CYBERCRIME

NÅR KRIMINALITETEN RYKKER ONLINE

DKR

DET KRIMINAL
PRÆVENTIVE RÅD

INDHOLD

HVAD ER 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.

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-ASSISTERETTEDE 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

BETALINGSKORTMISBRUG, NETBANKINDBRUD OG PHISHING

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.

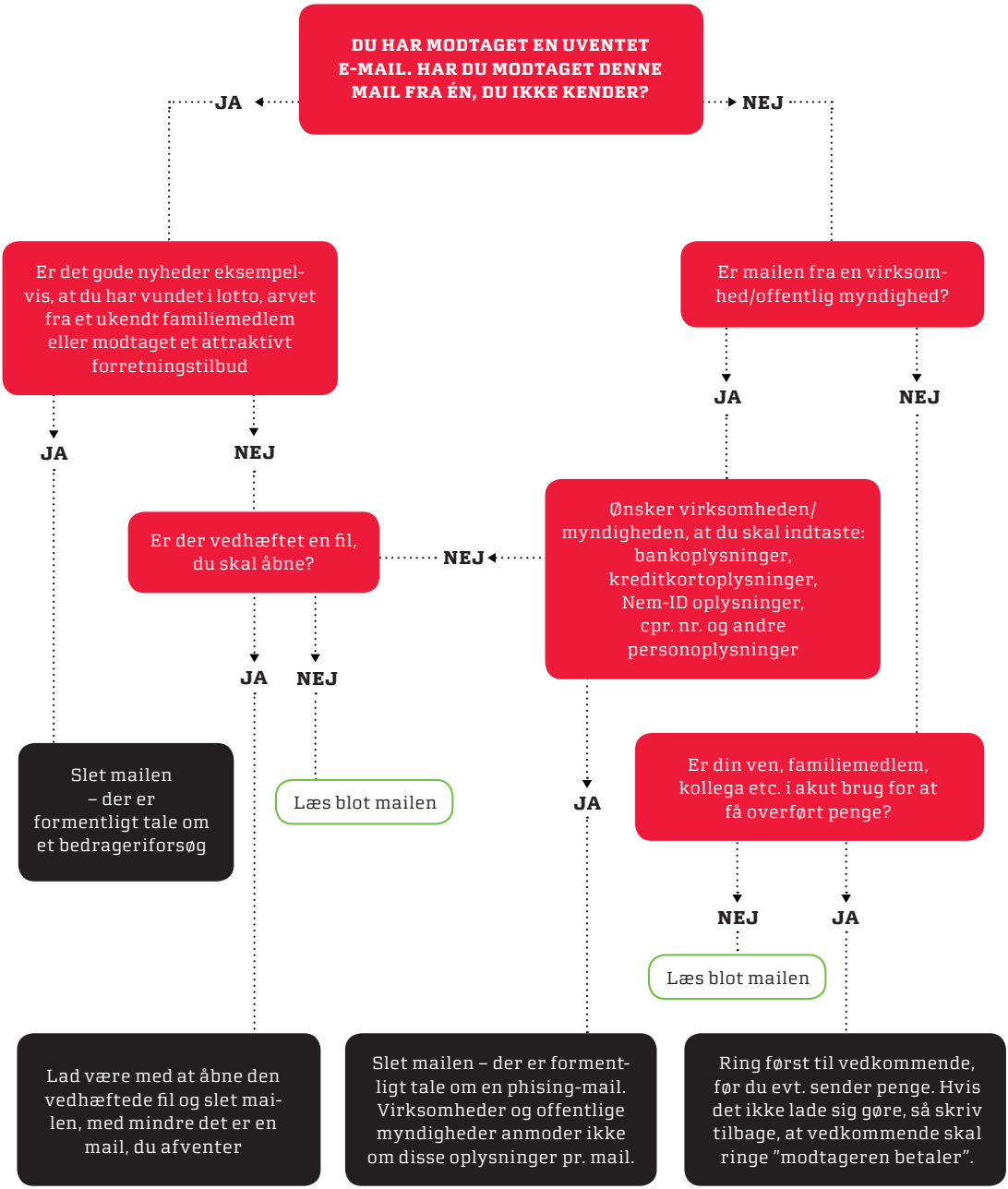
I mange tilfælde skyldes betalingskortmisbruget dog ikke ens egen adfærd, men derimod at den virksomhed, hvor man har brugt sit kort, har for dårlig sikkerhed. Det gælder både køb hos almindelige butikker og køb i internetforretninger. Betalingskortmisbrug kan også hænge sammen med "skimming", hvor kriminelle 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 efterlig-

UNDGÅ BETALINGSKORTMISBRUG 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.

UNDGÅ AT BLIVE SNYDT AF PHISHING-MAILS



ne 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 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.

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.

SÅDAN NEDSÆTTER DU RISIKOEN FOR IDENTITETSTYVERI

- Undlad at opgive personlige oplysninger som fx CPR-nr. 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 fx både CPR-nr. og kontooplysninger og dermed får lettere ved at misbruge din identitet.
- Undlad at smide fysiske breve i skraldespanden, hvor personlige oplysninger, som fx CPR-nr., er synlige. Hvis du vil smide breve ud, kan du fx rive papiret itu eller overstrege de personlige oplysninger.
- Tøm din fysiske postkasse jævnligt, så breve med personlige oplysninger ikke ligger der i længere tid.
- Kontakt dit forsikringsselskab - nogle forsikringsselskaber hjælper dig, hvis din identitet bliver misbrugt.

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.

Selvom mange hvert år udsættes for identitetstyveri, er der heldigvis kun få sager, hvor det har været nødvendigt for ofret at få et nyt CPR-nr.

FUPBUTIKKER PÅ INTERNETTET

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 1.100 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.

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.

UNDGÅ AT BLIVE SNYDT, NÅR DU HANDLER PÅ INTERNETTET

- Undlad at handle i webbutikker med mange sprogfejl og "skæve" priser. Det er ofte udenlandske bedragere, der står bag de falske webbutikker, og de benytter tit computerprogrammer til at oversætte priser og tekst. Tal som 399 kroner eller 149 kroner optræder sjældent på de falske webbutikker, som derimod ofte indeholder skæve priser som fx 531,72 kroner.
- Vær skeptisk, hvis butikken sælger mærkevarer, der er alt for billige. Falske webbutikker sælger ofte internationalt kendte mærkevarer til en pris, der er væsenligt lavere end prisen i andre butikker.
- Undersøg sælgeren. Du kan fx google den webbutik, du overvejer at købe varer fra og undersøge, om der er kontaktoplysninger på sælgeren (fx telefonnummer, adresse og mailadresse). Vær skeptisk, hvis en webbutik, der fremstår professionel, har en mistænkelig mailadresse som kontaktoplysning, dvs. en mailadresse, som ikke er knyttet til virksomheden, men til en privatperson.

Se mere på www.e-mærket.dk.

TAL OG IT-KRIMINALITET

507

INTERNETFUPBUTIKKER BLEV ANMELDT TIL POLITIET I 2015

66

MILL. KR. ER TABT PGA. DANKORTMISBRUG I DK I 2015.

34.400

DANSKERE BLEV UDSAT FOR IDENTITETSTYVERI I 2014

2

PERSONER HAR I 2014 FÅET NYT CPR. NUMMER PGA. IDENTITETSTYVERI.

7

NETBANKINDBRUD I 2015

22.700

DANSKERE BLEV SNYDT I 2014, DA DE HANDLEDE PÅ INTERNETTET.

150.000

DANSKERE BLEV UDSAT FOR DE TYPISKE FORMER FOR IT-KRIMINALITET I 2014

74.400

DANSKERE FIK MISBRUGT DERES BETALINGSKORT I 2014

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 EFTERRETNINGS-TJENESTE – CENTER FOR CYBER-SIKKERHED 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.

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 undersiden "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.

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 penge-overførselsbureauer, 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 kæresteforhold, 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.

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).

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 in

ternettet 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 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. 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 bil-

ledet/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 bru-

gerens 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.

Det Kriminalpræventive Råd
Ejby Industrivej 125 - 135
2600 Glostrup
45 15 36 50
dkr@dkr.dk
www.dkr.dk

Tryk: MercoPrint
Oplag: 500
DKR nr.: 15-401-0377
ISBN: 978-87-92966-37-7
Juni 2016