DA ANALYSE

MARTS 2025

DIGITALISERING OG AI

Privacy og datasikkerhed 2025

Delanalyse 1: It-sikkerhed og -kriminalitet

Indhold

Analysens hovedresultater

Analysen viser, at sikkerhedsniveauet blandt den danske befolkning ikke har ændret sig meget siden 2023. Kun 6 procent af befolkningen følger 7-8 af de anbefalede sikkerhedsforanstaltninger og har dermed et højt sikkerhedsniveau, mens 35 procent følger 0-2 af anbefalingerne og har et meget lavt sikkerhedsniveau.

Hovedparten af befolkningen, 63 procent, bruger nogle af deres passwords flere steder eller det samme password til alle deres enheder og tjenester. Desuden skifter 63 procent ikke deres vigtigste passwords jævnligt, og 28 procent har ikke to-faktor godkendelse på deres vigtigste passwords. Analysen viser også, at 70 procent af befolkningen har hjulpet andre med digitale løsninger, og 45 procent af dem har fået indsigt i et eller flere passwords fra den person, de har hjulpet.

Desuden bruger 64 procent af befolkningen "husk-mig"-funktionen som loginmetode enten *altid, ofte* eller *af og til*. Selvom det kan være bekvemt, er der sikkerhedsrisici forbundet med "husk-mig"-funktionen. Hvis nogen får adgang til ens enhed, kan de også få adgang til de steder, hvor man bruger funktionen, og dermed få indsigt i følsomme oplysninger som fx bankoplysninger. Derudover er disse cookies eftertragtede for hackere, da de kan anvendes til at hacke e-mailkonti. For at beskytte sig mod denne type angreb anbefales det at slette cookies regelmæssigt. Analysen viser, at 13 procent af dem, der bruger "husk-mig"-funktionen *altid, ofte* eller *af og til*, sletter cookies eller browserdata på ugebasis.

Analysen viser også, at 58 procent af befolkningen har IoT-enheder i hjemmet, hvoraf 38 procent enten *slet ikke* eller *i ringe grad* forholder sig til, om deres IoT-enheder er sikret mod angreb udefra. Desuden har 55 procent af den danske befolkning været udsat for en eller flere typer af it-kriminalitet indenfor de seneste to år. De mest udbredte former for it-kriminalitet er phishing/smishing, falske konkurrencer og telefonopringninger eller beskeder fra kriminelle, der udgiver sig for at være ens bank. Politiet advarer om, at kriminalitetsformen "bekendt i knibe" er i stigning, hvor analysen viser, at 12 procent har været udsat for det indenfor de seneste to år.

Endelig viser analysen, at 83 procent af befolkningen tager backup af deres vigtigste dokumenter og filer, hvilket er på niveau med tidligere tilsvarende undersøgelser. Cloud er den mest anvendte backup-løsning blandt befolkningen (54 procent), efterfulgt af ekstern harddisk (33 procent). 27 procent bruger mere end én backup-løsning.

Sikkerhed på nettet

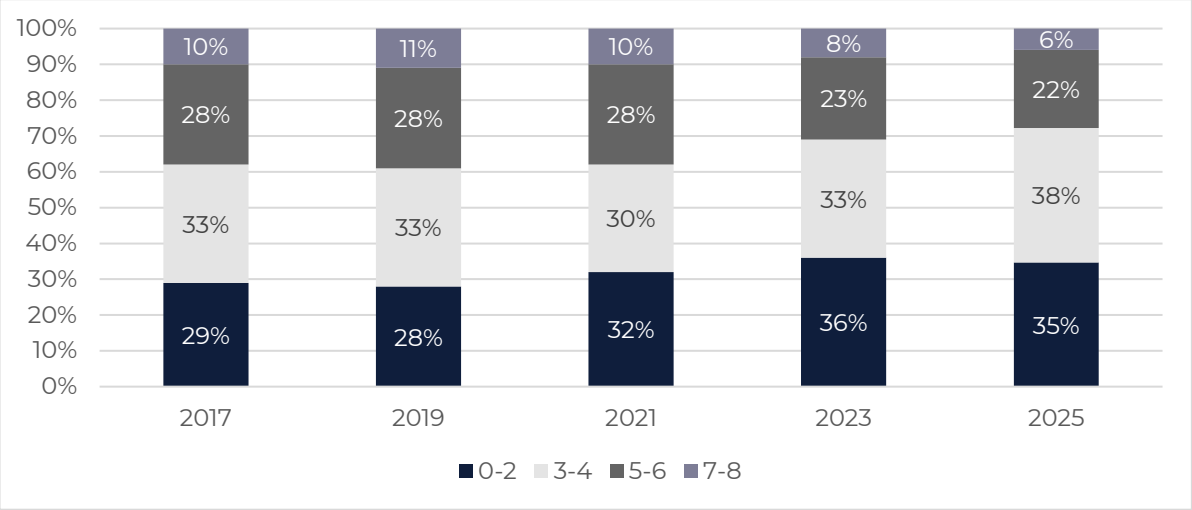
Digitaliseringen har stor betydning for danskernes liv. Vi bruger internettet til fx at kommunikere, være i kontakt med det offentlige, handle og få hjælp fra digitale assistenter. Men digitalisering rejser også spørgsmål om privatliv, data- og it-sikkerhed. It-kriminalitet er et voksende problem, hvor kriminelle konstant bliver dygtigere. Det er svært at undgå virus og malware, og mange oplever datatyveri eller økonomisk bedrageri. Selvom det er udfordrende at beskytte sig fuldstændigt, kan man med forholdsregler gøre det sværere for kriminelle og reducere skaderne.

Vi har i nærværende og tidligere undersøgelser spurgt befolkningen, om de følger nedenstående otte sikkerhedsanbefalinger. Vi har kategoriseret besvarelserne på en skala fra 0-8, baseret på, hvor mange af de otte anbefalinger befolkningen følger. Et højt sikkerhedsniveau svarer til 8, mens et lavt sikkerhedsniveau er 0, hvis man ikke følger nogen af de almindelige sikkerhedsanbefalinger. Indekset er baseret på, hvor mange af udsagnene i bilagstabel 1 respondenterne har svaret henholdsvis "aldrig" eller "altid" til, samt at de har svaret "ja" til, at deres netværk/wifi er beskyttet af en kode, de selv har oprettet, jf. bilagstabel 2.

1. Klik aldrig på links uden at vide, hvor det linker til.
2. Åbn aldrig ukendte vedhæftede filer.
3. Opdater altid antivirusprogrammer på computere og andre enheder til nyeste version.
4. Opdater altid browser på computere og andre enheder til nyeste version.
5. Opdater altid dit styresystem på computere og andre enheder til nyeste version.
6. Brug aldrig åbne netværk på fx cafeer, museer, offentlig transport eller andre lignende steder.
7. Brug aldrig USB-nøgler til flere computere.
8. Brug altid kryptering af hjemmenetværk.

Figur 1 giver et billede af befolkningens samlede sikkerhedsniveau. 6 procent af befolkningen følger 7-8 af anbefalingerne og har dermed et højt sikkerhedsniveau. 22 procent følger 5-6 af anbefalingerne. 38 procent følger 3-4 af anbefalingerne, og 35 procent følger 0-2 af anbefalingerne og har dermed et meget lavt sikkerhedsniveau. Figur 1 viser også, at sikkerhedsniveauet ikke har forandret sig meget, siden undersøgelsen senest blev gennemført i 2023.

Figur 1. Sikkerhedsniveau for beskyttelse af computer og netværk. Fordelt på årstal.



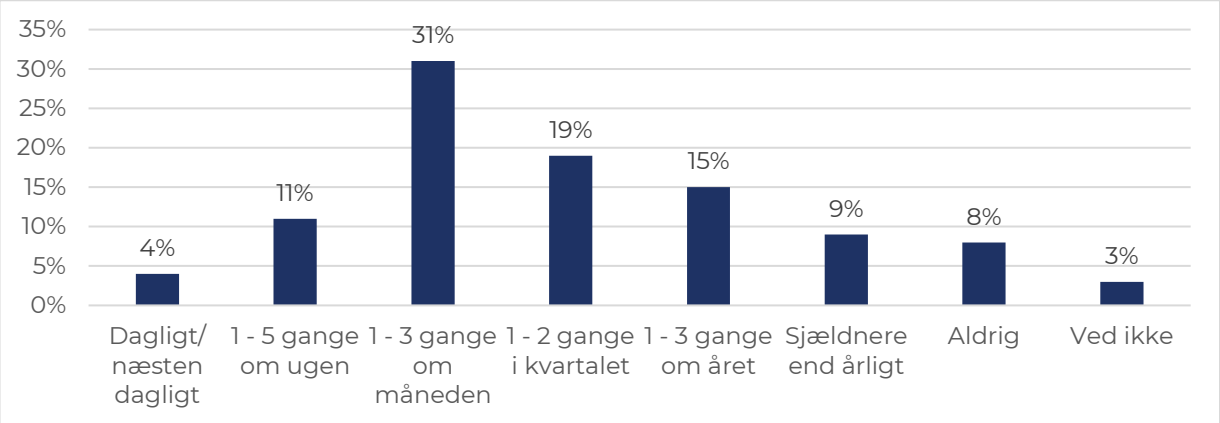
Note: besvarelser=2002.

Selvom brugere af digitale devices følger anbefalingen "klik aldrig på links uden at vide, hvor det linker til", kan brugeren alligevel blive udsat for interaktionsfri og fjernbetjente angreb – også kaldet "zero-click exploits". NSA (National Security Agency)1 har tidligere anbefalet, at man blandt andet kan slukke sin telefon minimum en gang om ugen og slå wi-fi og bluetooth fra, når man ikke bruger det, for at beskytte sig mod angreb2. Figur 3 illustrerer, at 15 procent af befolkningen slukker deres telefon på ugebasis. 13 procent slår altid eller ofte wi-fi fra, og 21 procent slår altid eller ofte bluetooth fra på deres devices, når de ikke bruger det. Det fremgår af figur 4.

Sikkerhedseksperter er delte i deres syn på NSA's anbefaling om at slukke telefonen[3]. At genstarte sin telefon kan have sine fordele, fx er det godt for telefonens batterilevetid[4]. Fra et sikkerhedsperspektiv mener nogle eksperter, at det giver mening at genstarte sin telefon ugentligt, da det kan hjælpe med at reducere risikoen for visse typer angreb, herunder zero-click- exploits, og fjerne de typer malware, der ikke kan overleve en genstart. Andre eksperter mener dog ikke, at det er nødvendigt at genstarte en gang om ugen, da disse typer af angreb er et tilbagevende problem for Apple- og Android-operativsystemer, hvorfor de hurtigt identificeres, og der udgives en ny softwareopdatering, der reducerer truslen. Dertil vil en genstart af sin smartphone ikke beskytte mod mere avancerede angreb, der er designet til at overleve i en smartphone, der slukkes og tændes igen.

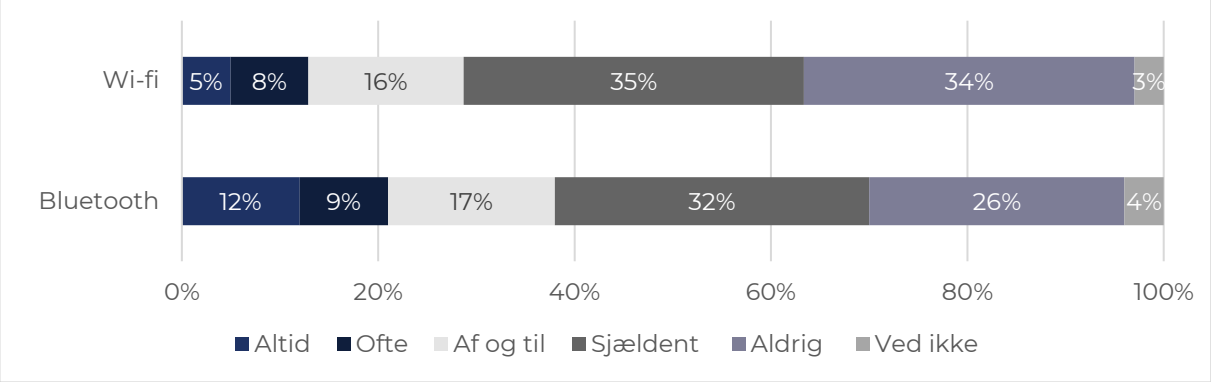
Det skader altså ikke at genstarte sin telefon en gang om ugen, men det er ikke en universel løsning på alle sikkerhedsproblemer. For at beskytte sig er det afgørende, at man installerer nye opdateringer af software, så snart de er tilgængelige, og gør brug af andre sikkerhedstiltag for at opnå bedst mulig beskyttelse.

Figur 3. Slukker telefonen.



Note: besvarelser=2002.

Figur 4. Slår bluetooth og wi-fi fra på devices, når det ikke bruges.



Note: besvarelser v. wifi=1923 og bluetooth= 1892.

[1] NSA (National Security Agency) er en af USA's efterretningstjenester.
[2] NSA Mobile Device Best Practices: https://www.documentcloud.org/documents/21018353-nsa-mobile-device-best-practices/
[3] https://www.forbes.com/sites/daveywinder/2024/10/24/nsa-tells-iphone-and-android-users-reboot-your-device-now/
[4] https://www.telia.dk/blog/guides-og-anbefalinger/sadan-forlanger-du-din-telefons-levetid/

Passwords

Passwords er et vigtigt greb til at beskytte sine devices og data. Opdaterer man ofte sine passwords, bruger stærke passwords, to-faktor godkendelse og forskellige passwords til forskellige enheder, så er man godt sikret mod angreb og at få stjålet sin data.

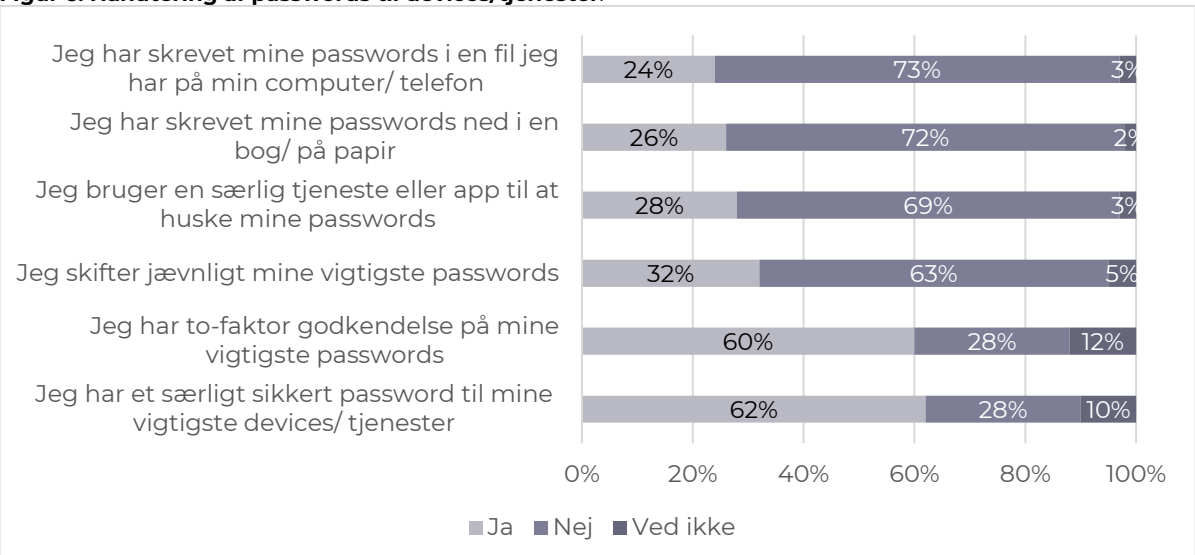
Undersøgelsen viser, at hovedparten af befolkningen bruger det samme password til alle deres devices/tjenester eller bruger nogle af deres passwords flere steder.

Figur 5. Håndtering af passwords til devices/tjenester.

Note: besvarelser=1920. Figuren er uden svarkategorien "ved ikke".

Figur 6 viser blandt andet, at hovedparten (63 pct.) af befolkningen ikke skifter deres vigtigste passwords jævnligt. Figuren viser også, at hver fjerde (28 pct.) ikke har to-faktor godkendelse og/eller et særligt sikkert password til deres vigtigste devices/tjenester.

Figur 6. Håndtering af passwords til devices/tjenester.



Note: besvarelser=2002 (undtaget spørgsmålet "Jeg har et særligt sikkert password til mine vigtigste devices/ tjenester", hvor der er besvarelser fra 1924 respondenter).

Nedenstående tabel 1 viser udviklingen i befolkningens håndtering af passwords fra 2017 og frem til 2025. Siden undersøgelsen senest blev foretaget i 2023, er der flere, der bruger en tjeneste, app eller fil til at gemme og huske deres passwords.

Tabel 1. Håndtering af passwords fordelt på år. Andel der har svaret "ja".

	2017	2021	2023	2025
Jeg har et særligt sikkert password til mine vigtigste tjenester	65%	66%	62%	62%
Jeg har to-faktor godkendelse på mine vigtigste password	25%	44%	53%	60%
Jeg bruger computeren til at huske mine password	25%	36%	36%	-
Jeg skifter jævnligt mine vigtigste password	30%	34%	27%	32%
Jeg bruger en særlig tjeneste eller app til at huske mine password	8%	16%	18%	28%
Jeg har skrevet mine password i en fil jeg har på min computer	10%	10%	10%	24%

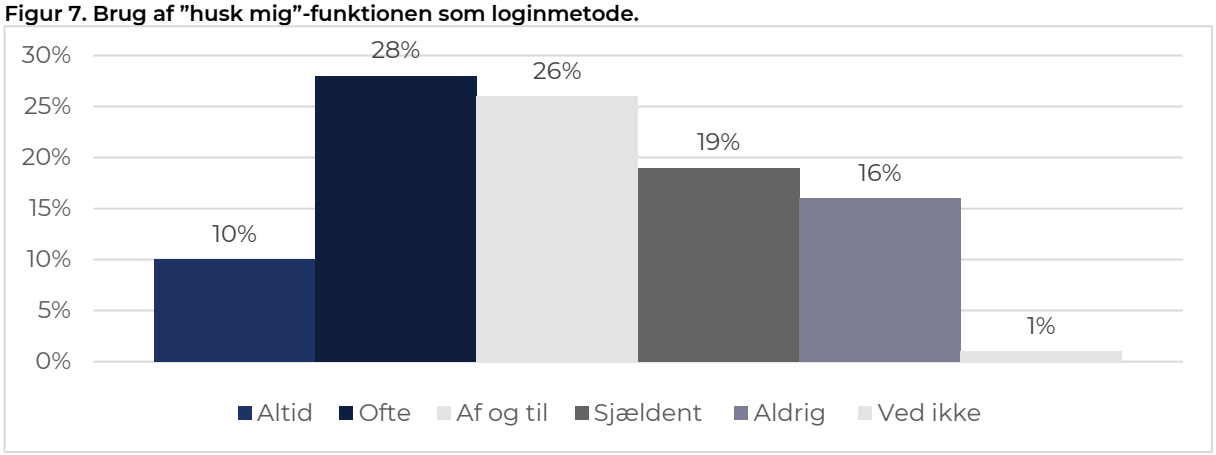
Note: Respondenterne har i 2025-undersøgelsen ikke haft mulighed for at svare "Jeg bruger computeren til at huske mine passwords", da vi har omformuleret spørgsmålet, og spurgt ind til, hvor ofte respondenterne bruger "husk mig"-funktionen, jf. figur 7.

Selvom man bruger stærke passwords, har forskellige passwords til forskellige enheder og bruger to-faktor-godkendelse, er der risiko forbundet med at bruge "husk-mig"-funktionen som loginmetode[5]. "Husk-mig"-funktionen er en cookie, der muliggør, at tjenesten eller hjemmesiden husker ens brugernavn og password, så man ikke behøver at skrive det, når man besøger hjemmesiden/tjenesten igen. Med "husk mig"-funktionen slipper man også for at skulle bruge to-faktor-godkendelse i 30 dage ad gangen, hvis man har tilsluttet det til givne login. Det kan fremstå bekvemt at bruge "husk mig"-funktionen, men det er forbundet sikkerhedsrisici. Blandt andet, hvis nogen får adgang til ens enhed, kan de få adgang til de steder, hvor man bruger "husk-mig"-funktionen og få indsigt i følsomme oplysninger, fx bankoplysninger. Derudover er disse "husk mig"-cookies eftertragtede for hackere at stjæle, da de kan anvendes til at hacke e-mailkonti.

For at beskytte sig mod denne type af angreb anbefaler FBI[6], at man regelmæssigt sletter cookies fra sin browser/sletter browserdata, udelukkende besøger hjemmesider med en sikker forbindelse (HTTPS) og holder øje med sine seneste loginhistorik[7]. Man kan også beskytte sig ved at undlade at bruge "husk-mig"-funktionen.

Figur 7 viser, at hovedparten (64 pct.) af befolkningen enten *altid, ofte* eller *af og til* bruger "husk-mig"-funktionen som loginmetode. Figur 8 viser, at 13 procent af dem sletter browserdata / cookies fra browseren dagligt eller på ugebasis.

Figur 7. Brug af "husk mig"-funktionen som loginmetode.



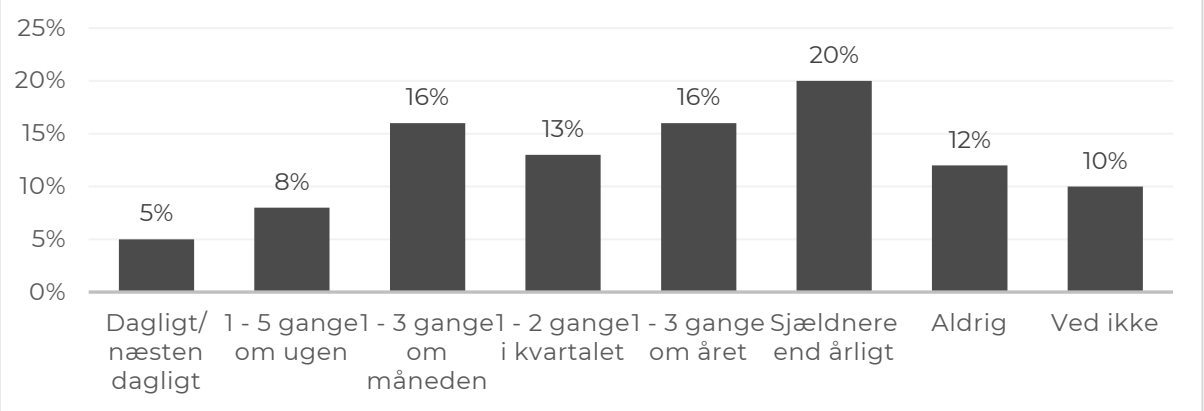
Note: besvarelser=1841.

[5] https://www.version2.dk/artikel/fbi-saadan-overtager-hackere-din-e-mailkonto-selv-med-multifaktorgodkendelse

[6] FBI (Federal Bureau of Investigation) er USA's nationale sikkerhedstjeneste.

[7] https://www.fbi.gov/contact-us/field-offices/atlanta/news/cybercriminals-are-stealing-cookies-to-bypass-multifactor-authentication

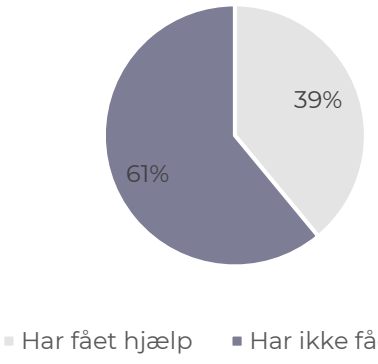
Figur 8. Sletter cookies fra browseren/ sletter browserdata.



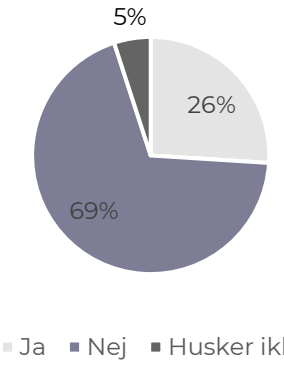
Note: besvarelser=1167. Besvarelserne er fra respondenter, der bruger "husk-mig"-funktionen som loginmetode enten "altid", "ofte", "af og til".

Udover at have forskellige og stærke passwords, to-faktor-godkendelse og være forbeholden med "husk-mig"-funktionen, er det vigtigt, at man ikke deler sine passwords med nogen – selv ikke med venner eller familie – selvom det kan fremstå trygt og belejligt, fx hvis man har brug hjælp til digitale udfordringer. Danmark er et af verdens mest digitaliserede lande[8], og det kan skabe anledning til, at man får brug for hjælp til at begå sig digitalt. Undersøgelsen viser, at hver fjerde (39 pct.) har fået hjælp digitale opgaver indenfor det seneste år, og blandt dem har 26 procent delt deres passwords med den/dem, de har fået hjælp fra. Det fremgår af figur 9 og 10.

Figur 9. Hjælp til digitale løsninger



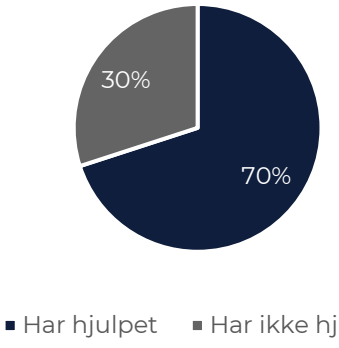
Figur 10. Har delt passwords med den/dem, de har fået hjælp fra



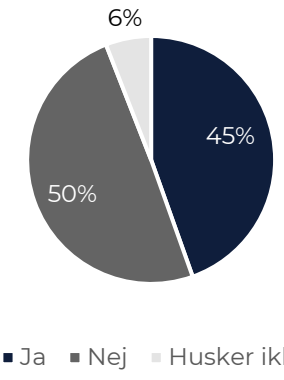
Note: besvarelser: figur 9=2002, figur 10=788.

70 procent har svaret, at de har hjulpet andre med digitale opgaver, hvoraf 45 procent af dem svarer, at de har fået indsigt i et eller flere passwords fra den, de har hjulpet. Det fremgår af figur 11 og 12. Selvom hjælpen oftest finder sted mellem familie og venner, hvilket kan virke trygt, bør man ikke dele sine passwords med andre. Digitaliseringsstyrelsen har lanceret et e-læringskursus for it-frivillige for at klæde dem på til at hjælpe borgere med digitale udfordringer og vejlede om sikker digital adfærd[9]. Selvom kurset er målrettet it-frivillige, kan det tilgås af alle og klæde en på til fx at hjælpe et familiemedlem uden at komme til at dele eller få indsigt i passwords eller personlige oplysninger.

Figur 11. Har hjulpet andre med digitale løsninger



Figur 12. Har fået indsigt i andres passwords



Note: besvarelser: figur 11=2002, figur 12=1395.

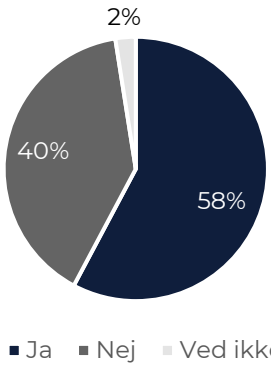
[8] https://www.dst.dk/da/Statistik/temaer/digitalisering

[9] https://www.digmin.dk/digitalisering/nyheder/nyhedsarkiv/2025/feb/nyt-e-laeringskursus-skal-goere-det-lettere-for-it-frivillige-at-hjaelpe-borgere-med-digitale-udfordringer

Smarte apparater i hjemmet (IoT-enheder)

Det er ikke kun ens computer, telefon eller netværk, der kan hackes. Det kan alle produkter og apparater, der kan tilsluttes internettet. Derfor er det vigtigt at sikre, at ens "smarte apparater"/IoT-enheder i hjemmet er beskyttet mod angreb. Et hackerangreb mod ens internetkoblede termostat, køleskab eller babyalarm er ikke kun problematisk, fordi det potentielt sætter produktet ud af funktion, men også fordi disse enheder kan fungere som adgangspunkter for hackere til hele ens netværk, hvilket fx kan kompromittere sikkerheden på ens computer, deaktivere indbrudsalarmer eller lignende. 58 procent af befolkningen har IoT-enheder i hjemmet, fx smart-tv, elpærer, indbrudsalarmer, babyalarmer, termostater, stemmestyrede personlige assistenter og lignende.

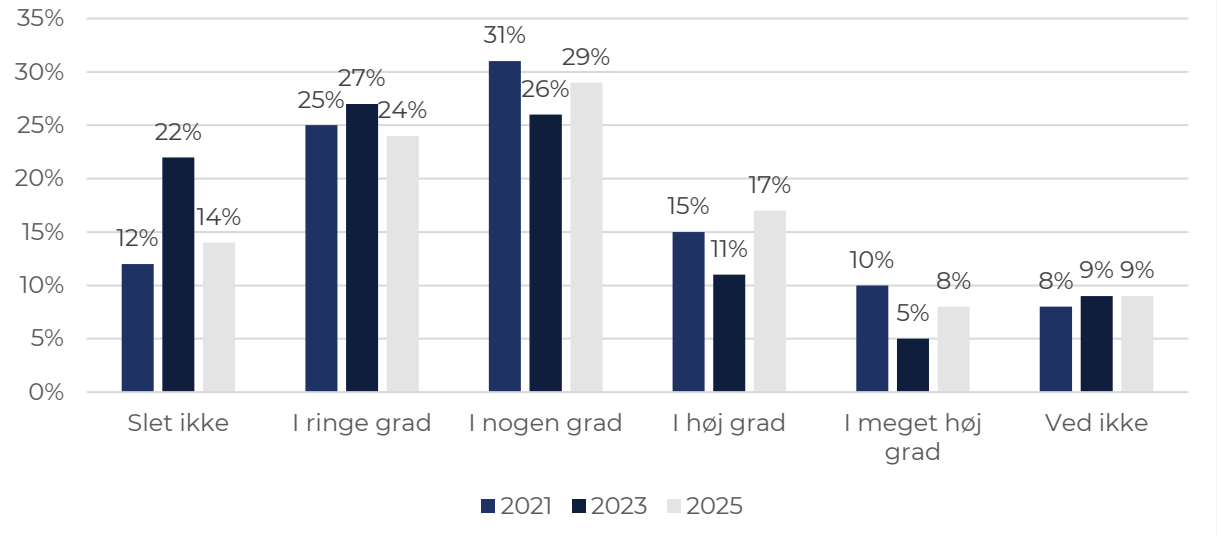
Figur 13. IoT-enheder i hjemmet



Figur 14 viser, i hvilken grad befolkningen forholder sig til, om deres smarte apparater i hjemmet er sikret mod angreb udefra. 38 procent af befolkningen forholder sig enten *slet ikke* eller *i ringe grad* til, om deres IoT-enheder er sikret mod angreb. 29 procent har svaret *i nogen grad* og 25 procent har svaret i *høj* eller *meget høj grad*. Figuren indikerer en generel stigning i befolkningens opmærksomhed på sikkerheden af deres IoT-enheder i hjemmet fra 2023 til 2025.

For at beskytte sine IoT-enheder bør man sikre, at alle enheder har stærke og unikke navne og adgangskoder, regelmæssigt opdatere enhedernes firmware[10], deaktivere unødvendige funktioner, man ikke ønsker at bruge, fx mikrofon eller fjernadgang og bruge et sikkert netværk med kryptering. Det kan også være en god idé at have ens sikkerhedssystem, fx indbrudsalarm, og adgangen til ens bankkonto på netværk adskilt fra ens IoT-enheder[11].

Figur 14. Forholder du dig til, om dit udstyr/apparater, der er koblet til internettet, er sikret mod angreb udefra?



Note: besvarelser: 2021=818, 2023=1136 og 2025=1212.

[10] Firmware er fast installeret software i produktet der styrer, hvordan produktet/hardwaren virker (ordnet.dk).
[11] https://www.kaspersky.dk/resource-center/threats/secure-iot-devices-on-your-home-network

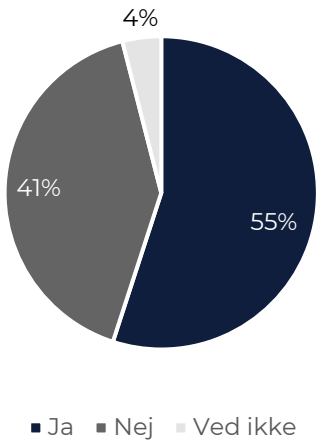
It-kriminalitet

It-kriminalitet er en stigende trussel i vores digitaliserede verden. Kriminelle anvender stadig mere sofistikerede metoder til at udføre forskellige former for it-kriminalitet, som kan have alvorlige konsekvenser for både enkeltpersoner og virksomheder. At være opmærksom på forskellige typer af it-kriminalitet og tage de nødvendige forholdsregler kan være med til at beskytte en og ens data mod svindel.

Figur 15 viser, at 55 procent af den danske befolkning har været udsat for en eller flere typer af it-kriminalitet indenfor de seneste to år.

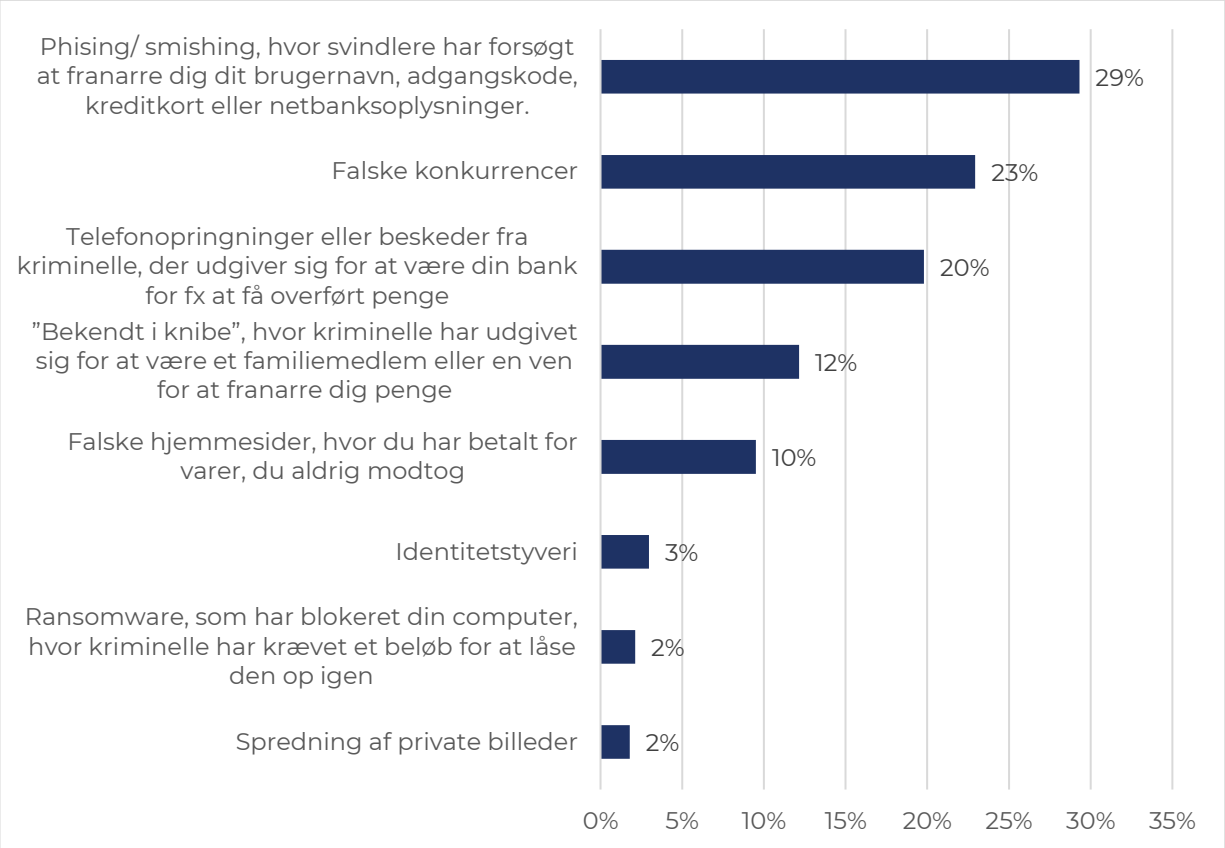
De tre mest udbredte former for it-kriminalitet er 1) phishing/smishing, 2) falske konkurrencer og 3) telefonopringninger eller beskeder fra kriminelle, der udgiver sig for at være ens bank. Det fremgår af figur 16.

Figur 15. Udsat for it-kriminalitet



Note: besvarelser=2002.

Figur 16. Typer af it-kriminalitet, befolkningen har været udsat for indenfor de seneste to år.

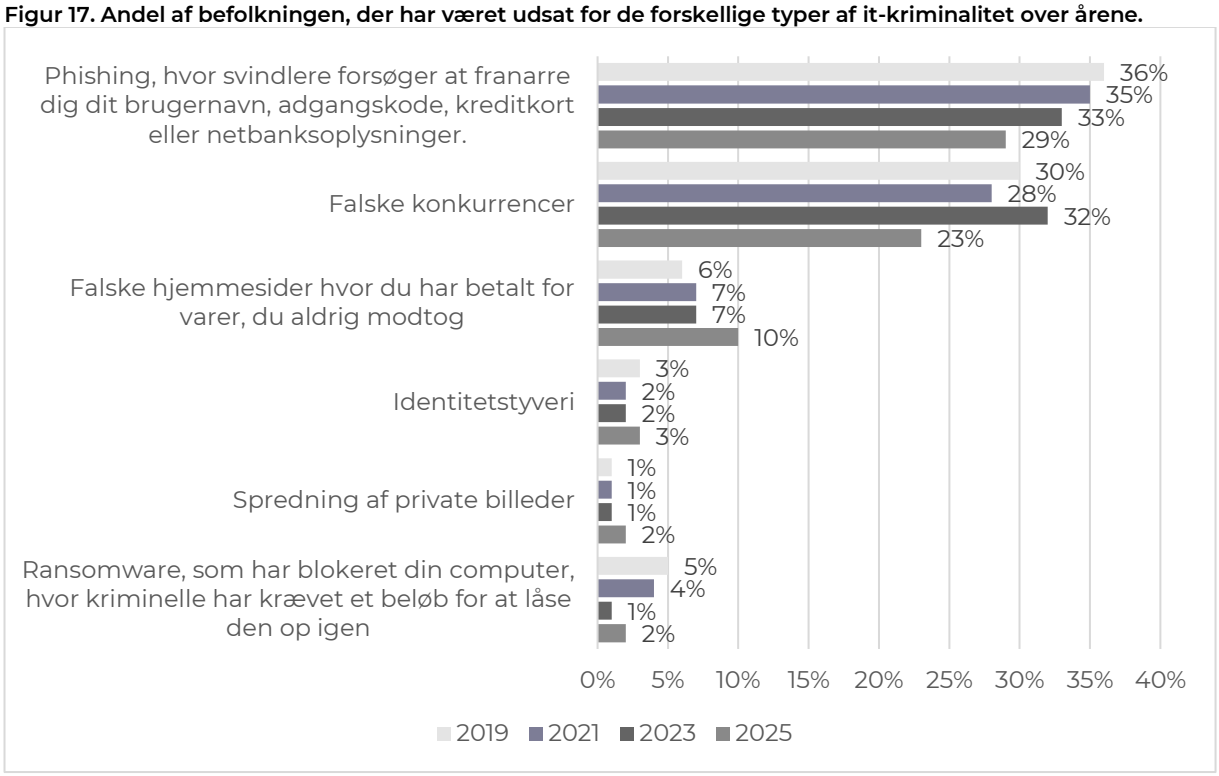


Note: besvarelser=2002.

Udbredelsen af forskellige former for it-kriminalitet ændrer sig med tiden, og kriminelle finder nye måder at svindle på. Figur 17 viser andelen af befolkningen, der har været udsat for forskellige typer af it-kriminalitet i 2019, 2021, 2023 og 2025. Figuren viser, at de to mest udbredte former for it-kriminalitet er svagt faldende sammenlignet med tidligere undersøgelser. Derimod antyder figuren en stigning i svindel med falske hjemmesider.

National enhed for Særlig Kriminalitet (NSK) advarer om en markant stigning i typen af svindel kaldet "bekendt i knibe"[12]. Svindleren udgiver sig for at være en bekendt, ven eller familiemedlem[13], sender en sms eller en besked og beder om pengeoverførsler, fordi de angiveligt er i knibe, fx har mistet deres telefon eller fået lukket deres bankkonto. Tidligere IDA-undersøgelser har ikke belyst kriminalitetsformen "bekendt i knibe", men dette års undersøgelser viser, at 12 procent har været udsat for "bekendt i knibe" indenfor de seneste to år. Det fremgår af figur 16.

Figur 17. Andel af befolkningen, der har været udsat for de forskellige typer af it-kriminalitet over årene.



Besvarelser: 2019=2019, 2021=2000, 2023=2000 og 2025=2002. I tidligere undersøgelser er der ikke spurgt ind til kriminalitetstyperne "bekendt i knibe" og "Telefonopringninger eller beskeder fra kriminelle, der udgiver sig for at være din bank for fx at få overført penge", hvorfor disse ikke fremgår i figur 17.

[12] https://politi.dk/national-enhed-for-saerlig-kriminalitet/nyhedsliste/svindlere-manipulerer-i-hoejere-grad-borgere-til-at-overfoere-penge/2025/02/24

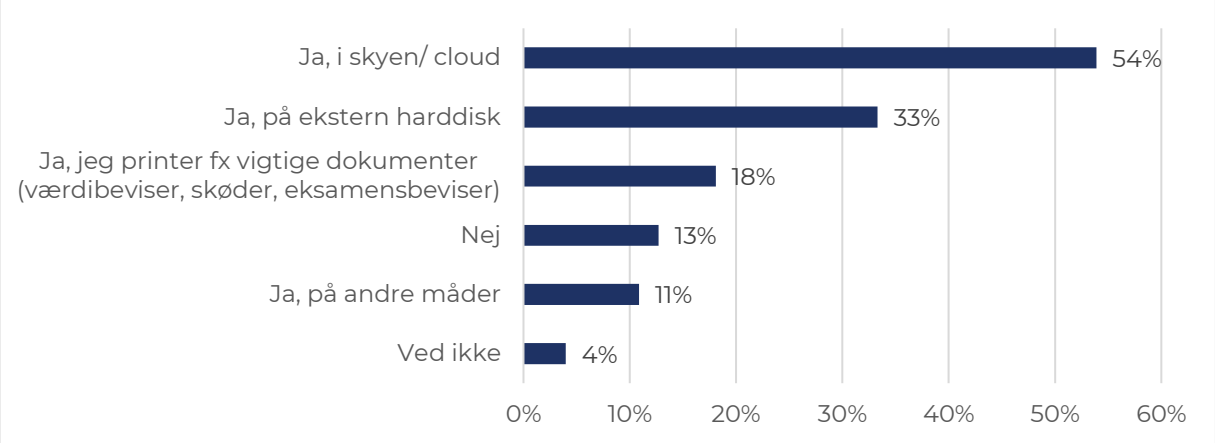
[13] https://politi.dk/national-enhed-for-saerlig-kriminalitet/nyhedsliste/digital-svindel-fra-bekendte-i-knibe-er-steget-voldsomt/2024/10/09

Backup

Er uheldet ude, og man er blevet hacket og har mistet data, er det vigtigt at have en kopi af sine vigtige dokumenter, fotos eller lignende. 83 procent af befolkningen tager backup. 13 procent gør det ikke, og dette har ikke ændret sig betydeligt siden undersøgelsen blev foretaget i 2017. Det fremgår af figur 18 og 19.

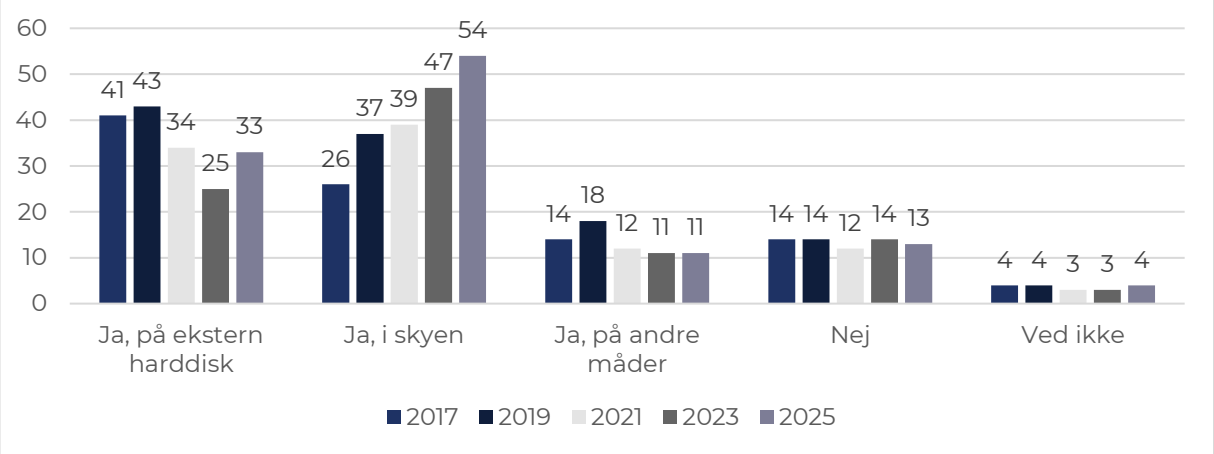
Over halvdelen (54 pct.) af befolkningen bruger i dag en cloudløsning/skyen til backup. Hver tredje bruger en ekstern harddisk til backup. Vil man være på den sikre side, er det en god løsning at have backup flere steder, da man fx kan risikere at miste en ekstern harddisk. 27 procent af befolkningen bruger mere end én backup-løsning.

Figur 18. Tager backup af vigtige dokumenter, fotos eller andre data.



Note: besvarelser=2002.

Figur 19. Tager backup af vigtige dokumenter, fotos eller andre data. Fordelt på år. Angivet i procent.



Besvarelser: 2017=2022, 2019=2019, 2021=2000, 2023=2000 og 2025=2002. Som det fremgår af figur 18, havde respondenterne i 2025-undersøgelsen også mulighed for at svare, at de tager backup ved at printe fx vigtige dokumenter, fotos eller lignende. Dette var ikke en svarkategori i tidligere undersøgelsen, hvorfor det ikke fremgår af figur 19.

Bilag

Bilagtabel 1. Hvor ofte gør du følgende?

	Altid	Ofte	Af og til	Sjæl-dent	Aldrig	Ved ikke	Frekvens
Hvor ofte klikker på links uden at vide hvor det linker til?	1%	2%	8%	40%	48%	1%	1963
Hvor ofte åbner du ukendte vedhæftede filer?	1%	2%	5%	28%	64%	1%	1973
Hvor ofte opdaterer du dine antivirusprogrammer på dine computere og andre enheder til nyeste version?	25%	18%	18%	18%	12%	9%	1877
Hvor ofte opdaterer du din browser på dine computere og andre enheder til nyeste version?	30%	22%	22%	15%	5%	6%	1840
Hvor ofte opdaterer du dit styresystem/ operativsystem på din computer, telefon og andre enheder til nyeste version, fx opdatering af Windows eller iOS-/softwareopdatering af iPhone?	39%	25%	19%	9%	3%	4%	1818
Hvor ofte bruger du åbne WiFi-netværk på fx cafeer, museer, offentlig transport eller andre lignende steder?	1%	7%	23%	43%	25%	1%	1917
Hvor ofte bruger du samme USB-nøgler/ -stik til flere computere?	4%	8%	14%	25%	41%	7%	1935

Bilagstabel 2. Er dit hjemmenetværk (wifi) beskyttet, så man kun kan komme på, hvis man kender adgangskoden?

	Procent
Ja, det er beskyttet af en adgangskode jeg selv har oprettet	60%
Ja, det er beskyttet af den adgangskode der fulgte med netværket	31%
Nej	2%
Jeg har ikke noget hjemmenetværk	2%
Ved ikke	5%
Total	100 %

Besvarelser: 2002

FOR YDERLIGERE INFORMATION, KONTAKT

Analyse : Olivia Sif Hahn Kristensen olsh@ida.dk
Presse : Ole Hoff-Lund ollu@ida.dk
Politik : Grit Munk gmu@ida.dk

FAKTA OM UNDERSØGELSEN

Undersøgelsen er foretaget af Analyseinstituttet Analyse Danmark for IDA. Dataindsamlingen blev gennemført i perioden fra den 09.12.2024 - 18.12.2024. Der er indhentet svar fra 2.002 respondenter, udtrukket blandt medlemmer af Norstats webpanel. Data er vægtet på regioner, køn og alder.

IDA - EN FORENING FOR VIDEN, NETVÆRK OG INTERESSEVARETAGELSE. MED OVER 165.000 MEDLEMMER.

IDA er Danmarks største fagforening og faglige fællesskab for ingeniører, cand.scient'er og it-professionelle. Danmark kæmper sammen med resten af verden om at skabe vækst og job samtidig med, at vi får løst de store samfundsudfordringer, vi og resten af verden står over for.