BILAG 1

Nedenfor ses en oversigt over de personer, du kan henvende dig til for at få information til din artikel.

Person	Titel/arbejde	Tilgængelig
Lisbeth Mærkedahl	Bibliotekar Hovedbiblioteket på Dokk1	Hele tiden
Ladan Hede Jakobsen Nina Marquard	Ofre for Dokk1-hackerne - Har fået hacket sit webcam og er blevet afpresset. - Har fået hacket sin facebookprofil.	Hele tiden
Lau Birk Kristensen	Politikommisær Leder af sektionen for økonomisk kriminalitet, Østjyllands Politi.	Pressemøde i Lille Sal kl. 11.15
Klaus Kristensen	Specialist i it-sikkerhed	Hele tiden
Ulla Malling	Projektchef for Danskernes Digitale Selvforsvar Forbrugerrådet Tænk	Hele tiden

BILAG 2:

PRESSEMEDDELELSE

21. januar 2020

Hovedbiblioteket i Aarhus advarer: Hackere har sendt phishing-mail ud til biblioteksbrugere

I mailen udgiver hackerne sig for at være Hovedbiblioteket og påstår, at brugerne har materialer med overskredet lånetid. Brugerne opfordres til at forny materialerne ved at klikke på det medsendte link, som giver hackerne adgang til brugerens computer.

"Du har 3 lån der er FOR GAMLE!!". Sådan starter en mystisk mail, som et ukendt antal brugere af Hovedbiblioteket i Aarhus har modtaget. Mailen indeholder også et link, der angiveligt leder til en side, hvor brugerne kan forny deres udlån og derved slippe for en bøde. Men i virkeligheden gør linket, at hackerne bag mailen får adgang til brugerens computer.

Mindst to brugere har fulgt linket med uheldige følger, og det er gennem deres henvendelser, at Hovedbiblioteket er blevet opmærksom på problemet. For at undgå, at flere personer falder i hackernes fælde, ønsker Hovedbiblioteket at udbrede kendskabet til phishing-mailen, så brugere hurtigt kan spotte den i deres indbakke. Den afviger nemlig på flere måder fra de mails, Hovedbiblioteket udsender i forbindelse med overskridelse af lånetiden:

- Afsenderen af phishing-mailen er dokk1service@gmail.com. Den rigtige mail er biblioteket@aakb.dk.
- Mailen gør opmærksom på, at man har "for gamle udlån", men lover, at man kan slippe for bøde, hvis man fornyer dem via linket. Men når et udlån først er overskredet, skal der altid betales gebyr.
- Afsenderen har i mailen indsat et foto af Dokk1, hvor Hovedbiblioteket er beliggende.

Hovedbiblioteket har meldt sagen til politiet. Det vides på nuværende tidspunkt ikke, om det kun er brugere af Hovedbiblioteket, der har modtaget phishing-mailen, eller om der er andre fællestræk, der kan pege i retning af gerningsmændene. Hovedbiblioteket hører derfor meget gerne fra alle, der har modtaget phishing-mailen.

Henvendelser herom kan rettes til bibliotekets hovedmail: dokk1-hovedbiblioteket@aarhus.dk.
Skriv "PHISHING" i emnefeltet.

Spørgsmål kan rettes til:
Lisbeth Mærkedahl
T 4185 6654 E lma@aarhus.dk

TEAM VOKSEN
Hovedbiblioteket
Kultur og Borgerservice
Aarhus Kommune

DOKK1

BILAG 3:

OBS: Forældede udlån

HD Hovedbiblioteket Dokk1 <dokk1service@gmail.com>

Til Nina Marquard

Svar | Svar til alle | Videresend | ...

to 02-01-2020 15:06

Kære biblioteksbruger

Du har 3 lån der er FOR GAMLE!! Men du kan stadig undgå at få en bøde hvis du fornyer dine udlån i dag. Klik på dette link for at komme ind på Dokk1s hjemmeside hvor du kan forny dine udlån:

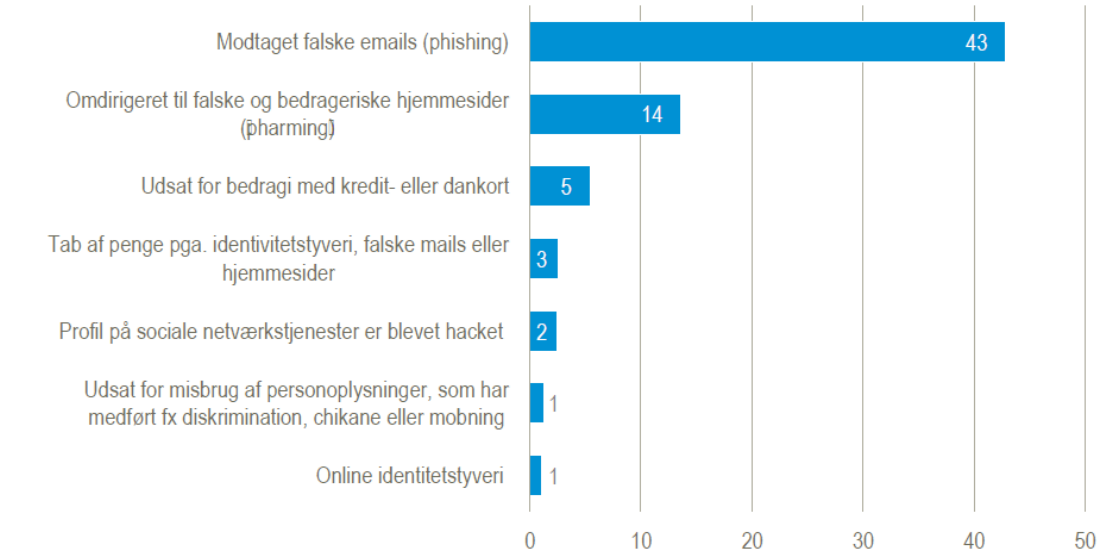
https://dokk1.weebly.com/

Venlig hilsen

Dokk1

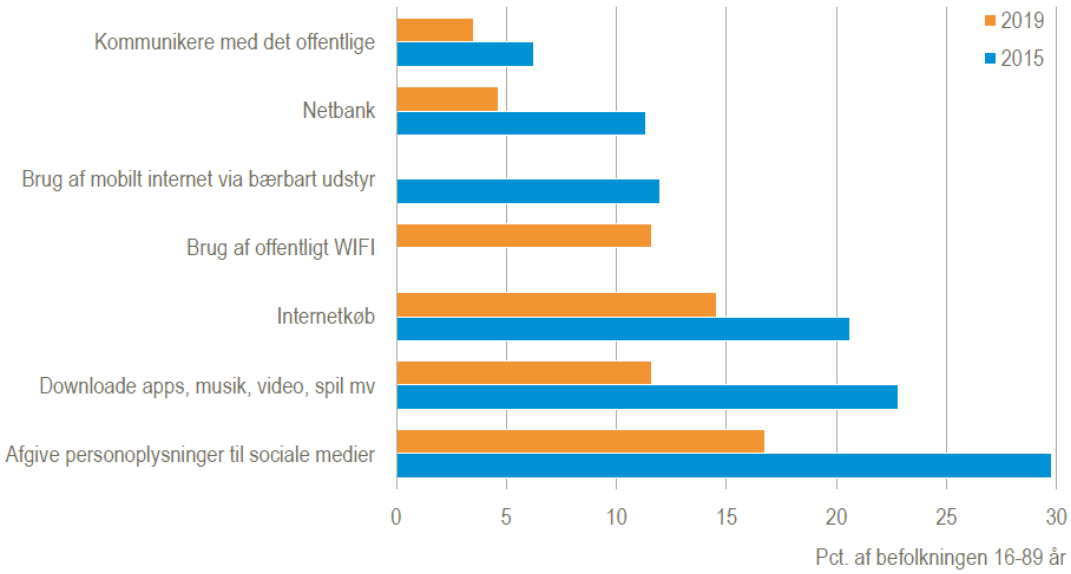
BILAG 4 - DATA FRA DANMARKS STATISTIK:

Oplevet it-kriminalitet i forbindelse med privat brug af internet inden for det seneste år. 2019



Kilde: www.statistikbanken.dk/bebrit19.

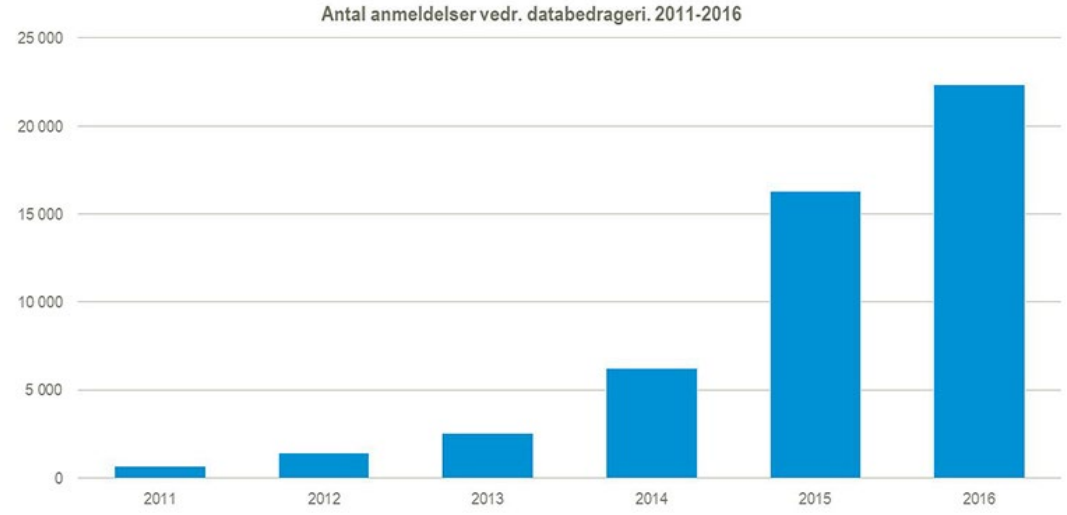
Sikkerhedsbekymringer ved konkrete private aktiviteter på internettet. 2019



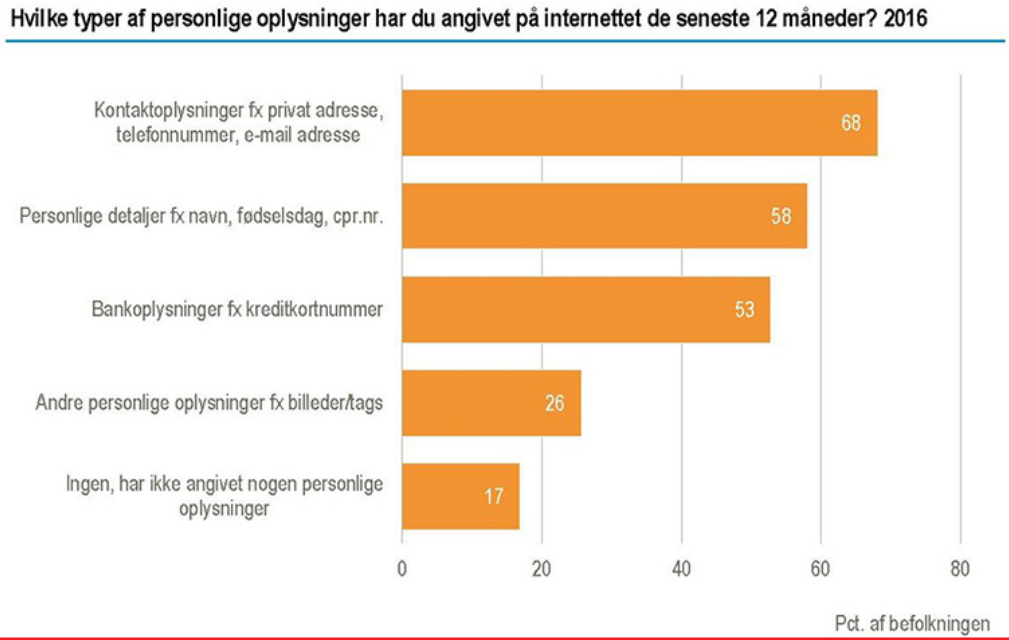
Kilde: Egne beregninger, som ikke kan genfindes i statistikbanken.

Link til originaltekst: kortlink.dk/249ph

Figur 1



Figur 2



Link til originaltekst: kortlink.dk/2446c

BILAG 5 - INTERVIEW MED PROFESSOR I PSYKOLOGI:

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: Det Kriminalpræventive Råd (2015): Angreb og overgreb i cyberspace – hvordan forebygger vi det?