fortrolige informationer.

IT-kriminalitet er altså blevet en faktor, der har betydning for alle; borgere såvel som myndigheder og virksomheder, og som spænder bredt fra små irritationsmomenter i dagligdagen til trusler, der potentielt kan have samfundstruende karakter.

Kilder:
Kruize, Peter (2015): Internetkriminalitet – Offerundersøgelse om identitetstyveri, bedrageri, afpresning og chikane i cyberspace, Det Kriminalpræventive Råd.
PricewaterhouseCoopers (PwC) (2015): Cybercrime survey 2015.
Sandywell, Barry (2010): "On the globalisation of crime: the Internet and new criminality", i: Yvonne Jewkes & Majid Yar (eds.) Handbook of Internet Crime, Abingdon: Routledge, s. 38-66.
Wall, David S. (2007): Cybercrime, Cambridge: Polity Press.
Wall, David S. (2010): "Criminalising cyberspace: the rise of the Internet as a 'crime problem'", i: Yvonne Jewkes & Majid Yar (eds.) Handbook of Internet Crime, Abingdon: Routledge, s. 88-103.

INTERVIEW MED KIM AARENSTRUP,
CENTERCHEF I RIGSPOLITIETS NATIONALE CYBER CRIME CENTER (NC3)

DANMARK SKAL VÆRE FØRENDE I AT HINDRE OG OPKLARE IT-KRIMINALITET

RIGSPOLITIETS NATIONALE CYBER CRIME CENTER (NC3) BLEV ETABLERET I FORÅRET 2014 MED DET FORMÅL AT BRINGE EKSTRA FOKUS PÅ BEKÆMPELSEN AF EN KRIMINALITETSFORM I VOLDSOM VÆKST. CENTERCHEF KIM AARENSTRUP LØFTER HER SLØRET FOR NOGLE AF NC3'S FREMTIDIGE TILTAG, DER SKAL BRINGE DANSK POLITI ET SKRIDT FORAN NETTETS FORBRYDERE.

HVORFOR ER DET NØDVENDIGT MED ET SÆRLIGT EFTERFORSKNINGSCENTER TIL IT-KRIMINALITET?

Ivrigheden efter at digitalisere har givet os en masse fordele, og i Danmark er vi langt foran, når det kommer til at bruge de mange tjenester, som digitaliseringen indebærer. Men det har jo også en bagside. Når man i et land som Danmark er førende inden for digitalisering og adaption, opstår der desværre også misbrug, og derfor må vi nødvendigvis også være førende inden for bekæmpelsen og forebyggelsen af IT-kriminalitet. NC3 er derfor oprettet som en specialenhed med fokus på digital kriminalitet, og vores funktion er at understøtte de enkelte politikredse i efterforskningen af IT-kriminalitet.

HVORDAN ADSKILLER EFTERFORSKNING AF IT-KRIMINALITET SIG FRA EFTERFORSKNINGEN AF KONVENTIONEL KRIMINALITET?

I virkeligheden er der mange ligheder mellem de to. Når du efterforsker konventionel kriminalitet, skal du sikre dig spor og beviser for at finde ud af, hvad der er sket. Har man med IT-kriminalitet at gøre, er det samme fremgangsmåde. Her er sporene bare ikke DNA, blodspor eller fingeraftryk. Her er sporene digitale spor såsom IP-adresser, logfiler og geodata. Efterforsker vi eksempelvis børnepornografi på nettet, kan det være helt afgørende at finde ud af, hvor og hvornår billederne er taget. I hackersager er det primært i logfilerne, vi skal kigge.

HVAD GØR SÅ IT-KRIMINALITET SPECIELT?

Dét, der er specielt ved IT-kriminalitet, er, at man kan opdele det i to kategorier: Vi kan kigge på den rene kriminalitetsform, som er defineret i politiets gerningskoder. Hackerparagraffen er et eksempel på det. Men vi kan også kigge på IT-kriminalitet som en fremgangsmåde for anden kriminalitet. Når man eksempelvis begår økonomisk bedrageri eller svindel, bruger man jo ofte de digitale medier til at svindle med. Her har digitaliseringen givet os mængder af fordele, men hver gang, der udvikles nye systemer, opstår der også nye fremgangsmåder for de kriminelle, og det er en af de store udfordringer for kriminalitetsbekæmpelsen.

HVAD GØR NC3 FOR AT MATCHE DE KRIMINELLE?

På et taktisk niveau tilstræber vi sammen med politikredsene at sætte et efterforskningshold med den rette sammensætning af kompetencer. Der er nemlig ingen IT-kriminelle, der kan det hele. Derfor er kunsten for os at sammensætte et hold, der har en teknologisk diversitet indbygget. Når vi møder gerningsmændene kan den enkelte kriminelle sagtens være ligeså dygtig – eller endnu dygtigere end os – på et område. Problemet for den kriminelle opstår, når han træder ud på en platform, hvor han ikke er lige så dygtig. Det kan eksempelvis være, når den kriminelle går fra Phishing af data via mailsystemer til at skulle arbejde med disse data på en anden platform, hvor han ikke er teknisk stærk. Det er typisk her, altså når hackeren træder uden for sit specialeområde – eller træder i den digitale spinat så at sige - at vi fanger ham.

HVAD VIL DET SIGE AT ARBEJDE STRATEGISK MED EFTERFORSKNING AF IT-KRIMINALITET?

I NC3 arbejder vi lige nu ud fra fem forskellige strategiske målsætninger, der sammen skal løfte visionen om at styrke samspillet mellem politi og samfund. Målsætningerne fokuserer på at have borgeren i centrum ved at skabe tryghed for den enkelte, på at styrke landets politikredse via uddannelse og teknologi, på at være samarbejdsorienterede i forhold til dansk erhvervsliv, på at opruste internt på kvalitet og kompetencer og på at bane vejen for mere forskning inden for cybercrime. Vi har arbejdet målrettet med denne form for strategiske overvejelser siden vores etablering i 2014, og på længere sigt er det meningen, at de skal bane vejen for et endnu mere strategisk Rigspoliti, hvor ambitionen er, at samspillet bringer Danmark op blandt de førende i at hindre og opklare IT-kriminalitet på verdensplan.

HVORDAN BLIVER MAN FØRENDE I AT HINDRE OG OPKLARE IT-KRIMINALITET?

Én ting er, at man er god til at efterforske. Men IT-kriminaliteten vokser og vokser jo. For at knække denne kurve, har vi derfor en ambition om at bane vejen for at agere mere proaktivt fremfor primært at arbejde reaktivt. Det kan vi gøre ved at have en mere analytisk tilgang til vores arbejde med IT-kriminalitet. En analytisk tilgang vil indebære, at vi kigger på de enkelte kriminalitetsformer og sporer os frem til særlige bevægemønstre. Vi undersøger også incitamentsstrukturer og sammenhænge mellem ofre, gerningsmænd og de forskellige kriminalitetsområder. Kort fortalt forestiller jeg mig, at vi ud over normale efterforskningsskridt også kigger på kriminalitetsformen som et sociologisk fænomen. Når vi bliver klogere på kriminalitetsformen, kan vi begynde at kigge på, hvordan vi kan handle proaktivt. Det kan være ved at gå i dialog med mulige ofre og således arbejde præventivt og skadesbegrænsende, eller det kan være ved at disrupte (red. afbryde) muligheden for at begå en særlig type af IT-kriminalitet ved eksempelvis at lukke et global kriminalitetsnetværk (botnet) ned eller på anden måde chikanere gerningsmændene i deres forehavende. Denne form for analytisk tilgang giver os en hel palette af forebyggelsesmuligheder, og det er blandt andet denne palette, der skal være med til at gøre os førende inden for feltet.

HVEM VINDER KAMPEN LIGE NU? HACKERNE ELLER POLITIET?

Efterforskningsmæssigt og på et teknologisk plan kan vi nogle ting i dag, som hackerne ikke troede, vi kunne. På nationalt såvel som globalt plan mener jeg derfor, at politiet sagtens kan matche hackerne. Men som med alle andre kriminalitetsformer er det sådan, at det er gerningsmanden, der bestemmer tid, sted og metode og på den måde er politiet notorisk et skridt bagefter. Men med den analytiske tilgang til efterforskningsarbejdet kommer vi tættere på at blive i stand til at træde et skridt foran de kriminelle.

ER DET REALISTISK, AT DANMARK BLIVER FØRENDE INDEN FOR FOREBYGGELSE AF IT-KRIMINALITET?

Vi er faktisk allerede godt på vej, fordi vi i Danmark løfter problemet som en samlet, national opgave. Vi er den nordiske politietat, der har været først ude og etablere et særligt center for cybercrime, og vores center er også det største. Derudover er vi lige nu ved at få etableret IT-udstyr i absolut verdensklasse, som også gør os førende på en lang række teknologiske parametre. Når det så er sagt, hjælper vi naturligvis hinanden på tværs af landegrænser, og det er derfor ikke et mål i sig selv at blive bedre end de andre. Det, der også kendetegner udfordringerne ved IT-kriminalitet, er jo netop, at det typisk er kriminalitet, der kan blive begået på tværs af landegrænser, hvorfor målet er et globalt samarbejde på højt niveau, som kan ruste os til at knække IT-kriminalitetskurven for fremtiden.

STRAFFERAMMEN FOR IT-KRIMINALITET

HACKING
– OP TIL 6 ÅRS FÆNGSEL
"Hacking er strafbar efter straffelovens § 263, der i meget grove tilfælde kan medføre straf af fængsel i op til 6 år. Den grove strafferamme er blandt andet tiltænkt personer, der forsøger at skaffe sig adgang til en virksomheds erhvervshemmeligheder."

NIGERIABREVE, PHISHING OG DATINGBEDRAGERI
– OP TIL 6 ÅRS FÆNGSEL
"At sende en mail eller på anden vis kontakte personer med det formål at franarre dem penge er forsøg på bedrageri, jævnfør straffelovens § 279, som kan straffes med fængsel op til 1 år og 6 måneder. I særligt grove tilfælde kan strafferammen dog stige til 6 år."

KØB AF KREDITKORTOPLYSNINGER
– OP TIL 8 ÅRS FÆNGSEL
"Hvis det ligger klart, at det sker for at kunne købe ind med andre menneskers kort, vil det være forsøg på databedrageri jævnfør straffelovens § 279a, hvor maksimumstraffen er op til 8 års fængsel. Selvom man ikke kan bevise et konkret forsøg på databedrageri, vil blandt andet køb af sådanne oplysninger være strafbar efter straffelovens § 301, hvor straffen kan gå op til 6 års fængsel i grove tilfælde."

KØB AF LOGININFORMATIONER
– OP TIL 6 ÅRS FÆNGSEL
"Der vil typisk kunne være tale om en overtrædelse af straffelovens § 263a, der i grove tilfælde har en maksimumstraf af fængsel i op til 6 år."

BESTILLING AF DDOSANGREB
– OP TIL 2 ÅRS FÆNGSEL
"Et DDoS-angreb vil være strafbart efter straffelovens § 293, stk. 2, hvor strafferammen i grove tilfælde kan gå op til 2 års fængsel. Den, der bestiller et sådant angreb, betragtes som medvirkende og kan straffes efter samme strafferamme."

KØB AF WEBCAMSERVICES
– OP TIL 6 MÅNEDERS FÆNGSEL
Efter straffelovens § 264a er det strafbart "uberettiget at iagttage personer, der befinder sig på et ikke-frit tilgængeligt sted". Det er blandt andet hjemme hos en selv. Strafferammen er fængsel i indtil 6 måneder."

Kilde: Lars Bo Langsted, professor og leder af International Economic Crime and Cyber Crime Research Centre (IECC), Juridisk Institut, Aalborg Universitet. Oversigten er tidligere bragt i Computerworld.

HVEM GØR HVAD?

Myndigheder	Arbejdsområde	Hvad kan du få hjælp til?
POLITIET www.politi.dk	Politiet har blandt andet til opgave at efterforske og forfølge strafbare forhold.	Hos politiet kan du både som borger eller virksomhed anmelde alle former for kriminalitet, herunder også IT-kriminalitet.
RIGSPOLITIETS NATIONALE CYBER CRIME CENTER (NC3) www.politi.dk	NC3 skal blandt andet bistå politikredsene med efterforskning af IT-relaterede straffesager. Samtidig skal centeret bidrage til den forebyggende indsats mod IT-kriminalitet.	Du kan som borger og virksomhed anmelde forbrydelser om hacking, DDoS-angreb samt seksuelt misbrug af børn, som involverer internettet, computere og så videre til NC3.
DATATILSYNET www.datatilsynet.dk	Datatilsynet er den statslige myndighed, der fører tilsyn med persondataloven.	Du kan som borger, virksomhed og myndighed få hjælp hos Datatilsynet, hvis du har spørgsmål om registrering og anden behandling af personoplysninger. Du kan klage til Datatilsynet, hvis du mener, at en behandling af oplysninger om dig ikke lever op til persondataloven.
FORSVARETS EFTERRETNINGSTJENESTE – CENTER FOR CYBERSIKKERHED www.fe-ddis.dk	Center for Cybersikkerhed har blandt andet til opgave at imødegå avancerede cyberangreb mod myndigheder og virksomheder, der er beskæftigede med samfundsvigtige funktioner.	Myndigheder, kommuner og virksomheder, der beskæftiger sig med samfundsvigtige funktioner kan i forbindelse med sikkerhedshændelser kontakte Netsikkerhedstjenesten døgnet rundt.
FORBRUGERSTYRELSEN www.forbrug.dk	Forbrug.dk er den offentlige forbrugerportal, hvor man finde viden om forbrugerforhold samt klage over erhvervsdrivende.	På hjemmesiden kan du få råd og vejledning om forbrugerrelaterede spørgsmål.
BORGER.DK www.borger.dk	Borger.dk er en borgerportal, der fungerer som borgernes adgang til det offentlige.	På hjemmesiden kan du bl.a. få generelle tips og råd til sikker adfærd på internettet.
ERHVERVSSTYRELSEN www.privacykompasset.erhvervsstyrelsen.dk	Erhvervsstyrelsen hjælper virksomheder med blandt andet at overholde lovgivning om privacy.	PrivacyKompasset er et online værktøj, der kan hjælpe virksomheder med at kortlægge deres brug af persondata og efterleve persondatalovgivningen.

EN RÆKKE MYNDIGHEDER OG ORGANISATIONER I DANMARK ARBEJDER MED AT FOREBYGGE, EFTERFORSKE OG RÅDGIVE OM IT-KRIMINALITET. OVERSIGTEN VISER, HVILKE OPGAVER DE FORSKELLIGE MYNDIGHEDER OG ORGANISATIONER VARETAGER, OG HVOR MAN SOM BORGER ELLER VIRKSOMHED KAN FÅ MERE VIDEN, RÅD, HJÆLP ELLER VEJLEDNING OM IT-KRIMINALITET, SIKKER NETADFÆRD OG PRIVACY.

Organisationer	Arbejdsområde	Hvad kan du få hjælp til?
RÅDET FOR DIGITAL SIKKERHED www.digitalsikkerhed.dk	Rådet er en uafhængig medlemsorganisation, som har til formål at fremme tryg IT-anvendelse i fremtidens digitale samfund.	På rådets hjemmeside kan du finde en række råd og vejledninger til at forbedre din eller din virksomheds digitale sikkerhed.
FORBRUGERRÅDET www.taenk.dk	Forbrugerrådet Tænk er en uafhængig medlemsorganisation, der har til formål at informere forbrugere om og forbedre deres rettigheder.	På rådets hjemmeside kan du på underside "Mit digitale liv", kan du finde gode råd og værktøjer til et mere sikkert digitalt liv.
MEDIERÅDET FOR BØRN OG UNGE www.dfi.dk	Medierådet er bland andet et videncenter for børn og unges brug af nye online teknologier.	På rådets hjemmeside kan du finde en række råd og vejledninger vedrørende børn og unges online liv.
DET KRIMINALPRÆVENTIVE RÅD www.dkr.dk	DKR er en uafhængig medlemsorganisation, der har til formål at forebygge kriminalitet og skabe et tryggere samfund.	På rådets hjemmeside kan du finde artikler, undersøgelser og gode råd om IT-kriminalitet.
E-MÆRKET www.emaerket.dk	e-mærket er en nonprofit-organisation, som er en mærkningsordning for sikker nethandel.	Du kan som forbruger kontakte e-mærkets telefoniske hotline, hvis du har brug for hjælp i forbindelse med en e-handel.
SIKKERCHAT www.sikkerchat.dk	Sikkerchat.dk er en oplysningsside, der har til formål at klæde børn og unge på til at færdes trygt internettet og på mobil.	Du kan både som ung, forælder eller lærer finde viden og værktøjer til at tackle problematisk mediebrug.
RETTIGHEDSALLIANCEN www.rettighedsalliancen.dk	Rettighedsalliancen er en interesseorganisation, som blandt andet bekæmper piratkopiering på internettet.	På hjemmesiden kan du som forbruger og myndighed få information og vejledning om, hvad der er lovligt og ikke lovligt, når det gælder ophavsretsligt beskyttet materiale på internettet.
DANSK INDUSTRI (DI DIGTIAL) www.digital.di.dk	DI Digital varetager DI's interesser på det IT- og telepolitiske område.	På hjemmesiden kan du som virksomhed (også som mindre virksomhed) finde IT-sikkerhedsvejledninger med videre.

EUROPOL

KRIMINALITET SOM EN SERVICEYDELSE

IT-KRIMINALITET ER IKKE LÆNGERE FORBEHOLDT EN SÆRLIG GRUPPE AF KRIMINELLE, MEN ER BLEVET TILGÆNGELIG FOR ALLE INTERESSEREDE. PÅ DEN SKJULTE DEL AF INTERNETTET EKSISTERER EN UNDERGRUNDSØKONOMI, HVOR HACKERE SÆLGER DERES VIDEN OG FÆRDIGHEDER SOM SERVICEYDELSER.

I løbet af de seneste par årtier har den digitale undergrundsverden udviklet sig fra at bestå af enkelte mindre grupper af hackere og telefon-hackere, som primært søgte spænding og indbyrdes prestige, til at være en blomstrende kriminel industri, som anslås at koste den globale økonomi over 300 milliarder dollars årligt.

Den digitale undergrundsverden er ikke blot kompleks og yderst dynamisk, den er også yderst fragmenteret. Der findes alle typer lige fra de mest sofistikerede kriminelle til nystartede cyberkriminelle, som alle har deres helt egne færdigheder og ekspertiseområder. Det er denne arbejdsfordeling og opdyrkelse af niche-funktionaliteter, som driver den kriminelle økonomi, og som har skabt en serviceydelse- eller "*crime-as-a-service*"-industri, hvor færdigheder gøres til en handelsvare. Det giver mange flere adgang til at udføre former for kriminalitet, som tidligere ville have krævet helt særlige tekniske forudsætninger.

DEN MØRKE DEL AF INTERNETTET

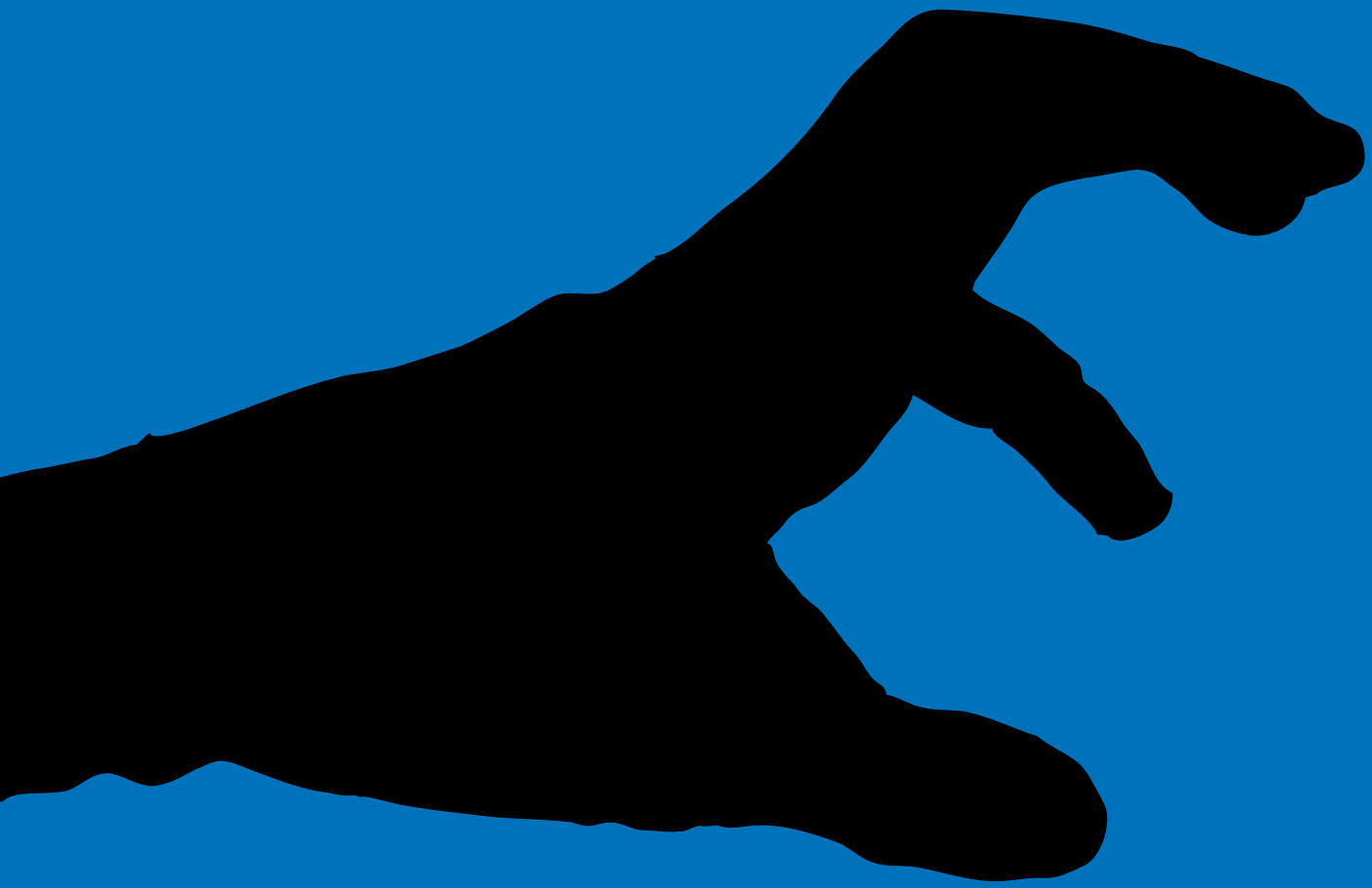
Undergrundsøkonomien afhænger i høj grad af markedspladser på nettet, hvor udbud og efterspørgsel mødes; steder, hvor man kan reklamere for, købe og sælge produkt- og serviceydelser, udveksle erfaringer og ekspertise. Indsamlingen og delingen af viden, som foregår disse steder, stimulerer også research og udvikling i forhold til kriminelle aktiviteter.

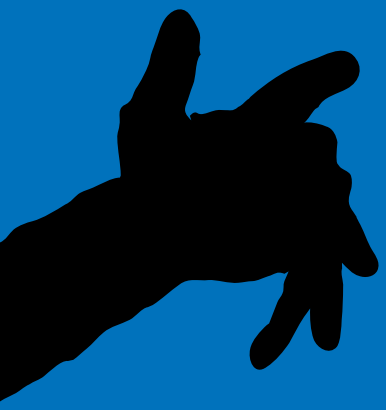
Sådanne fora kan enten omhandle specifikke emner (for eksempel et produkt eller en specialiseret service som hacking eller betalingskortsvindel - det vil sige tyveri og svindel med betalingskortoplysninger), eller være organiseret som mere generaliserede fora, der beskæftiger sig med en bred vifte af emner og produkttyper, og som dermed understøtter hele spektret af cyberkriminalitet og tilbyder alle mulige logistiske løsninger til dem, der ønsker at begå cyberkriminalitet.

Siden disse fora begyndte at dukke op i starten af årtusindeskiftet, er de blevet meget mere sofistikerede med en højere ekspertise og et bredere udvalg af produkter, en højere grad af professionalisme og mere avancerede sikkerhedsforanstaltninger.

> Et enkelt forum på russisk med over 13.000 medlemmer og tæt på 4.000 besøgende dagligt havde mere end 20 underfora, som dækkede emner som online-sikkerhed, instruktioner, betalingskortsvindel, botnet, web-design samt hvidvaskning af penge. Over hele forummet var der mere end 75.000 individuelle diskussionstråde.

Traditionelt har disse fora været at finde enten på det åbne eller det dybe net (Deep Web), men de cyberkriminelle fællesskaber optræder i højere og højere grad på det såkaldt mørke net (Darknet). De samme mekanismer, som tilbyder brugere anonymitet, gør det muligt at hoste indhold anonymt på netværkene, tilsyneladende uden at indholdet kan spores, samtidigt med,





at det er tilgængeligt. Denne teknologi har dannet grobund for det, som er blevet kendt som skjulte services.

De skjulte tjenester optræder generelt i to former, som undergrundsfora og kriminelle markedspladser. Darknet undergrundsfora fungerer typisk ligesom de fora, vi ser på det åbne internet, nemlig som mødesteder med diskussioner og elektroniske opslagstavler for mange forskellige fællesskaber. På *Darknet* kan man således finde undergrundsfora, som er helliget narkotika, hacking, betalingskortsvindel og pædofili.

KRIMINELLE MARKEDSPLADSER

Selvom der kan forekomme handel med illegale produkter på sådanne fora, er *Darknet* primært blevet berygtet for sine specialiserede kriminelle markedspladser, hvoraf *Silk Road* nok er den mest kendte. På disse markedspladser kan brugerne få fat i illegale produkter eller serviceydelser af enhver art, herunder narkotika, våben, lægemidler og steroider, forfalskede dokumenter, kreditkort, hacking-teknologi - ja selv lejemordere. *Silk Road* har affødt adskillige andre sites, så som *Agora*- og *Outlaw*-markederne og – efter nedlukningen af *Silk Road* i oktober 2013 – *Silk Road 2.0*. I august 2014 blev antallet af sådanne markeder opgjort til mindst 39. Hovedparten af dem er på engelsk, men man kan dog også finde markedspladser på andre sprog, blandt andet finsk, fransk, italiensk, polsk og russisk.

På trods af den øgede beskyttelse og anonymitet, som *Darknet* giver brugerne, opererer de mere sofistikerede og farlige cyberkriminelle fora stadig på det åbne internet. Dette skyldes muligvis en opfattelse af, at disse netværk giver større kontrol over den interne sikkerhed, end hvad en *Darknet*-infrastruktur kan give, samt bedre netværkshastigheder.

TILLID OG SIKKERHED

Hvad enten vi taler om det åbne net eller *Darknet*, er det ikke altid ligetil at opnå adgang til disse markedsplatforme. Jo mere sofistikeret et forum er, desto skrappere er adgangsbegrænsningerne. På de fora, hvor sikkerheden er højest, skal nye medlemmer først anbefales og godkendes af eksisterende medlemmer.

Inden for disse fora finder man ofte en rigid hierarkisk struktur (som er unik for cyberkriminalitet), hvor brugerne får tildelt specifikke roller og ansvarsområder. Sådanne strukturer gør det muligt for fællesskaberne at føre intern kontrol, holde styr på deres medlemstal samt skille sig af med uønskede eller besværlige medlemmer.

Foraene vil også have en masse forhandlere, som forummets medlemmer kan købe serviceydelser og produkter af. For at opnå status som forhandler kræves det typisk, at man har afgivet

prøver på ens ydelser eller produkter til moderatorernes godkendelse. Forhandlernes produkter og tjenester bliver løbende anmeldt og bedømt af kunderne. Konceptet med brugerbedømmelser og omdømme svarer til det, man finder på lovlige kommercielle websteder, selvfølgelig bortset fra, at det kan være svært at finde cyberkriminelle med et godt omdømme.

CROWD- OG OUTSOURCING

De kriminelle markedspladser tilbyder en samlende platform for kriminelle ydelser, som forskellige enkeltindivider sidder inde med. De gængse definitioner på organiseret kriminalitet er derfor ikke dækkende for den digitale undergrundsøkonomi. Relationerne mellem de cyberkriminelle er ofte flygtige – sommetider er det begrænset til den konkrete transaktion - således, at de cyberkriminelle sjældent har nogen som helst kontakt med hinanden offline. I stedet er det disse markeder, som skaber et organiseret netværk af kriminelle relationer. Der er dog en stigende tendens til, at enkeltindivider finder sammen i grupper for at udføre specifikke projekter eller angrebskampagner, men selv sådanne grupper er ikke præget af samme hierarki og struktur, man normalt ser blandt grupper inden for den organiserede kriminalitet.

I en lidt forenklet forretningsmodel kan en cyberkriminels portefølje omfatte kompetencer inden for ondsindet software (malware), understøttende infrastrukturer, stjålne persondata og finansielle oplysninger samt redskaber til at skabe indtjening på baggrund af de kriminelle aktiviteter. Når sådanne kompetencer bliver udbudt, enten gennem salg eller som serviceydelser, er det relativt let for nyindviede cyberkriminelle uden særlig meget erfaring eller teknisk snilde at iværksætte cyberangreb med uforholdsmæssigt store skadevirkninger og udføre dem for meget få midler. Muligheden for at outsource væsentlige dele af deres aktiviteter gør desuden de erfarne cyberkriminelle i stand til at hellige sig deres kerneaktiviteter, hvorved de kan blive endnu mere effektive og specialiserede.

Kilder:
Artiklen er en oversat reproduktion af Europol (2014): The Internet Organised Crime Threat Assessment (iOCTA), kapitel 3.
Deep dot net (2013): Updated: List of Dark Net Markets (Tor & 12P) (https://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/).
Saadawi, Tarek, Louis H. Jordan, Jr. & Vincent Boudreau (eds.) (2013): Cyber Infrastructure Protection, Strategic Studies Institute & U.S. Army War College Press (http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1145.pdf).
The European Parliament (2013): The Economic, Financial and Social Impacts of Organised Crime in the European Union (http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493018/IPOL-JOIN_ET(2013)493018_EN.pdf).
McAfee (July 2013): The Economic Impact of Cybercrime and Cyber Espionage (http://www.mcafee.com/nl/resources/reports/rp-economic-impact-cybercrime.pdf).
Rand Corporation (2014): Markets for Cybercrime Tools and Stolen Data (http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf).

NÅR FORBRYDELSER BLIVER DIGITALE
FORBRYDELSER MOD BORGERE

Kapitel 2

FORBRYDELSER MOD BORGERE

IT-KRIMINALITET SOM RAMMER BORGERE

IT-KRIMINALITET KAN RAMME BÅDE VIRKSOMHEDER, BANKER, ORGANISATIONER OG PRIVATE PERSONER. SIDSTNÆVNTE KALDES FOR BORGERRETTET IT-KRIMINALITET, OG DET ER DENNE FORM FOR IT-KRIMINALITET, SOM KAPITEL 2 HANDLER OM.

Selvom der er stor forskel på, hvordan kriminalitet udøves på internettet i forhold til kriminalitet i den "virkelige" og analoge verden, er der dog ofte tale om de samme kriminalitetstyper. Ligesom man kan udsættes for bedrageri eller tyveri i den virkelige verden, kan det samme også forekomme som IT-kriminalitet. Forskellen ligger i, at hvor man i den virkelige verden får stjålet sin pung ved lommetyveri eller indbrud, så kan kriminelle anvende internettet til at stjæle ens penge. Det kan eksempelvis være ved, at ens kortoplysninger bliver kopieret, at man har oplyst sine betalingskortoplysninger via en falsk hjemmeside, eller at man har fået installeret et skadeligt program på computeren, der kan aflure ens koder. Samtidig deler vi store mængder private oplysninger på internettet som billeder, private beskeder, videoklip og andet, som gør, at kriminelle har mulighed for at afpresse eller chikanere folk på måder, som tidligere ikke var muligt.

På trods af, at langt de fleste danskere i dag er online og bruger internettet på daglig basis, er IT-kriminalitet heldigvis kun noget som sker relativt sjældent. Til sammenligning oplever danskerne mere end tre gange så ofte at få stjålet ting i den virkelige verden i forhold til at blive udsat for økonomisk bedrageri på internettet (heri er medregnet betalingskortmisbrug, identitetstyveri og handelsbedrageri).

Selvom de fleste danskere ikke er udsat for IT-kriminalitet, er der stadig god grund til at være opmærksom på, hvordan man undgår at blive snydt af kriminelle på internettet og lære at tage sine forholdsregler for at beskytte sig selv.

Nedenfor er tre almindelige IT-kriminalitetstyper beskrevet sammen med en række gode råd til, hvordan man kan nedbringe risikoen for at blive offer for IT-kriminalitet.

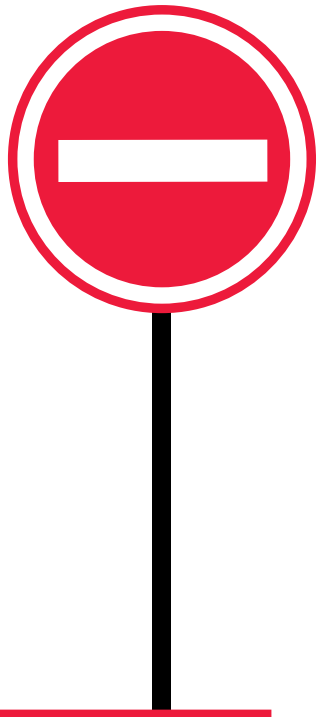
DIGITALT TYVERI – PHISHING, SKIMMING OG PHARMING

IT-kriminelle anvender en lang række mere eller mindre avancerede metoder til at stjæle penge fra borgere. Det mest almindelige er misbrug af betalingskort, men i få tilfælde kan kriminelle også skaffe sig adgang til private personers netbank. Typisk opdages misbruget først, når man selv opdager, at der er blevet foretaget ukendte køb/transaktioner, eller hvis banken spærrer kortet eller kontoen på grund af mistænkelige transaktioner.

Fælles for begge typer af forbrydelser er, at kriminelle ved at snyde forbrugere får adgang til vigtige økonomiske oplysninger som betalingskortoplysninger eller NemID.

I mange tilfælde skyldes betalingskortmisbruget dog ikke ens egen adfærd, men derimod at den virksomhed, hvor man har brugt sit kort, har for dårlig sikkerhed. Det gælder både køb hos almindelige butikker og køb i internetforretninger. Betalingskortmisbrug kan også hænge sammen med "skimming", hvor kriminelle eksempelvis har monteret en falsk front på en hæveautomat, der kopierer oplysningerne fra de betalingskort, som anvendes i automaten.

En anden situation, hvor det kan gå galt er, at man ved en fejl oplyser sine betalingskortoplysninger, NemID eller andre "log-in"-oplysninger til kriminelle,

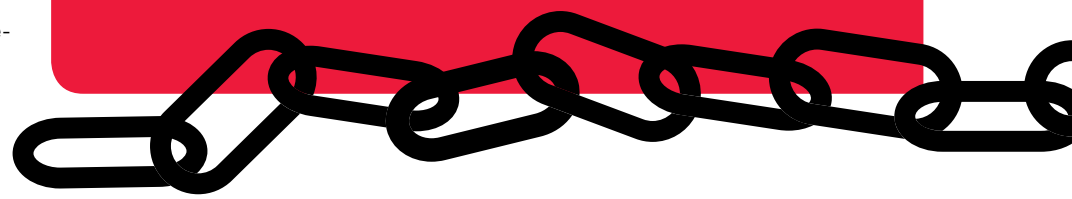


fordi man bliver snydt af en såkaldt phishing-mail. Phishing-mails er kendetegnet ved, at man modtager en e-mail fra en afsender, som man fejlagtigt tror er ens bank eller en anden troværdig virksomhed eller myndighed. I lang tid har disse mails været lette at gennemskue blandt andet på grund af dårligt sprog, men de kriminelle, der står bag phishing-mailene bliver stadig bedre og bedre – både til at formulere e-mails i et troværdigt sprog og til at efterligne logoer. Ingen reelle virksomheder eller myndigheder anmoder dog om betalingskortoplysninger, NemID eller andre log-in-informationer via e-mail eller sms. Derfor skal man aldrig, uanset hvor overbevisende mailen er, sende sådanne oplysninger over e-mail.

Ved de mere avancerede former for bedrageri kan kriminelle have oprettet pharming-sider, som er hjemmesider, der til forveksling ligner en rigtig netbank eller en kendt internetbutik, og som har til formål at få offeret til at indtaste sine økonomiske oplysninger. Via eksempelvis e-mails sender IT-kriminelle links til de falske hjemmesider, og man bør derfor aldrig åbne

GODE RÅD TIL AT UNDGÅ BETALINGSKORT-MISBRUG OG NETBANKINDBRUD:

- ☛ Tjek, at betalingen foregår over en krypteret forbindelse, når du eksempelvis handler på nettet (kig efter hængelås-logoet eller "https" i browserens adressefelt).
- ☛ Vær skeptisk, når nogen uopfordret sender dig en mail. Og lad være med at trykke på links eller åbne filer, med mindre du har fuld tillid til afsenderen.
- ☛ Log altid på din netbank via browserens adressefelt og ikke via et link i eksempelvis en mail.
- ☛ Kig jævnligt på din netbank og tjek, om der er posteringer (også småbeløb), du ikke kender til.
- ☛ Vær opmærksom på, at reelle virksomheder eller myndigheder aldrig vil sende en mail, hvor der anmodes om at få oplyst kortoplysninger, NemID eller andre "log-in"-oplysninger.
- ☛ Beskyt din pinkode, når du anvender dit betalingskort.



links i e-mails, som man modtager fra en ukendt afsender. En anden indgang til privates økonomiske oplysninger er via installation af malware på offerets computer. Malware er skadelige programmer, der eksempelvis kan give kriminelle mulighed for at overvåge ens computer og dermed få adgang til personlige og økonomiske oplysninger.

De mange forskellige måder, som IT-kriminelle anvender til at skaffe sig adgang til privates økonomiske oplysninger, kan virke uigennemskuelige og give anledning til utryghed. Heldigvis er misbrug af betalingskort og indbrud i netbank områder, hvor man som forbruger er godt beskyttet. I de fleste tilfælde hæfter man nemlig ikke selv for tabet, men der kan dog i visse tilfælde være en selvrisiko. Eksempelvis, hvis man ikke straks efter, at man har opdaget misbruget, får kort eller konto spærret, eller hvis kortet er blevet udnyttet ved brug af pinkoden.

Selvom man i udgangspunktet er godt beskyttet, er det selvfølgelig altid ubehageligt at blive udsat for tyveri. Udover forskrækkelsen i at opdage, at der er hævet penge på ens konto for ting, man ikke kender til, så kan det være frustrerende at skulle have nyt kort, ændre i betalingsserviceaftaler og så videre.

IDENTITETSTYVERI

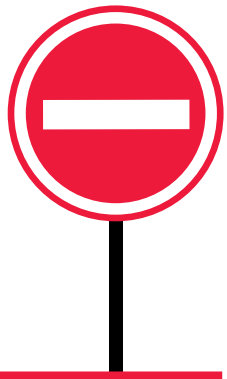
Begrebet identitetstyveri henviser til den situation, hvor en person misbruger en anden persons personoplysninger (eksempelvis navn, CPR-nummer, mailkonto) eller identitetsbeviser (eksempelvis kørekort, sygesikringsbevis) typisk med henblik på at opnå en økonomisk gevinst. Identitetstyveri er derfor mere en beskrivelse af en metode til at begå kriminalitet frem for en selvstændig forbrydelse, og det er da heller ikke forbudt at være i besiddelse af andres personoplysninger eller identitetsbeviser. Det kan derfor i mange sammenhænge være mere retvisende at tale om identitets*misbrug* frem for identitets*tyveri*.

Der kan være mange forskellige formål med at udgive sig for at være en anden, som kan spænde lige fra, at man ikke er gammel nok til at komme ind på et diskotek og derfor anvender sin storesøsters kørekort, til at forfalske en underskrift for at begå bedrageri eller bestille varer og abonnementer med det formål at chikanere. Begrebet "identitetstyveri" er derfor ikke et nyt fænomen, men er særligt interessant i forhold til IT-kriminalitet, fordi identifikations-processer i mange sammenhænge er blevet automatiseret. Det vil sige, at er man blot i besiddelse af de rette informationer, eksempelvis brugernavn, password og NemID, så sker der ikke en kontrol af, hvem der rent faktisk indtaster disse oplysninger. Det er derfor muligt på en helt anden måde end tidligere at oprette eksempelvis låne- eller abonnementsaftaler eller få adgang til private og personfølsomme oplysninger, såsom helbredsoplysninger, uanset hvor i verden man befinder sig, forudsat at man er besiddelse af de rette adgangsoplysninger.

Ligesom ved betalingskortmisbrug er man som borger i udgangspunktet godt beskyttet, hvis man udsættes for identitetsmisbrug, fordi man ikke er juridisk forpligtet af, at andre har misbrugt ens identitetsoplysninger eksempelvis til at optage et lån. Identitetstyveri kan dog være en meget ubehagelig oplevelse, fordi det kan være en langvarig og opslidende proces at overbevise kreditorer og andre om, at man ikke selv har foretaget de pågældende køb eller lån. Samtidig kan der også være en usikkerhed forbundet med, hvad identitetstyvene egentlig har fået af oplysninger, og om de bliver brugt i andre sammenhænge, solgt videre til andre, og om man derfor kan føle sig sikker fremover.

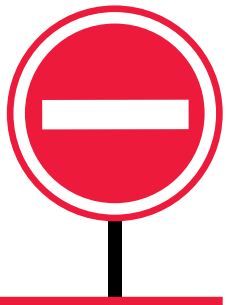
OBS!

Hvis dine identitetsoplysninger er blevet misbrugt, er det vigtigt straks at oplyse kreditor skriftligt om, at du har været udsat for identitetstyveri og derfor ikke ønsker at betale regningen. Det kan ofte være en god idé at vedlægge en kopi af en politianmeldelse.



GODE RÅD TIL AT UNDGÅ IDENTITETSTYVERI:

- Undlad at opgive personlige oplysninger, som fx CPR-nummer i mails eller på sociale medier.
- Sørg for ikke at opbevare alle dine personlige kort i samme pung. Hermed kan du forhindre, at kriminelle får adgang til for eksempel både CPR-nummer og kontooplysninger og dermed får lettere ved at misbruge din identitet.
- Undlad at smide fysiske breve i skraldespanden, hvor personlige oplysninger, som for eksempel CPR-nummer, er synlige. Inden du smider et sådan brev ud, kan du for eksempel rive papiret itu eller overstrege de personlige oplysninger.
- Undlad at bruge samme adgangskode til alle dine profiler, mailkonti med mere. Et godt password består af mindst otte tegn, store og små bogstaver samt tal og specialtegn.



GODE RÅD TIL AT UNDGÅ AFPRESNING OG FORSKUDSBEDRAGERI:

- Undgå at sende nøgenbilleder eller lignende over mobilen eller internettet. Hvis du sender nøgenbilleder af dig selv er det en god idé, at du ikke kan genkendes på billederne, for eksempel kan du tage billedet, uden at dit ansigt er synligt.
- Vær sikker på, hvem du overfører penge til, inden du gør det, og vær skeptisk, hvis en person, du dater over internettet, og som du ikke har mødt, beder dig om at overføre penge.
- Vær skeptisk, når nogen uopfordret sender dig en mail. Og lad være med at trykke på links eller åbne filer, med mindre du har fuld tillid til afsenderen.
- Hav altid en backup af dine vigtigste billeder og dokumenter liggende. Så er du mindre sårbar over for vira og over for at blive afpresset for penge for at få adgang til dine dokumenter på computeren (ransomware).

AFPRESNING OG BEDRAGERI

Mange har efterhånden prøvet at modtage en e-mail, hvor man bliver stillet tusindvis – ja sågar millioner – af kroner i udsigt. Heldigvis havner langt de fleste af disse breve og e-mails i skraldespanden. Desværre er der stadig en lille gruppe af personer, som lader sig lokke og derfor ender med at miste penge.

Nigeriabreve – eller forskudsbedrageri – er en moderne variation af et gammelt svindelnummer, hvor metoden er, at offeret på forhånd betaler et pengebeløb med henblik på efterfølgende at opnå et eller andet ønskværdigt, som imidlertid aldrig bliver indfriet. Det kan eksempelvis være, at vedkommende betaler et beløb med henblik på senere at modtage et større beløb (Nigeriabreve), eller at offeret betaler penge til en person i udlandet, som vedkommende troede han/hun datede, men som efterfølgende viser sig at være en bedrager (datingbedrageri).

Der findes utallige varianter, men de mest kendte involverer ofte en højtstående embedsmand eller general, som skal have hjælp til at smugle et stort pengebeløb ud af et konfliktramt land. For at pengene kan udbetales, skal offeret altid forudbetale nogle udgifter til eksempelvis afgifter, advokatregninger eller bestikkelse. Pengene skal typisk overføres ved brug af pengeoverførselsbureauer, som eksempelvis Western Union eller MoneyGram, fordi pengemodtageren på den måde har bedre mulighed for at forblive anonym. Andre typer af bedrageri, som følger samme metode er eksempelvis meddelelser om store lotterigevinster, arv fra ukendte familiemedlemmer eller beskeder fra venner, som akut har brug for penge. I stedet for penge kan gevinsterne også være kærkesteforhold, kur mod sygdom eller andet.

Hvor forskudsbedrageri knytter sig til situationer, hvor offeret betaler penge på forskud med henblik på at opnå noget, knytter *internet-afpresning* sig typisk til situationer, hvor offeret afpresses til at betale penge med henblik på at undgå noget. Afpresning fungerer ofte ved, at offeret trues med, at vedkommende vil få misbrugt eller ødelagt sine private data eller billeder, hvis han/hun ikke betaler et beløb til afpresseren.

En form for afpresning er såkaldt *sexafpresning*, hvor gerningspersonen typisk har fået adgang til private billeder, film eller lignende af offeret – ofte med et seksuelt indhold – som vedkommende så truer med at offentliggøre, hvis ikke vedkommende betaler et pengebeløb eller sender flere billeder.

En anden form for afpresning er såkaldt ransomware (ransom = løsesum), hvor der er blevet installeret noget malware (ondsindet software) på offerets computer, der fastlåser brugerens adgang til de data, som ligger på computeren. For at få adgang til oplysningerne igen afpresses offeret til at betale en løsesum til bagmændene bag det skadelige softwareprogram. En anden version af denne form for afpresning er, at offeret blot narres til at tro, at han/hun ikke kan få adgang til sine data, uden at gerningspersonerne dog i realiteten har installeret det skadelige ransomware-program.

For de personer, der udsættes for afpresning og forskudsbedrageri, er denne form for bedrageri typisk meget ubehagelig. Ved datingbedrageri er der tale om, at offeret er blevet snydt af en person i udlandet, som man troede, man datede, og der er derfor tale om en form for svindel, hvor det ikke kun er penge, men også følelser, der kommer i klemme. Tilsvarende er sexafpresning også en form for kriminalitet, der ofte er meget ubehageligt for offeret. Dels fordi offeret ved, at en uønsket person har adgang til meget private billeder eller optagelser af vedkommende, og dels fordi offeret har mistet kontrollen med, hvem der fremadrettet kan få materiale at se.

Kilder: De gode råd og dele af artiklen er også bragt i Det Kriminalpræventive Råds pjece om IT-kriminalitet: Det Kriminalpræventive Råd (2015): Cybercrime – Når kriminaliteten rykker online.

HVOR MANGE DANSKERE UDSÆTTES FOR IT-KRIMINALITET?

IT-KRIMINALITET RETTET MOD BORGERNE

Der anmeldes kun et begrænset antal sager om IT-kriminalitet rettet mod private danskere til politiet, og det reelle omfang af såkaldt borgerrettet IT-kriminalitet kan derfor ikke fastslås ved brug af anmeldelsesdata. For at få et bedre indblik i, hvor mange danskere som udsættes for IT-kriminalitet, benyttes i stedet såkaldte offerundersøgelser. Ved offerundersøgelser spørges et repræsentativt udsnit af danskerne (mellem 16 og 74 år), om de har været udsat for forskellige former for kriminalitet på internettet i løbet af det seneste år. Det nyttige ved offerundersøgelser er, at de både indfanger de tilfælde af kriminalitet, der anmeldes, og de tilfælde, der ikke anmeldes. Hermed giver offerundersøgelser også indsigt i, hvor stor en andel af ofrene, der anmelder den forbrydelse, de har været udsat for. Det kalder man anmeldelsestilbøjeligheden.

Det Kriminalpræventive Råd har i 2014 fået foretaget en offerundersøgelse om IT-kriminalitet rettet mod private borgere, som blev udgivet i april 2015.[1]

Offerundersøgelsen viste, at cirka 3,6 procent af danskerne oplevede at blive udsat for IT-kriminalitet i 2014[2], når der spørges ind til identitetstyveri, bedrageri, chikane og forskellige former for afpresning. Det svarer til omkring 150.000 danskere. Omtrent halvdelen af disse tilfælde skyldes betalingskortmisbrug.

Risikoen for at blive udsat for IT-kriminalitet i 2014 var nogenlunde den samme som året før, hvor en lignende undersøgelse pegede på, at 4,0 procent af danskerne i 2012/2013 blev udsat for IT-kriminalitet.

1 Undersøgelsen er udarbejdet af ph.d. og kriminolog Peter Kruize fra Københavns Universitet, som også har stået for udarbejdelsen af tidligere offerundersøgelser på området.

2 Data er indsamlet fra august 2014 til og med januar 2015. I undersøgelsen er spurgt til, om man har været udsat for IT-kriminalitet inden for de seneste 12 måneder. Det vil sige, at undersøgelsen primært dækker 2014, men også medtager information fra personer, der blev udsat i perioden fra august 2013 og frem til januar 2015. I denne sammenhæng anvendes termen 2014 dog forsimplende for den omtalte tidsperiode, da der hovedsagligt er tale om kalenderåret 2014.

DANSKERNES UDSATHED FOR IT-KRIMINALITET

Ca. 74.400
danskere udsat i 2014

BETALINGSKORTMISBRUG
ved betalingskortmisbrug forstås, at en anden person har anvendt offerets Dankort eller andet betalingskort til at købe en vare eller ydelse på internettet, uden at kortets ejer har givet tilladelse til det

Ca. 22.700
danskere udsat i 2014

NETHANDELBEDRAGERI
Nethandelsbedrageri henviser til de situationer, hvor en person sælger en vare over internettet, men aldrig modtager betaling for varen, eller hvor en person køber en vare, som vedkommende aldrig modtager, eller som viser sig at være en billig kopi.

Ca. 34.400
danskere udsat i 2014

IDENTITETSTYVERI
Identitetstyveri vil sige, at en anden person har anvendt offerets personoplysninger (fx navn, CPR-nr., mailkonto) eller identitets- beviser (fx kørekort, sygesikringsbevis) uden vedkommendes tilladelse med henblik på at opnå en økonomisk gevinst.

Knap 16.000
danskere udsat i 2014

CHIKANE
Chikane vil her sige, at en person har brugt internettet til at chikanere en anden person. Det kan fx være ved at skrive negative beskeder om offeret på sociale medier, sende beskeder fra offerets mailkonto, foretage ændringer på offerets facebook-profil mm.

NIGERIABREVE
På baggrund af en mail, som offeret har modtaget (ofte fra en udenlandsk afsender), betaler offeret et beløb i den tro, at han/hun senere modtager et større beløb.

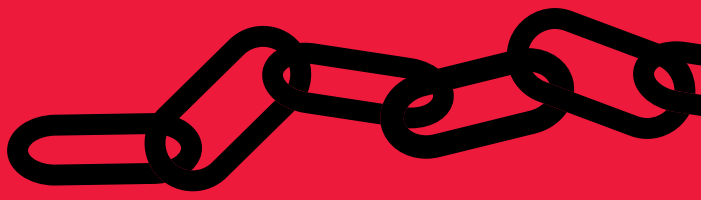
SEXAFPRESNING
Offeret afpresses til fx at betale penge for at undgå at kompromitterende billeder/film af ham/hende offentliggøres.

RANSOMWARE
IT-kriminelle skaffer sig adgang til offerets computer, som de derefter blokerer, indtil vedkommende betaler en løsesum, for at få sine data fri igen

DATINGBEDRAGERI
En person offeret dater over internettet, og som vedkommende måske har overført penge til, viser sig at være en bedrager

For få i undersøgelsen til at lave et præcist estimat

Kilde: Kruize, Peter (2015): Internetkriminalitet 2014 – Offerundersøgelse om identitetstyveri, bedrageri, afpresning og chikane i cyberspace, Det Kriminalpræventive Råd.



INTERVIEW MED PROFESSOR DOKTOR PETER FISCHER
PSYKOLOGISK INSTITUT, REGENSBURG UNIVERSITET, TYSKLAND

SVINDELMAILS BRUGER KENDTE SALGSTEKNIKKER

VI KENDER DEM ALLE SAMMEN. DE FALSKE SPAMMAILS, DER ØNSKER TILLYKKE MED DEN STORE LOTTERIGEVINST ELLER TILBYDER EN "BUSINESS PROPOSAL", DER LYDER FOR GOD TIL AT VÆRE SAND. DE KALDES FOR NIGERIABREVE OG HAR FAKTISK EKSISTERET I MANGE ÅR. BAGMÆNDENE UDNYTTER PSYKOLOGISKE FAKTORER OG KENDTE SALGSKNEB, NÅR DE FORSØGER AT LOKKE FOLK I FÆLDEN.

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. Og det er ikke uden grund:

"*Bagmændene bag svindelmailene ved præcis, 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 professor doktor 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 begyndte 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 eksempelvis Uganda, Irak, Holland og USA.

Ud over 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 deres 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.

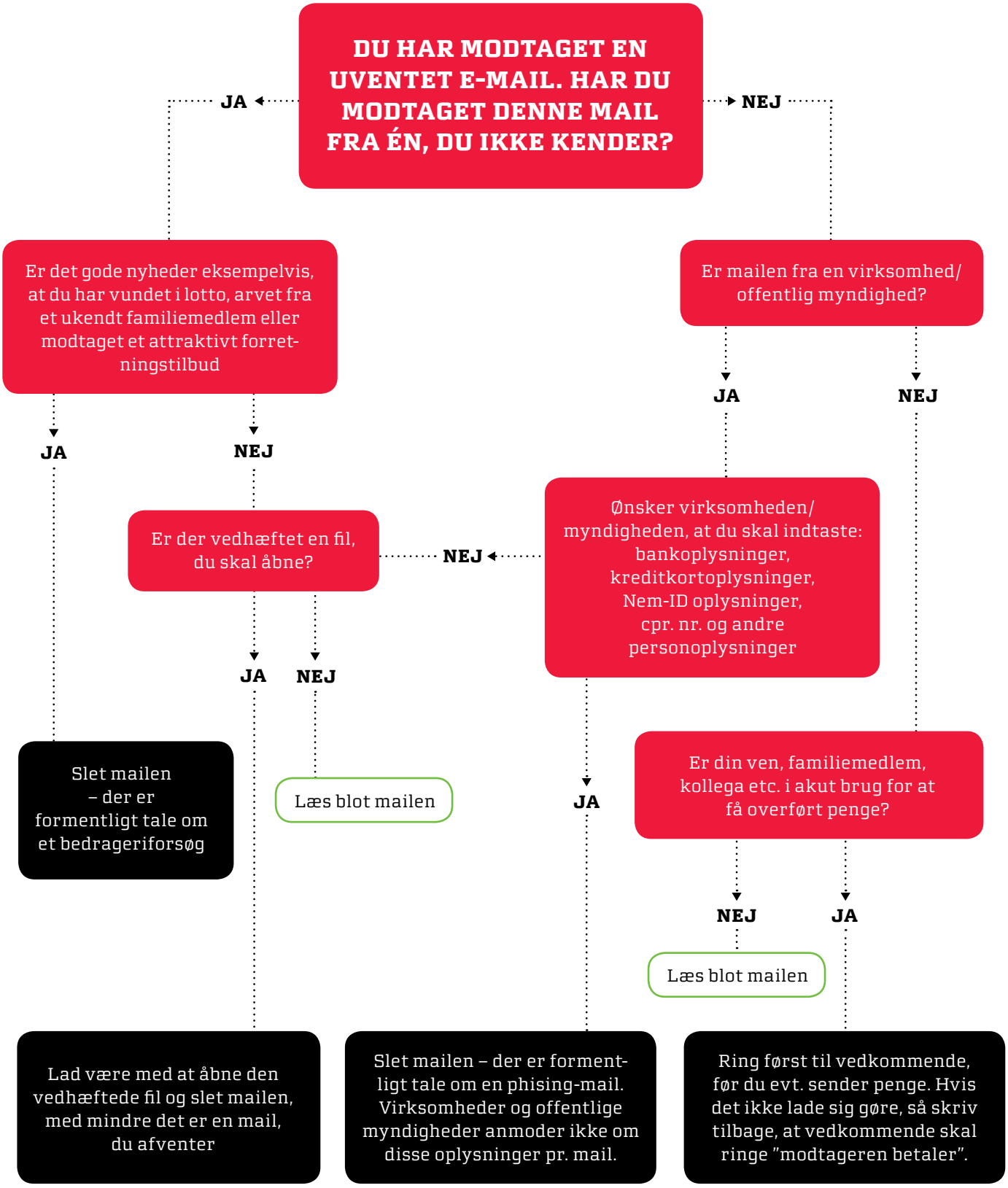
TRE TYPER OFRE

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 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.

Forskudsbedrageri er, når et offer narres til at betale forud for en ydelse. Det kan eksempelvis være et Nigeriabrev, hvor det potentielle offer anmodes om et lille pengebeløb til gengæld for senere at modtage en stor arv fra en ukendt person.

Kilde: Interviewet er tidligere bragt i Det Kriminalpræventive Råds publikation: Det Kriminalpræventive Råd (2015): Angreb og overgreb i cyberspace – hvordan forebygger vi det?

UNDGÅ PHISHING-MAILS



E-MÆRKET

UDENLANDSKE FUPBUTIKKER LOKKER DANSKERNE I KØBSFÆLDEN

IT-KRIMINELLE HAR FOR ALVOR FÅET ØJNENE OP FOR FALSKE WEBBUTIKKER SOM EN MÅDE AT BEDRAGE DANSKE FORBRUGERE PÅ. FUPBUTIKKERNE LIGNER TIL FORVEKSLING ALMINDELIGE WEBBUTIKKER, OG DERFOR HOPPER FLERE DANSKERE MED BEGGE BEN I KØBSFÆLDEN.

Mange danskere oplever, at varer, som er købt over nettet, aldrig bliver leveret, eller at varen, man modtager, er en ulovlig kopi. En af grundene er, at danskerne handler på nettet som aldrig før. Men en anden væsentlig årsag er, at der også er en kraftig stigning i antallet af falske webbutikker. Da e-mærket begyndte at interessere sig for disse fupbutikker i starten af 2011, kendte e-mærket til 10 fupbutikker. Siden da er tallet kun steget. I 2013 var tallet 750 butikker, og i dag er der over 1100 butikker.

De falske webbutikker ligner efterhånden de almindelige netbutikker til forveksling, og de bliver konstant bedre til at efterligne lovlydige butikker. Den seneste tendens er, at fupbutikkerne opkøber gamle domæner og bruger dem som snydeplatform. Hvor fupbutikkerne tidligere har heddet (og ofte stadig hedder) noget med eksempelvis "sko", "billig" og "Danmark", udnytter flere af fupmagerne troværdige brands.

SPOT EN FUPBUTIK

Det er både den erfarne og mindre erfarne online-shopper, der falder for fupbutikkernes tricks. Selvom det kan være svært at gennemskue fupbutikkerne, så er der nogle særlige kendertegn, man som forbruger kan være opmærksom på. En fupbutik tilbyder ofte kendte og populære varemærker til et godt stykke under normalprisen, og sproget på hjemmesiden bærer præg af at være oversat af en maskine. Derudover findes der sjældent kontaktoplysninger til virksomheden, og der bliver ikke svaret på de mails, man sender til netbutikken.

En effektiv måde at stoppe bedragerne på er ved at få lukket de falske hjemmesider. En vigtig kilde til at opdage mistænkelige netbutikker er forbrugerne, som både gør e-mærket og andre forbrugere opmærksomme på disse butikker. e-mærket har også indgået et samarbejde med Bagmandspolitiet (SØIK), hvor de løbende bliver orienteret om fupbutikker.

De danske og EU-baserede hjemmesider kan forholdsvis let lukkes af myndighederne. Politiet kan dog hverken lukke alle de falske butikker eller fange alle bagmændene. Særligt ikke dem, der befinder sig uden for Europas grænser. Og selv i de tilfælde, hvor en bagmand bliver dømt, er chancen for, at man som forbruger kan få sine penge retur ganske lille.

Den bedste måde at undgå at blive snydt på er derfor helt at undgå at handle i disse webbutikker. Her er der særligt fem råd, der kan hjælpe til at spotte en fupbutik.

TEST: KAN DU SPOTTE EN FUPBUTIK?

Du kan selv teste, hvor god du er til at spotte en fupbutik. e-mærket har i samarbejde med DR-Skole lavet et online undervisningsunivers, hvor du kan teste dine færdigheder.
Tag testen her: http://www.dr.dk/skole/samfundsfag/fup

1. SPROGFEJL
En typisk fupbutik er lavet af udenlandske svindlere. Derfor er sprog og priser oversat til dansk ved hjælp af maskiner. Det betyder, at fupbutikkerne er præget af dårligt dansk og åbenlyse grammatiske fejl.

2. SKÆVE PRISER
Valutaomregningsmaskiner runder hverken op eller ned, så velkendte danske priser som 299 kroner eller 749 kroner er en sjældenhed på fupbutikkerne. I stedet er priserne skæve som for eksempel 243,67 kroner.

3. ALLE VARER ER PÅ TILBUD
Fupbutikker elsker tilbud. Ikke nok med at de typisk sælger verdenskendte mærkevarer som Burberry, Mulberry, Nike og Marc Jacobs til priser langt under, hvad man normalt betaler for den ægte vare. De har også tilbud på alle varer.

4. INGEN ADRESSE, TELEFONNUMMER ELLER E-MAIL
Det er svært at kontakte en fupbutik. Som regel skriver de ikke deres fysiske adresse, og det er heller ikke muligt at ringe til dem, fordi nummeret ikke er oplyst. Af og til er der en e-mailadresse, men typisk er det en fra en gratis mailadressehjemmeside som hotmail eller gmail.

5. FULD AF TILLIDSSKABENDE LOGOER
Fupbutikkerne er glade for at vise, at de er til at stole på, derfor bruger de ofte rigtig mange både velkendte og ukendte logoer for at skabe troværdighed.

HVAD ER E-MÆRKET

e-mærket er den danske certificeringsordning, der arbejder for tillidsfuld e-handel mellem kunder og erhvervsdrivende. Med e-mærket er du som kunde dækket af en køberbeskyttelse med en økonomisk sikring på op til 10.000 kroner per handel, og samtidig bliver den erhvervsdrivende løbende kvalitetssikret af e-mærkets jurister, så du er sikret en tryg og gennemskuelig e-handel.

e-mærket er en nonprofit organisation stiftet i 2000 af Forbrugerrådet Tænk, Dansk Erhverv, DI, FDIH, Finansrådet, Dansk IT og HK.

NÅR FORBRYDELSER BLIVER DIGITALE
HACKING

7

Kapitel 3

HACKING

HACKER-FORBRYDELSER

FORETAGER MAN EN INTERNETSØGNING PÅ ORDET CYBERCRIME, ER RESULTATET OFTE ET BILLEDE AF EN HÆTTEKLÆDT PERSON, DER SIDDER FORAN EN COMPUTERSKÆRM. IT-KRIMINALITET OG HACKING ER DA OGSÅ TO BEGREBER, SOM ULØSELIGT ER BUNDET SAMMEN.

Hacking var ikke fra begyndelsen associeret med noget negativt, men var derimod oprindeligt forbundet med computerentusiaster omkring Massachusetts Institute of Technology (MIT) i USA i 1960'erne, som var i stand til at opfinde nytænkende løsninger på tekniske problemer. Forbrydelserne var i begyndelsen også af relativ beskeden karakter som eksempelvis at sikre sig adgang til gratis telefonering. I takt med, at samfundet er blevet mere og mere digitaliseret, og computere er blevet netværksforbundne, er den skade, hackere kan begå, også blevet større. Hacking sker dog på daglig basis og er i dag blevet en milliardstor undergrundsindustri, hvor kriminelle hackere kan sælge deres evner som kommercielle tjenesteydelser. Hacking anvendes også i vidt omfang i forbindelse med industrispionage samt af stater som en del af en forsvars- og efterretningsvirksomhed.

HVAD ER HACKING?

Den almindelige forståelse af hacking er i dag den proces, hvor en person (hackeren) skaffer sig uberettiget adgang til et informationssystem. Med en sammenligning fra den analoge verden er der således tale om et indbrud i et computersystem, hvor de IT-kriminelle typisk enten stjæler information eller udøver hærværk på computeren eller netværket. Metoderne kan variere fra det helt simple, hvor hackerne gætter kodeord til ultraavancerede og målrettede angreb, som udføres af stater.

Hacking fungerer typisk ved, at hackeren identificerer og udnytter sikkerhedshuller til at skaffe sig adgang til et computersystem. Et simpelt eksempel på et sådan sikkerhedshul kan være, når det er muligt gentagende gange at indtaste et forkert kodeord, uden at den pågældende konto bliver spærret. Det gør det muligt at gætte kodeordet, hvis man kører et program, som automatisk afprøver alle ord i retskrivningsordbogen. Dette er netop årsagen til, at det anbefales, at kodeord indeholder andre tegn end blot bogstaver.

En vigtig del af det at udføre et hackerangreb er derfor at kunne lokalisere sikkerhedshuller og sårbarheder både i computersystemer, men også i sikkerhedsrutiner, som efterfølgende vil kunne blive udnyttet. Typisk vil en hacker anvende forskellige tekniske programmer, der gør ham/hende i stand til at lokalisere og identificere sikkerhedshuller. De dygtigste hackere er selv i stand til at udvikle de nødvendige hjælpeværktøjer, hvor de mindre dygtige bliver nødt til at få hjælp af andre eller kopiere teknikker eller værktøjer. Hacking kræver dog ofte også en mere manuel tilgang, hvor hackeren er nødt til at prøve sig frem. I mange tilfælde er hacking derfor en lang og tidskrævende proces, som ofte kræver solide tekniske færdigheder, tålmodighed og vedholdenhed.

Da hackere typisk har stor viden om, hvordan computersystemer og netværk fungerer, kan de også begå andre former for kriminalitet, som ikke indebærer, at de skaffer sig adgang til computersystemer. For tiden er der særligt to typer af cyberangreb, som forvolder store tab for virksomheder og personer. De såkaldte DDos angreb og Ransomware.

DDos-angreb er en betegnelse for en ondsindet metode til at overbelaste en hjemmeside, så den ikke virker. DDos-angreb udføres ved, at en person, som kontrollerer en masse computere, får dem alle til på én gang og i én uendelighed at forespørge den samme internetadresse med det resultat, at ingen andre kan komme i forbindelse med hjemmesiden.

Ransomware er en form for virus, der gør skade på den inficerede computer ved at kryptere og dermed spærre brugerens data. Herefter modtager offeret en meddelelse om, at vedkommende kun kan få sine data frigjort, hvis vedkommende betaler en løsesum (løsesum = ransom).

DEN SOCIALE SIDE AF HACKING

I mange tilfælde kan det være lettere at skaffe sig adgang til en computer eller et netværk ved at få oplyst et kodeord frem for at gætte det. Denne side af hacking er også kendt som social engineering, der ofte handler om, at hackeren udgiver sig for at være en anden, end han/hun egentlig er, og formår at overbevise/manipulere medarbejdere til at oplyse centrale informationer (så som kodeord eller sikkerhedsindstillinger) eller ligefrem skaffer sig fysisk adgang til en virksomhed. Hackeren kan eksempelvis udgive sig for at være virksomhedens IT-udbyder, en samarbejdspartner eller noget helt tredje. Nogle gange går hackeren efter en tilfældig medarbejder, men andre gange ligger der en omfattende research forud for, at en virksomhed kontaktes, hvor hackeren eksempelvis går målrettet efter medarbejdere med indsigt i virksomhedens IT-systemer. Forestillingen om den asociale hætteklædte hacker, der arbejder isoleret i et mørkt rum, er derfor noget forsimplet.

HACKING SOM EN SUBKULTUR

Umiddelbart kan det lyde som en underlig beskæftigelse at forsøge at bryde ind i computersystemer. Hacking er dog ikke blot et håndværk, men er også en subkultur med egne regler, etik og historie. Der findes talrige udgivelser om hackeretikken, men særligt bogen Hackers - Heroes of the Computer Revolution af Steven Levy fra 1984 har haft en særlig betydning for hackermiljøet på grund af dens dogmer for hacking, der blandt andet knytter sig til fri informationsadgang.

I en andet kendt værk fra 1986 – det såkaldte *hacker manifesto* - fremgår kontrasten mellem samfundets opfattelse af hackere som kriminelle og hackernes egne selvopfattelser som personer drevet af søgen efter viden.
"*We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals*" (*The Hacker's Manifesto*).

Mange hackere anser sig altså ikke som kriminelle, men tager udgangspunkt i den grundlæggende idé om total informationsfrihed og mener, at deres handlinger skal ses som en måde til at forstå verden bedre på. Faktum er dog, at mange hackere udnytter deres evner udelukkende for at begå kriminelle handlinger, hvorfor hackerne traditionelt også er blevet opdelt i to arketyper: Hackere med gode intentioner (som eksempelvis at afsløre sikkerhedshuller i systemer) og hackere med kriminelle motiver (hærværk, økonomisk gevinst med videre), også kaldet *White Hats* og *Black Hats*.

Fælles for begge typer af hackere er, at de anvender de samme metoder og tekniker. Derfor bliver hacking som en kriminalitetsforebyggende metode også mere og mere anvendt. I dag tilbyder mange virksomheder en dusør til hackere, som er i stand til at finde sårbarheder, så de kan lukkes, inden hackere med kriminelle hensigter finder dem.

Kilder
Kruize, Peter (2013): Kriminalitet i en digitaliseret verden, Københavns Universitet.
Meinel, Carolyn (2006): "How Do Hackers Break Into Computers?", i: Bernadette Schell & Clemens Martin (eds.) Webster's New World Hacker Dictionary, Indianapolis: Wiley Publishing, Inc., s. 373-380.
Peikari, Cyrus & Seth Fogie (2004): Maximum Wireless Security, uddrag bragt af Computerworld (http://www.computerworld.com/article/2563639/mobile-wireless/wireless-hacking-techniques.html).
The Mentor (1986): The Hacker's Manifesto (https://www.usc.edu/~douglast/202/lecture23/manifesto.html)

THOMAS LUND-SØRENSEN, CHEF FOR CENTER FOR CYBERSIKKERHED,
FORSVARETS EFTERRETNINGSTJENESTE

CYBERSPIONAGE:

EN KONSTANT TRUSSEL FOR VIRKSOMHEDER OG MYNDIGHEDER

FREMMEDE EFTERRETNINGSTJENESTER, STATSSTØTTEDE GRUPPER OG ENKELTPERSONER BRUGER I STIGENDE GRAD INTERNETTET TIL AT SPIONERE MOD DANMARK. DE FORSØGER AT AFDÆKKE VIGTIGE IT-SYSTEMER OG STJÆLE VIDEN. DET STILLER STORE KRAV TIL SIKKERHEDSFORANSTALTNINGER OG BEREDSKAB.

Forsvarets Efterretningstjeneste skriver i risikovurderingen for 2015: "*Spionage mod offentlige myndigheder og virksomheder udgør fortsat den alvorligste cybertrussel mod Danmark og danske interesser. Spionagen udføres primært af statslige og statsstøttede grupper. Gennem de seneste år er omfanget af cyberspionage mod Danmark steget betydeligt, og gruppernes metoder og teknikker er blevet mere avancerede. Truslen fra cyberspionage mod danske myndigheder og virksomheder er meget høj.*"

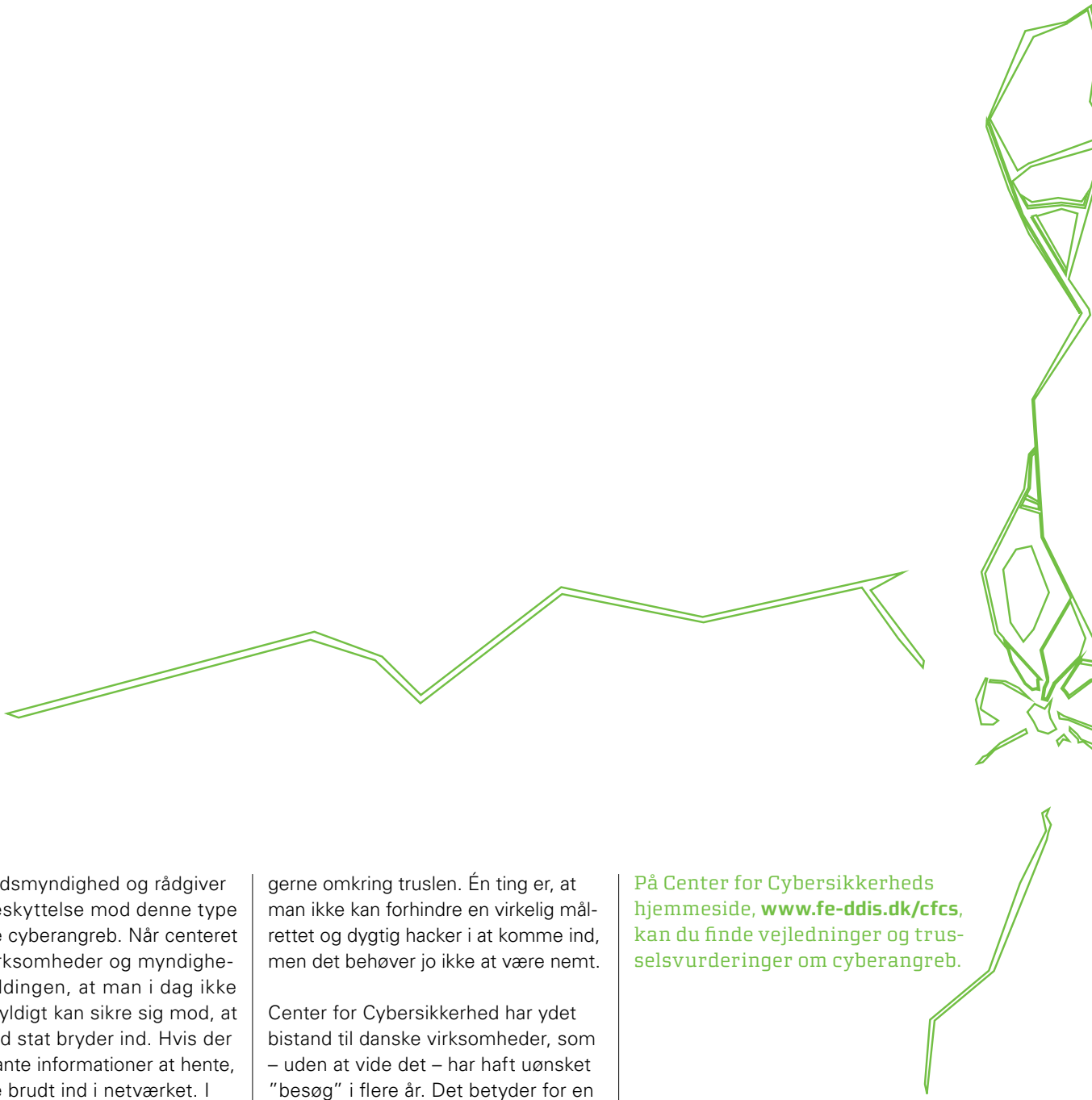
Man kan spørge sig selv, hvorfor truslen skulle være særlig alvorlig nu, når truslen for spionage mod højteknologiske virksomheder har eksisteret i mange år. Men muligheden for at anvende internettet til spionage har gjort det lettere og samtidigt mindre risikofyldt at stjæle information. Det er de færreste virksomheder – danske såvel som udenlandske – som kan beskytte sig effektivt mod angreb fra andre stater, og endnu færre, der er i stand til at erkende i tide, at et angreb finder sted. Det skyldes blandt andet, at det er lettere at være angriber end forsvarer på internettet.

En virksomhed skal til enhver tid kunne beskytte alle systemer, som den har forbundet til internettet. Alle systemer skal være opdaterede og robuste over for angreb, og netværkene skal være sikrede mod misbrug eller ulovlig indtrængen. Virksomheder kan have tusindvis af computere og mobile enheder på netværket, der alle skal forsvares. Virksomheden skal have personer og processer på plads, der sikrer, at netværk og systemer er robuste og opdaterede. Angriberen skal kun finde én fejl eller svaghed for at få fodfæste i virksomheden. Én computer, der ikke er opdateret, ét program, der ikke er opdateret, eller én bruger, som klikker på et link, der medfører, at angriberen uset installerer en bagdør, som lukker angriberen ind i netværket.

KENDSKAB TIL EGEN RISIKOPROFIL ER NØDVENDIG

Forsvarets Efterretningstjenestes Center for Cybersikkerhed er den nationale

I dag skal en virksomhed fokusere på at erkende, at der er indbrud i gang, og succeskriteriet bliver at minimere den tid, det tager fra, at et angreb erkendes, til angriberen er fjernet fra netværket igen.



IT-sikkerhedsmyndighed og rådgiver omkring beskyttelse mod denne type avancerede cyberangreb. Når centeret rådgiver virksomheder og myndigheder, er meldingen, at man i dag ikke selv endegyldigt kan sikre sig mod, at en fremmed stat bryder ind. Hvis der er interessante informationer at hente, vil der blive brudt ind i netværket. I dag skal en virksomhed fokusere på at erkende, at der er indbrud i gang, og succeskriteriet bliver at minimere den tid, det tager fra, at et angreb erkendes, til angriberen er fjernet fra netværket igen. Beskyttelse mod denne type angreb handler ikke om at købe endnu et stykke teknologi. Beskyttelse opnås primært ved at have et stærkt ledelsesfokus, at have dygtige medarbejdere ansat, som forstår truslen, og ved, hvordan virksomhedens aktiver skal beskyttes.

Derudover skal virksomheden kende sin egen risikoprofil i forhold til truslen, robustheden af IT-infrastrukturen og graden af opmærksomhed hos brugerne omkring truslen. Én ting er, at man ikke kan forhindre en virkelig målrettet og dygtig hacker i at komme ind, men det behøver jo ikke at være nemt.

Center for Cybersikkerhed har ydet bistand til danske virksomheder, som – uden at vide det – har haft uønsket "besøg" i flere år. Det betyder for en virksomhed, at angriberen har kunnet læse med i alle udviklingsplaner, ordrer og regnskaber. Centeret har også set virksomheder, der har bekæmpet, hvad de troede var gængse cyberangreb, uden at erkende, at de mange og hyppige cyber-angreb var et udtryk for, at der var uønsket besøg i deres netværk.

TO TYPER CYBERSPIONAGE TRUER

I 2014 udgav Center for Cybersikkerhed en risikovurdering om truslen fra avancerede angreb. Af den fremgår det, at et antal danske virksomheder, herunder virksomheder af betydelig størrelse og betydning for Danmark, har været udsat for denne avancerede type angreb. Cyberspionage er altså ikke kun en risiko for naboen. Alene i 2014 håndterede centeret konkret 585 cybersikkerhedshændelser blandt centerets civile og militære kunder.

På Center for Cybersikkerheds hjemmeside, **www.fe-ddis.dk/cfcs**, kan du finde vejledninger og trusselsvurderinger om cyberangreb.

Der er typisk to måder, en virksomhed bliver angrebet på ved cyberspionage. Der kan være tale om et såkaldt "spear phishing"-angreb, som er et målrettet angreb mod enkeltindivider i virksomheden. Det kan eksempelvis være systemadministratoren eller en chef, som modtager og åbner en mail, der både virker relevant, overbevisende og tillidsvækkende. Men der er tale om en forfalsket mail, der indeholder et link til

SIKRINGSTILTAG	MEDARBEJDER-MODSTAND	ETABLERINGS-OMKOSTNINGER	DRIFTS-OMKOSTNINGER
Udarbejd positivliste over applikationer af godkendte programmer for at forhindre kørsel af ondsindet eller uønsket software	**MEDIUM**	**HØJ**	**MEDIUM**
Opdatér programmer, for eksempel Adobe Reader, Microsoft Office, Flash Player og Java, med seneste sikkerhedsopdateringer, højrisiko inden for to dage	**LAV**	**LAV**	**HØJ**
Opdatér operativsystemet med seneste sikkerhedsopdateringer, højrisiko inden for to dage. Undgå Windows XP eller tidligere	**LAV**	**MEDIUM**	**MEDIUM**
Begræns antallet af brugerkonti med domæne- eller lokaladministrator-privilegier. Disse brugere bør anvende separate uprivilegerede konti til email og websurfing	**MEDIUM**	**MEDIUM**	**LAV**

en skadelig kode eller en vedhæftet fil med en skadelig kode. Ved klik på link eller fil installeres et skadeligt program på brugerens computer, som angriberen anvender til at få yderligere fodfæste i virksomhedens netværk.

Der kan også være tale om et såkaldt "watering hole"-angreb, hvor en bruger besøger en legitim hjemmeside, for eksempel tilhørende en tænketank, inden for et relevant fagområde. Den legitime hjemmeside er inficeret med en skadelig kode, der eksekveres, hvis IP-adressen på den besøgende bruger tilhører den "rigtige" virksomhed. Andre besøgende på hjemmesiden modtager intet unormalt. Som ved "spear phishing"-angreb installeres en skadelig kode på computeren, men i dette tilfælde skal brugeren normalt ikke klikke på et link for at blive inficeret. Det er tilstrækkeligt blot at besøge hjemmesiden.

Center for Cybersikkerhed har set begge angrebsmetoder anvendt mod både danske virksomheder og offentlige myndigheder. Den gode nyhed er dog, at ikke alle angreb lykkes.

SIKKERHEDSTILTAG SKAL BESKYTTE VIRKSOMHEDEN

Selv om det ikke er muligt at gardere sig 100% mod angreb, så kan man som virksomhed komme langt med at beskytte sig med en række tiltag.

Det første skridt er at implementere nedenstående "top fire"- sikkerhedstiltag. Hvis disse implementeres, reducerer man sandsynligheden for, at angreb lykkes med op til 80%.

Når angriberne forsøger at finde svagheder i forsvaret, går de også efter de lette mål, for eksempel programmer, der ikke er opdaterede med de seneste rettelser. Således har Center for Cybersikkerhed observeret, at angriberne forsøgte at komme ind i en myndighed ved at udnytte en to år gammel sårbarhed, der – i det konkrete tilfælde – var rettet hos myndigheden, hvorfor angrebet ikke lykkedes. I et andet tilfælde, som centeret observerede, var der tale om, at en sårbarhed var til stede, men angrebet mislykkedes, da den ramte bruger ikke havde administrative rettigheder på compute-

DESIGNET TIL AT FORHINDRE ELLER DETEKTERE	DESIGNET TIL AT HJÆLPE MED AT MODVIRKE ANGREBSFASE 1	HJÆLPER MED AT MODVIRKE ANGREBSFASE 2	HJÆLPER MED AT MODVIRKE ANGREBSFASE 3
BEGGE	JA	JA	JA
FORHINDRE	JA	MULIGT	NEJ
FORHINDRE	JA	MULIGT	MULIGT
FORHINDRE	MULIGT	JA	MULIGT

Fra vejledningen: "Cyberforsvar der virker".

ren, hvorfor den skadelige kode ikke kunne installeres.

Eksemplerne illustrerer, hvorfor ovennævnte basale tiltag medvirker til at beskytte virksomheden mod angreb. Der er tale om tiltag, som enhver virksomhed bør kunne gennemføre i dag, så det er bare om at komme i gang.

Center for Cybersikkerhed har udgivet en vejledning, som beskriver, hvordan en virksomhed kan nedbringe sandsynligheden for, at et angreb lykkes. Vejledningen "Cyberforsvar der virker" kan hentes på Center for Cybersikkerheds hjemmeside.

CENTER FOR CYBERSIKKERHED

Center for Cybersikkerheds hovedopgave er at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af. Centeret opdager cyberspionage enten via centerets Netsikkerhedstjeneste eller via et tip fra samarbejdspartnere. Samfundsvigtige virksomheder kan efter anmodning tilsluttes Netsikkerhedstjenesten og dermed opnå bedre beskyttelse mod avancerede angreb. Du kan læse mere om centeret og vores opgaver på www.feddis.dk/cfcs

HVORDAN KAN DANSKE VIRKSOMHEDER RUSTE SIG TIL FREMTIDENS IT-KRIMINALITET?

DET ER AFGØRENDE, AT MAN SOM VIRKSOMHED ER FORBEREDT PÅ EVENTUELLE IT-ANGREB. BÅDE FOR AT KUNNE REAGERE HENSIGTSMÆSSIGT, HVIS MAN BLIVER RAMT, MEN OGSÅ FOR AT FOREBYGGE. HELDIGVIS ER DER ER GODE RÅD AT HENTE FOR VIRKSOMHEDER, DER ØNSKER AT RUSTE SIG TIL FREMTIDENS UDFORDRINGER INDEN FOR IT-KRIMINALITET.

Ifølge Rigspolitiets Nationale Center for Cyber Crime (NC3) har ni ud af ti danske virksomheder haft uautoriseret besøg i deres IT-systemer. Tallet beror på en kvalitativ vurdering, fordi man hos politiet arbejder med et betydeligt mørketal. Mange danske virksomheder melder nemlig ikke hackerangreb til politiet, fordi man ikke er interesseret i at udstille sine sårbarheder, i frygt for at forbrugere og offentlighed vender ryggen til, hvis IT-sikkerheden og dertilhørende personlige data er i risiko for at blive kompromitteret. Stigmatisering er en betydelig udfordring for fremtidens IT-sikkerhed, fordi det skaber en barriere for dialog mellem politi og erhvervsliv.

For at komme denne stigmatisering til livs efterspørger flere brancheforeninger, at der etableres enkel og nem anmeldelse af IT-kriminalitet til politiet, ligesom det også bør overvejes, hvorvidt nogle anmeldelser kan forblive anonyme. Fraværet af anmeldelser er en udfordring for politiet, da mørketallet hindrer videndeling og hermed forebyggelse. Stigmatiseringen bliver derfor ikke kun en barriere, men også en negativ spiral. Det er formentlig umuligt helt at undgå, at virksomheder bliver ramt af malware med videre, men hurtig videndeling mellem politi og virksomheder om potentielle trusler er alfa og omega i forhold til at forebygge, at andre virksomheder bliver ramt af IT-kriminalitet.

Foruden stigmatisering skal danske virksomheder ofte mestre en svær balance, når det kommer til IT-sikkerhed. På den ene side stilles der store eksterne krav fra kunder og myndigheder om brugervenlighed og sikkerhed, hvor det ofte kan være vanskeligt at fremme det ene, uden at det sker på bekostning af det andet. På den

anden side sættes der også store interne krav dels om en høj grad af beskyttelse af virksomhedens vitale data og dels om sorte tal på bundlinjen. De mange forskellige krav kan gøre det svært at finde den rette balance mellem for meget og for lidt IT-sikkerhed, fordi begge situationer kan vise sig at være en dyr affære. Med den stigende digitalisering vil kravene og kompleksiteten af disse afvejninger kun højnes, og det er derfor nødvendigt, at IT-sikkerhed ikke udelukkende varetages af IT-medarbejdere, men også bliver et ledelsesansvar.

GODT PÅ VEJ MOD BEDRE IT-SIKKERHED I SMÅ OG MELLEMSTORE VIRKSOMHEDER

IT-sikkerhed kan være en udfordring for særligt små og mellemstore virksomheder, fordi de ofte ikke har de nødvendige kompetencer og ressourcer. Disse virksomheders sårbarhed kan dog forebygges ved at implementere en række IT-sikkerhedsinitiativer. Et vigtigt element er at tænke IT-sikkerhed hele vejen rundt: Det starter og slutter ikke kun i teknologi, men går fra medarbejderadfærd over ledelsesstrategi til teknologi og proces.

10 TILTAG, DER FORBEDRER VIRKSOMHEDENS IT-SIKKERHED

Opdater software

IT-sikkerhed er en kontinuerlig proces, og et overblik over, hvilke typer software virksomheden er i besiddelse af, er vigtigt. Det indebærer også, at der udvikles en rutine, som sikrer, at virksomheden er informeret om, hvornår der offentliggøres nye trusler og IT-sikkerhedsbaserede opdateringer til software.

Tænk i IT-sikkerhed som et ledelsesansvar

Implementer IT-sikkerhed som en ledelsesopgave frem for udelukkende at placere det ved en IT-medarbejder. På den måde er ledelsen med til at minimere omkostninger, der kan opstå i forbindelse med IT-sikkerhedshændelser, mens du løbende kan investere i IT-sikkerhed. På den måde kan ledelsen også være med til at sikre, at virksomheden føres videre, hvis uheldet er ude.

Lav en overordnet IT-politik

Sørg for at lave en IT-sikkerhedspolitik i samarbejde med den personaleansvarlige og IT-ansvarlige for at sikre, at de ressourcer virksomheden bruger på IT, anvendes optimalt.

Foretag backup

Det er umuligt at forhindre, at angreb på eller tab af data sker. Derfor bør virksomheden tage backup af alle data og systemer på en struktureret måde.

Identificer IT-aktiver og vurdér risici

Data og informationer er aktiver, og derfor skal deres værdi estimeres på samme måde som virksomhedens andre aktiver. Det vil gøre virksomheden i stand til at vurdere de økonomiske konsekvenser ved et eventuelt IT-angreb. På denne måde kan virksomheden kortlægge, hvordan den er afhængig af IT-aktiver, og udarbejde en plan for, hvordan den beskyttes for fremtiden.

Invester i anti-virussoftware

En af de trusler, der historisk har voldt mest skade på IT-systemer, er udbredelsen af virus, og mængden af virus er eksplosivt stigende. Sørg for at investere i virusprogrammer, som kan passivisere vira og fange andre skadelige programmer som orme og trojanske heste.

Anvend en firewall

Når virksomheden kommunikerer elektronisk med omverdenen, indebærer det også, at omverdenen kan kommunikere ind i virksomheden. Anvend en firewall til at lukke de porte, som du ikke ønsker at kommunikere igennem.

Skab en IT-sikkerheds-kultur

En IT-sikkerhedskultur blandt medarbejderne fremmes gennem uddannelse og opmærksomhedsskabende initiativer. Virksomheden har en IT-sikkerhedskultur, når medarbejderne tænker og opfører sig på måder, der tager højde for IT-sikkerheden.

Læs virksomhedens logfiler

Virksomhedens IT-systemer generer en række logfiler for en række forskellige computere og netværk. Med disse informationer kan man se, om virksomheden er udsat for forsøg på uvedkommende indtrængning, og dermed kan man tage de forebyggelsesmæssige forholdsregler. Denne viden kan spare virksomheden for mange penge.

Udnævn en IT-ansvarlig i virksomheden

Ved at gøre dette kan ledelsen gennem én person sikre, at IT-sikkerhedspolitikken føres ud i livet i overensstemmelse med forretningsstrategien.

Kilder:
Dansk Industri, Dansk Erhverv og Rådet for Digital Sikkerhed (2015, 11. november): Fælles brancheoplæg om bekæmpelse af cybercrime, oplæg ved National Cyber Crime Konference, Rigspolitiets Nationale Cyber Crime Center (NC3).
Dansk Industri, ITEK og Ministeriet for Videnskab, Teknologi og Udvikling (2015): De ti vigtigste IT-sikkerhedsinitiativer – en kortfattet guide for mindre og mellemstore virksomheder.
Stark, Felix Bakkergaard (2015, 28. oktober): Ni ud af 10 danske virksomheder har været hacket, DI Business.
Theede, Rasmus (2015, 11. november): Sikkerhed i Balance, oplæg ved National Cyber Crime Konference, Rigspolitiets Nationale Cyber Crime Center (NC3).
De 10 gode råd til IT-sikkerhedsinitiativer er adapteret fra Dansk Industri, ITEK og Ministeriet for Videnskab, Teknologi og Udvikling (2015): De ti vigtigste IT-sikkerhedsinitiativer – en kortfattet guide for mindre og mellemstore virksomheder.

INTERVIEW MED RAOUL CHIESA, RÅDGIVER FOR FN

HACKER-BEGREBET SPÆNDER VIDT

NUTIDENS HACKERE ER IKKE BARE DIGITALE DRENGERØVE. DE ER SOFISTIKEREDE, 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 blandt andet rådgiver for UNICRI, som er FN's tværregionale researchinstitut for kriminalitet og lovgivning.

I FN har han blandt andet 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 for eksempel samarbejdede med myndighederne om 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 for eksempel 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.

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 blandt andet rådgiver for UNICRI, som er FN's tværregionale researchinstitut for kriminalitet og lovgivning og forfatter til bogen: Profiling Hackers.

Raoul Chiesa var blandt oplægsholderne på Den Kriminalpræventive Dag 2015.

MILLIARDDOLLAR INDUSTRI

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

"*Det er en milliarddollar industri, 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 sporet. 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.

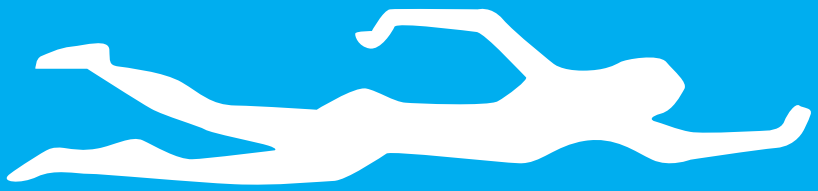
De kriminelle aktiviteter på nettet spænder lige fra bedrageri, identitetstyveri, afpresning, falske hjemmesider og angreb på offentlige og private virksomheders computersystemer til cyberkrigsførelse, hvor en nationalstat trænger ind på en anden nationalstats computernetværk for for eksempel at spionere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

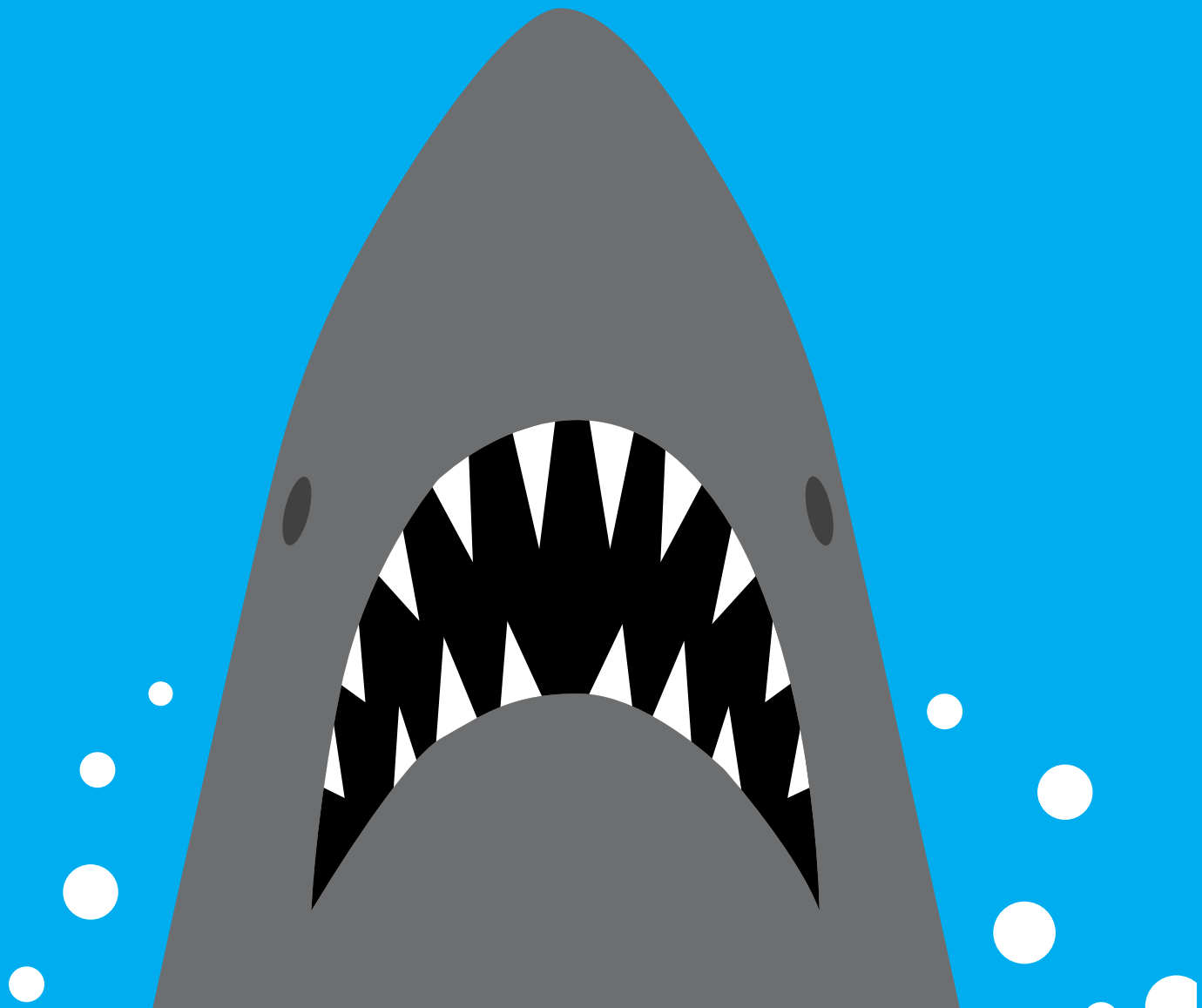
DEN AFSKRÆKKENDE EFFEKT VED LOVGIVNING, DOMME OG TEKNISKE FORHINDRINGER

KATEGORI	BESKRIVELSE	LOVGIVNING	DOMME FOR ANDRE HACKERE	EGEN DOM	TEKNISKE FORHINDRINGER
"SCRIPT-KIDDIE"	Script kids interesserer sig primært for resultaterne af deres angreb og har hverken den nødvendige viden eller lyst til at lære egentlige hacker-tekniker. De anvender derfor software og hackerværktøjer udviklet af andre frem for selv at udvikle og finde løsninger.	**INGEN BETYDNING**	**INGEN BETYDNING**	**HØJ – STOPPER VED FØRSTE DOM**	**STOR BETYDNING**
"CRACKER"	Udtrykket "cracker" bliver brugt om hackere, som finder glæde ved at gøre skade på IT-systemer og som i modsætning til script kids har egentlige hackerevner.	**INGEN BETYDNING**	**INGEN BETYDNING**	**INGEN BETYDNING**	**MODERAT BETYDNING**
"DEN ETISKE HACKER"	Den etiske hacker er motiveret af den intellektuelle udfordring ved at finde fejl og svagheder i IT-systemer med videre. Denne viden dokumenteres og deles ofte med henblik på at øge sikkerheden frem for at misbruge sikkerhedshullerne.	**INGEN BETYDNING**	**INGEN BETYDNING**	**HØJ – STOPPER VED FØRSTE DOM**	**INGEN BETYDNING**
"DEN STILLE, PARANOIDE OG DYGTIGE (SPD) HACKER"	Den stille og paranoide hacker har mange lighedstræk med den etiske hacker, men er langt mere forsigtig. Den væsentligste forskel er, at SPD-hackeren ikke deler sin viden til gavn for andre.	**INGEN BETYDNING**	**INGEN BETYDNING**	**INGEN BETYDNING**	**INGEN – DET ER DERES PROFESSION**
"CYBER-KRIGEREN"	Cyber-krigeren sælger sin ydelse til højestbydende. Motivationen er penge eller idealer. Cyber-krigeren foretrækker at holde lav profil og angriber sjældent spektakulære mål som virksomheder, men foretrækker mindre mål.	**INGEN BETYDNING**	**INGEN BETYDNING**	**INGEN BETYDNING**	**INGEN – DET ER DERES PROFESSION**
"INDUSTRI-SPIONEN"	Industrispionen udnytter den moderne informationsteknologi til at stjæle virksomhedshemmeligheder frem for at udsmugle mikrofilm og kopiere sagsakter.	**INGEN BETYDNING**	**INGEN BETYDNING**	**INGEN BETYDNING**	**INGEN BETYDNING**
"MYNDIGHEDS-HACKEREN"	Myndighedshackeren arbejder med spionage, kontraspionage, overvågning af andre stater, enkeltpersoner, terroristgrupper samt vital infrastruktur (for eksempel el, vand og varme).	**N/A**	**N/A**	**N/A**	**N/A**

Kilde:
Chiesa, Raoul, Ducci, Stefania og Ciappi, Silvio, "Table C3: Deterrent Effect of Laws, Sentences, and Technical Difficulties" samt side 52-56, Profiling Hackers The Science of Criminal Profiling as Applied to The World of Hacking, Auerbach Publications, 2009
Interviewet er tidligere bragt i Det Kriminalpræventive Råds publikation: Det Kriminalpræventive Råd (2015): Angreb og overgreb i cyberspace - hvordan forebygger vi det?

NÅR FORBRYDELSER BLIVER DIGITALE
BØRN OG UNGE PÅ NETTET





Kapitel 4

BØRN OG UNGE PÅ NETTET

ANDREAS GRUBBE KIRKELUND, BØRNERÅDET

MOBNING I DEN VIRTUELLE VIRKELIGHED – OG VOKSNES ANSVAR

KRÆNKENDE ELLER SÅRENDE INDHOLD PÅ DE SOCIALE MEDIER ER ET VELKENDT FÆNOMEN FOR MANGE UNGE. OG DEN DIGITALE MOBNING OPLEVES OFTE EKSTRA VOLDSOMT, FORDI DEN KAN VÆRE SVÆR AT SLIPPE VÆK FRA. DERFOR BØR VOKSNE I HØJERE GRAD INTERESSERE SIG FOR BØRN OG UNGES ONLINE-TRIVSEL – OGSÅ SELVOM DE NYE PLATFORME KAN VIRKE SVÆRT TILGÆNGELIGE.

Børn og unge er online som aldrig før. Stort set alle unge er udstyret med en smartphone og har adgang til nettets mangfoldigheder døgnet rundt. Rigtig mange – ikke kun unge – tjekker deres telefon som det første, når de vågner, og som det sidste, inden de falder i søvn. En undersøgelse, som Børnerådet har lavet, viser, at næsten en tredjedel af de unge i 7. klasse er online i mere end fire timer dagligt. Og der er al mulig grund til at tro, at det tal ikke har toppet endnu.

Som udgangspunkt er der intet galt med at være meget på nettet. Her kan børn og unge søge viden, stille deres nysgerrighed og blive underholdt på en måde, som tidligere generationer ikke engang kunne drømme om. Mulighederne på nettet kan bidrage til deres udvikling og give dem platforme for kreative udfoldelser, som er helt nye – og måske kan være svære at forstå og tage del i for generationerne før.

Nettet giver også børn og unge andre måder at danne fællesskaber på. Særlige interesser kan dyrkes på et helt andet niveau, fordi der altid kan findes ligesindede med samme interesser. Børn og unge kan være legekammerater, venner og spille-makkere, selvom de sidder i hver deres ende af landet - eller verden.

De nye medier understøtter altså fællesskaber, venskaber, kreativitet og inspiration – men samtidig er de også enestående "gode" platforme for mobning. Præcis som med alle de positive ting, nettet kan være med til at fremme og styrke, bliver mobning på nettet af en anden potens, end børn og unge tidligere har oplevet. På nettet bliver mobning forstærket, ukontrolleret og permanent tilgængeligt. Mobning er ikke længere lokalt. Det har et globalt ekko. Og så kan det være helt anonymt.

På nettet kan alting være tilgængeligt hele tiden – og det forsvinder ikke af sig selv. Hvis man vil slippe væk fra det, så er man samtidig tvunget til at melde sig helt ud af fællesskabet – både det virtuelle, men også nogle gange det fysiske. Blandt andet derfor oplever børn og unge mobning på nettet som noget meget voldsomt.

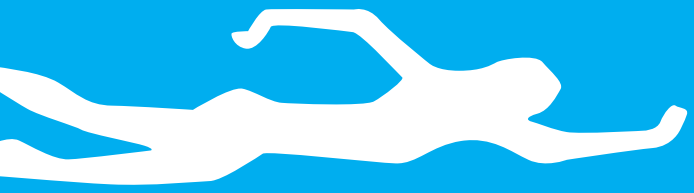
MOBNING PÅ NETTET I ANDEN POTENS

Mobning på nettet adskiller sig især fra almindelig mobning på tre forskellige måder:

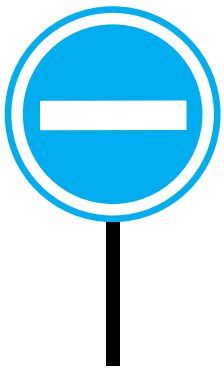
- Tid: Mobningen kan foregå på alle tider af døgnet – ikke kun, når man er til stede.
- Mangfoldiggørelse: Mobningen kan hurtigt deles og nå ud til uoverskueligt mange.
- Anonymitet: Afsenderen kan skjule sig bag falske profiler eller anonyme brugernavne.

Fælles for de tre er, at der er uvished forbundet med dem. En uvished, som forstærker følelsen af afmagt og øger presset på den, der er udsat for mobning:

- Hvornår kommer næste lede besked, og hvor længe vil den være tilgængelig? = tid
- Hvor mange har set det? = mangfoldiggørelse
- Hvem står bag? = anonymitet



“PÅ NETTET KAN ALTING VÆRE TILGÆNGELIGT HELE TIDEN – OG DET FORSVINDER IKKE AF SIG SELV. HVIS MAN VIL SLIPPE VÆK FRA DET, SÅ ER MAN SAMTIDIG TVUNGET TIL AT MELDE SIG HELT UD AF FÆLLESSKABET – BÅDE DET VIRTUELLE, MEN OGSÅ NOGLE GANGE DET FYSISKE”.



Børnerådets undersøgelser viser, at jo mere børn og unge er tilstede på de sociale medier, jo oftere er de også udsat for mobning. Det kan være alt fra ondsindede beskeder til trusler eller krænkende billeder, som enten sendes direkte eller uploades, så alle kan se dem.

Og rammerne ændres løbende, i takt med at nye platforme og interaktionsformer dukker op. Børn og unge er ofte firstmovere, når det kommer til at benytte nye sociale medier. De tager hurtigere end de fleste voksne de nye platformes præmisser for interaktion til sig. På få år er mængden og udvalget af sociale medier vokset hastigt. Facebook, Instagram, SnapChat, YouTube, Ask.fm og videre til noget nyt i morgen. Hvis man som voksen ikke selv er aktiv på de nye platforme, kan det være en udfordring at sætte sig ind i præmisserne for dem.

FORÆLDRES ROLLE OG ANSVAR

Det kan virke som noget af en jungle at skulle følge med i børn og unges færden på nettet. Hvad er det vigtigt at huske på, og hvordan skal man reagere? Herunder oplistes fem generelle forholdsregler, som voksne og forældre kan tage for at hjælpe de unge til trygt at kunne begive sig rundt på nettet.

1. VIS INTERESSE FOR DIT BARNS LIV ONLINE

Desværre oplever næsten 40 procent af børn og unge, at deres forældre sjældent eller aldrig interesserer sig for, hvad de laver på nettet. Derfor må første skridt til at hjælpe børn og unge være, at vi som voksne og forældre udviser en interesse for det liv, de lever online. Når vi forstår, hvad der foregår, og hvordan det foregår, øges vores mulighed for at hjælpe, når noget går skævt, eller en situation er eskaleret. Dermed ikke sagt, at vi skal være eksperter i sociale medier, før vi kan hjælpe i mobbe-situationer. Voksne er, uanset hvad, i højere grad rustede til at klare konflikter – og det er vigtigt at huske, så man ikke bliver teknik-forskrækket og lader børnene i stikken.

2. HJÆLP MED AT SKABE ET TRYGT RUM

En anden ting, der er vigtig at huske omkring børn og unges kommunikation, er, at voksne ofte vil tolke deres sprogbrug som ekstremt. Der skal som regel ikke så meget til, før de "elsker" eller "hader" noget. Men selvom unge inden for fællesskabet godt kan afkode hinandens sprogbrug, er det stadig vigtigt for voksne at hjælpe de unge til at skabe et rum, hvor de ikke krænker og overtræder hinandens grænser. Sprog skaber virkelighed – og hvis man som voksen er med til at fremme et miljø, med respekt for forskellighed, så er vi en godt skridt på vej mod noget, der kan forebygge mobning – både on- og offline.

3. HUSK AT MOBNING SKER I FÆLLESSKAB

Som en tredje ting er det også vigtigt at betragte mobning som noget, der sker i et fællesskab - og ikke nødvendigvis som en konflikt med en tydelig undertrykker og et tydeligt offer. Mobning sker, når andre ikke siger fra, eller når de ligefrem bakker op i form af sprog og handling. Som voksen er det derfor vigtigt, at man har et indblik i, hvordan fællesskabet fungerer. Og indblik i unges online-fællesskaber kræver, at man som voksen spørger ind og viser interesse.

4. VIS TILTRO – SÅ BLIVER DET NEMMERE FOR BARNET AT BETRO SIG

For det fjerde er det vigtig at tro på barnet eller den unge. Det er deres oplevelse af situationen, der i første omgang er det vigtigste. Og hvis noget opleves som mobning af et barn eller af en ung, skal det ikke affejes som drilleri eller narrestreger. Hvis et barn henvender sig til en voksen med et problem for derefter at blive negligeret, bliver det ikke nemmere for barnet at betro sig – selvom mobningen fortsætter. Stil derfor ikke spørgsmålstegn til, om noget er mobning eller ikke er mobning, men tag barnet alvorligt og find hoved og hale i de forskellige parters versioner af situationen.

Den første reaktion kan i mange tilfælde være at "anmelde" et givent opslag eller billede til udbyderen af tjenesten. De fleste sociale medier har efterhånden en funktion, der gør det muligt, at indberette sprogbrug og indhold, hvis det opleves krænkende. Man kan også ofte helt blokere en bruger fra at kunne komme i kontakt. Denne løsning er som oftest kortsigtet - dog dermed ikke sagt, at den ikke kan virke.

5. HUSK DIT ANSVAR!

Alt efter situationen kan man som voksen gøre flere ting. Og det er naturligvis op til den voksne – gerne i fællesskab med kollegaer eller forældre – at afgøre dette. I nogle tilfælde skal forældrene inddrages, og i andre grove tilfælde (for eksempel, hvis der er tale om trusler af den ene eller anden slags) skal politiet måske involveres.

Der er altså ingen tvivl om, at mobning på nettet stiller store krav til forældre og voksne. Men vi må, for børnenes skyld, ikke svigte dem her. Så det sidste punkt, der er vigtigt at huske, er, at uanset hvad, så er det stadig de voksnes ansvar, at børn og unge kan være trygge, der hvor de færdes.

“FACEBOOK, INSTAGRAM, SNAPCHAT, YOUTUBE, ASK. FM OG VIDERE TIL NOGET NYT I MORGEN. HVIS MAN SOM VOKSEN IKKE SELV ER AKTIV PÅ DE NYE PLATFORME, KAN DET VÆRE EN UDFORDRING AT SÆTTE SIG IND I PRÆMIS-SERNE FOR DEM”.

CASE: SSP KØBENHAVN

NÅR SLAGSMÅLET FLYTTER FRA SKOLEGÅRDEN TIL FACEBOOK

DIGITAL DANNELSE BLANDT UNGE ER ET AF DE VIGTIGSTE FOREBYGGELSESOMRÅDER FOR SSP KØBENHAVN. I DAG STARTER SLAGSMÅLET NEMLIG HYPPIGT PÅ DE SOCIALE MEDIER, INDEN DET RYKKER TIL SKOLEGÅRDEN.

Med afsæt i en tresporet strategi til adfærdsændring på de sociale medier, hvor både fagprofessionelle, forældre og unge inddrages, har SSP København engageret de unge og fået dem til at uddanne hinanden i digital dannelse på sociale medier – en metode, som nu er ved at blive udrullet som et pilotprojekt på udvalgte skoler i København.

Projektet kan implementeres i alle kommuner i Danmark og her fortæller souschef i SSP København, Mikael Kelk, om baggrunden, processen og metoden for projektet.

HVAD ER BAGGRUNDEN FOR PROJEKTET?

Jeg talte med en skoleleder på Tingbjerg Heldagsskole, som sagde: "Slagsmålet i skolegården er flyttet ind på Facebook". Og det citat, synes jeg, rammer projektet rigtig godt ind.

Udfordringen med de unge på sociale medier er blandt andet, at den måde, der kommunikeres på via eksempelvis Facebook, er anderledes, end den måde, der kommunikeres på i den virkelige verden. På Facebook kommunikerer du skriftligt – og du kan ikke tage det tilbage, du har skrevet. Det kan leve videre i andre sammenhænge og på andre platforme. De valg, de unge træffer på de digitale sociale platforme kan have konsekvenser nu og i fremtiden. Det tænker de unge ikke nødvendigvis over, og det bliver vi simpelthen nødt til at uddanne dem i. Man kan kalde det "digital dannelse". For os betyder det blandt andet, at de unge skal træffe nogle oplyste valg, når de færdes på sociale medier.

HVAD LIGGER DER I EN TRESPORET STRATEGI TIL ADFÆRDSÆNDRINGER?

Vi taler om det gode oplyste valg på de sociale medier i tre spor: Et trivselsskabende spor, et kriminalitetsrettet spor og et spor rettet mod de unges risikoadfærd.

Trivselssporet er udadrettet, og her kan man for eksempel tale om mobning og udelukkelse på de sociale medier. Det forekommer på de sociale medier, ligesom det forekommer i skolegården, på gaden og i klubben.

I det *kriminalitetsrettede spor* har vi fokuseret på at uddanne de unge. De skal vide, at noget af det, de gør og skriver på de sociale medier, kan være kriminelt. Det kan for eksempel være ulovligt at true andre.

Det tredje spor – *risikoadfærdssporet* – vender indad mod den unge selv. Det fokuserer på de unges egen risikoadfærd og handler om at lære de unge at

facebook

passe på sig selv. Det er for eksempel ikke nødvendigvis en god idé at sende udfordrende billeder af sig selv til andre, ligesom der også kan være risici forbundet med at chatte med fremmede. Mange unge risikerer også at kaste sig ud i konflikter på de sociale medier, uden at de egentlig er klar over det.

De tre spor har vi viderebragt til tre målgrupper: fagprofessionelle, forældre og selvfølgelig de unge selv. I projekter som dette er det nemlig vigtigt at klæde alle grupper fagligt på til opgaven. Man kan jo ikke forvente, at vi kan uddanne unge i digital dannelse, hvis vi ikke selv ved nok om, hvad det egentlig indebærer. Til dette formål engagerede vi undervisere fra politiet og kommunikationsfaglige personer.

BRUGTE I SAMME STRATEGI OVER FOR ALLE MÅLGRUPPER?

Vi bruger faktisk samme tilgang over for fagprofessionelle og forældre: "At forstå, spotte og handle".

For det første skal både lærere og forældre forstå, hvorfor det er vigtigt for de unge at være sociale på de digitale medier. Der ligger en enorm kraft i de sociale medier, som os, der ikke er vokset op med en iPad i hånden, måske ikke helt forstår. Herudover er det vigtigt, at vi ikke kun lærer os selv at forstå, men også accepterer, at de sociale medier er enormt vigtige for mange unge.

Næste skridt er at lære at spotte et problem på de sociale medier. Her skal man lede efter tegn på mistrivsel blandt de unge eller tegn på, at der foregår en konflikt på de sociale medier, som ikke nødvendigvis er en del af klasseværelset eller aftensmadsbordet.

Når man har lært at spotte et problem, skal man lære at handle. Det kan være ved at tale med sit barn eller elev om en eventuel udfordring eller bringe det op på et forældremøde. Nøjagtigt som hvis man havde spottet et slagsmål i skolegården eller på legepladsen.

HVORDAN BLIVER DE UNGE ENGAGERET?

Med forståelse, accept og opbakning på skolen og hjemmefra, kan vi engagere de unge. Vi har tidligere haft god erfaring i at arbejde med den metode, som vi kalder for ung-til-ung-kommunikation, hvor vi inddrager de unge som ungeambassadører. Metoden virker, fordi vi som mennesker har det med at lytte til, og ikke mindst tilpasse vores adfærd efter, budskaber fra mennesker, vi kan relatere os til.

Når vi engagerer unge i dette projekt, fungerer det sådan, at den lokale SSP'er samler en 7. klasse. Hele klassen bliver kørt igennem de samme tre spor som lærerne og forældrene, men det faglige indhold er naturligvis tilpasset de unge i et undervisningsforløb på skolen. Vi inviterer både eksterne fagfolk, der kan klæde de unge fagligt på, og kommunikationsfolk, der kan uddanne de unge i, hvordan budskabet skal formidles, når man er ambassadør. Politiet bliver også inviteret til at fortælle de unge om de mulige konsekvenser, der kan være ved at være på sociale medier.

Herefter får de unge selv mulighed for at melde sig som ambassadører. Dem, der melder sig som ambassadører for projektet, får til opgave at gå ud i de mindre klasser og "skubbe" til de mindre elevers adfærd og hjælpe dem med at tage det gode valg på de sociale medier.

Herefter får de unge selv mulighed for at melde sig som ambassadører. Dem, der melder sig som ambassadører for projektet, får til opgave at gå ud i de mindre klasser og "skubbe" til de mindre elevers adfærd, og hjælpe dem med at tage det gode valg på de sociale medier.

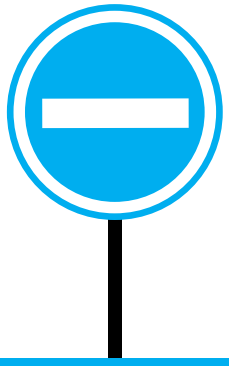
HVORDAN TOG DE UNGE OG FORÆLDRENE IMOD PROJEKTET?

De unge syntes virkelig, at emnet var relevant for dem. De ville gerne lære, og endnu vigtigere, ville de gerne give viden fra sig. Det fantastiske ved ung-til-ung-kommunikation er også, at de mindre elever enormt gerne vil lytte til og lære fra de "store" elever.

For mange forældre var projektet faktisk lidt af en øjenåbner. Mange forældre ved ikke, hvad der foregår på de sociale medier. Det var derfor også vigtigt for os at italesætte, at de sociale medier ikke er farlige, man skal bare kunne håndtere dem. Nøjagtig ligesom det ikke er farligt at træde ind i en skolegård, så længe man kan begå sig socialt.

HVAD SKAL MAN VÆRE OPMÆRKSOM PÅ, NÅR MAN ENGAGERER UNGE SOM AMBASSADØRER?

Når man engagerer de unge som ambassadører, skal man acceptere, at de har en alder og erfaring, der gør, at de måske vælger at gå ud af et spor, man som voksen ikke nødvendigvis selv vil vælge. Men det er uhyre vigtigt at kunne give ansvaret fra sig og stole på de unge. De unge vil enormt gerne inddrages, og vi tror på, at hvis vi klæder de unge ordentligt på, så kan de også tage det rigtige valg, hvilket jo er kernen i vores arbejde.



MIKAEL KELKS RÅD TIL ANDRE, DER GERNE VIL I GANG MED AT ARBEJDE MED UNGE OG DIGITAL DANNELSE:

- Tænk i flere spor, så indsatsen favner bredt, og så de unge kan genkende sig selv i nogle af de problematikker, der berøres.
- Tving dig selv til at forstå præmissen for, hvorfor de unges forhold til sociale medier er anderledes, og accepter, at det er sådan. Herefter skal man tænke i, hvordan man kan spotte og handle på problemer. Men særligt det første trin er vigtigt, og det er der faktisk mange, der springer over.
- Tænk i tre målgrupper. Når vi også involverer de fagprofessionelle og børnenes forældre, sikrer vi opbakning og forankring af projektet.
- Et godt råd er også at tænke i ung-til-ung-kommunikation. Det engagerer de unge, og vi ved, at det virker, fordi vi gerne vil lytte og rette vores adfærd til efter mennesker, vi kan relatere os til.
- Lad være med at give de unge forbud mod at være på de sociale medier. Helt overordnet tror vi nemlig ikke på forbud. Derimod tror vi på at klæde de unge på til selv at tage de rigtige valg: Hvis der er en swimmingpool, så lær de unge at svømme. På samme måde giver vi de unge redskaber og rammerne til at kunne begå sig på de sociale medier frem for at give dem forbud.

KUNO SØRENSEN, PSYKOLOG I RED BARNET

GROOMING
– EN STRATEGISK PROCES

DET KAN VIRKE UFORSTÅELIGT, AT EN KVIK OG VELFUNGERENDE TEENAGER MØDES MED EN 20 ÅR ÆLDRE MAND FOR AT VÆRE SAMMEN SEKSUELT. MEN DEN MANGLENDE FORSTÅELSE KOMMER OFTE, FORDI VI KUN SER SLUTRESULTATET OG IKKE HAR HAFT MULIGHED FOR AT FØLGE DEN LANGE PROCES, DER TRIN FOR TRIN HAR FØRT FREM TIL MØDET. FORUD FOR ET SEKSUELT OVERGREB ER NEMLIG OFTE GÅET EN LÆNGERE PROCES, HVOR KRÆNKEREN HAR BEARBEJDET ET BARN ELLER EN UNG TIL AT OVERSKRIDE SINE GRÆNSER. DENNE PROCES KALDES FOR "GROOMING" OG INVOLVERER EN RÆKKE FASER, SOM KRÆNKEREN GENNEMGÅR MED BARNET FOR AT KUNNE BEGÅ OVERGREBET – ONLINE ELLER FYSISK. DENNE ARTIKEL BELYSER DE GROOMING-PROCESSER, VI SER ONLINE.

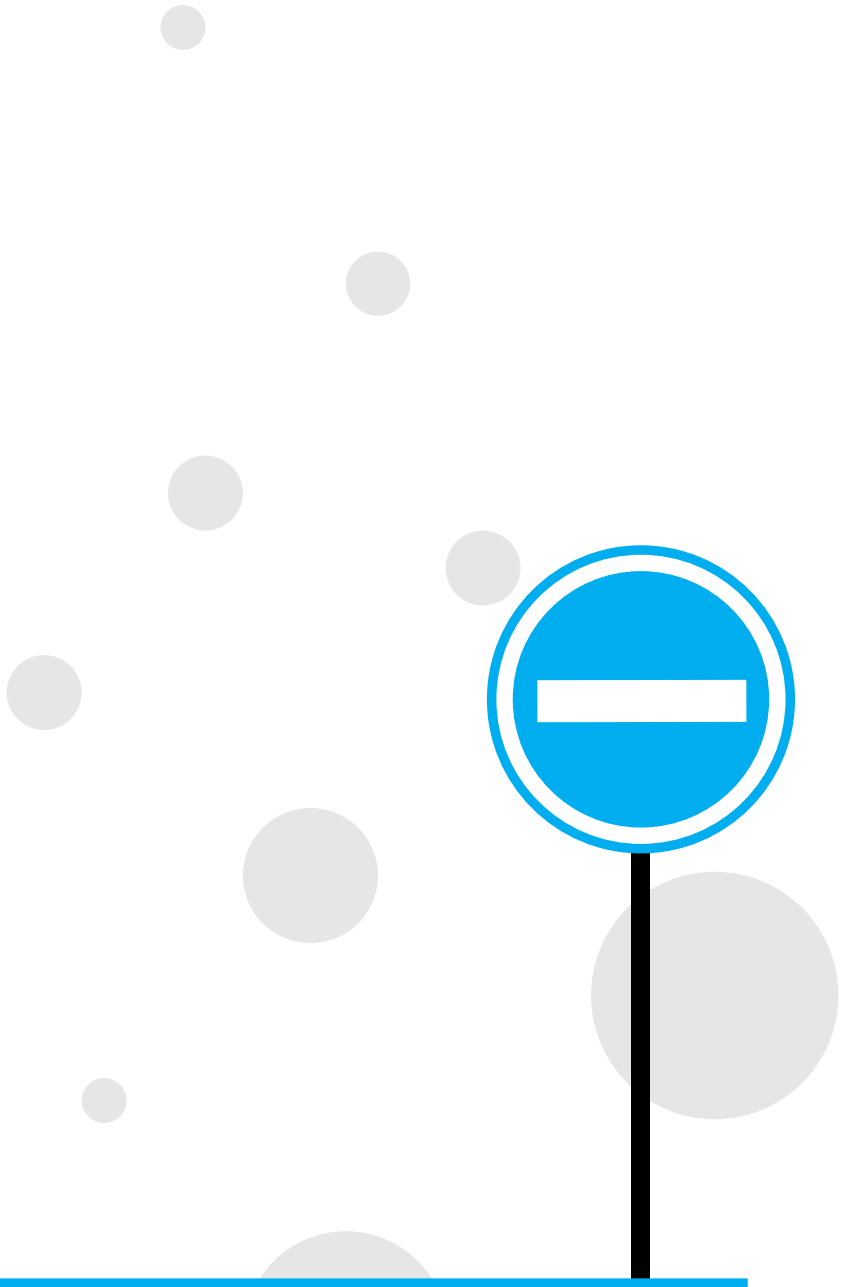
Det engelske ord *grooming* betyder at pleje, passe og soignere sig selv eller andre, men kan også henvise til at optræne og forberede nogen på noget, der skal ske. Grooming bruges derfor som en samlet betegnelse for den proces, hvor en ældre og mere erfaren krænker bruger manipulation, løgne, smiger og ros samt påfører ofret ansvar og skyldfølelse for på den måde at få ofret til (tilsyneladende frivilligt) at medvirke i seksuelle aktiviteter, der har til formål at tilfredsstille krænkeren. Det er ikke nyt, at børn udsættes for grooming og seksuelle overgreb. Men krænkere har fået nye muligheder med udviklingen inden for IT og sociale medier. Arketypen på en børnelokker, der lokker med en slikkepind på legepladsen, må konstatere, at der er bedre muligheder for at skabe kontakt til børn i de online-universer, som børnene tilbringer så meget tid i.

HVEM ER OFRENE FOR GROOMING?

Det er naturligt at spørge, hvem der kan blive udsat for en krænkers grooming. Erfaringerne viser, at alle børn kan blive offer for en seksuel krænker online, og vi har set eksempler på, at selv ressourcestærke børn er blevet narret og manipuleret af krænkeren til at gå langt ud over de grænser, de ellers selv mente, de havde. Men vi kan også registrere, at børn med lavt selvværd og dårlige sociale relationer er ekstra sårbare over for grooming. Krænkerens tilbud om opmærksomhed, ros og anerkendelse gør særligt stort indtryk på børn, som ikke føler sig forstået, rummet og inkluderet i hverdagen. Desuden har vi gennem de senere år set flere eksempler på, at unge teenagepiger er særligt udsatte for online-krænkere.

Barnet er villigt til at gå langt i groomingforløbet, fordi krænkeren tilbyder børnene positive oplevelser eller erfaringer. Det kan eksempelvis være ros, anerkendelse, støtte, en at se op til eller et økonomisk tilskud. Helt centralt i groomingprocessen er derfor også oplevelsen af det tillidsbrud, der sker, når den voksne afslører sine reelle hensigter med den positive opmærksomhed og kontakt.

Børnene har ikke på forhånd en forståelse af, at den psykiske manipulation, som grooming er, virker gennem medierne og gradvist får flyttet deres egne grænser. Når det går galt, føler de, at



de har været naive, de er skamfulde og ydmygede i en sådan grad, at de fleste helst ikke vil involvere andre i deres oplevelse, men prøve at glemme det hurtigst muligt.

GROOMING-PROCESSENS FASER

Mere systematiske analyser af sager om online-relaterede seksuelle overgreb på børn peger på, at mange af disse overgrebssager gennemløber nogenlunde de samme faser. Rækkefølgen kan variere lidt fra sag til sag, for eksempel hvornår det seksuelle tema introduceres, ligesom nogle faser kan lappe ind over hinanden eller fremstå tydeligere end andre. Grooming-forløbet er illustreret i grafikken her på siden.

GODE RÅD FRA KUNO SØRENSEN

1. Anerkend, at venskaber på de sociale medier er en uundværlig del for børn og unges sociale liv – manglende tilstedeværelse i de sociale medier fører til social eksklusion.
2. Vis en aktiv og positiv interesse for børnenes færden på de sociale medier – det er ligeså vigtig en del af deres liv som skole og fritidsinteresser.
3. Fortæl børnene, at de har ret til at få deres grænser respekteret – lovgivning, moral og etik er det samme i den fysiske verden som i cyberspace.
4. Tal med børnene om, at der også findes børnelokkere, svindlere og bedragere på nettet – og at de kan være med til at stoppe de kriminelle, når de fortæller om det til en voksen.
5. Fortæl børnene, at i sager om seksuelle krænkelser på nettet, er det den voksne, der er den kriminelle – og at børn har ret til at blive beskyttet og få hjælp mod voksnes overgreb.

GROOMING-PROCESSENS FASER

1

DEN KONTAKTSKABENDE FASE

I den kontaktskabende fase udvælger krænkeren sig potentielle ofre. Krænkeren skaber en profil på nettet, enten som barn eller som voksen. Formålet er at skabe en profil, som barnet eller den unge synes er interessant, eller som fanger barnets nysgerrighed. Målet er at fremstå som en attraktiv ven for barnet og dermed mindske barnets skepsis eller kritiske fornuft.

2

OPBYGNING AF VENSKABET

Når krænkeren har etableret kontakt til et potentielt offer, forsøger han at få afdækket de særlige problemer, ønsker eller drømme, som barnet eller den unge tumler med. Det er her, krænkeren mange gange er meget dygtig til at få spurgt ind til det, som motiverer barnet til at fortsætte og udbygge kontakten til den fremmede. Når krænkeren har fundet et eller flere temaer at kommunikere om, sørger krænkeren for at vise en personlig interesse. For eksempel ved at spørge deltagende, vise omsorg og give anerkendelse.

8

FASTHOLDE HEMMELIGHEDEN

Undervejs i hele grooming-processen – men især når det seksuelle tema er blevet introduceret – sørger krænkeren for at påpege, at det, barnet og han har sammen, er noget helt specielt, som andre ikke vil kunne forstå eller acceptere, og at det derfor er vigtigt, at barnet ikke fortæller andre om deres særlige kontakt. Når processen er nået så langt, at barnet har været udsat for seksuelle krænkelser, vil krænkeren igen minde barnet om, at det ikke må afsløre, hvad der er sket.

7

DET FYSISKE MØDE ARRANGERES

For nogle krænkere er det endelige mål at mødes med barnet i den fysiske verden for at gennemføre de seksuelle aktiviteter med barnet. I mange sager bygger det fysiske møde på den tillid og det venskab, som er blevet opbygget. Det er for barnet eller den unge ikke et møde med en fremmed, men tværtimod en ven eller fortrolig person, som de mener, de kan stole på.

HVORFOR GÅR NOGLE BØRN SÅ LANGT?

For at kunne forstå, hvorfor nogle børn går så langt i det venskab, der opbygges i en grooming-proces, er det vigtigt også at se på de positive erfaringer og oplevelser, som krænkeren tilbyder barnet.

Krænkeren giver ofte barnet *opmærksomhed, ros og anerkendelse*, som sårbare børn har svært ved at modstå. Krænkeren kan også iscenesætte sig som *en sød voksenven*, der forstår og støtter barnet, når det bliver drillet, har svært ved at få venner eller skændes med mor og far. Krænkeren kan også repræsentere en *erfaring og modenhed*, som barnet ser op til og gerne vil have andel i. Endelig kan krænkeren lokke med forskellige *økonomiske tilskud* som en ny smartphone.

Børnene har ikke på forhånd en forståelse for, at den psykiske manipulation (grooming-processen) virker gennem medierne og gradvist får flyttet deres egne grænser.

Kilde: Artiklen er tidligere bragt i Red Barnets publikation: Red Barnet (2015): Hvor slemt ka' det være? – En antologi om it-relaterede seksuelle overgreb på børn og unge.

3

RISIKOVURDERINGER

Krænkeren ved, at han er ude i et ulovligt ærinde, hvorfor han undervejs i grooming-processen vil træffe nogle valg, som skal nedsætte risikoen for at blive afsløret. Det kan være ved at flytte korrespondancen fra åbne chatfora til lukkede. Krænkeren kan også spørge ind til voksne omsorgspersoner omkring barnet. Endelig vil krænkeren også afprøve barnets evne til at holde på en hemmelighed, fordi det kan være risikabelt, hvis barnet fortæller for meget.

4

DEN ENESTE ENE

Når krænkeren vurderer, at der er en god mulighed for at få barnet til at medvirke i de seksuelle planer, som krænkeren har, er næste fase at styrke relationen imellem dem. Relationen intensiveres, og krænkeren understreger, hvor meget de hører sammen, at det er vigtigt, at de har tillid til og kan stole på hinanden. Barnet bliver opfordret til at betro sig til krænkeren, og han vil bekræfte igen og igen, at barnet har stor betydning i hans liv.

6

DET DIGITALE OVERGREB ARRANGERES

Det digitale overgreb kan startes over webcam, eller ved at barnet bliver bedt om at sende billeder af sig selv. Barnet overtales gradvist, og hver gang giver krænkeren anerkendelse og ros. Det kan også lykkes at overtale barnet til at sende erotiske billeder med mindre og mindre tøj på. Hvis barnet oplever, at dets grænse er nået, skifter krænkeren attitude. Fra at være rar og anerkendende går krænkeren til at stille mere direkte krav og komme med trusler. Barnet er nu fanget ind af krænkerens manipulerende forførelse og er blevet narret eller presset til at overskride sine egne grænser.

5

DET SEKSUELLE TEMA INTRODUCERES OG AFPRØVES

Det seksuelle tema kan introduceres ved at spørge til erfaringer med kærester eller at kysse rigtigt. Det kan også være spørgsmål om, hvordan kroppen er udviklet. Krænkeren tilbyder sin viden og erfaring, og ofte forklarer krænkere ved efterfølgende retssager, at det netop var barnets behov for at skaffe sig viden fra en erfaren person, der fik samtalerne til at handle så meget om seksuelle temaer.

VIL DU VIDE MERE?

Læs mere om grooming-processerne i bogen "Hvor slemt kan det være?" tilgængelig på www.redbarnet.dk/anmeld under "Ressourcer".

NÅR FORBRYDELSER BLIVER DIGITALE
HVORDAN SIKRER VI VORES DIGITALE PRIVATLIV?

Kapitel 5

HVORDAN SIKRER VI VORES DIGITALE PRIVATLIV?

RASMUS THEEDE, FORMAND FOR RÅDET FOR DIGITAL SIKKERHED

PRIVATLIVET: DEN DIGITALE TIDSALDERS STORE UDFORDRING

VI LEVER PÅ GODT OG ONDT I ET AF DE MEST DIGITALISEREDE SAMFUND, HVOR ALT POTENTIELT KAN DELES MED ALLE. DET HAR DERFOR ALDRIG VÆRET MERE RELEVANT AT DISKUTERE, HVORDAN, HVORNÅR OG HVILKE INFORMATIONER, VI SOM BORGERE ØNSKER AT DELE MED ANDRE.

Danskerne har med 32 "ting" koblet til internettet (så som mobiltelefon, Ipads og så videre) en andenplads på listen over verdens mest internetforbundne folkefærd – kun overgået af Sydkorea. Vores offentlige digitaliseringsmuligheder er et forbillede for mange lande omkring os, men de private virksomheder er også rigtig godt med.

Men når nu Danmark er foregangsland, når det kommer til digitalisering, er vi det så også, når det gælder borgernes ret til netop privatliv og effektiv beskyttelse af borgernes data?

Men når Danmark nu er forgangsland, når det kommer til digitalisering, er vi det så også, når det gælder borgernes ret til netop privatliv og effektiv beskyttelse af borgernes data?

DET FORBUNDNE SAMFUND

Den digitale tidsalders nye, komplekse muligheder for deling af data giver os mange nye muligheder. Det gælder for eksempel, når vi skal udfylde vores selvangivelse, når vores læge hurtigt skal have adgang til vores patientdata, eller når vi blot vil dele familiebilleder med andre. De gevaldige datamængder, de såkaldte big data, giver unikke muligheder for at indsamle, opbevare og analysere enorme mængder af data om os alle sammen.

Skyggesiden af digitaliseringen er dog, at den er blevet så kompleks, at det ofte er umuligt for selv IT-professionelle at vide, hvilket data der indsamles om os, hvor dataet befinder sig, hvad det bliver brugt til, og om det nogensinde bliver slettet. Vores data er nemlig ikke længere kun på papir og låst sikkert inde i skabe og skuffer. Vores data er højst sandsynligt ikke en-

gang længere på en server, som står sikkert låst inde i et lokale hos den virksomhed eller myndighed, der nu engang behandler vores data. I dag er databehandling i sandhed global, og vi bliver nødt til at tage højde for, hvordan vi benytter for eksempel "data i skyen", hvem der har adgang til vores data og de juridiske restriktioner på tværs af landegrænser.

HVEM ER DOG INTERESSERET I VORES PRIVATE DATA?

Private data er i sagens natur først og fremmest beregnet til at servicere os selv og altså til at være begrænset til de myndigheder og virksomheder, som – helst efter vores tilladelse – har brug for dem. Men indsamling og analyse af store datamængder er også en overordentlig god forretning for virksomheder, der lever af at indsamle, analysere og sælge disse data. Vores forbrugsvaner på internettet, sundhedsoplysninger og private interesser siger nemlig overordentlig meget om os som forbrugere, og det har uvurderlig værdi for mange virksomheders markedsføring og valg af kundesegmenter.

På den mørke side af internettet er der ligeledes stor efterspørgsel efter private data. Identitetstyveri, kreditkortsvindel og direkte handel med identiteter er nemlig desværre blevet en del af hverdagen på internettets skyggeside.

RETTEN TIL DIGITALT PRIVATLIV ER I DEFENSIVEN

Der er ingen tvivl om, at den hastighed, som den danske digitalisering er foregået i, har sat vores privatliv alvorligt under pres. Især offentlige myndigheder, men også private virksomheder, ligger inde med et væld af data om danskerne i form af helbredsoplysninger, økonomiske oplysninger og sociale forhold.

Sikkerheden, og dermed beskyttelsen af borgernes data, har dog ofte haft svært ved at følge med i samme tempo, hvilket flere gange er blevet påpeget af både Datatilsynet og Rigsrevisionen samt belyst i pressen, når der eksempelvis sker tab af data om danskerne. Det kan vi selvfølgelig ikke være tjent med. For at kunne bryste os af at være et af verdens bedste lande til digitalisering, bliver vi nødt til at være mindst lige så gode til at beskytte vores personlige data. Det kræver et personligt ansvar fra borgerne og bedre lovgivning. Men det kræver også, at vi får privatlivsbeskyttelse helt ind under huden på vores IT-systemer fra starten, det såkaldte "Privacy by Design".

DET PERSONLIGE ANSVAR

I en digital tidsalder er alle nødt til at tage ansvar for at beskytte privatlivets fred. Både os selv som borgere og de virksomheder og myndigheder, der opbevarer, behandler og benytter vores data. Vi bliver ofte bedt om at afgive en række personlige oplysninger på inter-

nettet, men det er de færreste, der læser og forstår de ofte lange forklaringer på, hvad man har tænkt sig at bruge data til, og om denne data videresælges til tredjepart. Meget tyder på, at vi er villige til at sælge ud af vores private data, hvis vi får noget igen. Vores personlige data giver som en digital valuta for eksempel adgang til sociale netværk, gratis e-mail eller noget helt tredje. Og indsamling af data om private personer så som vores forbrugsvaner, hvor vi befinder os fysisk eller på nettet, eller hvad vi interesserer os for, er en god forretning – men kan også misbruges, hvis vi ikke er forsigtige.

Om vi vil det eller ej, er vi borgere i et digitalt samfund, og derfor er vi nødt til at tage et personligt ansvar. Det er op til os alle sammen at overveje nøje, hvad vi vil dele med andre, lægge på sociale medier, og hvad prisen rent faktisk er for at dele vores data ("det med småt"). Derudover er vi nødt til at sætte os ind i internettets farer samt vide, hvordan vi beskytter os imod dem. Store dele af de digitale identitetstyverier og andre former for IT-kriminalitet, vi ser i dag, kunne være undgået med basisviden og omtanke.

PRIVATLIVSBESKYTTELSE SKAL MED FRA STARTEN

Privacy bør ikke betyde, at vi ikke udnytter teknologiens muligheder til at forbedre vores kommunikation og skabe nye muligheder for effektivisering og innovation. Men teknologiens muligheder skal i høj grad respektere privatlivets fred – uden at borgere eller systembrugere skal sætte sig ind i komplekse, tekniske problemstillinger for at gennemskue, hvad der sker med privat data, og hvordan de beskyttes. En stor udfordring med mange af de IT-systemer, der benyttes i dag – især i det offentlige – er, at de er fra en tid, hvor privatlivsbeskyttelse ikke havde samme fokus som i dag. De er populært sagt ikke "Privacy by Design".

Hvis vi skal tage privatlivsbeskyttelse seriøst fremover – og det skal vi – nytter det ikke, at vi til stadighed udvikler IT-systemer, hvor privatlivsbeskyttelse ikke er med i selve systemets grund-DNA. Både dem, der bestiller og udvikler IT-systemer, skal derfor være særligt opmærksomme på Privacy by Design. Privacy by Design bygger på syv helt fundamentale principper, blandt andet at privatlivsbeskyttelse skal være slået til fra start, samt at der tænkes privatliv helt fra før de personlige data overhovedet kommer ind i systemet, til de forlader systemet igen.

Hvis vi tænker os godt om, tager et personligt ansvar, sørger for tidssvarende lovgivning og gennemtænker privatlivsbeskyttelse i IT-systemer fra starten, er der ingen grund til, at vi ikke både kan udnytte de mange fordele ved digitaliseringen og samtidig respektere privacy – privatlivets fred.

LARS BO LANGSTED, PROFESSOR, LEDER AF INTERNATIONAL ECONOMIC CRIME AND CYBER CRIME RESEARCH CENTRE (IECC), JURIDISK INSTITUT, AALBORG UNIVERSITET

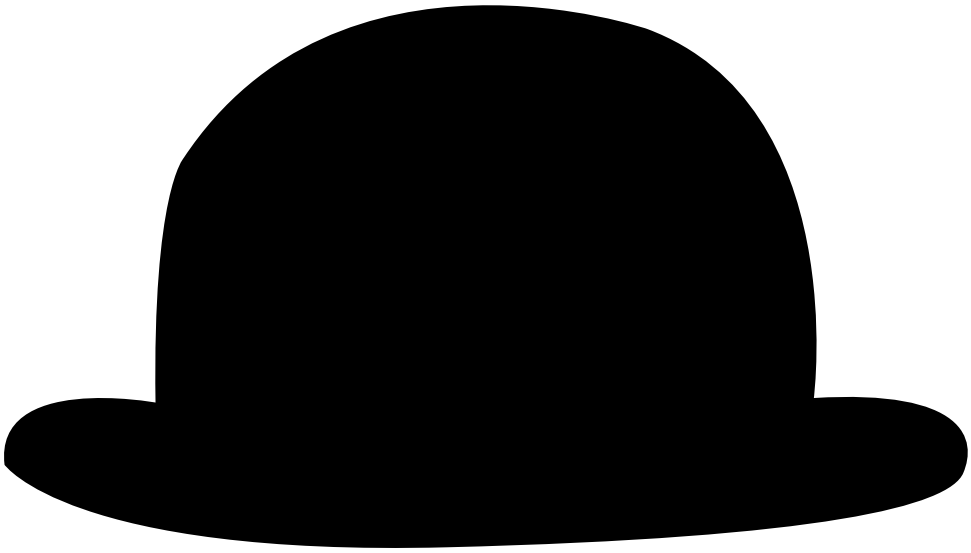
IT-KRIMINALITET KENDER INGEN GRÆNSER

I DAG FOREGÅR MANGE KRIMINELLE HANDLINGER VIA INTERNETTET UDEN AT DER SÆTTES MANGE SPOR I DEN FYSISKE VERDEN. SAMTIDIG KENDER INTERNETTET I SAGENS NATUR INGEN GRÆNSER, OG DET GIVER UDFORDRINGER BÅDE FOR LOVGIVERE, POLITI, ANKLAGEMYNDIGHED OG DEN ENKELTE BORGER.

Hacking, databedrageri, phishing og afpresning er alt sammen en del af det nye kriminalitetsbillede. Det nye er ikke, at mennesker begår kriminelle handlinger. Det nye er, at de i dag i meget høj grad foregår via internettet og kun sætter sig få direkte spor i den fysiske verden. Det er en udfordring for lovgiver og for politi og anklagemyndighed, og det er en udfordring for den enkelte borger.

Lige siden Kong Hammurabi for omkring 4000 år siden lavede en af de første skrevne love, har vi forfinet, justeret og tilrettet vores love – men stort set altid med henblik på fysiske fænomener. Den moderne teknologi behøver ingen pengesedler, virksomhedernes værdier er deres data og programmer, og deres hemmeligheder er lagret i filer. Det siges, at »data er de nye dollars«, men det er vores lovgivning ikke rigtigt indrettet til endnu. Selvfølgelig har vi fået regler om persondatabeskyttelse, teleselskabers pligter med hensyn til håndtering af data og bogføringens oplagring i "skyen". Men bortset fra disse helt specielle tilfælde og regler er al anden regulering tænkt og skrevet "analogt". Det skaber ikke bare usikkerhed hos politi, anklagemyndighed, domstole og forsvarere. Det skaber en grundlæggende usikkerhed på og tvivl om, hvorvidt vores lovgivning beskytter det, der er værdifuldt i den moderne verden, og i tilstrækkelig grad afspejler de nye måder at være samfund på.

En helt særlig udfordring er, at internettet i sagens natur ikke kender nogen grænser. Hvor vi i den fysiske verden passerer landegrænser og opholder os på forskellige landes territorium, transporteres data tværs over landegrænser med ufattelig hastighed og oplysninger opbevares på servere i mange forskellige lande. Sender man en mail fra Århus til Hamborg, transporteres den måske via Sverige, England og Holland, og den "sky", man har lagt sine oplysninger og billeder "op i", er i virkeligheden en server, der står i Californien. Det, der af brugerne opfattes som noget "stedløst", er i realiteten knyttet til transport- og lagringsmedier, der meget konkret står på forskellige landes territorium. Folkeretten, som er den del af juraen, der handler om, hvad de enkelte lande må i forhold til hinanden, siger meget klart, at hvert land bestemmer over sit eget territorium. Det gælder med hensyn til de love og regler, der skal gælde i det pågældende land, og det gælder for politiets muligheder for at foretage efterforskning.



Dansk politi kan således kun efterforske på dansk territorium. Skal der efterforskes i Tyskland, skal tysk politi gøre det på vegne af dansk politi.

Vi kan forestille os, at en hacker sidder i Brasilien. Hans filer og programmer opbevares på én server i Colombia og én i USA, han forsøger at hacke sig ind i en tysk virksomhed, hvis server befinder sig i Danmark, og hans kommunikationslinje er via det undersøiske kabel i Atlanterhavet og fire forskellige lande. Det skifter i øvrigt, hvilke lande der bliver brugt som "transitlande" for kommunikationen. Her er forbrydelsen knyttet til en række forskellige lande, og de kompetencer, de forskellige landes politi og anklagemyndighed har, rækker ikke videre end til deres eget land. Forestiller vi os, at den hacking, der er sket, efterforskes af tysk politi, skal de spørge Danmark om tilladelse til at efterforske i serveren i Danmark hvis de ønsker dette. De skal samtidig spørge amerikansk og colombiansk politi med hensyn til de servere, der er benyttet af hackeren, og endelig må de bede brasiliansk politi om bistand til for eksempel ransagning hos eller afhøring af gerningsmanden.

Indtil vi måske en dag finder ud af, at internettet bør behandles som et samlet sted, hvor der gælder nogle særlige regler også for efterforskning, må vi klare os med den gamle model. Den forudsætter naturligvis hurtigt og effektivt samarbejde mellem de forskellige landes politi. Selvom vi har en konvention om cybercrime, og vi har Interpol og Europol, er det indlysende, at det er et besværligt system og slet ikke svarende til den digitale virkelighed.

Og udfordringerne slutter ikke her. Pudser vi krystalkuglen, behøver vi ikke at se særligt langt ud i fremtiden før "Internet of Things" er en realitet: Det vil sige, at vores bil taler med vores køleskab, der taler med vores mobiltelefon og så videre. Og når tingene taler sammen, er det til stor gavn og glæde for os alle sammen. Men det kan også udnyttes af kriminelle, der eksempelvis via internettet aflæser indholdet af vores meget fysiske køleskab eller aflytter eller måske ligefrem fjernstyrer vores bil. Så er vi pludselig tilbage i den fysiske verden igen, og spørgsmålet er så, om vores almindelige regler kan håndtere den omvej?

INTERVIEW MED CHRISTIAN WERNBERG-TOUGAARD, FORMAND FOR IT-BRANCHENS UDVALG FOR IT-SIKKERHED

VI SKAL FORBEREDE OS PÅ EN FREMTID I DIGITAL SAMMEN-SMELTNING

EN AF LANDETS FØRENDE EKSPERTER INDEN FOR IT-SIKKERHED CHRISTIAN WERNBERG-TOUGAARD, GIVER HER SIT SYN PÅ FREMTIDENS DIGITALE KRIMINALITETSUDFORDRINGER OG INTRODUCERER BEGREBET "DET HYPER-KONVERGEREDE SAMFUND". ET SAMFUND, HVOR TEKNOLOGIER VIL SMELTE SAMMEN OG SKÆRPE KRAVENE TIL DEN DIGITALE BORGER.

Tager vi et kig i krystalkuglen, vil de typer af kriminalitet, som vi kender i dag, ikke nødvendigvis være meget anderledes i fremtiden. Der vil stadig være tyveri, bedrageri, indbrud og folk, der manipulerer med information. Det, der kommer til at ændre sig, er den måde, kriminaliteten bliver begået på.

Forestil dig en gammeldags bankrøver. Hvis han ville begå tyveri, skulle han fysisk gå ind i en bank og true sig til penge. Indbrudstyven skulle ind i et hus, mens bedrageren skulle anskaffe sig fysiske dokumenter. Alle tre er eksempler på forskellige indgange til forskellige former for kriminalitet. Fremtidens digitaliserede samfund vil være ét stor hus, hvor alt data er samlet på ét sted. Kommer den IT-kyndige kriminelle først ind ad denne dør, åbner der sig et kriminelt slaraffenland, hvor der er frit valg på alle hylder.

De offentlige myndigheder og de private virksomheder har derfor selvsagt databeskyttelse i højsædet, og de gør det overordnet set godt. Men der er flere og flere danske borgere, der ikke er klædt på til denne udvikling, fordi vi stadig er analoge borgere i et digitalt samfund. Og det gør os yderst sårbare. Som analoge borgere kan vi nemlig godt finde ud af at låse vores dør og lukke vores vinduer, når vi forlader vores hjem. Men vi ved ikke, hvordan vi låser den digitale dør eller beskytter digitale data. Og det er den primære kriminalitetsudfordring for fremtidens digitale samfund.

Sådan tegner Christian Wernberg-Tougaard fremtidens kriminalitetsbillede, og for ham er det forbundet med begrebet hyperkonvergens. En tilstand, hvor vi er omgivet af teknologier, der alle er smeltet sammen.

I FREMTIDEN SMELTER ALLE TEKNOLOGIER SAMMEN

Vi starter med at gå tilbage til år 2000, hvor man forudså en teknologisk udvikling, som man efterhånden må sige er realiseret i dag.

"Spoler vi tiden tilbage til årtusindskiftet, var det helt store modeord "konvergens", som kort kan defineres ved, at man forudså, at tingene ville begynde at smelte sammen. Dengang forestillede vi os, at vi på vores telefo-

ner ville kunne se, hvad der var i fjernsynet, og høre, hvad der var i radioen, på samme tid. Den type konvergens, som vi snakkede om tilbage i 2000, er nu realiseret. Du kan jo eksempelvis bruge din iPad til hvad som helst", forklarer Christian Wernberg-Tougaard.

I fremtiden begynder vi at ane en virkelighed, hvor den mobile verden, de sociale medier, big data, cloud teknologier og "internet of things" smelter sammen og begynder at konvergere. I det øjeblik, det sker, kommer der til at opstå helt nye muligheder og helt nye funktioner. Det kalder Christian Wernberg-Tougaard det hyperkonvergerede samfund. Inden vi når dertil, bliver vi nødt til at spørge os selv, hvad der sker, når man realiserer en type samfund, hvor alt er forbundet, alle datakilder hænger sammen, og samfundets duelighed er afhængig at det digitale.

"Der er klare fordele ved, at tingene begynder at konvergere i højere grad. Søger du eksempelvis på en rejse i dag, har alle nok oplevet, at der dukker rejseannoncer op på andre websteder. For fremtiden vil man være i stand til at opsamle alle dine data, så hvis du har vist interesse for Kina, vil man kunne skræddersy rejser til Kina til dig. På den måde bliver det hele meget mere serviceorienteret, fordi man vil kunne give dig lige præcis det, du er interesseret i", fortæller Christian Wernberg-Tougaard optimistisk, men uddyber, at der også er udfordringer og risici forbundet med det hyperkonvergerede samfund:

"I dag kan indbrudstyve spore dine interesser via de sociale medier. De kan finde ud af, at du interesser dig for cykling og har en meget dyr cykel. De kan også se, når du er ude at rejse og på den måde regne ud, hvornår de kan begå indbrud. Den form for brug af data og informationer, som vi frivilligt stiller til rådighed, kommer til at være en kilde til en konstant strøm af utryghed".

Fremtiden vil for Christian Wernberg-Tougaard blive endnu mere ekstrem. I dag har vi smart-cars, der kan køre og tænke selv. For fremtiden vil vi se dette i endnu højere grad:
"Vi vil eksempelvis se endnu flere smart-cars, men nok også droner og fjernstyrede fly. Det er der en masse fordele i, men kigger vi på det fra et kriminalitetsperspektiv, åbner der sig jo pludselig en masse muligheder for de kriminelle. Mulighederne for snyd, manipulation og svindel med digitale værktøjer kommer til at eksplodere. Hvis du eksempelvis bliver i stand til at tage kontrollen over en personbil, kan du bruge det som afpresning, og vi kan jo kun gisne om, hvad man kan bruge kontrollen over et fly til", forklarer han.

DET SVAGESTE LED

Det hyperkonvergerede samfund kommer altså til at have betydning for alle, hvad enten man er offentlig myndighed, privat virksomhed eller borger. Det baner vej for fantastiske muligheder, men det åbner også for en ekstrem sårbarhed, hvis man ikke forstår at passe på sig selv og "låse døren efter sig". Sårbarheden hænger sammen med det svageste led, og ifølge Christian Wernberg-Tougaard er det svageste led den almene borger:
"Der er en ekstrem diskrepans imellem, at man på den ene side kræver, at borgerne er fuldt ud digitalt dannede og kan beskytte sig, mens man på den anden side ingen læring eller støtte yder i forhold til at uddanne os i at være digitale borgere", siger han og understreger, at der ikke findes nogen andre områder, hvor man har så høje forventninger til borgerne uden at uddanne dem.

For at imødekomme denne udfordring, mener Christian Wernberg-Tougaard, at det er alfa omega, at vi begynder at ruste os på fremtiden ved at uddanne borgerne. For når borgeren er det svageste led, som det er tilfældet i øjeblikket, hvor IT-kriminelle ofte nemt kan udnytte og angribe borgerens teknologier, så har det offentlige en særlig forpligtelse i at uddanne borgerne i digital dannelse. Men det er ikke kun det offentliges ansvar. Der skal være en balance mellem borgeransvaret, det offentliges ansvar og producenternes ansvar for at forebygge fremtidens IT-kriminalitet.

HVOR LIGGER ANSVARET?

For Christian Wernberg-Tougaard vil fordelingen af ansvaret i vid udstrækning ligne den fordeling, vi kender i dag. Grundlæggende kommer vi nemlig til at have et fælles ansvar for, at borgeren lærer at låse den digitale dør: "*Som privatperson har du et ansvar for at danne dig en grundviden om den teknologi, du benytter dig af. Og her må vi gerne stille krav til borgerne. Det er eksempelvis en god idé at læse brugsanvisningen til dit nye webcam, før du bruger det. Omvendt har producenten et ansvar i produktudviklingen i forhold til at udbyde et sikkert produkt og leve op til minimumskravene, mens det er de offentlige myndigheder, der må stille minimumskravene til producenterne og definere det sikkerhedsansvar, de skal leve op til",* fortæller han.

VI SKAL GØRE OS BEKENDTE MED DEN DIGITALE VIRKELIGHED

Som borgere har vi altså selv et ansvar for vores digitale sikkerhed, og til dette formål peger Christian Wernberg-Tougaard på tre relativt simple forholdsregler, som også rækker ind i fremtiden:

1. Gør dig bekendt med den teknologi, du anvender: Forstå, hvad den kan, og hvordan du er beskyttet. For fremtiden kommer vi til at opleve en flodbølge af teknologier, vi kan drage stor nytte af, og vi bliver som borgere nødt til at tage ansvar for at lære disse teknologer at kende.
2. Gør, som du ville have gjort, hvis personen stod over for dig. Som mennesker er vi i stand til afkode andre mennesker, når vi står over for dem. Vi kan afgøre, om vi har tillid til dem eller ej, men den samme form for tilstedeværelse kan være svær at etablere i den digitale verden. Overvej derfor altid, om du ville handle på samme måde i den virkelige verden, som du gør i den digitale.
3. Som forælder skal du kunne tage ansvar for at opdrage og hjælpe dine børn med at forstå og navigere i den digitale verden. Har du ikke den fornødne viden, er det dit ansvar at skaffe den.

Afslutningsvis pointerer Christian Wernberg-Tougaard, at vi skal huske på, at vi lige nu befinder os i en transformationsfase. Som samfund har vi endnu ikke etableret en fuldendt forståelse for, hvad det vil sige at være digital borger i et digitalt samfund. Og det er også helt forståeligt: "*Modsat den analoge virkelighed, som har eksisteret i millioner af år, har vi kun levet med de her teknologier i 20 år*", siger han og uddyber, at Danmark trods alt er på vej i den rigtige retning: "*Vi har en enorm høj grad af adaption, hvilket vil sige, at vi er rigtig gode brugere af de digitale muligheder. Men der er brug for, at vi opbygger en forståelse for den digitale virkelighed. Vi bliver nødt til at have respekt for den læringskurve, der er i at gå fra det analoge til det digitale samfund, og uddannelse vil gøre os i stand til at øge samfundets robusthed over for IT-kriminelle, og her kan vi i Danmark gribe muligheden for at blive foregangsland*".

VINCENT F. HENDRICKS, PROFESSOR I FORMEL FILOSOFI, DR.PHIL., PH.D., KØBENHAVNS UNIVERSITET.
LEDER FOR CENTER FOR INFORMATION OG BOBLESTUDIER (CIBS), KØBENHAVNS UNIVERSITET.

TILLID I EN DIGITAL VIRKELIGHED

SAMFUNDSDEBATTØR OG PROFESSOR VINCENT HENDRICKS REFLEKTERER OVER BEHOVET FOR DIGITAL DANNELSE I ET ONLINE DEMOKRATISK SAMFUND. SOCIALE MEKANISMER SOM TILLID OG BLUFÆRDIGHED ER NEMLIG AFGØRENDE I DEN DIGITALE VIRKELIGHED, LIGESOM I DEN ANALOGE VERDEN. DET GÆLDER IKKE MINDST I FOREBYGGELSEN AF IT-KRIMINALITET, HVOR ALLE SKAL TAGE ET AKTIVT ANSVAR.

Den forståelse af demokrati, vi abonnerer på i dag, er en, der har rod i oplysningstiden, hvor netop viden, indsigt og visdom blev hyldet som hjørnesten i en stabil samfundsorden og grundpiller i et demokrati baseret på frihed, lighed og broderskab. Præcis vores demokratiske samfundsordens vartegn og primære bindemiddel - tillid - er samtidig også denne ordens største svaghed. Uden tillid mellem borgerne, tillid til de folkevalgte, tillid til, at der ikke foregår korruption i system og forretning, og tillid til at der opretholdes lov og orden, ville det være overordentligt svært at opretholde et samfundssystem. Et samfundssystem, hvor den enkelte borgers selvstændighed, individuelle behov og beslutninger respekteres, samtidig med at alle andre borgeres ditto er afstemt. Demokrati er altså en stor og meget kompliceret koordinationsøvelse, og information er hovedstolen i dette koordinationsspil. Uden information, ingen koordination, og uden koordination, intet demokrati.

Med information kan man oplyse, men tager vi udgangspunkt i IT-kriminalitet, kan man ligeledes udnytte information og manipulere med mennesker, meninger og markeder, hvis man kan styre informationsindholdet og de kanaler, hvorigennem information transmitteres. Og hvad betyder det så for det fælles bindemiddel, tilliden?

Internettet har åbnet nye platforme og muligheder for at finde meningsfæller. Men det er også ganske let at polarisere. På den måde kan en gruppe forskyde sig mod et standpunkt, der er mere ekstremt eller radikalt end det, de enkelte medlemmer selv ville være villige til at abonnere på. Denne mekanisme kaldes polarisering, og polarisering kan lede til ekstremisme, hvad enten det er i politisk, religiøs eller social forstand. Hvis der er noget, som demokratier har vist sig at være relativt sensible over for, så er det præcis ekstremisme og radikalisering. Fra tid til anden kan informationsteknologi og sociale medier være med til at stimulere sådanne tendenser og få dem til at antage dimensioner og en rækkevidde, der aldrig er set før – og nu med lysets hast i bogstaveligste forstand. Hverken ekstremisme eller radikalisering er nævneværdigt tillidsskabende.

“LÆGGER MAN PERSONLIGE OPLYSNINGER, BILLEDER, MATERIALE UD OG OP, SÅ ER DET IKKE LÆNGERE DINE, OG ANDRE KAN POTENTIELT FÅ FAT I DEM, OG HVAD DERTIL KAN HØRE. DET KAN MÅSKE BETALE SIG AT VÆRE EN SMULE BLUFÆRDIG PÅ NETTET, SOM MAN OGSÅ TIT ER DET ANALOGT - DET KAN FAKTISK BESKYTTE ÉN IKKE AT VÆRE FOR FLAMBOYANT ONLINE”.

“AT REGULERE NETTET BLIVER NOK SVÆRT, SÅ EN DEL REGULERING KOMMER SÅLEDES TIL AT LIGGE HOS BRUGERNE OG DERES REFLEKTEREDE OMGANG I EN DIGITAL VIRKELIGHED SOM SUPPLEMENT TIL DEN ANALOGE. SOM MENNESKER ER VI OGSÅ SOCIALE DYR, SÅ VI ER IKKE UPÅVIRKELIGE OVER FOR, HVAD ANDRE MENER OM OS. SOCIALE SANKTIONER MOD DEM, DER FORBRYDER SIG MOD, HVAD MAN KAN TILLADE SIG, VIRKER OFTE BEDRE END FORBUD”.

Tilsvarende kan der med lyshastighed dannes meningsbobler, hvor alle angiveligeligt mener det samme om alt fra #marius, #voteman til "Vestager: Sådan er det jo", politiske bobler om "Fattig-Carina", "Dovne-Robert", "Panoramagate" eller "Frikadeller i børnehaven". At vi alle har fået en megafon til offentligheden og kan afgive vores mening, til tider reflekteret og andre gange som lemminger, betyder heller ikke med bydende nødvendighed, at vi er blevet mere oplyste eller tager bedre beslutninger. Specielt ikke, hvis vi i øvrigt er i tvivl, mens vi afgiver vores mening. Og den enkelte "synes godt om", "upvote", kommentar eller anden online-gestus er ligegyldig: Det er mængden af aggregerede "synes godt om", "upvotes" eller kommentarer, der pludselig kan udgøre et meget kraftigt signal om, hvad der antageligvis er det rigtige at mene, synes og gøre. Og det kan videre få horder til at blive tilskuere, lemminger eller hoppe med på vognen af uhyrligheder – fra digital mobning, smædekampagner, shitstorms og rygtedannelse til dårlige aktieinvesteringer og køb af dubiøse finansprodukter, der kan ryste markeder. Intet af dette er synderlig tillidsskabende, og faktisk kan det være potentielt demokratiundergravende, hvis det blæses op i storskala.

Kriminalitet er heller ikke tillidsskabende – og IT-kriminalitet til lands, til vands og i luften, blandt frænder og fjender i sociale netværk, lokalt og globalt, og med høj-potent hastighed, ja, den lader vi stå et øjeblik sammen med hacking, phishing, malware, oddjobs, identitetstyverier og hævntogter.

HVAD KAN BORGERNE GØRE?

Hvad kan der gøres? For det første skal man nok gøre sig klart, at vi med internettet, informationsteknologi og sociale medier har fået tilføjet en digital virkelighed, som er forbundet med den analoge. Men eftersom vores erfaringshorisont med den digitale virkelighed er lille (Facebook har eksempelvis lige haft tiårsjubilæum), —så daterer vores erfaring omvendt med den analoge virkelighed cirka 250.000 år tilbage – så længe vi har været mennesker. Derfor er det også forventeligt, at der er en del "børnesygdomme" forbundet med at forstå den digitale virkelighed, og hvordan man skal gebærde sig i den, og forstå, hvordan den præcist er forbundet med den virkelighed, vi kender så godt.

Ikke desto mindre er der et par forholdsregler, man kan tage som bruger og borger. Størstedelen af, hvad du tror, er dit på nettet, er ikke dit. Eksempelvis tilhører din profil udbyderen af den sociale platform, som ejer alt, hvad der før var dit: Tekster, billeder, likes, upvotes, netværk. Udbyderen leverer serverpladsen, skaber infrastrukturen, styrer trafikken, bestemmer, hvilken skabelon du kan præsentere dig selv i, og i sidste ende hvad brugeren kan tillade sig at præsentere, hvordan og ikke mindst for hvem. Det betyder, at lægger man personlige oplysninger, billeder, materiale ud og op, så er det ikke længere dine, og andre kan potentielt få fat i dem, og hvad dertil kan høre. Det kan måske betale sig at være en smule blufærdig på nettet, som man også tit er det analogt – det kan faktisk beskytte en ikke at være for flamboyant online.

Meningstilkendegivelser på nettet kan være forpligtende på samme måde, som de er det ved middagsbordet eller i det fysisk offentlige rum, selvom "synes godt om", "upvotes", kommentarer og "selfies" kan synes som omkostningsneutrale investeringer. Det interessante er ikke, at du synes godt om, men hvorfor og ikke mindst også, hvorfor andre skulle følge dig i din mening. Det kræver refleksion, overvejelse og argumenter. Og sandsynligheden for, at du falder for tilskuereffekter, lemmingeffekter eller hopper med på vognen, falder drastisk i takt med, hvor meget du tænker dig om.

At regulere nettet bliver nok svært, så en del regulering kommer således til at ligge hos brugerne og deres reflekterede omgang i en digital virkelighed som supplement til den analoge. Som mennesker er vi også sociale dyr, så vi er ikke upåvirkelige over for, hvad andre mener om os. Sociale sanktioner mod dem, der forbryder sig mod, hvad man kan tillade sig, virker ofte bedre end forbud. At forebygge IT-kriminalitet er et kompliceret strukturelt problem: Hvis jeg alene forsøger at regulere, så batter det ikke noget, så hvorfor skulle jeg? Hvis alle andre forsøger at regulere, hvorfor skulle jeg så? Det faktum, at jeg giver den gas, troller, snyder, bedrager, hopper med på vogne, hvis alle andre opfører sig ordentligt, betyder jo ikke noget. Sådan tænker jeg, sådan tænker alle andre, og så ender det med, at intet bliver gjort. Dette strukturelle problem kender man som fangernes dilemma.

Vi bliver alle nødt til at tage et aktivt ansvar for, at vi ikke ender i fangernes dilemma, når det gælder IT-kriminalitet – og anden kriminalitet for den sags skyld. Kriminalitet og tillid er en cocktail, der blandes meget dårligt, og uden tillid så glem koordination, og skyd så en hvid pil efter demokratiet.

NÅR FORBRYDELSER BLIVER DIGITALE
ORDBOG

Kapitel 6

ORDBOG

Antivirusprogram er et program, der kan opfange og blokere vira på din computer, inden de kan nå at gøre skade på computeren. Der findes både gratis antivirusprogrammer og programmer, som man kan købe.

APT-angreb (Advances Persistent Threat) er målrettede og langvarige angreb, der har til formål at trænge ind i et netværk ofte med henblik på spionage. APT-angreb består af flere faser og er baseret på forudgående research om målet for angrebet.

Big Data er et begreb, som overordnet betyder indsamling og analyse af enorme mængder data, blandt andet med det formål at kunne finde nye sammenhænge (korrelationer) og tendenser. Big data kan eksempelvis bruges af virksomheder og myndigheder til at få en bedre forståelse af kunde- og borgeradfærd og af præferencer.

Bitcoin er en virtuel valuta, som hverken er reguleret af nationale eller internationale regler. Bitcoin er kendetegnet ved, at overførslen sker direkte mellem afsender og modtager, således at det ikke er nødvendigt med et mellemled som eksempelvis en bank. Herudover er Bitcoin kendt for, at transaktioner kan ske anonymt.

Et **botnet** er et netværk af computere inficeret med malware, som gør det muligt for en person at kontrollere computerne. Botnets kan bestå af flere tusinde computere og kan for eksempel bruges til at foretage overbelastningsangreb på hjemmesider (se DDos-angreb) eller til at sende spam-beskeder.

Cloud-computing eller *skyen* er et begreb, der dækker over computerprogrammer med videre, som ikke installeres lokalt (eksempelvis på ens egen computer), men derimod befinder sig på en ekstern server, der kan tilgås via internettet. Programmer og tjenester som Facebook, Spotify eller Gmail er eksempler på dette.

Computervirus er et program, som kan skade andre programmer. Virusprogrammer kan for eksempel slette vigtige data eller programfiler på den inficerede computer. En computervirus skal aktiveres manuelt, ved at brugeren for eksempel åbner en fil, som vedkommende har tillid til.

Crime-as-a-Service er et begreb, der henviser til, at IT-kriminalitet også kan være en serviceydelse, hvor gerningsmanden alene sælger sin viden/evner, men ikke selv har en selvstændig interesse i målet. Ikke IT-kyndige personer har således mulighed for at købe de nødvendige serviceydelser for at kunne begå alvorlige IT-forbrydelser, såsom hackerangreb, betalingskortmisbrug med videre.

Darknet er den del af internettet, hvor det kræver særlige programmer for at kunne navigere rundt. Det er således ikke muligt at anvende en almindelig browser som Internet Explorer eller en søgemaskine som Google til at tilgå Darknet. Det særlige ved Darknet er, at ens færden foregår anonymt. Derfor er denne del af internettet særlig brugbar for personer, som ønsker at kunne kommunikere uden at blive overvåget.

Datingbedrageri er, når en person indleder et virtuelt forhold, og vedkommende eksempelvis lokkes til at overføre penge til rejseudgifter med det formål, at vedkommende kan møde den person, han/hun dater, i virkeligheden. Senere viser det sig dog, at den person, som modtog pengene, er en bedrager, og at forholdet kun var indledt for at franarre offeret penge.

DDos-angreb er en betegnelse for en ondsindet metode til at overbelaste en hjemmeside, så den ikke virker. DDos-angreb udføres ved, at en per-

son, som kontrollerer en masse computere, får dem alle til på én gang og i én uendelighed at forespørge den samme internetadresse med det resultat, at ingen andre kan komme i forbindelse med hjemmesiden. DDoS står for Distributed Denial of Service (distribueret servicenægtelse).

Deep Web er den del af internettet, hvor hjemmesider enten er beskyttet af kodeord eller ikke indeholder de links og kendetegn, der gør dem synlige for internetbaserede søgemaskiner. Hjemmesider kan derfor kun anvendes, hvis man kender den præcise adresse eller har det rette kodeord. I modsætning til Darknet registreres ens internetadfærd dog generelt på Deep Web.

Doxing er en proces, hvor der indsamles informationer om en person eller virksomhed, ofte ved brug af åbne internetkilder så som sociale medier, søgemaskiner, databaser med videre. Formålet med doxing er ofte at "afsløre" anonyme personer.

En **firewall** beskytter mod uønsket adgang til ens private netværk fra et ubeskyttet offentligt netværk. På nogle computere er firewall'en automatisk slået til, når man køber computeren.

Forskudsbedrageri er, når offeret lokkes til at betale et beløb for at kunne modtage et eller andet ønskværdigt. Det kan for eksempel være Nigeriabreve, hvor det potentielle offer anmodes om et pengebeløb til gengæld for senere at modtage en stor arv fra en ukendt person. Det kan også være forudbetaling for at modtage en stor lotterigevinst fra et lotteri, man ikke har deltaget i. Der er også tale om forskudsbedrageri, hvis man lokkes til at overføre penge til en person, man dater i udlandet, men som i virkeligheden er en bedrager (se datingbedrageri). Ved forskudsbedrageri opnår man ikke det, man er blevet lovet, men mister i stedet de overførte penge.

Grooming henviser til børnelokkeri på internettet. Der vil typisk være tale om, at en voksen skaber en form for tillidsrelation til et barn over internettet, for eksempel i et chatforum, med det formål senere at forgribe sig seksuelt på barnet.

Hævnporno (revenge porn) er, når materiale (ofte billeder eller film) med seksuelt indhold deles på internettet uden tilladelse fra personen, der optræder på billedet/filmen. Hævnporno udføres ofte af ekskærester, der deler privat seksuelt materiale på internettet eksempelvis som hævn for det afbrudte forhold.

Identitetstyveri er, når en persons identitetsoplysninger bliver misbrugt – typisk med henblik på, at gerningspersonen opnår en økonomisk gevinst. Identitetsmisbruget kan for eksempel bestå i, at der optages lån, købes ting eller oprettes abonnementer i offerets navn. De personlige oplysninger kan for eksempel være CPR-nummer, adgangskoder, sundhedsoplysninger eller andre følsomme persondata.

Internet-of-things henviser til det fænomen, at stadig flere genstande får indbygget sensorer og internetadgang, hvilket indebærer, at genstande kan fjernstyres, fjernovervåges og reagere i forhold til omgivelserne. Perspektiverne går lige fra køleskabet, der automatisk bestiller mælk, til "intelligente byer", som på baggrund af sensorer i vand, luft, trafik med videre er i stand til at udnytte byens ressourcer på den mest optimale måde.

En **IP-adresse** (Internet Protokol-adresse) er et unikt nummer som eksempelvis en computer bruger til at kommunikere med en anden computer for at sikre, at kommunikationen mellem de forskellige enheder ikke bliver blandet sammen.

En **keylogger** er et program, der registrerer, hvad der skrives på tastaturet på en computer inficeret med keyloggerprogrammet. Det bruges til at spionere mod brugeren af den inficerede computer oftest med henblik på at opsnappe passwords, kontonumre og andre følsomme oplysninger.

Mainframe er et udtryk for en industriel computer, som blandt andet er karakteriseret ved dens evne til at håndtere store mængder af input, stor driftsikkerhed samt evnen til at køre i lange tidsintervaller uden afbrydelser.

Malware er et skadeligt softwareprogram designet til at ødelægge eller skade data på computere inficeret med det pågældende program. Der findes mange forskellige typer af malware, der opererer på forskellige måder. Eksempler er vira, orme, trojanske heste, keyloggers og ransomware.

Et **Nigeriabrev** er typisk en e-mail fra en ukendt person, som har til formål at få modtageren til at overføre et mindre beløb mod at vedkommende efterfølgende modtager en stor økonomisk genvist – enten i form af en lotterigevinst, en arv fra et ukendt familiemedlem, et godt forretningstilbud eller et større beløb som tak for, at man har hjulpet en person med eksempelvis at smugle guld eller kontanter ud af et afrikansk land. Svindlen består i, at offeret aldrig modtager den lovede gevinst, men derimod blot mister de penge, vedkommende har overført.

En **orm** minder om en computervirus, men til forskel fra en virus kan en orm sprede sig fra computer til computer automatisk. En orm skal dermed ikke aktiveres af en person for at kunne inficere en computer og skabe ødelæggelser og funktionsforstyrrelser.

Pharming er en metode til typisk at stjæle person- eller betalingskortoplysninger ved at oprette en falsk hjemmeside, som kan forveksles med ægte hjemmesider. Svindlere kan eksempelvis oprette en fup-butik, hvor den uvidende forbruger indtaster kreditkortoplysninger i forbindelse med et (falsk) køb.

Phishing er en metode, hvor svindlere forsøger at narre internetbrugere til at oplyse brugernavn, adgangskode, kreditkort- eller netbanksoplysninger med videre. Brugeren får tilsendt en e-mail, hvor afsenderen tilsyneladende er en virksomhed, som man generelt har tillid til, eksempelvis ens bank, SKAT, en fragtvirksomhed eller lignende. I mailen opfordres modtageren til at indsende oplysningerne per e-mail eller logge ind på en falsk internetside, der til forveksling ligner bankens eller SKATs rigtige hjemmeside.

Ransomware er en form for virus, der gør skade på den inficerede computer ved at kryptere og dermed spærre brugerens data. Herefter modtager offeret en meddelelse om, at vedkommende kun kan få sine data frigjort, hvis vedkommende betaler en løsesum (løsesum = ransom).

Sexafpresning (sextortion) er når gerningspersonen har skaffet sig adgang til seksuelle billeder eller lignende af offeret, som bruges til at true offeret til enten at sende flere billeder eller til at betale et pengebeløb, hvis offeret vil undgå, at billederne offentliggøres.

Sexting henviser til det at sende seksuelt udfordrende beskeder, billeder eller videoer over en mobiltelefon.

Hjemmesiden **Silk Road** var det mest kendte onlinemarked for illegale produkter. Hjemmesiden – som befandt sig på den mørke del af nettet (Darknet) – kan sammenlignes med "Amazon.com" eller "eBay" blot for narkotika med videre. Silk Road blev lukket i 2013 af FBI, men der findes i dag talrige lignende sider på nettet.

Smishing er det samme som *phishing*, men i stedet for at forsøge at franarre oplysninger via e-mail, sker henvendelsen via SMS.

Spear phishing er det samme som *phishing*, men er mere målrettet. I stedet for at sende en generisk mail til en masse forskellige ukendte personer, så udvælger den kriminelle sig ved spear phishing et enkelt mål og anvender troværdige oplysninger ved eksempelvis at udgive sig for at være en eksisterende samarbejdspartner eller ved bruge ens korrekte navn og titel.

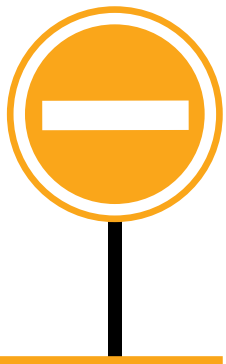
Spyware er et program, som indsamler oplysninger om brugerens aktiviteter på internettet, hvilke hjemmesider man besøger, og hvilke søgeord, man anvender. Disse oplysninger sendes derefter tilbage til personen, der står bag programmet.

TOR-netværket (The Onion Router network) er et gratis computerprogram, som gør det muligt at koble sig på Tor-netværket. Programmet anonymiserer dels brugerens digitale "fingeraftryk" og giver dels adgang til den skjulte del af internettet (Deep Web og Darknet).

En **trojansk hest** er et skadeligt computerprogram (malware), der er gemt i et softwareprogram, som virker godartet, så offeret narres til at downloade programmet.

Et **watering hole-angreb** henviser til den situation, hvor en bruger besøger en legitim hjemmeside, som er blevet inficeret med en skadelig kode, der aktiveres, hvis IP-adressen på den besøgende bruger tilhører den "rigtige" virksomhed. Andre besøgende på hjemmesiden bliver ikke angrebet.

En **Zero-day** er et udtryk for et opdaget sikkerhedshul i et computerprogram, som er ukendt for producenten. Udtrykket kommer af, at producenten ikke har tid til (zero-day) at forebygge eller at reducere skadevirkninger ved et angreb.



GODE RÅD

3 simple råd – som kan beskytte dig i hverdagen

- Tjek jævnligt din netbank for, om der er posteringer (også småbeløb), du ikke kender til.
- Lad være med at åbne links, filer eller dokumenter i mails, med mindre du har fuld tillid til afsenderen, og mailen ikke virker mistænkelig.
- Lad være med at oplyse personlige oplysninger (kortoplysninger, kontooplysninger eller passwords og lignende) i mails. Ingen reelle virksomheder eller myndigheder anmoder om disse oplysninger over mail eller sms.

Hvis du vil gøre mere, så kan du følge disse gode råd:

- Tjek om forbindelsen er sikker, før du køber ting på nettet. Når du betaler, skal der være et hængelåslogo eller stå "https" i browserens adressefelt (URL'en). Eksempelvis: https://www.dkr.dk
- Tag en backup af dine vigtigste billeder og dokumenter. Du kan eksempelvis gemme dem på en USB-stick eller anvende en cloud-service. Så er du mindre sårbar for at miste dem enten ved et uheld eller ved kriminelle handlinger.
- Hvis dine identitetsoplysninger er blevet misbrugt, er det vigtigt straks at kontakte kreditor og oplyse, at du har været udsat for identitetstyveri og derfor ikke ønsker at betale regningen.
- Undlad at handle i webbutiker med mange sprogfejl og "skæve" priser.
- Brug ikke samme kodeord til forskellige konti. Et godt password består af mindst 8 tegn (store og små tegn, tal og specialtegn). Der findes forskellige app's og programmer, som kan hjælpe med at finde på og administrere dine kodeord. Søg efter "password management".
- Husk at opdatere alle dine programmer på din computer.
- Husk at indstille privatlivsindstillingerne på Facebook og på andre sociale medier, så du ved, hvem der har adgang til din profil.

GODE RÅD TIL FORÆLDRE

- Tal med dine børn om deres online liv. Selv hvis du ikke kender den nyeste app eller nyeste chatplatform, kan du sagtens have en generel snak om god og sikker adfærd på internettet.
- Sørg for at orientere dig på de internetsider, som dine børn færdes på, og få gerne dine børn til at vise dig rundt på siderne og forklare dig om dem.
- Husk at lytte, hvis dine børn fortæller om oplevelser, de har haft på nettet, og tag dine børns bekymringer alvorligt.
- Hjælp dine børn med at indstille privatlivsindstillingerne på Facebook og på andre sociale medier, så deres profil er lukket, og så det kun er deres venner, der kan se deres opslag, billeder og så videre.

GODE RÅD TIL BØRN OG UNGE

- Husk, at du kan indstille Facebook og andre sociale medier, så din profil er privat, og så det kun er dine venner, der kan se dine opslag, billeder og så videre. Det er okay at spørge om hjælp.
- Undgå at sende nøgenbilleder eller lignende over mobilen eller internettet. Hvis du sender nøgenbilleder eller lignende af dig selv, er det en god idé, at du ikke kan genkendes på billederne. Eksempelvis kan du tage billedet, så dit ansigt ikke er synligt.
- Tal med dine forældre eller andre, hvis du oplever noget ubehageligt på internettet. De vil kunne hjælpe dig. Måske kan du samtidig hjælpe med at forhindre, at andre bliver udsat for det samme.
- Spørg dine forældre til råds, når du handler på internettet – særligt hvis du køber ting uden for Europa.