DKR
DET KRIMINAL PRÆVENTIVE RÅD

DIGITAL RISIKOADFÆRD

EN UNDERSØGELSE AF BORGERES DIGITALE RISIKOADFÆRD, IT-KRIMINELLES ADFÆRD OG MYNDIGHEDERS OG VIRKSOMHEDERS ARBEJDE MED AT FOREBYGGE BORGERRETTET IT-KRIMINALITET.

DIGITAL RISIKOADFÆRD

En undersøgelse af borgeres digitale risikoadfærd, it-kriminelles adfærd og myndigheders og virksomheders arbejde med at forebygge borgerrettet it-kriminalitet

København, februar 2021

Gemeinschaft
Dronningensgade 79, st tv
1420 København K
www.gemeinschaft.dk

ISBN: 978-87-92966-65-0
DKR.nr.: 20-123

Denne rapport er udarbejdet for Det Kriminalpræventive Råd i samarbejde med Forbrugerrådet Tænk

DKR
DET KRIMINAL PRÆVENTIVE RÅD

Forbrugerrådet Tænk

INDHOLD

INDLEDNING

SVINDEL MIDT I EN TRAVL HVERDAG

Line trommer utålmodigt med fingrene på bordpladen. Hun har bestilt et par sko, som hun længe har haft kig på, på nettet. De skal indvies i aften, men pakken med skoene lader vente på sig. Line opdaterer sin mail igen og sukker frustreret. Pludselig vibrerer hendes telefon. I beskeden står der: Din pakke 596421-DK venter på levering. Bekræft venligst betalingen (12 kr.). Indtast og bekræft for at modtage din pakke i dag https://track-postdk.com/?n=008462. Endelig! tænker Line og skynder sig at trykke på linket. Line er irriteret over de ekstra 12 kr. i fragt, for hun har allerede betalt for levering. Men det er jo så lidt, og så kan hun have skoene på i aften.

Et andet sted i byen nærmer klokken sig 17. Lars' hjerte hamrer. Han nåede lige metroen, inden dørene smækkede i. Hans søn Gustav hiver ham i ærmet. "Jeg er sulten, far". Lars stryger ham over håret og gennemgår aftenens planer i hovedet. Et smut i Netto efter flåede tomater, hjem og så få gang i aftensmaden, Gustav skal have lusekur, og så kan han lige nå at kigge på noget arbejde. Lars finder sin telefon frem og tjekker sin mail. Yousee har sendt en mail om opdatering af kontooplysninger. Opdateringen skal ske inden for 24 timer, ellers bliver kontoen spærret. Lars skæver op til metroens digitale display. Han kan lige nå det inden Amagerbro. Lars fisker sit dankort frem og begynder at taste. "Næste station Amagerbro", lyder det fra højtaleren. Lars trykker 'bekræft' og skynder sig at hive Gustav med ud af metroen. Han har en mærkelig fornemmelse i maven, da de forlader stationen, men han er ikke sikker på hvorfor.

BAGGRUND

Danmark har et stort udbud af digitale tjenester, som bliver omfavnet af både borgere og virksomheder, og ifølge FN er Danmark verdensmester i digital omstilling.[1] Den digitale omstilling betyder, at danske borgere hver dag gør brug af et stort udbud af digitale tjenester. Fra togbilletten, der bestilles via SMS, over e-mailen, der kan tjekkes nemt og hurtigt på farten, til netbank og e-Boks, hvorfra borgeren på alle tider af døgnet kan overføre penge og modtage henvendelser fra offentlige myndigheder.

Den digitale omstilling tilbyder også danske myndigheder og virksomheder en række gevinster, bl.a. en let og effektiv digital kommunikation med borgere og kunder. Men i takt med udbredelsen af det digitaliserede hverdagsliv stiger både borgeres, myndigheders og virksomheders risiko for at blive svindlet på internettet.

I 2019 oplevede op imod 468.000 borgere at være udsat for kriminalitet begået på internettet.[2] Det er signifikant flere end i 2018, og tendensrapporter peger på, at udviklingen fortsætter de kommende år. Ofre for it-kriminalitet er i særlig grad udsat for misbrug af kortoplysninger, og i den forbindelse er phishing et vigtigt værktøj for it-kriminelle. [3]

En undersøgelse fra 2020 over danskernes informationssikkerhed viser, at 52 pct. af befolkningen mellem 16 og 89 år i 2020 havde oplevet at modtage e-mails med forsøg på phishing. It-kriminelle indtager samtidig nye platforme. 30 pct. har således oplevet svindel via SMS (smishing), mens 21 pct. har oplevet svindel via opkald (vishing) en eller flere gange inden for det seneste år.[4] Derfor skal borgere være på vagt overfor svindel via både e-mail, SMS og opkald, og herudover være opmærksomme på falske hjemmesider, som udgiver sig for at være webshops, falske annoncer på de sociale medier, falske kokurrencer, som høster personlige data, og mange andre svært gennemskuelige forsøg på svindel.

1 UN (2020). United Nations E-Government Survey 2020. United Nations.

2 Pedersen, Anne-Julie Boesen m.fl. (2020). Udsathed for vold og andre former for kriminalitet. Justitsministeriet.

3 Larsen, Henrik m.fl. (2020) Danskernes informationssikkerhed 2020. Digitaliseringsstyrelsen m.fl.

4 Larsen, Henrik m.fl. (2020) Danskernes informationssikkerhed 2020. Digitaliseringsstyrelsen m.fl..

En lang række aktører arbejder allerede med at forebygge it-kriminalitet, der rammer borgere. Men som ovenstående opgørelser indikerer, er der fortsat et stort behov for at klæde danskerne ordentligt på med viden og værktøjer til at modstå it-kriminalitet.

RAPPORTENS FORMÅL

Denne rapport er bestilt af Det Kriminalpræventive Råd i samarbejde med Forbrugerrådet TÆNK. Hovedformålet er at tilvejebringe dybdegående viden om adfærdsmønstre i relation til it-kriminalitet inden for tre indsatsspor; *1) borgere, 2) it-kriminelle og 3) myndigheder og virksomheder.*

Rapporten tager afsæt i, at danske borgere i høj grad har taget myndigheders og virksomheders digitale kommunikation til sig som et effektivt og lettilgængeligt værktøj i hverdagen, og at både borgere, myndigheder og virksomheder har stor gavn af dette. Rapporten understreger samtidig, at trods borgernes opmærksomhed på risikoen for it-kriminalitet, der følger med den udbredte digitalisering, skaber den digitale kommunikation utilsigtet en mulighed for, at it-kriminelle kan svindle borgere. Undervejs fremlægger rapporten analyser af, hvordan it-kriminelle udnytter den digitale kommunikation, samt hvilke tiltag borgere, myndigheder og virksomheder gør brug af i forsøget på at forebygge phishing.

Den tilvejebragte viden skal bidrage til at identificere og igangsætte kompetenceudviklende og adfærdsændrende initiativer, som kan give borgere, virksomheder, myndigheder m.fl. en reflekteret forståelse af handlemuligheder og konsekvenser i forbindelse med phishing. Videnindsamlingen skal dermed inspirere til nye måder at adressere og håndtere it-kriminalitet på. Det overordnede sigte med analysen er således at mindske antallet af danskere, der bliver svindlet via it-kriminalitet.

Rapporten giver et opdateret og nuanceret videngrundlag, der kan kvalificere fremtidige indsatser og sikre, at nye initiativer adresserer relevante udfordringer med den tilsigtede effekt. Rapporten henvender sig til fagprofessionelle, der arbejder med forebyggelse af økonomisk it-kriminalitet.

OM RAPPORTEN

Rapporten er udarbejdet på baggrund af danske og internationale studier af it-kriminalitet og en antropologisk undersøgelse. Undersøgelsen er gennemført ved interviews med borgere, tidligere it-kriminelle, repræsentanter fra politi, virksomheder og myndigheder og forskere. Samlet set baseres undersøgelsen både på kvalitative og kvantitative data. Den kvalitative analyse skal således ikke ses alene, men som et supplement til og en nuancering af den kvantitative viden.

Rapporten består af fire kapitler. Første kapitel beskriver borgeres digitale risikoadfærd. Herefter følger rapportens andet kapitel, der kortlægger, hvordan it-kriminelle udnytter og efterligner myndigheders og virksomheders digitale kommunikation, når de forsøger at svindle borgere på internettet. Det tredje kapitel analyserer myndigheders og virksomheders adfærd som afsendere af digital kommunikation, herunder virksomheders og myndigheders håndtering af phishing-angreb. Det fjerde og sidste kapitel er en analyse af den gensidige adfærdspåvirkning, der foregår mellem borgere, it-kriminelle, myndigheder og virksomheder. I kapitlet fremlægges også en række perspektiver på det videre arbejde med at skabe kompetenceudviklende og adfærdsændrende initiativer til at styrke borgeres digitale sikkerhed.

Nogle af de myndigheder og virksomheder, der har deltaget i undersøgelsen, optræder anonymt i rapporten, og andre gør ikke.

Borgerne, de tidligere it-kriminelle, repræsentanterne fra politi, virksomheder og myndigheder og forskere takkes for at bidrage med vigtige erfaringer og indsigt til udarbejdelsen af rapporten.

God læselyst!

1

BORGERNES BRUG AF DIGITAL KOMMUNIKATION

Dette kapitel præsenterer borgeres brug af digital kommunikation med særligt fokus på digitaliseringens gevinster og borgernes risikoadfærd i deres digitaliserede hverdag. Kapitlet er baseret på kortlægninger af danskernes informationssikkerhed samt danske og internationale studier af borgeres digitale adfærd. Derudover er kapitlet baseret på interviews med borgere, adfærdsforsker Andreas Lieberoth og analyser af adfærdsekspert Morten Münster.

DIGITALISERINGENS GEVINSTER

I 2020 har FN for anden gang i træk kåret Danmark som det land, der er længst fremme med offentlig digitalisering, og dermed er Danmark ifølge FN fortsat verdensmester i digital omstilling. Det skyldes bl.a., at Danmark har et stort udbud af digitale tjenester, som borgere og virksomheder har taget til sig, og at Danmark har en god balance mellem en effektiv offentlig digitalisering og muligheden for at hjælpe den enkelte borger.[5] Danmark er desuden kendetegnet ved et højt niveau af medmenneskelig tillid, hvilket understøtter en tillidsfuld digital kommunikation mellem borgere og myndigheder og virksomheder. Det høje niveau af tillid medvirker imidlertid til, at mange danskere ikke har den rette skepsis, når de eksempelvis handler på nettet eller modtager en mail med en anmodning om at indtaste personlige oplysninger.

Den digitale omstilling skaber store gevinster for både borgere, virksomheder og den offentlige sektor. Digitale løsninger som Digital Post og selvbetjeningsløsninger giver mulighed for at flytte både finansielle og menneskelige ressourcer fra administrative opgaver til velfærdssamfundets kerneydelser.[6] Og for virksomheder kan en digital omstilling være nøglen til at øge produktiviteten og væksten og skabe nye jobs og vinde tabte jobs tilbage fra udlandet.[7]

Foruden finansielle gevinster skaber digitaliseringen en hurtigere og mere effektiv kommunikation mellem myndigheder, virksomheder og borgere. I den undersøgelse, der er gennemført i forbindelse med udarbejdelse af denne rapport, har myndigheder og virksomheder over en bred kam givet udtryk for, at digital kommunikation er 'den eneste farbare vej'. Lederen af team sociale medier i PostNord forklarer:

> **"Mails og SMS'er har i mange tilfælde erstattet brevet, når vi skal opdatere vores kunder om deres forsendelser. Og det er både vi og vores kunder glade for, da det f.eks. betyder, at man kan få besked om en pakke, man kan hente samme dag på vej hjem fra arbejde. Så i forhold til brugervenlighed, er digital kommunikation det eneste rigtige. Der er dog altid undtagelser, og den digitale kommunikation kan ikke stå alene, så her kommer brevet ind i billedet".**

Den digitale omstilling har således forandret kommunikationen mellem myndigheder, virksomheder og borgere, hvilket myndigheder og virksomheder generelt beskriver som positivt. Flere virksomheder fremhæver f.eks. digital kommunikation og tilstedeværelse på digitale platforme som en integreret del af deres virke og forretningsstrategi.

Risiko for it-kriminalitet

Trods de åbenlyse gevinster ved den digitale omstilling er myndigheder og virksomheder også opmærksomme på, at digital kommunikation skaber en risiko for, at it-kriminelle svindler dem selv og borgere. Flere myndigheder og virksomheder erkender, at de som

5 UN (2020). United Nations E-Government Survey 2020. United Nations.

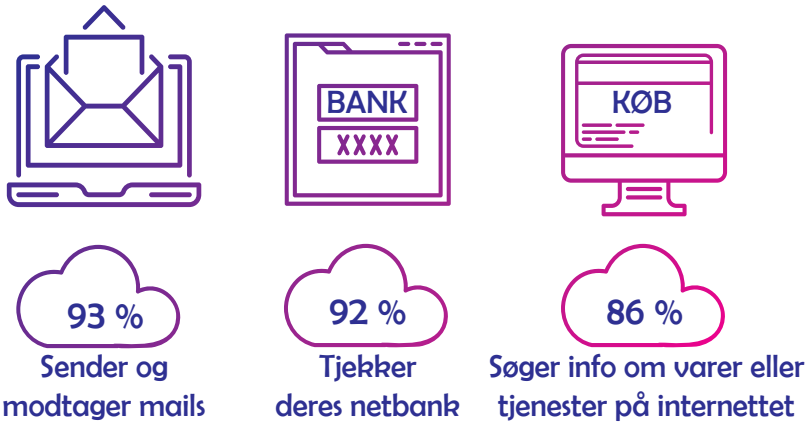
6 Dansk Erhverv (2020). Dansk Erhvervs digitale politik — Vækst gennem digitalisering. Dansk Erhverv.

7 Erhvervsministeriet (2018). Strategi for Danmarks digitale vækst. Erhvervsministeriet.

afsendere af digital kommunikation til borgere har et medansvar for at forebygge, at borgere bliver svindlet af it-kriminelle. Myndigheders og virksomheders håndtering af risikoen for, at it-kriminelle svindler borgere og dem selv, udfoldes i rapportens øvrige kapitler.

BORGERNE HAR TILLID TIL DIGITAL KOMMUNIKATION

Den danske befolkning har i den grad omfavnet den digitale kommunikation. 78 pct. af danske borgere mellem 16 og 89 år logger på internettet flere gange dagligt, 85 pct. finder oplysninger på offentlige myndigheders hjemmesider, og 65 pct. sender oplysninger via myndighedernes digitale selvbetjeningsløsninger. Danskerne bruger i høj grad også digitale løsninger til andet end kommunikation med offentlige myndigheder. [8]



Ud over de mere traditionelle anvendelsesformål bruger danskerne internettet til at kommunikere med hinanden. 80 pct. af danskerne bruger sociale medier, 83 pct. sender meddelelser via Messenger, og 65 pct. har ringet op med lyd- og videoopkald over nettet.[9] Den igangværende Covid-19-pandemi har desuden betydet, at flere borgere arbejder hjemmefra og dermed tilgår arbejdspladsens systemer via fjernadgang. Det ændrede brugsmønster kan gøre det vanskeligt at opretholde arbejdspladsens sædvanlige sikkerhedsforanstaltninger. Det kan f.eks. gælde system- og softwareopdateringer, fravalg af VPN-forbindelse eller flerfaktorgodkendelse.[10]

Borgernes stigende brug af digital kommunikation hænger sammen med, at danskerne generelt har stor tiltro og tillid til hinanden og til den offentlige sektor. For det tillidsfulde forhold 'smitter af' på borgernes brug af digital kommunikation med myndigheder og virksomheder og gør, at borgerne tør sende deres personlige oplysninger til myndigheder og virksomheder.[11] 81 pct. af danskerne har tillid til, at offentlige myndigheder passer godt på deres personlige oplysninger, og 72 pct. oplever, at offentlige myndigheders selvbetjeningsløsninger er overskuelige.[12]

BORGERNE ER OPMÆRKSOMME PÅ RISIKO FOR IT-KRIMINALITET

Nogle danskere har betænkeligheder ved at kommunikere digitalt med myndigheder og virksomheder. I forbindelse med indførelsen af GDPR, har håndtering af persondata og informationssikkerhed fyldt i danskernes bevidsthed. De danske myndigheder udvikler desuden løbende awareness-kampagner målrettet borgere med henblik på at styrke borgeres digitale sikkerhed. I efteråret 2020 lancerede sikkerdigital.dk eksempelvis kampagnen "Et klik kan ændre alt" med fokus på at ruste familier til en mere sikker digital hverdag.[13]

8 Tassy, Agnes m.fl. (2020). It-anvendelse i befolkningen 2020. Danmarks Statistik.

9 Tassy, Agnes m.fl. (2020). It-anvendelse i befolkningen 2020. Danmarks Statistik.

10 CFCS (2020). Trusselsvurdering: Cybertruslen mod Danmark under COVID-19-pandemien. Center for Cybersikkerhed.

11 Digitaliseringsstyrelsen (2016). Et stærkere og mere trygt digitalt samfund. Digitaliseringsstyrelsen.

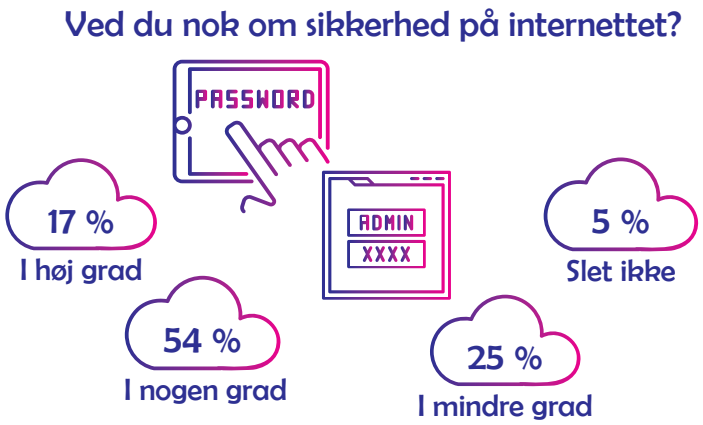
12 Tassy, Agnes m.fl. (2020). It-anvendelse i befolkningen 2020. Danmarks Statistik.

13 Sikkerdigital.dk (2020). Et klik. sikkerdigital.dk 2020.

Den øgede opmærksomhed på digital sikkerhed og myndigheders og virksomheders håndtering af data har muligvis påvirket, at 26 pct. af danskerne oplever, at de personlige oplysninger, de videregiver til offentlige myndigheder, kan havne i "de forkerte hænder", f.eks. på grund af datatyveri. Borgernes bekymring for at blive snydt af it-kriminelle har betydning for deres adfærd på internettet, og de er særligt bekymrede for at blive udsat for it-kriminalitet i forbindelse med onlinekøb, download af apps, musik og øvrige filer samt brug af offentlig wi-fi.[14]

BORGERNES VIDEN OM IT-SIKKERHED

Blot 17 pct. af danskerne vurderer, at de 'i høj grad' ved tilstrækkeligt om sikkerhed på internettet. 54 pct. vurderer, at de 'i nogen grad' ved tilstrækkeligt om sikkerhed på internettet, 25 pct. vurderer, at deres viden 'i mindre grad' er tilstrækkelig, mens 5 pct. vurderer, at de 'slet ikke' ved nok. Særligt danskere over 65 år oplever, at de ikke ved nok om it-sikkerhed. 9 pct. af de 65-74-årige vurderer, at de 'slet ikke' har tilstrækkelig viden om it-sikkerhed, og 12 pct. af de 75-89-årige vurderer det samme.[15]



57 pct. af danskerne lærer om cyber- og informationssikkerhed gennem venner og familie, og særligt kvinder får deres viden om onlinesikkerhed fra nære relationer. Generelt vurderer mænd i højere grad end kvinder, at deres viden om sikkerhed på internettet 'i høj grad' er tilstrækkelig. Det gælder for hver fjerde danske mand, mens hver tiende danske kvinde vurderer det samme.[16] De danske mænds og kvinders egne vurderinger af deres viden om sikkerhed på internettet understøttes af andre undersøgelser, der peger på, at kvinder er mere tilbøjelige til at tro på indholdet i phishing-mails, end mænd er.[17]

Selvom størstedelen af danskerne vurderer, at de blot 'i nogen grad' ved tilstrækkeligt om sikkerhed på internettet, er fem ud af seks borgere bevidste om, at de kan beskytte sig på internettet og mindske risikoen for, at deres oplysninger havner i 'de forkerte hænder', ved at gøre brug af en række sikkerhedsforanstaltninger. Ni ud af ti danskere anvender NemID, og 75 pct. af borgerne er påpasselige med at videregive personlige oplysninger på sociale medier. Derudover tjekker 51 pct. af borgerne sikkerheden på websites, når de skal videregive personlige oplysninger, 62 pct. har slået automatisk opdatering af programmer og systemer til på deres computer, og 32 pct. gør brug af cookie-blokering og anonymitetstjenester.[18]

14 Tassy, Agnes m.fl. (2020). It-anvendelse i befolkningen 2020. Danmarks Statistik.

15 Tassy, Agnes m.fl. (2020). It-anvendelse i befolkningen 2020. Danmarks Statistik.

16 Tassy, Agnes m.fl. (2020). It-anvendelse i befolkningen 2020. Danmarks Statistik.

17 Lian, Tian m.fl. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. ACM Trans. Comput.-Hum. Interact 26(5):1-35.

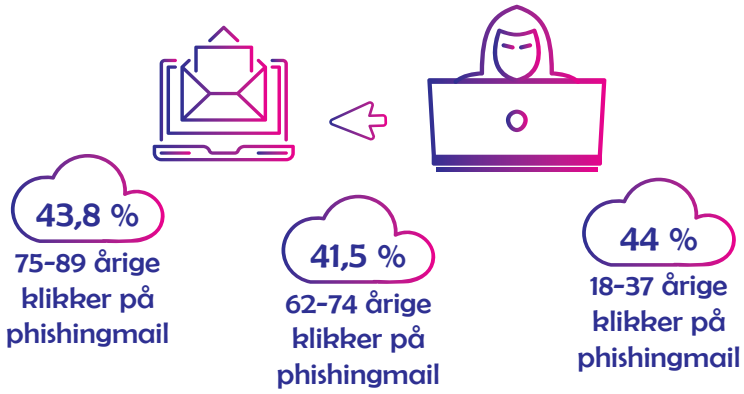
18 Tassy, Agnes m.fl. (2020). It-anvendelse i befolkningen – 2019. Danmarks Statistik.

Sikre passwords
Generelt er borgerne også opmærksomme på vigtigheden af at have et godt password. 75 pct. af danskerne har adgangskoder på mellem seks og ti tegn, og 18 pct. har koder på over 11 tegn. Det er imidlertid stadig i underkanten, for til stærke adgangskoder anbefales mindst 12 karakterer.[19] Og en lang adgangskode er vigtigere end kompleksiteten af adgangskoden.[20]

En foranalyse af danskernes informationssikkerhed peger på, at unge har relativt flere passwords end ældre, men mangler afklaring, ift. hvilket password der skal holdes unikt. Ældre har derimod brug for sikre måder at konstruere og opbevare et mindre antal passwords på. Ældre borgere er dog generelt skeptiske over for password-manager-teknologien og efterspørger muligheden for at opbevare deres passwords fysisk. Unge mellem 18 og 39 år er mere trygge ved password-manager og indstillede på at benytte teknologien.[21]

Blot 17 pct. af borgerne anvender dog password-manager-programmer, og 42 pct. angiver, at de bruger forskellige kodeord til f.eks. mail, NemID mv., mens 37 pct. anvender tofaktorlogin.[22]

Overvurderer egne evner
Det er imidlertid værd at være opmærksom på, at internationale studier viser, at borgere har en tendens til at overvurdere egne evner til at genkende phishing-mails.[23] I en undersøgelse af sammenhængen mellem alder og phishing blev en række simulerede phishing-mails sendt til borgere i aldersgruppen 18-89 år. 43,8 pct. af de 75-89-årige klikkede på et link i den fremsendte phishing-mail. Henholdsvis 41,5 pct. af de 62-74-årige og 44 pct. af de 18-37-årige klikkede ligeledes på det falske link.



Deltagerne i aldersgruppen 18-37 år var imidlertid signifikant mere bevidste om risikoen for at blive udsat for phishing, mens deltagerne fra de to øvrige aldersgrupper angav en lav tilbøjelighed til at tro på indholdet af en phishing-mail.[24] Undersøgelsens resultater understreger risikoen for, at borgeres reelle viden om sikkerhed på internettet er lavere, end de selv vurderer den til at være.

Adfærdsforsker Andreas Lieberoth bekræfter tendensen i disse studier og påpeger, at alle borgere er i risikozonen for at blive svindlet via phishing, fordi mennesker i vidt omfang overvurderer egne evner til at gennemskue svindel. Han forklarer: "Folk tror, de er klogere, end de er. Det er derfor, at de kan snydes. For vi har alle sammen dumme dage". En rådgiver i CFCS fastslår ligeledes: "Alle kan falde i gryden og blive snydt. Det handler ikke om, at man er dummere end andre". Og en medarbejder fra LCIK istemmer: "Uanset hvor ofte vi fortæller borgerne, at de ikke skal udlevere deres personoplysninger, vil det alligevel ske, fordi vi trods alt blot er mennesker, og der kan være mange årsager, når en borger bliver franarret sine oplysninger".

19 Larsen, Henrik m.fl. (2020). DKCERT Trendrapport 2020. DKCERT og DeiC.

20 CFCS (2020) Vejledning Passwordsikkerhed. Center for Cybersikkerhed.

21 Frost, Lasse m.fl. (2017). For-analyse af danskernes informationssikkerhed. /KI.7 m.fl.

22 Larsen, Henrik m.fl. (2020). Danskernes informationssikkerhed 2020. Digitaliseringsstyrelsen m.fl.

23 Ebner, Natalie C., m.fl. (2018). Uncovering Susceptibility Risk to Online Deception in Aging. Journals of Gerontology: Psychological Sciences 00(00): 1-12.

24 Ebner, Natalie C., m.fl. (2018). Uncovering Susceptibility Risk to Online Deception in Aging. Journals of Gerontology: Psychological Sciences 00(00): 1-12.

BORGERNES UHENSIGTSMÆSSIGE ADFÆRD

At der er forskel på borgernes viden om, hvordan de kan beskytte sig imod it-kriminalitet, og deres adfærd – f.eks. at borgerne ved, at det er vigtigt at have et godt password, men at det kun er 42 pct. af borgerne, der vurderer, at deres egne passwords er gode – skyldes ifølge adfærdsekspert Morten Münster, at viden ikke nødvendigvis ændrer adfærd.[25] Med andre ord vil mere viden om phishing i sig selv ikke ændre borgeres digitale adfærd. Borgere vil fortsat genbruge deres passwords, fordi de ikke kan huske lange passwords, og videregive deres personlige oplysninger på sociale medier, selvom de ved, at det er risikofyldt.

Ifølge Morten Münster er det nødvendigt, at der præsenteres konkrete værktøjer til, hvordan man kan følge anbefalinger om f.eks. it-sikkerhed. For hvis en borger blot præsenteres for en række anbefalinger uden sådanne værktøjer, vil resultatet ofte være, at borgeren ikke følger de velmenende anbefalinger.[26] Og dermed vil borgeren fortsat agere uhensigtsmæssigt på internettet.

INGEN FYSISKE FARESIGNALER PÅ NETTET

En fundamental barriere for hensigtsmæssig digital adfærd er den digitale kontekst i sig selv. For mennesket er evolutionært udviklet til at vurdere sikkerhedsrisici på baggrund af fysiske faresignaler, men der er ikke nogen fysiske faresignaler i den digitale verden. Og det gør det vanskeligt for borgere at vurdere, hvornår de er i fare på internettet.[27]

For borgere kan blive udsat for phishing-angreb i situationer, hvor de føler sig trygge og derfor 'har paraderne nede' – f.eks. ved højlys dag i eget hjem, og hvor der ikke er nogen fysiske faresignaler, som kan gøre borgerne opmærksomme på, at der er fare på færde. Til sammenligning vil borgere generelt i langt højere grad være opmærksomme på potentielle risici, hvis de som fodgængere bevæger sig langs en uoplyst, menneskетom gade og pludselig føler sig forfulgt. I sådan en situation vil den mørke gade og manglen på aktivitet fungere som fysiske faresignaler, som gør borgerne opmærksomme på situationens risici, og som giver anledning til at søge væk fra eventuelle farer.

Den menneskelige hukommelse

Når borgere agerer uhensigtsmæssigt på internettet – det vil sige, når de mod bedre vidende anvender korte passwords eller klikker på et link i en mistænkelig mail – skyldes det ifølge en analyse af danskeres informationssikkerhed en række kognitive bias i menneskers tænkning. F.eks. genbruger borgere deres passwords, fordi der er grænser for, hvor meget menneskets hjerne kan huske. Og når borgere skal konstruere og huske et større antal passwords, strækker det hukommelsesevnen til det yderste. Derfor genbruger borgere ofte korte passwords, som er lette at huske, til flere hjemmesider.[28]

25 Münster, Morten Sehested (2017). Jytte fra Marketing er desværre gået for i dag – sådan bruger du adfærdsdesign til at skabe forandringer i den virkelige verden. Gyldendal Business.

26 Münster, Morten Sehested (2017). Jytte fra Marketing er desværre gået for i dag – sådan bruger du adfærdsdesign til at skabe forandringer i den virkelige verden. Gyldendal Business.

27 Frost, Lasse m.fl. (2017). For-analyse af danskernes informationssikkerhed. /Kl.7 m.fl.

28 Frost, Lasse m.fl. (2017). For-analyse af danskernes informationssikkerhed. /Kl.7 m.fl.

I analysen af danskernes informationssikkerhed kortlægges en række psykologiske barrierer for hensigtsmæssig digital adfærd. En af disse psykologiske barrierer er menneskets evne til at genkende mønstre, f.eks. i kommunikationssituationer. Og it-kriminelle misbruger denne evne til mønstergenkendelse ved at præsentere borgere for e-mails i et velkendt design fra en tilsyneladende autoritativ afsender. For det svækker borgernes agtpågivenhed og kan føre til, at borgere videregiver personlige oplysninger på internettet, selvom de er bekendte med de potentielle risici.[29] Gode tilbud, travlhed og tillid til autoriteter er ligeledes faktorer, som it-kriminelle udnytter til at svindle borgere.[30]

Endelig peger analysen på, at mennesker generelt fokuserer på at undgå tab her og nu frem for at opnå gevinster på sigt. Det er en af årsagerne til, at mange borgere ikke tager backup. For sikkerhedskopiering forhindrer først datatab og ransomware-afpresning på sigt og er endda ingen garanti for at undgå tab.[31] I rapportens andet kapitel uddybes det, hvordan it-kriminelle gør brug af disse psykologiske barrierer i menneskers tænkning, når de forsøger at svindle borgere ved hjælp af phishing.

Spamfiltre

Adfærdsforsker Andreas Lieberoth fremhæver mailprogrammers spamfilter som en hjælpende foranstaltning til at undgå uhensigtsmæssig digital adfærd. Han fortæller:

> **"Spamfiltret er jo et 'nudge' på den måde, at der ikke er noget i dit spamfilter, der forhindrer dig i at svare Mr. Thomas, som er advokat i Sydafrika. Men når du kigger på en mail, som er blevet klassificeret som spam af et system, som er klogere end dig, og som er trænet til at opdage de her ting, vil du allerede have paraderne oppe og være mindre tilbøjelig til overhovedet at reagere".**

Forsker og it-sikkerhedsekspert Daniela Oliveira gør imidlertid opmærksom på, at selvom teknologiske løsninger som spamfiltre reducerer antallet af phishing-mails massivt, er disse teknologiske løsninger i sig selv ikke nok. Og det efterlader ifølge Oliveira borgeres personlige vurdering som 'the last line of defense'. It-kriminelle bliver samtidig dygtigere til at udarbejde troværdige phishing-angreb i myndigheders og virksomheders navn, og det stiller yderligere krav til borgeres evne til at skelne illegitime phishing-forsøg fra legitim digital kommunikation.[32] Mange borgere har dog kun begrænset viden om, hvordan f. eks. en usikker hjemmeside ser ud, og hvilke risici en usikker hjemmeside indebærer. Og det vanskeliggør borgeres vurdering af, hvad der er legitim digital kommunikation fra myndigheder og virksomheder, og hvad der er it-kriminelles forsøg på svindel.[33]

BORGERNES TRAVLE HVERDAG

En yderligere årsag til, at det kan være vanskeligt for borgere at skelne mellem myndigheders og virksomheders digitale kommunikation og it-kriminelles phishing-angreb, er, at borgere typisk modtager phishing, imens de er i gang med 'alt muligt andet'.

Som den indledende empiriske vignet til denne rapport illustrerer, modtager borgere phishing, imens de er i gang med hverdagens øvrige gøremål. En phishing-mail kan tikke ind, imens en ung mand venter på sin pakke, en svindler kan ringe til en udmattet forretningskvinde på vej hjem i toget efter en lang arbejdsdag, en annonce med et godt tilbud kan springe en dreng i øjnene, idet han tjekker sin Instagram, og en ældre kvinde kan blive udsat for live-phishing, imens hun forsøger at foretage et køb på internettet. Med andre ord modtager borgere phishing, imens de er i gang med at leve et travlt hverdagsliv, og hvor de ikke nødvendigvis er opmærksomme på risikoen for at blive svindlet på internettet. For svindlen ligner henvendelser, som er helt legitime, og som borgere håndterer digitalt hver eneste dag.

---

29 Frost, Lasse m.fl. (2017). For-analyse af danskernes informationssikkerhed. /KI.7 m.fl.

30 Rajivan, Prashanth og Cleotilde Gonzalez (2018). Creative Persuasion: A Study on Adversarial Behaviors Strategies in Phishing Attacks. Frontiers in Psychology 9(135):1-14. Se desuden Vishwanath, Arun m.fl. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems 51(3):576-586.

31 Frost, Lasse m.fl. (2017). For-analyse af danskernes informationssikkerhed. /KI.7 m.fl

32 Oliveira, Daniela m.fl. (2020). The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behavior Research Methods. 1-11.

33 Frost, Lasse m.fl. (2017). For-analyse af danskernes informationssikkerhed. /KI.7 m.fl.

Og danskernes hverdag er præget af travlhed. I 2018 var danskernes gennemsnitlige ugentlige arbejdstid 37 timer og 59 minutter. Og 37 pct. af danskerne arbejdede mellem 39 og 44 timer om ugen. Derudover brugte de 18-74-årige i gennemsnit 3,2 timer dagligt på indkøb, husarbejde, gør-det-selv-arbejde og børneomsorg. De mange arbejdstimer bidrager til et øget pres og en større udbredelse af stress. I 2018 følte 12 pct. af kvinderne og 9 pct. af mændene sig ofte stressede, mens 47 pct. af kvinderne og 58 pct. af mændene nogle gange følte sig stressede. [34]

Hverdagens travlhed kan dermed også være en væsentlig barriere for danskernes it-sikkerhed og være med til at gøre det vanskeligt for borgere at skelne it-kriminelles phishing-angreb fra myndigheders og virksomheders digitale kommunikation. Ikke mindst fordi borgere hver dag foretager mange legitime interaktioner og transaktioner på internettet, som forløber helt uproblematisk. I et travlt hverdagsliv kan borgere derfor ikke altid skelne den ene phishing-mail, der slap igennem spamfilteret, fra rækken af legitime mails.

ALLE KAN BLIVE OFFER FOR IT-KRIMINALITET

Som det fremgår, er der en række barrierer for, at borgere agerer hensigtsmæssigt på internettet. Og selvom borgere generelt føler sig trygge ved at kommunikere digitalt med myndigheder og virksomheder, er der fortsat udbredt risiko for, at de bliver svindlet på internettet. Og i takt med at flere transaktioner mellem borgere og virksomheder og myndigheder foregår digitalt, bliver it-kriminelles mulighedsrum for at svindle på internettet også større.

Antallet af anmeldelser om it-relateret økonomisk kriminalitet viser også, at mange danskere – desværre – har oplevet at blive svindlet på internettet. I 2019 modtog politiets Landsdækkende center for it-relateret økonomisk kriminalitet (LCIK) knap 27.000 anmeldelser. Samhandelsbedrageri på internettet udgør langt det største sagsområde med 36,9 pct. af anmeldelserne, mens misbrug af kortoplysninger og misbrug af adgang til netbank m.m. udgør henholdsvis 22 pct. og 6,3 pct. [35]

MØRKETAL

En offerundersøgelse peger imidlertid på, at det langtfra er alle, der anmelder it-kriminalitet til politiet, og dermed er antallet af ofre for phishing-angreb forbundet med et betydeligt mørketal. Det skyldes også, at mange ofre ikke er klar over, at it-kriminelle har fået adgang til deres personoplysninger. Borgere bliver typisk først opmærksomme på, at de er blevet udsat for phishing, når der bliver trukket penge fra deres konto, eller når en virksomhed kræver betaling for en vare eller en ydelse, som de ikke har bestilt. Borgere, der opdager, at de er blevet lokket til at indtaste betalingskortoplysninger på en pharming-side eller afgive personoplysninger til en illegitim afsender, kan dermed fejlagtigt tro, at handlingen ikke har konsekvenser. Ved phishing foregår den kriminelle handling og handlingens konsekvenser imidlertid ikke altid synkront. Derfor kan konsekvenserne vise sig med stor forsinkelse, og borgere kan dermed ikke gå ud fra, at forsinket effekt er det samme som ingen effekt.[36]

Adfærdsforsker Andreas Lieberoth beskriver forløbet således:

> **"Omkostningen kan godt ramme flere måneder eller år senere, fordi man ikke er klar over, at nogen har fået fat i ens kode til en hjemmeside, som man har brugt for længe siden. Men hvis man har brugt den samme kode til noget andet, som er mere personfølsomt, så kan det blive problematisk. Det kan også være, at der er blevet lagt et lille stykke malware på ens computer, som bliver styret af nogle andre, som venter på, at du skal dumme dig på et senere tidspunkt".**

34 Bonke, Jens m.fl. (2018). Hvordan bruger danskerne tiden? Gyldendal.

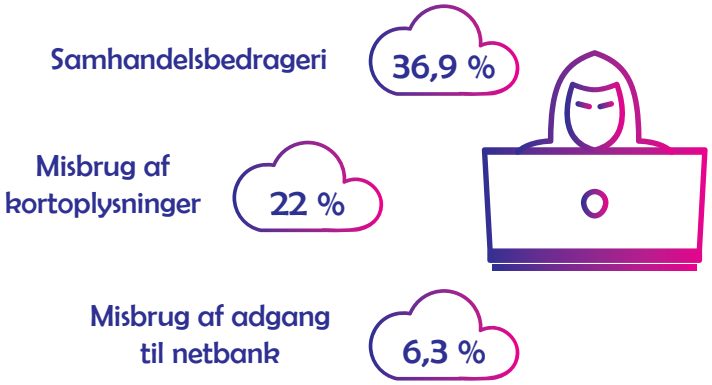
35 Politi (2020). Analyse: Politiet har modtaget knap 27.000 anmeldelser om it-relateret økonomisk kriminalitet i 2019. Rigspolitiet 2020.

36 Kruize, Peter (2019). Identitetsmisbrug belyst fra flere vinkler. Det Kriminalpræventive Råd og Det Juridiske Fakultet, Københavns Universitet.

Et øjebliks uopmærksomhed kan således udnyttes af it-kriminelle og dermed have afgørende betydning for borgeres digitale sikkerhed.[37]

76 pct. af respondenterne i den føromtalte offerundersøgelse, der havde været ofre for økonomisk misbrug, havde ikke anmeldt sagen til politiet. Det på trods af at økonomisk misbrug ofte kræver en politianmeldelse, hvis offeret ønsker at blive kompenseret for sit økonomiske tab.[38]

En kortlægning af it-anvendelse i den danske befolkning viser, at over halvdelen af danskere mellem 16 og 89 år har oplevet én eller flere sikkerhedsproblemer i form af bedrag, hacking, virus eller andre skadelige programmer. 43 pct. angiver at have modtaget phishing-mails inden for det seneste år, og dermed udgør phishing-mails det mest udbredte sikkerhedsproblem. Den næstmest udbredte form for it-kriminalitet er forsøg på at omdirigere internetbrugere til fupbutikker eller andre typer hjemmesider med forfalsket indhold. Det har hver syvende dansker været udsat for.[39] Endelig har hver 20. dansker oplevet misbrug af kredit- eller dankort.



Selvom mange danskere bliver udsat for forsøg på svindel, slipper de fleste med skrækken. I en undersøgelse af danskernes informationssikkerhed svarede 64 pct. af de adspurgte respondenter, at de havde prøvet at modtage phishing, vishing eller smishing.[40]

OPSUMMERING

Den digitale omstilling skaber store gevinster for både borgere, myndigheder og virksomheder, bl.a. en hurtigere kommunikation mellem parterne. Og den danske befolkning har i den grad omfavnet den digitale kommunikation. Det hænger bl.a. sammen med, at danskerne generelt har stor tillid til hinanden og til den offentlige sektor. Og borgerne tør derfor videregive deres personlige oplysninger til myndigheder og virksomheder, fordi de har tillid til, at der bliver passet godt på dem.

Borgerne er samtidig bekymrede for at blive svindlet af it-kriminelle, og det har betydning for deres adfærd på internettet. En væsentlig del af den danske befolkning vurderer, at de kun i nogen grad har tilstrækkelig viden om sikkerhed på internettet, og det kan være med til at gøre det vanskeligt for borgerne at skelne it-kriminelles phishing-angreb fra myndigheders og virksomheders legitime digitale kommunikation. Og alle borgere er i risikozonen for at blive svindlet af phishing, fordi mennesker i vidt omfang overvurderer deres egne evner til at gennemskue svindel på internettet, og fordi phishing-angrebene i stadig højere grad ligner legitime henvendelser.

37 Sikkerdigital.dk (2020). De digitale svindlere kender din adfærd. sikkerdigital.dk 2020.

38 Kruize, Peter (2019). Identitetsmisbrug belyst fra flere vinkler. Det Kriminalpræventive Råd og Det Juridiske Fakultet, Københavns Universitet.

39 Tassy, Agnes m.fl. (2020). It-anvendelse i befolkningen – 2019. Danmarks Statistik.

40 Larsen, Henrik m.fl. (2020). Danskernes informationssikkerhed 2020. Digitaliseringsstyrelsen m.fl.

Med henblik på at undgå, at deres personlige oplysninger havner i 'de forkerte hænder', gør størstedelen af borgerne brug af en række sikkerhedsforanstaltninger. Generelt beskytter borgerne sig dog ikke imod it-kriminalitet i det omfang, som de ved er hensigtsmæssigt. For mere viden ændrer ikke nødvendigvis menneskers adfærd, og det kan være vanskeligt for borgerne at følge gode og velmenende anbefalinger om it-sikkerhed uden konkrete værktøjer til, hvordan de kan gøre det på en nem og overskuelig måde.

Derudover er der en række kognitive bias i menneskers tænkning, som udgør barrierer for, at borgere agerer hensigtsmæssigt på internettet. Og disse kognitive bias udnytter it-kriminelle, når de bruger phishing til at forsøge at svindle borgere. En yderligere barriere for, at borgere agerer hensigtsmæssigt på internettet, er, at borgerne ikke nødvendigvis er opmærksomme på risikoen for at blive svindlet på internettet, når de modtager phishing. For borgere modtager typisk phishing, når de er i gang med 'alt muligt andet', og dermed er hverdagens travlhed en væsentlig barriere for danskernes it-sikkerhed.

2

IT-KRIMINELLES UDNYTTELSE AF DIGITAL KOMMUNIKATION

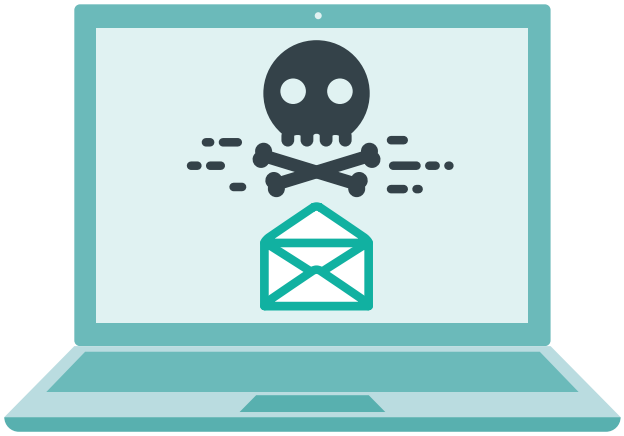
Dette kapitel analyserer, hvordan it-kriminelle udnytter myndigheders og virksomheders digitale kommunikation til at svindle borgere på internettet. Undervejs beskrives fænomenet phishing, og hvordan it-kriminelle bruger phishing til at svindle borgere, myndigheder og virksomheder. Kapitlet er baseret på internationale studier af phishing og it-kriminalitet generelt samt interviews med tidligere it-kriminelle, repræsentanter fra dansk politi, Center for Cybersikkerhed og adfærdsforsker Andreas Lieberoth.

IT-KRIMINELLE UDNYTTER DIGITALISERINGEN

Myndigheders og virksomheders stigende brug af digital kommunikation skaber utilsigtet en mulighed for, at it-kriminelle kan svindle borgere, fordi det giver it-kriminelle mulighed for at efterligne den digitale kommunikation, som myndigheder og virksomheder gør brug af til at kommunikere med borgere.[41]

Internettet giver desuden it-kriminelle mulighed for at foretage svindlen i en størrelsesorden, som vanskeligt kan lade sig gøre ved traditionel kriminalitet. Antallet af potentielle ofre er således langt større ved it-kriminalitet end ved traditionel kriminalitet, fordi it-kriminalitet giver de kriminelle mulighed for at svindle mange på én gang.[42]

En af de måder, hvorpå it-kriminelle kan efterligne myndigheders og virksomheders digitale kommunikation og forsøge at svindle borgere, er ved at udsætte borgere for et phishing-angreb, hvor hensigten er at franarre borgerne deres personlige oplysninger.[43] I de fleste tilfælde tager phishingen form af opportunistiske angreb, hvor it-kriminelle sender en generisk phishing-mail til tusindvis af mailadresser. I andre tilfælde udfører it-kriminelle mere komplekse og målrettede phishing-angreb.[44]



41 Finansministeriet (2018). National strategi for cyber- og informationssikkerhed. Finansministeriet. Se desuden Shulzhenko, Nadiia og Snizhana Romashkin (2020). Internet fraud and transnational organized crime. Juridical Tribune 10(1):162-172.

42 Det Kriminalpræventive Råd (2016). Når forbrydelser bliver digitale – En antologi om IT-kriminalitet og adfærd på nettet. Det Kriminalpræventive Råd.

43 Det Kriminalpræventive Råd (2016). Når forbrydelser bliver digitale – En antologi om IT-kriminalitet og adfærd på nettet. Det Kriminalpræventive Råd.

44 CFCS (2020). Cybertruslen mod Danmark. Center for Cybersikkerhed.

Et typisk phishing-angreb har to komponenter: en indledende e-mail og en forfalsket hjemmeside.[45] I den e-mail, som offeret modtager, forsøger en it-kriminel at lokke vedkommende til at sende personlige oplysninger som betalingskortoplysninger, billeder af NemID eller andre log-in-informationer ved et efterligne myndigheders og virksomheders digitale kommunikation med borgere. Ved hjælp af phishing udnytter it-kriminelle således borgernes tilvænning til digital kommunikation med myndigheder og virksomheder og borgeres generelle tillid til, at det er sikkert at videregive deres personlige oplysninger og foretage køb via myndigheders og virksomheders digitale selvbetjeningsløsninger. Ved mere avancerede former for svindel opretter it-kriminelle pharming-sider, der til forveksling ligner en myndigheds eller virksomheds reelle hjemmeside, og som har til formål at få offeret til at indtaste sine betalingskortoplysninger.[46]

Hvis en borger tilgår den forfalskede hjemmeside, kan den it-kriminelle også foretage såkaldt live-phishing. Her overføres borgerens betalingskortoplysninger til den it-kriminelles server, i samme øjeblik borgeren indtaster sine oplysninger på den forfalskede hjemmeside. Betalingskortoplysningerne kan den it-kriminelle bruge til at foretage et køb med, samtidig med at borgeren forsøger at foretage sit køb. Når borgeren modtager en SMS, der beder om en bekræftelse af købet, er det i virkeligheden den it-kriminelles illegitime køb, som borgeren ender med at bekræfte.

På den måde omgår it-kriminelle den tofaktorgodkendelse, der er designet til at beskytte borgere mod svindel på internettet, og udnytter, at borgerne har vænnet sig til en sikkerhedsprocedure, som de ikke nødvendigvis forstår formålet med. Og dermed kan det være vanskeligt for borgerne at afkode det som svindel. [47]

SOCIAL ENGINEERING

Når it-kriminelle forsøger at svindle borgere ved phishing-angreb, udnytter de dog ikke blot borgeres tilvænning til digital kommunikation med myndigheder og virksomheder. Ifølge forsker og it-sikkerhedsekspert Daniela Oliveira udnytter it-kriminelle også menneskelig adfærd, når de bruger phishing til at lokke borgere til at videregive deres personlige oplysninger. Oliveira beskriver phishing som en form for 'social engineering', som betyder, at it-kriminelle gør brug af psykologisk manipulation, fordi de udnytter borgeres egen adfærd til at svindle dem. [48]

Krogen, linen og loddet

Den psykologiske manipulation foregår ifølge adfærdsforsker Andreas Lieberoth i tre trin: krogen, linen og loddet. Lieberoth forklarer: "'Krogen' er den der lille ting, der fanger vores opmærksomhed. Så er der 'linen', der i klassisk svindelsprog kaldes 'telling the tale', fordi man får skabt en historie og får folk ombord. Endelig er der 'loddet', hvor berøvelsen finder sted. Det, som man i svindelsprog kalder 'the touch', og hvor pengene skifter hænder".

En it-kriminel kan f.eks. udgive sig for at være en borgers bank og sende en mail med en vigtig meddelelse om kompromittering af borgerens bankkonto.

45 Larsen, Henrik m.fl. (2018). Danskernes informationssikkerhed. Digitaliseringsstyrelsen m.fl.

46 Det Kriminalpræventive Råd (2016). Når forbrydelser bliver digitale – En antologi om IT-kriminalitet og adfærd på nettet. Det Kriminalpræventive Råd.

47 Sikkerdigital.dk (2020). Livephish. Sikkerdigital.dk 2020.

48 Oliveira, Daniela m.fl. (2020). The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behavior Research Methods. 1-11.

Krogen
Afsenderen og emnefeltet er den 'krog', der fanger borgerens opmærksomhed. I selve mailen kan der f.eks. stå, at borgerens bankkonto er blevet spærret, og at vedkommende skal tilgå bankens hjemmeside via et fremsendt link og indtaste brugernavn og adgangskode for at genåbne kontoen.

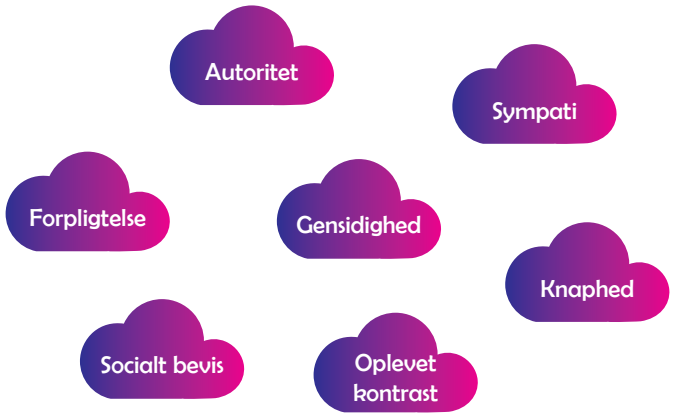
Linen
Historien om den spærrede konto er således den 'line', der skal få borgeren tilstrækkelig overbevist til at trykke på linket.

Loddet
Hvis borgeren klikker på linket i mailen og indtaster sine oplysninger, er angrebet nået til 'loddet', og borgeren er blevet et offer for kompromittering af personoplysninger, som den it-kriminelle kan udnytte.

Adfærdsforsker Andreas Lieberoth

Forsker og it-sikkerhedsekspert Oliveira gør opmærksom på, at mennesker altid har forsøgt at svindle hinanden. Den svindel, som phishing bygger på, er således ikke ny – den er bare blevet digital. Og som tidligere nævnt er phishing – ligesom andre former for svindel – designet til at manipulere menneskers følelser og udnytte menneskers kognitive bias med henblik på at få modtageren til at foretage hurtige og uigennemtænkte beslutninger.[49]

Syv kognitive bias
Psykolog Robert Cialdini har kortlagt syv af disse kognitive bias, som phishing ofte appellerer til, og som kan få mennesker til at handle i strid med egne interesser.



Autoritet henviser til menneskers tilbøjelighed til at efterleve krav fra autoritetsfigurer, mens forpligtelse indikerer, at mennesker, der har taget et standpunkt i en given sag, ofte vil føle sig forpligtede til at fastholde standpunktet. En borger kan dermed føle sig forpligtet til at besvare en henvendelse, der adresserer et standpunkt, som borgeren tidligere har givet udtryk for. It-kriminelle kan udnytte menneskers bias for sympati, fordi mennesker ifølge Cialdini har en tendens til at tro på henvendelser fra folk, de holder af eller har noget til fælles med. Gensidighed adresserer menneskers ønske om at gengælde en god

49 Ted 2020. Why we fall for phishing emails — and how we can protect ourselves. Ted 2020.

gerning, mens knaphed får en genstand eller et tilbud til at fremstå mere værdifuldt. Og socialt bevis udnytter menneskers tendens til at følge flertallet. Endelig refererer oplevet kontrast til menneskers opfattelse af den relative forskel mellem to vilkår, der præsenteres i umiddelbar forlængelse af hinanden. Hvis det første vilkår opfattes som relativt bedre end det andet, vil mennesker have en tendens til at opfatte det første vilkår som markant bedre, end det reelt er.[50]

De it-kriminelle kan udnytte disse bias ved f.eks. at udgive sig for at være en myndighed og dermed drage fordel af menneskets tendens til at adlyde autoritetsfigurer eller fremsende en mail med et tilbud om en gratis ydelse og dermed drage fordel af menneskets tendens til at gengælde en generøs gestus. På denne måde udnytter it-kriminelle borgeres egen adfærd og deres kognitive bias, når de bruger phishing til at svindle borgerne.[51] En tidligere it-kriminel, der er blevet interviewet til denne undersøgelse, fortæller:

> **"Man finder jo hurtigt ud af, hvad der er efterspørgsel på. Og for eksempel plejer Skanderborg Festival at blive udsolgt på en time eller to. Det samme gælder Roskilde Festival. Og der er jo rigtig mange, der ikke når at få billet. Så jeg har mange gange foregivet at jeg har haft billetter, som folk kunne købe".**

I dette eksempel udnytter den tidligere it-kriminelle det, som Cialdini kalder knaphedsprincip ved at foregive at sælge en vare, som på grund af knaphed og stor efterspørgsel opleves som meget værdifuld.

PHISHING RAMMER OGSÅ MYNDIGHEDER OG VIRKSOMHEDER

Det er dog ikke kun borgere, der bliver svindlet af it-kriminelle ved phishing-angreb. Phishing rammer også myndigheder og virksomheder, og i 2019 oplevede 3 pct. af danske virksomheder, at fortrolige data var blevet videregivet som følge af cyberkriminalitet, herunder phishing. 11 pct. af virksomhederne havde desuden oplevet sikkerhedsproblemer ved aktiviteter online, heriblandt phishing-e-mails, bedrageri, hacking eller identitetstyveri.[52]

En tidligere it-kriminel, der er blevet interviewet til denne undersøgelse, fortæller: "Mit fokus var mest på virksomheder, fordi det gav mulighed for at få større beløb".

Mange myndigheder og virksomheder oplever en stigende trussel fra målrettede ransomware-angreb. Her forsøger it-kriminelle at afpresse myndigheder og virksomheder for store pengebeløb ved at kryptere centrale dele af deres it-systemer ved hjælp af ransomware. Målrettede ransomware-angreb sker ofte efter en indledende kompromittering af myndigheden eller virksomheden med malware, der er blevet spredt ved hjælp af phishing.[53] Phishing er således et grundlæggende element i en række forskellige former for it-kriminalitet og fungerer ofte som et 'første skridt' i såkaldte APT-angreb (Advanced Persistent Threat-angreb).[54]

Ved phishing-angreb mod myndigheder og virksomheder, såkaldt Business Email Compromise-fraud, udgiver it-kriminelle sig for at være en medarbejders kollega eller en samarbejdspartner og anvender troværdige oplysninger som medarbejderens korrekte navn og titel.[55] Borgere kan dog også udsættes for målrettede angreb. I disse tilfælde adresseres offeret typisk med navn, og henvendelsens indhold er udformet, så det fremstår relevant for offeret.[56] Henvendelsen kan også indeholde et tidligere eller et nuværende password for at intimidere offeret og øge henvendelsens troværdighed.[57]

---

50 Lian, Tian m.fl. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. ACM Trans. Comput.-Hum. Interact 26(5):1-35.

51 Lian, Tian m.fl. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. ACM Trans. Comput.-Hum. Interact 26(5):1-35.

52 Danmarks Statistik (2020). Halvdelen har oplevet it-sikkerhedsproblemer. Danmarks Statistik.

53 CFCS (2020). Cybertruslen mod Danmark. Center for Cybersikkerhed.

54 Lian, Tian m.fl. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. ACM Trans. Comput.-Hum. Interact 26(5):1-35.

55 Det Kriminalpræventive Råd (2016). Når forbrydelser bliver digitale – En antologi om IT-kriminalitet og adfærd på nettet. Det Kriminalpræventive Råd.

56 Lian, Tian m.fl. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. ACM Trans. Comput.-Hum. Interact 26(5):1-35.

57 IC3 (2020). Online Extortion Scams Increasing During the Covid-19 Crisis. Internet Crime Complaint Center 2020.

MEDARBEJDERE OVERFOR BORGERE

Phishing rettet mod egne medarbejdere udgør en reel risiko for myndigheder og virksomheder, fordi det kan kompromittere myndighedernes og virksomhedernes it-infrastruktur. En Senior IT Security Advisor i DSB fortæller:

> **"Phishing-mails til medarbejdere fylder mere i DSB end phishing-mails til kunder. Alle statistikker viser, at 94 pct. af al malware kommer ind via phishing-mails til medarbejdere. Så hvis bare en medarbejder indtaster sine credentials i et link fra en phishing-mail, så går det galt for virksomheden".**

Samtidig kan medarbejderrettet phishing have konsekvenser for borgere, hvis kunde- eller borgeroplysninger også kompromitteres.

Myndigheder og virksomheder er desuden forpligtede til at melde kompromittering af egen it-infrastruktur til Datatilsynet, hvilket gør intern kompromittering til et offentligt anliggende. Det er en af grundene til, at de myndigheder og virksomheder, der har deltaget i denne undersøgelse, tager en række forholdsregler i forhold til medarbejderrettet phishing og arbejder aktivt med at beskytte sig selv imod de konsekvenser, som medarbejderrettet phishing kan medføre. Deres forholdsregler i forhold til medarbejderrettet phishing beskrives i rapportens tredje kapitel.

Selvom myndigheder og virksomheder generelt har større fokus på medarbejderrettet phishing end borgerrettet phishing, siger de medvirkende aktører enstemmigt, at det ærgrer dem, når it-kriminelle udsender phishing til borgere i virksomhedens eller myndighedens navn. En chefkonsulent i Udviklings- og Forenklingsstyrelsen siger: "Det er jo synd for borgerne, hvis de får en phishing-mail og bliver snydt". Og lederen af team sociale medier i PostNord fortæller: "Når en kunde har tastet sine oplysninger og tydeligvis er blevet snydt, så tænker man jo: 'Åh, stakkels Karen. Det var ikke godt'".

Phishing rettet mod borgere opleves dog ikke som en teknisk trussel for myndighederne og virksomhederne. Selvom der ikke er risiko for kompromittering af net- eller informationssystemer, kan phishing rettet mod borgere dog være forbundet med tab af omdømme og tillid. Chefkonsulenten i Udviklings- og Forenklingsstyrelsen uddyber:

> **"Det er jo som sagt synd for borgerne, når de bliver snydt, men det er ikke en teknisk trussel os, fordi det ikke er farligt for vores organisation".**

Angreb målrettet private borgere har ikke desto mindre vidtrækkende konsekvenser for den enkelte. Dels kan phishing-angreb føre til store økonomiske tab og angst blandt ofrene. Dels indebærer phishing misbrug af ofrenes identitet. Identitetsmisbrug har særlig betydning i den digitale tidsalder, hvor borgere som tidligere nævnt handler, bruger netbank og opbygger relationer online. Her udgør angrebene nemlig ikke kun en økonomisk, men også en sikkerhedsmæssig trussel for den enkelte borger. [58]

MOTIVATIONEN ER ØKONOMISK BERIGELSE

Generelt er it-kriminelle motiveret af muligheden for økonomisk berigelse, og det gør sig også gældende for it-kriminelle, der bruger phishing til at svindle borgere, virksomheder og myndigheder.[59] Som tidligere beskrevet er tendensen til flere og mere målrettede ransomware-angreb mod myndigheder og virksomheder ligeledes en måde, hvorpå it-kriminelle kan afpresse myndigheder og virksomheder for store pengebeløb ved at kryptere data i centrale it-systemer eller høste data.

En tidligere it-kriminel fortæller: "Alt det her med at skaffe penge, det fyldte bare mere og mere. Og så var jeg bare i det. Det var en mission at skaffe flere og flere penge".

De til tider mange og store beløb, som it-kriminelle kan erhverve sig ved brug af phishing,

58 Karuppannan, Jaishankar (2008). Identity related Crime in the Cyberspace: Examining Phishing and its impact. International Journal of Cyber Criminology 2(1):10-15.

59 Det Kriminalpræventive Råd (2016). Når forbrydelser bliver digitale – En antologi om IT-kriminalitet og adfærd på nettet. Det Kriminalpræventive Råd.

kan ifølge LCIK være en af grundene til, at de kriminelle i nogle tilfælde organiserer sig i kriminelle netværk, der kan hjælpe med at skaffe såkaldte muldyr. Muldyr er personer, der vidende eller uvidende hjælper med at hvidvaske penge fra kriminalitet. Det gælder f.eks. sager, hvor en borger har fået franarret sine betalingskortoplysninger, og hvor der efterfølgende bliver hævet store beløb fra borgerens konto. De illegalt erhvervede penge overføres til muldyrets konto og hæves derefter kontant til de kriminelle.[60]

DIGITAL DISTANCE

At it-kriminelle ikke møder deres ofre ansigt til ansigt, når de svindler dem ved hjælp af phishing, har betydning for de it-kriminelles opfattelse af de mennesker, som de gør til ofre for deres kriminelle handlinger. It-kriminelle, der gør brug af phishing, har typisk ikke et ønske om at gøre nogen ondt, men de skænker typisk heller ikke deres ofre en tanke.

For når it-kriminelle ikke møder de mennesker, som de forsøger at svindle, vokser afstanden mellem offeret og gerningspersonen. Og for mange it-kriminelle har det den virkning, at offeret og kriminalitetens konsekvenser føles uvedkommende. Og dermed bliver den dårlige samvittighed flygtig og nem at lægge til side. En tidligere it-kriminel fortæller:

> **"Jeg har ikke set dem som mennesker på den måde. De har bare været datapunkter af en eller anden slags".**

At offeret og kriminalitetens konsekvenser føles uvedkommende for gerningspersonen, gør sig også gældende ved andre former for it-kriminalitet. En dokumentarserie på DR3 fra 2020 følger debattør og twerkdanser Louise Kjølsen, der over en længere periode modtager anonyme trusselsmails. Under en digital konfrontation fortæller gerningspersonen, under dæknavnet Morten, at han til daglig opfører sig pænt, men at internettet fungerer som hans kriminelle løbebane. Morten fortæller: "Jeg ser jo ikke folk fysisk, når jeg skriver trusler til dem, så det er nemmere at være ekstrem på nettet".[61]

Adfærdsforsker Andreas Lieberoth forklarer, at det er nemmere at dehumanisere sit offer, når man som it-kriminel bare sender en mail og faktisk aldrig er i personlig kontakt. Med andre ord opfatter it-kriminelle generelt ikke deres ofre som mennesker, men blot som mailadresser, telefonnumre eller talrækken på et dankort.

Ovenstående eksempler illustrerer, at internettet kan virke som et filter, der frasorterer sociale informationer og gør det nemmere at anlægge en anden opførsel digitalt, end man ville gøre offline. Det digitale filter, der f.eks. frasorterer høre-, lugte- og følesansen, gør det vanskeligt for to parter at opbygge gensidig forståelse og tillid online, hvilket kan accelerere gensidige misforståelser, uenighed og konflikt.[62] De samme vilkår gør sig gældende for modtagere af phishing, og borgeres evne til at afkode afsenderens hensigter vanskeliggøres, som tidligere beskrevet, således også af den digitale kontekst.

PHISHING ER BÅDE MÅLRETTET OG TILFÆLDIGT

60 Politi (2019). Politiet advarer om at unge kan være muldyr for kriminelle. Politi 2019.

61 DR (2020). Hvem vil voldtage Louise?: Konfrontation. Danmarks Radio 2020.

62 Center for Digital Dannelse (2020). Hvorfor så mange misforståelser på nettet? Center for Digital Dannelse 2020.

Som tidligere beskrevet er der overordnet to typer af phishing, som it-kriminelle kan gøre brug af: opportunistiske angreb, hvor it-kriminelle sender en generisk phishing-mail til tusindvis af mailadresser, eller mere komplekse og målrettede phishing-angreb.

Ifølge LCIK foregår phishing og smishing ofte ved tilfældige spredehaglskampagner, der bliver rundsendt uden forudgående research. Det gælder dog ikke vishing, hvor gerningspersoner ringer op til de forurettede. Her har gerningspersonerne i nogle tilfælde vist sig i forvejen at have forbindelse til kriminelle miljøer. Den indledende udvælgelse af ofre sker bl.a. på baggrund af en antagelse om offerets alder baseret på eksempelvis navn. Herefter ses det ofte, at gerningsmanden har sat sig mere eller mindre ind i offentligt tilgængelige oplysninger om offeret med henblik på at kunne franarre vedkommende hans eller hendes personlige oplysninger.

Metoden gik bl.a. ud over borgeren Bodil Jensen, der i 2019 blev ringet op af en mand, som udgav sig for at være ansat i hendes bank. Svindleren ringede under påskud af at ville afværge en ulovlig overførsel fra Bodil Jensens konto og udbad sig i den forbindelse login-oplysninger til hendes netbank og NemID. Vishing-angrebet kostede Bodil Jensen 42.000 kr. Og det er ikke tilfældigt, at netop Bodil Jensen blev offer for svindlen. Som beskrevet ovenfor ringer danske it-kriminelle nemlig i mange tilfælde målrettet til borgere, hvis navn typisk tilhører den ældre del af befolkningen, da disse borgere forventes at være nemme ofre for it-relateret økonomisk kriminalitet.[63]

Ved avanceret phishing målrettet borgere har de kriminelle indsigt i, hvad danskerne 'hopper på', bl.a. ved at de holder sig orienteret om store begivenheder på global og regional skala for at kunne målrette phishing-angrebene. En analytiker i politiets Nationale Cyber Crime Center (NC3) beskriver avanceret phishing målrettet borgere på følgende måde:

> **"Den avancerede phishing mod borgere er målrettet den danske befolkning. Disse kampagner udnytter danske begivenheder som årsopgørelse eller Covid-19-testresultater. Målrettet, eller avanceret, phishing mod borgere er altså stadig relativt brede kampagner, som er designet til at snyde en større gruppe af mennesker, eller danskerne som befolkning".**

I nogle tilfælde anvender it-kriminelle dog også modtagerens navn i phishing-mailen for at øge henvendelsens troværdighed.[64]

Ifølge samme analytiker i NC3 udgør den målrettede phishing den største trussel af de to typer af phishing. Det skyldes dels, at henvendelserne er gennemarbejdede, dels at de både er målrettede og kontekstrelevante for modtageren. Som tidligere beskrevet får det henvendelserne til at fremstå troværdige, hvilket dels gør det vanskeligt for borgere at gennemskue svindlen, dels får borgere til at sænke paraderne.

PHISHING ER NEMT OG BEKVEMT FOR IT-KRIMINELLE

Ifølge LCIK er det generelt mere bekvemt for kriminelle at begå it-kriminalitet end traditionel kriminalitet, og det gælder i særdeleshed for phishing. En af de væsentligste forskelle mellem it-kriminalitet og traditionel kriminalitet som indbrud og røveri er, at it-kriminelle kan sende phishing-mails til borgere og virksomheder, uden at gerningsmanden møder sit offer ansigt til ansigt. Det betyder, at risikoen for at blive fanget og stillet til ansvar i forsøget på at udøve kriminalitet er mindre i mange gerningsmænds øjne. En tidligere it-kriminel, der er blevet interviewet til denne undersøgelse, fortæller:

> **"Det har været ret nemt. Det er jo nok også derfor, man gør det. Fordi det har været for nemt. Men man tænker bare ikke over det i nuet. Havde det været sværere, kunne jeg godt have fundet på at trække mig".**

63 DR (2019). 80-årige Bodil blev franarret NemID og 42.000 kroner: 'Han var så venlig og tiltalende'. Danmarks Radio 2020.

64 Lian, Tian m.fl. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. ACM Trans. Comput.-Hum. Interact 26(5):1-35.

En medarbejder fra LCIK forklarer:

> **"Hvis du begår vold eller røveri på gaden, er gevinsten ofte relativt lav, men straffen høj, fordi der er tale om personfarlig kriminalitet. Hvis du derimod fra-narrer folk deres personlige oplysninger, kan gevinsten være langt højre, men straffen lavere, fordi det ikke er personfarlig kriminalitet".**

Fraud-as-a-Service

Det er dog ikke alene den digitale distance, der gør phishing mere bekvemt end traditionel kriminalitet. I dag kan it-kriminelle købe onlinehjælpepakker med lister over lette ofre, kontaktoplysninger, skadelig malware m.v. på dark web, og det sænker barren for, hvem der kan phishe.[65] Lederen af svindelbekæmpelse hos MobilePay fortæller: "Det foregår på samme måde, som når jeg spørger tre leverandører, hvad et nyt regnskabsprogram til mit firma koster. Du kan også finde tre leverandører, som kan sælge dig borgeres kortoplysninger, eller hvad du nu har brug for, og så kan du bare vælge den billigste af de tre".

Det nye organiserede marked for it-relateret økonomisk kriminalitet bliver kaldt Fraud-as-a-Service (FaaS) og giver adgang til en platform for køb og salg af alt fra DDoS-angreb til stjålne betalingskort og login-oplysninger.[66] Og ifølge lederen af svindelbekæmpelse hos MobilePay er muligheden for at købe onlinehjælpepakker med til, at de it-kriminelle ikke behøver at have særlige it-kompetencer.

I takt med at kriminelle netværk bliver mere organiserede, vil it-kriminelle ofte specialisere sig i afgrænsede dele af et angreb, hvilket skaber en større arbejdsdeling internt i det kriminelle miljø. Udviklingen understøtter et kompetenceløft i det it-kriminelle miljø, hvor specialister udfører de kriminelle angreb. Selvom FaaS bidrager til at sænke barren for, hvem der kan begå it-kriminalitet, øger professionaliseringen og specialiseringen samtidig produktiviteten blandt eksisterende it-kriminelle.[67]

HACKERE

Trods professionaliseringen og specialiseringen adskiller it-kriminelle, der gør brug af phishing, sig markant fra hackere. Hackere bruger deres stærke it-kompetencer til at søge efter viden eller sikre fri informationsadgang, og derfor bliver hackere ofte beskrevet som en del af en subkultur.[68] Et studie beskriver hackere som kreative, ukonventionelle og selvretfærdige individer med en udtalt tilbøjelighed til at lyve og bedrage andre.[69] Mens barren for it-kriminelle, der benytter sig af phishing, bliver beskrevet som uforholdsmæssigt lav, er hacking således i højere grad forbundet med særlige egenskaber og kompetencer.

En tidligere hacker, der er blevet interviewet til denne undersøgelse, fortæller desuden:

> **"Der har helt sikkert været noget status i det. Jeg gik jo meget op i bare at hente så meget information som muligt i forbindelse med et angreb. Og jeg har jo brugt noget af den information, jeg hentede, til at bevise over for andre, at det her, det havde jeg faktisk gjort".**

Eftersom hacking er forbundet med særlige kompetencer, kan der således også være prestige og social status at hente i hackerangreb.

---

65 Oliveira, Daniela m.fl. (2020). The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behavior Research Methods. 1-11.

66 Infosec (2018). Fraud as a Service (FaaS): Everything You Need to Know. Infosec 2020.

67 CFCS (2020). Drømmer cyberkriminelle om tillidsfulde relationer? Center for Cybersikkerhed 2020.

68 Det Kriminalpræventive Råd (2016). Når forbrydelser bliver digitale – En antologi om IT-kriminalitet og adfærd på nettet. Det Kriminalpræventive Råd.

69 Rajivan, Prashanth og Cleotilde Gonzalez (2018). Creative Persuasion: A Study on Adversarial Behaviors Strategies in Phishing Attacks. Frontiers in Psychology 9(135):1-14.

FIRE TYPER AF IT-KRIMINELLE

Som det fremgår af ovenstående beskrivelser, bruger it-kriminelle internettes muligheder på forskellige måder. På baggrund af publikationer fra CFCS,[70] interviews med tidligere it-kriminelle samt cases fra danske nyhedsmedier er der identificeret fire persontyper, personaer. De fire personaer repræsenterer fremtrædende måder, som it-kriminelle forholder sig til at bruge phishing til at svindle borgere, virksomheder og myndigheder på. Personaerne skal ikke betragtes som faktiske it-kriminelle, men snarere som fire analytiske yderpunkter, som tydeliggør forskellige måder at forholde sig til phishing på i en dansk kontekst.

Personaerne skal derfor heller ikke forstås som eksklusive. Flere it-kriminelle vil typisk kunne genkende sig i flere personaer, da de kan kombineres på forskellige måder og dermed udgøre forskellige it-kriminelles måder at gøre brug af phishing på.

OPPORTUNISTEN

"Folk er naive, når de videregiver deres kortoplysninger. De stoler bare blindt på, at opkaldet kommer fra deres bank. Nogle gange tænker jeg, at folk sgu selv er ude om det. Folk burde tænke sig om. Det er det, der gør det nemt. Altså, for nemt".

– en tidligere it-kriminel

Opportunisten betragter phishing ud fra et mulighedsperspektiv. Opportunisten synes, at det er så nemt at begå it-kriminalitet, at det 'ville være dumt at lade være'. Derfor tænker opportunisten sjældent over konsekvenserne ved sine handlinger og føler ikke dårlig samvittighed over for sine ofre. I stedet betragter opportunisten ofrene som naive og mener, at det er 'deres egen skyld', at de ikke passer bedre på deres personoplysninger. Det overrasker ofte opportunisten, at ofre ikke er mere skeptiske, når de modtager uventede henvendelser.

VOVEHALSEN

"Det startede med, at jeg for mange år siden levede af at spille poker. Jeg havde en sponsor, der betalte mine rejser og pokerturneringer. Men den sponsor mistede jeg, og så skulle jeg selv ud og skaffe pengene. Jeg kendte nogle andre, som lavede noget med svindel, og da jeg blev desperat, røg jeg ind i det net. Når man lever et liv i overhalingsbanen, så handler det bare om at have penge nok. Så jeg havde slet ikke tid til at tænke over, at jeg kunne blive taget, og hvad jeg ville miste ved det".

– en tidligere it-kriminel

Vovehalsen betragter phishing ud fra et risikoperspektiv. Vovehalsen føler sig presset til at begå it-kriminalitet på grund af ydre omstændigheder. Det kan f.eks. være, at vovehalsen har stiftet gæld, som skal tilbagebetales inden for en kort frist. I sin desperation efter hurtig økonomisk berigelse tyer vovehalsen til phishing. Vovehalsen har ofte stiftet gæld for at opretholde en ekstravagant livsstil, som er kommet uden for vovehalsens økonomiske rækkevidde, og det giver en følelse af tab af prestige og anerkendelse.

Det giver vovehalsen dårlig samvittighed at tænke på sine ofre, men vovehalsen ser ingen anden vej ud af sine problemer. I et radioprogram på P3 fortæller en anonym kilde om at svindle borgere på nettet ved at modtage betaling for varer, som svindleren ikke er i besiddelse af. Ifølge den anonyme kilde startede kriminaliteten som et forsøg på at tilbagebetale en gæld, men for at kunne tilbagebetale gælden blev det nødvendigt at svindle stadig flere. Svindleren har dårlig samvittighed over for både sine ofre og sin familie, men kan ikke se en vej ud af svindlen. [71]
Casen fra P3 illustrerer, hvordan vovehalsen for hvert angreb kommer dybere ind i et kriminelt netværk, der får vovehalsens gæld og antallet af kriminelle handlinger til at vokse.

70 Se bl.a. CFCS (2020). Drømmer cyberkriminelle om tillidsfulde relationer? Center for Cybersikkerhed 2020.

71 DR P3 (2020). Den sorte boks – Svindler edition. Danmarks Radio P3 2020.

BAGMANDEN

"Der er ikke så mange i Danmark, der er gode til at bruge dark web, så jeg har lidt af en ekspertise, som andre gerne vil have glæde af. Derudover betragter jeg det, jeg laver, som ovre i den milde afdeling. I forhold til de penge, man kan tjene, er strafferammen lav, så det giver ikke særlig lang tid i fængslet".

– en tidligere it-kriminel

Bagmanden betragter sin rolle i phishing ud fra et sammenlignelighedsperspektiv. Bagmanden udvikler skadelig malware og udarbejder hjælpepakker med personoplysninger, som bagmanden videresælger til andre kriminelle på dark web. Bagmanden har dermed ikke ansvar for at sprede phishing, hvilket giver bagmanden en stabil indkomst med en relativt lav risiko.

Gennem salg af færdigudviklet malware og hjælpepakker indtager bagmanden en vigtig rolle i Fraud-as-a-Service (FaaS) og Ransomware-as-a-Service (RaaS). Bagmanden bidrager dermed til at sænke tærsklen for, hvem der kan udføre it-kriminalitet. Samtidig er bagmanden bevidst om, at strafferammen for videresalg af personoplysninger ofte er mildere, end hvis personoplysningerne anvendes til at foretage illegale pengeoverførsler. Og bagmanden opfatter det ikke som sit ansvar, hvad solgte personoplysninger eller malware bliver anvendt til af andre it-kriminelle. Bagmanden færdes hjemmevant på dark web og føler sig på afstand af sine ofre, som han meget sjældent er i direkte kontakt med.

OPRØREREN

"Jeg har bedre samvittighed, når det er en virksomhed, jeg snyder, fordi jeg ved, at de er dækket af en forsikring. Så de får pengene hjem igen. Lige så vel får jeg dårligere samvittighed, når jeg snyder en privatperson, for selv hvis de får pengene igen, kommer det til at tage længere tid. Det er ikke så rart at tænke på".

– en tidligere it-kriminel

Oprøreren betragter phishing ud fra et samvittighedsperspektiv. Oprøreren legitimerer sin gerning ved at angribe virksomheder i stedet for private borgere. Rationalet er dels, at virksomheder råder over større pengesummer end private borgere, dels at virksomheder er forsikret og derfor får dækket deres tab. Oprøreren betragter virksomheder som en samlet enhed og tænker ikke på de potentielle konsekvenser for virksomhedens medarbejdere.

Oprøreren benytter sig af BEC-fraud målrettet medarbejdere. Derudover kan oprøreren indgå som partner i FaaS- eller RaaS-samarbejder. Oprøreren målretter sine angreb mod virksomheder, fordi det gør det muligt at få adgang til større pengesummer. Oprøreren vægter dermed kvantitet frem for hurtig økonomisk berigelse. Derfor er oprøreren også villig til at bruge måneder på at afvikle et veltilrettelagt angreb.

OPSUMMERING

Myndigheders og virksomheders stigende brug af digital kommunikation skaber utilsigtet en mulighed for, at it-kriminelle kan svindle borgere. For it-kriminelle kan efterligne myndighedernes og virksomhedernes digitale kommunikation og udnytte borgernes tilvænning til at videregive personlige oplysninger og foretage køb via digitale selvbetjeningsløsninger.

Når it-kriminelle bruger phishing til at lokke borgere til at videregive deres personlige oplysninger, udnytter de også borgernes menneskelige adfærd. Phishing er en form for 'social engineering', hvor it-kriminelle gør brug af psykologisk manipulation og udnytter borgernes egen adfærd til at svindle dem. Phishing er designet til at manipulere med menneskers følelser og udnytte menneskers kognitive bias med henblik på at få borgerne til at foretage hurtige og uigennemtænkte beslutninger.

Det er dog ikke kun borgere, der bliver svindlet af it-kriminelle ved phishing-angreb. Phishing rammer også myndigheder og virksomheder, og phishing rettet mod egne medarbejdere udgør en reel risiko for myndigheder og virksomheder, fordi det kan kompromittere deres it-infrastruktur samt påføre organisationerne tab. Myndighederne og virksomhederne oplever derimod ikke borgerrettet phishing som en teknisk trussel, men det ærgrer dem, når borgere modtager phishing i deres navn.

It-kriminelle, der bruger phishing til at svindle borgere, myndigheder og virksomheder, er motiveret af muligheden for økonomisk berigelse. De har typisk ikke et ønske om at gøre nogen ondt, men de skænker ofte heller ikke deres ofre en tanke. For når it-kriminelle ikke møder de mennesker, som de forsøger at svindle, vokser afstanden mellem offeret og gerningspersonen, og dermed føles offeret og kriminalitetens konsekvenser ofte uvedkommende for de it-kriminelle.

Det er generelt mere bekvemt for kriminelle at begå it-kriminalitet end traditionel kriminalitet, og det gælder i særdeleshed for phishing. Det skyldes dels, at strafferammen for it-kriminalitet og phishing er lavere end ved personfarlig kriminalitet, selvom gevinsten kan være den samme, dels at de it-kriminelle undgår at møde deres ofre ansigt til ansigt, dels at de kan købe onlinehjælpepakker, dels at det er muligt for it-kriminelle at udnytte borgernes kognitive bias, når de forsøger at svindle borgere ved hjælp af phishing.

3

MYNDIGHEDERS OG VIRKSOMHEDERS HÅNDTERING AF BORGERRETTET PHISHING

Dette kapitel præsenterer myndigheders og virksomheders håndtering af borgerrettet phishing samt det kapløb, der i praksis udspiller sig mellem myndigheder, virksomheder og it-kriminelle i forhold til henholdsvis at forebygge og gøre brug af phishing. Kapitlet er baseret på danske studier af borgeres online- og offlineadfærd, internationale studier af økonomisk it-relateret kriminalitet samt interviews med borgere og repræsentanter fra myndigheder, virksomheder, politi og Center for Cybersikkerhed.

BORGERNE ER KILDEN TIL VIDEN OM PHISHING

Den undersøgelse, der er gennemført i forbindelse med udarbejdelse af denne rapport, viser, at nogle borgere håndterer deres bekymring for at blive svindlet på internettet ved at henvende sig til myndigheder og virksomheder, når de er i tvivl om, hvorvidt en konkret mail, SMS eller et opkald er legitim kommunikation fra myndigheder og virksomheder eller phishing.

Og det er ofte borgernes henvendelser, der gør, at myndigheder og virksomheder får kendskab til, at deres navn bliver brugt i borgerrettet phishing. For mange myndigheder og virksomheder opsøger ikke selv information om, hvorvidt deres navn bliver brugt i borgerrettet phishing, dels fordi borgerrettet phishing som tidligere nævnt ikke udgør en teknisk risiko for myndigheder og virksomheder, dels på grund af den indsats, der skal til, for at forudse og forebygge denne form for phishing. "Det er borgerne, der er en af vores store kilder omkring phishing", siger en afdelingschef i Sundhedsdatastyrelsen.

Nogle myndigheder forsøger dog at forhindre it-kriminelle i at svindle borgere ved at søge efter falske hjemmesider, der misbruger myndighedens navn. En chefkonsulent i Udviklings- og Forenklingsstyrelsen fortæller:

> **"Skatteforvaltningen har særlige systemer, som gennemsøger nettet for phishing-sider. Når systemerne finder phishing-sider, forsøger vi at lukke dem, før de når til borgerne. Vi kan af tekniske årsager ikke undersøge hele internettet, så noget phishing vil altid ramme borgerne. Når vi får kendskab til sådan phishing, forsøger vi at lukke siderne".**

For nogle myndigheder og virksomheder gælder det altså, at de primært får kendskab til, at borgere har modtaget phishing i deres navn, når borgere henvender sig med spørgsmål og anmeldelser til dem, mens andre søger efter og forsøger at nedlukke hjemmesider, som it-kriminelle vil bruge til at svindle borgere i deres navn.

At det typisk er borgere, der gør myndigheder og virksomheder opmærksom på, at de har modtaget phishing i deres navn, betyder også, at borgere er 'the first line of defense' i forhold til borgerrettet phishing, som en afdelingschef i Sundhedsdatastyrelsen kalder det. Han uddyber: "Flere og flere af sundhedssektorens tjenester afhænger af borgerne og deres indsats. De er vores 'first line of defense', fordi det er dem, der opdager udfald i tjenesterne. Og det er også dem, der bliver påvirket direkte".

Det er dog sårbart for borgerne at være 'first line of defense' i forhold til borgerrettet phishing. For i de fleste tilfælde må borgerne forlade sig på deres egen mavefornemmelse og skepsis samt velmenende råd fra myndigheder og virksomheder, når de modtager phishing. Og dermed er borgerne samtidig 'det svageste led' i håndteringen af borgerrettet phishing.

LEGITIME HENVENDELSER FORVEKSLES MED SVINDEL

Indimellem får myndighederne og virksomhederne henvendelser fra borgere, der forveksler deres digitale kommunikation med phishing.

En bruger har f.eks. indsendt følgende tip via appen Mit digitale selvforsvar:

> **"Har her til morgen modtaget SMS fra GLS om, at pakke vedrørende Covid19 er på vej, med link til fuldmagt. Jeg afventer ingen pakke nogen steder fra. Har heller ikke hørt/set i medierne, at der bliver sendt noget ud til borgerne. Så jeg tænker, at situationen og GLS udnyttes. Har ikke trykket på linket" (tip #13427).**

Forbrugerrådet Tænk har efterfølgende kontaktet afsenderen med henblik på at verificere, om der var tale om svindel. Det viste sig, at SMS'en var afsendt af GLS og havde til formål at redegøre for virksomhedens Covid-19-tiltag i forbindelse med pakkeudlevering. I dette tilfælde var der således tale om legitim digital kommunikation fra en virksomhed.

En anden borger er også blevet mistænksom overfor en mail, og derfor har vedkommende indsendt følgende tip via Mit digitale selvforsvar:

> **"Jeg har fået en mail, som sandsynligvis skulle komme fra SKAT, om min årsopgørelse. Men i selve mailen er der links til, at jeg kan rette i min årsopgørelse…" (tip #12358).**

Forbrugerrådet Tænk har efterfølgende kontaktet afsenderen med henblik på at verificere, om der var tale om svindel. Også denne borger har forvekslet digital kommunikation med phishing.

Netop fordi det kan være vanskeligt for borgere at skelne it-kriminelles phishing-angreb fra myndigheders og virksomheders digitale kommunikation, mener en rådgiver hos Center for Cybersikkerhed (CFCS), at borgere ikke bør opfattes som dem, der alene har ansvar for at beskytte deres personlige oplysninger på nettet. Hun siger:

> **"Borgerne er en del af sikkerhedsbilledet, men de har ikke ansvaret for det her. Det kræver en større fælles indsats".**

I internationale undersøgelser argumenteres der også for, at både myndigheder og ikkestatslige organisationer har et ansvar for at udbrede kendskabet til borgeres risiko for phishing.[72] Fra flere sider italesættes borgeres digitale sikkerhed således som et bredt forankret ansvar, der skal adresseres i fællesskab.[73]

PROCEDURER FOR BORGERRETTET PHISHING

Alle de myndigheder og virksomheder, der har deltaget i denne undersøgelse, har en procedure for, hvordan de håndterer borgerrettet phishing.

Myndighederne håndterer bl.a. borgerrettet phishing ved at:

- Stille sig til rådighed for henvendelser fra borgere, der er i tvivl om, hvorvidt de har modtaget phishing fra dem.
- Forsøge at nedlukke falske domæner og eventuelt opsøge borgere, hvis oplysninger er blevet kompromitteret.
- Advare om phishing-angreb på egen hjemmeside, sociale medier og i pressen.
- Nogle myndigheder udsender desuden en advarsel via appen Mit digitale selvforsvar, såfremt de er en del af netværket bag appen.

72 Karuppannan, Jaishankar (2008). Identity related Crime in the Cyberspace: Examining Phishing and its impact. International Journal of Cyber Criminology 2(1):10-15.

73 Dansk Erhverv (2020). Dansk Erhvervs digitale politik – Vækst gennem digitalisering. Dansk Erhverv.

Virksomhederne håndterer bl.a. borgerrettet phishing ved at:

- Stille sig til rådighed for henvendelser fra borgere, der er i tvivl om, hvorvidt de har modtaget phishing fra dem.
- Advare om phishing-angreb på egen hjemmeside og på sociale medier.
- Nogle virksomheder udsender desuden en advarsel via appen Mit digitale selvforsvar, såfremt de er en del af netværket bag appen.

Derudover oplever virksomheder generelt et stigende behov for at have Chief Information Security Officers (CISO) blandt deres ansatte med ansvar for virksomhedens it-sikkerhed.[74] Virksomheder med tilknyttede CISO-funktioner vil ofte have en procedure for håndtering af borgerrettet phishing i lighed med ovenstående generelle træk for håndtering af borgerrettet phishing.

Det skal bemærkes, at de myndigheder, der har deltaget i denne undersøgelse, i forskellig grad har direkte kontakt til borgere. Og netop omfanget af myndighedernes direkte kommunikation med borgere vurderes at have afgørende betydning for, hvordan myndighederne håndterer borgerrettet phishing. Der kan derfor være myndigheder, der håndterer borgerrettet phishing anderledes, end ovenstående liste godtgør. Nogle myndigheder vil vurdere, at de gør mere for at sikre borgeres digitale sikkerhed, mens andre vil vurdere deres indsats som mere snævert fokuseret.

Derudover skal det bemærkes, at de virksomheder, der har indgået i undersøgelsen, er større danske virksomheder, som alle jævnligt bliver misbrugt af it-kriminelle, der sender phishing til borgere i deres navn. I en opgørelse fra appen Mit digitale selvforsvar er PostNord og Matas i 2020 fortsat blandt de ti mest udsatte virksomheder med henholdsvis 1.212 og 302 tips fra brugere om phishing i virksomhedernes navn. De to virksomheder er også en del af netværket bag appen Mit digitale selvforsvar. Virksomhederne har således både stor erfaring med borgerrettet phishing og er en del af et professionelt samarbejde omkring håndtering af borgerrettet phishing. Det forventes derfor, at mange andre danske virksomheder – særligt små og mellemstore virksomheder – ikke har en procedure for, hvordan de skal håndtere borgerrettet phishing.

Små og mellemstore virksomheder udsættes også

Selvom mange små og mellemstore virksomheder ikke har lige så omfattende procedurer for håndtering af phishing, som ovenstående eksempler godtgør, bliver små og mellemstore virksomheder også udsat for it-kriminalitet. Faktisk kan de være særligt udsatte, fordi mange fejlagtigt betragter sig selv som 'uinteressante' for it-kriminelle og derfor ikke tager de nødvendige forholdsregler for at beskytte sig imod it-kriminalitet. En opgørelse viser f.eks., at 71 pct. af alle årlige datalækager stammer fra små virksomheder. [75]

Flere større virksomheder oplever dog også, at det 'koster mange ressourcer' at håndtere henvendelser om borgerrettet phishing. Og derfor ønsker flere af virksomhederne, at deres håndtering af borgerrettet phishing fungerer som 'hjælp til selvhjælp'. Direktør for Teknologi og Organisation i Matas fortæller:

> **"Inde på vores hjemmeside kan du se, at der er screendumps af forskellige ting, vi har fået fra vores kunder. Det positive ved det er, at det jo i virkeligheden er kunderne, der hjælper hinanden. Vi agerer bare formidlingscentral".**

Det er ligeledes en måde at gøre deres kunder 'selvhjulpne' på, når PostNord henviser deres kunder til appen Mit digitale selvforsvar. Lederen af team sociale medier i PostNord forklarer:

> **"Vi sender både advarsler ud på appen for vores egen skyld og for kundernes skyld. For hvis vi kan få mange kunder til at hente appen, så behøver de ikke henvende sig, næste gang de får en fup-besked. Og når det f.eks. er juletid, hvor vi virkelig har meget arbejde, er det positivt, hvis kunderne selv ved, hvordan de skal håndtere sådan nogle beskeder".**

74 Infosecurity (2015). Secure Your Future with a Virtual CISO. Infosecurity 2015.

75 Shulzhenko, Nadiia og Snizhana Romashkin (2020). Internet fraud and transnational organized crime. Juridical Tribune 10(1):162-172.

AWARENESS-KAMPAGNER OM MEDARBEJDERRETTET PHISHING

Flere myndigheder og virksomheder har også fokus på, at deres medarbejdere bliver bedre til at skelne legitim digital kommunikation – både intern og ekstern kommunikation – fra phishing-angreb.

Derfor arbejder flere myndigheder og virksomheder med awareness-kampagner til at forebygge medarbejderrettet phishing, der som beskrevet i det forrige kapitel udgør en større teknisk trussel for myndigheder og virksomheder end borgerrettet phishing.

I DSB er der introduceret en såkaldt 'hacker-knap', som gør det muligt for medarbejdere at anmelde phishing-mails. En 'hacker-knap' er naturligvis i udgangspunktet en teknologisk løsning, men den bliver af en Senior IT Security Advisor i DSB beskrevet som en del af et større arbejde med at skabe awareness om phishing blandt DSB's medarbejdere. For ønsket er at give medarbejdere i DSB et konkret og effektivt adfærdsanvisende værktøj til at håndtere phishing, og ifølge DSB's Senior IT Security Advisor er det adfærdsanvisende element ved 'hacker-knappen' centralt. Hun forklarer:

> **"It-sikkerhed handler ikke om it. Det handler om menneskelig adfærd. Og derfor er vi nødt til at angribe phishing-mails med viden om adfærd. Og det giver så meget mening at styrke menneskers it-sikkerhed ved at arbejde med deres adfærd i stedet for at give dem en bedre tech-forståelse. Min påstand er, at man ikke behøver at forstå det it-mæssige for at skabe en bedre it-sikkerhed hos mennesker".**

Formålet med at skabe awareness om phishing blandt DSB's medarbejdere er at styrke medarbejdernes evne til at genkende phishing. "Vi afholder en konkurrence, hvor et antal medarbejdere får at vide, at de er særligt udvalgt til at deltage. For vi mennesker bliver altid glade for at være særligt udvalgte", fortæller DSB's Senior IT Security Advisor. Hun fortæller videre: "De får at vide, at de får en phishing-mail i løbet af en uge, at de skal kunne genkende den, og at de derfor får fem råd til, hvordan de kan genkende phishing-mails." Ved at afholde en konkurrence bliver rådene mere vedkommende for medarbejderne, fordi de skal bruge dem til at deltage i konkurrencen.

I DSB arbejdes der således ud fra samme antagelse, der tidligere er beskrevet i denne rapport; velmenende anbefalinger om it-sikkerhed skal ledsages af konkrete værktøjer til, hvordan anbefalingerne kan følges på en nem og overskuelig måde.[76]

Udviklings- og Forenklingsstyrelsen gør også brug af awareness-kampagner, så deres medarbejdere bliver bedre til at genkende phishing-mails. En chefkonsulent i Udviklings- og Forenklingsstyrelsen beskriver myndighedens awareness-kampagner som en 'undervisningsøvelse'. Han forklarer:

> **"Lige præcis i dag er vi i gang med at lave en phishing-øvelse. Jeg har sendt en phishing-mail ud til 138 medarbejdere, hvori der står, at deres system er løbet tør for plads. Og når de så trykker på linket i mailen, kommer de til en hjemmeside, hvor der står 'ups, du har trykket på en phishing-mail'".**

De myndigheder og virksomheder, der gør brug af awareness-kampagner, vurderer, at awareness-kampagner er et brugbart og effektivt værktøj til at styrke medarbejderes it-sikkerhed, fordi de gør phishing-angreb konkrete og vedkommende for deres medarbejdere. En afdelingschef i Sundhedsdatastyrelsen fortæller: "Internt i koncernen arbejder vi med awareness bl.a. i forhold til phishing. Og det, der virkelig virker, er, når vi kan fremhæve konkrete eksempler på potentielle sikkerhedshændelser i koncernen. Så det virker først, når det er nærværende. Hvis jeg bare siger 'nu skal I være opmærksomme på phishing-mails, fordi der er mange af dem hen over sommerferien', så giver det ikke en fløjtende fis. Det skal kædes op på noget håndgribeligt".

76 Münster, Morten Sehested (2017). Jytte fra Marketing er desværre gået for i dag – sådan bruger du adfærdsdesign til at skabe forandringer i den virkelige verden. Gyldendal Business.

Matas forsøger også at styrke deres medarbejderes it-sikkerhed ved at etablere en grundlæggende awareness blandt medarbejderne. Og deres erfaringer på området er positive. "Vi har for nylig haft en phishing-test blandt vores medarbejdere, og det gjorde mig meget klogere på vores udfordringer. Så jeg overvejer at indføre det som et fast element i vores arbejde", fortæller direktøren for Teknologi og Organisation i Matas.

Selvom myndighedernes og virksomhedernes oplevelser er, at awareness-kampagner er et brugbart og effektivt værktøj til at styrke medarbejderes it-sikkerhed, kan denne undersøgelse ikke dokumentere awareness-kampagnernes effekt. Der findes også en række andre awareness-kampagner, som arbejder med at forebygge cyberkriminalitet blandt både borgere og virksomheder, men størstedelen af disse kampagner er ikke blevet evalueret. I andre tilfælde er evalueringerne ikke blevet offentliggjort. De manglende evalueringer gør det vanskeligt at vurdere kampagnernes effekt, og kampagnernes virkning er således snarere oplevet end målbar. [77]

Appen Mit digitale selvforsvar er imidlertid et eksempel på et tiltag, hvis oplevede effekt kan dokumenteres. En brugerundersøgelse fra 2019 viser, at 97 pct. af app-brugerne oplever appens indhold som relevant, og at 96 pct. oplever appen som brugbar. Samtidig vurderer 82 pct. af brugerne, at appens indhold har øget deres opmærksomhed på svindel på nettet. Brugerundersøgelsen dokumenterer således en oplevet forebyggende effekt blandt app-brugerne. [78]

MYNDIGHEDERS OG VIRKSOMHEDERS OPFATTELSE AF EGET ANSVAR

Nogle af de myndigheder og virksomheder, der har deltaget i undersøgelsen, erkender, at de som afsendere af digital kommunikation til borgere har et medansvar for at forebygge, at borgere bliver svindlet af it-kriminelle. Direktøren for Teknologi og Organisation i Matas siger: "Man kan ikke sige sig fri for at have et ansvar og en rolle i det her. Jeg betragter det som en teknologisk opdragelsesrolle".

Nogle af myndighederne og virksomhederne er opmærksomme på, at it-kriminelle forsøger at efterligne deres digitale kommunikation til borgere, og at deres kommunikation dermed kan misbruges af it-kriminelle til at udarbejde endnu mere troværdig borgerrettet phishing. De er også opmærksomme på, at nogle borgere forveksler deres digitale kommunikation med phishing. De erkender således, at det har en betydning, hvordan deres digitale kommunikation med borgerne foregår, og at de kan være med til at forebygge, at borgere bliver svindlet af phishing i deres navn.

Trods denne erkendelse er der ikke nogen af de myndigheder og virksomheder, der har deltaget i undersøgelsen, der har ændret i deres digitale kommunikation med borgere med henblik på at forebygge, at borgere bliver svindlet via phishing.

Frem for konkrete ændringer i selve kommunikationen med borgere er det mere udbredt blandt de myndigheder og virksomheder, der har deltaget i undersøgelsen, at gøre brug af teknologiske løsninger til at forebygge, at it-kriminelle misbruger deres kommunikation til at svindle borgere. Dette uddybes i et kommende afsnit i dette kapitel.

Brugervenlighed overfor it-sikkerhed

Flere af de myndigheder og virksomheder, der har deltaget i undersøgelsen, erkender, at deres digitale kommunikation med borgere kan foregå på måder, som i højere grad forebygger, at borgere bliver svindlet af phishing. Men når man spørger dem, hvorfor de ikke gør mere, svarer de med forskellige versioner af: "Vi vil ikke gøre det for besværligt for borgerne" eller "Vores kunder vælger bare vores konkurrenter, hvis det ikke er nemt at handle med os".

77 Epinion og Det Kriminalpræventive Råd (2015). Kriminalitetsforebyggelse og kampagner – En litteraturgennemgang af kampagneteorier, -metoder og -strategier. Epinion og Det Kriminalpræventive Råd.

78 Epinion og Forbrugerrådet Tænk (2019). Brugerevaluering af 'Mit digitale selvforsvar'. Epinion og Forbrugerrådet Tænk.

Det betyder altså, at de fleste myndigheder og virksomheder prioriterer brugervenlighed mindst lige så højt som it-sikkerhed. Det kan skyldes, at myndigheder og virksomheder som tidligere nævnt ikke betragter borgerrettet phishing som en teknisk risiko, der kan kompromittere deres virke. Men det vidner i langt højere grad om, at myndigheder og virksomheder står i et dilemma: De vil gerne forebygge borgerrettet phishing, men samtidig er det væsentligt, at deres digitale kommunikation er brugervenlig.

For myndigheder har behov for at sikre, at borgere tilgår fremsendte informationer vedrørende SKAT, e-Boks eller egen læge. Og virksomheder konkurrerer på markedsvilkår, og i en digital hverdag er det afgørende at kunne fastholde kundernes opmærksomhed, sikre lettilgængelige indkøbsmuligheder og effektiv formidling af nyheder og tilbud. Derfor er det for både myndigheder og virksomheder lige så vigtigt, at deres digitale kommunikation er brugervenlig, som at den er sikker.

Af hensyn til brugervenlighed har PostNord endda lavet en ændring i deres kommunikation, som kan gøre det sværere for deres kunder at skelne legitim kommunikation fra phishing. Lederen af team sociale medier i PostNord fortæller:

> **"I starten kunne vi sige til vores kunder, at vi ikke sender SMS'er med links, som handler om betaling. Så hvis der var nogen af vores kunder, der fik en SMS om noget med betaling og et link, så skulle de bare slette den. Men vi vil gerne gøre det nemt for vores kunder, så nu sender vi selv SMS til dem, hvis der kommer en pakke fra udlandet til fortoldning. Og i de SMS'er sender vi et link med, som kunderne kan trykke på for at betale for tolden".**

Hos flere af de myndigheder og virksomheder, der har deltaget i undersøgelsen, er der løbende dialog om forholdet mellem brugervenlighed og sikkerhed i forhold til den digitale kommunikation med borgere. Og hos flere af myndighederne og virksomhederne er der også en oplevelse af, at hensyn til it-sikkerhed er blevet en større del af kommunikationen til borgere. I en større dansk virksomhed er mere sikker kommunikation et eftertrædt 'næste skridt'. En it-sikkerhedsspecialist i denne virksomhed fortæller:

> **"I øjeblikket er det ikke muligt for os at udforme mails på måder, så it-kriminelle ikke kan efterligne en mail fra os. Men det er klart vores ønske, at det kan lade sig gøre".**

En medarbejder hos LCIK vurderer dog, at det kan være vanskeligt for myndigheder og virksomheder at gøre ret meget ved borgerrettede phishing-forsøg, der bliver sendt i deres navn. Mange myndigheder og virksomheder er klar over, at phishing-forsøg finder sted i deres navn, men at det kan være svært at gøre noget ved, hvis domæne og gerningsmænd er i udlandet, og de it-kriminelle kan hurtigt oprette nye falske domæner og spoofede telefonnumre.

Derfor er fokus som nævnt ofte på at lære borgerne, hvordan de kan genkende phishing-forsøg, og at de ikke skal udlevere personlige oplysninger, hvis de er i tvivl. Fokus er på oplysning og forebyggelse, fordi det er en langt bedre udnyttelse af ressourcer, end at jagte gerningsmænd på den anden side af jorden. Vurderingen peger dermed også på, at en effektiv bekæmpelse af it-kriminalitet skal understøttes af koordinerede og flerstrengede indsatser på tværs af virksomheder, myndigheder og borgere.

DET SVÆRE KAPLØB

Ifølge LCIK kan det således af flere årsager være svært for virksomheder og myndigheder at forhindre borgerrettede phishing-forsøg. Foruden de nævnte årsager er det også svært at forebygge og mindske borgerrettet phishing, fordi de it-kriminelle generelt bliver dygtigere til at udarbejde troværdig phishing i myndigheders og virksomheders navn.[79]

79 Det Kriminalpræventive Råd (2016). Når forbrydelser bliver digitale – En antologi om IT-kriminalitet og adfærd på nettet. Det Kriminalpræventive Råd.

En rådgiver fra CFCS fortæller:

> **"It-kriminelle er blevet så dygtige i dag. Man har tit talt om, at der i phishing var stavefejl eller mærkelige formuleringer på dansk, men man er kommet videre fra det sted. Nu er de it-kriminelle blevet bedre, så stavefejl og mærkelige formuleringer er ikke længere en tommelfingerregel, man kan bruge".**

Ingen reelle virksomheder eller myndigheder anmoder dog om betalingskortoplysninger, NemID eller andre log-in-informationer via e-mail, SMS eller opkald, og det er således fortsat en gældende tommelfingerregel.[80]

Ikke desto mindre er de it-kriminelles forbedrede evner til at formulere e-mails i et troværdigt sprog og til at efterligne logoer med til at gøre det endnu vanskeligere for borgere at skelne mellem myndigheders og virksomheders digitale kommunikation og it-kriminelles phishing-angreb. Forsker og it-sikkerhedsekspert Daniela Oliveira påpeger også, at mange borgere fortsat tror, at phishing er en mail fra den berygtede 'nigerianske prins', men hun understreger, at moderne phishing-e-mails kan være svære at skelne fra legitime e-mails. Omfattende amerikanske undersøgelser tyder på klikfrekvenser så høje som 20 pct. for de mest effektive phishing-e-mails, og derfor anslås phishing at koste milliarder af dollars hvert år.[81]

Selvom det kan være svært at forhindre borgerrettet phishing, forsøger flere myndigheder og virksomheder at forebygge, at it-kriminelle misbruger deres digitale kommunikation til at svindle borgere. Og det gør de ved at bruge forskellige teknologiske løsninger. Det gør de, dels fordi de ønsker at være med til at forebygge, at borgere bliver svindlet af phishing i deres navn, dels fordi det som et led i Danmarks nationale cyber- og informationssikkerhedsstrategi er besluttet, at statslige myndigheder skal efterleve en række tekniske minimumskrav med henblik på at sikre et højt fælles sikkerhedsniveau i staten. De fleste af disse krav skulle implementeres senest d. 1. juli 2020.[82]

Filtre

De myndigheder, der har deltaget i denne undersøgelse, er derfor bl.a. underlagt krav om at implementere DMARC-filtre. Anvendelsen af Domain-based Message Authentication, Reporting, and Conformance (DMARC) medvirker til at sikre et domænenavn fra at blive misbrugt til phishing.[83] En chefkonsulent fra Udviklings- og Forenklingsstyrelsen fortæller:

> **"Vi har DMARC-filtre, som gør, at man ikke kan sende mails som SKAT. Og vi gør stort set alt det, der er 'best practise' på området. Udfordringen er, at phishing kan omgå teknikken".**

Flere af de virksomheder, der har deltaget i undersøgelsen, bruger sårbarhedsscanninger og egne servere til at håndtere borgerrettet phishing. Flere af myndighederne og virksomhederne beskriver dog udviklingen af teknologiske løsninger til at håndtere borgerrettet phishing og andre former for svindel som et kapløb mod de it-kriminelle'. En it-sikkerhedsspecialist i en større dansk virksomhed forklarer det på følgende måde:

> **"Vi kører alle mulige forskellige tjek løbende. Så vi forsøger at beskytte os imod alle de forskellige metoder, som it-kriminelle kan gøre brug af. Men det er bare et kapløb mod de it-kriminelle".**

Myndighedernes og virksomhedernes oplevelse er altså, at de it-kriminelle som regel finder en måde at omgå deres teknologiske løsninger på. Og det lader også til at være tilfældet. Som beskrevet i kapitel 2 er det f.eks. muligt for it-kriminelle at omgå den tofaktor-

80 Det Kriminalpræventive Råd (2016). Når forbrydelser bliver digitale – En antologi om IT-kriminalitet og adfærd på nettet. Det Kriminalpræventive Råd.

81 Oliveira, Daniela m.fl. (2020). The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behavior Research Methods. 1-11.

82 Sikkerdigital.dk (2020). Tekniske minimumskrav for statslige myndigheder. Sikkerdigital.dk 2020.

83 Sikkerdigital.dk (2020). DMARC (anti-phishing). Sikkerdigital.dk 2020.

godkendelse, der er designet til at beskytte borgere mod svindel på internettet. Ved hjælp af såkaldt live-phishing er det muligt for it-kriminelle at få borgere til at bekræfte deres illegitime køb ved at få borgere til at tilgå forfalskede hjemmesider.[84]

Det er således et svært kapløb mod it-kriminelle at forsøge at forebygge og mindske borgerrettet phishing. Og særligt hvis man forsøger at vinde kapløbet med teknologiske løsninger, fordi det som nævnt ofte er muligt for it-kriminelle at finde måder at omgå de teknologiske løsninger på.

OPSUMMERING

Nogle borgere henvender sig til den pågældende myndighed eller virksomhed, når de er i tvivl om, hvorvidt de har modtaget phishing. Og derfor får myndighederne og virksomhederne indimellem henvendelser fra borgere, der forveksler deres legitime kommunikation med phishing.

For nogle myndigheder og virksomheder gælder det, at de primært får kendskab til, at borgere har modtaget phishing i deres navn, når borgere henvender sig med spørgsmål og anmeldelser til dem. Andre forsøger at forhindre, at it-kriminelle kan svindle borgere i deres navn, ved at søge efter og nedlukke pharming-hjemmesider.

At det typisk er borgere, der gør myndigheder og virksomheder opmærksom på, at de har modtaget phishing i deres navn, betyder, at borgere er 'the first line of defense' i forhold til borgerrettet phishing. Det er dog sårbart for borgerne, fordi de må forlade sig på deres egen mavefornemmelse og skepsis samt velmenende råd fra myndigheder og virksomheder, når de modtager phishing.

Netop fordi det kan være vanskeligt for borgere at skelne it-kriminelles phishing-angreb fra myndigheders og virksomheders digitale kommunikation, påpeges det, at det kræver en større fælles indsats at forebygge borgerrettet phishing. Flere af de myndigheder og virksomheder, der har deltaget i undersøgelsen, erkender også, at deres digitale kommunikation med borgere kan foregå på måder, som i højere grad forebygger, at borgere bliver svindlet af phishing. De fleste myndigheder og virksomheder har imidlertid behov for at sikre effektiv og lettilgængelig kommunikation, synlighed og markedsføring og prioriterer derfor brugervenlighed lige så højt som it-sikkerhed.

Det kan dog også være vanskeligt for myndigheder og virksomheder at gøre ret meget ved borgerrettet phishing, bl.a. fordi it-kriminelle hurtigt kan oprette nye falske domæner og spoofede telefonnumre, og fordi de it-kriminelle generelt bliver dygtigere til at udarbejde troværdig digital kommunikation i myndigheders og virksomheders navn. Og det kan gøre det endnu vanskeligere for borgere at skelne mellem myndigheders og virksomheders digitale kommunikation og it-kriminelles phishing-angreb.

Flere myndigheder og virksomheder bruger teknologiske løsninger til at forsøge at forebygge, at it-kriminelle misbruger deres digitale kommunikation til at svindle borgere. Flere myndigheder og virksomheder beskriver dog udviklingen af teknologiske løsninger som et 'kapløb' mod de it-kriminelle', fordi de it-kriminelle finder måder at omgå de teknologiske løsninger på.

84 Sikkerdigital.dk (2020). Livephish. Sikkerdigital.dk 2020.

4

PERSPEKTIVER PÅ STYRKELSE AF BORGERES DIGITALE SIKKERHED

Dette kapitel indledes med en analyse af den gensidige adfærdspåvirkning, der foregår mellem borgere, it-kriminelle, myndigheder og virksomheder. Kapitlet er baseret på de foregående kapitler og er således en sammenfatning og en opsummering af de tidligere præsenterede analyser. I forlængelse af analysen af den gensidige adfærdspåvirkning fremlægges en række perspektiver på det videre arbejde med at skabe kompetenceudviklende og adfærdsændrende initiativer til at styrke borgeres digitale sikkerhed.

DEN GENSIDIGE ADFÆRDSPÅVIRKNING

Som det fremgår af de tidligere kapitler, skaber den stigende brug af digital kommunikation mellem borgere, myndigheder og virksomheder utilsigtet en mulighed for, at it-kriminelle kan efterligne den digitale kommunikation og dermed svindle borgere, myndigheder og virksomheder.[85]

Og det *er* vanskeligt for borgere at skelne it-kriminelles phishing-angreb fra myndigheders og virksomheders digitale kommunikation. Bl.a. fordi it-kriminelle bliver dygtigere til at udarbejde troværdige phishing-angreb i myndigheders og virksomheders navn,[86] og i et travlt hverdagsliv kan det være svært for borgerne at adskille en phishing-mail fra legitime mails fra f.eks. deres bank. Og det udnytter de it-kriminelle for at få borgerne til at foretage hurtige og uigennemtænkte beslutninger.[87]

En fundamental barriere for, at borgere kan agere sikkert på internettet, er den digitale kontekst i sig selv. For mennesket er evolutionært udviklet til at vurdere sikkerhedsrisici på baggrund af fysiske faresignaler, men der er ikke nogen fysiske faresignaler i den digitale verden. Og det gør det vanskeligere for borgere at vurdere, hvornår de er i fare på internettet.[88]

Borgerne er dog generelt opmærksomme på, at der er en risiko for at blive svindlet på internettet. Og størstedelen er også bevidste om, at de ved brug af en række sikkerhedsforanstaltninger kan mindske risikoen for, at deres oplysninger havner i 'de forkerte hænder'. Borgerne gør bl.a. brug af NemID, videregiver kun personlige oplysninger på sociale medier i begrænset omfang, opdaterer sikkerhedsprogrammer, anvender tofaktorgodkendelse og forsøger at have et godt password.[89]

Trods sådanne sikkerhedsforanstaltninger er alle borgere i risikozonen for at blive svindlet via phishing, fordi mennesker i vidt omfang overvurderer deres egne evner til at gennemskue svindel på internettet. Og derfor udviser alle borgere fra tid til anden digital risikoadfærd. F.eks. ved borgerne generelt, at det er vigtigt at have et godt password, men mange genbruger alligevel deres passwords og videregiver deres personlige oplysninger på de sociale medier, selvom de ved, at det er risikofyldt. Og det skyldes kognitive bias i menneskers tænkning. F.eks. genbruger borgere deres passwords til flere hjemmesider, fordi der er grænser for, hvor meget menneskets hjerne kan huske.[90]

85 Finansministeriet (2018). National strategi for cyber- og informationssikkerhed. Finansministeriet. Se desuden Shulzhenko, Nadiia og Snizhana Romashkin (2020). Internet fraud and transnational organized crime. Juridical Tribune 10(1):162-172.

86 Oliveira, Daniela m.fl. (2020). The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behavior Research Methods. 1-11.

87 Ted 2020. Why we fall for phishing emails — and how we can protect ourselves. Ted 2020.

88 Frost, Lasse, Kristian Sørensen og Simon Bentholm (2017). For-analyse af danskernes informationssikkerhed. /Kl.7, Digitaliseringsstyrelsen og Erhvervsstyrelsen.

89 Tassy, Agnes n.fl. (2020). It-anvendelse i befolkningen 2020. Danmarks Statistik.

90 Ebner, Natalie C., m.fl. (2018). Uncovering Susceptibility Risk to Online Deception in Aging. Journals of Gerontology: Psychological Sciences 00(00): 1-12.

Disse kognitive bias misbruger it-kriminelle ved at manipulere med borgerne og udnytte borgernes egen adfærd til at svindle dem. Det sker f.eks. ved, at it-kriminelle udgiver sig for at være en myndighed og dermed drager fordel af menneskets tendens til at adlyde autoritetsfigurer. It-kriminelle kan også drage fordel af menneskets tendens til at gengælde en generøs gestus ved at fremsende en mail med et tilbud om en gratis ydelse. [91]

Ligesom menneskets kognitive bias er borgernes travle hverdagsliv en væsentlig barriere for deres it-sikkerhed. For et utal af behov, gøremål og pligter påkalder sig borgernes opmærksomhed og fjerner fokus fra risikoen for at blive svindlet af it-kriminelle. Dermed er borgernes travle hverdagsliv også med til at gøre det lettere for de it-kriminelle at svindle borgerne. Og eftersom mange anbefalinger om it-sikkerhed strider imod menneskets umiddelbare handle- og tankemønstre, følger borgerne ikke de velmenende anbefalinger, hvis ikke de får konkrete værktøjer til, hvordan de kan følge dem i en travl hverdag.

Økonomisk vinding og anonyme ofre
De it-kriminelles udnyttelse af borgernes kognitive bias og deres travle hverdagsliv blotlægger, at it-kriminelle typisk ikke skænker deres ofre en tanke. It-kriminelle har typisk ikke et ønske om at gøre nogen ondt – de er alene motiveret af muligheden for økonomisk berigelse – men deres ofre og kriminalitetens konsekvenser for deres ofre føles ofte uvedkommende for de it-kriminelle. For de it-kriminelle møder ikke deres ofre ansigt til ansigt, fordi svindlen foregår digitalt, og det gør det nemt for de it-kriminelle at lægge deres dårlige samvittighed til side.

Netop det, at svindlen foregår digitalt, giver de it-kriminelle muligheder for at foretage svindlen i en størrelsesorden, som vanskeligt kan lade sig gøre ved traditionel kriminalitet. Og det er en af årsagerne til, at it-kriminalitet og phishing i særdeleshed er mere bekvemt at begå for kriminelle end traditionel kriminalitet. Det er dog ikke alene det, der gør phishing mere bekvemt end traditionel kriminalitet. I dag kan it-kriminelle købe online hjælpepakker med lister over lette ofre, kontaktoplysninger, skadeligt malware m.v. på dark web, og det sænker barren for, hvem der kan phishe.[92] Og endelig er strafferammen for it-kriminalitet med til at gøre phishing bekvemt for it-kriminelle. For strafferammen for it-kriminalitet og phishing er lavere end for personfarlig kriminalitet – selvom gevinsten kan være højere.

Der er med andre ord ikke mange barrierer for kriminelle, der gerne vil forsøge at svindle borgere via phishing. Og derfor er der et stigende antal af borgere, der bliver ofre for it-kriminalitet.[93] Nogle borgere håndterer denne risiko ved at henvende sig til myndigheder og virksomheder, når de er i tvivl om, hvorvidt de er blevet udsat for et svindelforsøg.

Myndigheders og virksomheders håndtering
Nogle myndigheder og virksomheder får primært kendskab til, at borgere har modtaget phishing i deres navn, når borgere henvender sig med spørgsmål og anmeldelser til dem, mens andre søger efter og forsøger at nedlukke hjemmesider, som it-kriminelle vil bruge til at svindle borgere i deres navn.

Og borgernes henvendelser til myndigheder og virksomheder viser, at nogle borgere forveksler den legitime digitale kommunikation med phishing. Myndigheder og virksomheder vil meget gerne stå til rådighed for borgernes henvendelser og spørgsmål vedrørende potentielle svindelforsøg, men flere virksomheder oplever også, at det 'koster mange ressourcer' at håndtere borgernes henvendelser. Derfor ønsker flere af virksomhederne, at deres håndtering af borgerrettet phishing fungerer som 'hjælp til selvhjælp'.

---

91 Lian, Tian m.fl. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. ACM Trans. Comput.-Hum. Interact 26(5):1-35.

92 Oliveira, Daniela m.fl. (2020). The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behavior Research Methods. 1-11.

93 Politi (2020). Analyse: Politiet har modtaget knap 27.000 anmeldelser om it-relateret økonomisk kriminalitet i 2019. Rigspolitiet 2020.

Ændring af den digitale kommunikation
Nogle myndigheder og virksomheder erkender, at de som afsendere af digital kommunikation til borgere har et medansvar for at forebygge, at borgere bliver svindlet af it-kriminelle. De er opmærksomme på, at it-kriminelle forsøger at efterligne deres digitale kommunikation til borgere, og at deres kommunikation dermed kan misbruges til at udarbejde endnu mere troværdig borgerrettet phishing. De er også opmærksomme på, at nogle borgere forveksler deres digitale kommunikation med phishing. De erkender således, at det har en betydning, hvordan deres digitale kommunikation med borgerne foregår, og at de kan være med til at forebygge, at borgere bliver svindlet af phishing i deres navn.

Trods denne erkendelse er det blot enkelte myndigheder og virksomheder, der har ændret i deres digitale kommunikation med borgere med henblik på at forebygge svindel. Til dels fordi myndigheder og virksomheder ikke betragter borgerrettet phishing som en teknisk risiko, der kan kompromittere deres virke. Men i langt højere grad, fordi myndigheder og virksomheder står i et dilemma: De vil gerne forebygge borgerrettet phishing, men samtidig er det væsentligt, at deres digitale kommunikation er brugervenlig.

For myndigheder har behov for at sikre, at borgere tilgår fremsendte informationer vedrørende SKAT, e-Boks eller egen læge. Og virksomheder konkurrerer på markedsvilkår, og i en digital hverdag er det afgørende at kunne fastholde kundernes opmærksomhed, sikre lettilgængelige indkøbsmuligheder og effektiv formidling af nyheder og tilbud. Derfor er det for både myndigheder og virksomheder lige så vigtigt, at deres digitale kommunikation er brugervenlig, som at den er sikker.

Det kan være svært for myndigheder og virksomheder at forhindre borgerrettede phishing-forsøg. Hvis f.eks. domæne og gerningsmænd er i udlandet, kan sagen være vanskelig at efterforske. Og it-kriminelle kan hurtigt oprette nye falske domæner og spoofede telefonnumre, som gør nye phishing-forsøg svære at forhindre.

Ikke desto mindre forsøger flere myndigheder og virksomheder at forebygge, at it-kriminelle misbruger deres digitale kommunikation til at svindle borgere, ved at bruge forskellige teknologiske løsninger. Flere af myndighederne og virksomhederne beskriver dog udviklingen af teknologiske løsninger til at håndtere borgerrettet phishing og andre former for svindel som et 'kapløb' mod de it-kriminelle.

EN STØRRE FÆLLES INDSATS

Ovenstående analyse af den gensidige adfærdspåvirkning, der foregår mellem borgere, it-kriminelle, myndigheder og virksomheder i forbindelse med phishing, godtgør, at der er komplekse vilkår forbundet med phishing. Der er bl.a. adfærds-, ressource- og markedsmæssige, juridiske og teknologiske forhold, som samlet set gør phishing til et omsiggribende fænomen.

Og arbejdet med at identificere og igangsætte kompetenceudviklende og adfærdsændrende initiativer, som kan give borgere, virksomheder, myndigheder m.fl. en reflekteret forståelse af handlemuligheder og konsekvenser i forbindelse med phishing, må tage afsæt i viden om denne kompleksitet.

Når man søger efter mulige fokusområder for de kompetenceudviklende og adfærdsændrende initiativer, er det umiddelbart nærliggende at fremhæve borgernes uhensigtsmæssige digitale adfærd og i forlængelse heraf fremføre, at borgerne skal lære at udvise en mere sikker digital adfærd. Et fokus på borgernes digitale adfærd alene vil dog være en forsimpling af de vilkår, der gør sig gældende ved phishing.[94]

94 Oliveira, Daniela m.fl. (2020). The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behavior Research Methods. 1-11.

For som det fremgår, forsøger borgere allerede i dag at beskytte sig imod it-kriminelles forsøg på at svindle dem via phishing. Men det er vanskeligt for borgere at skelne it-kriminelles phishing-angreb fra myndigheders og virksomheders digitale kommunikation. Og velmenende anbefalinger om it-sikkerhed synes ikke at beskytte borgerne i tilstrækkelig grad – og særligt ikke, hvis de velmenende råd ikke er omsat til konkrete værktøjer til, hvordan borgerne kan følge dem i en travl hverdag.[95]

Man må således konstatere, at borgere alene ikke kan 'tage kampen op' mod it-kriminelle. For dels er det ikke muligt for borgere til fulde at beskytte sig imod phishing-angreb, dels er det ikke muligt for borgere at ændre på de vilkår, som er med til at gøre det bekvemt for it-kriminelle at svindle borgere via phishing. Det er f.eks. ikke muligt for borgere at fjerne it-kriminelles mulighed for at købe onlinehjælpepakker, forandre strafferammen for it-kriminalitet, få de it-kriminelle til at stoppe med at udnytte deres menneskelige bias m.v. "Det kræver en større fælles indsats" at beskytte borgernes personlige oplysninger på internettet, som en rådgiver fra CFCS påpeger.

Spørgsmålet er, hvad denne større fælles indsats rummer. Denne rapport alene vil ikke kunne udlægge, hvad den større fælles indsats bør bestå af. Men på baggrund af rapportens analyser kan der fremhæves en række væsentlige forebyggelsesindsatser, som kan udgøre grundlaget for det videre arbejde med at skabe kompetenceudviklende og adfærdsændrende initiativer til at styrke borgeres digitale sikkerhed. Disse forebyggelsesindsatser præsenteres i det følgende afsnit.

95 Frost, Lasse, Kristian Sørensen og Simon Bentholm (2017). For-analyse af danskernes informationssikkerhed. /KI.7, Digitaliseringsstyrelsen og Erhvervsstyrelsen.

FOREBYGGELSESINDSATSER

Forebyggelsesindsatserne tager afsæt i, at borgernes digitale sikkerhed kan styrkes på forskellige måder og ikke alene, ved at borgerne skal gøre noget andet og mere, end de gør i dag. Borgernes digitale sikkerhed kan også styrkes ved, at andre aktø rer arbejder med at forebygge it-kriminalitet på nye måder.

1 PARTNERSKABER OM NYE MÅDER AT FOREBYGGE IT-KRIMINALITET PÅ

Der kan med fordel dannes forpligtende partnerskaber mellem repræsentanter fra myndigheder, virksomheder og politi, som i fællesskab udvikler initiativer sammen, der har til formål at forebygge borgerrettet it-kriminalitet.

En række eksisterende netværk arbejder allerede på at øge borgeres digitale sikkerhed. Disse netværk skal udvikles og styrkes, så der også fremover findes stærke alliancer på tværs af myndigheder, virksomheder og politi.

I regi af disse forpligtende partnerskaber kan der bl.a. inviteres til konferencer eller gå-hjem-møder, hvor indsigter fra nærværende rapport præsenteres for en bredere kreds af professionelle aktører, der arbejder med forebyggelse af borgerrettet it-kriminalitet. I partnerskaberne kan der også afholdes workshops med relevante aktører med henblik på at udvikle fælles bæredygtige råd.

2 ERFARINGSUDVEKSLING OM IT-KRIMINELLES ANGREBSFORSØG

Flere af de myndigheder og virksomheder, der har deltaget i denne undersøgelse, efterspørger større mulighed for erfaringsudveksling om forsøg på angreb mod myndighedens eller virksomhedens it-infrastruktur.

I øjeblikket oplever mange myndigheder og virksomheder, at det er sårbart at dele erfaringer med brister på it-sikkerheden eller it-kriminelles forsøg på angreb mod myndighedens eller virksomhedens it-infrastruktur. For selvom der er villighed til og interesse for at dele erfaringer og gode råd, frygter mange myndigheder og virksomheder, at det kan have konsekvenser for deres kernevirksomhed. Frygten er, at myndigheden eller virksomheden vil blive opfattet som for dårligt rustet til at opretholde en tilstrækkelig grad af it-sikkerhed over for såvel borgere som medarbejdere. Af samme grund efterspørger flere virksomheder og myndigheder, at en fremtidig videndelingsplatform faciliteres af en neutral aktør. Ønsket er, at erfaringsudvekslingen om it-kriminelles angrebsforsøg både foregår internt og på tværs af myndigheder, virksomheder og politi.

3 UDVIKLING AF BEST PRACTICE-PRINCIPPER FOR DIGITAL KOMMUNIKATION

Myndigheder og virksomheder ønsker, at deres digitale kommunikation til både borgere og egne medarbejdere er sikker. Ikke desto mindre er der behov for at kunne kommunikere nemt og effektivt, og det betyder i mange tilfælde, at it-kriminelle har mulighed for at efterligne myndigheders og virksomheders digitale kommunikation. Dette skal ses i sammenhæng med, at it-kriminelle generelt bliver bedre til at udvikle vellignende phishing og smishing.

Virksomheder og myndigheder efterspørger derfor hjælp til at udvikle den digitale kommunikation, således at it-kriminelle har sværere ved at efterligne indholdet. Det gælder f.eks. brugen af logoer, tekst og links, der skal udvikles til at understøtte en mere sikker digital kommunikation. Der kan desuden med fordel tænkes i nye sikre kommunikationsplatforme som erstatning for 'åbne' mailprogrammer. Her kan tekniske løsninger blive en løftestang for mere sikker digital kommunikation.

4 AWARENESS-KAMPAGNER

Danske myndigheder udvikler løbende awareness-kampagner målrettet borgere med henblik på at styrke borgernes digitale sikkerhed. Disse awareness-kampagner kan med fordel lade sig inspirere af myndigheders og virksomheders erfaringer med awareness-kampagner for deres medarbejdere. Myndigheders og virksomheders awareness-kampagner har til formål at 'træne' medarbejderes evne til at genkende og rapportere phishing, f.eks. ved brug af en hackerknap eller konkurrencer.

Borgere og medarbejdere deler en række fælles vilkår ift. at håndtere henholdsvis borgerrettet og medarbejderrettet phishing. Bl.a. er både borgere og medarbejdere mennesker, der skal forholde sig til digital kommunikation i en travl hverdag. Men der er naturligvis også nogle vilkår, der er forskellige for borgere og medarbejdere ift. at håndtere borgerrettet og medarbejderrettet phishing. Derfor kan myndigheders og virksomheders tiltag i forbindelse med medarbejderrettet phishing ikke uden videre iværksættes til at styrke borgeres digitale sikkerhed. De kan dog tjene som inspiration til awareness-kampagner rettet mod borgere.

5 SIKRE MÅDER AT OPBEVARE PASSWORDS PÅ

Lækkede passwords samt for korte og usikre passwords er en lettilgængelig vej for it-kriminelle til at kompromittere borgeres digitale sikkerhed. Der er dermed et potentiale i at understøtte en sikker opbevaring af borgeres passwords gennem både teknologiske og adfærdsorienterede tiltag.

Derfor er der behov for at igangsætte nærmere undersøgelser af borgeres villighed til password-manager-programmer eller andre muligheder for sikker opbevaring. De eksperter, der er blevet interviewet til denne undersøgelse, peger enstemmigt på password-manager-teknologien som et godt og effektivt værktøj til at beskytte borgeres adgangskoder. Denne undersøgelse fremhæver, at blot 10 pct. af borgerne anvender password-manager-programmer, og at ældre borgere generelt er skeptiske over for password-manager-teknologien og efterspørger muligheder for at opbevare deres passwords fysisk. Til gengæld er unge mellem 18 og 39 år mere trygge ved password-manager og indstillede på at benytte teknologien.

6 IT-KRIMINELLE SKAL KONFRONTERES MED KONSEKVENSERNE

Der er behov for at forandre it-kriminelles syn på deres ofre som ansigtsløse datapunkter. For så længe it-kriminelle ikke skænker deres ofre en tanke, og kriminalitetens konsekvenser for deres ofre føles uvedkommende for de it-kriminelle, er der ikke nogen 'moralsk stopklods' for de it-kriminelle.

Derfor skal der skabes de rette rammer for, at it-kriminelle konfronteres med de konsekvenser, it-kriminaliteten har haft for deres ofre både psykisk og økonomisk. Indsatsen skal bidrage til at afholde tidligere it-kriminelle fra at 'falde tilbage' i en kriminel løbebane og kan med fordel foregå i samarbejde med aktører, der har erfaring med lignende indsatser.

KONKLUSION

Denne rapport har tilvejebragt dybdegående viden om adfærdsmønstre i relation til it-kriminalitet blandt borgere, it-kriminelle, myndigheder og virksomheder. Den tilvejebragte viden skal bidrage til at identificere og igangsætte kompetenceudviklende og adfærdsændrende initiativer, som kan give borgere, myndigheder, virksomheder m.fl. en reflekteret forståelse af handlemuligheder og konsekvenser i forbindelse med phishing. Det overordnede sigte med analysen er at mindske antallet af danskere, der bliver svindlet via it-kriminalitet.

Rapporten tager sit afsæt i, at Danmark har et stort udbud af digitale tjenester, og at den danske befolkning i den grad har omfavnet myndigheders og virksomheders digitale kommunikation. Borgernes stigende brug af digital kommunikation hænger sammen med, at danskerne generelt har stor tiltro og tillid til hinanden og den offentlige sektor, og derfor tør borgerne videregive deres personlige oplysninger til myndigheder og virksomheder.

Den stigende brug af digital kommunikation mellem borgere, myndigheder og virksomheder skaber utilsigtet en mulighed for, at it-kriminelle kan efterligne den digitale kommunikation og dermed svindle borgere, myndigheder og virksomheder. Et overordnet fokus for analysen er således, at myndigheders og virksomheders digitale kommunikation kan udnyttes i den borgerrettede svindel.

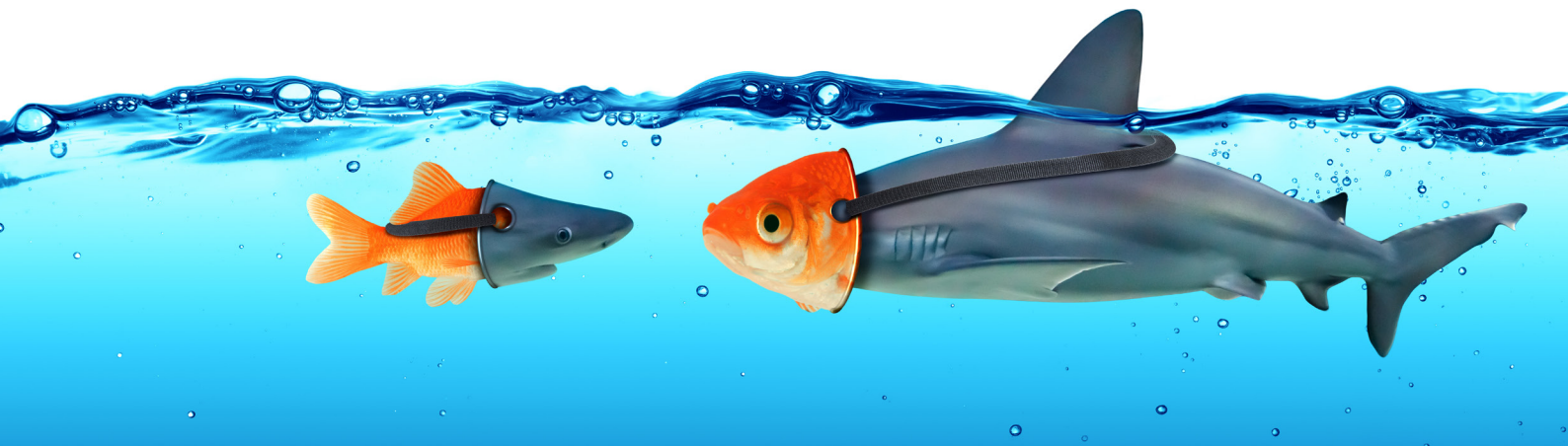
Rapporten konstaterer, at det er vanskeligt for borgere at skelne mellem it-kriminelles phishing-angreb fra myndigheders og virksomheders digitale kommunikation. Bl.a. fordi it-kriminelle bliver stadigt dygtigere til at formulere e-mails i troværdigt sprog og til at efterligne myndigheders og virksomheders logoer.

Rapporten påpeger også, at borgernes travle hverdagsliv er en væsentlig barriere for danskernes it-sikkerhed. For et utal af behov, gøremål og pligter påkalder sig borgernes opmærksomhed og fjerner fokus fra risikoen for at blive svindlet af it-kriminelle. Og eftersom mange anbefalinger om it-sikkerhed strider imod menneskets umiddelbare handle- og tankemønstre, følger borgerne ikke de velmenende anbefalinger, hvis de ikke får konkrete værktøjer til, hvordan de kan følge dem.

Rapporten godtgør, hvordan der foregår en gensidig adfærdspåvirkning mellem borgere, it-kriminelle, myndigheder og virksomheder i forbindelse med phishing. Og at der således er komplekse vilkår forbundet med phishing. Der er bl.a. adfærds-, ressource- og markedsmæssige, juridiske og teknologiske forhold, som samlet set gør phishing til et omsiggribende fænomen.

På den baggrund konkluderer rapporten, at borgere alene ikke kan 'tage kampen op' mod it-kriminelle. Det kræver en større fælles indsats at bekæmpe phishing. En indsats, der går på tværs af myndigheder, virksomheder og politi, og som tager højde for de komplekse vilkår, der gør sig gældende ved phishing.

Rapporten præsenterer afslutningsvis en række væsentlige forebyggelsesindsatser, som kan udgøre grundlaget for det videre arbejde med at skabe kompetenceudviklende og adfærdsændrende initiativer til at styrke borgeres digitale sikkerhed.



METODE

Denne rapport er udarbejdet af den antropologiske analyse- og rådgivningsvirksomhed Gemeinschaft i efteråret 2020. Den grundlæggende metode i undersøgelsen af årsag og virkning af digital risikoadfærd er desk research og kvalitative interviews.

Desk researchen består af danske og internationale publikationer om phishing, dataindsamling fra appen Mit digitale selvforsvar og danske og internationale vejledninger i digital sikkerhed. Desk researchen har kvalificeret undersøgelsens interviews og dannet afsæt for den videre analyse.

Der er gennemført 15 interviews og fire opfølgende interviews med repræsentanter fra politi, virksomheder og myndigheder og forskning. Derudover er der foretaget fire interviews med borgere og to interviews med tidligere it-kriminelle.

Borgere er blevet interviewet om deres oplevelser med phishing samt deres opfattelse af egen digitale sikkerhed, og virksomheder og myndigheder er blevet interviewet om deres håndtering af borgerrettet og medarbejderrettet phishing.

Forskere og repræsentanter fra politiet er blevet interviewet om it-kriminelles motiv og modus samt om, hvilke tendenser der kendetegner it-relateret økonomisk kriminalitet i dag. Endelig har interviewene med tidligere it-kriminelle bidraget med såvel viden om it-kriminelles organisering og kontekst som de it-kriminelles motiv og modus. Kortlægning af relevante aktører til interviews samt kvalificering af undersøgelsens empiriske materiale er foregået i tæt samarbejde med Det Kriminalpræventive Råd og Forbrugerrådet Tænk.

Der er gennemført interviews med følgende repræsentanter fra politi, virksomheder og myndigheder og forskning:

- Andreas Lieberoth, adfærdsforsker og lektor, Aarhus Universitet
- Sikkerhedskonsulent, en dansk bank
- Analysechef, analytiker og rådgiver, Center for Cybersikkerhed
- John V. Rasmussen, it-sikkerhedsspecialist og Kaare O. Nielsen, information security supervisor, Coop Teknologi, Coop Danmark A/S
- Eskil Sørensen, cybersikkerhedsformidler, DKCERT
- Senior IT Security Supervisor og Fraud Manager, DSB
- Sektionsleder og medarbejdere, politiets Landsdækkende center for it-relateret økonomisk kriminalitet (LCIK)
- Direktør for Teknologi og Organisation, Matas
- Leder af svindelbekæmpelse hos MobilePay
- Analytiker, Rigspolitiets Nationale Cyber Crime Center (NC3)
- Leder af team sociale medier, PostNord
- Afdelingschef og It-specialist, Sundhedsdatastyrelsen
- Chefkonsulent, Udviklings- og Forenklingsstyrelsen

LITTERATUR

Bonke, Jens og Anders Eiler Wiese Christensen (2018). *Hvordan bruger danskerne tiden?* Gyldendal.

Center for Digital Dannelse (2020). *Hvorfor så mange misforståelser på nettet?* Center for Digital Dannelse 2020. Link: https://digitaldannelse.org/vidensbase/hvorfor-sa-mange-misforstaelser/.

CFCS (2020). *Cybertruslen mod Danmark*. Center for Cybersikkerhed.

CFCS (2020). *Drømmer cyberkriminelle om tillidsfulde relationer?* Center for Cybersikkerhed.

CFCS (2020). *Trusselsvurdering: Cybertruslen mod Danmark under COVID-19-pandemien.* Center for Cybersikkerhed.

CFCS (2020). *Vejledning Passwordsikkerhed.* Center for Cybersikkerhed.

Dansk Erhverv (2020). *Dansk Erhvervs digitale politik – Vækst gennem digitalisering.* Dansk Erhverv.

Danmarks Statistik (2020). *Halvdelen har oplevet it-sikkerhedsproblemer.* Danmarks Statistik.

Det Kriminalpræventive Råd (2016). *Når forbrydelser bliver digitale – En antologi om IT-kriminalitet og adfærd på nettet.* Det Kriminalpræventive Råd.

Digitaliseringsstyrelsen (2016). *Et stærkere og mere trygt digitalt samfund.* Digitaliseringsstyrelsen.

DR (2019). 80-årige Bodil blev franarret NemID og 42.000 kroner: 'Han var så venlig og tiltalende'. *Danmarks Radio 2020.* Link: https://www.dr.dk/nyheder/indland/80-aarige-bodil-blev-franarret-nemid-og-42000-kroner-han-var-saa-venlig-og.

DR P3 (2020). Den sorte boks – Svindler edition. *DR P3 2020.* Link: https://www.dr.dk/radio/p3/den-sorte-boks-podcast/den-sorte-boks-podcast-2020-06-26-06-01.

DR (2020). 'Vi kommer og voldtager dig :-)'. Da Louise modtog dén mail, ændrede hendes liv sig med ét. *Danmarks Radio 2020.* Link: https://www.dr.dk/mitliv/vi-kommer-og-voldtager-dig-da-louise-modtog-den-mail-aendrede-hendes-liv-sig-med-et.

DR (2020). Hvem vil voldtage Louise: Konfrontation. *Danmarks Radio 2020.* Link: https://www.dr.dk/drtv/se/hvem-vil-voldtage-louise-konfrontationen_201890.

Ebner, Natalie C., Ellis M. Donovan, Lin Tian, Harold A. Rocha, Huizi Yang, Sandeep Dommaraju, Adam Soliman, Damon L. Woodard, Gary R. Turner, R. Nathan Spreng og Daniela S. Oliveira (2018). Uncovering Susceptibility Risk to Online Deception in Aging. *Journals of Gerontology: Psychological Sciences* 00(00): 1-12.

Epinion og Det Kriminalpræventive Råd (2015). *Kriminalitetsforebyggelse og kampagner – En litteraturgennemgang af kampagneteorier, -metoder og -strategier.* Epinion og Det Kriminalpræventive Råd.

Epinion og Forbrugerrådet Tænk (2019). Brugerevaluering af *'Mit digitale selvforsvar'*. Epinion og Forbrugerrådet Tænk.

Erhvervsministeriet (2018). *Strategi for Danmarks digitale vækst*. Erhvervsministeriet.

Finansministeriet (2018). *National strategi for cyber- og informationssikkerhed.* Finansministeriet.

Frost, Lasse, Kristian Sørensen og Simon Bentholm (2017). *For-analyse af danskernes informationssikkerhed.* /Kl.7, Digitaliseringsstyrelsen og Erhvervsstyrelsen.

Hasselbalch, Gry (2016). *Digital Tryghed – de væsentligste digitale udfordringer for forbrugere i Danmark.* Forbrugerrådet Tænk og TrygFonden.

Infosecurity (2015). Secure Your Future with a Virtual CISO. *Infosecurity 2015*. Link: https://www.infosecurity-magazine.com/opinions/secure-your-future-with-a-virtual/.

Infosec (2018). Fraud as a Service (FaaS): Everything You Need to Know. *Infosec 2020*. Link: https://resources.infosecinstitute.com/topic/fraud-as-a-service-faas-everything-you-need-to-know/.

IC3 (2020). Online Extortion Scams Increasing During the Covid-19 Crisis. *Internet Crime Complaint Center 2020*. Link: https://www.ic3.gov/Media/Y2020/PSA200420.

Karuppannan, Jaishankar (2008). Identity related Crime in the Cyberspace: Examining Phishing and its impact. *International Journal of Cyber Criminology* 2(1):10-15.

Kruize, Peter (2019). *Identitetsmisbrug belyst fra flere vinkler.* Det Kriminalpræventive Råd og Det Juridiske Fakultet, Københavns Universitet.

Larsen, Henrik, Torben B. Sørensen og Nicolai Devantier (2018). *Danskernes informationssikkerhed.* Digitaliseringsstyrelsen, KL, Danske Regioner, DKCERT og DeiC.

Larsen, Henrik, Torben B. Sørensen og Nicolai Devantier (2020). *Danskernes informationssikkerhed 2020*. Digitaliseringsstyrelsen, KL, Danske Regioner, DKCERT og DeiC.

Larsen, Henrik og Nicolai Devantier (2020). *DKCERT Trendrapport 2020*. DKCERT og DeiC.

Lian, Tian, Daniel E. Capecci, Donovan M. Ellis, Harold A. Rocha, Sandeep Dommaraju, Daniela S. Oliveira og Natalie C. Ebner (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Trans. Comput.-Hum. Interact 26(5)*:1-35.

Münster, Morten Sehested (2017). *Jytte fra Marketing er desværre gået for i dag – sådan bruger du adfærdsdesign til at skabe forandringer i den virkelige verden.* Gyldendal Business.

Oliveira, Daniela, Ziad M. Hakim, Natalie C. Ebner, Sarah J. Getz, Bonnie E. Levin, Tian Lin, Kaitlin Lloyd, Vicky T. Lai, Matthew D. Grilli og Robert C. Wilson (2020). The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. *Behavior Research Methods.* 1-11.

Pedersen, Anne-Julie Boesen, Britta Kyvsgaard og Flemming Balvig (2020). *Udsat for vold og andre former for kriminalitet.* Justitsministeriet.

Politi (2020). Analyse: Politiet har modtaget knap 27.000 anmeldelser om it-relateret økonomisk kriminalitet i 2019. *Rigspolitiet 2020.* Link: https://politi.dk/rigspolitiet/nyhedsliste/lcik-aarsanalyse/2020/06/24.

Politi (2019). Politiet advarer om at unge kan være muldyr for kriminelle. *Politi 2019.* Link: https://politi.dk/syd-og-soenderjyllands-politi/nyhedsliste/muldyr/2019/10/06.

Rajivan, Prashanth og Cleotilde Gonzalez (2018). Creative Persuasion: A Study on Adversarial Behaviors Strategies in Phishing Attacks. *Frontiers in Psychology* 9(135):1-14.

Shulzhenko, Nadiia og Snizhana Romashkin (2020). Internet fraud and transnational organized crime. *Juridical Tribune* 10(1):162-172.

Sikkerdigital.dk (2020). De digitale svindlere kender din adfærd. *sikkerdigital.dk 2020*. Link: https://sikkerdigital.dk/borger/etklik/svindlere-kender-din-adfaerd/.

Sikkerdigital.dk (2020). Livephish. *Sikkerdigital.dk 2020.* Link: https://sikkerdigital.dk/borger/etklik/livephish/.

Sikkerdigital.dk (2020). Tekniske minimumskrav for statslige myndigheder. *Sikkerdigital.dk 2020.* Link: https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav/.

Sikkerdigital.dk (2020). DMARC (anti-phishing). *Sikkerdigital.dk 2020*. Link: https://sikkerdigital.dk/myndighed/tekniske-tiltag/dmarc/.

Sikkerdigital.dk (2020). Et klik. *sikkerdigital.dk 2020*. Link: https://sikkerdigital.dk/borger/etklik/.

Tassy, Agnes, Monika Bille Nielsen og Ditte Trier Jakobsen (2020). *It-anvendelse i befolkningen – 2019*. Danmarks Statistik.

Tassy, Agnes, Monika Bille Nielsen (2020). *It-anvendelse i befolkningen 2020.* Danmarks Statistik.

Ted 2020. Why we fall for phishing emails – and how we can protect ourselves. *Ted 2020.* Link: https://ideas.ted.com/why-we-fall-for-phishing-emails-and-how-we-can-protect-ourselves/.

UN (2020). *United Nations E-Government Survey 2020.* United Nations.

Vishwanath, Arun, Tejaswini Herath, Rui Chen og Jingguo Wang (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems* 51(3):576-586.