Digitaliseringstyrelsen
KL
Danske Regioner
DKCERT
DeiC

Danskernes informationssikkerhed

December 2020

2020

Indhold

1. Resume

Denne rapport bygger på en undersøgelse, som analysebureauet MEGAFON A/S har gennemført i sommeren 2020 for Digitaliseringsstyrelsen, KL, Danske Regioner og DKCERT[1]. Rapporten er udarbejdet som led i Den fællesoffentlige digitaliseringsstrategi 2016-2020. Undersøgelsen giver en status på oplevelser med, kendskab til og adfærd inden for informationssikkerhed hos to grupper: Borgere og offentligt ansatte.

De fællesoffentlige parter og DKCERT har tidligere udarbejdet rapporter vedr. borgernes informationssikkerhed i 2013, 2014, 2015, 2016 og 2018. De offentligt ansatte indgik også i undersøgelsen i 2016 og 2018. Enkelte steder i analysen vil det derfor også være muligt at følge udviklingen på borgere og offentligt ansattes informationssikkerhed.

Rapporten er henvendt til alle aktører, der er interesseret i at få en status på informationssikkerheden i Danmark. Rapporten kan læses i sin helhed, hvorved læseren får et grundlæggende indblik i borgere og offentligt ansattes oplevelser, viden og adfærd inden for informationssikkerheden, eller den kan bruges til opslag i undersøgelsens enkeltdele.

Hovedkonklusioner vedr. borgernes informationssikkerhed

Analysen undersøger i hvilken grad, borgerne oplever udvalgte digitale trusler, hvordan de agerer, når de møder truslerne, samt hvilke konsekvenser truslen har haft for de ramte. Dernæst tager analysen temperaturen på borgernes efterlevelse af gode råd til en sikker digital adfærd. Endeligt undersøges, hvilke barrierer og drivere der er til stede, for at borgere kan opnå en bedre digital sikker adfærd.

Stigning i antallet af phishing-forsøg

Flere borgere oplever phishing-forsøg – 64 pct. har oplevet at blive udsat for forsøg på phishing inden for det seneste år – enten via mail, sms eller telefon. Dette er en stigning fra 2018, hvor 51 pct. oplevede truslen.

[1] DKCERT er Danmarks akademiske CSIRT (Computer Security Incident Response Team) og bygger på en vision om at skabe værdi for uddannelses- og forskningssektoren i form af øget informationssikkerhed. Det sker gennem offentliggørelse af viden om informationssikkerhed skabt gennem samarbejde med den offentlige og private sektor, forsknings- og undervisningsverdenen samt internationale samarbejdspartnere.

Mere specifikt har 52 pct. af borgerne i 2020 oplevet mail-phishing, 30 pct. sms-phishing og 21 pct. telefonisk phishing. De færreste oplyser at have faldet i phishing-fælden.

De fleste borgere angiver, at de slettede phishing-henvendelserne eller ikke foretog sig yderligere, og flere oplyser også, at de advarede omgangskredsen om phishing-forsøget. Tilbøjeligheden til at gøre noget efter at have modtaget en falsk mail, fx at ændre kodeord, stiger med alderen. Således er det kun 30 pct. af de 18-29-årige, der foretager sig forebyggende handlinger som følge af phishing-mails, mens 63 pct. af de 60+-årige handler forebyggende på baggrund af phishing-mails.

Omkring hver tiende snydes i nethandler
Borgerne handler mere og mere på nettet, og specielt under nedlukningen i foråret 2020 skete der en stigning i handel på nettet. Omkring en ud af ti oplever svindel i forbindelse med nethandel. Konsekvensen for disse borgere er oftest, at de aldrig får varen tilsendt (37 pct.), eller at de lider et økonomisk tab (38 pct.), som ikke er relateret til ikke at få varen tilsendt – fx uforklarlige træk på konto. Borgerne handler også i høj grad med hinanden via platforme som Facebook Marketplace, DBA mm. Her oplever omkring en ud af tyve at blive snydt, og også her er konsekvenserne oftest, at borgerne ikke får varen tilsendt (46 pct.), eller at de i øvrigt lider et økonomisk tab (51 pct.).

Borgerne efterlever oftere de "nemme" anbefalinger om god sikkerhedsadfærd
Siden 2018 har informationsportalen sikkerdigital.dk[2] været et af omdrejningspunkterne for kommunikation om informationssikkerhed til borgere, virksomheder og den offentlige sektor. Analysen undersøger, i hvilken grad borgerne efterlever de råd til daglig digital sikkerhed, der kommunikeres på sikkerdigital.dk.

Ni ud af ti borgere (89 pct.) angiver, at de i høj/meget høj grad efterlever anbefalingen om at beskytte deres trådløse netværk i hjemmet med en kode. Syv ud af ti borgere oplyser, at de i høj/meget høj grad efterlever anbefalingerne om automatisk opdatering af deres computer (71 pct.) og telefon/tablet (70 pct.). Efterlevelse af anbefalingen om brug af antivirus-produkter er en del højere på computer (73 pct.) end på telefon og tablet (41 pct.).

Mere end halvdelen af borgerne (54 pct.) angiver, at de høj/meget høj grad efterlever anbefalingen om at undgå at anvende åbne trådløse netværk, der ikke har en kode, eller hvor alle benytter samme kode, mens 24 pct. oplyser, at de efterlever anbefalingen om anvendelse af VPN-forbindelse, når de bruger trådløse netværk.

[2] Digitaliseringsstyrelsen og Erhvervsstyrelsen står bag sikkerdigital.dk i samarbejde med en række samarbejdspartnere.

Lidt under halvdelen angiver, at de i høj/meget høj grad efterlever anbefalingen om jævnligt at tage sikkerhedskopi af data på computer (44 pct.) og tablet/telefon (46 pct.).

Kodeord er den af anbefalingerne, de færreste oplyser at efterleve. Kun 16 pct. oplyser, at de i høj/meget høj grad efterlever anbefalingen om, at et kodeord er over 12 tegn og ikke genbruges flere steder. 17 pct. oplyser, at de i høj/meget høj grad efterlever anbefalingen om brug af passwordmanager, mens 37 pct. oplyser, at de i høj/meget høj grad efterlever anbefalingen om to-faktorlogin. Ydermere angiver kun 42 pct., at de i høj/meget høj grad efterlever anbefalingen om, at kodeord til fx mail, NemID mv. skal være forskellige.

Overordnet set tegner der sig et billede af, at de anbefalinger, hvor man "blot" skal slå en funktion til som fx automatisk opdatering[3] eller beskyttelse af netværk med kode, i højest grad bliver efterlevet. De anbefalinger, der kræver aktive handlinger (fx sikkerhedskopi), kognitiv energi (lange og unikke kodeord) eller teknisk indsigt (VPN og passwordmanager) efterleves sjældnere.

Jo mere opmærksomme borgere er på trusler, jo bedre adfærd udøver de
74 pct. af borgerne angiver at være opmærksomme på risikoen for bedrageri og cyberkriminalitet. Dette er sammenligneligt med niveauet for 2018. Ligeledes kan resultaterne fra 2018 og 2020 sammenlignes, når det kommer til, hvorvidt borgerne mener, at risikobetonet adfærd medfører øget risici for fx tab af data (omkring 90 pct. for begge år). Endelig er der også overensstemmelse mellem 2018 og 2020, ift. hvor godt borgerne føler sig klædt på til at beskytte sig mod de digitale trusler (hhv. 61 og 64 pct.).

I denne analyse er der en sammenhæng mellem, at de borgere, der er opmærksomme på trusler og risikobetonet adfærd samt føler sig godt klædt på, i højere grad angiver at efterleve de gængse anbefalinger til daglig sikkerhedsadfærd.

Efterlevelse opnås, når ønsket adfærd ikke er krævende
Dog er opmærksomhed på digitale trusler i sig selv ikke tilstrækkeligt til, at borgerne generelt efterlever anbefalingerne til god daglig sikkerhedsadfærd. Analysen har undersøgt de barrierer og drivere, som borgerne selv angiver, har betydning for deres efterlevelse af anbefalinger.

De yngste borgere (18-29 år) angiver i højere grad end øvrige aldersgrupper, at det er manglende tid/overskud, der er årsagen til, at de ikke altid efterlever anbefalingerne. De ældste borgere angiver i højere grad manglende viden som årsag til, at de ikke efterlever anbefalingerne.

De fleste borgere oplyser, at deres efterlevelse af de gode sikkerhedsråd ville forbedres, hvis rådene var mindre besværlige at efterleve (50 pct.), samt at det skulle være bedre formidlet, hvad man skulle gøre (31 pct.). Interessant her er også, at

[3] Visse opdateringer kræver dog brugerens aktive handling, fx genstart af enhed.

andelen, der svarer, at ingenting kan få dem til at få en mere sikker adfærd, bliver større med alderen.

Samlet set kan konkluderes, at hvis det synes krævende at ændre sin digitale adfærd, er det svært at finde overskud til at få det gjort. Yderligere påviser analysen, at der er højest efterlevelse af de anbefalinger, der er lettest at efterleve. Det lader til, at borgerne gerne prioriterer tiden til at efterleve anbefalinger, hvis det synes tilgængeligt og ikke for tidskrævende at udføre den ønskelige adfærd.

Arbejdspladser og uddannelsesinstitutioners uddannelsesindsatser smitter af på privaten
De fleste oplyser, at de får deres viden om informationssikkerhed fra nyhedsmedier, tv, magasiner og aviser (60 pct.) samt omgangskredsen (54 pct.). Mange angiver dog også arbejdspladsen eller uddannelsesinstitutionen som kilde til deres viden (45 pct.). Sidstnævnte repræsenterer en stor stigning i forhold til 2018 (28 pct.). Stigningen lader til at være sket på bekostning af at få ens viden fra nyhedsmedier, tv, magasiner og aviser (72 pct. i 2018) samt sociale medier (38 pct. i 2018). Analyser peger på, at jo mere formel kilden til viden er, i jo højere grad har man en adfærd, der er kompatibel med den risiko, man udsætter sig for.

Forældres sikkerhedsadfærd smitter af på børnene
Der er overordnet set sket en stigning i andelen af borgere, der hjælper deres børn med at have en god digital adfærd på nettet i forhold til andelen i 2018. Derudover lader der til at være en tendens til, at forældre, der i højere grad efterlever sikkerhedsanbefalinger, også i højere grad hjælper deres børn med at have en god adfærd. Til eksempel ses en klar sammenhæng mellem den voksnes efterlevelse af anbefalingen om lange, unikke kodeord og hjælp til børn om det samme. Således oplyser 92 pct. af de, der i høj/meget høj grad efterlever anbefalingen om lange, unikke kodeord, at de (eller en anden i husstanden) hjælper deres barn med, at kodeord skal være lange, unikke og personlige.

Hovedkonklusioner vedr. offentligt ansattes informationssikkerhed

Analysen undersøger i hvilken grad, de offentligt ansatte har oplevet udvalgte digitale trusler, samt hvordan de agerer, når de møder truslerne. Dernæst gøres status på dels de offentligt ansattes efterlevelse af gængse informationssikkerhedsretningslinjer på arbejdspladsen samt på deres efterlevelse af retningslinjer, der går på hjemmearbejde. Endeligt undersøges barrierer og drivere for, at offentligt ansatte har en sikker digital adfærd og efterlever arbejdspladsers retningslinjer for informationssikkerhed.

Knap halvdelen af offentligt ansatte udsættes for forsøg på phishing
Inden for det seneste år har op mod halvdelen af de offentligt ansatte (46 pct.) i forbindelse med deres arbejde prøvet at modtage mail, sms eller chat-besked fra en ukendt person med et link, som afsenderen opfordrede til at klikke på, hvilket er sammenligneligt med 2018 (48 pct.). De fleste offentligt ansatte oplyser, at de som det første sletter beskeden. Derudover oplyser mange offentligt ansatte, at de følger arbejdspladsens retningslinjer. Disse kan ret beset indeholde at slette

mailen, men det er vigtigt at få viden om efterlevelsen, da retningslinjerne netop er udtryk for den praksis, de enkelte offentligt ansatte skal følge. Hver arbejdsplads' trusselsbillede og dermed ønskede handlinger kan være forskellige. I modsætning til forsøg på phishing, så er det de færreste offentligt ansatte (3 pct.), der har oplevet virus eller andre typer skadelige programmer i forbindelse med arbejdet inden for det seneste år. Dette er et markant fald fra 2018 (11 pct.), der dog kan skyldes en ændring i spørgemåden, eller at myndighederne er blevet bedre til at beskytte sig mod denne trussel. Endnu færre (1 pct.) har oplevet, at et program spærrede for adgangen til deres arbejdscomputer eller data og krævede betaling for at åbne dem (ransomware).

Flere håndterer fortrolige og følsomme oplysninger sikkert
Offentligt ansattes daglige adfærd på arbejdspladsen er afgørende for, at organisationer er sikre. Kodeord er ligesom for private borgere en udfordring for de offentligt ansatte. Umiddelbart ses et positivt fald fra 2018 (37 pct.) til 2020 (26 pct.) i andelen af offentligt ansatte, der genbruger kodeord til flere systemer og tjenester. Dog ses samtidig, at 22 pct. anvender samme kodeord privat som på arbejdet.

Retningslinjerne vedrørende håndtering af information er bedre forankrede end kodeordspolitikkerne. Således angiver de fleste at efterleve retningslinjerne om at låse computeren (85 pct.), om at bruge "sikker print"-løsninger (80 pct.) og om at bære synligt id-kort (85 pct.), såfremt arbejdspladsen har retningslinjer om dette. Når det kommer til at håndtere fortrolige og følsomme oplysninger sikkert, er der sket en stigning i antallet af offentligt ansatte, der i hverdagen sender denne type oplysninger (fra 30 pct. i 2018 til 38 pct. i 2020). Blandt de offentligt ansatte, der håndterer disse oplysninger, er der sket en stigning i andelen, der sender fortrolige oplysninger til borgere eller andre via sikre kanaler (77 pct. i 2018 til 85 pct. i 2020). Samtidig ses et fald fra 21 pct. i 2018 til 9 pct. i 2020 af offentligt ansatte, der sender denne type oplysninger via arbejdsmail/åbent mailsystem.

COVID-19-pandemien sætter pres på retningslinjer for hjemmearbejde
Under nedlukningen af flere offentlige arbejdspladser i 2020 er hjemmearbejde for mange blevet hverdag, og flere organisationer står derfor i nye og vigtige opgaver ift. at sikre hjemmearbejdspladserne. De fleste offentligt ansatte (63 pct.) oplyser, at de blev godt klædt på til at arbejde hjemmefra på sikker vis.

Dog angiver 23 pct., at de bruger en privat computer eller en blanding af arbejdscomputer og privat computer til at arbejde hjemmefra. Brug af privat computer i arbejdsmæssig sammenhæng er problematisk, hvis den ikke er godkendt af arbejdspladsen. Specielt adgange til systemer, automatiske sikkerheds- og antivirusopdateringer, automatisk back up og håndtering af informationer kan være vanskeligt på en privat computer, der er uden for arbejdspladsens miljø.

Fildelingstjenester er en populær metode til udveksling af større arbejdsdokumenter, der ikke kan håndteres via fx Outlook. To tredjedele af de, der benytter

fildelingstjenester, oplyser, at de anvender de tjenester, som arbejdspladsen stiller til rådighed, mens en tredjedel anvender andre tjenester, som de selv finder.

Kommunikationskanaler som Skype, Teams og Zoom benyttes flittigt til virtuelle møder ved hjemmearbejde. 91 pct. af de offentligt ansatte, der benytter kommunikationskanaler, angiver, at de bruger de kanaler, der er stillet til rådighed af arbejdspladsen.

Samlet set oplyser 14 pct. af de offentligt ansatte, at deres arbejdsplads ikke har retningslinjer for brug af disse fildelingstjenester og kommunikationskanaler i forbindelse med hjemmearbejde, og hele 23 pct. ved ikke, om der er retningslinjer[4].

Endelig har analysen spurgt til, hvordan trådløse netværk anvendes, når de offentligt ansatte ikke arbejder inden for arbejdspladsens fysiske rammer. Her ses, at 35 pct. af de offentligt ansatte anvender en VPN-forbindelse i forbindelse med arbejde uden for arbejdspladsen, og 53 pct. oplyser, at de bruger et privat hjemmenetværk med kode.

Sammenhæng mellem opmærksomhed på digitale trusler og efterlevelse af retningslinjer
Ligesom for borgerne ses det i undersøgelsen blandt de offentligt ansatte, at der er en tendens til at: Jo mere opmærksom man angiver at være på bedrageri og cyberkriminalitet, og jo mere man mener, at risikobetonet adfærd udgør en sårbarhed, des oftere angiver man også, at man kender arbejdspladsens retningslinjer for informationssikkerhed, samt at man følger dem.

Et par observationer understøtter sammenhængen mellem opmærksomheden og den konkrete adfærd, som de offentligt ansatte har oplyst. Jo mere opmærksom den offentligt ansatte er, jo oftere: Anvendes forskellige adgangskoder til forskellige systemer, låses computeren når den forlades, anvendes VPN ved hjemmearbejde og følges arbejdspladsens retningslinjer ved phishing-forsøg – blot for at tage et par eksempler.

Fald i offentligt ansattes efterlevelse af informationssikkerhedspolitikker og -retningslinjer
65 pct. af respondenterne angiver, at de i høj/meget høj grad er bekendte med de informationssikkerhedspolitikker og/eller retningslinjer, der er gældende for deres arbejde, hvilket er sammenligneligt med 2018. Der ses en lille stigning i andelen af offentligt ansatte, der har modtaget undervisning eller information om retningslinjerne (fra 63 pct. i 2018 til 69 pct. i 2020).

Samtidig er der sket en stigning i antallet af respondenter, der angiver, at de til tider undlader at følge retningslinjerne: I 2018 undlod 8 pct. til tider at følge retningslinjerne, mens det gælder for 15 pct. i 2020. 32 pct. angiver i 2020, at de enten ikke ved, hvor ofte de undlader at følge retningslinjerne, eller at de mindst en gang om ugen eller oftere undlader at efterleve dem. Stigningen i andelen, der til

[4] Dataindsamlingen er sket fra den 29. juni til d. 14. juli. Der kan som en konsekvens af COVID-19 være sket ændringer i forhold til spørgsmålet siden.

tider undlader at følge retningslinjerne, må siges at være problematisk. Stigningen kan være et udtryk for, at hjemmearbejde har gjort det sværere at efterleve retningslinjerne. Uanset diagnosen bør udviklingen give anledning til refleksion på arbejdspladserne.

Informationssikkerhedspolitikker og -retningslinjer skal være nemmere og mere relevante
Blandt de offentligt ansatte, der svarer, at de til tider undlader at efterleve arbejdspladsens informationssikkerhedsretningslinjer og -politikker, svarer flest, at det skyldes, at det gør deres daglige arbejde besværligt/umuligt at udføre (61 pct.). 32 pct. angiver, at de selv vurderer, om det er nødvendigt at efterleve i de enkelte arbejdssituationer.

De offentligt ansatte er også blevet spurgt til, hvad der skulle ændres for, at de oftere ville efterleve arbejdspladsens informationssikkerhedspolitikker og -retningslinjer. Næsten halvdelen (48 pct.) oplyser, at det skulle være nemmere at efterleve reglerne. Yderligere 24 pct. angiver, at retningslinjerne skulle være mere relevante for deres arbejde.

Arbejdspladser bør således overveje, hvordan den ønskede adfærd bliver nemmere at gå til for de ansatte, uden at det går ud over den ansattes kerneopgave – enten via stærkere formidling eller organisatoriske/tekniske tiltag, der støtter den ansatte i oftest at træffe det ønskede valg. Yderligere bør arbejdspladser overveje, hvad der er det rigtige niveau af sikkerhed for respektive medarbejdergrupper, således at retningslinjerne anses som relevante for den enkelte.

Rapportens opbygning

Rapporten er opdelt efter to respondentgrupper.

Borgernes informationssikkerhed omtales i kapitel 2-4. Kapitel 2 omhandler digitale trusler, borgerne oplever, hvordan de agerer i relation til truslen samt truslens konsekvens for den udsatte. Kapitel 3 tager temperaturen på borgernes efterlevelse af en række råd til sikker adfærd, og kapitel 4 undersøger borgernes opmærksomhed på digitale trusler, deres barrierer og drivere for at have en sikker digital adfærd samt deres kilder til viden om informationssikkerhed.

Offentligt ansattes informationssikkerhed fremgår af kapitel 5-8. Kapitel 5 omhandler de trusler, de udsættes for, samt hvordan de offentligt ansatte agerer i mødet med truslerne. Kapitel 6 undersøger offentligt ansattes adfærd i daglige situationer på arbejdspladsen, mens kapitel 7 stiller skarpt på deres adfærd, når de arbejder et andet sted end den fysiske arbejdsplads. Kapitel 8 undersøger opmærksomheden på digitale trusler, kendskabet til og efterlevelsen af arbejdspladsens informationssikkerhedspolitikker og -retningslinjer samt barrierer og drivere for oftere at efterleve retningslinjerne.

Kapitel 9 indeholder forklaring på de fagudtryk, der anvendes i analysen, mens kapitel 10 uddyber metodetilgangen.

Borgernes informationssikkerhed

2. Borgerrettede trusler og deres konsekvenser

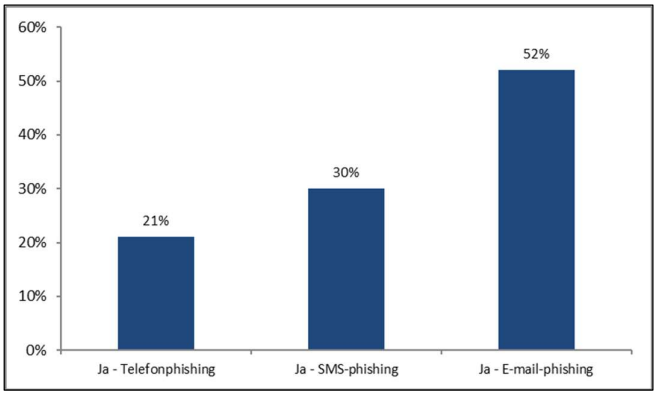
Kapitlet undersøger, i hvilken grad borgerne oplever udvalgte digitale trusler, hvordan de agerer, når de møder truslerne, samt hvilke konsekvenser truslen har haft for de ramte.

Phishing – den hyppigst oplevede trussel

Phishing[5] er vejen ind til data. Phishing er, når it-kriminelle enten via mails, sms ("smishing") eller telefonopkald ("vishing" – voice phishing) forsøger at franarre borgerne deres personlige oplysninger som fx betalingskortoplysninger, NemID-oplysninger eller andre private oplysninger. Phishing er også en metode til at lokke individer til at klikke på links eller downloade dokumenter og filer, der viser sig at indeholde skadelig malware. Malware, der så kan installeres på ofrenes enheder og gøre skade, gøre dem til en del af et botnet[6] eller på anden måde udføre skadelige handlinger, evt. med cyberkriminalitet for øje.

At phishing bliver stadig mere udbredt – selv om det er en relativt gammel metode – er et udtryk for, at det virker og er billigt at udføre. Center for cybersikkerhed har ydermere i en trusselsvurdering fra november 2020 vurderet, at phishingmails i dag indgår i de fleste cyberangreb, og at de udgør en alvorlig trussel mod alle myndigheder, virksomheder og borgere i Danmark.[7]

64 pct. af danskerne har oplevet et phishing-forsøg via mail, sms eller telefon inden for det seneste år, mens 8 pct. har oplevet alle tre former for phishing. 52 pct. oplyser, at de har været udsat for et eller flere forsøg på mail-phishing inden for det seneste år (figur 1). Hvad sms-phishing (smishing) og telefon-opkald-phishing (vishing) angår, har hhv. 30 pct. og 21 pct. oplevet det en eller flere gange inden for det seneste år.



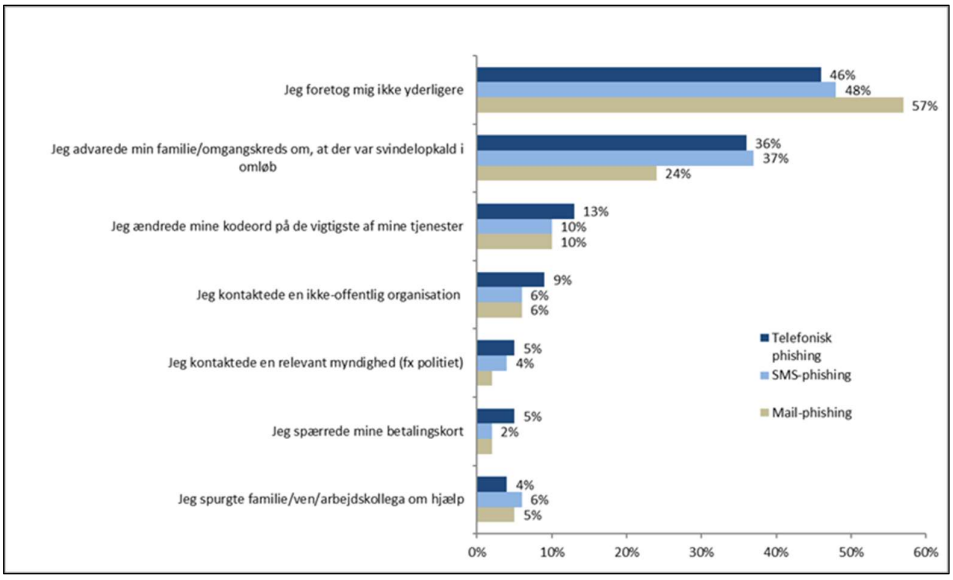
Figur 1 Borgernes oplevelser af telefonisk, sms- og mailphishing.

[5] Se ordforklaring i kapitel 9, side 68.
[6] Se ordforklaring i kapitel 9, side 67.
[7] https://cfcs.dk/da/cybertruslen/trusselsvurderinger/phishing/

I 2016 og 2018 blev der spurgt til fænomenet "phishing", uden at respondenterne havde mulighed for at svare differentieret i forhold til phishingkanal. Fra 2016 til 2018 var der et fald fra 58 pct. til 51 pct. i andelen af borgere, der havde været udsat for forsøg på phishing. Dermed er der fra 2018 til 2020 sket en markant stigning i antallet af oplevede phishing-forsøg, fra 51 pct. i 2018 til 64 pct. i 2020.

Heldigvis synes borgerne at være godt med på denne trussel, idet kun 2 pct. af respondenterne i 2020 faktisk udleverer de efterspurgte oplysninger ved enten e-mail-, sms- eller telefon-phishing. Når truslen stadig er så tilstedeværende på trods af angiveligt lavt succes, kan det hænge sammen med selve forretningsmodellen for nogle typer af phishing: Svindlerne sender massevis af mails, sms'er mm. ud, som rammer mange i håb om, at blot få falder i, og de dermed kan opnå økonomisk gevinst eller gevinst i form af brugernes data.

Borgernes ageren efter et phishing-forsøg tyder på, at det er en trussel, som borgerne er forholdsvist vant til (figur 2). Således angiver de fleste, at de intet foretager sig, hvilket sandsynligvis er et udtryk for netop at ignorere eller slette henvendelsen (eller lægge på). Dette stemmer med myndighedernes gængse anbefalinger angående phishing-henvendelser.



Figur 2 Borgernes angivelse af handlinger som følge af oplevelser med hhv. telefon-, SMS- og mail-phishing. Figuren viser kun, hvad borgerne har gjort som den første handling.

Der er en lyst til at advare omgangskredsen blandt borgerne, når det kommer til phishing. Det er positivt, da det kan bidrage til at skabe en endnu højere sikkerhedsbevidsthed blandt borgerne.

Når det handler om sms- og telefonisk phishing, er der flere, der advarer omgangskredsen, nemlig hhv. 37 pct. (smishing) og 36 pct. (vishing). Det kan skyldes, at smishing og vishing i kontekst af cyberkriminalitet er nyere end mailphishing, og at der derfor i højere grad er opmærksomhed på denne trussel. Derudover kan trusler på ens telefon føles mere personligt rettet end mailphishing, hvorfor flere agerer på dette.

Der ses en tendens til, at desto ældre respondenterne er, desto flere foretager sig forebyggende handlinger efter forsøg på sms-phishing (smishing).

Blandt de 18-29-årige er det således kun lidt mere end hver tredje (38 pct.), der handler på smishing fx med at ændre kodeord, mens denne andel stiger med alderen og er på 2 ud af 3 (67 pct.) blandt de 60+-årige.

Tilbøjeligheden til at handle på mail-phishing stiger ligeledes med alderen. Således er det kun 30 pct. af de 18-29-årige, der foretager sig forebyggende handlinger som følge af phishing-mails, mens 63 pct. af de 60+-årige handler forebyggende på baggrund af phishing-mails.

Nethandel – et spørgsmål om tillid

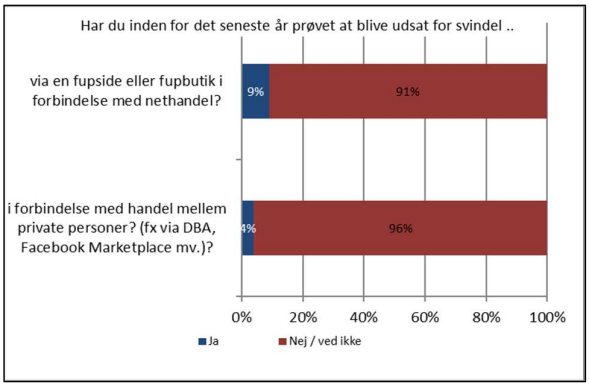
Nethandel har oplevet en stigning gennem de sidste mange år og ikke mindst under coronakrisen i foråret 2020. En opgørelse fra Foreningen af danske internethandlende (FDIH)[8] viser, at der er sket en stigning på 5 pct. i nethandel i Danmark i første halvår 2020 i forhold til samme periode 2019. FDIH's omsætningstal viser, at en stor del af stigningen kan tilskrives nedlukningsperioden fra marts til maj.

Desværre tiltrækker den øgede trafik kriminelle, der benytter det store fokus på nethandel til selv at gøre forretninger – forretninger som både kan relateres til falske webshops eller misbrug af tilliden mellem privatpersoner, hvis kontakten mellem de handlende er skabt via platforme som fx DBA, eBay, Facebook Marketplace mv. Således oplyser 9 pct. af borgerne, at de har oplevet svindel i forbindelse med nethandel en eller flere gange inden for det seneste år, mens 4 pct. har oplevet svindel i forbindelse med handel mellem private (figur 3).

37 pct. af de borgere, der har været udsat for svindel i forbindelse med nethandel, får aldrig varen tilsendt, mens 38 pct. lider et økonomisk tab, som ikke er relateret til ikke at få varen tilsendt – fx uforklarlige træk på konto (figur 4). Det er interessant, at så relativt mange (30 pct.) ikke oplever konsekvenser ved et svin-

[8] https://www.fdih.dk/analyser/fdih-e-handelsanalyser/ars-og-halvars-rapporter/e-handelsanalysen-1-halvar-2020#

delforsøg. Det kan tyde på en god skepsis hos 30 pct. af "de udsatte", som opfanger forsøget på svindlen uden at afgive de kritiske oplysninger, der kan føre til økonomisk tab. Det kan også være udtryk for, at banken dækker det økonomiske tab, hvorfor borgerne ikke angivet tabet.

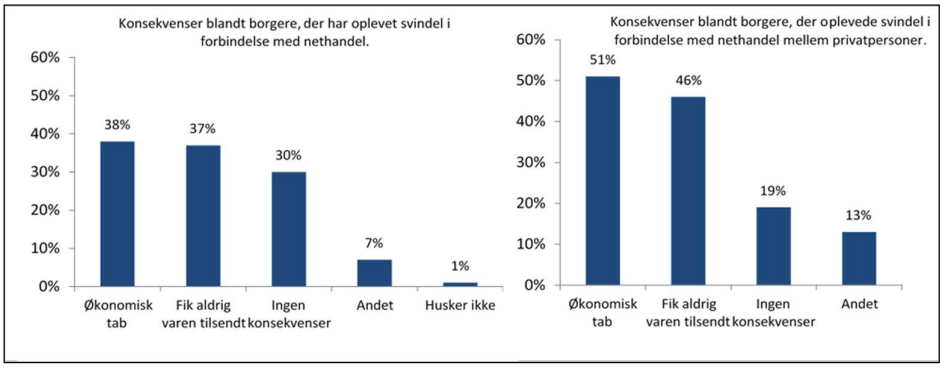


Figur 3 Borgernes oplevelser med svindel i forbindelse med nethandel og samhandel.

Blandt de borgere, der har oplevet svindel ifm. nethandel mellem privatpersoner, fik 51 pct. aldrig varen tilsendt, 46 pct. led i øvrigt et økonomisk tab, og 19 pct. oplevede ikke konsekvenser.

Således kan det tyde på, at borgerne har sværere ved at opfange svindel ved samhandel på diverse platforme – sandsynligvis fordi handel på disse platforme er mindre formaliseret end nethandel hos fx online-butikker. Der er sjældent faste krav til gennemførslen af handlen, hvilket giver svindlere mere spillerum.

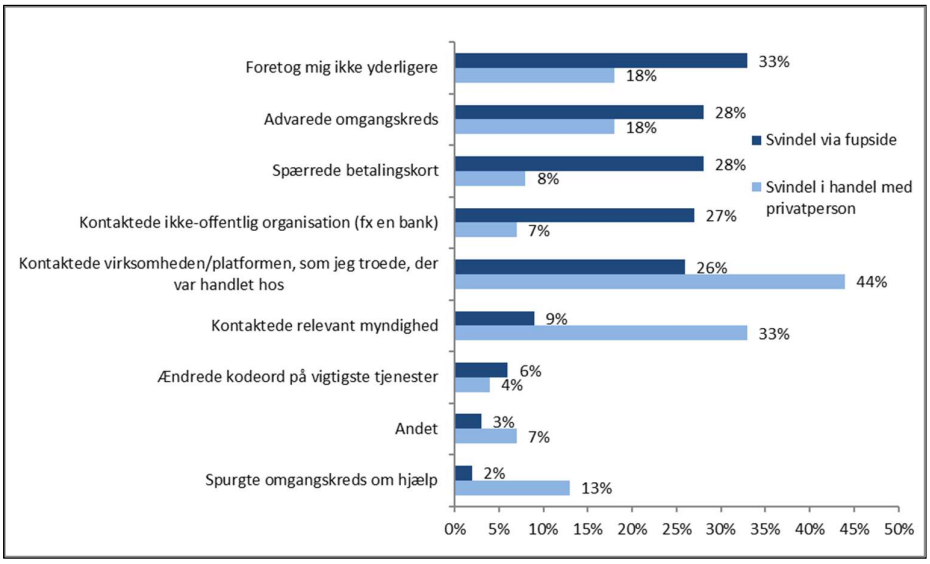
Når man kigger på de handlemønstre, som borgerne angiver efter at have oplevet hhv. svindel ved nethandel og ved samhandel tegner sig et interessant mønster: Når borgerne bliver udsat for svindel ved samhandel mellem private perso-



Figur 4 Borgernes angivelse af konsekvenserne ved svindel ved nethandel med butikker og mellem privatpersoner.

ner via platforme, er de meget mere tilbøjeligt til at efterspørge hjælp hos myndigheder, omgangskreds og samhandelsplatformene end ved nethandelssvindel. Det kan have at gøre med, at bagmændene ved en fupwebshop som oftest ikke er til at identificere eller finde, mens samhandler i højere grad indeholder har kontaktinformationer og dermed sandsynligvis bedre mulighed for at hjælpe brugerne i de tilfælde, hvor en handel går galt.

Når borgerne bliver udsat for svindel ved nethandel, er handlemønstrene mere spredte. Flere borgere spærrer deres betalingskort end ved samhandel, hvilket kan hænge sammen med, at dette i højere grad er det dominerende betalingsmiddel ved nethandel. Det er interessant, at så mange (33 pct.) ikke foretager sig noget efter at have oplevet svindel ved nethandel ift. svindel ved samhandel. Igen kan det måske hænge sammen med den manglende viden om den konkrete svindler, da ved nethandel ikke er knyttet en profil til svindleren. Yderligere kan det være udtryk for manglende viden om ens muligheder og rettigheder ved nethandelssvindel (figur 5).



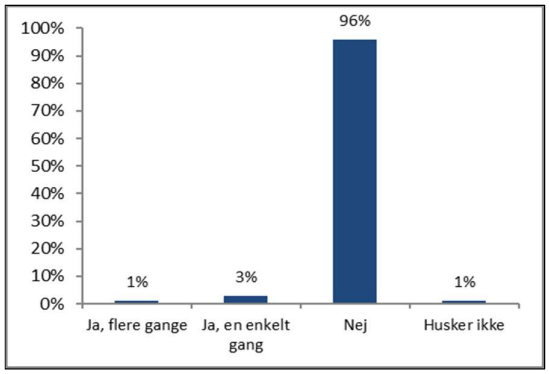
Figur 5 Borgernes handlinger efter svindel ifm. nethandel mellem privatpersoner og med butikker.

Det er bemærkelsesværdigt, at advarsel til omgangskredsen fylder så meget som 28 pct. ved butikssvindel og 18 pct. ved svindel ifm. privat samhandel. Det siger noget om en sund sikkerhedskultur, hvor mange borgere ønsker at tage ansvar for at øge sikkerheden og beskytte andre mod at komme i klemme.

Virus og skadelige programmer – altid en trussel

Virus[9] og malware er ondsindede programmer, der har til formål at skade brugerens computer og de data, der ligger på den. Det kan gøre stor skade på kort tid, derfor er det vigtigt at sikre sig imod. Fx kan virus og malware slette data, forhindre adgang til tjenester eller stjæle informationer. Virus kan sprede sig ved at kopiere sig ind i andre programmer. Det kan være svært for den almindelige bruger

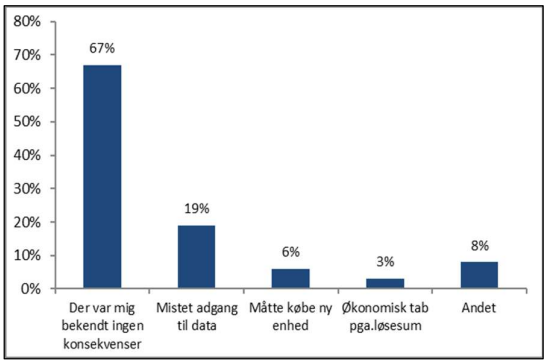
[9] Se ordforklaring i kapitel 9, side 71.



Figur 6 Borgernes svar på, om de inden for det seneste år har oplevet virus eller lignende skadelige programmer.

at kende forskel på, om det er en virus eller malware, der har forvoldt skade; derfor spørges der i undersøgelsen til symptomet (oplevelse af spærret computer eller programmer) frem for diagnosen (virus, malware mm.).

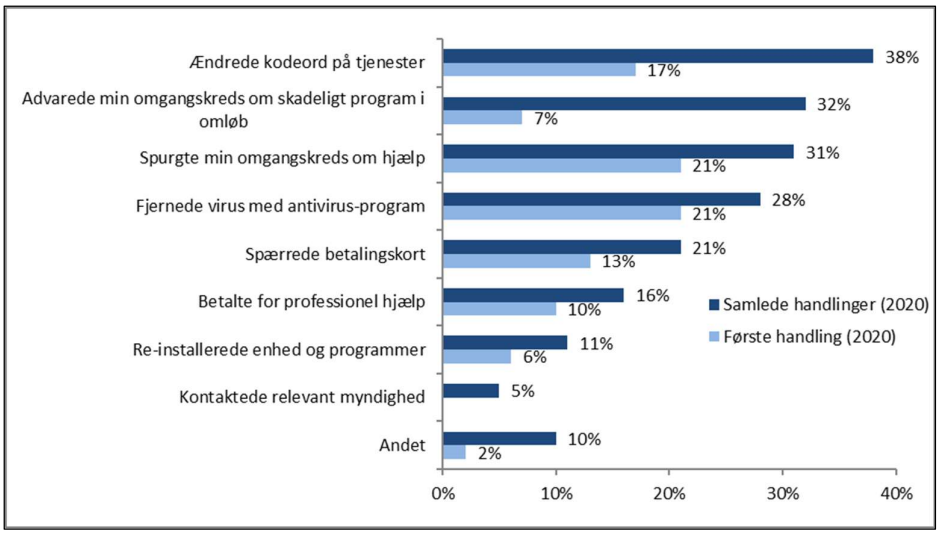
4 pct. af borgerne (figur 6) har inden for det seneste år oplevet at blive ramt af virus og andre skadelige programmer en gang (3 pct.) eller flere gange (1 pct.). Af disse har det for 67 pct. ikke haft nogen konsekvenser, mens det for 19 pct. af borgerne har haft den konsekvens, at de har oplevet at miste adgang til data, og 6 pct. har måttet købe en ny enhed, mens tre procent har lidt et økonomisk tab som følge af, at de har skulle betale en løsesum (figur 7).



Figur 7 Borgernes angivelse af oplevede konsekvenser ved at blive ramt af skadelige programmer.

I de tidligere undersøgelser har vi spurgt om borgernes gennemgående oplevelser med virus og andre typer skadelige programmer hen over årene. I 2018 svarede 34 pct., at de på et tidspunkt havde oplevet (dvs. ikke kun inden for det seneste år), at deres pc var inficeret med virus og andre typer skadelige programmer. Det repræsenterede en stigning på 3 pct.-point fra 31 pct. i 2016.

Hvad gør man så, når man har været udsat for virus og malware? Vi har formuleret spørgsmålet, så respondenterne har haft mulighed for at prioritere deres handlinger for at se det dominerende handlingsmønster (figur 8). De fleste fjerner virus med antivirusprogram (21 pct.) og spørger omgangskredsen om hjælp (21 pct.) som det første. 13 pct. oplyser, at de spærrer for deres betalingskort som det første, mens 10 pct. betaler for professionel hjælp. 17 pct. oplyser, at de som det første ændrer deres kodeord på tjenester, hvilket er fornuftigt at gøre,



Figur 8 Borgernes handlinger efter oplevelser med virus og andre skadelige programmer. Op til tre svar er angivet i prioriteret rækkefølge.

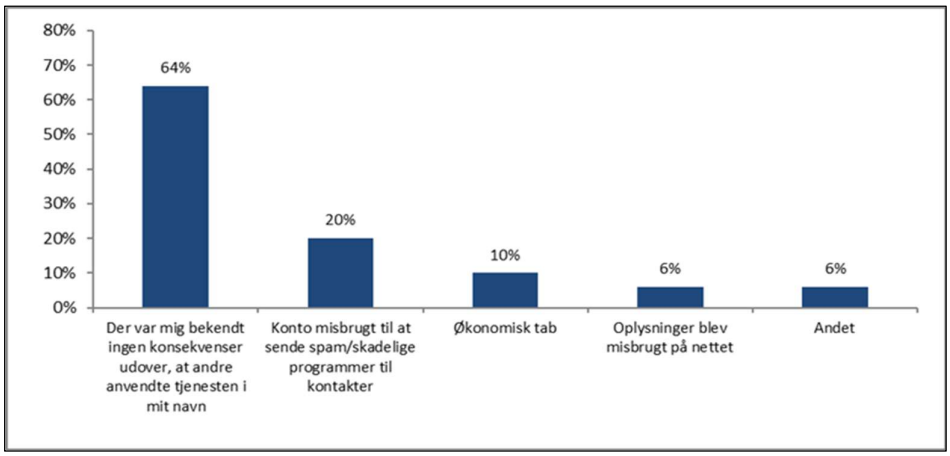
for dermed kan man fx hindre virus og andre skadelige programmer i at få tilgang til de tjenester, man er tilknyttet. Fx er bestemte typer malware som keylogger og sniffer[10] typisk udviklet med det formål at aflure brugernavn og kodeord til tjenester.

Mens den første handling viser det dominerende handlingsmønster, giver den samlede andel af handlinger indblik i det generelle handlingsmønster. Her er der størst svarandel på ændring af kodeord på tjenester (38 pct.), 32 pct. advarer omgangskredsen, eller de spørger omgangskredsen om hjælp (31 pct.). 28 pct. oplyser, at de fjerner virus med et antivirusprogram, og 21 pct. spærrer betalingskort. Alt sammen fornuftige handlinger, der vidner om god forståelse for, at der er behov for handling.

At miste adgang til én tjeneste fører til højere sikkerhed på andre tjenester

Relativt få borgere (5 pct.) har oplevet at miste adgangen til tjenester (fx Facebook, LinkedIn, mail mv) inden for det seneste år. Konsekvenserne har for de flestes vedkommende været, at andre har anvendt tjenesten i deres navn (64 pct.). 20 pct. har oplevet, at kontoprofilen er blevet anvendt til spredning af spam og andre skadelige programmer, 6 pct. har oplevet misbrug af egne oplysninger på nettet, og økonomisk tab har ramt 10 pct. (figur 9).

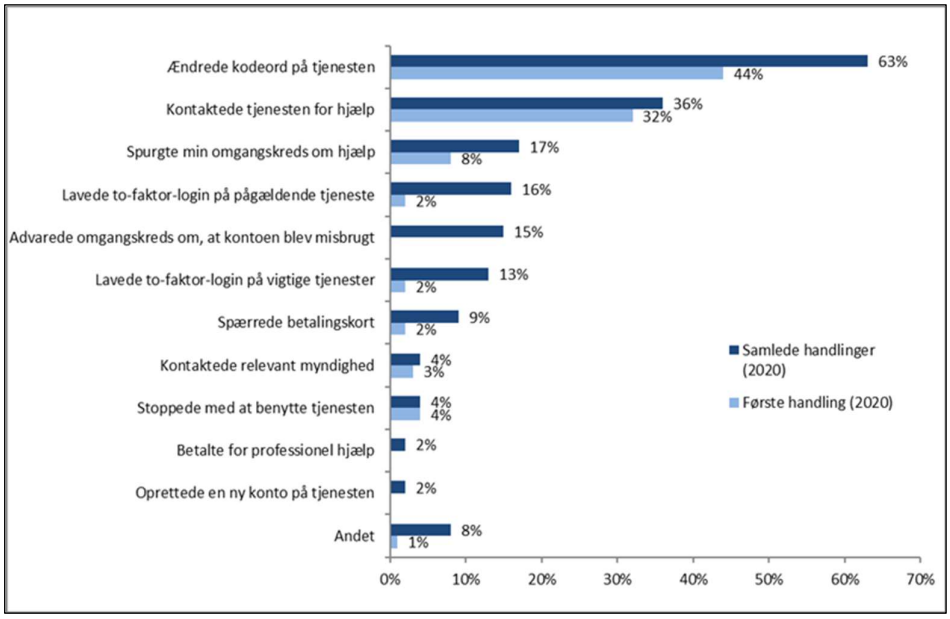
[10] Se ordforklaring i kapitel 9 af hhv. keylogger (side 67) og sniffer (side 69).



Figur 9 Borgernes angivelse af oplevede konsekvenser ved at miste adgangen til en tjeneste.

Også her har vi bedt respondenterne om at prioritere deres handlinger for at få indblik i det dominerende handlingsmønster. Den mest udbredte første adfærd efter at have oplevet konsekvenserne ved at miste adgang til tjenester er at skifte-kodeord (figur 10). Det gør samlet set 44 pct. af de udsatte som det første. Næst flest kontakter tjenesten for at få hjælp (32 pct.), mens hjælp fra omgangskredsen spiller en mindre fremtrædende rolle her (8 pct.) som den første handling.

Det tyder på en fornuftig og dominerende bevidsthed om at få spærret adgangen hurtigt ved skift af kodeord, og at borgerne er godt klædt på til at håndtere denne udfordring.



Figur 10 Borgernes handlinger ved mistet adgang til tjenester. Op til tre svar kan gives i prioriteret rækkefølge.

Fordelingen af de samlede handlinger efter at have mistet ens adgang fordeler sig på ændring af kodeord på tjenesten (63 pct.), mens 36 pct. kontakter tjenesten, og 15 pct. advarer omgangskredsen. Generelt er den bedste metode til at beskytte en tjeneste som fx en konto på et socialt medie eller en e-mailkonto at have et stærkt kodeord og aktivere to-trins-login. 16 pct. angiver, at de, som en af deres handlinger efter at have mistet adgangen til en tjeneste, laver to-faktorlogin[11] på den pågældende tjeneste, mens 13 pct. oplyser, at de aktiverer to faktorlogin på andre tjenester. Det vidner om, at borgerne lærer af oplevelserne på en tjeneste og øger sikkerheden på andre.

Opsamling

Dette kapitel har fokuseret på, hvilke trusler borgerne bliver udsat for, hvordan de handler, når de møder dem, samt hvad konsekvenserne har været for de uheldige borgere, der har oplevet truslerne blive til hændelser. Næste kapitel vil gøre status på de gængse sikkerhedsråd, som anbefales til borgere, der gerne vil beskytte sig bedst muligt mod digitale trusler.

[11] Se ordforklaring kapitel 9, side 71.

3. Status på efterlevelse af gode råd

Kapitlet undersøger i hvilken grad, borgerne efterlever de anbefalinger, der kan bidrage til en god digital hygiejne og adfærd.

Siden 2018 har informationsportalen sikkerdigital.dk[12] været et af omdrejningspunkterne for kommunikation om informationssikkerhed til borgere, virksomheder og den offentlige sektor. Kapitlet tager udgangspunkt i de råd til daglig digital sikkerhed, der kommunikeres på sikkerdigital.dk.

Rådene omfatter bl.a. anbefalinger til sikre kodeord, trådløse netværk, sikkerhedskopiering, anvendelse af antivirusprogrammer, opdatering af systemer og programmer samt nethandel.

I det følgende gøres status på, i hvilken grad borgerne efterlever disse råd i deres dagligdag. I næste kapitel undersøges, hvorfor de gode sikkerhedsråd til tider ikke efterleves – både ud fra borgernes egne tilbagemeldinger og ud fra gængs adfærdsteori.

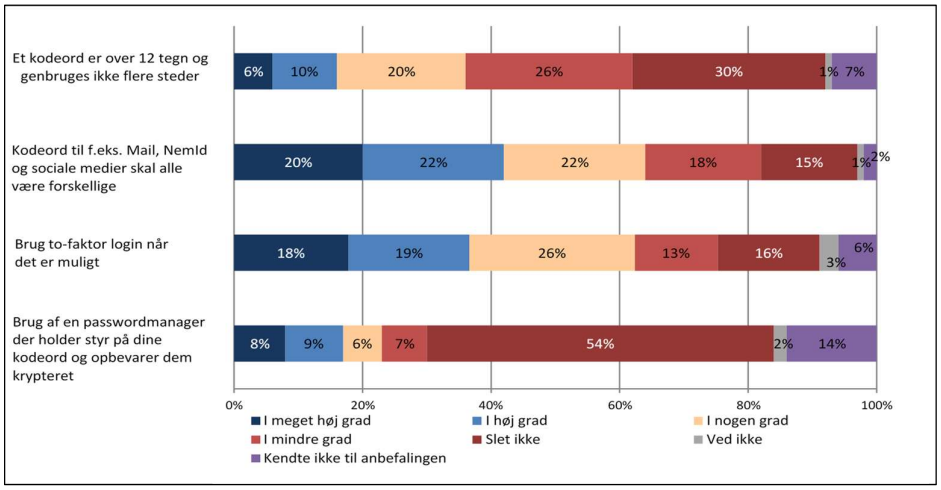
Kodeord – nøglen til data

Kodeord er en grundlæggende præmis i beskyttelse af data og enheder. Et kodeord er nøglen til at få adgang til data, uanset om det er data på en telefon, en profil på et socialt medie eller en bankkonto. At et kodeord bør være på 12 tegn og derover er et udtryk for, at nøglen skal være svær at bryde for it-kriminelle. Derudover anbefales det, at kodeord ikke genbruges, da kendskab til et kodeord til én tjeneste dermed vil give adgang til andre tjenester.

Der er imidlertid en tendens til ikke at efterleve anbefalingen blandt borgerne (figur 11). Kun 16 pct. anfører, at de i høj/meget høj grad efterlever anbefalingen, mens hele 55 pct. kun i mindre grad eller slet ikke efterlever den. Det er ikke overraskende, at mange kæmper med at have lange og unikke kodeord, når et stigende antal tjenester bliver digitale, hvorved der kræves flere og flere kodeord per bruger. At huske mange forskellige og lange kodeord er vanskeligt. Samtidig tillader mange udbydere af tjenester stadig brug af korte kodeord, hvorfor borgerne ikke tvinges til at lave lange kodeord.

Til gengæld ser det ud til, at efterlevelsen af anbefalingen om brug af forskellige kodeord til særligt vigtige tjenester som mail, NemID og sociale medier er slået bedre igennem, idet 42 pct. af borgerne anfører, at de i høj/meget høj grad efterlever anbefalingen.

[12] Digitaliseringsstyrelsen og Erhvervsstyrelsen står bag sikkerdigital.dk i samarbejde med en række samarbejdspartnere.



Figur 11 Borgernes angivelse af, i hvilken grad de efterlever anbefalingerne vedrørende kodeord.

Dette modsvares imidlertid af, at 33 pct. oplyser, at de i mindre grad eller slet ikke efterlever anbefalingen, mens 2 pct. ikke kendte til anbefalingen.

Udfordringen med genbrug af kodeord er, at det ikke kræver særlig stor indsats for ondsindede aktører at teste om et kodeord ét sted i kombination med brugernavn eller e-mail kan bruges andre steder. Dette kan ske, hvis der fx er sket et datalæk af brugernavne og kodeord fra en tjeneste. Cyberkriminelle kan således afprøve, om de lækkede kodeord – eller kendte almindelige kodeord – i kombination med brugernavn eller e-mail giver adgang til andre tjenester.

En anden udfordring ved kodeord er, at de kan være genstand for password spray-attack[13]. Her anvendes de hyppigst brugte kodeord til test på samtlige brugere på en tjeneste.

Fordi kodeord er et af de svageste led i sikkerhedskæden, er to-faktor login vigtig at implementere.

Borgere under 40 år efterlever i mindre grad end borgere på 40 år og der over anbefalingen om forskellige kodeord. Således angiver kun 37 pct. af de 18-39 årige, at de i høj/meget høj grad følger anbefalingen mod 46 pct. blandt borgere på 40 år og derover.

To-faktorlogin kaldes også to-faktorsikkerhed eller multifaktorlogin/autentifikation/sikkerhed og er en metode til at øge sikkerheden ved systemer, hvor login ikke kun kræver brugernavn og password, men også en ekstra unik kode. NemID er et eksempel på en løsning med to-faktorlogin.

[13] Se ordforklaring i kapitel 9, side 68.

To-faktorlogin gør login mere sikkert, fordi det er sværere og mere ressourcekrævende for de kriminelle – udelukkende digitalt – at kompromittere to-faktorlogin, selvom rigtigt meget phishing går ud på også at få fat i den engangskode, som "den anden faktor" fx udgøres af[14]. 37 pct. af borgerne oplyser, at de i høj/meget høj grad efterlever anbefalingen om brug af to-faktor login, hvor det er muligt, mens 28 pct. i mindre grad/slet ikke gør det.

Færre af de 60+-årige benytter sig i høj/meget høj grad af to-faktorlogin, når det er muligt (25 pct.) sammenlignet med de øvrige aldersgrupper.

Passwordmanager – ikke en integreret del af borgernes digitale sikkerhed
En passwordmanager[15] er et program, der opbevarer alle brugerens kodeord beskyttet med kryptering, og som ofte også kan generere lange og komplekse kodeord, unikt til hver tjeneste. For at få adgang til databasen over passwords skal man indtaste et masterpassword.

Passwordmanagers har været på gaden i mange år, men kun udbredt hos slutbrugerne inden for de sidste 10-15 år. Af den grund kan det ikke overraske, at 14 pct. ikke kender anbefalingen, og over halvdelen (61 pct.) slet ikke efterlever anbefalingen (figur 11). En passwordmanager kan være en overvindelse for mange at tage i anvendelse. Blot det at finde en manager, der passer til én, og som man har tillid til, kan være svært. I praksis er der dog tale om et digitalt nøgleskab, som blot kræver én nøgle. Det er det, der gør en passwordmanager til et godt og nemt redskab at anvende.

I forhold til anvendelsen ses der en tendens til, at brugen af passwordmanager falder med alderen. Blandt de 18-29-årige er det således 24 pct., der svarer, at de i høj grad/meget høj grad følger anbefalingen i modsætning til de 60+ årige, hvor 9 pct. benytter passwordmanager.

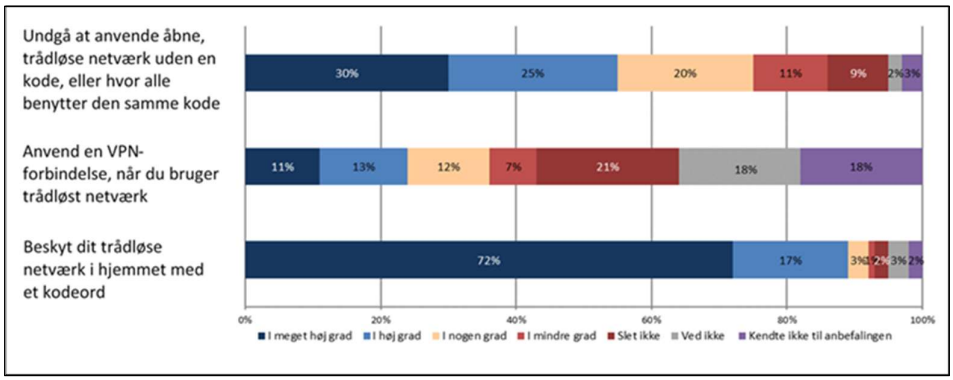
Trådløst netværk – en stor del af hverdagen

Brug af trådløse netværk[16] er en nærmest uundgåelig del af danskernes hverdag og en tjeneste, mange cafeer og trafikknudepunkter stiller til rådighed. Men der er samtidig en risiko for, at andre brugere på netværket potentielt kan se de data, der bliver sendt via netværket.

54 pct. oplyser, at de i høj/meget høj grad efterlever anbefalingen (figur 12) om ikke at bruge åbne trådløse netværk eller netværk, hvor alle bruger samme adgangskode. En femtedel svarer, at de i mindre grad/slet ikke efterlever anbefalingen.

[14] Den anden faktor ved to-faktorlogin behøver ikke at være en engangskode – det kan være et hardwaretoken, et fingeraftryk eller andet.
[15] Se ordforklaring i kapitel 9, side 68.
[16] Se ordforklaring i kapitel 9, side 70.

I hjemmet er der til gengæld mere konsekvent anvendelse af kodebeskyttede trådløse netværk, selv om der kan ses et mindre fald på 5 pct.-point fra 2018. Således oplyste 94 pct. af borgerne i 2018, at de beskytter deres trådløse netværk i hjemmet med kodeord, mens 89 pct. her i 2020 oplyser, at de i høj/meget høj grad efterlever anbefalingen.



Figur 12 Borgernes angivelse af, i hvilken grad de efterlever anbefalingerne vedrørende trådløse netværk.

Årsagen til den høje andel kan skyldes, at stort set alle leverandører af trådløst netværk til borgere leverer routeren med kodeord, som i modsætning til tidligere er et unikt kodeord. I mange år blev routere leveret med et standardkodeord, hvilke gjorde det nemmere at kompromittere. At routere nu har unikke kodeord er et eksempel på, at en branches enighed om standardopsætninger kan have en sikkerhedsmæssig effekt.

Mange (18 pct.) kender ikke eller efterlever kun i mindre grad eller slet ikke (28 pct.) anbefalingen om at anvende VPN – et virtuelt privat netværk[17]. VPN sikrer en sikker, krypteret[18] forbindelse, hvorved man uden risiko for at blive offer for datahøst kan anvende et åbent, trådløst netværk. Det sikrer også kryptering af fx e-mails. E-mails, webtrafik, filoverførsler og fjernadgange i åbne kanaler kan i realiteten læses af udefrakommende, men ikke hvis kanalen er krypteret. I 2018 oplyste 13 pct. af borgerne, at de bruger VPN uden for hjemmet, mens 24 pct. i 2020 oplyser, at de i høj/meget høj grad efterlever anbefalingen om brug af VPN. Der er således sket en stigning blandt borgere, der sikrer deres forbindelse grundigt.

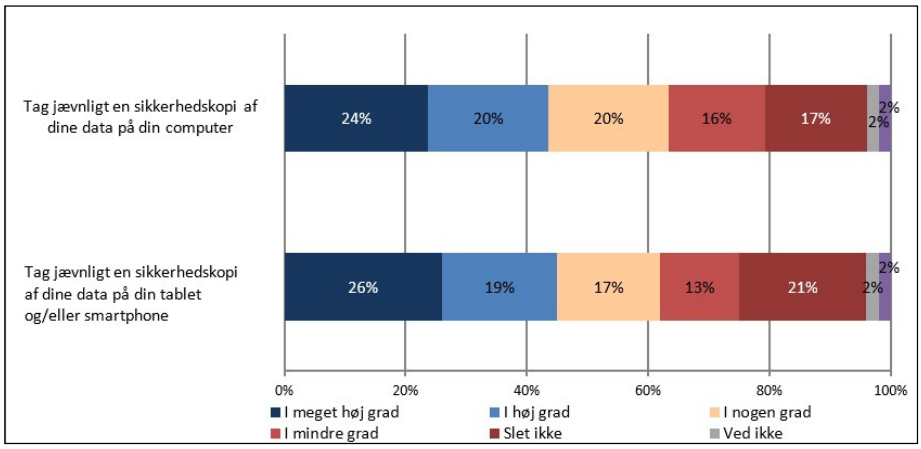
Tendensen til at følge anbefalingen om at undgå åbne trådløse netværk stiger med alderen. Således er det kun 39 pct. af de 18-29-årige, der i høj grad/meget høj grad efterlever denne, i modsætning til de 60+ årige, hvor 63 pct. i høj grad/meget høj grad undgår de åbne netværk.

Færre personer under 40 år (18 pct.) efterlever i høj grad/meget høj grad anbefalingen om at benytte en VPN-forbindelse.

[17] Se ordforklaring i kapitel 9, side 71.
[18] Se ordforklaring i kapitel 9, side 67.

Sikkerhedskopiering – den bedste beskyttelse mod teknisk nedbrud og ransomware

Sikkerhedskopiering er den bedste metode til at imødegå ransomware[19] eller andre hændelser, hvor man mister adgangen til sine data. Sikkerhedskopiering kan ikke hindre et angreb, men det kan afbøde konsekvenserne.



Figur 13 Borgernes angivelse af, i hvilken grad de efterlever anbefalingerne vedrørende sikkerhedskopiering af data på computer og telefon/tablet.

I 2020 oplyser 44 pct. at de i høj grad/meget høj grad efterlever anbefalingerne om sikkerhedskopiering, og 33 pct. af borgerne oplyser, at de i mindre grad/slet ikke efterlever anbefalingen (figur 13). I perioden fra 2013 til 2018 oplyste op mod 41 pct., at de jævnligt tog sikkerhedskopi. Dermed er der ikke sket den store udvikling i borgernes efterlevelse af anbefalingen om jævnligt at tage en sikkerhedskopi.

Der er stort set ingen forskel at spore mellem andelen af borgere, der følger anbefalingerne om sikkerhedskopiering af data på telefon og tablet og sikkerhedskopiering af computer.

Færre af de 18-29-årige angiver, at de i høj/meget høj grad (34 pct.) lever op til anbefalingen om sikkerhedskopiering af pc sammenlignet med de øvrige aldersgrupper.

De 30-49-årige (54 pct.) skiller sig ud i forhold til efterlevelse af anbefalinger om sikkerhedskopiering af data fra telefon og tablet, da flere i disse aldersgrupper svarer, at de i høj/meget høj grad følger anbefalingen.

[19] Se ordforklaring i kapitel 9, side 69.

Automatisk opdatering – en grundforudsætning for beskyttelse af informationer

Brug af automatisk softwareopdatering[20] af programmer er en effektiv måde at være sikker på, at programmer altid er installeret med den nyeste version. Herved bliver evt. sårbarheder rettet og kan ikke misbruges i angreb. En sårbarhed kan fx være en programmeringsfejl, som giver uvedkommende adgang til at køre skadelig software på systemet og derved læse, ændre eller ødelægge data.

Andelen der i høj grad/meget høj grad efterlever anbefaling om automatisk opdatering af computer stiger med alderen. Blandt de 18-29-årige er det således kun 60 pct., mens andelen stiger med alderen og ender på 78 pct. blandt de 60+-årige.

Andelen, der i høj grad/meget høj grad efterlever anbefaling om brug af antivirusprogram på computer, stiger ligeledes med alderen. Således er det 59 pct. af de 18-29-årige, mens andelen er 85 pct. blandt de 60+-årige.

Producenterne af software udsender løbende opdateringer af programmer, og uden automatisk opdatering kræver det et manuelt tjek fra brugerne. Ofte kræver en gennemførelse af automatisk opdatering dog, at man genstarter sin enhed. Gøres dette ikke, er enheden stadig sårbar.

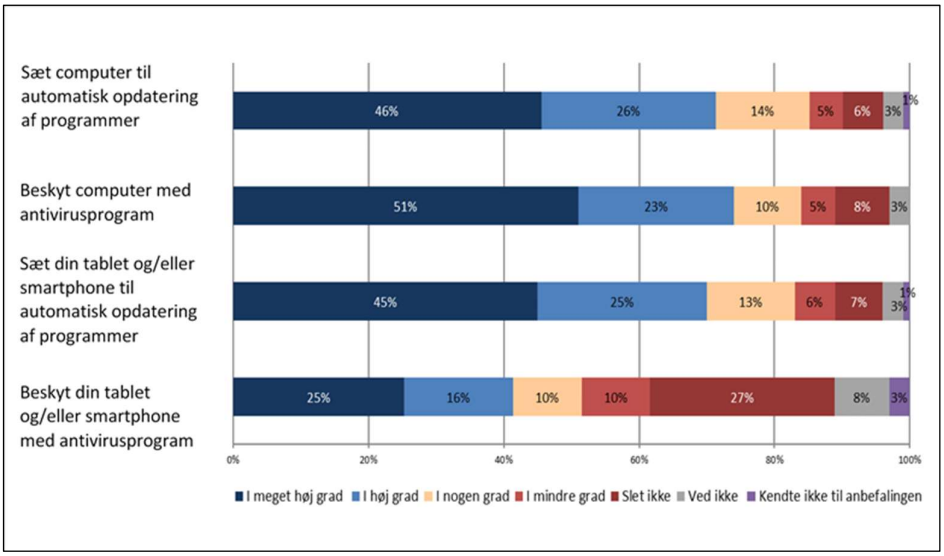
Næsten 3 ud af 4 (71 pct.) svarer i 2020, at de i høj/meget høj grad følger anbefalingen om, at computeren sættes til automatisk at hente og installere opdatering til programmer, mens det for telefon og tablets vedkommende drejer sig om 70 pct. (figur 14).

I 2018 oplyste knap 80 pct., at de har slået automatisk opdatering af programmer til på deres computer. En andel, der har været nogenlunde konstant i alle de år, vi har stillet spørgsmålet. Andelen af borgere, der oplyser, at de efterlever anbefalingen vedr. opdateringer af telefon/tablet, er stort set de samme som mht. computer. På trods af variation i spørgemåden bør det nok give anledning til bekymring, at borgerne i mindre grad end tidligere år efterlever anbefalingen om automatisk at hente opdateringer til computer, telefon og tablet, da dette som nævnt er en effektiv måde at lukke sårbarheder fra producenternes side. Dog skal det nævnes, at der er en teoretisk mulighed for, at borgerne stadig installerer opdateringerne til deres enheder blot manuelt frem for automatisk. Dette har undersøgelsen ikke afdækket.

Anvendelse af antivirus kan til en vis grad beskytte enhederne mod skadelig software, der forsøger at udnytte sårbarheder. Men også kun i vis grad, idet antivirusprogrammer også skal holdes opdateret for at imødegå skadelig software.

[20] Se ordforklaring i kapitel 9, side 71.

I 2020 oplyser 73 pct., at de i høj/meget høj grad efterlever anbefalingen om anvendelse af antivirus på deres computer. Fra 2013 til 2018 skete der et fald fra 80 pct. til 59 pct. i andelen af borgere, der oplyste, at de anvender antivirus-produkter på computeren. Der kan dermed spores en tendens til, at faldet er standset. Det er positivt, da en af forudsætningerne for en god beskyttelse er antivirusprogrammer.



Figur 14 Borgernes angivelse af, i hvilken grad de efterlever anbefalinger vedrørende automatisk opdatering og brug af antivirusprogrammer.

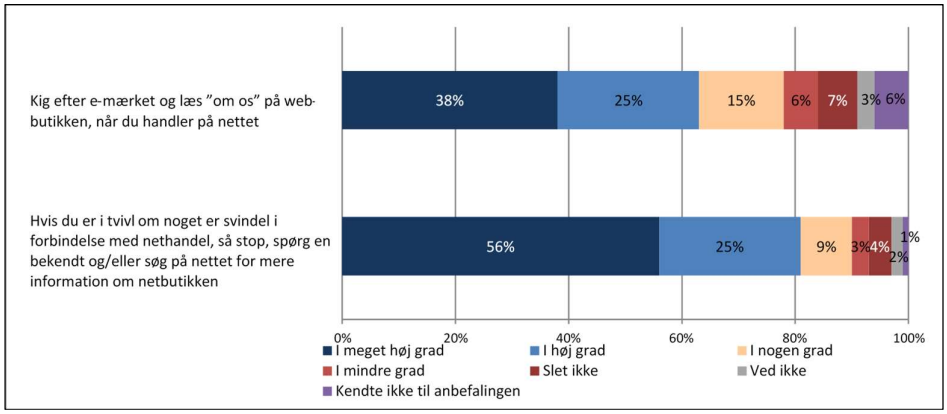
Kun 41 pct. af borgerne efterlever i høj/meget høj grad anbefalingen om brug af antivirusprogram på deres telefon og/eller tablet i 2020. Den høje grad af efterlevelse af anbefalingen vedr. computer kan muligvis skyldes, at antivirus-produkter ofte indgår i købet af computeren. Om ikke andet indgår det ofte som en prøveperiode, hvorfor brugeren i højere grad vænner sig til, at det er sund fornuft at have antivirus-produkter til sin computer.

Dette står i modsætning til køb af tablet og telefon, hvor antivirus sjældent indgår. Dermed anses det muligvis ikke som en naturlig del af beskyttelsen af ens enheder, samtidig med at man selv aktivt skal foretage købet af antivirus-produktet.

Nethandel – opmærksomhed og skepsis som bedste værn

Fupbutikker kan til forveksling ligne rigtige internetbutikker, og det kan være svært at gennemskue hvilke butikker, der er den ægte vare. Anbefalingerne om sikker nethandel handler derfor også om sund skepsis: Hvis tilbuddet er for godt til at være sandt, så er det det nok også. Det handler om at minimere risikoen for, at ens tillid bliver misbrugt. Anbefalingerne vedr. nethandel handler også om at være opmærksom på tegn som fx en utroværdig "Om os"-side eller at holde øje med e-mærket, som er et udtryk for, at webshoppen lever op til en række krav og regler, som certificeringsordningen har stillet op. Mange borgere oplyser heldigvis, at de efterlever de gode råd og principper, når de handler på nettet. 63 pct.

siger således, at de i høj eller meget høj grad efterlever anbefalingen om at kigge efter e-mærket og læse "om os" på webbutikken, når de handler, mens 8 ud af 10 (81 pct.) angiver, at de spørger en bekendt eller søger om mere information om netbutikken, hvis de i tvivl, jf. figur 15.



Figur 15 Borgernes angivelse af, i hvilken grad de efterlever anbefalingerne vedrørende handel på internettet.

Opsamling

Samlet set kan det konkluderes, at borgernes efterlevelse af alle de ovenstående anbefalinger angående daglig sikkerhedsadfærd er højest på de områder, der er nemmest af efterleve. Således er der flest, der oplyser, at de efterlever anbefalingen om at beskytte deres trådløse netværk i hjemmet med en kode og automatisk opdaterer deres computere, telefon og tablet. Omvendt er der færre borgere, der lykkes med at få taget sikkerhedskopier ofte og få lavet lange og unikke kodeord.

I det næste kapitel dykkes dybere ned i de årsager, som borgerne har angivet som betydende for, at de ikke altid efterlever de anbefalinger, der er anses som grundlæggende for en sikker adfærd.

4. Barrierer og drivere for at udøve en god digital sikkerhedsadfærd

Kapitlet undersøger barrierer og drivere for at efterleve de gode råd om digital sikkerhed. Yderligere undersøges borgernes kilde til viden om sikkerhed, samt i hvilken grad de hjælper deres egne børn med digital sikkerhed.

Menneskers adfærd er afgørende for informationssikkerheden. Dels fordi mennesker i sig selv udgør en væsentlig sårbarhed, når det kommer til sikkerhed. Men også fordi mennesker udgør et afgørende bolværk mod digitale trusler. Hvis vi kan komme tættere på viden om, hvordan vi kan maksimere efterlevelsen af gode sikkerhedsråd, ville informationssikkerheden kunne øges væsentligt.

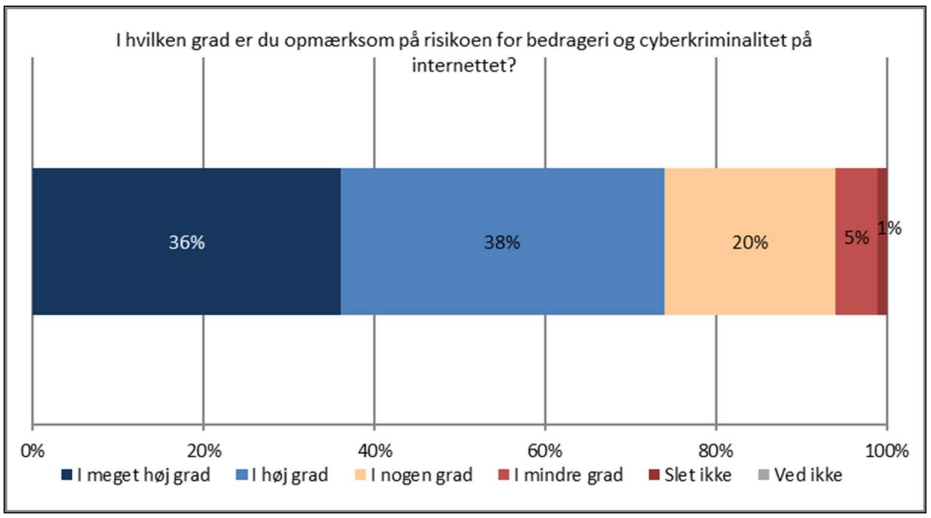
Fundamentet for at have en ønskelig sikkerhedsadfærd er typisk, at man som borger er opmærksom på digitale trusler og risici ved at være ubeskyttet på nettet. Opmærksomhed er således typisk en nødvendighed, men ikke en tilstrækkelighed for at have en god adfærd. Derfor undersøges først status på borgernes opmærksomhed på cyberkriminalitet og holdning til risikobetonet adfærd samt deres selvtillid i at beskytte sig på nettet.

Dernæst undersøges det nærmere, hvilke årsager borgerne selv angiver som udslagsgivende for, hvorfor de til tider ikke efterlever de råd, som kan anses som grundlæggende for at have en god daglig sikkerhedsadfærd.

Endeligt vil kapitlet undersøge, hvor borgerne får deres viden om digital sikkerhed fra, og hvilken betydning kilden til viden om digital sikkerhed kan have ift. at sikre borgerne bedst muligt.

Hvor opmærksomme er borgere på digitale trusler og risici?

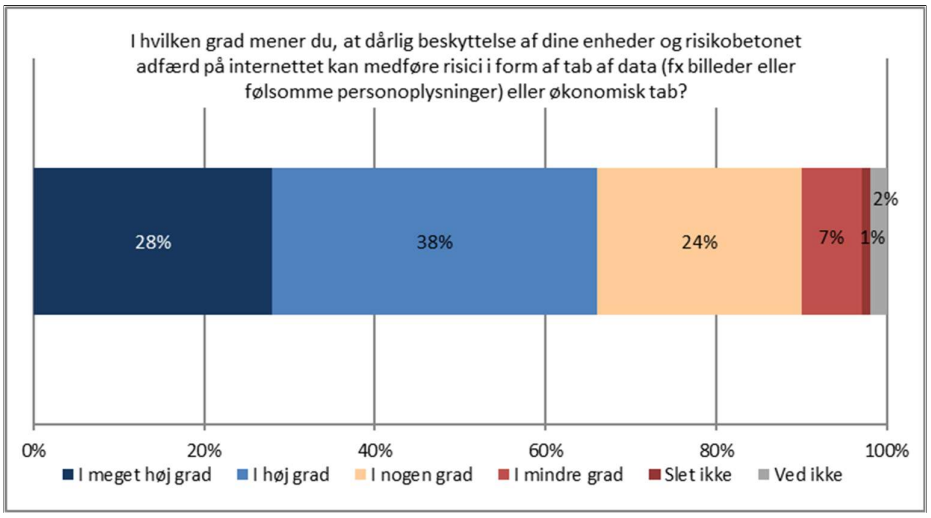
Mange borgere (74 pct.) angiver i høj/meget høj grad, at de er opmærksomme på risikoen for cyberkriminalitet og bedrageri, mens kun 6 pct. er i mindre grad eller slet ikke opmærksomme (figur 16). I 2018 svarede 90 pct. af borgerne "ja" til, at de var opmærksomme på trusler mod deres enheder (computer, tablet eller smartphone). Det tilsyneladende fald i borgernes opmærksomhed fra 2018 til 2020 kan skyldes en ændring i spørgemåden. Tilbage er dog stadig en stor andel af borgere, der i 2020 angiver at være opmærksom på risikoen.



Figur 16 Borgernes opmærksomhed på bedrageri og cyberkriminalitet på internettet.

Der ses i øvrigt en klar tendens til, at opmærksomheden stiger med alderen. Blandt de 18-29-årige svarer kun 2 ud af 3 (67 pct.) således, at de i høj grad/meget høj grad er opmærksomme på bedrageri og cyberkriminalitet på internettet, mens andelen blandt de 60+-årige er på 81 pct.

Et andet element af at være opmærksom på digitale risici er ens holdning til, hvilken betydning dårlig beskyttelse af enheder og en risikobetonet adfærd har for, at man bliver sårbar over for trusler. Derfor har undersøgelsen spurgt til netop dette. 66 pct. af borgerne anfører her, at de i høj/meget høj grad mener, at risikobetonet adfærd medfører øget risiko for datatab (figur 17).



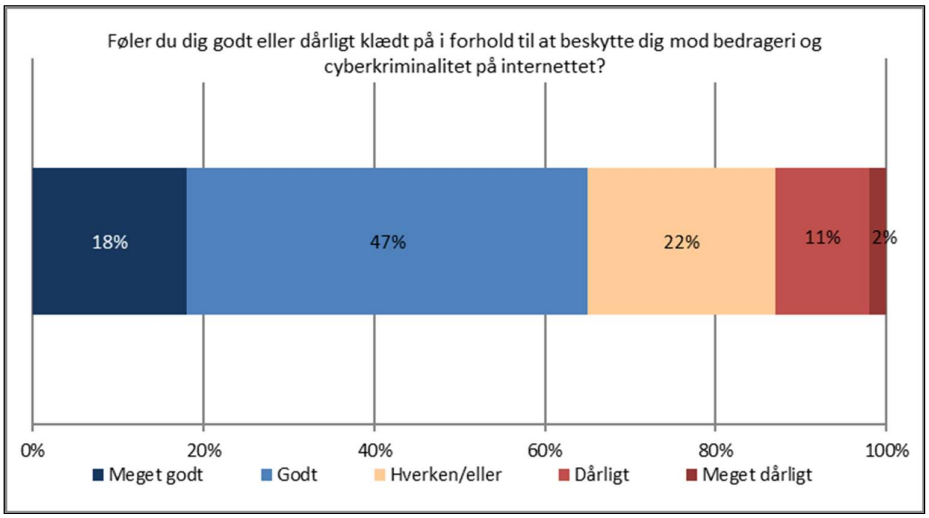
Figur 17 Borgernes opfattelse af betydningen af dårlig beskyttelse og risikobetonet adfærd i forhold til risikoen for tab af data eller økonomisk tab.

Yderligere angiver 24 pct., at de i nogen grad mener, at der er risici ved risikobetonet adfærd og dårlig beskyttelse. Dette er sammenligneligt med 2018, hvor respondenterne kunne svare ja eller nej på, om de var klar over, at dårlig beskyttelse af enheder og risikobetonet adfærd kunne medføre konsekvenserne identitetstyveri, tab af adgang til sociale medier, tab af data, tab af penge. Omkring 90 pct. af respondenterne svarede i 2018 ja på dette spørgsmål. Sammenlægges svarene "i nogen grad", "i høj grad" og "i meget høj grad" i dette års undersøgelse, angiver samlet set 90 pct. af borgerne en af disse, hvorved andelen kan siges at være på niveau med andelen, der i 2018 svarede "ja".

Også hvad angår opfattelsen af dårlig beskyttelse og risikobetonet adfærd ser vi aldersbetingede forskelle. Blandt de 60+-årige svarer flere, at de i høj/meget høj grad (78 pct.) mener, at dårlig beskyttelse og risikoadfærd kan medføre tab af data. Omvendt er det færre blandt de 30-39-årige (56 pct.) og 40-49-årige (59 pct.), som i høj /meget høj grad mener dette.

Endeligt har undersøgelsen spurgt til, om borgerne føler sig godt eller dårligt klædt på i forhold til at beskytte sig mod bedrageri og cyberkriminalitet på nettet. Det er i høj grad et subjektivt spørgsmål "at føle sig klædt på", men det kan fortælle noget om borgernes selvtillid, når det kommer til digital sikkerhed.

64 pct. oplyser, at de føler sig godt/meget godt klædt på, mens samlet set 35 pct. svarer "hverken/eller", "dårligt" eller "meget dårligt" klædt på (figur 18). I 2018 svarede 61 pct. af respondenterne, at de følte sig godt klædt på i forhold til at beskytte sig mod cybertrusler, mens 37 pct. svarede nej. Der er dermed en mindre justering i spørgemåden og nuanceringen i svarmulighederne. Resultatet for de to år er dog sammenlignelige, og det kan også konstateres, at der ikke er sket en udvikling blandt borgerne.



Figur 18 Borgernes angivelse af, hvordan de føler sig klædt på i forhold til beskyttelse mod bedrageri og cyberkriminalitet.

Det giver ikke nødvendigvis sig selv, at man har en god digital sikkerhedsadfærd, fordi man er opmærksom på problematikken. Dog er der i denne undersøgelse netop en tendens til, at: Jo mere opmærksom man angiver at være på cyberkriminalitet og bedrageri, og jo mere man mener, risikobetonet adfærd udgør en sårbarhed, des mere angiver man at efterleve anbefalingerne til en sikker digital adfærd.

Borgere, der er meget opmærksomme på bedrageri og cyberkriminalitet på internettet samt faren ved dårlig beskyttelse af enheder og risikobetonet adfærd på internettet, angiver i højere grad at efterleve de gode råd om 1) kodeord, 2) trådløse netværk, 3) sikkerhedskopiering af data, 4) automatisk opdatering af programmer og brug af antivirusprogrammer samt 5) handel på internettet.

Til eksempel angiver 42 pct. af de borgere, der i høj/meget høj grad er opmærksomme på bedrageri og cyberkriminalitet på internettet, at de i høj/meget høj grad efterlever anbefalingen om to-faktor login. Det samme gør sig kun gældende for 14 pct. af de borgere, der i mindre grad/slet ikke er opmærksomme på bedrageri og cyberkriminalitet.

Ligesom det ikke giver sig selv, at man udøver god sikkerhedsadfærd, blot fordi man er opmærksom på risici og trusler, giver det heller ikke sig selv, at man udøver god sikkerhedsadfærd, fordi man føler sig godt klædt på til at gøre det. I undersøgelsen ses dog igen en sammenhæng mellem disse to forhold: At føle sig godt klædt på til at beskytte sig – altså at have en "sikkerhedsselvtillid" – hænger i denne analyse også sammen med at angive at have en god, daglig sikkerhedsadfærd.

Til eksempel gælder det, at blandt borgere, der i høj/meget høj grad efterlever anbefalingen om lange kodeord, angiver 76 pct., at de føler sig godt/meget godt klædt på i forhold til at beskytte sig på nettet. Blandt borgere, der i mindre grad/slet ikke følger anbefalingen, er det 61 pct., der føler sig godt/meget godt klædt på.

Borgere, der i høj/meget høj grad er opmærksomme på bedrageri og cyberkriminalitet, advarer i langt højere grad (47 pct.) deres omgangskreds, når de møder en phishing-trussel sammenlignet med borgere, der er mindre opmærksomme (5 pct.)

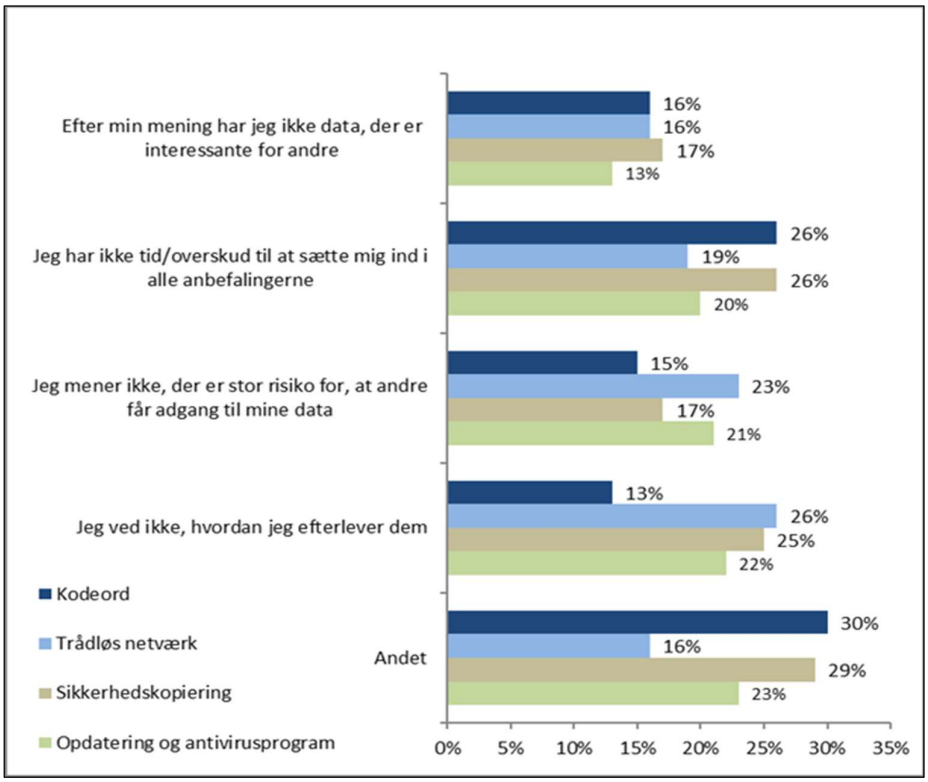
Hvorfor efterleves de gode sikkerhedsråd ikke?

Dermed ses overordnet en tendens til, at opmærksomhed på trusler og risici højner sandsynligheden for at have en ønskelig sikkerhedsadfærd.

Men hvis vi skal komme endnu nærmere, hvad der kræves for, at flere borgere vil efterleve de gode råd om sikker adfærd, er det relevant dels at spørge borgerne

selv, dels at skæve til adfærdsvidenskaben, der peger på nogle grundlæggende indsigter, man kan lade sig guide af[21].

Undersøgelsen har spurgt til, hvorfor anbefalingerne ikke efterleves. Spørgsmålet er stillet til de borgere, der svarer, at de i mindre grad/slet ikke lever op til én eller flere af anbefalingerne i forrige kapitel om fx kodeord og trådløse netværk. Svarene er samlet i figur 19. Årsagen til at manglende efterlevelse af anbefalinger angående nethandel ikke er taget med i denne figur skyldes små variationer i spørgemåden[22]. Dog flugter svarene om, hvorfor rådene ikke efterleves ved nethandel, med nedenstående svar.



Figur 19 Borgernes angivelse af årsager til ikke at efterleve anbefalingerne om hhv. kodeord, trådløse netværk, sikkerhedskopiering og automatisk opdatering og antivirusprogram.

Grundlæggende er der en stor spredning i svarene, og "Andet"-kategorien fylder samtidig godt i respondenternes samlede svar. Det kan være et udtryk for, at de resterende svarkategorier ikke er rammende. Den store spredning kan også være udtryk for, at det kan være svært at sætte fingeren på, hvorfor man ikke har den

[21] Daniel Kahneman (2011), 'Thinking, Fast and Slow' og OECD (2019), 'Tools and Ethics for Applied Behavioural Insights: The BASIC Toolkit' https://www.oecd.org/gov/regulatory-policy/tools-and-ethics-for-applied-behavioural-insights-the-basic-toolkit-9ea76a8f-en.htm

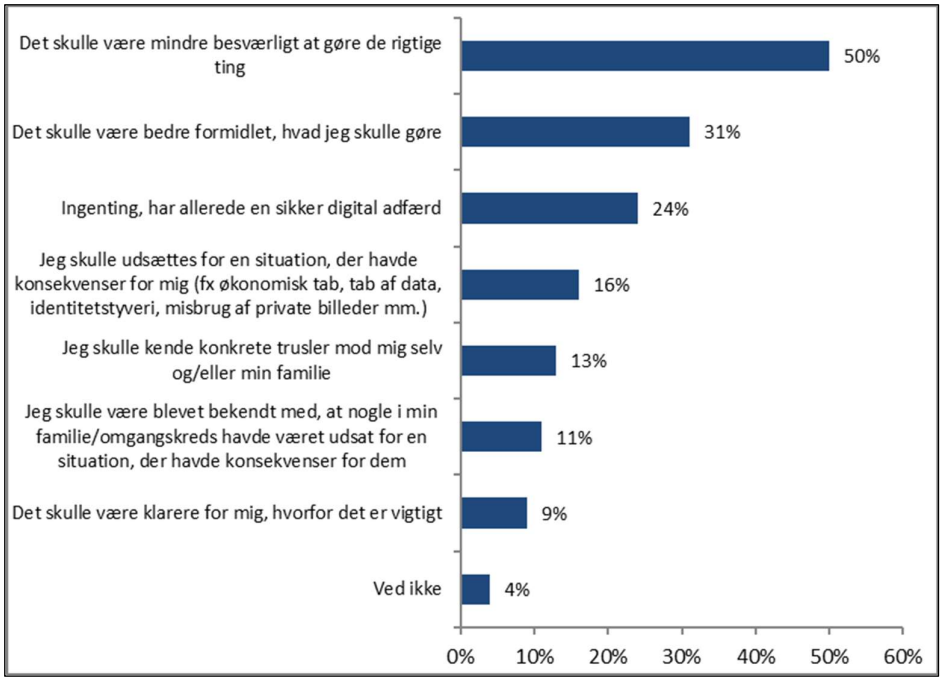
[22] Ved nethandel var der angivet følgende svarmuligheder: "Jeg handler sjældent/aldrig på nettet", "Jeg mener ikke, der er stor risiko for, at jeg bliver snydt, når jeg handler på nettet", "Jeg har ikke tid/overskud til at sætte mig ind i anbefalingerne", "Jeg ved ikke, hvordan jeg efterlever dem" og "Andet".

adfærd, som man måske egentlig godt ved, er den bedste og mindst risikobetonede. Borgernes kvalitative uddybninger af "Andet"-kategorien spænder lige fra dovenskab, til at der ikke er behov for efterlevelse, risikovillighed, glemsomhed, brug af papir til at huske kodeord osv.

Respondenterne angiver også manglende tid/overskud og manglende viden som årsager til ikke at efterleve anbefalingerne. Her er det interessant, at de yngste borgere (18-29 år) i højere grad end øvrige angiver manglende tid/overskud som svar på, hvorfor anbefalingerne ikke efterleves, mens de ældste borgere i højere grad angiver, at de ikke ved, hvordan de skal efterleve anbefalingerne.

Ganske vist svarer færrest, at de ikke har data, der er interessante for andre, og næst-færrest angiver, at de ikke ser en stor risiko for, at andre skulle kunne få adgang til deres data. Dog kan disse svar potentielt hænge sammen med ikke at føle tid/overskud til at efterleve anbefalingerne. Hvis man mener, at risikoen for, at hackere synes, man er interessant, er lille, og man heller ikke mener, at ens data er interessante i sig selv, så vil digital sikkerhed sandsynligvis ikke være dér, hvor man lægger størstedelen af sin tid og overskud.

Adspurgt hvad der kunne ændre deres digitale adfærd, svarer borgerne også netop, at det skulle være mindre besværligt at efterleve anbefalingerne (50 pct. jf. figur 20), samt at det skulle være bedre formidlet, hvad man skulle gøre (31 pct.).



Figur 20 Borgernes angivelse af, hvad der kan ændre deres digitale adfærd i hverdagen.

Det peger dels ned i en mulig sammenhæng mellem manglende efterlevelse af anbefalingerne som udtryk for manglende viden, jf. respondenterne i figur 19, der ikke vidste, hvordan de efterlever de gode råd. Men det peger netop også ned

i manglende tid og overskud, som mange også angav som årsag i ovenstående. Hvis det synes krævende at ændre sin digitale adfærd, er det svært at finde tid/overskud til at få det gjort. Yderligere viste konklusionen i foregående kapitel, at der er højest efterlevelse af de anbefalinger, der er lettest at efterleve. Det lader til, at borgerne gerne prioriterer tiden til at efterleve anbefalinger, hvis det synes tilgængeligt og ikke for tidskrævende at udføre den ønskelige adfærd.

Således peger det også på en tendens, som meget adfærdsvidenskab groft skåret har peget på: Hvis man ønsker at skabe en bestemt adfærd blandt en målgruppe, skal man overveje, hvordan man kan gøre adfærden attraktiv eller let at gå til for målgruppen. Man kan ikke forvente, at en ønsket adfærd automatisk kommer ved at give målgruppen den tilstrækkelige viden og opmærksomhed. Man bliver nødt til at formidle sine budskaber på en måde, der for modtageren er meningsfuld og skabe en klar handlemulighed. Det skal ske på det rigtige tidspunkt, hvor modtageren har mulighed for at foretage den ønskelige sikkerhedshandling, og det skal gentages for, at målgruppen fastholder den gode adfærd. Endeligt, og vigtigst, skal man overveje, hvorvidt man rent systemisk kan gøre det gode sikkerhedsvalg attraktivt/tvungent for modtageren. Hvis det fx kun er muligt at lave et nyt kodeord til en tjeneste, hvis det er langt og ikke er brugt andre steder, vil det være en del lettere at efterleve denne sikkerhedsadfærd.

Andelen, der svarer, at ingenting kan få dem til at få en mere sikker adfærd, stiger med alderen. Således angiver kun 17 pct. af de 18-29-årige dette, hvorefter andelen stiger til 32 pct. blandt de 60+-årige.

Figur 20 peger også på en anden tendens: Borgerne angiver, at de i højere grad ville efterleve sikkerhedsrådene, hvis de fik truslen tættere på sig ved, at enten de eller bekendte blev udsat for konsekvenser, eller hvis de kendte til de konkrete trusler mod sig selv eller bekendte. En mulig forklaring kan være, at trusler, der er så abstrakte som virusangreb, er svære at forholde sig til at imødegå i modsætning til mere konkrete trusler som fx en modkørende lastbil. Sandsynligheden er ikke nødvendigvis større, men konsekvensen er lettere at forholde sig til. Man kan også forestille sig, at der ved digitale trusler kan være et tilfælde af tilvænning: Man har hørt meget om trusler i fx medierne, men sandsynligheden for, at det går rigtig galt, synes ikke så stor, da man jo ofte er på nettet uden at tage stilling til trusler.

Samtidig fremgik det af kapitel 2, at relativt få borgere angiver at opleve de digitale trusler, de er blevet spurgt til i denne analyse – bortset fra phishing-truslen. Hvis en organisation ønsker at ændre en bestemt adfærd er det dermed væsentligt at overveje, om der blandt borgerne overhovedet er tilstrækkelig erfaring med truslerne til at motivere dem til at ændre handlemønstre på egen hånd. En risiko er, at organisationers fokus på at bevidstgøre borgere om truslerne via fx kampagner ikke har en stor adfærdsmæssig effekt, da erfaringsgrundlaget er for spinkelt.

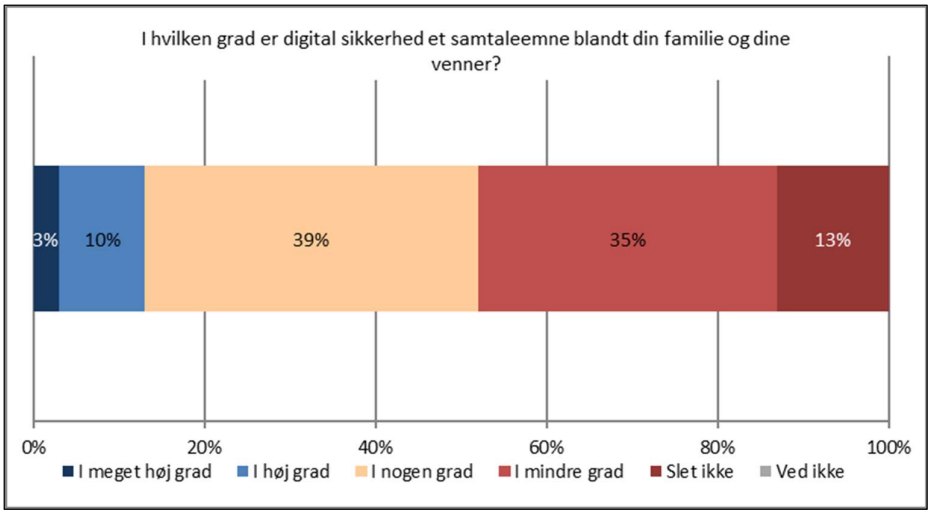
Disse forhold kan være med til at belyse, hvorfor borgerne ikke altid efterlever de gode råd, som anses for grundlæggende for at have en god sikkerhedsadfærd.

Hvis det skal lykkes, at flere borgere udøver en god, daglig sikkerhedsadfærd, hvor de efterlever de anbefalingerne til en god digital adfærd, skal man således overveje, hvordan man både systemisk og kommunikativt kan imødekomme borgernes ønske om, hvad der skal til: Det skal være lettere og mere attraktivt for dem at gøre de rigtige ting, og/eller borgernes erfaringer med trusler og konsekvenser skal højnes. Sidstnævnte dog helst i form af fx reelle cases, man kan spejle sig i, frem for konkrete erfaringer på egen krop.

Borgernes kilder til viden om digital sikkerhed

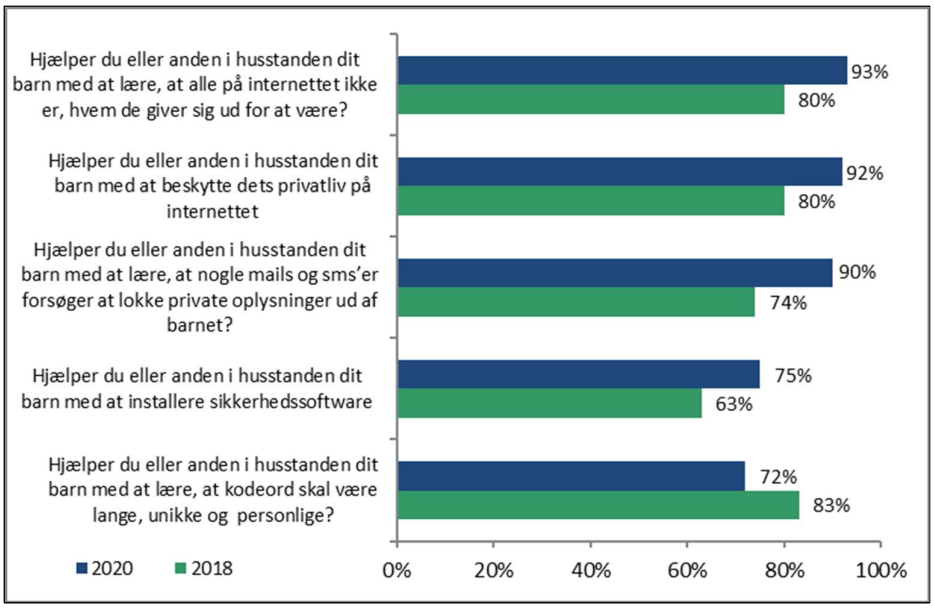
Digital sikkerhed kan for nogle virke uvedkommende og svært, fordi truslerne synes abstrakte, og fordi løsningerne virker tekniske og svært tilgængelige. Derfor er det undersøgt, i hvilken grad digital sikkerhed er et samtaleemne for borgerne. Tesen her er, at des mere digital sikkerhed bliver et samtaleemne, des mere vil man bryde tabuer om digital sikkerhed som uvedkommende og svært, som kan være en barriere for nogle.

Kun 13 pct. angiver, at digital sikkerhed i høj/meget høj grad er et samtaleemne, mens hele 48 pct. anfører, at det i mindre grad eller slet ikke er det (figur 21).



Figur 21 Borgernes angivelse af, i hvilken grad digital sikkerhed et samtaleemne blandt familie og venner.

Undersøgelsen afdækker også, i hvilken grad forældre hjælper deres børn med at udøve den gode sikkerhedsadfærd. I 2020 kan vi konstatere, at der på de fleste områder ses en stigning fra 2018 i andelen af borgere, der hjælper deres børn med sikkerhed på nettet. Dette fremgår af figur 22.



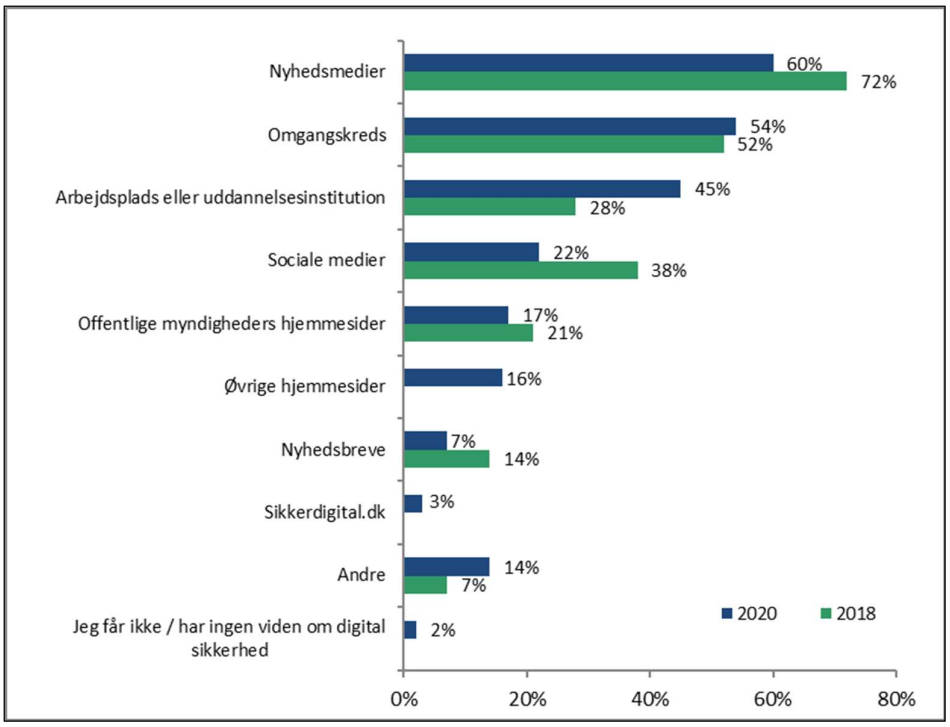
Figur 22 Borgernes hjælp med digital sikkerhed til deres barn.

Kun i forhold til andelen af forældre, der lærer deres barn om kodeord, er der sket et fald fra 2018 til 2020. En ændring i formuleringen af spørgsmålet kan måske forklare udviklingen i dette resultat, da der i 2018 blev spurgt til, om man hjalp med et sikkert kodeord uden at udspecificere, hvad det indebar.

Uanset *er* kodeord en grundlæggende præmis for god digital sikkerhed. Det er nøglen til mange af de ting, der er værd at beskytte – også for børn, der tidligt befinder sig på sociale medier og computerspil. Ligesom med alle andre gode vaner, som børn gerne skal lære, er det selvfølgelig vigtigt, at forældre sættes i stand til at hjælpe deres børn i den digitale verden – hermed ikke sagt, at indsatser i uddannelsessystemet ikke fortsat skal prioriteres.

Der ses yderligere en klar sammenhæng mellem den voksnes efterlevelse af anbefalingen om lange, unikke kodeord og hjælp til børn om det samme. Således oplyser 92 pct. af de, der i høj/meget høj grad efterlever anbefalingen om lange, unikke kodeord, at de (eller en anden i husstanden) hjælper deres barn med at kodeord skal være lange, unikke og personlige.

Endeligt har vi i denne del af undersøgelsen spurgt til, hvor borgerne får deres viden om sikkerhed fra. I 2018 viste undersøgelsen, at nyhedsmedier var den stærkeste kilde til viden om informationssikkerhed. Denne kilde er sammen med sociale medier på retur til fordel for arbejdspladsen eller uddannelsesinstitutionen som kilde til viden (figur 23).



Figur 23 Borgernes angivelse af, hvor de har deres viden om digital sikkerhed fra.

Stigningen fra 28 pct. i 2018 til 45 pct. i 2020 tegner et billede af, at oplæringsindsatsen i professionelle sammenhænge smitter af i borgernes private liv uden for arbejdspladsen. Viden fra omgangskredsen er også en betydelig kilde for borgerne, hvilket bekræfter tendensen fra 2018 om, at borgerne søger information i deres eget netværk og bruger hinanden til at løse sikkerhedsudfordringer.

Netop selve kilden til viden om sikkerhed kan være afgørende for kvaliteten af den information, man får, samt i sidste ende, hvor god mulighed man har for at handle hensigtsmæssigt. Det er en af konklusionerne i rapporten "Normenn og digital sikkerhetskultur"[23], der undersøger nordmændenes kilder til viden om informationssikkerhed. Rapporten peger på, at jo mere formel kilden er (dvs. ikke baseret på viden fra en selv eller omgangskreds, men i højere grad baseret på kurser og uddannelse), jo bedre vil folk være til at udøve en adfærd, der er kompatibel med den risiko, de udsætter sig for.

Med denne indsigt in mente må det derfor anses som en positiv udvikling, at de uddannelsesindsatser, der gennemføres på arbejdspladser og uddannelsesinstitutioner, er blevet en mere betydelig kilde til viden om informationssikkerhed for borgerne.

[23] https://norsis.no/wp-content/uploads/2018/11/Nordmenn-og-digital-sikkerhetskultur-2018-web.pdf

Offentligt ansattes informationssikkerhed

5. Trusler rettet mod offentligt ansatte og de ansattes handlemønstre

Kapitlet undersøger, hvilke digitale trusler offentligt ansatte oplever, og hvordan de agerer i mødet med truslerne.

Mange offentligt ansatte arbejder med fortrolige data, hvad enten det er borgernes følsomme personoplysninger, eller det er kritiske data i fx administrationen. Det gør dem til en udsat gruppe i forhold til truslen fra såvel cyberkriminalitet som spionage og i forhold til generel kompromittering af sikkerheden på arbejdspladsen.

Offentligt ansatte arbejder typisk i organisationer, hvor der er krav om, at der skal være styr på den grundlæggende sikkerhed, bl.a. som følge af kravet om implementering af ISO 27001 og tekniske minimumskrav i staten eller efterlevelse af principperne i ISO 27001 i kommuner og regioner samt overholdelse af databeskyttelsesloven (GDPR).

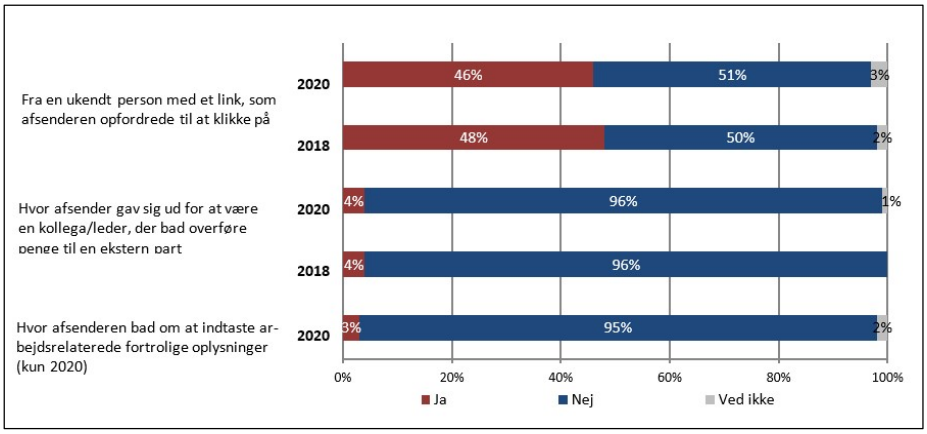
Den tekniske sikkerhed varetages typisk af bl.a. systemadministratorer, som sikrer implementering af grundlæggende sikkerhedstiltag, fx begrænsning i administratorprivilegier, godkendte programmer, procedurer for automatisk opdatering af systemer og programmer mv.

Men også organisationer, der lever op til minimumskrav og sikrer daglig styring af informationssikkerhed, oplever udfordringer med informationssikkerheden. Offentligt ansatte udsættes således for en række digitale trusler og hændelser, som kan være vanskelige at beskytte sig mod. Dette kapitel undersøger de offentligt ansattes oplevelser med digitale trusler samt deres handlinger og konsekvenserne i mødet med truslerne.

Phishing – en vedvarende trussel

Phishing-beskeder[24] på mail og/eller sms er ligesom for borgerne en vedvarende trussel for alle, der arbejder med data og informationer. Næsten halvdelen af medarbejderne (46 pct.) i den offentlige sektor oplyser, at de inden for det seneste år har været udsat for et eller flere forsøg på phishing, hvor de opfordres til at klikke på et link – hvad enten phishingforsøget er sket via sms, chat eller mail (figur 24). Det er på samme niveau som i 2018, hvor 48 pct. havde oplevet phishing-forsøg.

[24] Se ordforklaring i kapitel 9, side 68



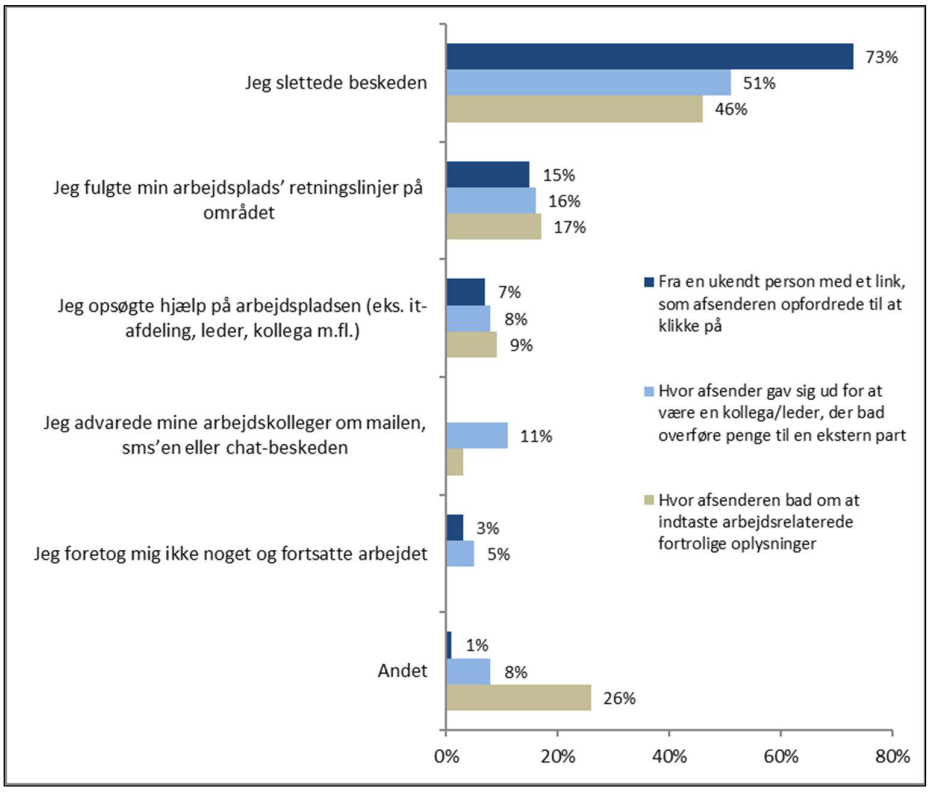
Figur 24 Offentligt ansatte, som en eller flere gange inden for det seneste år har oplevet at modtage en ondsindet e-mail, sms eller chatbesked fra en ukendt person med en opfordring til handling.

CEO-fraud[25] – også kaldet direktørsvindel eller Business Email Compromise - er også en trussel, som offentligt ansatte skal forholde sig til. 4 pct. af de offentligt ansatte svarer, at de inden for det seneste år en eller flere gange har oplevet at modtage sms-, mail- eller chatbeskeder fra personer, der gav sig ud for at være en chef eller kollega, og som bad dem overføre penge til ekstern part, enten en enkelt gang eller flere gange. Det svarer ligeledes til niveauet fra 2018.

3 pct. oplyser, at de har været udsat for forsøg på at blive lokket til at indtaste arbejdsrelaterede fortrolige oplysninger. Det kan være via mail, sms eller chat med link til et websted, hvor oplysninger tastes ind.

Hvad gjorde de offentligt ansatte efter et phishing-forsøg?
Figur 25 viser de offentligt ansattes første handling efter et phishing-forsøg. De fleste anfører, at de sletter beskeden som det første. Næst flest af de offentligt ansatte oplyser, at de som det første følger retningslinjer til håndtering af beskeder med links, direktørsvindel eller en opfordring til indtastning af fortrolige oplysninger.

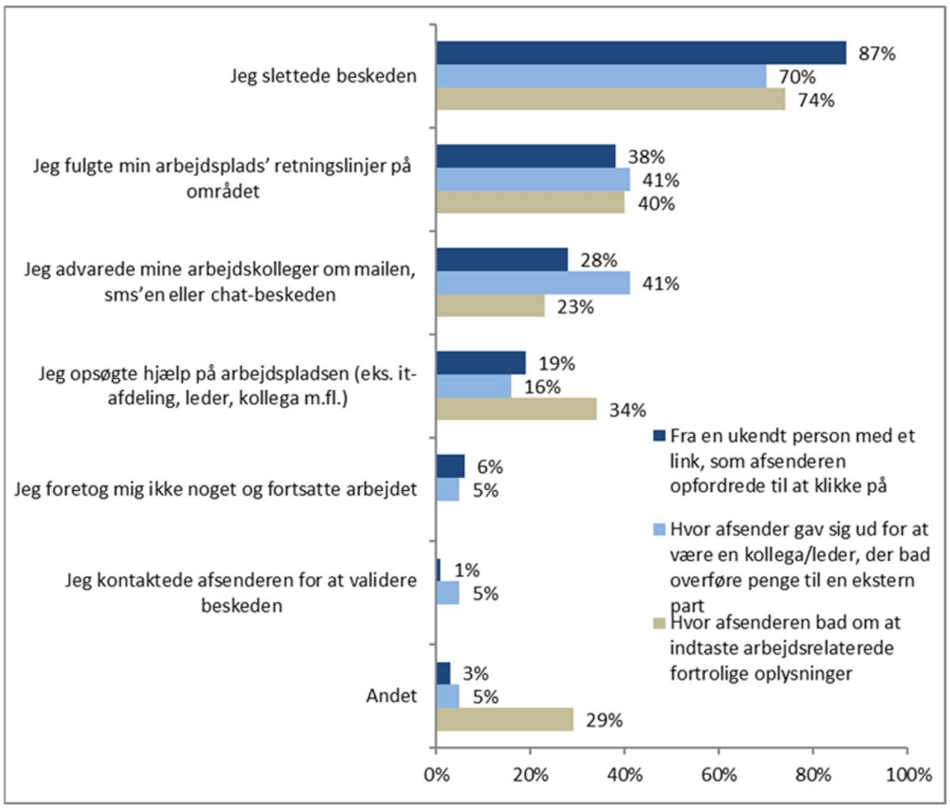
[25] Se ordforklaring i kapitel 9, side 67.



Figur 25 Offentligt ansattes angivelse af den første handling, de foretog, da de modtog en mistænkelig mail, sms eller chatbesked.

Ser man på de samlede handlinger, som det fremgår af figur 26, oplyser mellem 38 pct. og 41 pct., at de som en del af deres samlede handlinger følger arbejdspladsens retningslinjer til håndtering af mail-, chat eller sms-beskeder, hvor de er blevet forsøgt lokket til at kompromittere informationssikkerheden, mens langt flest stadig sletter henvendelsen.

Svindlere behøver kun ét forkert klik på en phishing-henvendelse for at komme ind, men det er positivt, at så mange offentligt ansatte foretager handlinger, som er sikkerhedsmæssigt "rigtige" enten ved at slette mailen, følge retningslinjerne eller opsøge hjælp på arbejdspladsen. Interessant er det at se, at advarsler til kolleger om forsøg på svindel fylder meget, særligt ved CEO-fraud, hvor 41 pct. angiver, at de advarer deres kolleger, hvis de støder på en afsender, der giver sig ud for at være en kollega/leder. Det kan være et udtryk for, at det føles mere indgribende, at phishing-forsøget har en personlig afsender, hvor navnet på ens kollega eller chef bliver brugt. Samtidig er det naturligt, at medarbejderne fortæller deres kollega, hvis dennes navn bliver brugt til svindel.



Figur 26 Offentligt ansattes samlede handlinger, da de modtog en mistænkelig mail, sms eller chat-besked.

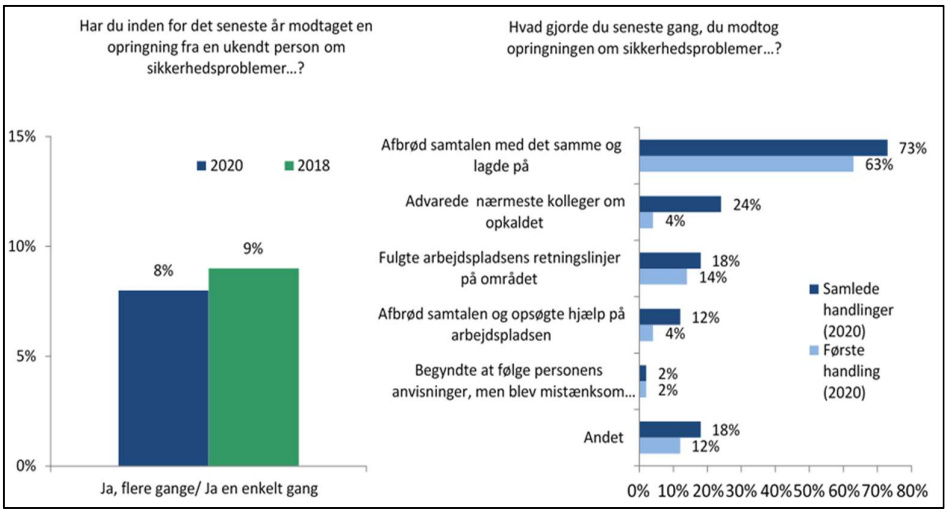
Falske telefonhenvendelser

Falske telefonhenvendelser er en form for phishing, der er lavteknologisk, og hvor et opkald fra fx udlandet kan se ud til at komme fra et dansk telefonnummer (spoofing[26]). Falske telefonhenvendelser kan dog også komme fra Danmark.

Den falske telefonhenvendelse har ofte til formål at lokke oplysninger, fx en e-mailadresse ud af ofrene, hvorefter der returneres en mail med en fil, der skal downloades. Det kan være opringninger fra ukendte personer, der oplyser, at der er alvorlige sikkerhedsproblemer med ofrets arbejdscomputer. Herved kan ofrene med henvisning til telefonsamtalen lokkes til at downloade malware, som installeres på ofrenes pc.

8 pct. af de offentligt ansatte har oplevet falske telefonhenvendelser, hvilket er et fald på 1 pct. i forhold til 2018. De fleste (63 pct.) oplyser i 2020, at de som det første afbryder samtalen, mens 14 pct. oplyser, at de følger arbejdspladsens retningslinjer som det første (figur 27).

[26] Se ordforklaring i kapitel 9, side 70.



Figur 27 Offentligt ansattes erfaringer med at modtage opringninger på deres arbejdstelefon fra ukendte personer, der oplyser, at der er alvorlige sikkerhedsproblemer med deres arbejdscomputer.

Ligesom ved de andre spørgsmål om handlinger som følge af en trussel har vi ikke indblik i arbejdspladsernes retningslinjer, og retningslinjerne kan netop angive at afbryde samtalen som det første. Mere end hver femte (24 pct.) angiver, at de som en af handlingerne advarer kolleger om opkaldet, hvilket kan hjælpe til, at kollegerne er opmærksomme og får afvist eventuelle forsøg på svindelopkald.

Virus og skadelige programmer – markant fald

Der ses et markant fald i andelen af offentligt ansatte, der en eller flere gange har oplevet virus og andre typer skadelige programmer[27] i perioden fra 2018 til 2020. Således er der sket et fald fra 11 pct. i 2018 til 3 pct. i 2020 (figur 28). Faldet kan muligvis skyldes en ændring i spørgemåden, da der i 2020 kun bliver spurgt til, om respondenten har oplevet truslen *inden for* det seneste år, mens der i 2018 ikke var samme periodebegrænsning. En anden mulighed er, at virusprogrammerne er blevet bedre, at truslen simpelthen er mindre til stede eller noget tredje.

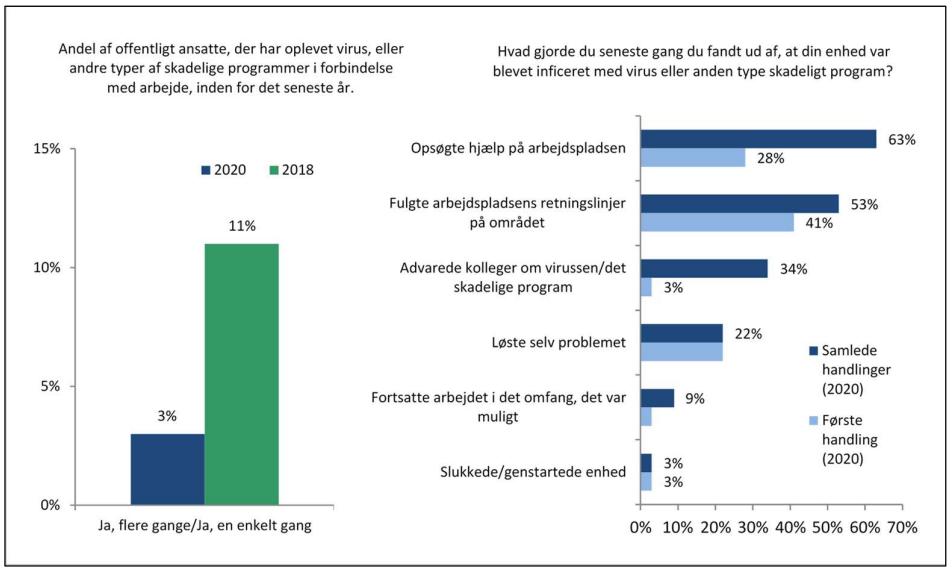
Figuren viser også, hvad de offentligt ansatte gør, efter at de har oplevet virus eller andre typer skadelige programmer. Ligesom på borgerområdet har vi bedt respondenterne svare i prioriteret rækkefølge for at få indblik i de dominerende handlingsmønstre. Det har været muligt for respondenterne at give op til tre svar, hvor første handling viser, hvad respondenterne gjorde først, mens "samlet" viser alle de handlinger, respondenterne har oplyst at have foretaget.

Handlingen "fulgte arbejdspladsens retningslinjer på området" er ganske åben og kan indeholde flere forskellige handlinger lige fra at ringe til et bestemt nummer til at trække netværksstikket ud. Kategorien er inkluderet, fordi dette vil være "den gode handling" i langt de fleste tilfælde. Arbejdspladser vurderer selv, hvad de ansatte skal gøre for at minimere risikoen for at blive udnyttet af en trussel

[27] Se ordforklaring i kapitel 9, side 71.

hos netop dem. Derfor er det relevant at undersøge, hvorvidt de offentligt ansatte følger egen arbejdsplads' retningslinjer, selvom det kan dække over flere handlinger.

At følge arbejdspladsens retningslinjer er således også den handling, flest foretager sig som det første. Det gør 41 pct. af de adspurgte, hvor 28 pct. opsøger hjælp på arbejdspladsen som det første. Ser man på de samlede handlinger, er det over halvdelen (53 pct.), der følger arbejdspladsens retningslinjer ved virus eller andre skadelige programmer, og 63 pct. opsøger arbejdspladsens hjælp. Over en tredjedel (34 pct.) advarer deres kolleger om virus/det skadelige program, hvilket kan hjælpe til, at andre på arbejdspladsen bliver opmærksomme og på vagt over for eventuelle angreb på deres programmer, og det dermed ikke spreder sig yderligere.



Figur 28 Offentligt ansattes oplevelser med virus og andre typer af skadelige programmer og efterfølgende handlinger.

Ved ransomware-angreb[28] sker der typisk det, at data bliver krypteret og dermed ulæselige, og organisationen afkræves en løsesum for at få mulighed for at genskabe data. I disse tilfælde er det særlig vigtigt at reagere straks og følge retningslinjerne og/eller opsøge hjælp. I forbindelse med offentligt kendte ransomware-angreb på større virksomheder er der eksempler på, hvordan systemadministratorers hurtige reaktion i form af nedlukning af netværket har kunnet hindre et skadeligt program i at sprede sig til hele organisationens systemer. Effektiv segmentering af netværk kan også modvirke konsekvenserne af ransomwareangreb. Det fremgår af undersøgelsen her, at kun 1 pct. af de offentligt ansatte har oplevet, at et program spærrede for adgangen til data og krævede betaling for at åbne igen. Det er et fald i forhold til 2018, hvor 2 pct. havde oplevet det.

[28] Se ordforklaring i kapitel 9, side 69.

6. Daglig sikkerhedsadfærd på arbejdspladsen

Kapitlet undersøger offentligt ansattes adfærd i dagligdagssituationer, der kræver en opmærksomhed på informationssikkerhed.

Den daglige adfærd i omgangen med informationer har stor betydning for informationssikkerheden i en organisation. Som ovenstående kapitel klargjorde, udgør offentligt ansatte både en angrebsflade og et forsvarsværk for organisationen. Derfor er det afgørende, at offentligt ansatte sættes i stand til at agere sikkert i hverdagen. Kapitel 8 omhandler, hvordan en organisation kan sikre, at offentligt ansatte i højere grad efterlever informationssikkerhedsretningslinjerne.

Dette kapitel præsenterer den adfærd, som offentligt ansatte angiver at have, når de i hverdagen udfører arbejdsopgaver, hvor informationssikkerheden potentielt kan kompromitteres. De udvalgte situationer, der spørges ind til, er baseret på fællesoffentlige erfaringer med situationer, der typisk kan skabe problemer for offentligt ansatte. Disse situationer vil også typisk være beskrevet i de fleste organisationers informationssikkerhedsretningslinjer.

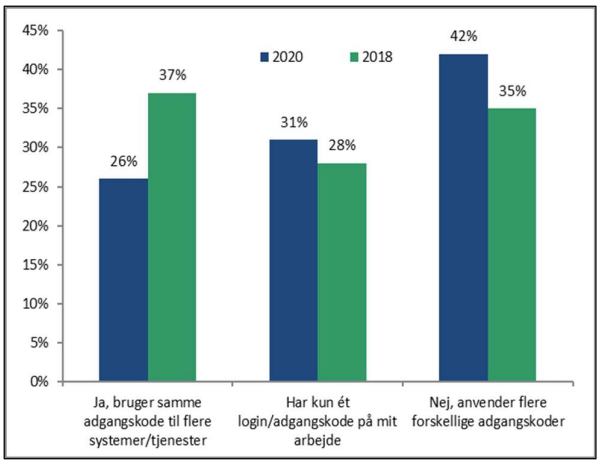
Håndtering af kodeord

Kodeord er ligesom for private borgere en udfordring for de offentligt ansatte. Mange har adskillige kodeord i spil – både privat og på arbejdspladsen – hvilket gør det sværere at håndtere. Særligt er genbrug af samme adgangskode en stor risikofaktorer ift. kompromittering af data.

Ganske vist er der sket et ikke ubetydeligt fald fra 2018 (37 pct.) til 2020 (26 pct.) i andelen af offentligt ansatte, der oplyser, at de genbruger kodeord til flere systemer og tjenester (figur 29). Men den store grad af genbrug er stadig en sårbarhed for offentlige arbejdspladser, da det er nemt for cyberkriminelle at teste et kompromitteret kodeord for genbrug.

Flere (31 pct.) oplyser, at de kun har ét login, dvs. single sign-on, hvilket er en marginal stigning i forhold til 2018. Single sign-on (SSO)[29] er en teknologi, der lader brugere logge ind på flere systemer med det samme sæt brugernavn og password og kan ses som et centraliseret alternativ til en passwordmanager[30].

[29] Se ordforklaring i kapitel 9, side 69.
[30] Se ordforklaring i kapitel 9, side 68.



Figur 29 Offentligt ansattes angivelse af, om de genbruger adgangskoder på deres arbejde.

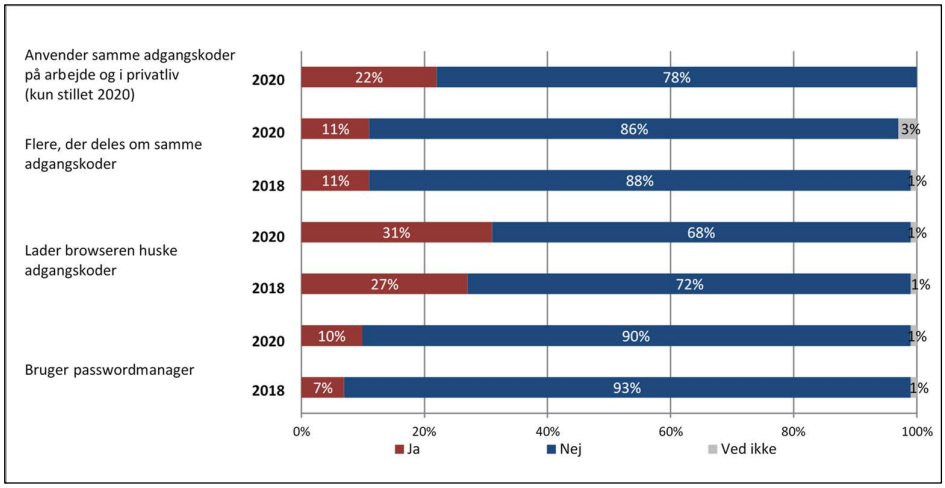
Hvad angår genbrug af adgangskoder mellem privatlivet og arbejdet, ses en tendens til at anvende samme adgangskoder på arbejde og i privatliv, som det fremgår af figur 30. Hele 22 pct. oplyser, at de alle steder eller enkelte steder genbruger adgangskoder fra privatlivet til arbejdspladsen og vice versa.

Det er et væsentligt problem for sikkerheden på arbejdspladsen, fordi kompromitterede kodeord nærmest med garanti forsøges brugt i andre sammenhænge. Dermed kan en dårlig sikkerhedskultur hjemme gå ud over sikkerheden på jobbet, ligesom det modsatte naturligvis også er gældende.

I 2020 er det fortsat gældende, at 11 pct. af de offentligt ansatte deler kodeord, hvilket også gjorde sig gældende i 2018 (figur 30). Hvis der kun findes én nøgle til et fælles it-system, er det en naturlig forklaring, der falder tilbage på opsætningen af systemet, som bør være håndteret i sikkerhedspolitikken og de mere tekniske retningslinjer. Men hvis det er en generel tendens, at man deler kodeord med hinanden, så går det ud over ledelsens overblik over, hvem der logger på et system og hvornår, ligesom det er et udtryk for en problematisk sikkerhedskultur, hvis systemer eller processer "tvinger" ansatte til at dele kodeord, eller hvis det bliver anset som acceptabelt at dele kodeord de ansatte i mellem.

Endeligt er der en lille stigning i antallet af respondenter, der lader browseren huske adgangskoder. Intentionen med spørgsmålet har været at undersøge, hvorvidt respondenterne undlader at have besværet med at huske forskellige adgangskoder ved at lade browseren huske dem for sig. Dette kan udgøre en risiko, i det man ved fysisk adgang til computeren har adgang til systemer mm. Dog kan spørgsmålet også være blevet forstået som, at man anvender browserens pass-

wordmanager til at huske kodeord. Dette anses som en anbefalelsesværdig løsning til håndtering af kodeord. Det er dermed vanskeligt at konkludere på en adfærdstendens ved dette spørgsmål.



Figur 30 Offentligt ansattes håndtering af adgangskoder.

Stigning i brug af passwordmanagers – dog fra lavt niveau
Der ses en stigning i anvendelse af passwordmanager fra 7 pct. i 2018 til 10 pct. i 2020. Interessant er det, at der er lige så få offentligt ansatte, der benytter passwordmanager, som den gruppe blandt borgerne, der i lavest grad benytter det; nemlig de 60+-årige hvor 9 pct. anvender passwordmanager.

Med en passwordmanager kan man have lange og unikke kodeord, uden at der er et behov for, at man skal huske hvert enkelt. Dvs. de kan minimere genbruget af adgangskoder i privat og arbejdsmæssig sammenhæng. Det kan anbefales, at passwordmanager anvendes, når der er behov for at gemme mange unikke passwords, og at valget af løsning baseres på organisationens risikovurdering. Dog vil det være op til organisationen at tilbyde en passwordmanager i overensstemmelse med risikovurderingen, således at de ansatte ikke selv skal finde dem på nettet.

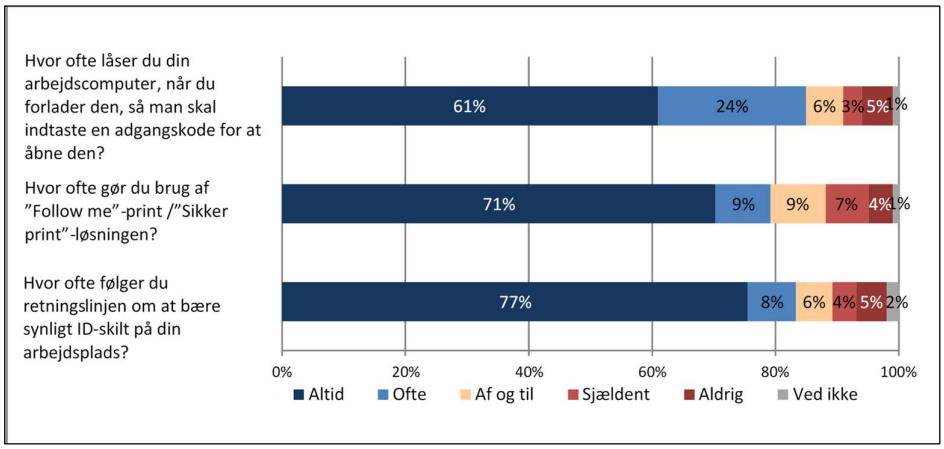
Håndtering af informationer

Det fremgår af de fleste informationssikkerhedspolitikker, at arbejdspladsen og dens medarbejdere skal sikre beskyttelse af organisationens informationer. Informationer findes både i fysisk og digitalt format og kan være tilgængelige for uvedkommende personer, fx hvis arbejdspc'er står åbne og papir glemmes i printeren.

For at imødegå risikoen for at uvedkommende får adgang til informationer, har mange arbejdspladser indført retningslinjer om lås af computeren, når den forlades, og der er etableret obligatoriske sikker print-løsninger.

En høj andel (85 pct.) af de offentligt ansatte svarer, at de altid (61 pct.) eller ofte (24 pct.) låser deres computer med adgangskode, når de forlader den (figur 31).

Brug af sikker print-løsninger ser også ud til at være vidt udbredt i den offentlige sektor, idet 53 pct. af de offentligt ansatte angiver, at deres arbejdsplads har en sikker print-løsning. Blandt disse oplyser 80 pct., at de altid (71 pct.) eller ofte (9 pct.) anvender løsningen.



Figur 31 Offentligt ansattes lås af arbejdscomputer, brug af "Sikker print-løsning" og efterlevelse af retningslinjer om brug af synligt Id-skilt.

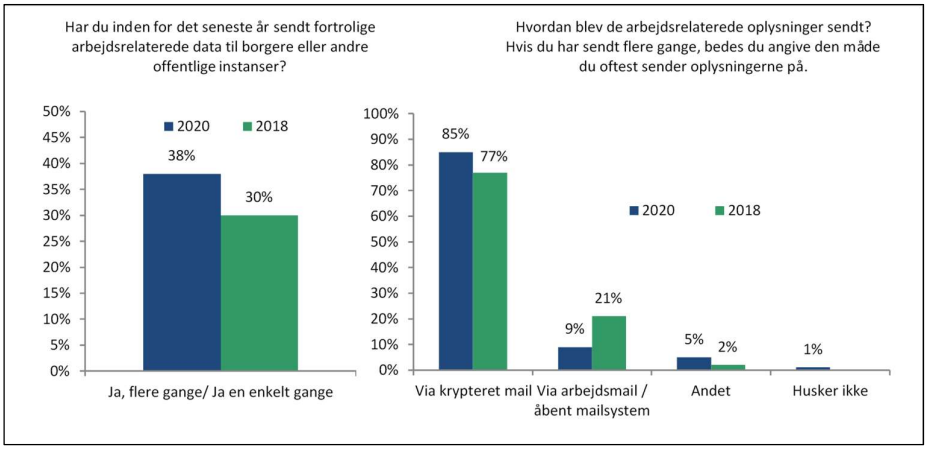
I relation til at beskytte informationerne har mange arbejdspladser et krav om, at ansatte bærer synligt id-kort, så det er synligt, at kun de rette personer bevæger sig rundt på arbejdspladsen.

Samlet set er det lige over en tredjedel af de offentligt ansatte (36 pct.), der angiver, at deres arbejdsplads har retningslinjer om, at man skal bære et synligt Id-kort på sig i det daglige arbejde. Blandt disse oplyser 85 pct., at de altid (77 pct.) eller ofte (8 pct.) bærer det. På den anden side er der 9 pct., der sjældent (4 pct.) eller aldrig (5 pct.) anvender synligt Id-kort, hvilket kan bunde i, at retningslinjerne ikke er nået ud til alle medarbejdere. I kapitel 8 præsenteres således, at 22 pct. svarer nej til at have modtaget information og/eller undervisning i informationssikkerhedspolitikker og-retningslinjer, og 9 pct. angiver, at de ikke husker, om de har modtaget information/undervisning.

69 pct. af de offentligt ansatte, hvis arbejdspladser har retningslinjer for at bære id-kort og for at bruge sikker print-løsninger, oplyser, at de altid eller ofte følger disse retningslinjer.

En anden parameter, som man kan måle omgang med informationer på, er, i hvilken grad de ansatte i den offentlige sektor er opmærksomme på at bruge de rigtige kanaler til udveksling af fortrolige oplysninger.

Der er en stigning fra 30 til 38 pct. i andelen af offentligt ansatte, der inden for det seneste år har sendt arbejdsrelaterede fortrolige data til borgere eller andre offentlige myndigheder (figur 32). Langt de fleste – og ligeledes en stigning i forhold til 2018 – anvender i 2020 krypteret mail (85 pct. mod 77 pct.), mens færre bruger åben mail (9 pct. mod 21 pct.).



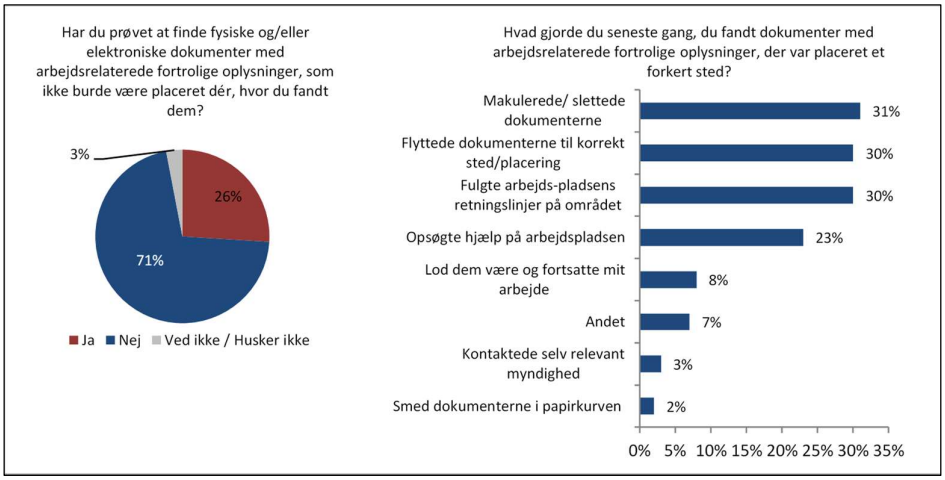
Figur 32 Offentligt ansattes adfærd i forbindelse med udveksling af fortrolige arbejdsrelaterede informationer.

Dette vidner om en høj grad af bevidsthed om at bruge sikre kanaler til fortrolige forsendelser. Bevidstheden kan muligvis finde sin årsag i indførelsen af databeskyttelsesforordningen i 2018, der givetvis for mange har medført en langt større opmærksomhed og bevågenhed på beskyttelse af borgere og organisationers oplysninger end tidligere.

Informationer findes som bekendt ikke kun i digital form, men også fysisk. Ligeså vel som det er vigtigt at håndtere digitale informationer sikkert, er det vigtigt at sikre, at fortrolige og følsomme informationer findes i et sikkert miljø. Vi har stillet spørgsmål til dette for at få indblik i, hvordan de ansatte handler, hvis de finder fortrolige og/eller følsomme informationer et sted, de ikke burde være. 26 pct. af de offentligt ansatte har prøvet at finde oplysninger, som ikke burde være placeret der, hvor de befandt sig (figur 33).

De fleste angiver, at de foretager en handling for at beskytte informationerne frem for blot at lade dem være. Det ses af figuren, hvor langt størstedelen handler enten ved at makulere dokumenterne (31 pct.), flytte dokumenterne til korrekt placering (30 pct.), efterleve arbejdspladsens retningslinjer (30 pct.) eller op-

søge hjælp på arbejdspladsen (23 pct.). Kun 8 pct. oplyser, at de lod dokumenterne være. Det vidner om god opmærksomhed på, hvornår dokumenter er forkert placeret og en evne til at handle på det.

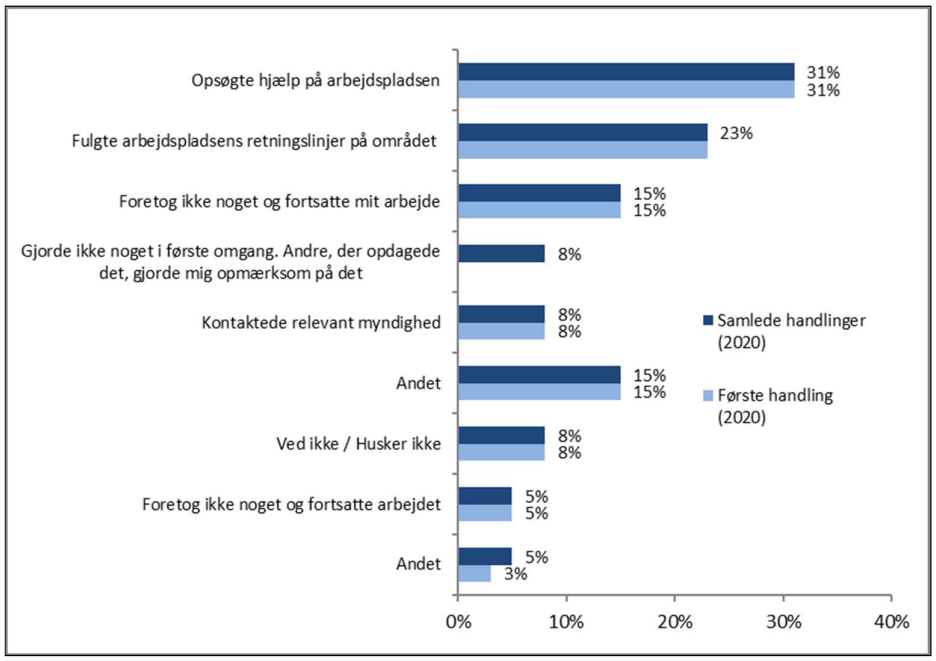


Figur 33 Offentligt ansattes erfaringer med forkert placerede fortrolige dokumenter.

Tab af informationer fysisk eller digitalt

De færreste offentligt ansatte har oplevet at miste informationer i forbindelse med deres arbejde. Således oplyser 98 pct. af de ansatte, at de ikke har prøvet at miste fysiske dokumenter og/eller USB-stik med arbejdsrelaterede fortrolige oplysninger. 1 pct. har oplevet tab af fysiske dokumenter, og ligeledes 1 pct. har oplevet at miste et USB-stik med fortrolige dokumenter.

Blandt de få offentlige ansatte, der har oplevet at miste fortrolige oplysninger (enten fysiske dokumenter eller USB-stik), angiver flest, at de opsøgte hjælp på arbejdspladsen (31 pct.), mens 23 pct. svarer, at de fulgte arbejdspladsens retningslinjer på området. 15 pct. svarer, at de ikke foretog sig noget og fortsatte deres arbejde (figur 34).



Figur 34 Offentligt ansattes handlinger efter oplevelser med at miste fortrolige oplysninger (enten fysiske dokumenter eller USB-stik).

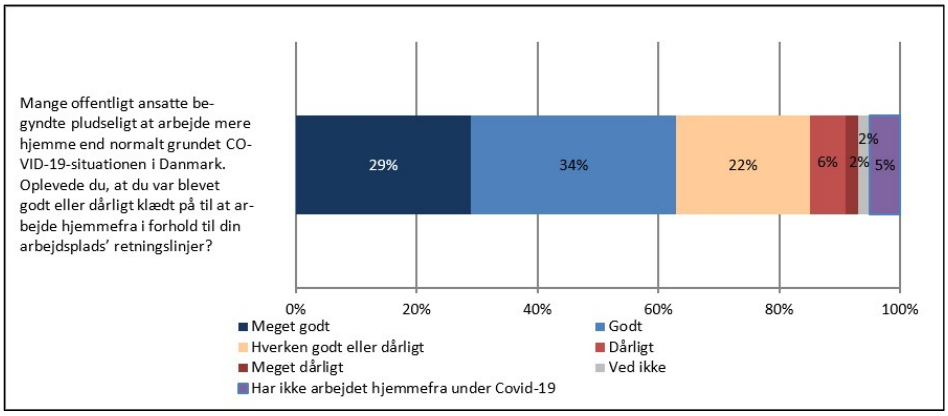
Ligesom i de øvrige spørgsmål har respondenterne haft mulighed for at svare, hvad de gjorde i prioriteret rækkefølge. De handlinger, som angives som første handlinger og de samlede fordelinger, er næsten identiske for dette spørgsmål. Det skyldes, at langt størstedelen kun angiver at have foretaget en enkelt handling i forbindelse med mistede fortrolige oplysninger.

Set i den kontekst ser der ud til at være god forståelse for, at man – hvis man har mistet fortrolige dokumenter – skal handle, når der sker et tab.

7. Daglig sikkerhedsadfærd uden for arbejdspladsen

COVID-19-pandemien resulterer i massivt øget hjemmearbejde for mange offentligt ansatte. Kapitlet undersøger offentligt ansattes digitale sikkerhed og adfærd, når de arbejder hjemme eller andre steder uden for arbejdspladsen.

Under nedlukningen af flere offentlige arbejdspladser i 2020 er hjemmearbejde blevet hverdag, og de fleste organisationer står derfor i nye og vigtige opgaver ift. at sikre hjemmearbejdspladserne. Brug af private enheder og åbne netværk samt brug af nye kommunikationstjenester og digitale værktøjer er pludselig gængse forhold, som sikkerhedsafdelinger skal sørge for at håndtere. Ligeledes bliver de offentligt ansattes sikkerhedsadfærd afprøvet på nye måder, når arbejdspladsen ikke danner fysisk ramme for arbejdet[31]. Det stigende arbejde uden for arbejdspladserne har også påvirket trusselsbilledet ift. de angrebsmetoder, hackerne vælger.



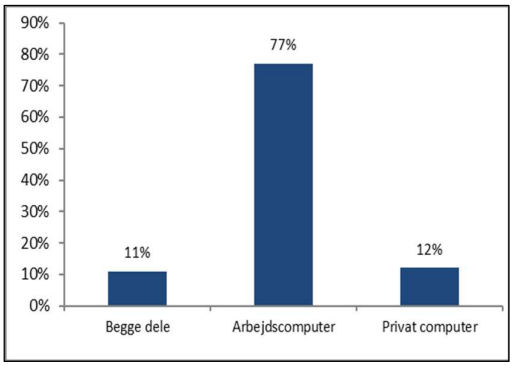
Figur 35 Offentligt ansatte og det at skulle arbejde hjemmefra under corona-situationen i sommeren 2020, hvor data blev indsamlet.

De fleste offentligt ansatte (63 pct.), der til tider arbejder hjemmefra, oplevede, at de var blevet godt/meget godt klædt på til at arbejde hjemmefra i forhold til arbejdspladsens retningslinjer (figur 35). Dette må ses som en høj andel taget i betragtning af, at de fleste offentlige arbejdspladser kun havde få dage til at forberede deres medarbejdere på den nye situation. Det kan dog også være et udtryk

[31] Digitaliseringsstyrelsen har lanceret sikkerdigital.dk/hjemme som en hjælp til de vigtigste huskeregler, når man arbejder uden for arbejdspladsens fysiske rammer.

for, at arbejdspladserne havde beredskabet i orden, og/eller at retningslinjerne for informationssikkerhed ved hjemmearbejde allerede var godt forankret i organisationen.

En af præmisserne ved sikkert hjemmearbejde er typisk, at medarbejderne har en arbejdscomputer stillet til rådighed. Det er vanskeligt som medarbejder, der ikke har informationssikkerhed som kerneopgave, på egen hånd at sørge for, at en privat computer lever op til kravene for en sikker computer til arbejdsbrug. Derfor har undersøgelsen spurgt til udbredelsen af brug af private computere til arbejdsbrug. 23 pct. angiver, at de bruger en privat eller en blanding af privat- og arbejdscomputer, når de arbejder hjemmefra (figur 36).



Figur 36 Offentligt ansattes anvendelse af privat computer ved hjemmearbejde.

Brug af privat computer i arbejdsmæssig sammenhæng er typisk problemfyldt, hvis den ikke er godkendt af arbejdspladsen. Specielt adgange til systemer, automatiske sikkerheds- og antivirus-opdateringer, automatisk back up og håndtering af informationer kan være vanskeligt på en privat computer, der er uden for arbejdspladsens miljø.

Derfor er det en smule bekymrende, at så mange anvender deres private computer, når de arbejder hjemme. En ubeskyttet privat computer er ofte set som trædested for en hacker ind i organisationssystemer.

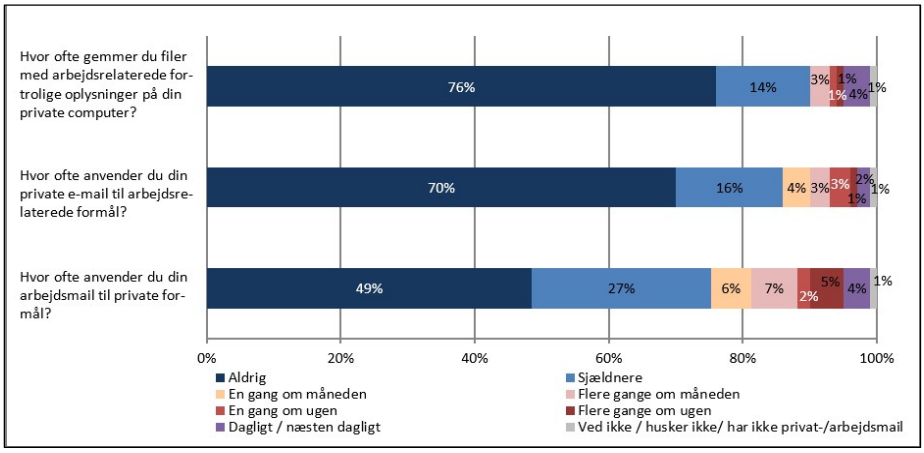
De offentligt ansatte, der anvender privat computer eller både arbejdscomputer og privat computer (dvs. samlet 23 pct.) er blevet stillet spørgsmål om håndteringen af informationer.

90 pct. oplyser, at de sjældnere end en gang om måneden eller aldrig gemmer filer med fortrolige oplysninger på deres private computer. Næsten lige så mange (86 pct.) oplyser, at de sjældent eller aldrig anvender deres private e-mail til arbejdsrelaterede formål, mens 76 pct. anvender arbejdsmailen til private formål (figur 37).

Det er grundlæggende problematisk for informationssikkerheden, hvis medarbejderne ikke formår at holde arbejdsrelaterede informationer og udstyr adskilt fra privatrelaterede, da det øger sandsynligheden for utilsigtede hændelser – herved risikerer medarbejdere at blive ubevidste insidere. Center for Cybersikkerhed vurderer i sin trusselsvurdering "Truslen fra bevidste og ubevidste insidere"[32], at ubevidste insidere er involveret i op mod halvdelen af sikkerhedshændelserne i

[32] https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/CFCS-PET-truslen-fra-bevidste-og-ubevidste-insidere.pdf

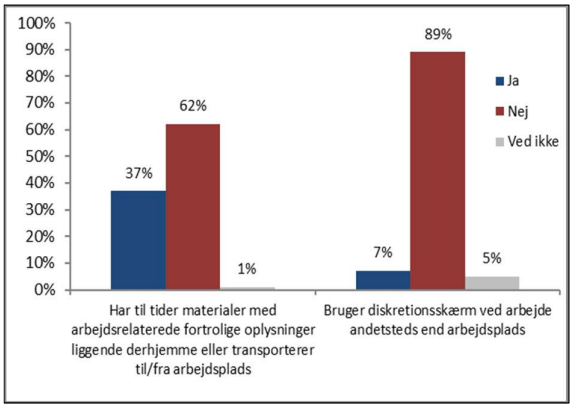
en organisation, og at cyberkriminelle udnytter disse forhold i forbindelse med angreb mod danske organisationer.



Figur 37 Offentligt ansattes anvendelse af privat computer ved hjemmearbejde og privat e-mail mv.

Håndteringen af informationer både fysisk og digitalt er en lige så vigtig faktor. En ting er at beskytte informationerne på arbejdspladsen, men hvordan ser det ud, når det handler om de informationer, man tager fysisk med sig uden for arbejdspladsen?

Det er første gang, spørgsmålet om omgangen med fortrolige dokumenter og brug af diskretionsskærm uden for arbejdspladsen stilles. Relativt mange (37 pct.) oplyser, at de til tider har arbejdsrelateret fortroligt materiale liggende hjemme eller transporterer det til og fra arbejde (figur 38).



Figur 38 Offentligt ansattes håndtering af informationer uden for arbejdspladsen.

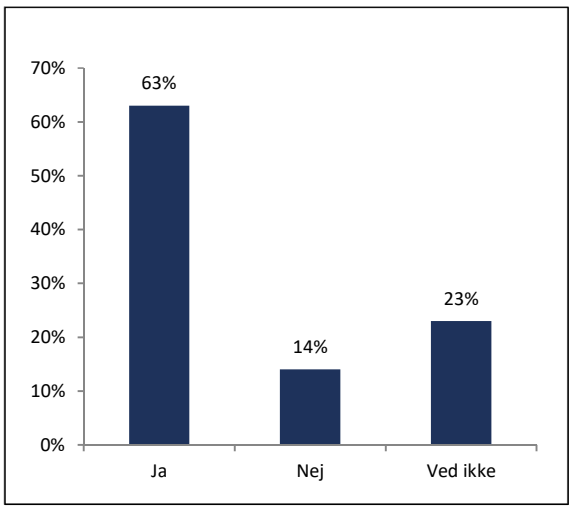
Hvis oplysninger transporteres og opbevares sikkert i henhold til arbejdspladsens retningslinjer udgør dette ikke et problem, da risikoen for datatab er minimeret. Men den høje andel af ansatte, der flytter oplysninger, bør give anledning til, at arbejdspladser undersøger omgangen med informationer under hjemmearbejde.

7 pct. oplyser, at de bruger diskretionsskærm, når de ikke er til stede på arbejdspladsen. Spørgsmålet kunne med fordel have været nuanceret med information om, hvorvidt der bliver brugt diskretionsskærm, når der arbejdes med fortrolige

oplysninger og ikke i alle situationer. Med denne præcisering havde andelen, der bruger diskretionsskærm, muligvis været højere.

Brug af tjenester og kanaler til udveksling af information

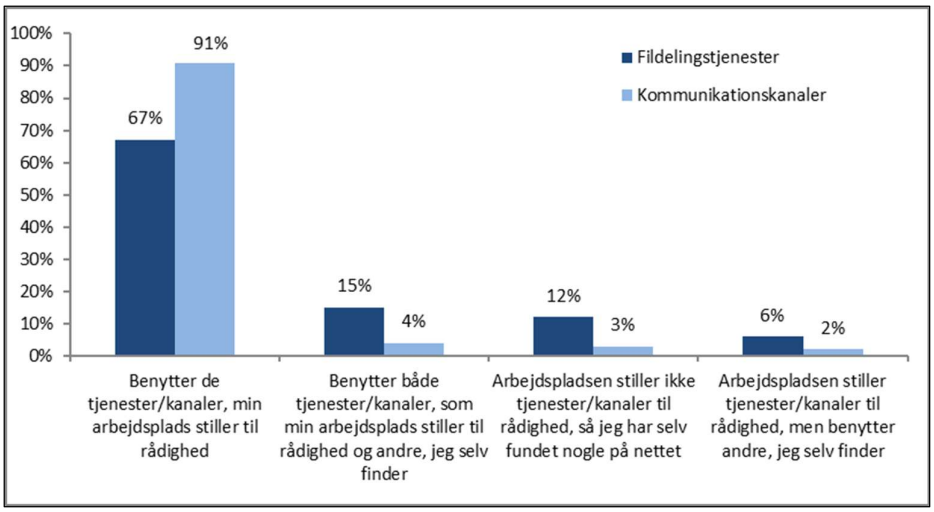
Fildelingstjenester er en populær metode til udveksling af større arbejdsdokumenter, der ikke kan håndteres via fx Outlook. Ligeledes bruges kommunikationskanaler som Skype, Teams og Zoom flittigt til virtuelle møder ved hjemmearbejde. Ud fra et sikkerhedsperspektiv skal arbejdspladserne ikke overlade det til de ansatte selv at finde tjenester og risikovurdere dem. Det vil altid være arbejdspladsens ansvar at stille værktøjer til rådighed, som lever op til arbejdspladsens sikkerhedskrav, således at udveksling af informationer sker i overensstemmelse med arbejdspladsens risikovurderinger.



Figur 39 Offentligt ansattes angivelse af, om deres arbejdsplads har retningslinjer for brug af fx mail, kommunikationskanaler og fildelingstjenester ifm. hjemmearbejde/arbejde andetsteds end på arbejdspladsen.

Af den grund er det afgørende at have retningslinjer for brug af kommunikationskanaler mm., som også er kommunikeret bredt ud i organisationen. 63 pct. af de offentligt ansatte oplyser, at arbejdspladsen har retningslinjer for brug af denne slags tjenester. 14 pct. oplyser, at der ikke er retningslinjer, mens hele 23 pct. ikke ved det (figur 39). Dette udgør en risiko, hvis de ansatte, der ikke ved det eller ikke har tjenester til rådighed, faktisk benytter tjenester, som de så potentielt selv finder på nettet. Uden en tilstrækkelig risikovurdering af tjenester kan der være risiko for, at følsomme data ikke behandles tilstrækkeligt sikkert, eller at databeskyttelseslovgivningen ikke overholdes.

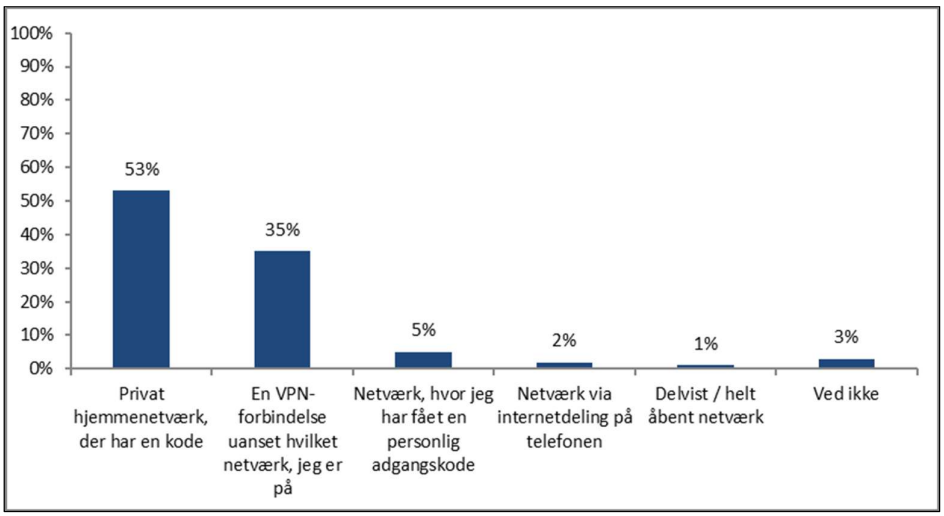
Når det kommer til den konkrete anvendelse af fildelingstjenester, oplyser 21 pct. af de offentligt ansatte, at de anvender netop disse. Af disse oplyser to tredjedele, at de anvender fildelingstjenester, som arbejdspladsen stiller til rådighed, mens en tredjedel anvender andre tjenester (figur 40). Selv om fildelingstjenester, man selv finder, godt kan være sikre, udgør det en risiko, at man sjældent er sikker på, hvor tjenesten opbevarer informationerne.



Figur 40 Offentligt ansattes brug af fildelingstjenester og kommunikationskanaler til virtuelle møder.

67 pct. af de offentligt ansatte oplyser, at de anvender kommunikationskanaler i deres arbejde. Af de 67 pct. oplyser 91 pct., at de anvender arbejdspladsens kanaler. Det tyder på en høj bevidsthed og forankring ift. hvilke kanaler, man bruger til virtuelle møder. Det er positivt, fordi det sikrer, at man kan drøfte fortrolige oplysninger over en kanal, der efterlever arbejdspladsens retningslinjer.

Trådløse netværk er også en kanal til udveksling af informationer. Trådløse netværk sender data som radiobølger, men enhver, der er inden for senderens rækkevidde, kan opsnappe signalerne, også selv om det er krypteret med adgangskode. Derfor anbefales det typisk, at man beskytter sig mod denne risiko ved at anvende VPN[33]. 35 pct. af de offentligt ansatte oplyser, at de anvender en VPN-



Figur 41 Offentligt ansattes brug af trådløse netværk, når de arbejder uden for arbejdspladsen.

[33] Se ordforklaring i kapitel 9, side 71

forbindelse i forbindelse med arbejde uden for arbejdspladsen, mens 53 pct. oplyser, at de bruger et privat hjemmenetværk med kode (figur 41).

Det er positivt, at mere end halvdelen er opmærksomme på, at deres internetforbindelse skal være beskyttet med en kode. Sikkerheden i dette forudsætter dog også, at man sørger for, at koden, der er på netværket, ikke er en generisk kode, som alle routere blot har fået fra fabrikantens side. Dette vil være meget let for hackere at prøve af. Hvis man anvender en VPN-forbindelse, vil denne kode dog være underordnet, idet VPN-forbindelsen sørger for, at trafikken mellem brugeren og serveren er krypteret. Derfor ville det være positivt, hvis endnu flere arbejdspladser sørgede for, at oprettelse af en VPN-forbindelse var obligatorisk for overhovedet at kunne komme på nettet på arbejdscomputeren. Dermed ville ansvaret for en sikker forbindelse ikke afhænge af, at den offentligt ansatte selv havde sørget for at sikre sin forbindelse.

8. Barrierer og drivere for at efterleve arbejdspladsens retningslinjer om informationssikkerhed

Kapitlet undersøger offentligt ansattes opmærksomhed på hhv. digitale trusler og risici samt informationssikkerhedspolitikker og -retningslinjer på deres arbejdsplads. Derudover undersøges de barrierer og drivere, der er for at efterleve retningslinjerne i hverdagen.

COVID-19-pandemien med massivt hjemmearbejde til følge har sat de offentlige arbejdspladsers retningslinjer og værktøjer til brug for hjemmearbejde på en prøve. Kapitlet viser, at der stadig er et arbejde med at sørge for, at det ikke er op til de enkelte ansatte at skabe et sikkert miljø for arbejde væk fra arbejdspladsens fysiske (og sikrere) rammer. Oplysning, undervisning og opsætning af tekniske barrierer er eksempler på tiltag, der kan bidrage til at sikre hjemmearbejdspladserne bedre. God adfærd tager dog typisk tid at opnå.

Dette kapitel vil undersøge, hvilke barrierer og drivere der er for at have en sikker adfærd i sit arbejde – uanset om man er til stede på arbejdspladsen, eller om man arbejder hjemmefra.

Kapitel 4 behandlede borgernes efterlevelse af de grundlæggende anbefalinger til at have en sikker digital hverdag. Kapitlet konkluderede, at få borgere foretager de ønskede sikkerhedsvalg, hvis de er besværlige/tidskrævende eller svære at forstå. Dette kapitel vil ligeledes undersøge, hvilke barrierer og drivere der er, for at de offentligt ansatte efterlever de informationssikkerhedspolitikker og -retningslinjer, som arbejdspladsen har.

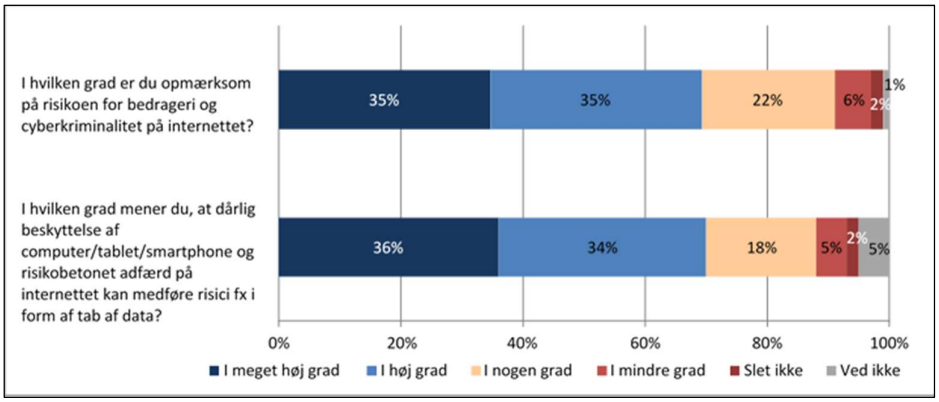
Sandsynligheden for, at en offentligt ansat efterlever en bestemt retningslinje om informationssikkerhed, vil typisk øges, hvis den offentligt ansatte faktisk har en opmærksomhed på dagsordenen om informationssikkerhed. Derfor undersøger kapitlet først status på de offentligt ansattes opmærksomhed.

Dernæst undersøges, hvordan det står til med efterlevelsen af de respektive arbejdspladsers informationssikkerhedsretningslinjer, samt hvad der er udslagsgivende for at have en bestemt sikkerhedsadfærd i sit arbejde.

Hvor opmærksomme er offentligt ansatte på digitale trusler og risici?

De offentligt ansatte (70 pct.) er jf. figur 42 marginalt mindre opmærksomme på risikoen for bedrageri og cyberkriminalitet på nettet, end tilfældet var med borgerne i kapitel 4 (74 pct.). En medvirkende årsag kan være, at man som offentligt

ansat har bevidstheden om, at der på arbejdspladsen findes en eller flere informationssikkerhedskoordinatorer, der er ansat til netop at være opmærksomme på disse risici. Til gengæld er de offentlige ansatte marginalt mere opmærksomme på dårlig beskyttelse og risikobetonet adfærd (70 pct.) end borgerne (66 pct.). Det kan skyldes, at mange af de offentlige ansatte i deres professionelle liv i højere grad håndterer fortrolige data, end borgere i almindelighed gør.



Figur 42 Offentligt ansattes opmærksomhed på bedrager på internettet og risikobetonet adfærd

En anden årsag til forskellen kan være – som det blev konkluderet i kapitel 4 – at uddannelsesindsatser i regi af uddannelsesinstitutioner og arbejdspladser er blevet en større kilde til borgernes viden om digital sikkerhed, hvilket tyder på, at denne type uddannelsesindsatser har haft en effekt ift. at højne opmærksomheden.

Ligesom for borgerne ses det i undersøgelsen blandt de offentligt ansatte, at der er en tendens til at: Jo mere opmærksom man angiver at være på bedrageri og cyberkriminalitet, og jo mere man mener, at risikobetonet adfærd udgør en sårbarhed, des oftere angiver man også, at man kender arbejdspladsens retningslinjer for informationssikkerhed, samt at man følger dem.

De offentligt ansatte, der oplyser at være opmærksomme på bedrageri og cyberkriminalitet, er i højere grad bekendte med sikkerhedspolitikker og retningslinjer på arbejdspladsen. 74 pct. af de ansatte, der i høj/meget høj grad er opmærksomme på cyberkriminalitet mv. oplyser, at de er bekendte med arbejdspladsens sikkerhedspolitikker og retningslinjer. Kun 40 pct. af de ansatte, der i mindre grad/slet ikke er opmærksomme på bedrageri og cyberkriminalitet, er bekendte med arbejdspladsens sikkerhedspolitikker og retningslinjer.

Yderligere ses det, at ansatte, der er opmærksomme, også oftere følger retningslinjerne. 76 pct. af de ansatte, der i høj/meget høj grad er opmærksomme på bedrageri og cyberkriminalitet, svarer "nej" til, at de nogen gange undlader at følge arbejdspladsens sikkerhedspolitikker og retningslinjer. Blandt ansatte, der i mindre grad/slet ikke er opmærksomme, er det kun 61 pct., der svarer "nej" til dette.

Et par observationer understøtter sammenhængen mellem opmærksomheden og den konkrete adfærd, som de offentligt ansatte har oplyst. Jo mere opmærksomme de offentligt ansatte angiver at være på bedrageri og cyberkriminalitet, jo bedre adfærd angiver de at have, når det kommer til:

- Anvendelse af forskellige adgangskoder til forskellige systemer.
- Anvendelse af passwordmanager.
- At låse deres computer, når den forlades.
- Anvendelse af "Follow-me" print/sikker print-løsningen på arbejdspladsen.
- Anvendelse af VPN-forbindelse i forbindelse med hjemmearbejde.
- Anvendelse af diskretionsskærm, når der ikke arbejdes fra den normale arbejdsplads.

Endvidere ses det, at de "opmærksomme offentligt ansatte", der inden for det seneste år har prøvet at modtage en phishing-henvendelse, oftere følger arbejdspladsens retningslinjer på området (41 pct.), oftere opsøger hjælp på arbejdspladsen (22 pct.) samt oftere advarer kollegaer om henvendelsen (31 pct.). Alt sammen handlinger, som er udtryk for en god sikkerhedskultur.

Blandt de ansatte, der i mindre grad/slet ikke er opmærksomme på bedrageri og cyberkriminalitet, angiver markant færre at foretage en af de ovenstående handlinger. Her er andelen, der følger retningslinjerne, opsøger hjælp og advarer kollegaer kun 5 pct. for alle tre handlinger.

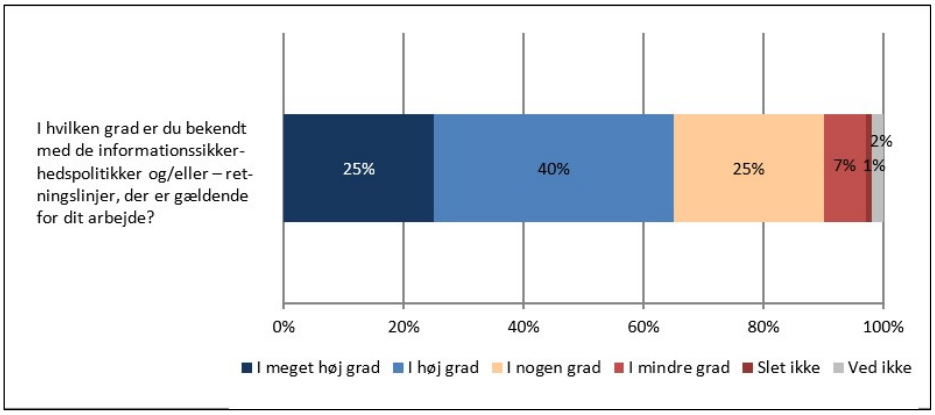
Samtidig ses en tendens til, at jo mindre opmærksomme de offentligt ansatte er på bedrageri og cyberkriminalitet, jo flere angiver, at de ikke foretog nogen handlinger, men blot fortsatte med at arbejde. Således angiver 1 ud af 5 offentligt ansatte (19 pct.), at de ikke foretog sig noget, men fortsatte med at arbejde, da de modtog en phishing-henvendelse. Blandt offentligt ansatte, der i høj/meget høj grad er opmærksomme på risikoen for bedrageri og cyberkriminalitet, er denne andel kun på 4 pct. Dette understøtter hypotesen om, at jo mere opmærksomme de ansatte er, jo flere forebyggende handlinger mod svindel foretages.

Det tyder således på, at der er en sammenhæng mellem at være opmærksom på farerne på nettet samt farer ved en risikobetonet adfærd og at foretage de handlinger, der anses som god daglig sikkerhedsadfærd.

Hvorfor efterleves arbejdspladsens retningslinjer ikke?

Sidste afsnit viste, at der umiddelbart er en sammenhæng mellem offentligt ansattes opmærksomhed på digitale trusler og den konkrete adfærd. Dette afsnit vil undersøge informationssikkerhedspolitikker og -retningslinjer mere nærgående, da disse er et grundlæggende element i organisationernes sikkerhedskultur. Politikker og retningslinjer for informationssikkerhed besluttes typisk af den øverste

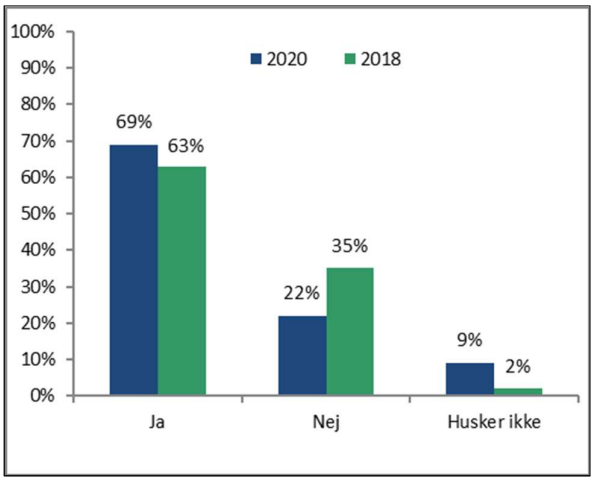
ledelse og er dermed udtryk for, hvad ledelsen forventer af medarbejderne ud fra den aktuelle trussels- og risikovurdering.



Figur 43 Offentligt ansattes kendskab til informationssikkerhedspolitikkerne og/eller retningslinjer på deres arbejdsplads.

Kendskab til informationssikkerhedspolitikker og retningslinjer er sjældent tilstrækkeligt til, at politikker og retningslinjer så faktisk efterleves. Dog vil kendskabet til dem typisk være en forudsætning. Således angiver 65 pct. af respondenterne, at de i høj/meget høj grad er bekendte med de sikkerhedspolitikker og/eller retningslinjer, der er gældende for deres arbejde (figur 43).

I 2018 svarede 57 pct. "ja" og 42 pct. "nej" til spørgsmålet om, hvorvidt de *havde sat sig* ind i it-sikkerheds- og informationssikkerhedspolitikken på deres arbejde. Stigningen kan sandsynligvis tilskrives en ændring i spørgemåden, idet spørgsmålet i 2020 er blevet præciseret til, at det ikke kun er den ansattes ansvar at *sætte sig ind* i retningslinjerne, men at arbejdspladsen også har et ansvar i at gøre de ansatte bekendte med dem.



Figur 44 Offentligt ansattes angivelse af, om de har modtaget undervisning i informationssikkerhedspolitikker og/eller -retningslinjer.

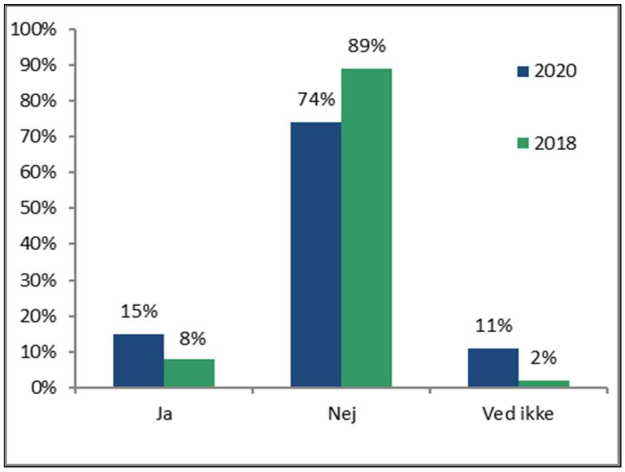
Derfor har undersøgelsen også netop spurgt til, om de ansatte har modtaget undervisning og information om retningslinjerne. I 2018 blev der spurgt til, om respondenterne var blevet informeret om informationssikkerhedspolitikken. I 2020 er spørgsmålet præciseret til at omhandle information og/eller undervisning, hvorfor der muligvis ses en lille stigning. 69 pct. oplyser, at de har modtaget information/undervisning, mens det drejede sig om 63 pct. i 2018 (figur 44).

Næsten en ud af ti (9 pct.) svarer, at de ikke kan huske, at de har modtaget information og/eller undervisning, hvilket er en stigning fra 2018.

Respondenterne er også blevet spurgt til, om de ved, hvem de skal kontakte på arbejdspladsen, hvis de har spørgsmål til informationssikkerhed. Dette må anses som et minimumsudbytte af at gennemføre en informations- eller undervisningsindsats på en arbejdsplads. 90 pct. angiver, at de ved, hvem de skal kontakte.

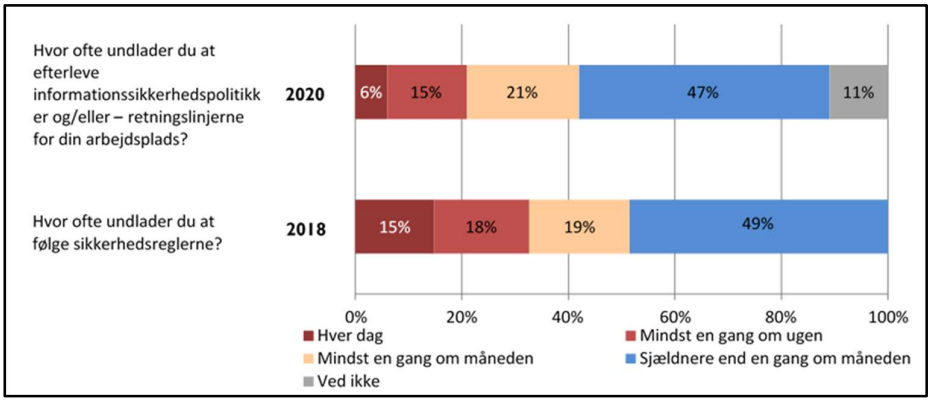
Undersøgelsens respondenter er også blevet spurgt til, om de til tider undlader at efterleve retningslinjerne. Her er der sket en stigning fra 2018, hvor de offentligt ansatte blev spurgt, om de nogen gange undlader at følge sikkerhedsreglerne, fordi de gør det besværligt at udføre arbejdet. Mens 15 pct. i 2020 svarer ja til, at de nogle gange undlader at efterleve informationssikkerhedspolitikker og -retningslinjer, svarede kun 8 pct. ja til dette i 2018 (figur 45).

Det er en bekymrende udvikling, fordi retningslinjerne netop er udtryk for arbejdspladsens definition af ønsket sikkerhedsadfærd, der skal støtte op om en god sikkerhedskultur. Stigningen kan have flere årsager: Måske har arbejdspladserne strammet deres retningslinjer eller måske har hjemmearbejde gjort det sværere at efterleve retningslinjerne. Uanset diagnosen bør udviklingen give anledning til refleksion på arbejdspladserne.



Figur 45 Offentligt ansattes angivelse af, om de til tider undlader at efterleve arbejdspladsens informationssikkerhedspolitikker og/eller retningslinjer.

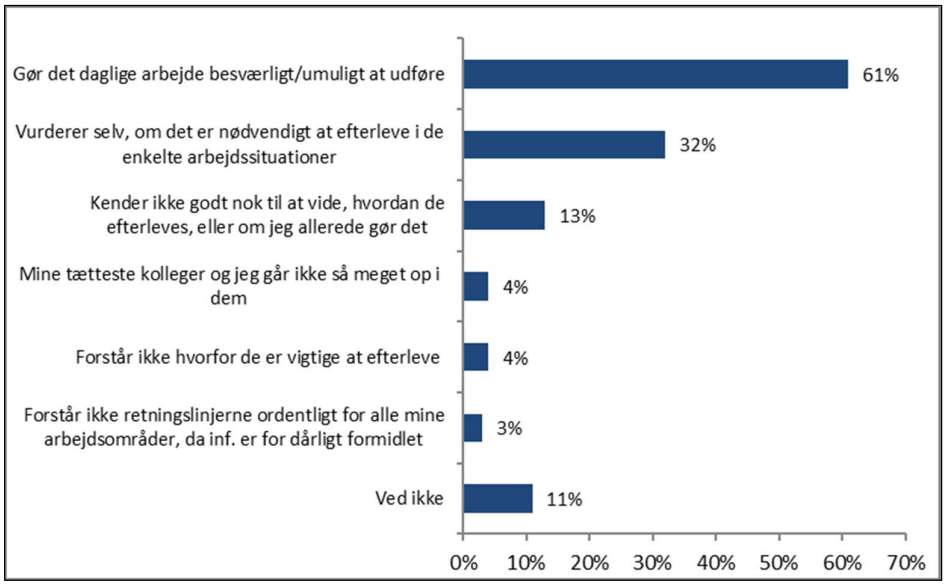
Respondenterne er også blevet spurgt om, hvor ofte de undlader at følge retningslinjerne (figur 46). Resultatet kan være vanskeligt at sammenligne med 2018, da der i 2020 er blevet tilføjet en "ved ikke"-kategori. Det fremgår dog, at 32 pct. enten ikke ved, hvor ofte de undlader at følge retningslinjerne, eller at de mindst en gang om ugen eller oftere undlader at efterleve dem.



Figur 46 Offentligt ansattes angivelse af, hvor ofte de undlader at efterleve informationssikkerhedspolitikker og/eller retningslinjerne for deres arbejdsplads.

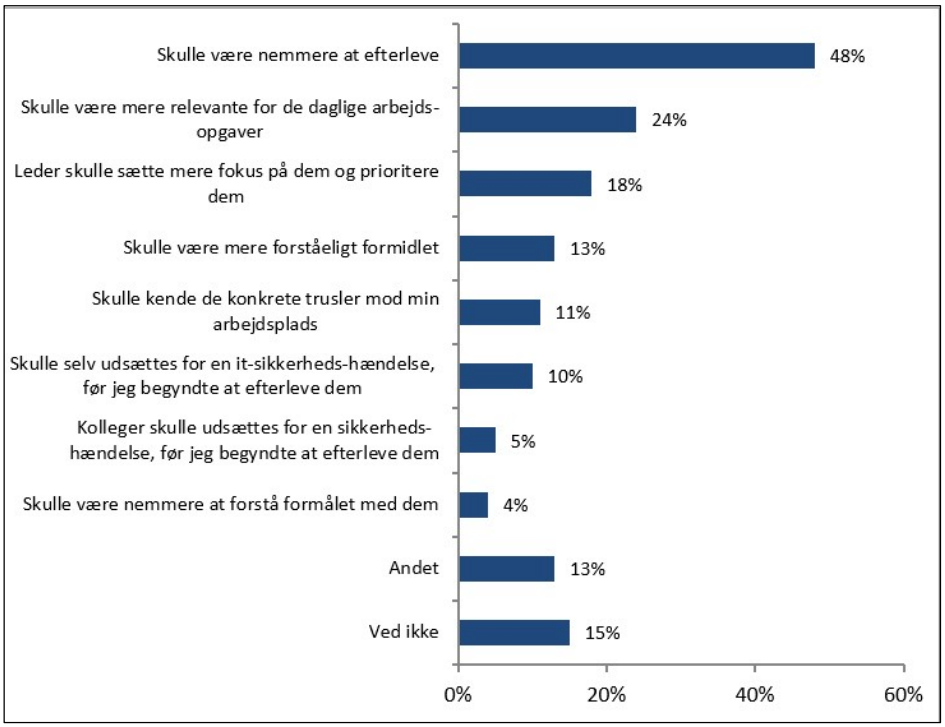
Dette er ligeledes en problematisk observation for arbejdspladserne, fordi det tyder på, at informationssikkerhedspolitikker og -retningslinjer ikke er forankret stærkt nok i organisationerne. Der kan være mange årsager hertil: Politikkerne og retningslinjerne er ukonkrete, de er dårligt formidlet, de besværliggør arbejdet osv., hvilket næste del af analysen vil fokusere på.

I tillæg dertil undersøges også drivere for de offentligt ansattes efterlevelse af informationssikkerhedspolitikker og -retningslinjer. Blandt de offentligt ansatte, der svarer, at de til tider undlader at efterleve arbejdspladsens informationssikkerhedsretningslinjer og -politikker, svarer flest, at det skyldes, at det gør deres daglige arbejde besværligt/umuligt at udføre (61 pct.). 32 pct. angiver, at de selv vurderer, om det er nødvendigt at efterleve i de enkelte arbejdssituationer (figur 47).



Figur 47 Offentligt ansattes grunde til ikke at efterleve informationssikkerhedspolitikker og/eller -retningslinjerne. Det har været muligt at angive op til to svar.

Begge forhold er problematiske for arbejdspladserne. Efterlevelsen af retningslinjerne bør være mulig, uden at det går ud over det daglige arbejde. Mange offentligt ansatte har ikke sikkerhed som en kerneopgave, hvorfor det er problematisk, hvis sikkerhed i sig selv besværliggør/umuliggør deres "rigtige" kerneopgaver, og de dermed potentielt bliver tvunget ud i selv at foretage de nødvendige vurderinger. Det vil nok sjældent blive anset som en legitim årsag ikke at kunne udføre sit arbejde pga. informationssikkerhedsretningslinjerne, hvis man fx arbejder i en hjemmepleje. Dette aspekt af den manglende efterlevelse kan arbejdspladser med fordel undersøge nærmere.



Figur 48 Offentligt ansattes angivelse af, hvad der skulle ændres for, at de oftere ville følge arbejdspladsens informationssikkerhedspolitik og/eller retningslinjer. Det har været muligt at angive op til tre svar.

De offentligt ansatte er også blevet spurgt til, hvad der skulle ændres for, at de oftere ville efterleve arbejdspladsens informationssikkerhedspolitikker og -retningslinjer (figur 48). Næsten halvdelen (48 pct.) oplyser, at det skulle være nemmere at efterleve reglerne, hvilket spejler de angivne barrierer fra figur 46. Yderligere 24 pct. angiver, at retningslinjerne skulle være mere relevante for deres arbejde.

De resterende svar fordeler sig ganske jævnt, og "Andet"-kategorien samt "Ved ikke" er flittigt anvendt. Samme tendens så vi i borgerdelen af analysen, når respondenterne blev spurgt til barrierer og drivere. Igen kan konkluderes, at svarkategorierne enten ikke har været rammende nok, at det varierer pga. individuelle forskelle, og/eller at respondenterne har haft svært ved præcist at

sætte fingeren på, hvad der er afgørende for, at man får en mindre risikobetonet adfærd.

Overvejende er tendensen dog klar, når det kommer til barrierer og drivere for de offentligt ansatte: Det skal være nemmere at agere sikkert, og retningslinjerne skal give mening ift. medarbejdernes arbejdsopgaver. Tidligere i kapitlet var vi inde på, at information om og kendskab til informationssikkerhedspolitikker og -retningslinjer ikke er tilstrækkeligt til, at medarbejderne efterlever retningslinjerne. Dette gør sig stadig gældende. Hvis arbejdspladsen ønsker, at medarbejderne skal have en bestemt adfærd (efterleve retningslinjerne), skal det overvejes, 1) hvordan adfærden kan gøres attraktiv og let at gå til, uden at det går ud over medarbejdernes kerneopgave samt 2) hvad der er det rigtige niveau af sikkerhed for respektive medarbejdergrupper, således at retningslinjerne anses som relevante for den enkelte.

Svarene på disse spørgsmål kan findes flere steder, hvilket altid vil afhænge af den enkelte arbejdsplads' kontekst. Man kan fokusere på, at budskaber om ønsket adfærd kommunikeres handlingsanvisende og på netop det tidspunkt, hvor medarbejderen skal træffe et valg om sin sikkerhedsadfærd. Man kan også som arbejdsplads undersøge muligheder for at sætte tekniske tiltag i værk, som tvinger medarbejderen til at træffe det ønskede valg – det kunne fx gøres ved, at systemer ikke tillader korte kodeord. Endelig kan organisationer overveje, om der kan etableres processer og organisatoriske tiltag, som kan støtte medarbejderne i den adfærd, man ønsker.

9. Ordforklaring

I analysen indgår en række begreber inden for informationssikkerhed. De forklares kort i dette kapitel.

Botnet

En bot (forkortelse af robot) er en computer, som er blevet inficeret med et skadeligt program, der giver angriberen mulighed for at tage kontrollen over computeren. Når det sker, kan en computer udføre opgaver over internettet, uden at computerens ejer ved det. De inficerede computere samles i store netværk, kaldet botnet, der fx kan anvendes af kriminelle til at udføre overbelastningsangreb, såkaldte Distributed Denial of-Service (DDoS) angreb, eller andre skadelige aktiviteter. Et botnet er således et net af pc'er eller andre internetopkoblede enheder (fx overvågningskameraer, alarmer eller andre "smarte" enheder), som uden deres ejeres vidende er overtaget og kan fjernstyres af bagmænd.

CEO-fraud (direktørsvindel)

Ved direktørsvindel (CEO-fraud, også kaldet BEC, Business E-mail Compromise) giver it-kriminelle sig ud for at være en ledende medarbejder i offerets virksomhed. Offeret vil typisk være ansat i bogholderiet eller en anden funktion med adgang til at overføre penge. Bagmændene sender en mail, der ser ud til at komme fra en ledende medarbejder. Vedkommende beder modtageren sørge for hurtigst muligt at overføre et beløb til en ny udenlandsk samarbejdspartner. Hastværket bliver brugt som begrundelse for, at medarbejderen ikke skal bruge tid på at gå gennem de normale kanaler og kontrolprocedurer. Hvis offeret falder for svindlen, får bagmændene de penge, der bliver overført.

Keylogger

En keylogger er en type overvågningssoftware, som bliver brugt til at "optage" tastetryk på en enhed, uden at brugeren er bevidst om det. Data om tastetryk bliver derefter sendt til den person, der har placeret keyloggeren på enheden. Keyloggere kan bruges til at opfange sensitive data såsom kodeord, bankinformation, kreditkortoplysninger eller lign. Keyloggere findes som hardware, der fx sættes ind i en enheds USB-indgang. Eller det findes som software, der installeres på enhederne. Den bedste måde at undgå keyloggere er at have installeret antivirusprogrammer og ikke at åbne dokumenter eller køre programmer fra ukendte kilder. Dertil kommer fysisk adgangskontrol med gæster og andre, der har adgang til enhederne, samt løbende kontrol af, om der sidder ukendte USB-enheder i hardwareenheder.

Kryptering

Kryptering er kodning af information ved hjælp af en digital nøgle. Kun indehaveren af nøglen kan bryde koden og få adgang til at læse informationerne. Ved

asymmetrisk kryptering anvendes to nøgler, en offentlig og en privat nøgle. Hvis man ønsker at sende en krypteret e-mail, skal afsenderen kende modtagerens offentlige nøgle. Afsenderen krypterer beskeden med modtagerens offentlige nøgle. Modtageren dekrypterer den med sin private nøgle. Hvis kommunikationen mellem en browser og et websted er krypteret, begynder web-adressen med HTTPS i stedet for HTTP.

Passwordmanager

En passwordmanager er et program, der opbevarer alle brugerens passwords beskyttet med kryptering. For at få adgang til databasen over passwords skal man indtaste et masterpassword. Derefter kan man kopiere og indsætte passwords i de tjenester, de tilhører. En fordel ved passwordmanagers er, at de letter administrationen af sikre passwords. En ulempe er, at hvis angribere får fat i databasen og knækker masterpasswordet, har de adgang til alle brugerens passwords. De fleste browsere giver mulighed for at gemme brugernavn og kodeord til web-tjenester. Hvis brugeren gør det, og en angriber får fat i vedkommendes computer, kan angriberen benytte de lagrede oplysninger til at få adgang til tjenesterne. I nogle tilfælde beskytter browseren kodeord ved at lagre dem krypteret, eller der kræves et kodeord, som brugeren skal indtaste, før der er adgang til at bruge de lagrede kodeord. Nogle browsere giver mulighed for at synkronisere lagrede kodeord på tværs af enheder. Dermed skal en angriber kun få fat i en enkelt enhed for at få adgang til alle de lagrede kodeord. Lagring af passwords i browseren udgør en sikkerhedsrisiko, der er størst, hvis angriberen får fysisk adgang til enheden.

Password spray-attack

Password spray-attack indebærer, at et system angribes, ved at populære eller lækkede kodeord afprøves på alle konti i et givent system. Er der mange brugere af et system i en organisation, er der en god chance for, at kodeordet giver adgang til systemet. Dette kaldes password spraying. Et spray-attack kan til en vis grad imødegås, hvis systemet er sat op til at lukke konti efter for mange mislykkedes forsøg. Dette kan en angriber imidlertid omgå ved kun at afprøve få passwords ad gangen på hver konto, for at undgå, at kontoen spærres. Til gengæld kan man vende tilbage til den pågældende konto senere og angrebet kan således fortsætte i langsomt tempo over lang tid.

Phishing (via mails, chat eller sms)

Phishing er en form for svindel, hvor svindlerne forsøger at narre fortrolige oplysninger fra offeret. Et typisk phishing-angreb har to komponenter: en indledende besked og et forfalsket websted, der også i sig kan være skadelig ved at udnytte sårbarheder i offerets computer. I den e-mail, chatbesked eller sms, som offeret modtager, forsøger afsenderen at lokke vedkommende til at gå ind på en bestemt webside. I beskeden kan der fx stå, at modtagerens bankkonto er blevet spærret, og at man skal gå ind på websiden og indtaste brugernavn og password for at åbne kontoen igen. Hvis offeret klikker på linket i mailen, vises en webside, der giver sig ud for at være den tjeneste, mailen henviser til. Her er der ind-

tastningsfelter, som offeret kan udfylde med de oplysninger, bagmændene er interesserede i. Hvis offeret falder for svindelnummeret, får uvedkommende adgang til fortrolige oplysninger. Det kan fx være kodeord, betalingskort- eller NemID-oplysninger eller arbejdsrelaterede fortrolige oplysninger.

Ransomware

Ransomware er skadelige programmer, der spærrer for brugerens adgang til data eller systemer. Bagmændene kræver betaling af en løsesum for at give brugeren adgang igen. Ofte krypterer bagmændene offerets data, så man skal betale for at få udleveret den nøgle, der kan dekryptere dem. Der er dog ingen garanti for, at man får sine data tilbage, selv om man betaler, ligesom der også er set eksempler på, at ofrene trues med at få offentliggjort data. I en række nyere tilfælde bevæger de kriminelle sig rundt i netværket hos den organisation, de angriber og forsøger bl.a. at slette eller ødelægge sikkerhedskopierne, inden ransomwaren aktiveres.

Sikkerhedskopiering

For at sikre at data ikke går tabt eller bliver ændret, kan man tage kopier af dem. En sikkerhedskopi kan blandt andet sikre, at offeret kan få adgang til sine data efter et angreb med ransomware eller "almindeligt" nedbrud af enheden. I stedet for at betale løsesummen ved ransomware kan offeret indlæse den seneste sikkerhedskopi. Dermed mister man kun de data, der er dannet, efter sikkerhedskopien blev taget. Af samme grund er det en fordel at tage hyppige sikkerhedskopier. Sikkerhedskopier kan tages på eksterne harddiske eller ved en cloud-løsning, hvor der kører et program på brugerens computer, der løbende kopierer ændrede filer over på en server på internettet. En fordel ved cloud-baseret sikkerhedskopiering er, at kopien altid er opdateret. Det kan dog også være en ulempe: Hvis et ransomware-program krypterer brugerens filer, bliver de krypterede filer straks sikkerhedskopieret. Dermed kan brugeren kun gendanne data, hvis cloud-tjenesten giver mulighed for at lagre data i flere versioner, så en tidligere, ukrypteret version kan gendannes. Det samme gælder, hvis man tager sikkerhedskopi til fx en ekstern harddisk. Den skal afkobles fra systemet, når kopien er taget.

Single sign-on

Single sign-on (SSO) er en teknologi, der lader brugere logge ind på flere systemer baseret på et login i et centralt system - kaldet en identitetstjeneste. SSO-teknologien gør det muligt på en sikker måde at overføre brugerinformation fra identitetstjenesten til de enkelte systemer, uden at brugeren skal logge ind endnu en gang. Hvis dette foregår inden for en organisations egne rammer kaldes det SSO. En fødereret SSO gør det muligt at udnytte en SSO-løsning på tværs af organisatoriske grænser. Fordelene er, at kontrol af identiteten kun skal sket et sted - hos identitetstjenesten - mens de oplysninger, der overføres til de enkelte systemer, kan begrænses til de absolut nødvendige. Derudover er der kun et sted der skal have et sikkert login - identitetstjenesten.

Sniffer

En sniffer er et program eller et stykke udstyr, som bruges til at overvåge data,

som bliver transmitteret over netværket. En sniffer kan både blive brugt til legitimt arbejde fx netværkshåndtering, men kan også bruges til at stjæle information. Uautoriserede sniffere kan være farlige for et netværks sikkerhed, fordi de kan være umulige at spore og kan blive placeret hvor som helst.

Spoofing

Spoofing er en metode for en angriber til at udgive sig for at være en anden, fx ikke-mistænkelig afsender af en besked, sms eller et telefonopkald. Det kan ske, hvis afsenderadressen på en email forfalskes, eller hvis et telefonnummer ændres til at se ud til at komme fra Danmark, hvor det i virkeligheden komme fra udlandet.

Softwareopdatering

Mange angreb udnytter sårbarheder i de programmer, ofrene anvender. En sårbarhed kan fx være en programmeringsfejl, der giver uvedkommende adgang til at køre skadelig software på systemet. Når softwareproducenterne opdager sårbarheder i deres produkter, udsender de opdateringer, der lukker sikkerhedshullerne. Det er derfor afgørende for sikkerheden, at software holdes opdateret. Sårbarheder forsøges ofte massivt udnyttet, så snart de bliver opdaget. Det sker primært i den nærmeste tid efter udsendelse af en opdatering. Det skyldes, at angriberne satser på, der går nogen tid, før brugerne får opdateret deres systemer. Alle moderne styresystemer kan sættes op til at installere opdateringer automatisk, men det samme gælder ikke altid de enkelte programmer. Nogle browsere opdateres automatisk. Automatisk opdatering af styresystemer og applikationer øger sikkerheden, men skal suppleres med manuel opdatering af de programmer, der ikke kan opdateres automatisk.

To-faktor-/multifaktorlogin

To-faktorlogin, også kaldet to-trinslogin, to-faktorsikkerhed, to-faktorautentifikation eller multifaktorautentifikation (MFA), er en metode til at øge sikkerheden ved systemer, der er beskyttet med brugernavn og kodeord. Her suppleres kodeordet med et eller flere ekstra elementer, som brugeren skal anvende for at få adgang. Det kan fx være ved brug af Nøgleapp'en, som det kendes fra NemID: Her skal brugeren først indtaste brugernavn og adgangskode. Derefter skal brugeren autentificere login'et på sin telefon via app'en. Dermed kan hackere ikke misbruge et brugernavn og kodeord, selvom de har fundet frem til dem, hvis de ikke har anden-faktoren – i dette eksempel telefonen. Normalt defineres to-faktor-/multifaktorlogin ved noget du ved (brugernavn/adgangskode) noget du har (fx telefon) og/eller noget du er (dvs. biometri som fx fingeraftryk).

Trådløse netværk

Trådløse netværk sender data som radiobølger. Derfor kan enhver, der er inden for senderens rækkevidde, opsnappe signalerne. Til at beskytte kommunikationen kan man anvende kryptering, der typisk følger standarden WPA2 (Wi-Fi Protected Access). Så er det kun brugere, der har kodeord til netværket, der kan se data på det. Hvis et trådløst netværk kan bruges, uden at man indtaster en adgangskode, er det ikke beskyttet med kryptering. Dermed kan de øvrige brugere

på nettet potentielt se de data, brugeren sender og modtager. Angribere kan fx udføre man-in-the-middle-angreb, hvor alle data fra offerets pc sendes gennem angriberens computer, før de sendes videre. Hvis netværket er beskyttet med en adgangskode, som alle deles om, kan andre brugere på nettet også få adgang til ens data. Man kan beskytte sig mod aflytning på trådløse netværk ved at anvende et VPN.

Virus, malware og andre skadelige programmer

Malware betyder malicious software og er en betegnelse for computerprogrammer, der gør ondsindede, skadelige eller uønskede ting der, hvor de er installeret. Begrebet dækker over alle kategorier af skadelige programmer herunder virus og orme. Programmerne kan fx give adgang til eller slette brugerens data, forhindre adgang til applikationer eller tjenester, eller på anden måde er generende. Virus dækker typisk over skadelige programmer, der spreder sig ved at kopiere sig ind i andre programfiler. Orme er skadelige programmer, der spredes via netværk.

Mange skadelige programmer er trojanske heste, der giver sig ud for at være tilforladelige programmer, men som i virkeligheden er skadelige. Ofte henter den trojanske hest flere skadelige programmer og installerer dem på computeren. Man kan beskytte sig mod skadelige programmer med antivirusprogrammer og ved at holde sin enhed opdateret. Firewalls kan i et vist omfang beskytte mod angreb fra orme.

Vishing (voice phishing, falske telefonhenvendelser)

Svindlere ringer til potentielle ofre og udgiver sig for at være fra fx Nets, politiet, banken eller Styrelsen for patientsikkerhed for at gøre opmærksom på et problem, som borgeren eller virksomheden tror kan være relevant. Formålet med opkaldene er at narre offeret til at afgive følsomme oplysninger, adgangskoder, NemID-nøgle mv. Tidligere var vishing mest kendt som opkald fra personer, der udgav sig for at komme fra Microsofts supportcenter, og som oplyste, at der var sikkerhedsproblemer med offerets computer. I disse tilfælde har formålet været at tillade åbning for fjernstyring af pc'en mhp. at installere skadelig software eller narre oplysninger ud af offeret.

VPN (virtuelt privat netværk)

Et virtuelt privat netværk (VPN) anvender kryptering til at beskytte information, der sendes over internettet. Et VPN kan udgøre en form for tunnel gennem internettet fra brugerens computer til serveren på vedkommendes arbejdsplads. Dermed er man beskyttet mod aflytning, selvom det skulle lykkes angribere at opsnappe de datapakker, der indgår i kommunikationen.

10. Analysens metodetilgang

Ændringer i spørgemåder

Formålet med denne undersøgelse er at afdække borgere og offentligt ansattes viden og adfærd inden for informationssikkerhed. Dermed afdækker undersøgelsen målgruppernes oplevede trusler og oplevede konsekvenser ved at blive ramt af hændelser, deres adfærd i forhold til truslerne og almen, god sikkerhedsadfærd, deres opmærksomhed på digitale trusler samt barrierer og drivere for at have en god sikkerhedsadfærd.

Undersøgelsen om borgere og offentligt ansattes informationssikkerhed er en opfølgning på tidligere undersøgelser gennemført i perioden 2013 til 2018. I år er der sket væsentlige ændringer i en række af spørgsmålenes formulering. Dette for at imødekomme ændringer i trusselsbilledet, for at få mere viden om konsekvenser og målgruppernes adfærd i mødet med specifikke trusler samt for at måle nærmere på de barrierer og drivere, målgrupperne angiver som betydningsfulde, når det kommer til at have den gode sikkerhedsadfærd.

Ændringerne i spørgsmålsdesignet har gjort det muligt at gennemføre andre typer analyser. Til eksempel kan sammenhængen mellem risikobevidsthed, målgruppernes opmærksomhed på cyberkriminalitet samt efterlevelse af de gode råd anskueliggøres. Dermed er en række af spørgsmålene fra tidligere år blevet ændret og andre udgået, hvilket har gjort muligheden for historiske sammenligninger særligt for borgernes vedkommende mindre. I det omfang, det har været muligt, er der trukket paralleller mellem de seneste års undersøgelser og dette års.

Målgruppen

Målgruppen for undersøgelsen har været et repræsentativt udsnit af den danske befolkning i alderen fra 18 til 74 år. For så vidt angår de offentligt ansatte, har målgruppen været et udsnit af offentligt ansatte i alderen 18-74 år – repræsentativt fordelt på sektorer (statslige myndigheder, regioner og kommuner) og arbejdslandsdel.

Indsamlingsmetode

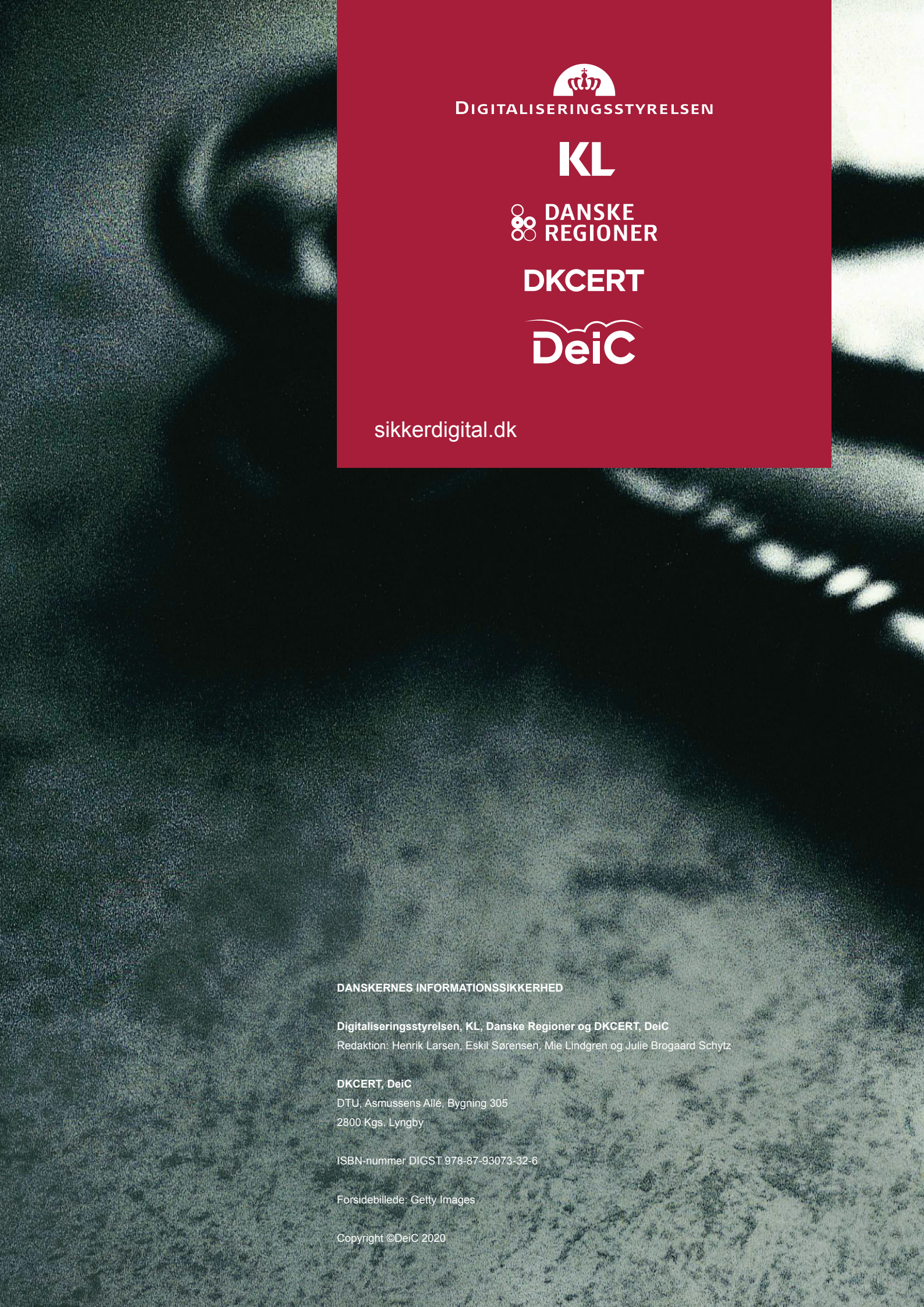
Til undersøgelsen er der taget udgangspunkt i en grundliggende dataindsamlingsmetode, hvor telefon- og webinterview er kombineret.

Dataindsamlingen blev gennemført i perioden d. 29. juni til d. 14. juli 2020.

Der er gennemført 1.029 interview blandt borgere i alderen 18-74 år i den danske befolkning, mens der er gennemført 1.030 interview blandt offentlige ansatte i Danmark.

Resultaterne i nærværende rapport er kommenteret inden for et 95 pct.-signifikansniveau. Dette betyder, at usikkerheden på et måleresultat kan angives ved et usikkerhedsinterval (konfidensinterval), dvs. et interval, der med en sikkerhed på 95 pct. indeholder populationsværdien. I kommenteringen kan der være +/- 1 pct. til forskel i sammenlægningen af resultater i forhold til procenttal, der står i parentes, hvilket skyldes afrundinger. Således kan fx 50 pct. af respondenterne have svaret "I høj grad" og 30 pct. "I meget høj grad". Men i sammenlægningen af de to svarmuligheder kan resultatet fx være 81 pct. grundet afrundinger af tal i parentes – fx fra 50,4 pct. til 50 pct. og fra 30,3 pct. til 30 pct., hvilket i sammenlægningen giver resultatet 80,7 pct. og deraf i hele tal 81 pct.

MEGAFON A/S er ansvarlig for dataindsamlingen, der ligger til grund for analysen, mens Digitaliseringsstyrelsen og DKCERT er ansvarlige for afrapportering og tolkninger i analysen.



DIGITALISERINGSSTYRELSEN

KL

DANSKE REGIONER

DKCERT

DeiC

sikkerdigital.dk

DANSKERNES INFORMATIONSSIKKERHED

Digitaliseringsstyrelsen, KL, Danske Regioner og DKCERT, DeiC
Redaktion: Henrik Larsen, Eskil Sørensen, Mie Lindgren og Julie Brogaard Schytz

DKCERT, DeiC
DTU, Asmussens Allé, Bygning 305
2800 Kgs. Lyngby

ISBN-nummer DIGST 978-87-93073-32-6

Forsidebillede: Getty Images