Styrelsen for Samfundssikkerhed / Danske Regioner / KL

Danskernes informations-sikkerhed 2024

Indhold

Perspektiver for digital sikkerhed i Danmark

Det aktuelle trusselsbillede i Danmark

Digital kriminalitet udgør i dag en stigende trussel for både borgere og offentligt ansatte i Danmark, og trusselsbilledet bliver stadigt mere komplekst og avanceret. Kriminelle udvikler hele tiden deres kompetencer og redskaber og benytter sig eksempelvis også af kunstig intelligens til at målrette og effektivisere deres angreb. I 2023 har Danmark oplevet en rekordstor stigning på 30 procent i anmeldelser om it-relateret økonomisk kriminalitet sammenlignet med 2022 (NCIKs årsrapport 2023). Udviklingen understreger nødvendigheden af, at både borgere og offentligt ansatte er rustede til at modstå digital kriminalitet.

Den globale politiske situation bidrager også til et forhøjet cybertrusselsniveau, hvor spændinger mellem stater og grupperinger øger risikoen for cyberangreb. Mere end nogensinde før er der brug for indsatser, for at borgerne skal kunne sikre sig i det samfund, vi lever i i dag.

Et trusselsbillede i forandring stiller stadigt større krav til borgere og offentligt ansatte

Denne analyse viser, at phishing er den mest udbredte digitale trussel mod både borgere og offentligt ansatte, og det udgør indgangen til mange andre former for digital kriminalitet. Næsten syv ud af ti danskere har oplevet phishingforsøg, og svindelmetoderne udvikler sig konstant for at omgå eksisterende sikkerhedsforanstaltninger og bliver fortsat sværere at gennemskue. På offentlige arbejdspladser vinder ransomware og CEO-fraud frem og udfordrer offentligt ansatte.

Undervisning i informationssikkerhed gør en forskel

Undervisning spiller en afgørende rolle for at øge sikkerhedsadfærden blandt offentligt ansatte. De ansatte, der har modtaget undervisning, vurderer, at de er bedre til at overholde arbejdsstedets retningslinjer og sikkerhedspolitikker, og flere vurderer, at deres digitale adfærd er sikker. Dog mangler en fjerdedel af de offentligt ansatte fortsat undervisning i informationssikkerhed – en gruppe, der også udviser lavere robusthed i forhold til sikker digital adfærd.

Udfordringer med at omsætte opmærksomhed på digitale trusler til sikker adfærd

Selvom både borgere og offentligt ansatte generelt har en høj grad af opmærksomhed på digitale trusler, omsættes bevidstheden ikke altid til sikre handlinger i praksis. Mange undlader eksempelvis at opdatere software og genbruger adgangskoder.

Blandt de offentligt ansatte spiller praktiske barrierer en væsentlig rolle. Næsten halvdelen oplever, at retningslinjerne er svære at huske og udføre konsekvent i hverdagen. Blandt borgerne ser man lignende udfordringer, hvor tekniske og forståelsesmæssige barrierer hæmmer en stabil sikkerhedsadfærd.

Det komplekse og stigende trusselsbillede stiller krav om løbende opmærksomhed og tilpasning. Digital kriminalitet udvikler sig hurtigt, og fremtidige indsatser kan være afgørende for at ruste danskerne til at møde de digitale udfordringer.

God læselyst

Styrelsen for Samfundssikkerhed / Danske Regioner / KL

Analysens formål og tilblivelse

Formålet med denne analyse er dels at give et aktuelt indblik i omfanget af digital kriminalitet rettet mod den danske befolkning, herunder både borgere og offentligt ansatte, dels at afdække deres vidensniveau, adfærd og bevæggrunde inden for digital sikkerhed. Analysen har til hensigt at sikre, at fremtidige informationsindsatser kan målrettes effektivt og præcist.

Denne analyse er udarbejdet af Pluss Leadership for Styrelsen for Samfundssikkerhed i samarbejde med Danske Regioner og KL og bygger på datagrundlag indsamlet af Verian. Analysen henvender sig til en bred vifte af aktører, herunder beslutningstagere, offentlige instanser, private virksomheder og andre interesserede parter.

Analysen blev første gang udgivet i 2013 og er siden blevet udgivet med et fast interval. Fra 2013 til 2016 blev den offentliggjort hvert år og fokuserede primært på borgernes informations-sikkerhed. I 2016 blev analysen udvidet til også at omfatte offentligt ansatte, og fra 2016 til 2024 er den udgivet hvert andet år. Tidligere stod Digitaliseringsstyrelsen som afsender på analysen, men med ressortomlægningen i august 2024 er denne opgave nu overtaget af Styrelsen for Samfundssikkerhed.

Analysen fokuserer på to hovedgrupper: danske borgere på 18 år og derover samt offentligt ansatte i offentlige selskaber, stat, regioner og kommuner. For at sikre en dybere forståelse af udfordringerne i hver gruppe er rapporten opdelt i to særskilte dele, der adresserer specifikke aspekter af informationssikkerhed for borgere og offentligt ansatte. Analysen er gennemført som en spørgeskemaundersøgelse og baseres derfor på selvrapporterede svar fra hhv. borgere og offentligt ansatte.

Første del: Borgernes informationssikkerhed

Denne del afdækker de mest aktuelle trusler, borgernes daglige sikkerhedsadfærd, digitale kompetencer samt de barrierer og drivkræfter, der påvirker deres adfærd.

Anden del: Offentligt ansattes informationssikkerhed

I denne del undersøges de cybertrusler, som offentligt ansatte møder i deres arbejdsliv, de offentligt ansattes adfærd i forhold til gældende informationssikkerheds-retningslinjer samt betydningen af uddannelse og adfærds-fremmende foranstaltninger.

Rapporten er designet til at kunne læses i sin helhed eller bruges som opslagsværk for specifikke områder inden for informations-sikkerhed. For de læsere, der ønsker detaljeret indsigt i metodikken bag undersøgelsen, findes et metodekapitel sidst i rapporten. Rapporten kan desuden anvendes til at sammenligne udviklingen i informationssikkerhed over tid, da visse resultater bygger videre på data fra tidligere års analyser.

Afslutningsvis giver denne analyse et grundlag for at forstå de aktuelle udfordringer og udviklings-tendenser inden for informationssikkerhed i Danmark. Ved at belyse både borgernes og de offentligt ansattes erfaringer, kompetencer og barrierer i forhold til cybertrusler understøtter rapporten indsatsen for en mere robust digital sikkerhed på tværs af samfundet.

1. Borgernes informations-sikkerhed

Det aktuelle trusselsbillede

Tre ud af fire danskere har været forsøgt svindlet inden for det seneste år

76% har været udsat for forsøg på digital svindel

22% er blevet svindlet eller franarret informationer (med/uden konsekvenser)

13% har oplevet konsekvenser af svindel/sikkerhedsbrud

Phishing: Den mest udbredte digitale trussel i Danmark

Phishing, som kan opdeles i smishing, phishing og vishing alt efter indgangsmetode, er i dag den trussel mod danskernes informationssikkerhed, som flest møder. Hele 68% af befolkningen har været forsøgt franarret personlige oplysninger, enten via sms (smishing), mail (phishing) eller opkald (vishing). Denne type svindel udnytter dagligdagens digitale interaktioner og kan være vanskelig at beskytte sig imod.

Svindel ved samhandel sker både blandt privatpersoner og på den digitale handelsplads

Cirka hver tredje dansker har oplevet svindel i forbindelse med samhandel – enten i form af svindel gennem fupannoncer og fupbutikker (19%), ved handel mellem private personer (17%) eller investeringssvindel (16%).

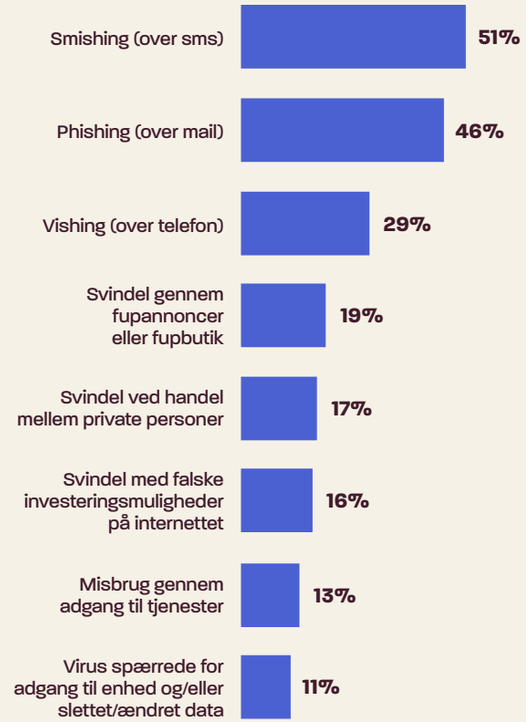
Store mørketal: Mange anmelder ikke it-kriminalitet

I 2023 kunne politiets Nationale Center for IT-Kriminalitet (NCIK) rapportere om flere end 32.000 anmeldelser fra private borgere. Den oftest anmeldte form for it-relateret økonomisk svindel i 2023 var phishing, der udgjorde 40% af alle anmeldelser. Det svarer til 12.765 unikke anmeldelser. Herefter fulgte anmeldelser om samhandel, som udgjorde 37% af alle anmeldelser. Hos politiet inkluderer denne kategori dog ikke investeringssvindel. Danmarks Statistik vurderer, at det kun er omkring en femtedel, der anmelder it-kriminalitet til politiet, hvorfor de reelle tal må formodes at være væsentligt højere.

Eksempler

Eksempler på konsekvenser ved digital svindel er økonomisk tab, fx gennem falske investeringer eller ved betaling for et produkt, der aldrig dukker op. Andre konsekvenser kan fx være misbrug af personlige oplysninger eller mistet adgang til data.

De mest udbredte former for svindel blandt danskere i 2024



Note: N=1.435.

Danskernes bevidsthed om digitale trusler

Danskerne er opmærksomme på truslen fra digital kriminalitet, og en stigende andel er bekymrede

Danskernes opmærksomhed på digital kriminalitet er uændret

Selvom opmærksomheden på digital kriminalitet har været stabil de senere år, er der sket et fald i andelen af danskere, der i meget høj grad er opmærksomme. I 2020 var det 36%, mens det tal er faldet til 29% i 2024. På trods af en stigning i antallet af svindelsager (se side 11) er danskernes opmærksomhed ikke fulgt med udviklingen.

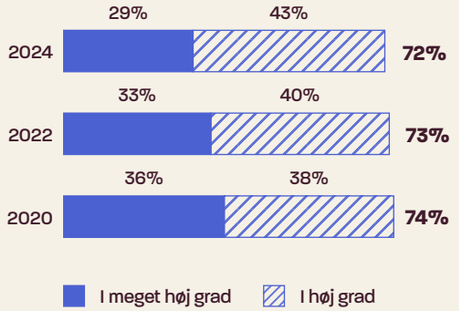
Opmærksomheden på digital kriminalitet varierer med alder og køn

Opmærksomheden på digital kriminalitet stiger med alderen, hvor ældre borgere generelt viser større bevidsthed om risikoen. Derudover er der en tydelig kønsforskel blandt de yngre. Blandt mænd i alderen 18-29 år er hele 75% i høj eller meget høj grad opmærksomme på digital svindel, mens 51% af kvinderne i samme aldersgruppe rapporterer den samme opmærksomhed. Overordnet set er mænd mere opmærksomme på truslen fra digital kriminalitet.

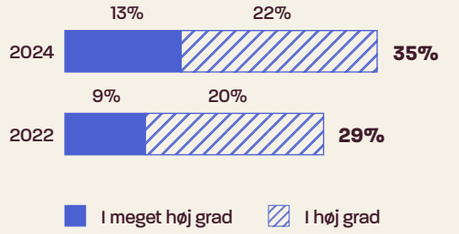
Bekymring for digital svindel er stigende

I 2022 var 29% af danskerne i høj eller meget høj grad bekymrede for at blive udsat for bedrageri og digital kriminalitet. I 2024 er det tal vokset til 35%

Udviklingen i andelen af danskerne, der i høj eller meget høj grad er opmærksomme på digital svindel



Udviklingen i andelen af danskerne, der i høj eller meget høj grad bekymrer sig om digital svindel



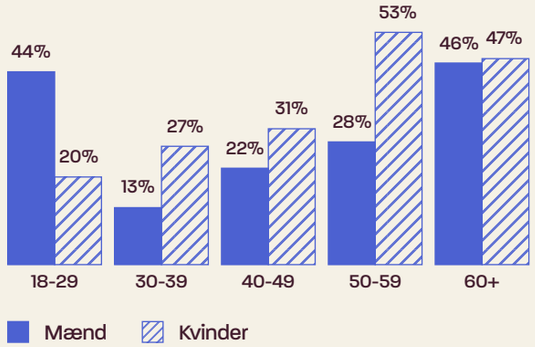
Note: Følgende spørgsmålstekst er anvendt: : "I hvilken grad er du opmærksom på risikoen for bedrageri og cyberkriminalitet på internettet?" og "I hvilken grad er du bekymret for at blive udsat for bedrageri og cyberkriminalitet på internettet?". N=1.435.

Digital kriminalitet bekymrer flere kvinder end mænd og flere ældre end yngre

Generelt er kvinder mere bekymrede end mænd, på nær i aldersgruppen 18-29-årige, hvor bekymringen er størst blandt mænd. På nær de unge mænd er det fortsat de ældre, som er mest bekymrede for digital kriminalitet.

På tværs af uddannelsesniveauer er bekymringen størst blandt de ufaglærte, hvor 44 % i meget høj eller høj grad er bekymrede.

Andel med høj eller meget høj grad af bekymring, fordelt på køn og alder



Note: N=1.435.

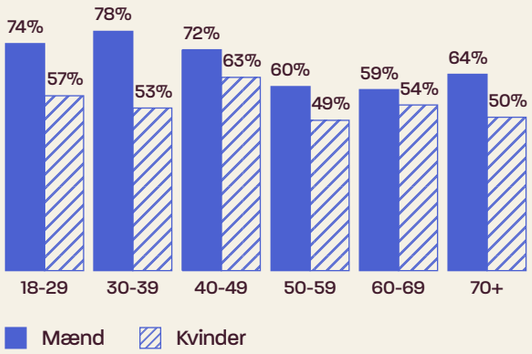
Digitale kompetencer

Flertallet af danskere føler sig godt klædt på – men oplever også barrierer for sikker digital adfærd

Ulighed i cybersikkerhedskompetencer blandt danske borgere

Cirka to tredjedele af borgerne føler sig godt eller meget godt klædt på til at beskytte sig mod bedrageri og digital kriminalitet, men andelen har oplevet et fald fra 67% i 2022 til 61% i 2024. Mænd føler sig generelt bedre klædt på end kvinder, og der er desuden et tydeligt uddannelsesgab. Væsentligt flere blandt de længst uddannede (lang videregående uddannelse) føler sig godt rustede til at håndtere digitale trusler sammenlignet med de kortest uddannede (ufaglærte).

Andel, der føler sig godt eller meget godt klædt på til at beskytte sig mod bedrageri og digital kriminalitet, fordelt på køn og alder



Note: N=1.435.

Praktiske og forståelsesmæssige barrierer udfordrer borgernes digitale sikkerhedsadfærd

Selvom mange danskere føler sig forberedte, oplever to tredjedele fortsat barrierer for at opretholde en sikker digital adfærd i hverdagen. For flertallet handler disse udfordringer om rent praktiske forhold: 23% oplever, at det er besværligt at holde styr på sikkerheds-foranstaltninger, 14% glemmer at følge anbefalingerne, mens 15% føler sig hæmmet af manglende viden.

Unge udfordres af omgangskredsens holdning til cybersikkerhed

For yngre danskere udgør manglende alvor omkring cybersikkerhed i omgangskredsen en væsentlig barriere (17% blandt de 18-29-årige oplever det, sammenlignet med 1-5% blandt øvrige aldersgrupper). Selvom mange unge ved, hvad de skal gøre for at sikre deres digitale adfærd, kan den manglende alvor i omgangs-kredsen bidrage til, at sikkerhedsforanstaltninger bliver nedprioriteret eller glemt i dagligdagen.

De fire oftest oplevede barrierer for sikker digital adfærd i hverdagen

Note: Besvarelse af spørgsmålet: Hvad oplever du, står i vejen for, at du kan have sikker digital adfærd i din hverdag? N=1.435.

Vil du vide mere?

Hvis du vil vide mere om digital sikkerhed, og hvordan du kan ruste dig selv bedst muligt, kan du læse mere hos bl.a. sikkerdigital.dk under Styrelsen for Samfundssikkerhed og politiet.dk under deres fore-byggelsesråd om økonomisk svindel på nettet.

Barrierer for den gode digitale adfærd

Vi er blevet dårligere til at følge anbefalinger for sikker digital adfærd

Tre ud af fire anbefalinger efterleves i ringere grad i 2024 end i 2022

Næsten en femtedel (17%) af danskerne kender ikke anbefalingerne og mangler derfor viden for at kunne styrke deres digitale adfærd. Og selv blandt dem, der kender anbefalingerne, ved 15% ikke, hvordan man efterlever dem. Denne andel er dog faldet fra 26% i 2022.

Andre barrierer for at efterleve anbefalingerne handler om forståelsen for risici ved manglende sikker digital adfærd.

- 17% mener ikke, at de har data, der er interessante for andre.
- 16% mener ikke, at der er stor risiko for at blive snydt, når man handler eller færdes på nettet.
- 14% mener ikke, at der er stor risiko for, at andre får adgang til deres data.

Generelt oplever danskerne barriererne for sikker digital adfærd som mindre end i 2022. 'Manglende tid og overskud' er sammenlignet med 2022 den barriere, der er reduceret mest – blot 8% oplever det i dag som en barriere mod 22% i 2022.

Godt klædt på

De 61% af danskerne, der føler sig godt klædt på til at beskytte sig mod bedrageri og digital kriminalitet, følger alle anbefalingerne i højere grad end dem, der ikke føler sig godt klædt på.

Anbefalinger

	Udvikling i andelen, der følger anbefalingen fra 2022 til 2024, i procentpoint	Andel af danskere i 2024, der efterlever anbefalingen i høj eller meget høj grad
Opdater din enhed med producentens seneste opdateringer	▼ -22%	46%
Tjek, at beløbet og butiksnavnet stemmer, når du får bekræftelses-sms	▼ -13%	66%
Tjek, om webadressen ser rigtig ud og kig efter sprogfejl og priser i skæve beløb	▼ -12%	73%
Vælg dit eget, stærke kodeord til dit trådløse netværk i hjemmet	▼ -12%	54%
Brug to-faktor-login, når det er muligt	▼ -12%	42%
Tag jævnligt en sikkerhedskopi af dine data på din computer	▼ -11%	33%
Sæt din tablet og/eller smartphone til automatisk at hente og installere opdateringer	▼ -9%	64%
Beskyt din computer med et antivirusprogram	▼ -9%	61%
Del aldrig dit kodeord med andre	▼ -8%	78%
Sæt din computer til automatisk at hente og installere opdateringer af programmer	▼ -8%	63%
Vælg dit eget stærke kodeord til din digitale enhed	▼ -8%	47%
Kodeord til f.eks. mail, MitID og sociale medier skal alle være forskellige	▼ -7%	44%
Undgå at anvende åbne, trådløse netværk uden kode	▼ -6%	44%
Opret en kreditadvarsel på borger.dk ved mistanke om identitetstyveri	▼ -6%	21%
Del aldrig dine MitID-oplysninger med andre	▼ -5%	91%
Anvend en VPN-forbindelse, når du bruger et åbent trådløst netværk uden kode	▼ -2%	21%
Brug en passwordmanager (et program eller en app)	△ 1%	20%
Beskyt din tablet og/eller smartphone med et antivirusprogram	△ 1%	37%
Kodeord skal være minimum 12 tegn	△ 2%	38%
Slå funktioner og enheder fra, hvis du ikke bruger dem	△ 2%	39%
Slet fremmede trådløse netværk fra telefonen/computeren efter brug	△ 5%	30%
Mød så vidt muligt sælger eller køber ansigt til ansigt*	-	45%
Tjek om varen sælges væsentligt billigere end hos andre*	-	51%

Note: *De to sidste spørgsmål blev i 2022 stillet som ét samlet spørgsmål, hvorfor direkte sammenligning ikke er mulig. Tabellen er baseret på andele, der 'i høj grad' eller 'i meget høj grad' følger anbefalingen. N=1.435.

Kilder til viden om informationssikkerhed

Danskernes foretrukne kilder til viden om digital sikkerhed har ændret sig siden 2022

Færre danskere får deres viden om digital sikkerhed gennem traditionelle nyhedsmedier

For blot to år siden fik seks ud af ti danskere deres viden om digital sikkerhed fra medierne, hvilket i dag kun er tilfældet for fire ud af ti. Tilsvarende oplever færre at få deres viden om digital sikkerhed via deres arbejdsplads eller på uddannelsen.

De nære relationer og sociale medier benyttes fortsat som kilde til viden

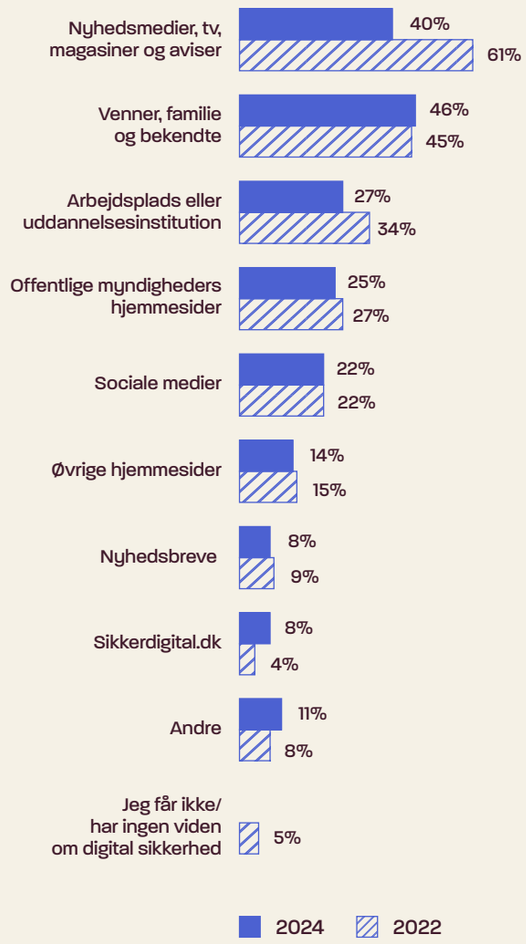
Samme faldende tendens gælder ikke for øvrige informationskilder såsom venner, familie og bekendte, der i dag er den største kilde til viden (46%), samt sociale medier og hjemmesider. Udviklingen i brugen af disse kilder ligger inden for få procentpoint sammenlignet med 2022.

Flere danskere bruger sikkerdigital.dk som informationskilde

Statens informationssite sikkerdigital.dk bruges i dag af 8% af danskerne, hvilket er en fordobling siden 2022.

Unge benytter sig i høj grad af sociale medier til at opnå viden om digital sikkerhed – og benytter også sikkerdigital.dk mere end andre aldersgrupper (13% af de 18-29-årige). De ældre benytter i høj grad deres omgangskreds til viden om digital sikkerhed (58% af de +70-årige).

Udviklingen i danskernes brug af kilder til viden om informationssikkerhed

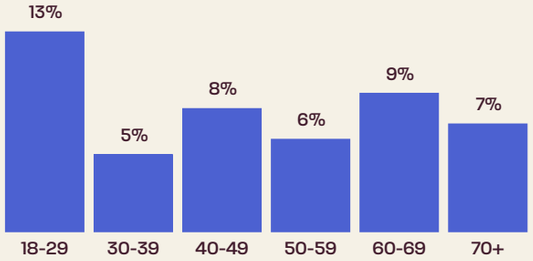


Note: Besvarelse af spørgsmålet: Hvor får du din viden om digital sikkerhed fra? Det har været muligt at give op til tre svar. N=1.435.

Traditionelle videnskilder bruges fortsat af de mest digitalt robuste

Af de danskere, der ikke har været svindlet inden for det seneste år, får en større andel deres viden fra traditionelle kilder som nyhedsmedier og arbejdspladsen. Flere her får også viden fra deres nære relationer sammenlignet med de danskere, som har været svindlet.

Andel, der bruger sikkerdigital.dk som kilde til viden om informationssikkerhed, opdelt på alder



Note: N=117, vægtet.

Truslen fra phishing

Phishing er den hurtigst voksende metode til at svindle danskerne

To ud af tre danskere har oplevet forsøg på phishing

68% af danskerne har været udsat for phishing-forsøg via opkald, sms eller mail – en stigning fra 57% i 2022. Blandt de personer, som har oplevet phishing via telefonkontakt – også kaldet vishing – har 18% også afgivet oplysninger til svindleren. Til sammenligning gælder det kun 9% af dem, der er blevet kontaktet via sms eller mail.

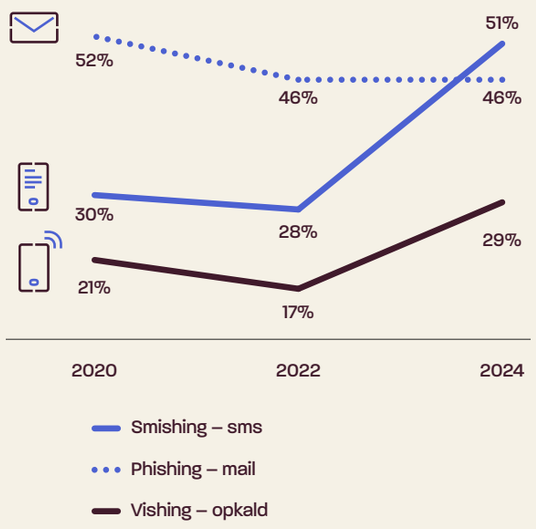
Svindlerne bruger i stigende grad sms og telefon-opkald til at narre danskerne. Derimod er phishing via mail faldet en smule (med 6 procentpoint). Denne udvikling kan skyldes, at nogle metoder er mere effektive end andre. En aktuel tendens er social engineering, der ofte ses i forbindelse med kontaktbedrageri. Et eksempel herpå er "bekendt i knibe"-svindel, der bl.a. foregår over sms, hvor svindlere udgiver sig for at være en nær relation i akut pengenød.

To tegn på, at det er et fupopkald

1. Kræver personen, at du udleverer dine personlige oplysninger eller overfører penge?
2. Forsøger personen at give indtryk af, at situationen er akut eller har store konsekvenser?

Find andre gode råd på sikkerdigital.dk

Udviklingen i typer af phishing



Note: Andelen af danskere der har mødt forsøg på de tre typer af phishing inden for det seneste år. N=1435.

Hvad er phishing?

Phishing er en form for svindel, hvor svindlere forsøger at narre personlige oplysninger fra offeret, såsom betalingskortoplysninger, kodeord eller MitID-oplysninger. Offeret kan fx blive lokket til at udlevere disse oplysninger ved at tro på en falsk historie eller ved at klikke på et link, der leder til en falsk loginside, hvor login-oplysningerne kan indtastes. Phishing kan foregå via mail, sms eller telefonopkald. Hvis offeret falder for svindelnummeret, kan det resultere i økonomiske tab, identitetstyveri eller tab af data.

Hvad er social engineering?

Social engineering er en bredere teknik, hvor svindlere bruger psykologiske metoder til at manipulere offeret til frivilligt at dele oplysninger. Her udnytter svindleren tillid og følelser. Mere avanceret social engineering trækker ofte på detaljer om offeret, som svindleren har fundet via sociale medier eller andre offentligt tilgænge-lige kilder gennem forudgående research.

Truslen fra phishing

Flere unge udsættes for forsøg på phishing, og flere franarres informationer

Yngre borgere er mere udsatte for phishingforsøg

Unge mellem 18 og 29 år er i højere grad mål for phishingforsøg end andre aldersgrupper. 25% af danskere, der angiver at have mødt phishing-forsøg, befinder sig i denne aldersgruppe, hvilket kan skyldes deres øgede digitale tilstedeværelse og brug af sociale medier, som øger deres eksponering overfor svindlere.

Yngre mænd er opmærksomme på risikoen for svindel

Mænd angiver generelt at have større opmærk-somhed over for svindel end kvinder. 75% af mændene er i høj grad eller meget høj grad opmærksomme, hvilket gælder for 69% af kvinderne. I aldersgruppen 18-29 år er forskellen mellem kønnene markant: 75% af de unge mænd i denne gruppe er i høj eller meget høj grad opmærksomme på truslen fra svindel, mens det kun gælder for 51% af kvinderne.

Opmærksomhed alene er ikke nok til at beskytte mod svindel

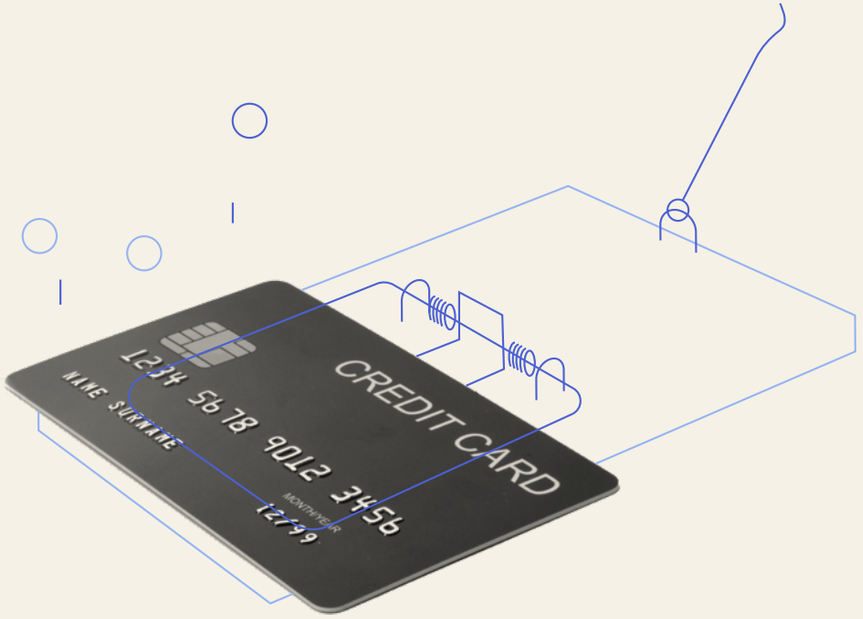
Unge mænd mellem 18 og 29 år bliver hyppigst franarret information. I 2024 blev 63% af de unge mænd i denne aldersgruppe franarret information. 19% af de unge kvinder mellem 18-29 år er blevet franarret information i løbet af det seneste år, mens det for de øvrige aldersgrupper er det 0-3%.

63%

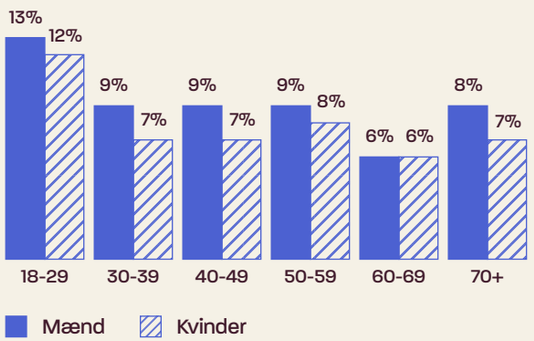
af mænd mellem 18-29 år har fået franarret information

19%

af kvinder mellem 18-29 år har fået franarret information

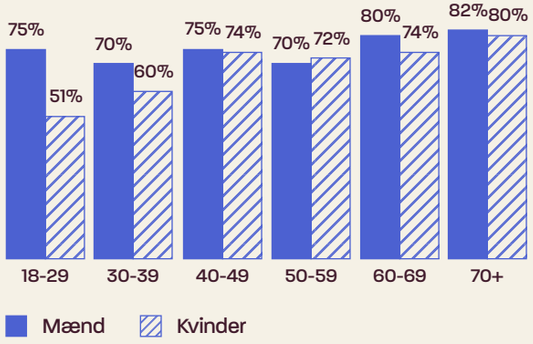


Fordeling på alder og køn af borgere, der har oplevet forsøg på phishing inden for det seneste år



Note: N=969, vægtet.

Andel med høj og meget høj grad af opmærksomhed på svindel fordelt på alder og køn



Note: N=1.435.

Truslen fra phishing

Danskerne handler ved forsøg på svindel – især når kontakten med svindleren opleves personligt

Telefonopkald udløser proaktive handlinger

Danskerne reagerer mest proaktivt på phishing-forsøg, når kontakten sker via telefonopkald. Den personlige kontakt gør, at 55% af danskerne handler efter et phishingopkald, fx ved at advare omgangskredsen eller anmelde hændelsen.

Blandt dem, der bliver snydt via telefon, anmelder 37% svindlen eller advarer deres netværk. Selv når de undgår at blive snydt, advarer 30% af borgerne stadig venner og familie. Sker forsøget på phishing via mail, er det kun 9% af de borgere, der faktisk bliver snydt, som advarer familie og venner.

61%

af borgerne handler efter phishingforsøg via telefonopkald

42%

af borgerne handler efter phishingforsøg via mail

Handlinger som reaktion på forsøg på phishing gennem telefonopkald

Note: N=414, vægtet.

Konsekvenser af phishing

Når en dansker bliver udsat for phishing, resulterer det i cirka halvdelen af tilfældene i egentlige konsekvenser, såsom økonomiske tab eller misbrug af personlige oplysninger. Telefonisk phishing fører oftest til konsekvenser som uautoriserede pengeoverførsler, oprettelse af falske konti i offerets navn eller direkte tyveri af finansielle informationer. Den direkte kontakt med svindleren kan skabe et større pres og gøre borgeren mere tilbøjelig til at dele personlige oplysninger.

Andel, der oplever økonomisk tab ved phishing

53% ved phishing på telefonopkald

50% ved phishing på SMS

50% ved phishing på mail

Truslen fra phishing

Mere end hver femte dansker er villige til at dele deres kodeord

Størstedelen af danskerne beskytter deres oplysninger

Phishing er en udbredt svindelform, så det er en god idé at tage forholdsregler for at beskytte sig selv bedst muligt. Det er en klar anbefaling aldrig at dele sine MitID-oplysninger eller kodeord med andre. Størstedelen af danskerne følger faktisk disse anbefalinger i høj eller meget høj grad. 91% af borgerne deler ikke deres MitID-oplysninger, mens 78% ikke deler deres kodeord med andre.

91% af danskere sørger for ikke at dele deres MitID-oplysninger med andre

78% af danskere sørger for ikke at dele deres kodeord med andre

For mange danskere har ikke klare forbehold mod at dele oplysninger

Følger man ikke disse anbefalinger i tilstrækkelig grad, risikerer man at stille sig selv dårligt i tilfælde af phishing. Ved både deling af MitID-oplysninger og kodeord er der danskere, som ikke i høj grad følger anbefalingerne. 7% følger slet ikke eller ved ikke, om de følger anbefalingen om ikke at dele kodeord. Det samme er gældende for 4%, når det handler om at dele MitID-oplysninger. Der er ikke væsentlige forskelle blandt danskerne alt efter, om man har været mødt af et svindelforsøg eller ikke.

Gode råd til at passe på dine oplysninger i hverdagen

- Send aldrig fortrolige oplysninger i e-mails, medmindre du kan kryptere e-mailen, og læg aldrig fortrolige og personlige oplysninger på sociale medier.
- Tænk over, om de oplysninger, du lægger på nettet, kan misbruges. Det kan fx være fortrolige oplysninger i et åbent CV.
- Log af, når du har brugt offentlige computere til fx at tjekke mail eller sociale medier. Slet også browserens historik, før du forlader computeren.
- Tjek dit papiraffald. Undlad at smide papirer med personlige oplysninger i skraldespanden eller affalds-containerne, før du har revet papirerne itu eller overstreget de personlige oplysninger.

Find andre gode råd på sikkerdigital.dk

Samhandel

Økonomisk svindel gennem samhandel er en stigende trussel

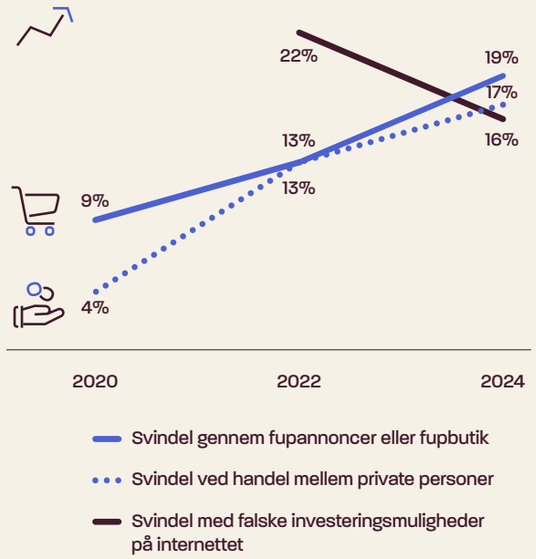
Hver tredje dansker forsøges svindlet gennem samhandel

Økonomisk svindel gennem samhandel er den næstmest udbredte trussel, som danskerne oplever, lige efter phishing. 35% af danskerne har mødt én eller flere former for svindel gennem samhandel. I 2024 har 19% af borgerne rapporteret, at de én eller flere gange har været udsat for svindel gennem fupannoncer eller fupbutikker – en stigning fra 13% i 2022. Desuden er svindel ved handel mellem privatpersoner steget med 3 procentpoint siden 2022. Ved svindel med fysiske varer omhandler det oftest varer som elektronik, tøj og tasker. Det kan også være online varer som billetter eller virtuel valuta.

Mange svindles ved fupannoncer og fupbutikker

Ved svindel gennem fupannoncer og fupbutikker lykkes svindlerne med deres foretagende i hele 37% af tilfældene. Handel mellem privatpersoner er også risikabelt. Her lykkes svindlerne i 31% af tilfældene. Til sammenligning lykkes det kun for svindlerne i 19% af tilfældene ved investeringssvindel.

Udviklingen i typer af svindel gennem samhandel



Note: Andelen af danskere, der har mødt forsøg på svindel gennem samhandel inden for det seneste år. N=1435.

Unge mænd oplever oftere samhandelssvindel

Unge, især unge mænd, oplever hyppigere økonomisk svindel i forbindelse med samhandel (17%). Denne gruppe rapporterer oftere om at blive udsat for svindel samt om at få franarret deres informationer (19% af alle mænd mellem 18-29 år). Dette kan skyldes, at unge generelt er mere tilbøjelige til at benytte digitale platforme til samhandel, hvilket potentielt øger deres eksponering for svindel. Færre ældre bliver narret, når de handler online eller privat.

Har du været udsat?

Har du været udsat for økonomisk svindel eller mistanke om det, kan du anmelde det digitalt på politiet.dk eller borger.dk. Det kan fx være svindel ved handel mellem privatpersoner, fuphjemmesider, e-mail, apps, sociale medier, identitetstyveri, falske fakturaer eller CEO-fraud.

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.

Læs mere i NCIK's nyeste årsrapport over it-relateret økonomisk kriminalitet.

Samhandel

Danskerne advarer hinanden om investeringssvindel

Samhandelssvindel giver konsekvenser for mange

Omkring halvdelen af dem, der bliver snydt ved fupannoncer eller fupbutikker og ved handel med private, oplever økonomiske konsekvenser, ligesom en stor andel aldrig modtager deres varer. Ved investeringssvindel får to tredjedele misbrugt deres personoplysninger på nettet, mens en tredjedel oplever økonomiske konsekvenser.

Danskerne handler aktivt efter svindelforsøg selv uden tab

Når danskerne udsættes for svindelforsøg gennem fupannoncer eller fupbutikker, reagerer mange aktivt – fx ved at advare deres omgangskreds eller kontakte den virksomhed, de troede, de havde købt varen hos. Hele 45% handler aktivt, selvom de ikke selv bliver snydt. For investeringssvindel er det 35% af borgerne, der handler aktivt, når de udsættes for forsøg på svindel.

Hurtig reaktion kan nedbringe konsekvenserne

At reagere hurtigt på svindelforsøg kan gøre en stor forskel i forhold til at minimere økonomiske konsekvenser. For at mindske konsekvenserne spærrer mange deres betalingskort (40% ved fupbutikker, 30% ved handel mellem privatpersoner), mens 26% kontakter deres bank efter begge typer svindel. Tilsvarende reaktioner sker ved investeringssvindel. Her spærrer 29% deres betalingskort, 29% kontakter myndighederne, mens 20% kontakter deres bank.

Investeringssvindel skaber større behov for at advare andre

Investeringssvindel er den form for samhandelssvindel, som flest danskere føler behov for at advare andre om. Blandt dem, der er blevet snydt gennem investeringssvindel, advarer 44% deres omgangskreds. Til sammenligning er det kun 21% af dem, der er snydt gennem fupannoncer eller fupbutikker, og 16% ved handel mellem privatpersoner, som advarer andre.

60%

af danskere foretager aktive handlinger, når de oplever forsøg på svindel fra privatpersoner – også selvom de ikke selv er blevet svindlet

44%

af alle borgere, der er faldet for investeringssvindel, advarer andre

Samhandel

Danskere, der har oplevet svindel, er mere opmærksomme på at efterleve gode råd til at afsløre samhandelssvindel

Oplevelser med svindel gør borgerne mere påpasselige

Borgere, der har oplevet svindel, er mere opmærksomme på at følge gode råd til at afsløre og undgå nye forsøg på økonomisk svindel. Særligt når det kommer til fupannoncer og fupbutikker, er erfaringen en stærk motivation for at være mere kritisk i vurderingen af websteder og annoncer. Hele 77% af de danskere, der har mødt forsøg på svindel, tjekker websider for sprogfejl og unaturligt lave priser. Den tilsvarende andel for de danskere, der ikke har oplevet forsøg på svindel, er 61%.

77% af alle, der har mødt forsøg på svindel, tjekker i høj eller meget høj grad websider for sprogfejl og skæve priser.

61% af alle, der ikke har mødt forsøg på svindel, tjekker i høj eller meget høj grad websider for sprogfejl og skæve priser.

Note: Opgjort efter andele, der svarer 'i meget høj grad' eller 'i høj grad' til spørgsmålet om, hvorvidt de følger anbefalingen: Tjek, om webadressen ser rigtig ud og kig efter sprogfejl og priser i skæve beløb. N=1435.

Ansigt til ansigt ved privat handel øger sikkerheden

Omkring halvdelen af danskerne er generelt opmærksomme på anbefalingerne for at undgå svindel ved privat handel. En vigtig anbefaling, som mange følger, er at møde sælgeren eller køberen ansigt til ansigt for at bekræfte varens eksistens og tilstand.

45% af danskerne møder i høj eller meget høj grad sælger eller køber ansigt til ansigt.

51% af danskerne tjekker i høj eller meget høj grad, om varen sælges væsentligt billigere end andre steder, hvilket kan være en indikation på svindel.

Denne praksis er konsistent uanset, om borgerne tidligere har været udsat for forsøg på svindel på nettet eller oplevet konsekvenser herved eller ej.

5 tegn, der kan afsløre svindel

1. Varen er markant billigere end andre steder
2. Der er priser i skæve beløb
3. Webadressen ser underlig ud
4. Beløbet og butiksnavnet er ændret, når du skal godkende købet
5. Der er ingen "om-os"-side på hjemmesiden, eller beskrivelsen lyder utroværdig

Find andre gode råd på sikkerdigital.dk

Indtrængen på enhed eller tjeneste

Danskernes digitale tjenester og enheder er i stigende grad mål for digital kriminalitet

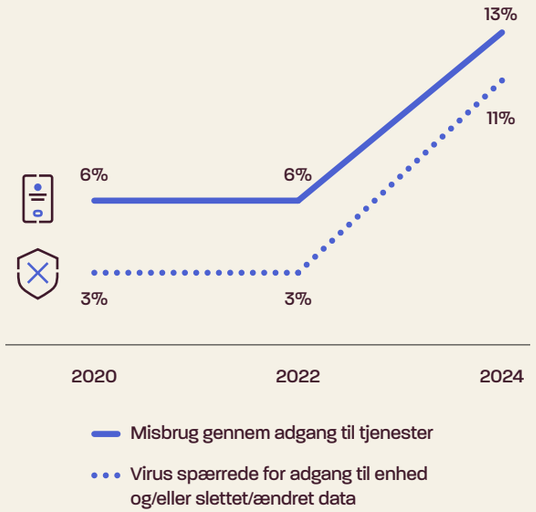
Stigning i misbrug af borgernes digitale tjenester

Inden for det seneste år har 13% af danskerne oplevet, at uvedkommende én eller flere gange har fået adgang til en af deres digitale tjenester, såsom Facebook, Instagram eller mail, og misbrugt den. Det er mere end en fordobling fra de forrige år, hvor kun 6% havde været udsat for denne form for svindel.

Flere oplever virus og skadelig software på deres enheder

Siden 2022 er andelen af danskere, der har været ramt af virus eller skadelige programmer, vokset fra 3% i 2022 til 11% i 2024. Disse angreb resulterer ofte i, at borgerne mister adgang til deres computer, tablet eller smartphone, og i nogle tilfælde fører det til tab af data eller ændringer i deres filer.

Udviklingen i misbrug af tjenester og virus



Note: Andelen af danskere, der har været udsat for hhv. misbrug af tjenester og virusangreb inden for det seneste år. N=1435.

Unge og især unge mænd rammes hyppigere af digital svindel

Unge, og særligt unge mænd, er – som ved de andre svindeltyper – også oftere udsat for indtrængen på deres tjenester og enheder. Den øgede sårbarhed kan hænge sammen med, at unge har en omfattende tilstedeværelse på sociale medier. Den digitale aktivitet gør dem til attraktive mål for svindlere.

Har du mistanke?

Borgere, der har mistanke om, eller har været udsat for, identitetstyveri, kan ringe til Cyberhotline for digital sikkerhed og få hjælp. Cyberhotline har døgnåbent alle årets dage. Ring 33370037

Hvad er identitetstyveri?

Identitetstyveri sker, når en person uberettiget overtager en andens identitet ved at få adgang til følsomme oplysninger som MitID, CPR-nummer eller kodeord. Disse oplysninger kan misbruges til at optage lån, overføre penge eller chikanere. Svindlen opstår ofte som følge af phishing via mail, sms eller telefon, hvor svindlere udgiver sig for at være fra myndigheder eller banker. Det er vigtigt at huske, at banker og offentlige myndigheder aldrig uopfordret vil bede om personlige oplysninger.

Indtrængen på enhed eller tjeneste

Mange danskere handler ikke ved misbrug af tjeneste eller enhed, selvom handling kan gøre en forskel

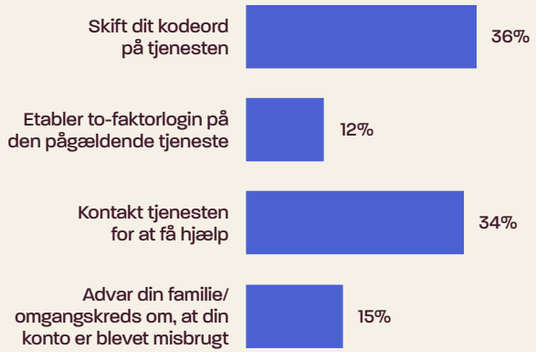
En tredjedel af danskerne følger anbefalinger for misbrug af tjeneste

Flest danskere vælger at skifte kodeord på deres tjeneste eller kontakte tjenesten for at få hjælp. Færre advarer familie og omgangskreds om, at deres konto er blevet misbrugt, og endnu færre etablerer to-trins-login.

Aktiv handling gør en forskel, men få reagerer ved misbrug af deres private tjenester

Selvom mange danskere oplever misbrug af deres digitale tjenester som Facebook, Instagram eller mail, er det kun en mindre del, der tager de anbefalede skridt for at stoppe det. På sikkerdigital.dk findes anbefalinger til at håndtere sådanne situationer. For de danskere, der følger anbefalingerne, undgår 42% yderligere konsekvenser.

Andel, der følger konkrete anbefalinger ved misbrug af tjeneste



Note: Besvarelse for spørgsmålet: Hvad gjorde du den seneste gang, at andre fik adgang til en af dine tjenester og misbrugte den?

Udvalgte svarkategorier vist, n=187, vægtet.

Effektiv reaktion på virusangreb kan forebygge alvorlige økonomiske konsekvenser

Virusangreb kan lamme privatpersoners enheder og få alvorlige konsekvenser for data og økonomi. Selvom en fjerdedel af de berørte vælger at installere antivirus eller anden beskyttelse, og en femtedel søger professionel hjælp, ender 14% af ofrene med at betale løsesum for at genvinde adgang til deres enheder. For dem, der reagerer hurtigt og effektivt, lykkes det 36% at stoppe virusangrebet uden yderligere skade.

35%

har oplevet, at deres tjeneste blev misbrugt til at snyde andre – noget der kan få alvorlige konsekvenser for både ejeren af kontoen og de personer, der snydes

Virusangreb har økonomiske konsekvenser for mange danskere

Virusangreb kan føre til økonomiske konsekvenser, selv når danskerne reagerer hurtigt. Omkring 27% af de ramte ender med at betale en løsesum, mens 29% vælger at investere i en ny enhed, når skaden er uoprettelig.

Hvad er en kreditadvarsel?

Hvis man har mistanke om identitetstyveri, kan man oprette en kreditadvarsel, som er en markering i CPR-registret, der advarer banker og virksomheder om at være ekstra opmærksomme på identitetskontrol, før de yder lån eller kredit. Denne beskyttelse benyttes ofte, når der er risiko for identitetsmisbrug, fx ved mistet pas eller kørekort. 40% af de danskere, der har oplevet konsekvenser af digital svindel, opretter en kreditadvarsel.

Indtrængen på enhed eller tjeneste

Danskerne ændrer ikke nødvendigvis adfærd ved sikring af enhed og tjeneste som følge af erfaringer med svindel

Ikke alle ændrer deres digitale sikkerhedsrutiner efter at have oplevet digital svindel

Personer, der har været udsat for digital svindel, undlader oftere at aktivere automatiske opdateringer på deres enheder. Dette efterlader dem mere sårbare over for fremtidige angreb, da disse opdateringer ofte indeholder kritiske sikkerhedsrettelser.

Til gengæld ses en mere sikker adfærd i forhold til brug af stærke kodeord og to-trins-login. 50% af dem, der har oplevet konsekvenser af svindel, anvender kodeord med over 12 tegn, mod 39% blandt dem, der kun har oplevet svindelforsøg. Den samme tendens gælder for to-trins-login, hvor oplevelsen af svindel ser ud til at motivere til øget digital sikkerhed.

Øget sårbarhed blandt danskerne

Flere anbefalinger til sikker digital adfærd kan forebygge svindel gennem virusangreb, men mange danskere følger dem ikke konsekvent. Færre end to tredjedele af danskerne følger anbefalingen om at beskytte deres computer med et antivirusprogram – et fald på 13% siden 2022. Den faldende tendens kan øge risikoen for digital svindel og understreger behovet for fortsat fokus på digital sikkerhed. Når man rammes af virusangreb, bliver antivirusprogrammet dog relevant. Her er det 28%, som får den fjernet virussen med antivirusprogrammet.

61%

af danskerne følger i høj eller meget høj grad anbefalingen om at beskytte deres computer med et antivirusprogram.

54%

af danskerne følger ikke anbefalingen om at bruge passwordmanager – det er ellers en god løsning til at holde styr på komplekse kodeord

Gode råd til at holde din computer fri for virus

1. Installér et antivirusprogram
2. Pas på med gratis USB-ladere på offentlige steder
3. Tænk dig om, inden du klikker på et link
4. Opdatér dine programmer

Find andre gode råd på sikkerdigital.dk

2. Offentligt ansattes informations-sikkerhed

Aktuelle trusler for offentligt ansatte

Mange offentligt ansatte møder forsøg på digital kriminalitet i deres arbejde

Ansatte i offentlige selskaber og i staten møder oftere digital kriminalitet end i andre delsektorer

Halvdelen af de offentligt ansatte har mødt én eller flere former for digital kriminalitet, som f.eks. phishing, malware-angreb, identitetstyveri og ransomware-angreb. Det dækker dog over markante forskelle afhængigt af delsektor. Mere end to tredjedele af ansatte i offentlige selskaber og staten har mødt digital kriminalitet, mens det samme gælder for under halvdelen af ansatte i regioner og kommuner. Forskellen betyder ikke nødvendigvis, at ansatte i regioner og kommuner ikke er i lige så høj risiko for digital kriminalitet. I offentlige selskaber og i staten kan den højere andel skyldes, at de ansatte her tilbringer en større del af arbejdsdagen foran en computer, hvilket øger eksponeringen og dermed risikoen for at møde digital kriminalitet.

Phishing er den form for digitale svindel, som flest offentligt ansatte møder

Ligesom for borgerne er phishing den mest udbredte digitale svindel blandt de offentligt ansatte. Næsten halvdelen har modtaget et link på mail, sms eller chat-besked fra en ukendt afsender, som opfordrede dem til at trykke på linket. Phishing kan være indgang til andre typer af digital kriminalitet, hvilket skaber et vist overlap mellem trusselformerne.

Andelen, der har mødt digital kriminalitet

71% af ansatte i offentlige selskaber

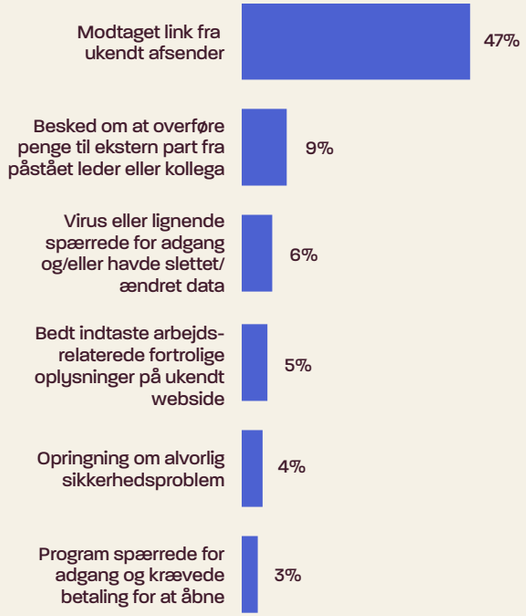
69% af ansatte i staten

44% af ansatte i regionerne

41% af ansatte i kommunerne

Offentligt ansatte omfatter medarbejdere i offentlig forvaltning, service og offentlige selskaber. Forvaltning og service opdeles i tre sektorer: stat, regioner og kommuner. Offentlige selskaber inkluderer fx DSB, Ørsted og kommunale forsyningsvirksomheder, der sælger markedsmæssige ydelser.

Typer af digital kriminalitet, offentligt ansatte har mødt i deres arbejde indenfor det seneste år



Note: N=1.019 Udvalgte svarkategorier vist, n=187, vægtet.

Information og undervisning

Færre offentligt ansatte modtager information og undervisning i informationssikkerhed

En fjerdedel af de offentligt ansatte mangler undervisning i informationssikkerhed

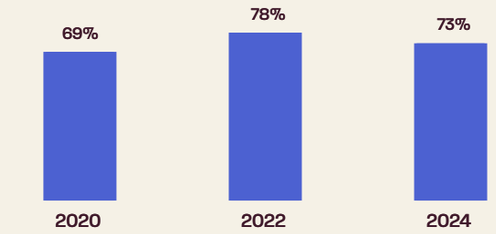
73% af de offentligt ansatte har modtaget undervisning eller information om politikker og/eller retningslinjer for informationssikkerhed på deres arbejdsplads, mens 18% ikke har modtaget information eller undervisning. 9% kan ikke huske, om de har fået undervisning. Andelen, der har fået undervisning, er faldet med 5 procentpoint siden 2022, men ligger fortsat over 2020-niveau på 69%.

Der er således stadig en fjerdedel af de offentligt ansatte uden et opdateret informationsgrundlag for at handle i overensstemmelse med arbejdspladsens sikkerhedspolitik. Dette kan udfordre en ensartet tilgang til informationssikkerhed og påvirke den offentlige sektors modstandsdygtighed mod digitale angreb.

Variation i undervisning på tværs af delsektorer

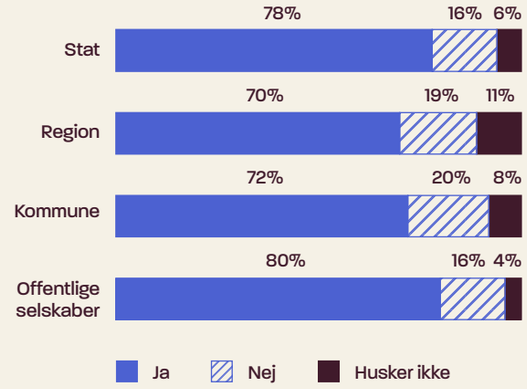
Den største andel af ansatte uden undervisning findes i regioner og kommuner, hvor hhv. 19% og 20% ikke har modtaget undervisning eller træning. Udfordringen gør sig dog også gældende i staten og offentlige selskaber.

Udvikling i andelen af offentligt ansatte, der har modtaget undervisning/ information i arbejdspladsens retningslinjer



Note: N = 1.019 (2024), 1.030 (2022) og 1.030 (2020).

Andel ansatte, der har modtaget undervisning/information i arbejdspladsens retningslinjer



Note: N=1.019.

Undervisning styrker de ansattes oplevelse af deres digitale adfærd

64% af offentligt ansatte, der har modtaget undervisning om informationssikkerhed, svarer, at deres digitale adfærd er sikker. Det gælder kun for 36% af dem, der ikke har fået undervisning.

Undervisning i arbejdsstedets retningslinjer betyder ikke, at de altid følges

12% af dem, der har modtaget undervisning, bryder nogle gange retningslinjerne – og 9% er usikre på, om de bryder dem. Det er en kilde til sårbarhed, at en gruppe ansatte bevidst eller ubevidst undlader at følge retningslinjerne. Særligt udfordrende er det, at 9% finder retningslinjerne så uklare, at de – trods undervisning – ikke ved, om de efterlever dem.

Kendskab til retningslinjer

Mange offentligt ansatte kender sikkerhedspolitikkerne, men der er stadig plads til forbedring

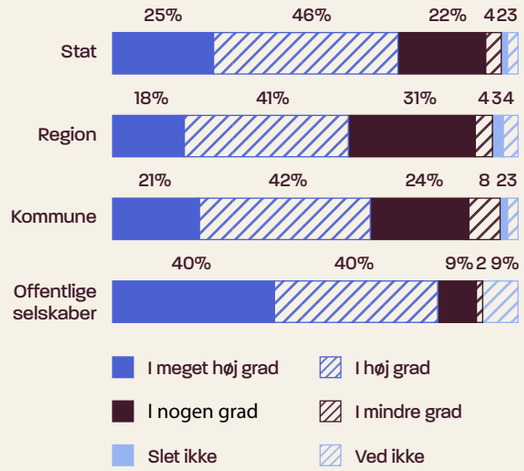
Størstedelen af de offentligt ansatte har et vist kendskab til arbejdsstedets sikkerhedspolitikker

89% af offentligt ansatte har kendskab til de gældende sikkerhedspolitikker på deres arbejde enten i nogen grad, i høj grad eller i meget høj grad. Der er dog stor variation på tværs af delsektorer, hvor en større andel i regionerne kun i nogen grad har kendskab til retningslinjerne (31%). På trods af et stabilt højt niveau af kendskab til politikkerne, er der sket et mindre fald siden 2022 på 3 procentpoint.

Undervisning har mærkbar betydning for kendskab

Blandt de ansatte i den offentlige sektor, der har modtaget undervisning eller information om arbejdspladsens sikkerhedspolitikker, vurderer 77%, at de i høj eller meget høj grad har kendskab til retningslinjerne. Også blandt de ansatte, der ikke har modtaget undervisning, mener mange at kende retningslinjerne. Selvom tallet er væsentligt lavere, er det fortsat 32%, der vurderer, at de i høj eller meget høj grad kender retningslinjerne.

Kendskab til arbejdspladsens informationspolitikker og/eller -retningslinjer



Note: N=1.019.

11%

undlader nogle gange at følge retningslinjerne på arbejdspladsen

13%

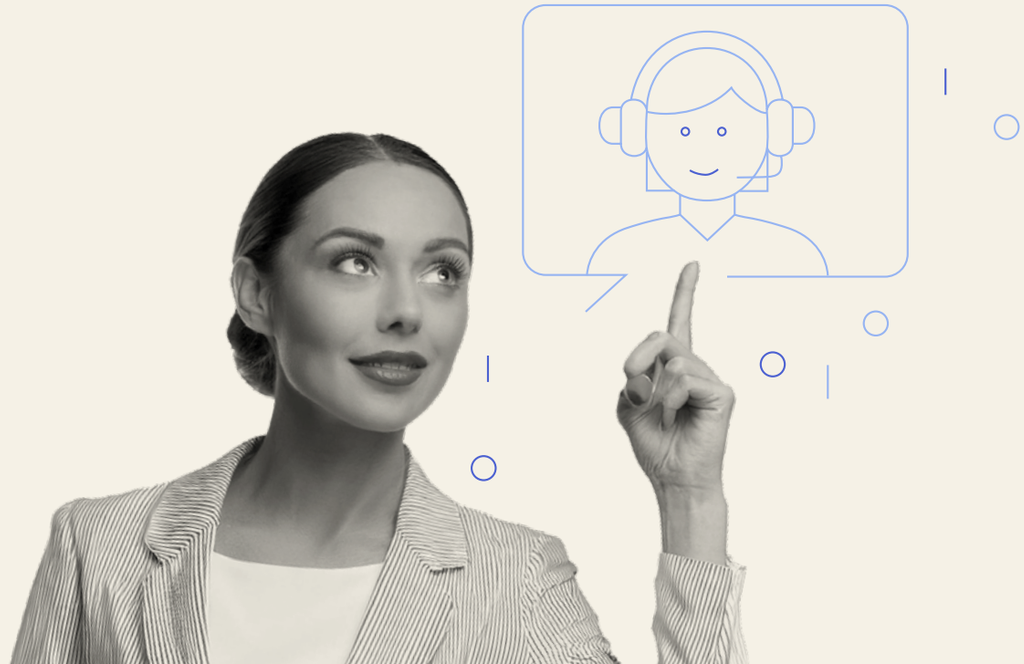
ved ikke, om de efterlever retningslinjerne

Nogle offentligt ansatte tilsidesætter jævnligt retningslinjerne

Selvom mange offentligt ansatte er bekendt med retningslinjerne, efterlever de dem ikke altid. Blandt dem, der til tider undlader at følge retningslinjerne, gør 50% det mindst en gang om måneden, og 22% bryder arbejdspladsens retningslinjer på ugentlig basis.

87% svarer ja til: "Ved du, hvem du skal kontakte på din arbejdsplads i forhold til informationssikkerhed?"

Note: N=1.019.



Offentligt ansattes bevidsthed om digitale trusler

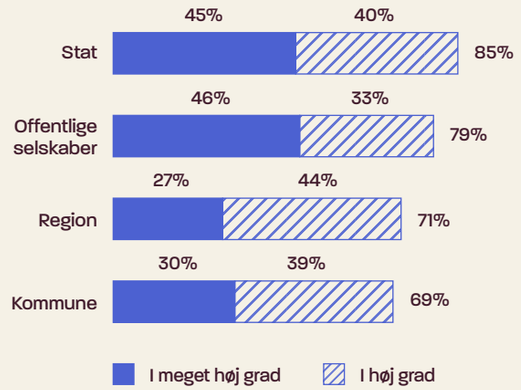
Der er udbredt opmærksomhed på digital kriminalitet blandt offentligt ansatte

Offentligt ansatte er opmærksomme på digital kriminalitet

Størstedelen af offentligt ansatte er bevidste om risikoen for bedrageri og digital kriminalitet på internettet. Kun 3% rapporterer, at de slet ikke er opmærksomme på trusler udefra. En større andel af ansatte i offentlige selskaber og staten er særligt opmærksomme på disse trusler, hvilket afspejler deres højere eksponering og større antal registrerede angreb i disse sektorer.

Større eksponering fører til højere opmærksomhed
Der er en klar sammenhæng mellem oplevet trusselniveau og opmærksomheden på digital kriminalitet: Jo oftere offentligt ansatte møder trusler i deres hverdag, desto højere er deres opmærksomhed omkring cybersikkerhed. Siden 2022 er opmærksomheden dog faldet en smule og er nu på niveau med 2020. Det fald kan muligvis hænge sammen med færre registrerede phishing-forsøg i 2024 sammenlignet med 2022, hvor en større andel oplevede forsøg på bedrageri.

Offentligt ansattes opmærksomhed på bedrageri og digital kriminalitet på internettet



Note: N=1.019.

Undervisning skærper opmærksomheden på sikkerhedstrusler

80% af de offentligt ansatte, der har modtaget information om eller undervisning i arbejdspladsens retningslinjer, er i høj eller meget høj grad opmærksomme på sikkerhedstrusler. Det gælder kun for 53% af de ansatte, som kan huske, at de ikke har modtaget undervisning.

Barrierer for den gode digitale adfærd

Offentligt ansatte forstår retningslinjerne, men synes, de er besværlige og glemmer at følge dem

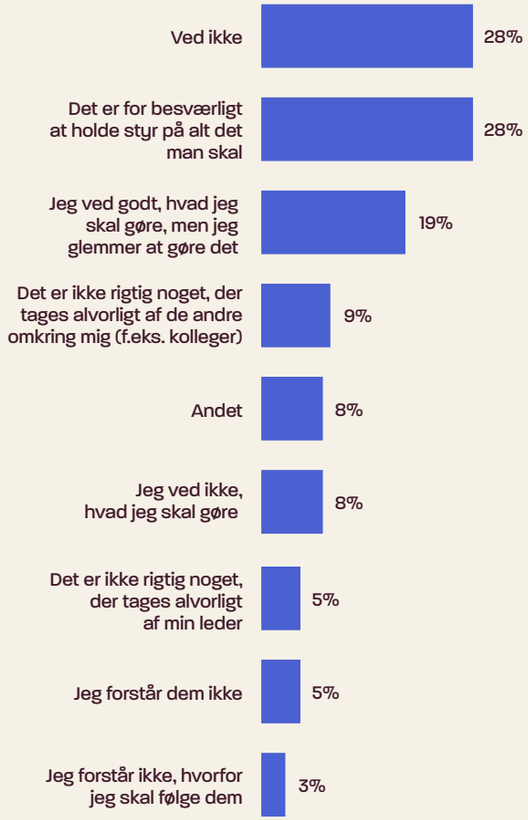
Fortsat svært at overføre retningslinjer til praksis

43% af de offentligt ansatte oplever fortsat barrierer for at følge sikkerhedspolitikkerne på deres arbejdsplads. Barrierne opleves særligt af de yngre ansatte og omhandler særligt, hvordan de overholdes i praksis snarere end problemer med at forstå dem.

Retningslinjerne er besværlige at holde styr på og glemmes nemt

Det er et fåtal af de offentligt ansatte, som ikke forstår retningslinjerne, eller hvorfor de skal følge dem. Barrierne ligger i at få inkorporeret den gode digitale adfærd i sin arbejdsdag, da mere end hver fjerde oplever det som besværligt at holde styr på, mens en femtedel glemmer at gøre det, de ved, de burde gøre.

Barrierer for at følge arbejdspladsens informationssikkerhedspolitikker og/eller -retningslinjer



Note: N=430, frasorteret de offentligt ansatte, som ingen barrierer oplever.

Undervisning i informationssikkerhed har betydning for medarbejdernes vurdering af deres adfærd

64% af offentligt ansatte, der har modtaget undervisning eller information om retningslinjer, oplever ingen barrierer. Det gælder kun for 36% af dem, der ikke har modtaget undervisning eller information. Blandt de ansatte, der vurderer deres adfærd som sikker, har 11% ikke modtaget undervisning. Det må betyde, at de får deres viden om informationssikkerhed andetsteds fra, men kan også dække over en mangel på viden om, hvad man ikke ved.

57% af de offentligt ansatte mener selv, at de har en sikker digital adfærd og oplever ingen barrierer

Det er særligt blandt statsligt ansatte og ansatte i offentlige selskaber, at der er flere, der ingen barrierer oplever. Alder er en markant faktor her, hvor flere end to tredjedele af ansatte over 50 år oplever deres adfærd som sikker, mens det er gældende for 38% af ansatte mellem 18-29 år og 44% af ansatte mellem 30-39 år.

Status på den gode sikkerhedsadfærd – adgangskoder

Smuthuller i sikkerheden: offentligt ansattes adgangs-kodevaner under pres

Gentagen brug af adgangskoder udfordrer

Der er steder, hvor de offentligt ansatte tager smuthuller, som kompromitterer deres digitale sikkerhed. Det er bl.a. ved brug af samme login, hvor 26% af offentligt ansatte bruger samme login til flere systemer/tjenester.

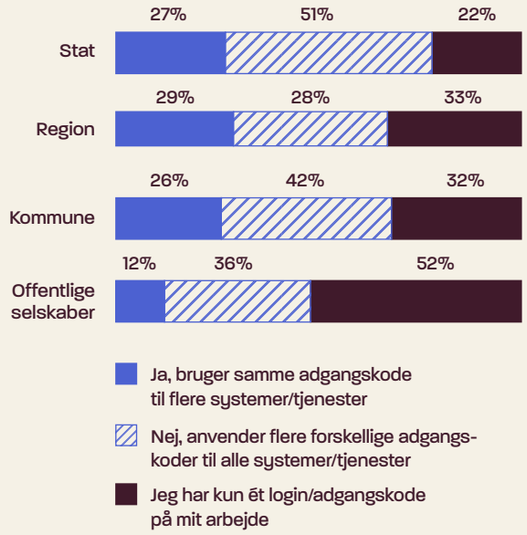
Mange offentligt ansatte bruger samme koder privat og professionelt

23% af offentligt ansatte bruger ét eller flere steder samme koder på arbejde som i deres privatliv. De offentligt ansatte, som har fået undervisning, er kun en smule bedre til at adskille kodeord privat og professionelt (8 procentpoint). Når man bruger de samme adgangskoder både privat og på arbejde, øger det risikoen for sikkerhedsbrud. Hvis et digitalt angreb kompromitterer en arbejdskonto, kan det også true den personlige sikkerhed, såfremt de samme adgangskoder anvendes. Ligeledes kan et angreb i privatlivet potentielt skade sikkerheden på arbejdspladsen, hvis adgangskoderne er de samme.

Anbefalinger til adgangskoder følges ikke af alle

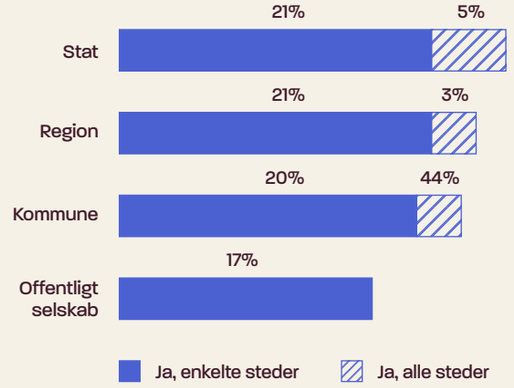
Der er flere anbefalinger, som skal hjælpe organisationer til en hensigtsmæssig politik omkring adgangskoder. Her er det en anbefaling at bruge en passwordmanager til at holde styr på de forskellige adgangskoder. Det er et fåtal af offentligt ansatte (18%), som bruger passwordmanager. Det er dog en stigning på 7 procentpoint siden 2022.

Andel, der bruger samme adgangskode til flere systemer/tjenester i deres job



Note: N=1019.

Andel, der bruger samme adgangskoder privat og professionelt



Note: N=1019.

Anbefalinger til styring af kodeordssikkerhed i myndigheder og organisationer

- Undgå unødigt komplicerede passwordregler – sigt efter god længde og lavere kompleksitet.
- Benyt tvunget passwordskift, hvis der findes tegn på eller mistanke om kompromittering.
- Anvend single sign-on for at gøre det nemt for brugerne at tilgå organisationens systemer.
- Anvend flerfaktor-autentifikation på al fjernadgang og alle privilegerede konti.
- Hav en negativliste for at forhindre brug af ofte anvendte passwords.
- Hjælp brugerne til sikker håndtering af passwords gennem regelmæssige awareness-tiltag.

Kilde: CFCS 2023 https://www.cfcs.dk/da/forebyggelse/vejledninger/passwords/

Status på den gode sikkerhedsadfærd – håndtering af fortrolige dokumenter

Offentligt ansatte reagerer på sikkerhedsbrud med fortrolige dokumenter

Offentligt ansatte handler, når de finder dokumenter med fortrolige oplysninger

Hovedparten af de offentligt ansatte, uafhængigt af delsektor, handler, når de oplever sikkerheds-brud i form af fejlplacerede dokumenter. Kun 3% smider dem i papirkurven, og 2% lader dem være. I stedet følger de offentligt ansatte i høj grad retningslinjerne på området og makulerer eller flytter dokumenterne, så de ikke længere ligger udsat.

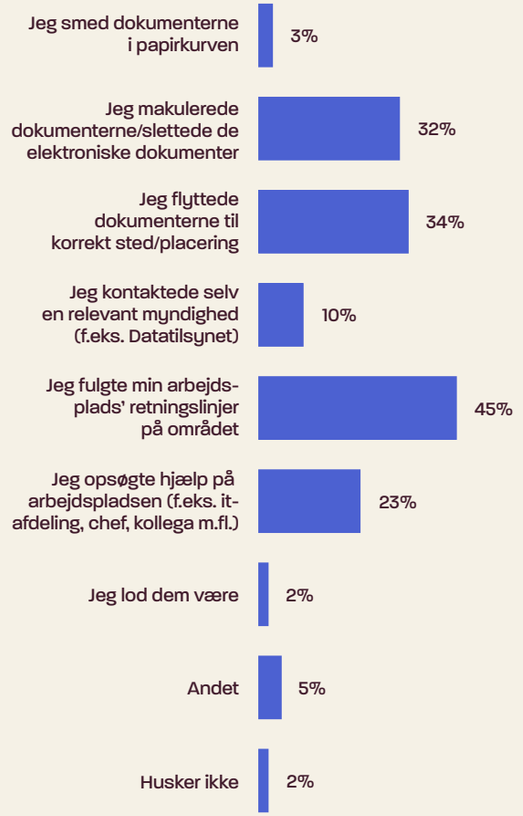
Fremgang i efterlevelse af retningslinjer

45% følger arbejdspladsens retningslinjer, når de finder fejlplacerede dokumenter. Det er en stigning på 10 procentpoint fra 2022.

20%

af offentligt ansatte, som nogle gange arbejder hjemme, bryder gældende GDPR-regler og har fortrolige oplysninger liggende hjemme (fx borgeres CPR-numre, navn eller adresse)

Håndtering af fortrolige dokumenter, der var placeret forkert

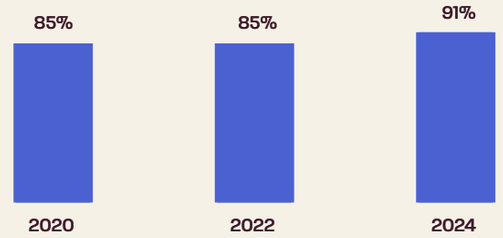


Note: Spørgsmål: Hvad gjorde du den seneste gang, du fandt dokumenter med arbejdsrelaterede fortrolige oplysninger, der var placeret et forkert sted? N=234, vægtet.

Flere offentligt ansatte sender fortrolige oplysninger via krypteret mail

Blandt de offentligt ansatte, der sender arbejds-relaterede fortrolige dokumenter, sender største-delen (91%) oplysningerne via krypteret mail. Det er en stigning på 6 procentpoint siden 2022. De er bedre i kommunerne (91%) end i staten (85%) og regionerne (81%) til at anvende krypteret mail. Alle ansatte i offentlige selskaber anvender sikker mail til at sende fortrolige oplysninger.

Andelen af arbejdsrelaterede fortrolige oplysninger sendt via krypteret mail



Note: N=286, vægtet.

Status på den gode sikkerhedsadfærd – fysiske og digitale foranstaltninger

Flere offentligt ansatte bruger arbejdsmailen privat, men holder privat mail ude af jobbet

De offentligt ansatte har flere foranstaltninger til at hjælpe dem med sikker digital adfærd

Foranstaltninger kan være en del af det fysiske setup af deres arbejdsstation og digitale løsninger som styresystemer og fildelingstjenester.

Beskeden fremgang i brugen af diskretionsskærme

Udviklingen i brugen af fysiske og digitale foranstaltninger er begrænset. Omkring to tredjedele låser altid deres skærm, når de forlader deres arbejdscomputer – et tal som ikke er i forbedring. Få (11%) bruger diskretionsskærm, når de arbejder andre steder end deres almindelige arbejdsplads. Det er dog næsten en fordobling siden 2022.

Stagnation i udbredelsen af sikker print og programopdateringer på offentlige arbejdspladser

To tredjedele har gennem deres arbejdsplads muligheden for "sikker print"-løsningen, hvor man bruger sit adgangskort eller en kode for at printe. Denne løsning er ikke blevet mere udbredt siden 2022 på trods af, at den fungerer som foranstaltning for sikker dokumentpraksis. Størstedelen opdaterer jævnligt programmer på deres arbejdscomputer, men tallet er faldet 3 procentpoint siden 2022. Det er fortsat få offentligt ansatte, der benytter fildelingstjenester i forbindelse med deres arbejde.

63% låser altid deres skærm

65% kan anvende "sikker print"

11% bruger diskretionsskærm

88% opdaterer styresystemer

22% anvender fildelingstjenester

Fordobling af offentligt ansatte, der bruger deres arbejdsmail til at sende private mails

Der er sket en bemærkelsesværdig udvikling i brugen af arbejdsmail og privat mail. Andelen af offentligt ansatte, der anvender deres arbejdsmail til private formål, er steget fra 21% i 2022 til 44% i 2024.

Stort fald i offentligt ansatte, der bruger privat mail til arbejdsformål

Omvendt er brug af privat mail til arbejdsformål faldet fra 44% i 2022 til 11% i 2024. En medvirkende forklaringsfaktor kan være det skærpede fokus på de gældende GDPR-regler og klarere retningslinjer for, hvornår og hvordan private konti må benyttes i arbejdsrelaterede sammenhænge.

44%

af de offentligt ansatte bruger deres arbejdsmail til private formål

Status på den gode sikkerhedsadfærd – hjemmearbejde

Offentligt ansatte føler sig godt klædt på til hjemmearbejde

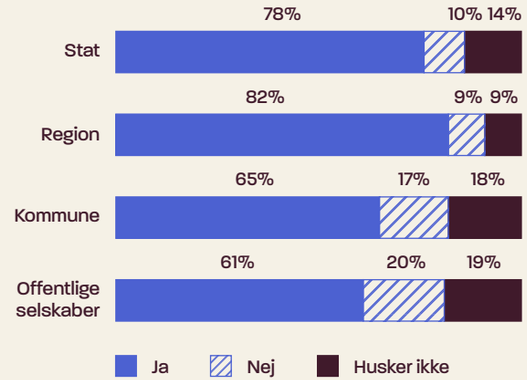
Ikke alle har, eller ved om de har, retningslinjer for informationssikkerhed, når de arbejder hjemme

Mere end halvdelen af de offentligt ansatte (54%) arbejder nogle gange hjemmefra. Det sker mest i staten og mindst i regionerne. Det til trods er der flest i regionerne (82%), som ved, at de har retningslinjer for informationssikkerhed ved hjemmearbejde. Næsten en tredjedel på tværs af delsektorer har ikke, eller ved ikke, om de har retningslinjer ved hjemmearbejde. Flest i offentlige selskaber og kommuner har ikke retningslinjer ved hjemmearbejde.

Offentligt ansatte føler sig godt klædt på til at arbejde hjemme

Størstedelen af de offentligt ansatte føler sig godt eller meget godt klædt på til at arbejde hjemmefra eller fra et andet sted end deres normale arbejdsplads. Der er ikke markante forskelle mellem delsektorer. Blandt kommunalt ansatte er der dog flere, som føler sig hverken godt eller dårligt klædt på (18% mod et gennemsnit på 14% for den samlede gruppe af offentligt ansatte).

Har arbejdspladsen retningslinjer for hjemmearbejde, fx ved håndtering af informationer og brug af udstyr?



Note: N=554, vægtet.

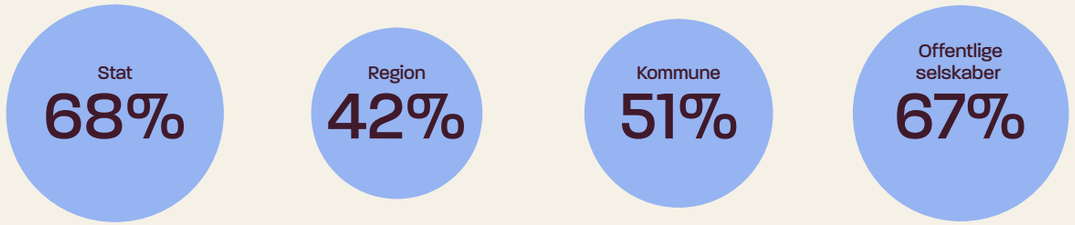
Høj netværkssikkerhed blandt offentligt ansatte ved hjemmearbejde

Offentligt ansatte benytter forskellige metoder for at sikre informationssikkerheden, når de arbejder uden for deres faste arbejdssted. Halvdelen af de offentligt ansatte (51%) arbejder på et privat, sikret netværk med kode, mens 39% bruger VPN-forbindelser, hvilket understøtter en høj grad af netværkssikkerhed. Kun 1% anvender åbne netværk til arbejdsformål.

Stigende brug af arbejdscomputer ved hjemmearbejde

Andelen af offentligt ansatte, der arbejder på private computere, er faldet fra 16% i 2022 til 12% i 2024.

Andelen af offentligt ansatte, der nogle gange arbejder hjemme, fordelt på delsektor



Truslen fra phishing og andre ondsindede henvendelser

Offentligt ansatte kender truslen fra phishing, men nye metoder kan udfordre informationssikkerheden

Phishing er fortsat den trussel, flest offentligt ansatte møder

Som hos borgerne er phishing også en udbredt trussel blandt offentligt ansatte. Omkring halvdelen af offentligt ansatte har oplevet at modtage et link fra en ukendt afsender med opfordring om at trykke herpå. Andelen, der udsættes for denne trussel, er dog faldet en smule de seneste to år.

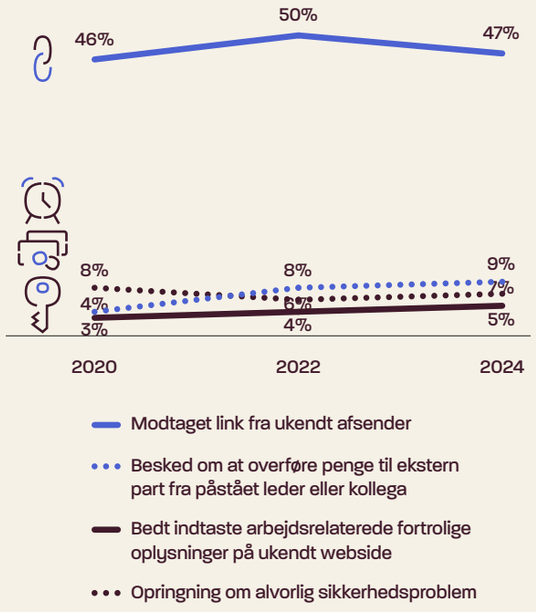
Offentligt ansatte udviser forsigtighed over for phishing, men få deler aktivt advarsler

Selvom mange offentligt ansatte modtager phishing-links, er det kun en meget lille andel, der klikker på dem (1%). Størstedelen forholder sig passivt til truslen og sletter beskeden (73%). Kun en mindre gruppe går et skridt videre og advarer kollegaer (32%) eller søger hjælp på arbejdspladsen (13%).

Nye ondsindede henvendelser vinder frem, og de er sværere at gennemskue for de ansatte

De tre øvrige former for ondsindede henvendelser er fortsat mindre udbredte, men flere er dog i vækst. Størst her er CEO-fraud, hvor de offentligt ansatte modtager en besked fra en afsender, som udgiver sig for at være deres leder eller kollega, og som beder om, at man overfører penge til ekstern part. 9% møder denne trussel. Heraf er det 4%, som ender med at overføre penge.

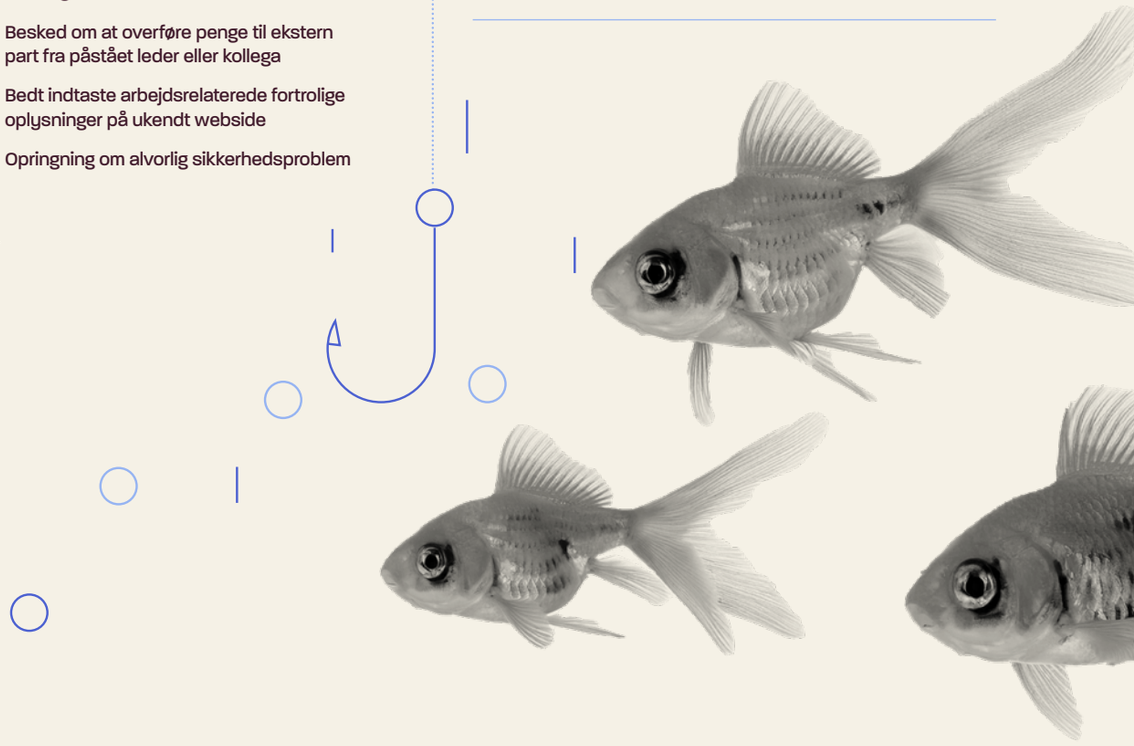
Udvikling i phishing og andre ondsindede henvendelser



Note: N=1.019.

Hvad er **CEO-fraud?**

Ved CEO-fraud modtager en medarbejder en besked, hvor afsenderen udgiver sig for at være en kollega eller leder og beder dem overføre penge til en ekstern part. Medarbejderen sidder ofte i en funktion med adgang til at håndtere penge og presses til at springe normale kontrolprocedurer over. Svindleren får derved pengene overført uden de sædvanlige sikkerhedstjek.



Truslen fra virus og ransomware

Flere offentligt ansatte oplever virus- og ransomware-angreb på arbejdspladsen

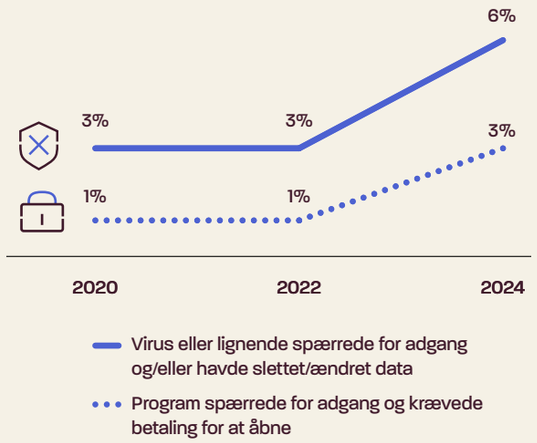
Virus og ransomware vokser frem på arbejdspladsen

På trods af at tilfældene fortsat er relativt få, møder flere end tidligere virus eller ransomware i deres arbejde. Med en stigning på 3 procentpoint er det nu 6% af de offentligt ansatte, der rammes af virus eller anden malware, der spærrer for adgangen til deres enheder og sletter eller ændrer i deres data, mens 3% oplever ransomware.

Mange håndterer ransomware ved at inddrage deres arbejdsplads

Når de offentligt ansatte møder ransomware, er det få, der intet foretager sig (3%). I stedet opsøger omkring halvdelen hjælp på arbejdspladsen, og en tredjedel advarer deres arbejdskollegaer.

Udvikling i virus og ransomware



Note: N=1.019.

47%

søger hjælp på arbejdspladsen, når de møder ransomware

21%

løser selv problemet, når de møder en virus

33%

advarer deres kollegaer, når de møder en virus

Hvad er ransomware?

Ransomware er en type online angreb, hvor it-kriminelle afpresser deres offer – typisk en virksomhed – ved at inficere deres system med malware. Det sker ofte ved, at en medarbejder kommer til at åbne en ondsindet fil eller link. Malwaren krypterer alle tilgængelige data, så de ikke kan tilgås. Herefter kræver angriberne løsepenge for at låse dataene op – deraf navnet ransomware.

Metode

Datagrundlag

Analysen af danskernes informationssikkerhed 2024 bygger på et datagrundlag fra to større spørgeskemaundersøgelser. Det ene spørgeskema er udsendt til borgere og er 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 tilsvarende repræsentativt udsnit af offentligt ansatte i Danmark, ligeledes fra 18 år og opefter. Alle data i undersøgelsen er selvangivet og afspejler respondenternes egen oplevelse.

Dataindsamlingen blev gennemført af analysevirksomheden Verian i perioden fra 6. august til 3. september 2024. I alt er der indsamlet svar fra 2.454 respondenter, fordelt på 1.435 borgere og 1.019 offentligt ansatte. Målet var at opnå minimum 1.000 besvarelser i hver målgruppe for at sikre tilstrækkelig statistisk sikkerhed i resultaterne.

Der er generelt taget højde for at undgå små tal. For at skabe troværdighed i besvarelserne har respondenterne deltaget anonymt i spørgeskemaundersøgelsen.

Dataindsamling

Spørgeskemaundersøgelserne blev gennemført blandt medlemmer af GallupForum-panelet, og datamaterialet blev vægtet for at sikre repræsentativitet i forhold til den samlede danske befolkning. For at sikre høj repræsentativitet blev dataindsamlingen gennemført i flere rul, hvilket sikrede et repræsentativt datasæt, der afspejler befolkningens sammensætning.

Datamaterialet for borgere er vægtet efter køn, alder og geografi i overensstemmelse med den aktuelle fordeling i Danmarks voksne befolkning, baseret på oplysninger fra Danmarks Statistik. For de offentligt ansatte er materialet vægtet efter sektor (stat, region, kommune og offentlige selskaber), geografi (arbejdsstedsregion) samt alder i forhold til fordelingen blandt offentligt ansatte i Danmark.

Databehandling og fortolkning af resultater

Analysen og fortolkningen af data er udarbejdet af Pluss Leadership. Spørgeskemaet er en gentagelse af undersøgelserne fra 2022 og 2020, hvor ordlyd og svarmuligheder er bibeholdt med få undtagelser, så resultaterne kan sammenlignes på tværs af årene. Udviklingen fra tidligere undersøgelser er flere steder inddraget for at vise, hvordan danskernes informationssikkerhed ændrer sig over tid.

Rapporten har desuden et udvidet fokus på, hvordan borgere og offentligt ansatte håndterer cybersikkerhedsrisici, samt hvilke forudsætninger og motivationer de har for at beskytte egne og andres data mod digitale angreb.

Sammenlignelighed med tidligere undersøgelser

Undersøgelsen indgår i en serie af analyser af danskernes informationssikkerhed, som er gennemført omtrent hvert andet år fra 2013 til 2022. Borgere har været i fokus for alle undersøgelserne, mens offentligt ansatte blev inkluderet i undersøgelsen fra 2016. Tidligere resultater er inddraget i rapporten, hvor det er relevant, for at muliggøre sammenligning af udviklingen. Hvis der ikke forekommer en sammenligning i rapporten, skyldes det, at spørgsmålet eller spørgsmålskategorierne er tilpasset.

Øvrige datakilder

Foruden spørgeskemaerne inddrager undersøgelsen også sekundære datakilder til at afdække danskernes informationssikkerhed. Hensigten med det 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.

Der er desuden inddraget indsigter fra politiet, som har bidraget med viden om digital kriminalitet og det generelle trusselbillede i Danmark. Det har særligt været brugt som supplerende viden om de kriminelles fremgangsmetoder, hvilke råd danskerne bør følge, samt hvor der særligt er behov for at sætte ind for at ruste danskernes informationssikkerhed.

Få mere information

Styrelsen for Samfundssikkerhed
samsik.dk

Danske Regioner
regioner.dk

KL
kl.dk

Danskernes informationssikkerhed 2024

Design: BGRAPHIC

ISBN: 978-87-85344-00-7