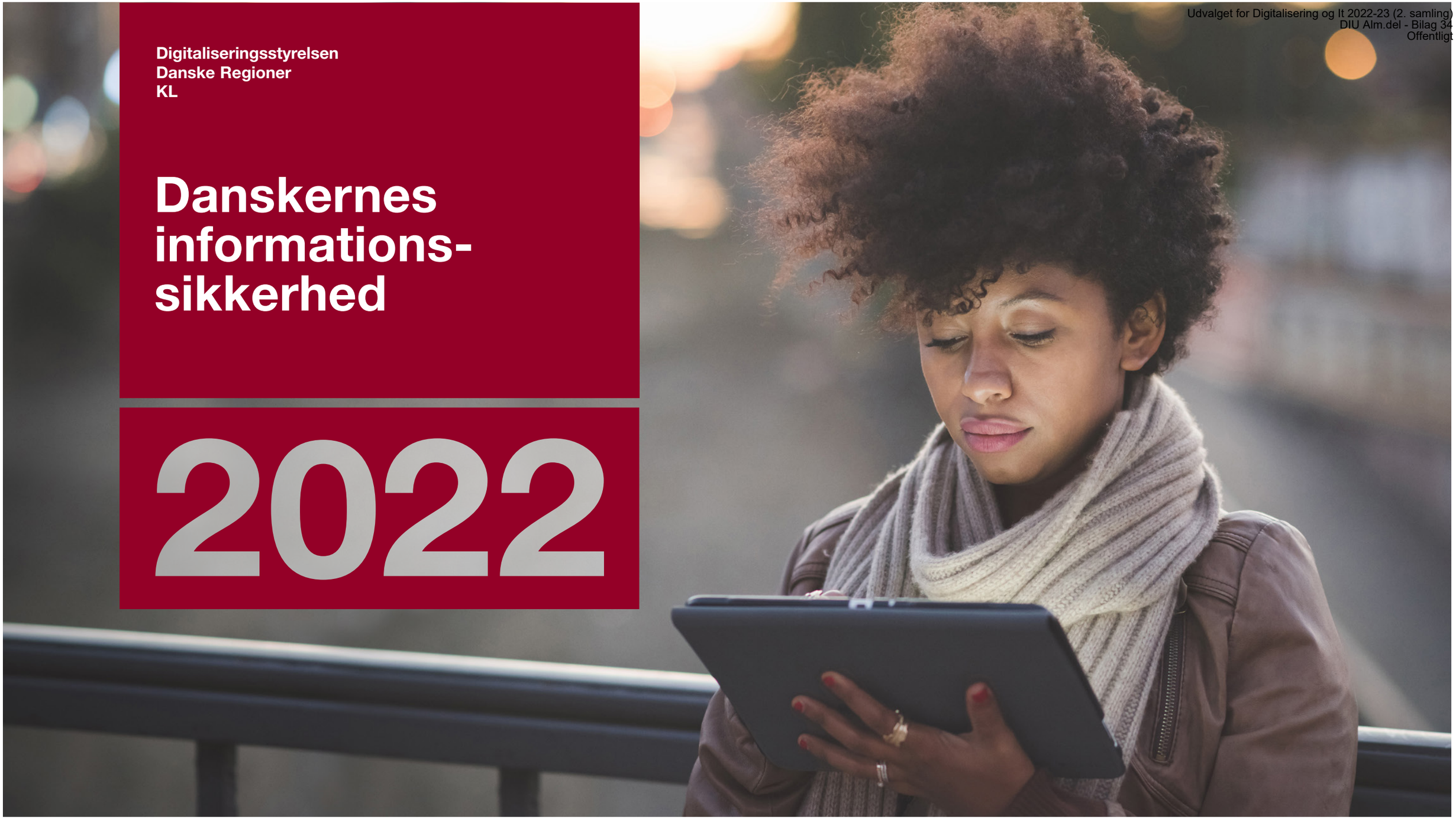
Digitaliseringsstyrelsen
Danske Regioner
KL

Danskernes informations-sikkerhed

2022



Indhold

Perspektiver for digital sikkerhed i Danmark

Danmark er en digital frontløber. Tre gange i træk har FN kåret Danmark til verdensmester i digitalisering. Og danskerne benytter internettet til daglige gøremål som aldrig før.

I takt med den øgede digitalisering af offentlige processer, services og daglige gøremål åbner der sig dog en række mulige angrebsflader.

Derfor er det afgørende, at borgere i det danske samfund kender til de trusler, de kan blive udsat for og har en god sikkerhedsadfærd, når de møder truslerne, så de ikke oplever de voldsomme konsekvenser ved at blive snydt økonomisk, miste alle deres billeder eller få stjålet deres digitale identitet.

Ligeledes er det afgørende, at offentligt ansatte er uddannet og klædt på til at navigere i en hverdag med flere digitale krav og trusler, så de er i stand til at passe på borgere og virksomheders oplysninger.

Et trusselsbillede i forandring

Svindlerne arbejder hårdt og forbedrer sig hele tiden. Derfor ser vi også en konstant udvikling i trusselsbilledet. Investeringssvindel, hvor de kriminelle fx lokker med Bitcoin-muligheder, og øget svindel i handler mellem privatpersoner på nettet er nogle af de trusler, som vi i dette års analyse kan se, er i vækst.

Samtidig kan vi se, at phishing-truslen, hvor svindlere forsøger at lokke oplysninger ud af privatpersoner eller offentligt ansatte, fortsat er den mest udbredte trussel.

Behovet for stærke digitale kompetencer

Nye trusler kræver nye evner, og det er en omfattende og afgørende opgave at kompetenceudvikle borgere og offentligt ansatte. Generelt kan vi i årets analyse se små gradvise forbedringer i borgere og offentligt ansattes daglige sikkerhedsadfærd, når det kommer til fx kodeord, sikkerhedskopiering og håndtering af fortrolig information.

Det tyder altså på, at vi er på vej i den rigtige retning. Men det er et langt sejt træk, og spørgsmålet er, om udviklingen går hurtigt nok til at følge med et trusselsbillede i hastig forandring.

Uddannelse, awareness og adfærdsindsatser virker

Hvor opmærksom man er på risikoen for digitale trusler, i hvilken grad man føler sig rustet til at beskytte sig på nettet, og hvor god en sikkerhedsadfærd, man generelt angiver at have, hænger sammen med, i hvilken grad man har modtaget information eller undervisning om god sikkerhedsadfærd. Det er en af de væsentlige konklusioner i årets analyse.

Det er dermed godt nyt for de mange personer, der dagligt arbejder på at forbedre sikkerhedskulturen i organisationer, eller som ofte hjælper sine egne børn med at være sikre på nettet. Den indsats gør en forskel.

Men en væsentlig konklusion er ligeledes, at en forbedring af sikkerhedsadfærden kræver forskellige indsatser med forskellige budskaber til forskellige målgrupper. Hvor unge angiver, at de mangler tid og overskud til at have en god adfærd, mener ældre, at en manglende god sikkerhedsadfærd skyldes, at de ikke har data, der er interessante for andre.

Der er således masser at tage fat på i styrkelsen af Danmarks digitale sikkerhed!

God læselyst

Tanja Franck Direktør Digitaliseringsstyrelsen	Tommy Kjelsgaard Vicedirektør Danske Regioner	Christian Harsløf Direktør KL

Læsevejledning

Denne analyse bygger på en dataindsamling, som analysebureauet Megafon har gennemført i sommeren 2022 for de fællesoffentlige parter Digitaliseringsstyrelsen, KL og Danske Regioner.

Adfærdsbureauet /KL.7 (en del af Implement Consulting Group) har bidraget med bearbejdning og analyse af rådata. Analysen er udarbejdet som led i den fællesoffentlige digitaliseringsstrategi mellem staten, kommuner og regioner.

Analysen undersøger to forskellige respondentgrupper: Borgere fra 18 år og op samt offentligt ansatte i hhv. stat, kommuner og regioner. I analysen vil der være særskilt fokus på de to respondentgrupper. Se endvidere metodekapitlet sidst i analysen for grundigere indblik i undersøgelsesdesignet.

De fællesoffentlige parter har tidligere udarbejdet analyser vedr. borgernes informationssikkerhed i 2013, 2014, 2015, 2016, 2018 og 2020. De offentligt ansatte indgik også i undersøgelsen i 2016, 2018 og 2020. Enkelte steder i analysen vil det derfor også være muligt at følge udviklingen i borgere og offentligt ansattes informationssikkerhed.

Analysen er henvendt til aktører, der har interesse for at følge udviklingen i informationssikkerhed i Danmark. Analysen kan læses i sin helhed eller benyttes som et opslagsværk.

Analysen er bygget op i to overordnede dele: Én, der omhandler borgerne, og én, der omhandler de offentligt ansatte. Borgerdelen afdækker først de mest aktuelle trusler rettet mod borgerne. Dernæst undersøges status på borgernes daglige sikkerhedsadfærd med udgangspunkt i anbefalinger, der findes på sikkerdigital.dk. Endeligt kaster analysen lys på de barrierer og drivere, der er for at opnå den gode sikkerhedsadfærd samt borgernes digitale kompetencer.

For de offentligt ansatte undersøges til start ligeledes de trusler, der er rettet mod offentligt ansatte. Dernæst undersøges, med udgangspunkt i typiske og gænge informationssikkerhedsretningslinjer, hvad status er på offentligt ansattes daglige sikkerhedsadfærd. Slutteligt undersøges de offentligt ansattes digitale kompetencer og betydningen af uddannelse, awareness og adfærdsindsatser.

1. Borgernes informations-sikkerhed

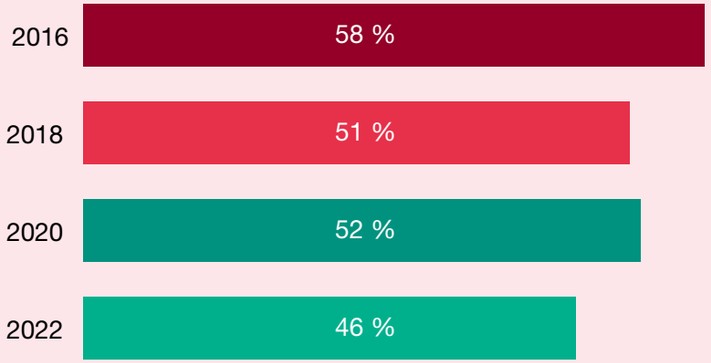
Phishing er den mest udbredte trussel, men få falder i fælden

57%

af borgerne har været udsat for phishing-forsøg enten via mail, sms eller telefonopkald. I 2020 var tallet

64%

Den type phishing-forsøg, som borgerne oftest oplever at blive udsat for, er phishing via mail. Men tallet er faldende.



Anm.: n = 1.006 (2022) og 1.029 (2020). Præcis n for 2016 og 2018 ang. dette spørgsmål kendes ikke. Den samlede stikprøve er dog >1000 personer.

OBS: 2016 og 2018 er dog ikke helt sammenlignelige med tallene fra 2020 og 2022, i det spørgsmålet ved de tidligere undersøgelser ikke var afgrænset til, hvorvidt man havde været udsat for truslen inden for det seneste år.

Hvad er phishing?

Phishing er en form for svindel, hvor svindlerne forsøger at narre personlige oplysninger, som fx kodeord, betalingskortoplysninger eller MitID-oplysninger, fra offeret.

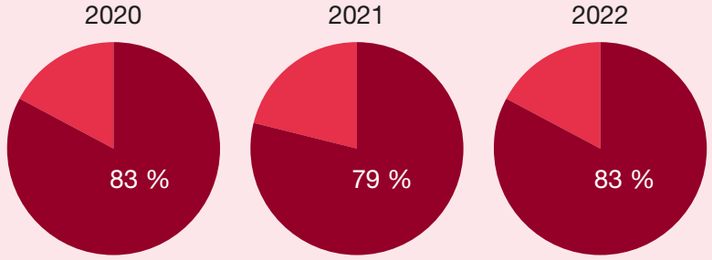
Offeret kan fx blive lokket til at udlevere sine personlige oplysninger på baggrund af en dækhistorie eller blive bedt om at klikke på et link, som fører til en falsk loginside, hvor offeret kan indtaste sine loginoplysninger.

Phishing kan både foregå via mail, sms eller telefonopkald.

Hvis offeret falder for svindelnummeret, kan det få konsekvenser i form af økonomiske tab, identitetstyveri eller tab af data.

At phishing er en udbredt og vedvarende trussel bekræftes, hvis man kigger på data fra app'en Mit Digitale Selvforsvar[1], hvor brugere kan indmelde de forskellige forsøg på digital svindel, de udsættes for, til andre brugeres gavn.

Antallet af anmeldelser relateret til phishing udgør således hovedparten af de samlede indmeldelser om svindel.



Kilde: Dataudtræk fra Mit Digitale selvforsvar, tallene er afrundede

1 Forbrugerrådet Tænk og TrygFonden står bag app'en Mit Digitale Selvforsvar. Det er vigtigt at være opmærksom på, at data ikke kan ses som repræsentativt for den samlede befolkning, da data baserer sig på app'ens brugere og de indmeldelser, de vælger at foretage. Størstedelen af app'ens brugere er mellem 65 og 74 år.

Forsøg på identitetstyveri er svært at gennemskue

Hvad er identitetstyveri?

Identitetstyveri er, når en person uberettiget overtager en andens identitet. Identitetstyveri sker ved, at en person får fat på oplysninger, som kan misbruges til på en andens vegne at optage lån, overføre penge fra netbank eller til at chikanere personen eller andre.

Typisk vil det dreje sig om NemID/MitID-oplysninger, andre kodeord eller CPR-nummer. I forhold til CPR-nummer sker svindlen typisk ved, at uvedkommende har fået fat på det i kombination med andre oplysninger som fx navn og adresse.

Identitetstyveri sker oftest som resultat af et vellykket forsøg på at lokke oplysninger fra borgere via enten mail, sms eller telefonopkald. Det kan være personer, man har en relation til, men vil oftest være personer, som udgiver sig for at være fra en offentlig myndighed eller bank, hvilket kan gøre det svært at gennemskue svindlen.

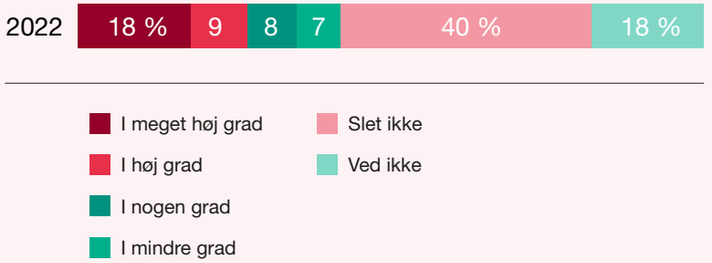
Banker og offentlige myndigheder vil dog aldrig uopfordret bede om personlige oplysninger som fx NemID-/MitID-oplysninger, adgangskoder eller CPR-nummer over mail, SMS eller opkald.

En kreditadvarsel kan gøre det sværere for svindlere at misbruge ens identitet. En kreditadvarsel er en markering i CPR, der sender signal til banker og virksomheder om, at de bør være særligt opmærksomme på, at det faktisk er den pågældende borger de indgår en aftale med, før de yder lån eller kredit. Det kan fx ske gennem ekstra identitetskontrol. En kreditadvarsel kan fx være relevant, hvis borgeren har mistet sit pas eller kørekort og er bekymret for, at det vil blive brugt til identitetsmisbrug.

60 pct. af borgerne har slet ikke mistanke om identitetstyveri. Hvis man frasorterer disse, har kun 27 pct. af de, som har haft mistanke om identitetstyveri, oprettet en kreditadvarsel i deres navn.

I hvilken grad efterlever du følgende anbefaling om kreditadvarsler?

Opret en kreditadvarsel på dit CPR-nummer på borger.dk, hvis du har mistanke om identitetstyveri



Anm.: n = 1.006.

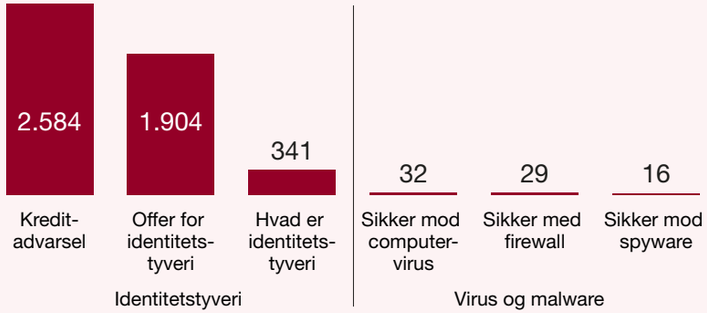
Identitetsmisbrug blev pr. 3. marts 2022 omfattet af straffeloven og blev gjort strafbart med bøde eller fængsel indtil 6 måneder.

Kilde: Folketinget, Lov om ændring af straffeloven (Kriminalisering af identitetsmisbrug), 2022

Tal fra den offentlige hjemmeside borger.dk bekræfter, at identitetstyveri er en trussel, som borgerne i høj grad efterspørger mere viden om.

Under siden "Internet og sikkerhed" er de tre mest besøgte undersider i 2022 således alle relateret til identitetstyveri. Til sammenligning kan ses, hvor relativt få besøgende andre sider relateret til digital sikkerhed havde i samme periode.

Gennemsnitlige månedlige besøgstal for undersider relateret til identitetstyveri samt virus og malware på siden "Internet-og-sikkerhed" på borger.dk, 2022



Kilde: borger.dk.

Borgere, der har mistanke om, eller har været udsat for, identitetstyveri, kan ringe til Hotline ved identitetstyveri og få hjælp.

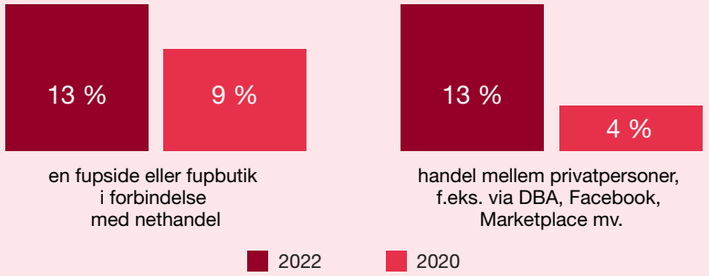
Hotlinen har døgnåbent alle årets dage.

Ring 33 98 00 98

Flere bliver udsat for (forsøg på) svindel i forbindelse med nethandel

Flere bliver udsat for forsøg på svindel via enten fupside/fupbutik eller samhandel mellem privatpersoner end tidligere år. Især svindel i forbindelse med handel mellem personer er steget markant[2].

Andelen af borgere, som inden for det seneste år har været udsat for svindel eller forsøg på svindel via hhv.:

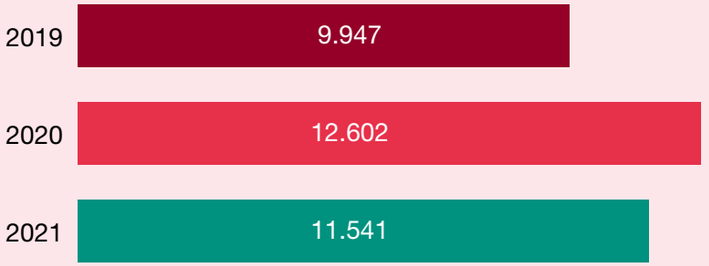


Anm.: n = 1.006 (2022) og 1.029 (2020).

Det skal dog bemærkes, at spørgemåden i de to undersøgelser ikke er fuldkommen identiske, og at dette kan forklare (noget af) stigningen. I 2022-undersøgelsen er det eksplicitet, at der både spørges ind til svindel og forsøg på svindel, mens dette ikke på samme måde er tilfældet i 2020-undersøgelsen.

Udviklingen bekræftes hos Politiets Nationale Center for IT-Kriminalitet (NCIK). De har oplevet en stigning i antallet af samhandelssager i de seneste år. Selvom anmeldelsestallene faldt en smule fra 2020 til 2021, tyder udviklingen fra 2019-2021 på, at det er et område i vækst.

Anmeldelsestal på samhandelsområdet



Kilde: NCIK årsrapport 2021

Samtidig udgør anmeldelser om svindel ifm. samhandel 43,4 pct. af alle anmeldelser til NCIK.

Hvad er nethandelssvindel?

Svindel i forbindelse med nethandel kan være relateret til falske netbutikker, der til forveksling ligner rigtige netbutikker, men som franarrer den handlende penge eller oplysninger. Nethandelssvindel dækker også over svindel mellem privatpersoner (samhandelssvindel), når man køber eller sælger brugte varer via fx DBA.

Blandt de borgere, som inden for det seneste år har været udsat for forsøg på svindel i forbindelse med nethandel, angiver 17 pct., at svindlen lykkedes. Typisk er konsekvensen ved svindel økonomisk tab, eller at varen aldrig bliver tilsendt, hvilket som udgangspunkt ikke er relateret til NemID/MitID.

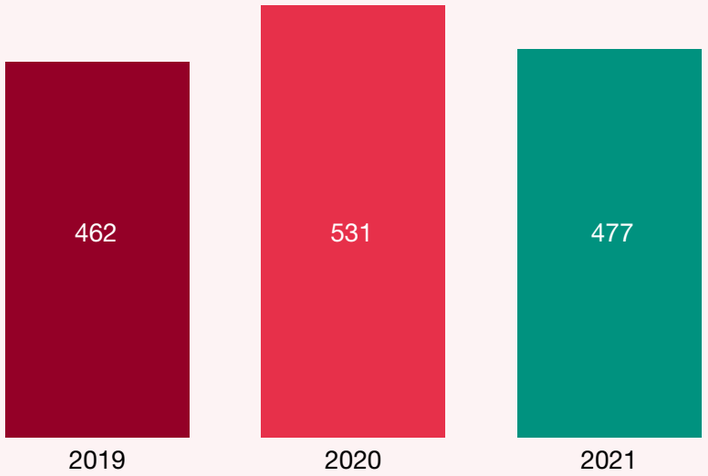
2 Tallene skal ses i lyset af, at nethandlen generelt er vokset de seneste par år jf. Danmarks Statistiks statistikbank om køb via internet inden for de sidste tre måneder (BEBRIT07).

Ældre udsættes oftest for forsøg på investeringssvindel

Der ses over de senere år et konstant antal anmeldelser om falske låne- eller investeringsmuligheder. Langt størstedelen af de anmeldelser om fuphjemmesider, som NCIK modtager, omhandler falske låne- eller investeringsmuligheder.

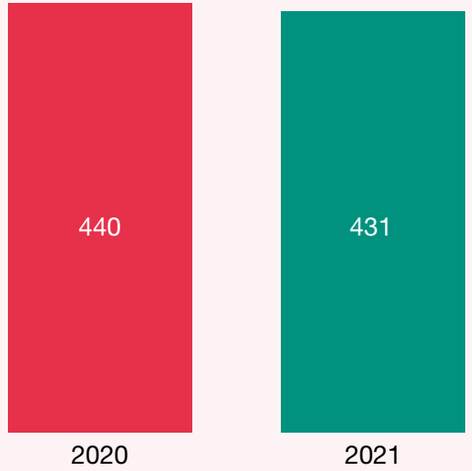
Antallet af anmeldelser voksede særligt fra 2019 til 2020, og selvom antallet af anmeldelser om fuphjemmesider faldt fra 2020 til 2021, forblev antallet af anmeldelser om falske låne- eller investeringsmuligheder på samme niveau.

Antal anmeldelser omhandlende fuphjemmesider modtaget hos NCIK, 2019-2021



Kilde: NCIK årsrapport 2021

Antal anmeldelser omhandlende falske låne- og investeringsmuligheder modtaget hos NCIK, 2019-2021



Kilde: NCIK årsrapport 2021

Hvad er investeringssvindel?

Investeringssvindel er en form for svindel, hvor den kriminelle lokker offeret med mulighed for økonomisk gevinst ved at købe fx aktier eller kryptovaluta (fx Bitcoins).

Offeret kontaktes typisk via sociale medier og hjemmesider og efterfølgende telefonisk af en person, som udgiver sig for at være investor eller investeringsrådgiver.

I nogle sager har offeret opdaget, at vedkommende er blevet svindlet, men de kriminelle genoptager kontakten og udgiver sig for at være advokater eller lignende, som kan hjælpe med at få det tabte beløb tilbage[3].

22%

af borgerne har inden for det seneste år været udsat for investeringssvindel eller forsøg på investerings-svindel en eller flere gange.

Ældre bliver oftere udsat for denne type svindel end yngre borgere. Blandt de 60+-årige er det 29 pct., der har været udsat for forsøg på investeringssvindel inden for det seneste år. Blandt de 18-29-årige er det 16 pct.

3 Kilde: NCIK årsrapport 2021

Borgerne er blevet bedre til kodeord

Borgerne er generelt blevet bedre til at efterleve anbefalingerne om kodeord sammenlignet med tidligere år.

Hvorfor er et stærkt kodeord vigtigt?

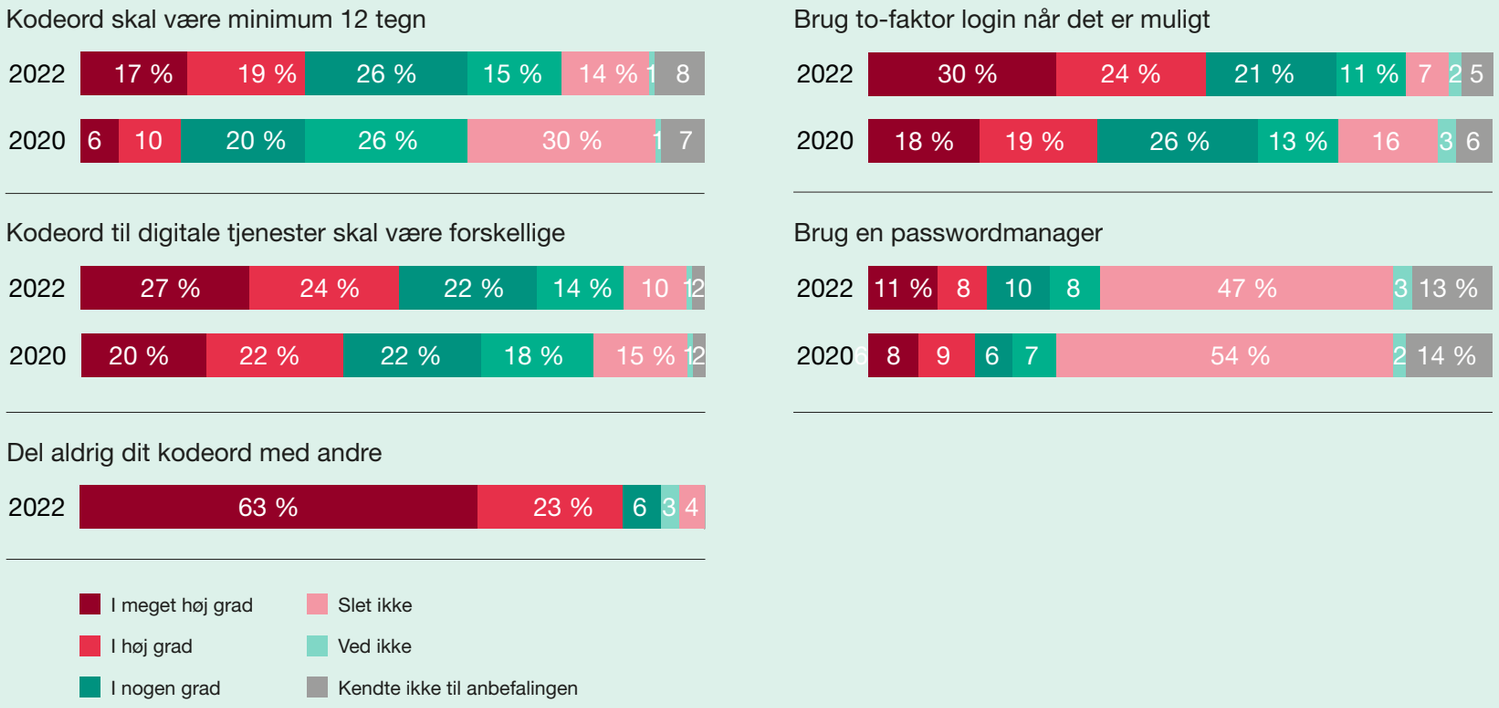
Kodeord er vigtige, fordi de er nøglen til at få adgang til data, uanset om det er data på en telefon, en profil på et socialt medie eller en bankkonto. Et stærkt kodeord er minimum 12 tegn og genbruges ikke flere steder.

Jo flere tegn et kodeord består af, desto flere kombinationer af tegn skal en svindler igennem for at ramme rigtigt, hvis de vil prøve sig frem. Lige så vel undgås det, at svindleren har adgang til mange af ens tjenester og oplysninger, hvis man undgår at genbruge sit kodeord flere steder.

Borgerne angiver i højere grad end tidligere år, at deres kodeord til digitale tjenester er forskellige. Der ses en stigning fra 2020 til 2022, og vi har undersøgt udviklingen siden 2014.

Borgerne er blevet bedre til at benytte sig af to-faktor login, når det er muligt. Der ses en markant stigning fra 2020 til 2022.

I hvilken grad efterlever du følgende anbefalinger om kodeord?



Anm.: n = 1.006 (2022) og 1.029 (2020).

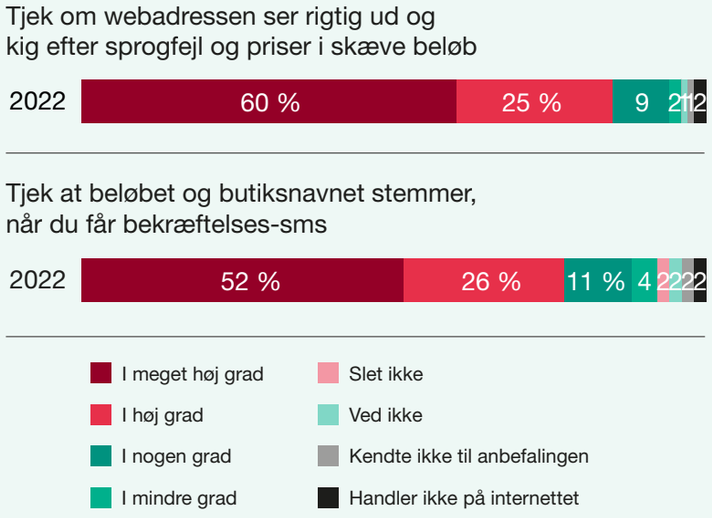
Borgerne har styr på sikker digital handel med virksomheder

Langt de fleste angiver, at de i høj eller meget høj grad efterlever anbefalingerne om sikker nethandel.

85 pct. af borgerne siger, at de i høj eller meget høj grad efterlever anbefalingen om at tjekke, at web-adressen ser rigtig ud, og kigge efter sprogfejl samt priser i skæve beløb, og 78 pct. siger, at de i høj eller meget høj grad efterlever anbefalingen om at tjekke, at beløbet og butiksnavnet stemmer, når de får en bekræftelses-SMS.

Frasorterer man de borgere, som slet ikke handler på nettet, er det hhv. 87 og 79 pct.

I hvilken grad efterlever du de følgende anbefalinger om handel på internettet med virksomheder?



Anm.: n = 1.006 (2022)

Vanskeligt at efterleve anbefalinger om sikker handel mellem privatpersoner

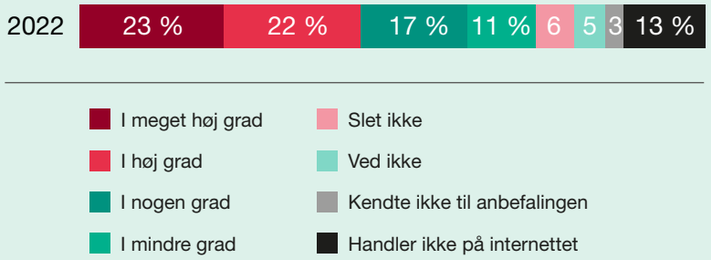
Hvor borgerne i høj grad efterlever rådene til sikker net-handel er billedet mere broget, når det kommer til borgernes sikkerhedsadfærd i forbindelse med digital handel mellem privatpersoner. Det vil sige en handel, der er startet på en digital platform, selvom den efterfølgende måtte rykke ud i den analoge verden.

Som tidligere beskrevet, udgør anmeldelser til politiet om svindel ifm. samhandel den langt største andel af det samlede antal anmeldelser (43,4 pct.).

Sammenholdt med, at borgerne, relativt til fx efterlevelsen af gode råd til handel med virksomheder, angiver at have en lav efterlevelse af anbefalingerne til sikker samhandel, er det et område med plads til forbedring. Svindlerne lader til at udnytte den manglende sikkerhedsadfærd på sam-handelsområdet.

I hvilken grad efterlever du følgende anbefaling om digital handel mellem privatpersoner?

Mød så vidt muligt sælger eller køber ansigt til ansigt og tjek om varen sælges væsentligt billigere end hos andre



Anm.: n = 1.006.

Når svindlerne skal lokke købere i fælden i en handel mellem privat-personer, foretrækker de varer med mange interesserede købere, så de er sikre på en hurtig gevinst. Ifølge politiets opgørelser optræder en række varekategorier ofte i anmeldelserne:

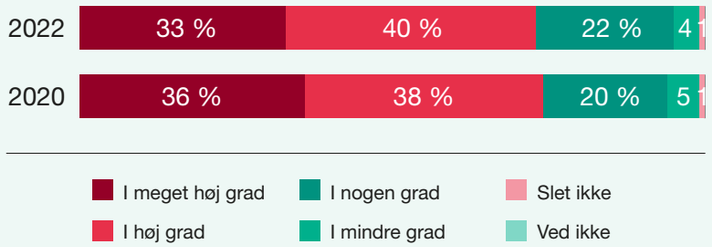
- Elektronik, fx mobiltelefoner og spillekonsoller (33 pct.)
- Tøj, tasker og tilbehør (11 pct.)
- Billetter, fx til koncerter eller festivaler (7 pct.)

Kilde: LCIK, It-relateret økonomisk kriminalitet, 2019

Opmærksomme borgere har den sikreste adfærd

73 pct. angiver, at de i meget høj eller høj grad er opmærksomme på risikoen for bedrageri og cyberkriminalitet på internettet. Det svarer til niveauet i 2020.

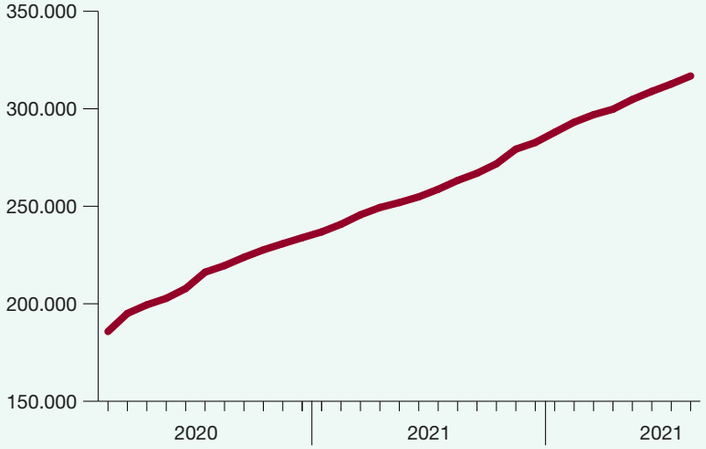
I hvilken grad er du opmærksom på risikoen for bedrageri og cyberkriminalitet på internettet?



Anm.: n = 1.006 (2022) og 1.029 (2020).

Data fra app'en Mit Digitale Selvforsvar[4] viser, at der er sket en jævn, konstant stigning i antallet downloads af app'en over de seneste par år. Det kunne således tyde på, at digital sikkerhed i stigende grad er et emne, som borgere er opmærksomme på og gerne vil gøre noget aktivt for at forbedre.

Downloads over tid



Kilde: Dataudtræk fra Mit Digitale selvforsvar

Ældre borgere angiver at være mere opmærksomme på trusler på nettet end de yngre borgere. Hvor 62 pct. af de 18-29-årige angiver, at de i meget høj grad elleri høj grad er opmærksomme, gælder det 77 pct. af de 60+-årige.

Kodeord:

••••••••• **89%**

af dem, som svarer, at de i høj elle i meget høj grad er opmærksomme på risikoen for trusler på nettet, efterlever i høj eller meget høj grad anbefalingen om aldrig at dele sit kodeord med andre. Modsat gælder det kun 62 pct. af dem, som svarer at de i mindre grad eller slet ikke er opmærksomme.

4 Forbrugerrådet Tænk og TrygFonden står bag app'en Mit Digitale Selvforsvar. Det er vigtigt at være opmærksom på, at data ikke kan ses som repræsentativt for den samlede befolkning, da data baserer sig på app'ens brugere og de indmeldelser, de vælger at foretage. Størstedelen af app'ens brugere er mellem 65 og 74 år.

Ældre borgere er mere bekymrede for bedrageri og cyberkriminalitet på internettet end yngre

28 pct. af borgerne angiver, at de i høj eller meget høj grad er bekymrede for at blive udsat for bedrageri og cyberkriminalitet på internettet. En lige så stor andel (29 pct.) angiver, at de i mindre grad eller slet ikke er bekymrede.

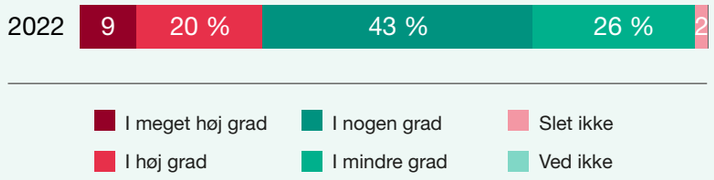
Borgere med stor tillid til egen sikkerhed er mindre bekymrede for cyberkriminalitet

Borgere der føler sig godt klædt på i forhold til at beskytte sig mod bedrageri og cyberkriminalitet er også mindre bekymrede for at blive udsat herfor.

Således er det kun 27 pct. af dem, som føler sig godt eller meget godt klædt på, som i høj grad eller i meget høj grad også er bekymrede for at blive udsat for bedrageri og cyberkriminalitet. Omvendt gælder det hele 41 pct. af dem, som føler sig dårligt eller meget dårligt klædt på.

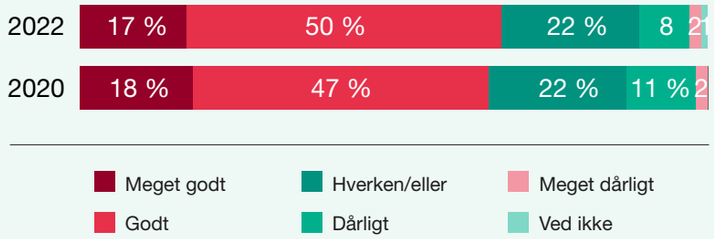
34 pct. af de 60+-årige angiver, at de i meget høj eller høj grad er bekymrede for at blive udsat for bedrageri og cyberkriminalitet på internettet, mens det kun er tilfældet for 20 pct. af de 18-29-årige.

I hvilken grad er du bekymret for at blive udsat for bedrageri og cyberkriminalitet på internettet?



Anm.: n = 1.006.

Føler du dig godt eller dårligt klædt på i forhold til at beskytte dig mod bedrageri og cyberkriminalitet på internettet?



Anm.: n = 1.006 (2022) og 1.029 (2020).

Forskellige aldersgrupper kalder på forskellige adfærdsgreb

Respondenter, der ikke eller kun i mindre grad efterlever anbefalingerne om sikker adfærd er blevet spurgt til årsagen til dette. Der tegner sig et broget billede.

Forskellige greb til forskellige aldersgrupper

Der tegner sig dog nogle mønstre, når vi ser på borgernes besvarelser fordelt på deres alder.

De unge svarer i højere grad, at de ikke har tid eller overskud til at sætte sig ind i anbefalingerne. 34 pct. af de 18-29-årige angiver dette som årsag, mens det kun er tilfældet for 19 pct. af borgerne på 40 år eller derover.

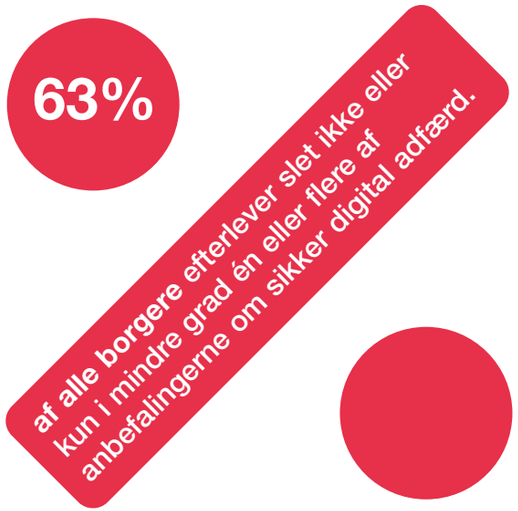
Omvendt svarer de ældre i højere grad, at de efter deres mening ikke har data, der er interessante for andre. 28 pct. af de 60+-årige angiver dette som årsag, mens det kun er tilfældet for 19 pct. af borgerne mellem 18 og 59 år.

Samlet viser det, at der er behov for en flerstrenget indsats for at forbedre borgernes digitale adfærd. Hvor der for de unge kan fokuseres på at gøre anbefalinger mindre krævende, kan der for de ældre sættes fokus på betydningen og vigtigheden af data.

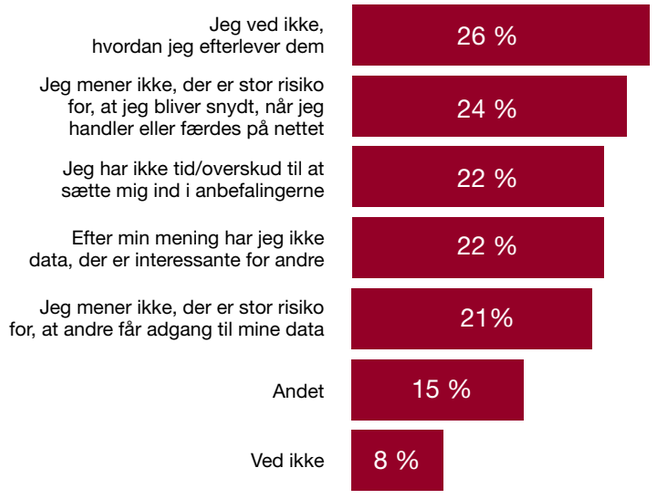
Hvordan kan man arbejde effektivt med adfærdsændringer?

Et hurtigt blik på gængs adfærdsteori[5] peger ligeledes på, at der er særligt tre greb, der er vigtige for at opnå en høj efterlevelse. Den rette adfærd skal være:

- LET – antallet af anbefalinger skal forsimples
- PÅMINDENDE – påmindelser på det tidspunkt, hvor der udføres handlinger relateret til sikkerhed
- TILGÆNGELIG – informationen skal være kendt og tilgængelig



Du har svaret, at du i mindre grad eller slet ikke efterlever nogle af anbefalingerne om sikker digital adfærd. Hvad er årsagen til det? Du kan angive flere svar



Anm.: n = 637.

5 OECD's The BASIC Toolkit; Kahneman: Thinking, fast and slow

Borgere, der får viden fra offentlige hjemmesider, har den bedste adfærd

I løbet af de seneste to år er der sket et fald i andelen af borgere, som får deres viden om digital sikkerhed fra deres omgangskreds og deres arbejdsplads eller uddannelses-institution. Til gengæld er der flere borgere, som i dag får deres viden fra offentlige myndigheders hjemmesider.

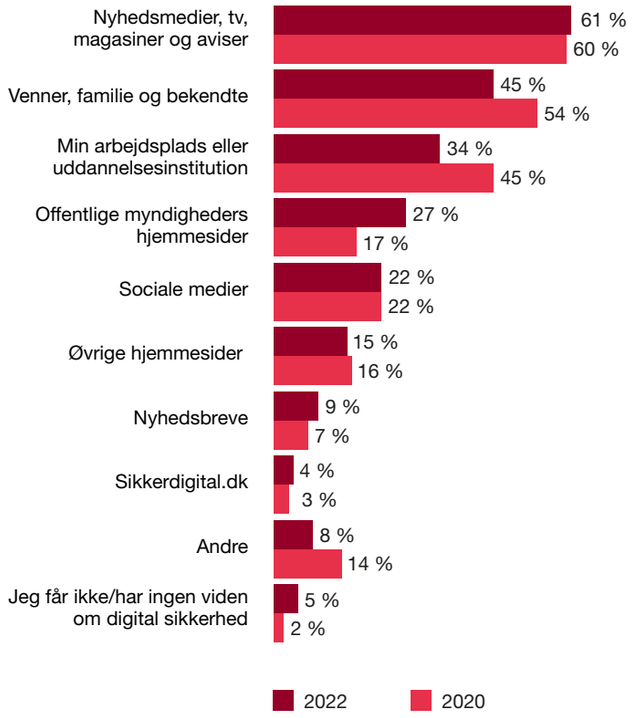
Denne udvikling bekræftes i besøgstallene fra sikkerdigital.dk[6]

Borgere, der angiver at få deres viden om digital sikkerhed fra sikkerdigital.dk, efterlever i højere grad anbefalingerne om sikker digital adfærd.
Eksempelvis efterlever

44%

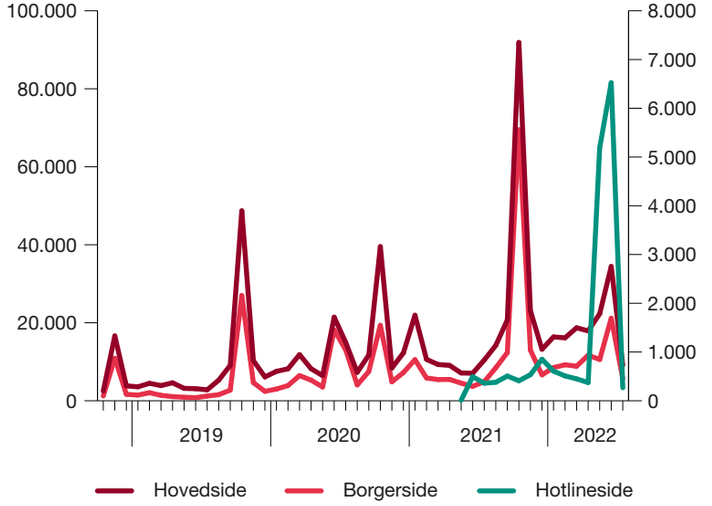
i høj eller meget høj grad anbefalingen om at bruge en passwordmanager.

Hvor får du din viden om digital sikkerhed fra?
Du kan angive op til 3 svar



Anm.: n = 1.006 (2022) og 1.029 (2020).

Antal besøgende på sikkerdigital.dk, opgjort på månedlig basis, 2018-2022



Anm.: Besøgstallene er opgjort som overordnede besøgstal i alt (dvs. ikke unikke antal besøgende). Antallet af besøgende på hovedsiden (mørkerød) og borgersiden (rød) aflæses på venstre akse. Antallet af besøgende på hotlinesiden (grøn) aflæses på højre akse.

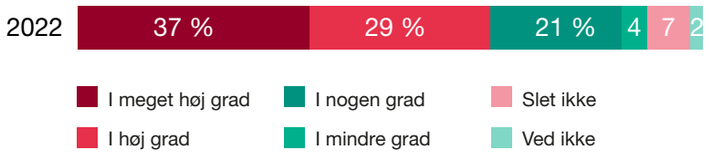
Kilde: sikkerdigital.dk.

6 Digitaliseringsstyrelsen og Erhvervsstyrelsen står bag sikkerdigital.dk, hvor borgere, virksomheder og myndigheder kan få hjælp til en sikker digital hverdag.

Voksnes kompetencer smitter af på deres børn

Blandt de borgere, der bor i samme husstand med et eller flere børn i alderen 5 til 17 år angiver 66 pct., at de i høj eller meget høj grad hjælper deres barn/børn med sikker adfærd på nettet.

I hvilken grad hjælper du eller en anden voksen i husstanden med, at barnet/børnene i husstanden lærer sikker adfærd på nettet (f.eks. at passe på personlige oplysninger og adgangskoder eller spotte digital svindel)?



Anm.: n = 169.

Blandt borgere, som føler sig godt eller meget godt klædt på til at beskytte sig mod bedrageri og cyberkriminalitet, svarer 73 pct., at de i høj eller meget høj grad hjælper barnet/børnene i husstanden med at lære sikker adfærd på nettet. Blandt dem, som føler sig dårligt eller meget dårligt klædt på, gælder det kun 40 pct.

15%

angiver, at digital sikkerhed i høj eller meget høj grad er ...

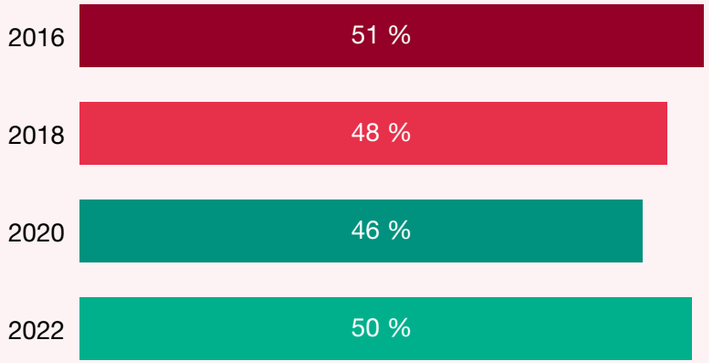
... et samtaleemne blandt deres familie og venner.

2.
Offentligt ansattes informations-sikkerhed

Offentligt ansatte er opmærksomme på truslen fra phishing

Ligesom det er tilfældet blandt borgere, er phishing den digitale trussel, som offentligt ansatte oftest møder, og det lader til at være en vedvarende trussel.

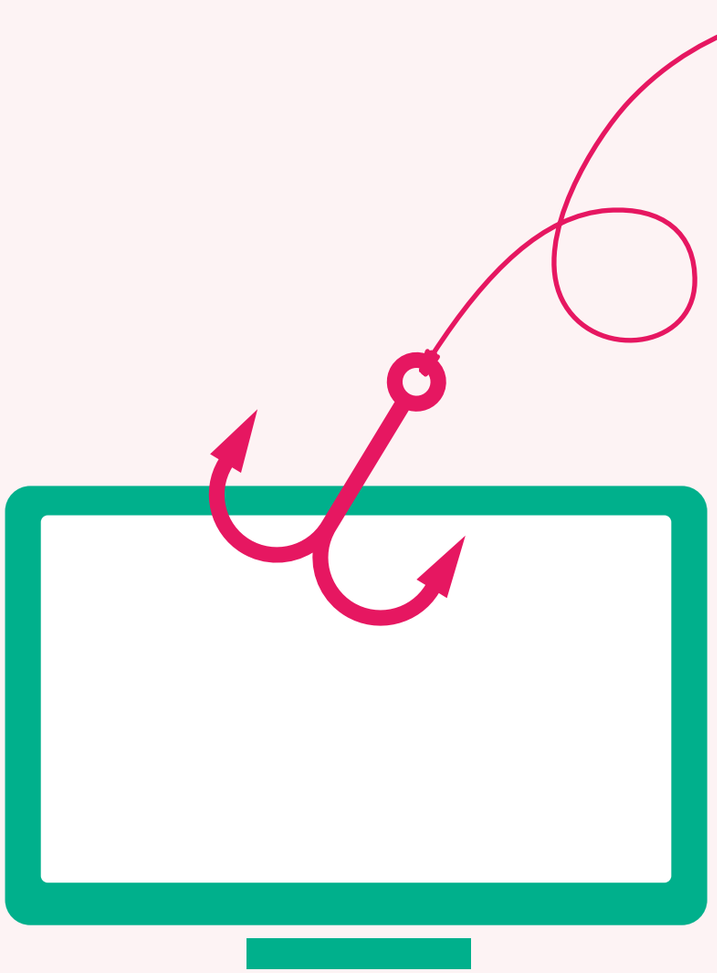
Har du inden for det seneste år på en computer, tablet eller smartphone, som du bruger i forbindelse med dit arbejde, modtaget en mail, sms eller chat-besked fra en ukendt person med et link, som afsenderen opfordrede dig til at klikke på?



Anm.: n = 1.030 (2022) og 1.030 (2020). Præcis n for 2016 og 2018 ang. dette spørgsmål kendes ikke. Den samlede stikprøve er dog >1000 personer.

OBS: 2016 og 2018 er dog ikke helt sammenlignelige med tallene fra 2020 og 2022, i det spørgsmålet ved de tidligere undersøgelser ikke var afgrænset til, hvorvidt man havde været udsat for truslen inden for det seneste år.

Kun 1 pct. af de offentligt ansatte oplyser, at de klikker på links, overfører penge eller indtaster de fortrolige oplysninger, som svindleren efterspørger.



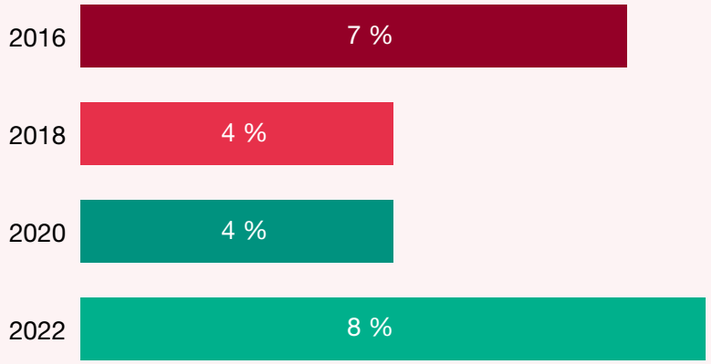
Stigende trussel fra CEO-fraud

Der er sket en fordobling i antallet af offentligt ansatte, som er blevet forsøgt svindlet via CEO-fraud, om end truslen stadig er på et relativt lavt niveau. I 2022 har 8 pct. af de offentligt ansatte oplevet truslen sammenlignet med 4 pct. i 2020.

Hvad er CEO-fraud?

Ved CEO-fraud modtageren medarbejderen en mail, sms eller chat, hvor afsenderen giver sig ud for at være en kollega eller leder på arbejdspladsen. Medarbejderen vil typisk være ansat i en funktion med adgang til at overføre penge. Svindleren beder vedkommende om at overføre penge til en ekstern part. Typisk vil svindleren forsøge at stresse medarbejderen til ikke at bruge tid på at gå gennem de normale kanaler og kontrolprocedurer ved pengeoverførsel. Svindleren modtager i sidste ende de overførte penge.

Har du inden for det seneste år på en computer, tablet eller smartphone, som du bruger i forbindelse med dit arbejde, modtaget en mail, sms eller chat-besked, hvor afsenderen gav sig ud for at være en kollega eller leder på din arbejdsplads, der bad dig overføre penge til en ekstern part?



Anm.: n = 1.030 (2022) og 1.030 (2020). Præcis n for 2016 og 2018 ang. dette spørgsmål kendes ikke. Den samlede stikprøve er dog >1000 personer.

Statsligt ansatte udsættes oftere for phishingforsøg end regionale og kommunale medarbejdere: 63 pct. har en eller flere gange modtaget en besked fra en ukendt person, hvori de opfordres til at klikke på et link, hvorimod det kun er 46 pct. af de kommunale medarbejdere og 34 pct. af de regionale medarbejdere.

Kodeordssikkerheden halter for medarbejdere

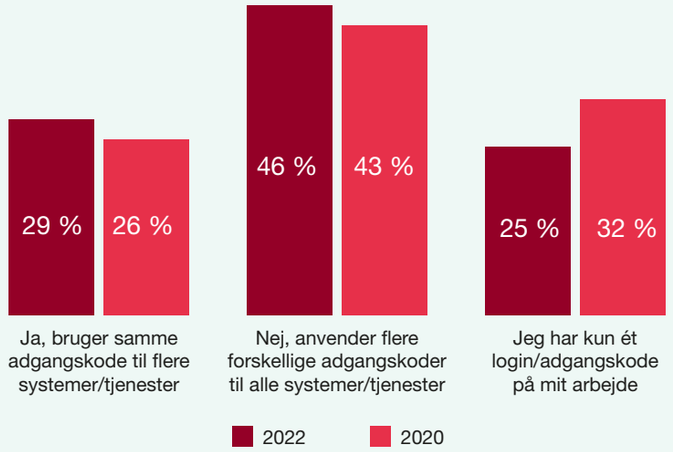
29 pct. bruger samme adgangskode til flere systemer eller tjenester, som de anvender i forbindelse med deres arbejde. Det er omtrent lige så mange som i 2020, men lavere end i perioden 2016-2018, hvor omfanget lå mellem 33 og 37 pct.

20 pct. oplyser, at de bruger samme adgangskoder på deres arbejde som i deres privatliv. Hvis hackeren har fået adgang til et privat kodeord, sættes arbejdspladsen dermed i øget risiko.

Usikre kodeord udnyttes af svindlere

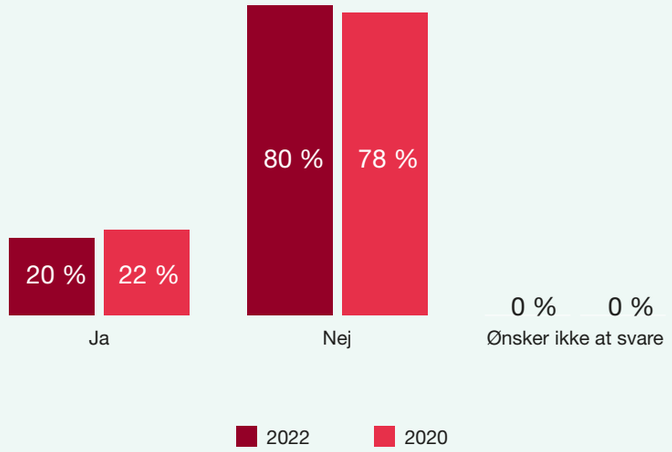
Kodeord er i høj kurs hos hackere. Det er en ofte anvendt og succesfuld angrebsmetode til at skaffe sig uautoriseret adgang til offentlige og private virksomheders kritiske informationer. Kodeord er i mange tilfælde nemme at få fat i og at bryde. Derfor er angrebsmetoden uhyre effektiv[7].

Bruger du samme adgangskode til flere af de systemer/tjenester, du bruger i dit job?



Anm.: n = 1.030 (2022) og 1.030 (2020).

Bruger du samme adgangskoder på dit arbejde, som du bruger i dit privatliv?



Anm.: n = 1.030 (2022) og 1.030 (2020).

7 Center for Cybersikkerhed, Passwordsikkerhed, 2020

Flere myndigheder vælger ”sikker print”

Sikker håndtering af fortrolige oplysninger

Korrekt håndtering af informationer er afgørende for, at borgere og virksomheder har tillid til myndigheder. Derfor er god adfærd i forbindelse med håndtering af oplysninger afgørende for myndigheders virke.

”Sikker print” er en løsning, hvor man skal bruge sit adgangskort eller taste en kode for at få lov at printe. Det kan minimere fejlprint, hvor fortrolige oplysninger som fx forretningskritiske informationer eller oplysninger om borgere bliver sendt til forkerte printere og bliver efterladt.

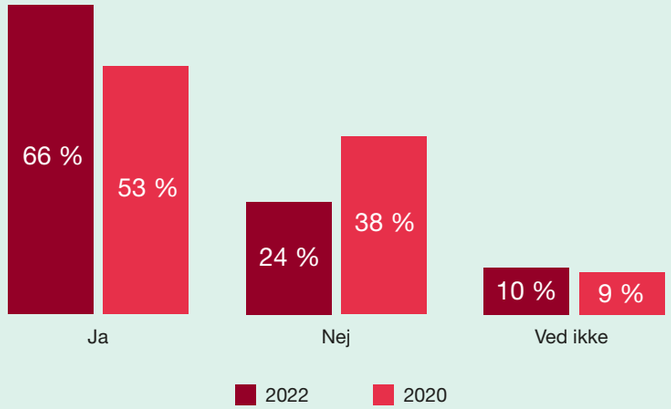
87%

låser ofte eller altid computeren, før den forlades.

En anden konkret metode til at undgå, at uvedkommende får adgang til oplysninger, er ved at låse sin computer, når den forlades, så der skal indtastes en kode for at låse den op.

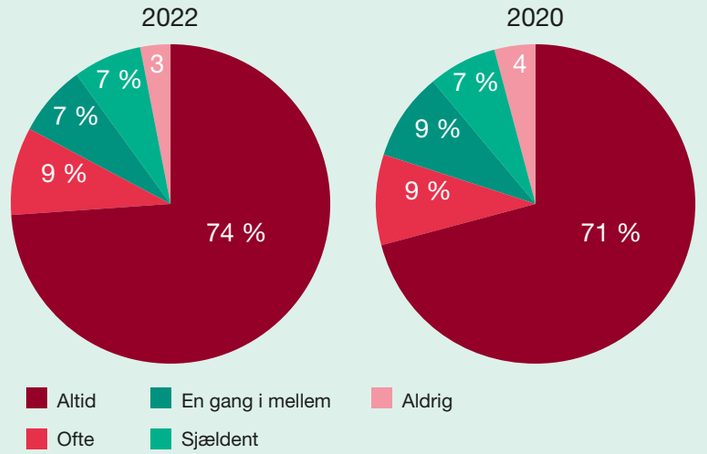
66 pct. angiver, at deres arbejdsplads har en ”sikker print”-løsning. Et stigende antal medarbejdere benytter også løsningen.

Har din arbejdsplads en ”Sikker print”-løsning?



Anm.: n = 1.030 (2022) og 1.030 (2020).

Hvor ofte gør du brug af ”Sikker print”-løsningen?



Anm.: n = 676 (2022) og 549 (2020).

Fejlplacerede oplysninger håndteres i stigende grad korrekt

Selvom de færreste offentligt ansatte (2 pct.) angiver, at de har prøvet at miste arbejdsrelaterede fortrolige oplysninger, så er der relativt mange, som har prøvet at finde dokumenter med arbejdsrelaterede fortrolige oplysninger, der var placeret et forkert sted. Således angiver 24 pct., at det er tilfældet.

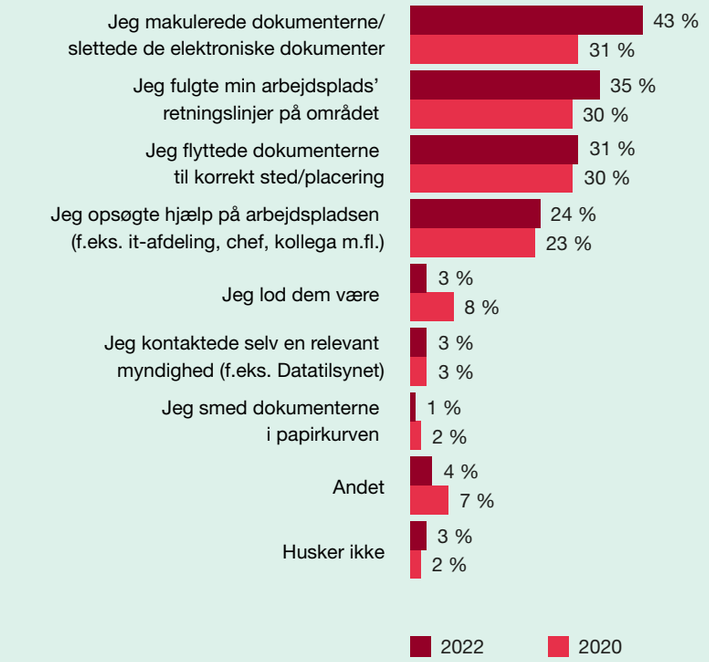
Dog angiver flere end tidligere, at de håndterede de fejlplacerede oplysninger på en hensigtsmæssig måde.

43 pct. angiver således, at de makulerede dokumenterne eller slettede de elektroniske dokumenter, efter de fandt dem på forkert sted. Det er flere end for to år siden, hvor 31 pct. gjorde det samme.

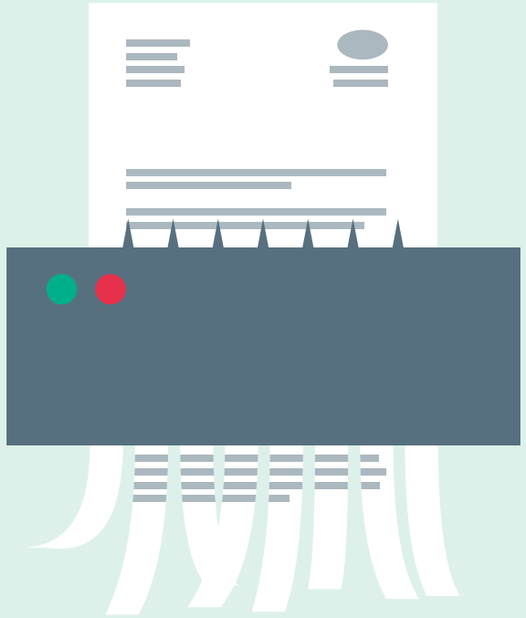
Kun 3 pct. af de offentligt ansatte oplyser, at de lod dokumenterne være. Det er et mindre fald i forhold til 2020, hvor 8 pct. oplyste det samme.

Samlet set tegner tallene et billede af, at de offentligt ansatte er blevet bedre til at håndtere arbejdsrelaterede oplysninger, som er placeret et forkert sted.

Hvad gjorde du den seneste gang, du fandt dokumenter med arbejdsrelaterede fortrolige oplysninger, der var placeret et forkert sted?



Anm.: n = 245 (2022) og 267 (2020).



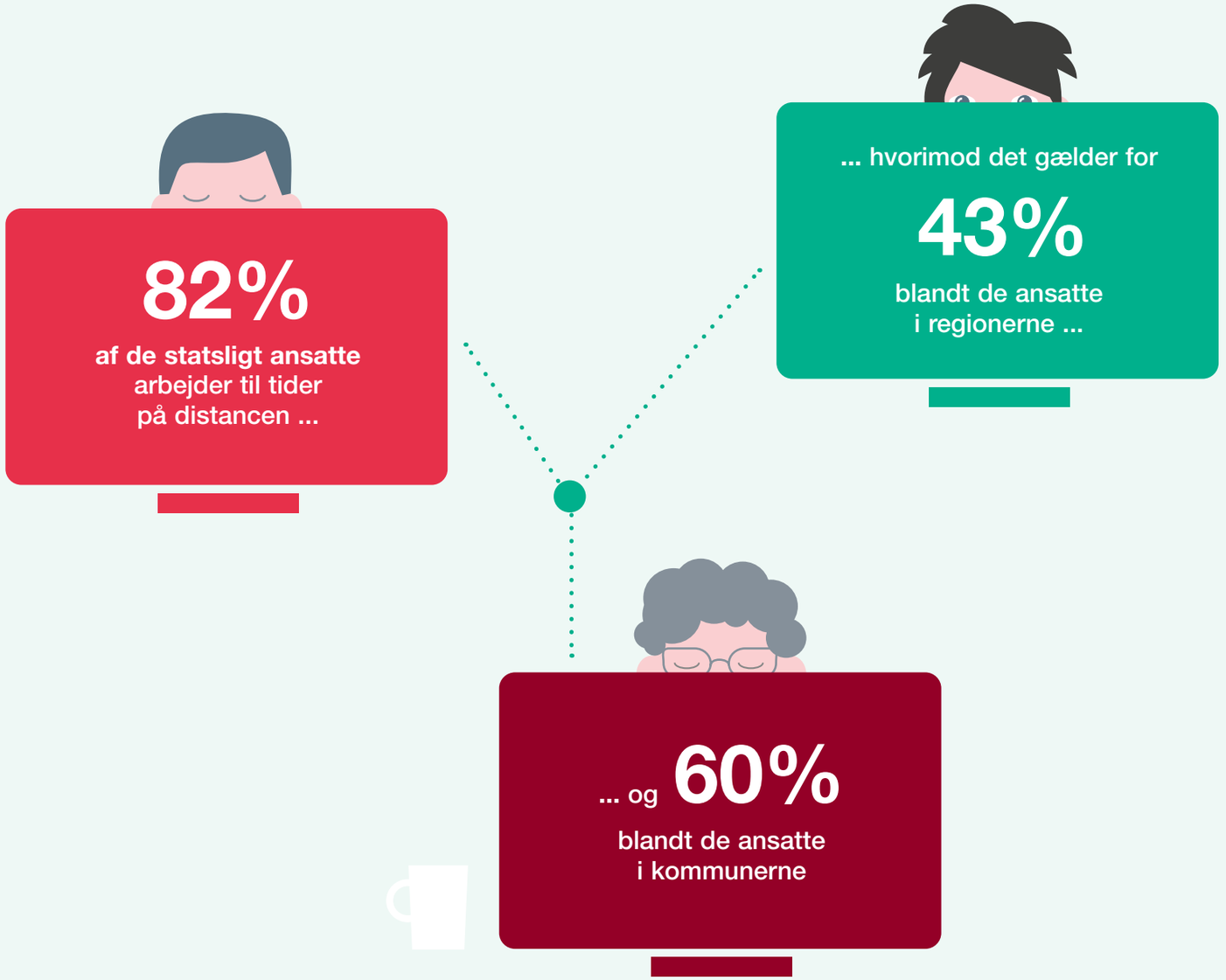
Distancearbejdspladserne bliver gradvist mere sikre

Distancearbejdspladser er blevet normalen

I 2020 lukkede mange offentlige arbejdspladser ned for fysisk fremmøde grundet Covid-19 pandemien, og mange begyndte at arbejde på distancen. Sidenhen er distancearbejde blevet mere udbredt, og mange offentligt ansatte (63 pct.) arbejder stadig til tider fra distancen frem for at møde fysisk på arbejdspladsen. Det er samme niveau (62 pct.) som under covid-19 i sommeren 2020.

Hvad udgør en sikker distancearbejdsplads?

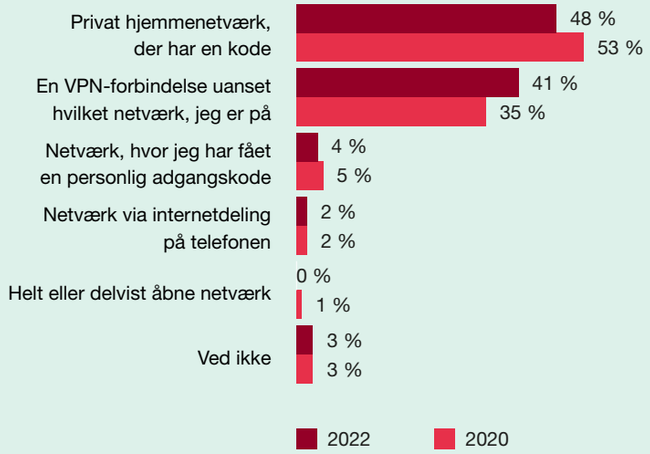
Brug af udstyr, der lever op til arbejdspladsens informationssikkerhedsretningslinjer og en sikker netværksforbindelse er blandt andre forhold afgørende for, at en distancearbejdsplads kan betegnes som sikker. Det kan være vanskeligt selv at sikre, at ens private udstyr lever op til alle de sikkerhedsmæssige krav, hvorfor det ofte er ønskeligt, at man kun benytter det udstyr, der stilles til rådighed af arbejdspladsen[8].



8 Center for Cybersikkerhed og Digitaliseringsstyrelsen har udgivet ”Beskyt organisationen: Opdater sikkerhedspolitikkerne til en »ny normal«” og ”God kultur ved distancearbejde”, der samler en række råd til at sikre organisationen ved distancearbejde.

41 pct. af offentligt ansatte anvender en VPN-forbindelse, der sørger for, at trafikken mellem brugeren og serveren er krypteret, hvilket er en stigning ift. 2020.

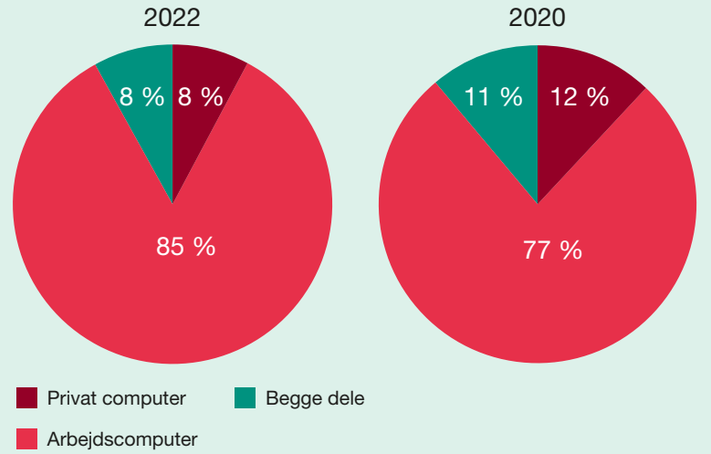
Hvilken type netværk/forbindelse anvender du oftest, når du arbejder andet sted end din arbejdsplads som for eksempel hjemmefra eller på en cafe?



Anm.: n = 646 (2022) og 639 (2020).

Færre anvender deres egen private computer ved hjemmearbejde sammenlignet med 2020.

Anvender du din private computer eller din arbejdscomputer, når du arbejder hjemmefra?



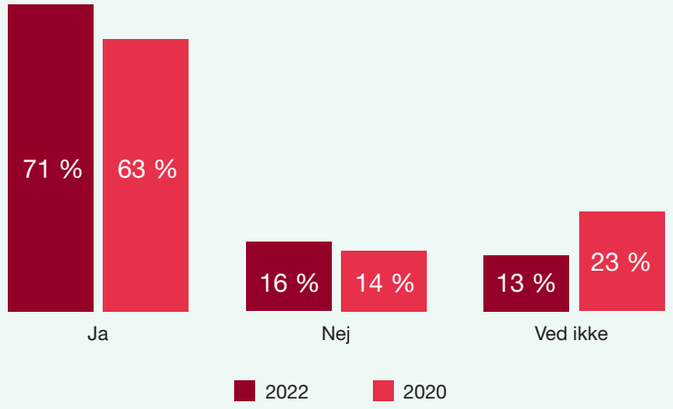
Anm.: n = 635 (2022) og 629 (2020).

Specifikke informationssikkerhedsretningslinjer for distancearbejde er blevet mere udbredte

Flere offentlige arbejdspladser har fået opdateret deres retningslinjer, så de afspejler den nuværende situation, hvor distancearbejde udgør en fast bestanddel af mange medarbejderes hverdag. Samtidig er der sket et fald i andelen, der ikke ved, om arbejdspladsen har retningslinjer for distancearbejde.

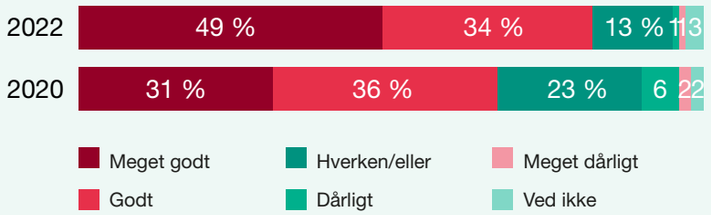
Samtidig angiver flere offentligt ansatte, at de føler sig bedre klædt på til at arbejde fra distancen.

Har din arbejdsplads retningslinjer for hjemmearbejde/ arbejde fra andet sted end din normale arbejdsplads, f.eks. når det kommer til håndtering af informationer samt brug af udstyr og kommunikationskanaler?



Anm.: n = 646 (2022) og 639 (2020).

Føler du, at du er klædt godt eller dårligt på til at arbejde hjemmefra/fra et andet sted end din normale arbejds-plads i overensstemmelse med din arbejdsplads' retningslinjer for informationssikkerhed?



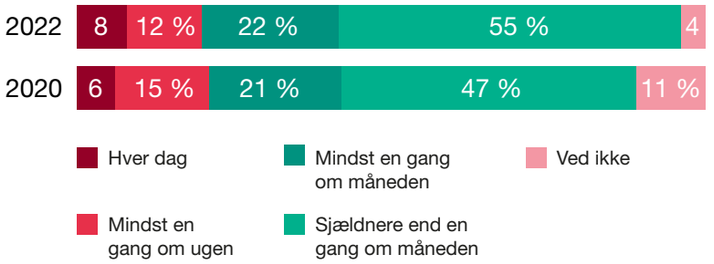
Anm.: n = 646 (2022) og 605 (2020).

af de medarbejdere, der har modtaget information om eller undervisning i arbejdspladsens retningslinjer, føler sig godt/meget godt klædt på til at arbejde fra distancen.
Det gælder kun for **66 pct.** af de, der ikke har modtaget information eller undervisning.

Det kniber stadig med efterlevelsen af informationssikkerhedsretningslinjerne

20 pct. af de offentligt ansatte, som angiver, at de nogle gange undlader at efterleve retningslinjerne, siger, at det sker mindst en gang om ugen.

Hvor ofte undlader du at efterleve informations-sikkerhedspolitikkerne og/eller -retningslinjerne for din arbejdsplads?



Anm.: n = 141 (2022) og 157 (2020).

Adspurgt om, hvad der er den største barriere for at efterleve retningslinjerne, svarer de ansatte selv, at den største barriere er, at det er for besværligt at holde styr på alt det, man skal, samt at de godt ved, hvad der er det rigtige at gøre, men at de glemmer at gøre det.

Hvorfor er informationssikkerheds-retningslinjer vigtige?

Medarbejdere er en af de største kilder til sårbarheder i organisationer[9].

En arbejdsplads' informationssikkerhedsretningslinjer er et udtryk for de risici, som organisationen har identificeret som særligt vigtige for den. Retningslinjerne beskriver, hvordan medarbejdere skal agere, for at organisationen kan være sikker og håndtere oplysninger hensigtsmæssigt.

Medarbejdere er typisk forpligtet kontraktmæssigt til at efterleve retningslinjerne, hvorfor mange organisationer træner og uddanner sine medarbejdere i dem.

81%

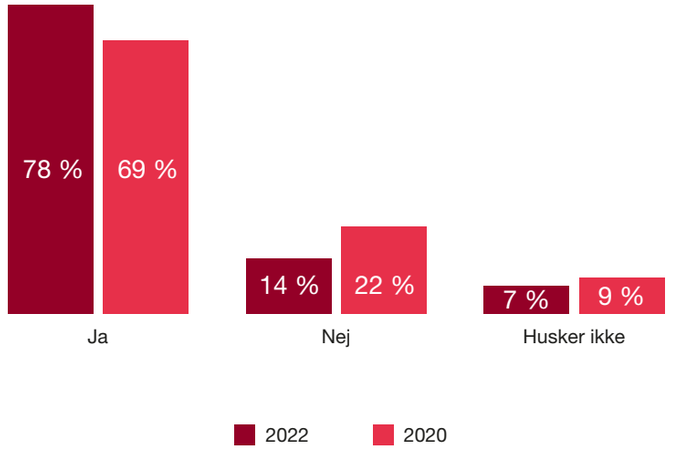
af de offentligt ansatte, der har modtaget undervisning eller information om deres arbejdsplads' retningslinjer er opmærksomme på risikoen for bedrageri og cyberkriminalitet på nettet. Det gælder kun for 58 pct. af dem, der ikke har modtaget undervisning eller information.

9 Hill, Michael: 90% of UK Data Breaches Due to Human Error in 2019, Infosecurity Magazine. M., Jacob: Human error is still the number one cause of most data breaches in 2021, Influencive. Datatilsynets statistikbank over fordeling af hændelser

Undervisning og awareness gør en mærkbar forskel for sikkerhedsadfærden

Der ses en stigning i andelen af medarbejdere, der har modtaget informationer om eller undervisning i deres arbejdsplads' informationssikkerhedspolitikker eller -retningslinjer.

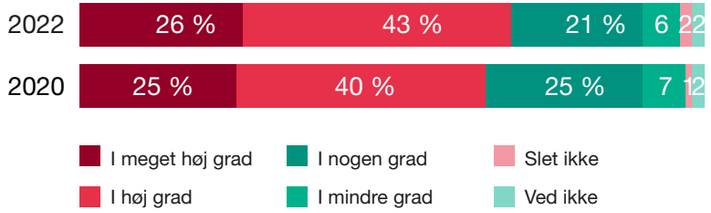
Har du modtaget information om og/eller undervisning i din arbejdsplads' informationssikkerhedspolitikker og/eller -retningslinjer?



Anm.: n = 1.030 (2022) og 1.030 (2020).

Samtidig ses en lille stigning i andelen af offentligt ansatte, som er bekendt med de informationssikkerhedspolitikker og/eller -retningslinjer, der er gældende for deres arbejde.

I hvilken grad er du bekendt med de informationssikkerhedspolitikker og/eller -retningslinjer, der er gældende for dit arbejde?



Anm.: n = 1.030 (2022) og 1.030 (2020).

67 pct. af de offentligt ansatte, der har modtaget undervisning om informationssikkerhed, svarer, at deres digitale adfærd er sikker. Det gælder kun for 43 pct. af dem, der ikke har fået undervisning. Kun 2 pct. af dem, der har fået undervisning, angiver, at de ikke ved, hvad de skal gøre i relation til informationssikkerhed.

Metode

Datagrundlag

Datagrundlaget for undersøgelsen består af to større spørgeskemaundersøgelser. Det ene spørgeskema er målrettet borgere og gennemført blandt et repræsentativt udsnit af den danske befolkning i alderen 18 år og opefter. Det andet spørgeskema er målrettet offentligt ansatte og er gennemført blandt et repræsentativt udsnit af de offentligt ansatte i alderen 18 år og opefter.

Således er al data i undersøgelsen, både hvad angår trusler og adfærd mm., selvangivet data og dermed et udtryk for respondentens egen oplevelse.

Dataindsamlingen er foretaget af analysevirksomheden MEGAFON i perioden fra d. 27. juni 2022 til d. 13. juli 2022. I alt er der indsamlet 2.040 interviews med en svarprocent på 43. Heraf er 1.010 interviews med borgere og 1.030 interviews med offentligt ansatte. Dette anses typisk som et passende antal interviews til at give tilstrækkelig statistisk sikkerhed for de opnåede resultater. Det skal dog bemærkes, at størrelsen på stikprøverne medfører, at små svarprocenter bygger på et lille antal personer. F.eks. betyder en svarandel på 3 pct. af de offentligt ansatte, at 31 personer har givet det pågældende svar. Det er fremhævet i rapporten, hvis resultaterne baserer sig på et sparsomt datagrundlag og derfor skal tolkes med forbehold.

Respondenterne har deltaget anonymt i undersøgelsen, hvilket er vigtigt for at skabe en høj grad af troværdighed i besvarelserne.

Inden undersøgelsens igangsættelse er der foretaget en foranalyse med 5 interview til brug for kontrol af spørgeskema og metode.

Dataindsamling

Interviewene er indsamlet via en kombination af internet- og telefoninterviews. Heraf er ca. 90 pct. indsamlet online og 10 pct. telefonisk. Internetinterviewene er indsamlet blandt medlemmer af MEGAFON-panelet, mens telefoninterviewene er indsamlet blandt danskere udtrukket simpelt tilfældigt fra MEGAFON's telefonnummerbase over samtlige fastnet- og mobilnumre i Danmark.

Denne kombinerede indsamlingsmetode sikrer en højere grad af repræsentativitet end en undersøgelse, der udelukkende er baseret på internetinterviews, da befolkningsgrupper, der bruger internettet i mindre grad end den generelle befolkning, får mulighed for at deltage i undersøgelsen via telefoninterviews.

Datamaterialet er desuden vægtet eller stratificeret med henblik på at sikre en så høj repræsentativitet som muligt i forhold til den samlede population. Datamaterialet for borgerne er vægtet efter køn, alder og område i forhold til den aktuelle fordeling i Danmarks befolkning[10].

Datamaterialet for offentligt ansatte er stratificeret efter ansættelsessted[11] og arbejdslandsdel i forhold til den aktuelle fordeling blandt de offentligt ansatte[12].

Fortolkning af resultater

I fortolkningen af resultaterne i rapporten fremhæves alene sammenhænge, der er statistisk signifikante. Til dette formål er der anvendt et signifikansniveau på 0,05, hvilket er alment accepteret. Dermed kan det med stor sandsynlighed siges, at de fremhævede sammenhænge ikke skyldes tilfældig variation.

Derudover kan det i beskrivelsen af resultaterne ske, at sammenlægninger af procenttal (vist i parenteser) ikke stemmer overens med summen af procenttallene i figurerne. Dette skyldes afrunding.

10 Kilde: Danmarks Statistiks, "Folketal pr. 1. januar 2022 efter køn, område, alder og tid" – www.statistikbanken.dk
11 Dette omfatter staten, regioner, kommuner og selvstændige offentlige virksomheder.
12 Dette omfatter staten, regioner, kommuner og selvstændige offentlige virksomheder.

Sammenligelighed med tidligere undersøgelser

Undersøgelsen indgår i en række undersøgelser af danskernes informationssikkerhed, som er gennemført ca. hvert andet år i perioden 2013 til 2020. I alle årene har borgerne været genstand for undersøgelsen, mens de offentligt ansatte har indgået i undersøgelsen siden 2016. Resultaterne fra de tidligere undersøgelser indgår i rapporten, hvor det er muligt og relevant at foretage en sammenligning. Hvis der ikke er foretaget en sammenligning i rapporten, skyldes det, at der er tale om et nyt eller væsentligt ændret spørgsmål.

I år er afgrænsningen af målgrupperne ændret i forhold til tidligere års undersøgelser. Hvor målgrupperne tidligere har været afgrænset til hhv. borgere og offentligt ansatte i alderen 18-74 år, er der i år ikke nogen øvre grænse for målgruppernes alder. Ændringen skyldes et ønske om at afdække informationssikkerheden blandt alle danskere, også de ældste. Det har altså ikke været tilfældet tidligere, hvor danskere på 75 år eller derover har været udeladt fra undersøgelsens målgrupper.

I den forbindelse skal det bemærkes, at den nye afgrænsning af målgrupperne har en vis betydning for sammenligneligheden med tidligere års undersøgelser. Årsagen er, at det kan føre til væsentlige ændringer i resultaterne, hvis gruppen af 75+-årige adskiller sig systematisk fra den øvrige del af målgruppen med hensyn til deres informationssikkerhed. Man kan eksempelvis forestille sig, at ældre borgere er mere udsatte for visse digitale trusler end yngre borgere. I så fald kan det ikke siges med sikkerhed, om et evt. højere trusselsniveau blandt borgerne skyldes et ændret trusselsbillede eller en ændring i opgørelsesmetoden. Alle de historiske sammenligninger i undersøgelsen skal derfor tolkes med det forbehold.

Øvrige datakilder

Foruden spørgeskemaerne inddrager undersøgelsen også sekundære datakilder til at afdække danskernes informationssikkerhed. Hensigten med dette er at tegne et så fuldendt billede af undersøgelsesområdet som muligt ved at perspektivere, sammenligne og supplere indsigterne fra spørgeskemaerne med viden og andre data på området. Det er tydeligt angivet i undersøgelsen, hvis data stammer fra andre kilder end spørgeskemaundersøgelserne.

Digitaliseringsstyrelsen
Danske Regioner
KL

digst.dk / regioner.dk / kl.dk

Danskernes informationssikkerhed 2022

Digitaliseringsstyrelsen
Danske Regioner
KL

Design: BGRAPHIC

ISBN: 978-87-93073-58-6