

Digital sikkerhetskultur 2026



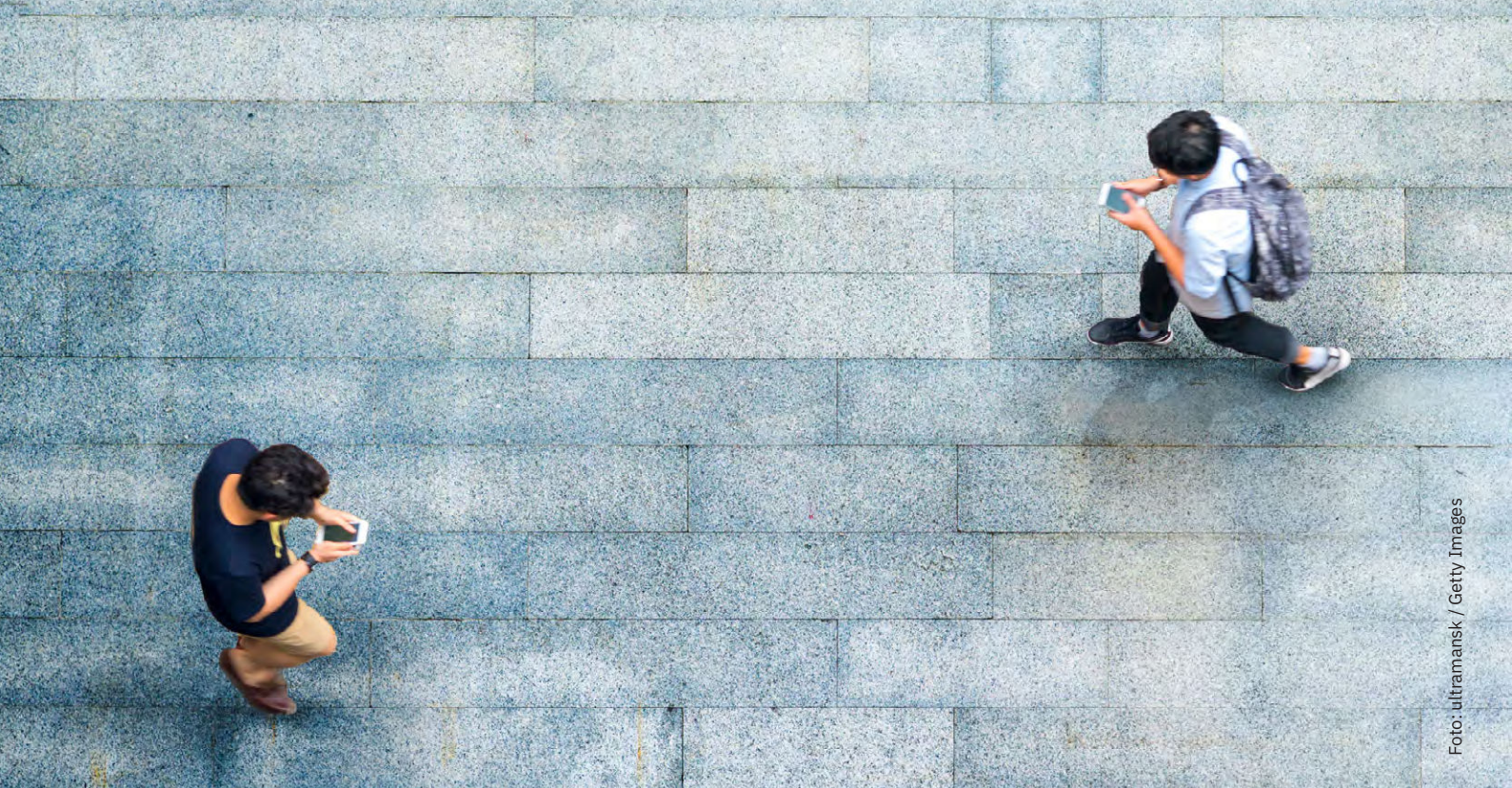


Foto: ultramansk / Getty Images

INNLEDNING

Digital sikkerhetskultur i en ny fase _____ 3

KAPITTEL 1

Digitale trusler – Kriminalitet i hverdagen _____ 6

KAPITTEL 2

Det digitale avtrykket – små spor, stor risiko _____ 12

INTERVJU

Hjernespesialist: Øvelse gjør fremdeles mester _____ 20

KAPITTEL 3

Digital dømmekraft: Når kunnskap ikke er nok _____ 22

KAPITTEL 4

Digital trygghet – hvem kan vi stole på? _____ 30

Digital sikkerhetskultur i en ny fase

Digital kriminalitet er blitt hverdagskriminalitet. Med kunstig intelligens blir de stadig vanligere angrepene mer troverdige, og våre egne valg viktigere enn noensinne.

En melding fra banken. Et gebyrvarsel fra parke-ringsselskapet. En pakke som venter. En lenke eller forespørsel fra en kollega. Det er i slike situasjoner vår digitale sikkerhet stadig oftere utfordres.

Nærmere 500 000 nordmenn har blitt svindlet for penger på nett de siste to årene. Rundt 100 000 har opplevd misbruk av sin personlige BankID, samtidig som Slettmeg.no i første halvår 2026 fikk 119 prosent flere henvendelser om seksuell utpressing enn i samme periode i fjor. Rundt 7 av 10 tror ikke, eller er usikre på, om de kan kjenne igjen KI-generert tekst eller lyd. Når angrepene blir mer troverdige, blir også hverdagsvalgene vanskeligere.

Truslene kommer ikke lenger bare som tekniske angrep mot systemer langt unna. De treffer oss hjemme og på jobb, gjennom tjenester vi bruker hver dag. De utnytter tillit, tidspress og usikkerhet.

Kunstig intelligens gjør det også vanskeligere å skille ekte fra falskt. Språket blir bedre, bildene mer troverdige og stemmer kan etterlignes. Svindelforsøk kan tilpasses personer, arbeidsplasser og situasjoner med en presisjon og hastighet som tidligere var nærmest utenkelig – også av kriminelle uten særlig mye digital kompetanse.

1 av 2 har ikke god kontroll over egne digitale avtrykk

Samtidig legger vi igjen stadig flere digitale avtrykk. Bilder, søk, interesser, kontaktopplysninger og informasjon om hvor vi jobber og hvem vi kjenner, kan hver for seg virke ubetydelige. Når opplysningene settes sammen, kan de brukes til svindel, utpressing og ID-tyveri. Bare 53 prosent opplever at de har god kontroll over hvilke opplysninger om dem, som finnes på internett. Kunstig intelligens og automatisert datainnsamling gjør det samtidig enklere for kriminelle å hente inn, analysere og koble sammen slike spor.

Det gjelder også informasjon vi selv legger inn i KI-tjenester. Nesten halvparten av befolkningen bruker nå tekstbaserte KI-verktøy ukentlig eller oftere. Blant disse oppgir 15 prosent at de har delt personopplysninger om seg selv, mens 13 prosent har delt interne jobbopplysninger.



Foto: Ilja C. Hendel / NSM

Vet mer, men handler ikke alltid deretter

Selv om rundt 70 prosent oppgir at de vet hvordan de skal beskytte seg på nett, sier 26 prosent at de tar sjanser som de vet kan være risikable. Det samme gapet ser vi i konkrete sikkerhetsvalg: 55 prosent mener det er risikabelt å ikke bruke totrinnspålogging, mens 41 prosent likevel ikke bruker dette der dette er mulig. Vi vet mer, men handler ikke alltid tryggere.

Årets rapport peker derfor på et skifte: Digital trygghet handler ikke bare om hva vi vet, men om hva vi faktisk gjør i øyeblikket. Stopper vi opp før vi klikker? Ofte handler det om å sjekke avsenderen en gang til, forstå hva vi faktisk deler, og bruke totrinnspålogging der det er mulig.

Nesten hver fjerde nordmann vet ikke om arbeidsplassen har regler for digital sikkerhet

Arbeidsplassen spiller også en viktig rolle. Det kan være utfordrende når skillet mellom jobb og privatliv viskes ut, og vi bruker de samme enhetene, tjenestene og vanene begge steder – spesielt når det ikke er tydelige og kjente regler for dette. Nesten hver fjerde yrkesaktive nordmann (24 prosent) vet ikke om arbeidsplassen deres har regler for digital sikkerhet – eller oppgir at slike regler ikke finnes.

Den tiende årlige undersøkelsen av nordmenns digitale sikkerhetskultur viser også at mye går i riktig retning. Mange kjenner farene, bruker grunnleggende sikkerhetstiltak og opplever at de har kunnskap til å beskytte seg. Utfordringen er at trusselbildet ofte utvikler seg raskere enn våre vaner endres.



Øvelse gjør mester – også med kunstig intelligens

Det betyr ikke at utviklingen er håpløs. Hjerne-spesialist Marte Roa Syvertsen peker på at hjernen kan trenes til tryggere reaksjonsmønstre. Øvelse gjør fremdeles mester, også når vi skal vurdere innhold som kan være laget med kunstig intelligens.

Derfor er det ikke nok å øke kunnskapen. Hovedutfordringen er å gjøre trygg digital atferd enklere å gjennomføre, og lettere å gjenta – hjemme, på jobb og i tjenestene vi bruker hver dag.

Dette er hovedbildet i årets rapport.

Digitale trusler – Kriminalitet i hverdagen

Digitale trusler som nettsvindel, ID-tyveri og utpressing rammer ikke lenger bare dem som tar sjanser på nett. De har blitt hverdagskriminalitet.

Angrepene rammer både privatpersoner og virksomheter – hjemme og på jobb. De er mer målrettede, mer sofistikerte og ofte drevet av store kriminelle nettverk.

Bare i løpet av de siste to årene har nærmere 500 000 nordmenn (11 prosent) blitt svindlet for penger på nett. I samme periode har 100 000 (to prosent) opplevd misbruk av sin personlige BankID.

NorSIS' rådgivningstjeneste Slettmeg har første halvår i år fått 119 prosent flere henvendelser om seksuell utpressing enn i samme periode i fjor. Ofrene trues med deling av intime bilder eller video og presses til å sende mer innhold, utføre seksuelle handlinger eller betale penger.

Særlig gutter og unge menn tar nærmest daglig kontakt for å få hjelp ut av slike situasjoner. Mørketallene er trolig store.

Flere får tilgang til avanserte svindelverktøy

Ifølge INTERPOLs globale trusselvurdering for 2026¹ er nettsvindel nå blant de største kriminalitetstruslene globalt, på linje med hvitvasking og narkotika. Bare fra 2024 til 2025 økte antall registrerte svindelvarsler hos dem med 54 prosent.

Utviklingen drives av teknologi. Kunstig intelligens gjør svindelforsøk mer overbevisende og mer målrettede. Samtidig gjør ny teknologi det mulig også for mindre kompetente aktører å gjennomføre operasjoner som tidligere krevde høyere kompetanse.

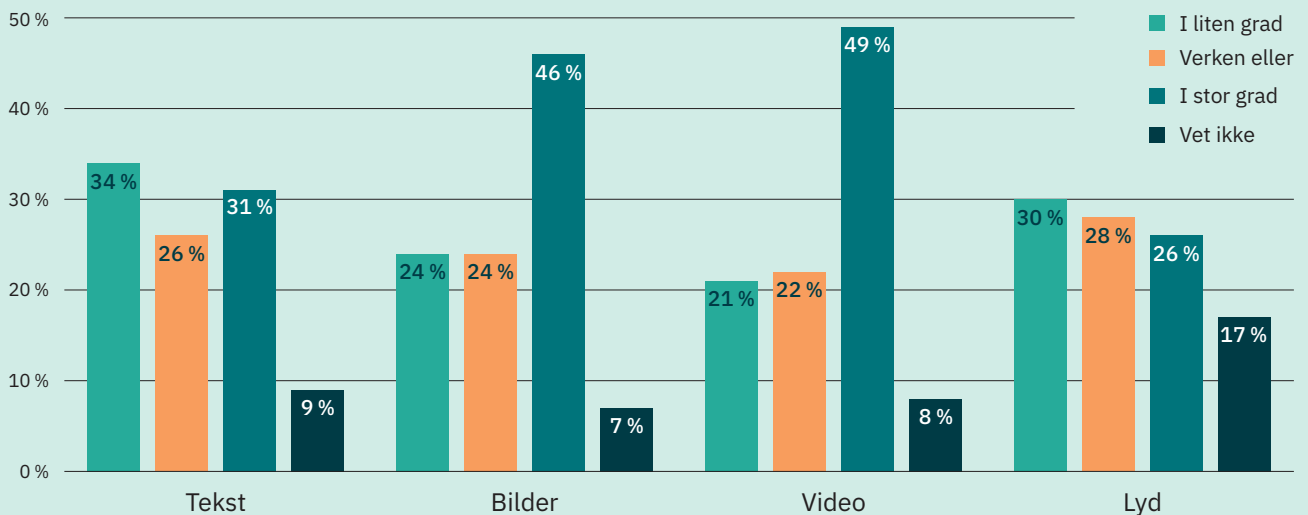
I NSM-rapporten Risiko 2026 pekes det på at mange cyberhendelser er knyttet til sosial manipulasjon, som phishing. De kriminelle bruker stadig mer sofistikerte metoder for å fremstå som legitime, ofte via e-post, meldinger eller sosiale medier, for å få tilgang til informasjon eller penger.

De kriminelle nettverkene samarbeider globalt og deler teknologi og metoder. Mange svindelforsøk er derfor ikke enkeltstående hendelser, men del av større, koordinerte operasjoner.

1 INTERPOL Global Financial Fraud Threat Assessment 2026

Gjenkjennelse KI-generert innhold

I hvilken grad mener du at du kan kjenne igjen når følgende er helt eller delvis laget ved hjelp av kunstig intelligens?



Flertallet sliter med å avsløre KI-generert innhold

Samtidig som cyberkriminaliteten øker og metodene blir mer sofistikerte, er flertallet av nordmenn usikre på om de greier å skille mellom ekte og KI-generert innhold.

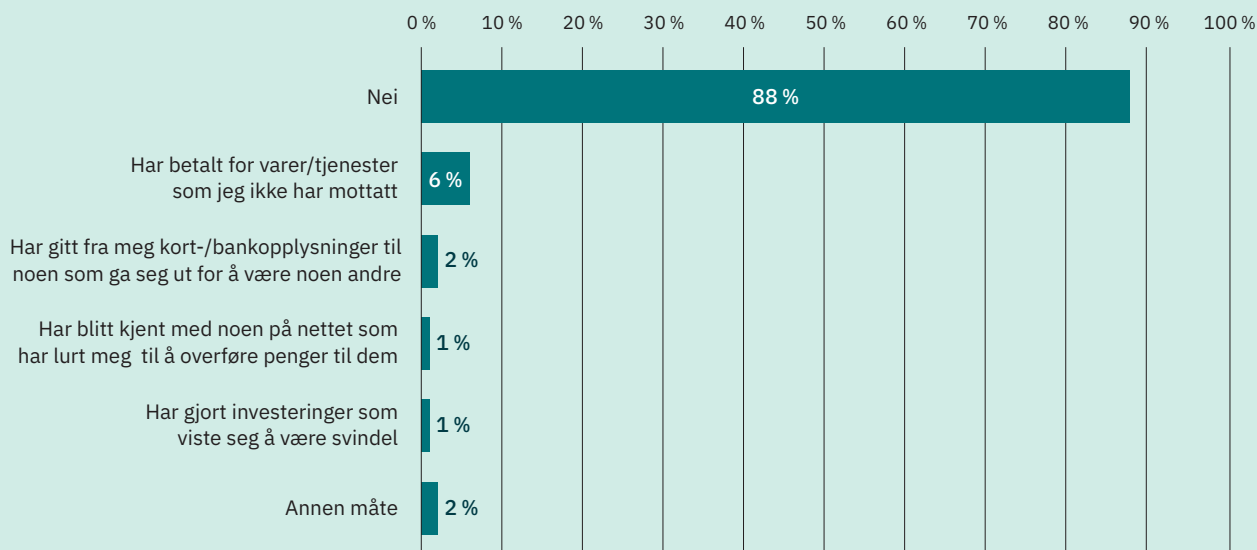
7 av 10 nordmenn tror ikke, eller er usikre på, om de kan kjenne igjen tekst eller lyd generert av kunstig intelligens. Nærmere 6 av 10 tviler på om de kan avsløre KI-genererte bilder på nett. Flest mener de kan kjenne igjen KI-generert video. Gjennomgående oppgir yngre at de i større grad enn eldre greier å kjenne igjen KI-generert innhold.

11 %

har blitt svindlet for penger på nett i løpet av de siste to årene

Pengesvindel

Har du opplevd at noen har svindlet deg for penger på internett i løpet av de to siste årene?



Mer enn 250 000 nordmenn har tapt penger på netthandel

Den klart vanligste svindelformen, som har rammet seks prosent av nordmenn over 18 år de siste årene, er at folk har betalt for varer eller tjenester på nett, som de ikke har mottatt. Det tilsvarer nærmere 300 000 nordmenn.

Nettbutikksvindel skjer i situasjoner de fleste kjenner godt, som kjøp av varer på nett via markeds plasser eller falske nettbutikker som fremstår som seriøse og legitime.

Rundt 75 000 nordmenn, 1,7 prosent, oppgir at de har delt kort- eller bankopplysninger med noen som har utgitt seg for å være andre.

Titusener oppgir også at de i løpet av de siste to årene har blitt lurt av investeringssvindel eller til å overføre penger til noen de har blitt kjent med på nett.

Økonomisk svindel på nett rammer bredt – både når det gjelder kjønn, alder og livssituasjon for øvrig.

Mer bekymring enn før

Nordmenns bekymring for digitale hendelser har økt siden den raske digitaliseringen under koronapandemien. Seks av syv vanlige bekymringer har i denne perioden blitt sterkere.

57 prosent oppgir at de i stor grad frykter misbruk av bank- eller kredittkort på nett. 39 prosent frykter å bli lurt til å gi fra seg betalingsinformasjon, passord eller annen sensitiv informasjon.

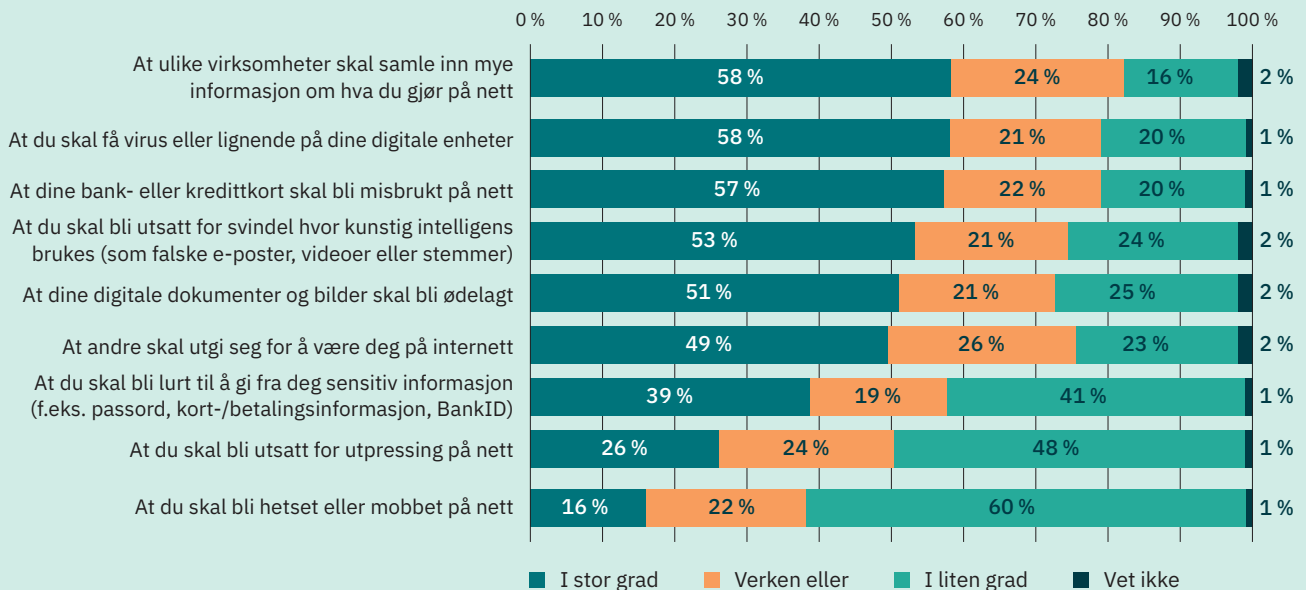
Mer enn halvparten, 53 prosent, er også i stor grad bekymret for svindel der kunstig intelligens er involvert, som falske e-poster, videoer eller telefonsamtaler.

53 %

av befolkningen er
bekymret for svindel der
kunstig intelligens er involvert

Bekymringer

I hvilken grad er du bekymret for at følgende skal skje med deg?



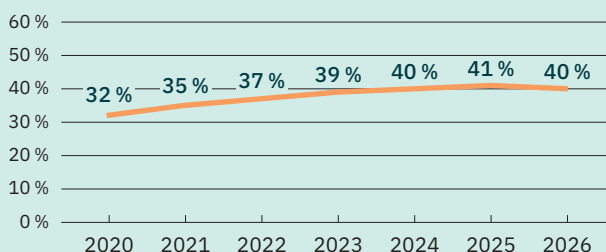
Risiko påvirker hva folk velger bort

Samtidig oppfatter nordmenn flere vanlige nett-aktiviteter som mer risikofylte enn tidligere. For sosiale medier har andelen økt fra 32 prosent i 2020 til 40 prosent i dag.

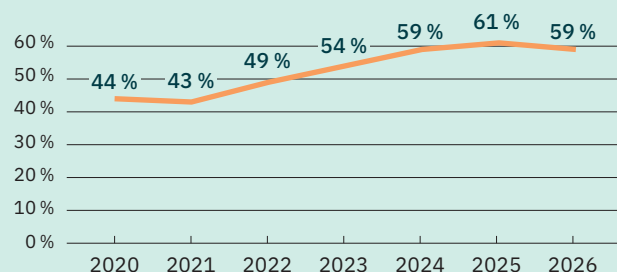
Andelen som lar være å bruke digitale tjenester av frykt for kriminalitet, har økt fra 44 prosent i 2020 til 59 prosent i dag, og har stabilisert seg på et høyt nivå.

Over halvparten oppgir at de har latt være å bruke nettbutikker av frykt for kriminalitet. Nesten like mange styrer unna piratnettsteder, tjenester der risikoen i stor grad er økonomisk.

Andel som forbinder sosiale medier med høy risiko

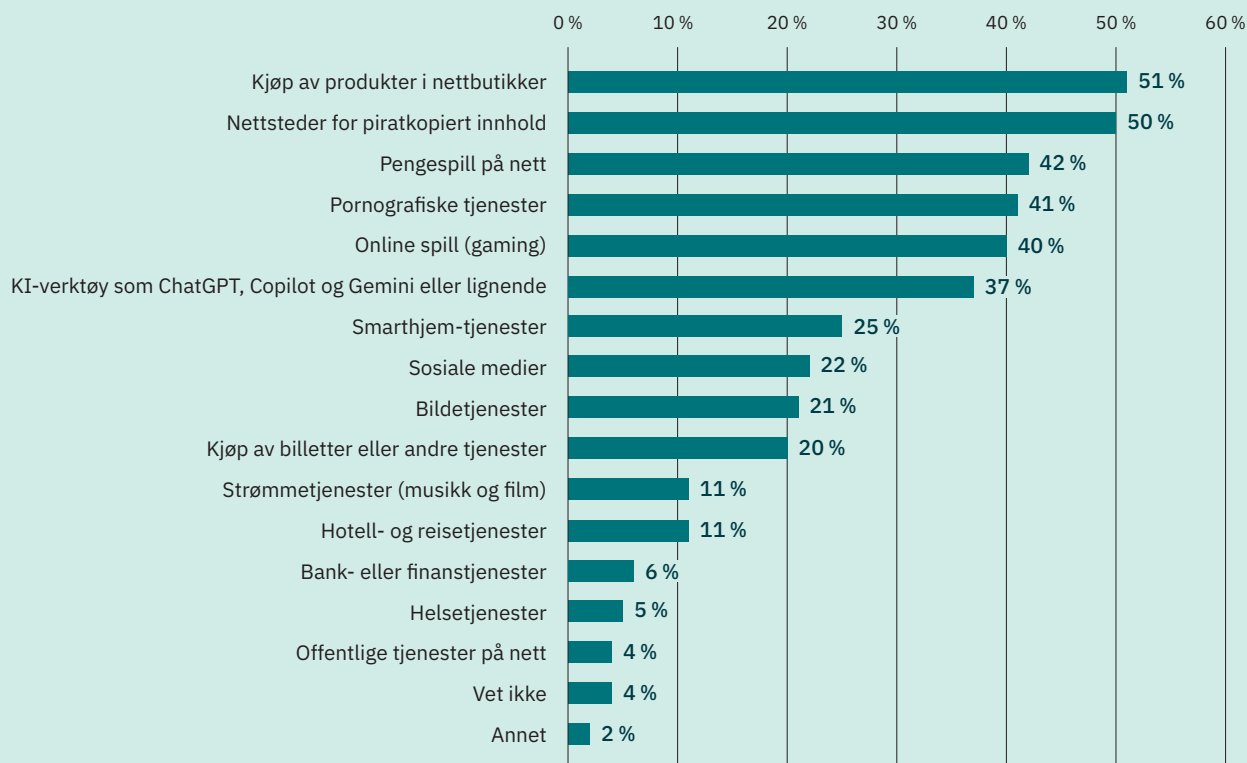


Unngår bruk av en tjeneste på internett på grunn av frykt for kriminelle eller ubehagelige hendelser



Type tjenester unngått

Hvilke typer tjenester på internett har du latt være å bruke?



Samtidig er bildet annerledes for sosiale medier. Selv om flere oppfatter disse som risikofylte, har andelen som lar være å bruke dem holdt seg rundt 20 prosent siden 2020.

Færre sier nå at de unngår bank- og finanstjenester som følge av uro for digitale trusler, hacking eller kriminalitet på nett: 6 prosent i dag, mot 11 prosent i 2020. Det tyder på at opplevd risiko ikke alene avgjør hva folk velger bort. Like viktig er hvilken type risiko det er, og hvor nødvendig tjenesten oppleves i hverdagen.



Det er veldig lett å bare trykke på «godta alt».

Det digitale avtrykket – små spor, stor risiko

Det er ikke deling av en e-postadresse, et telefonnummer eller et bilde som gjør oss mest sårbare på nett. Risikoen oppstår når mange av våre digitale spor kobles sammen til et stadig mer presist bilde av hvem vi er.

Ifølge årets sikkerhetskulturundersøkelse er nettopp dette blant de digitale bekymringene som treffer bredest i befolkningen. 58 prosent av nordmenn er i stor grad bekymret for at virksomheter samler inn informasjon om hva de gjør på nett. Bekymringen har økt svakt over tid.

Bare litt over halvparten av nordmenn, 53 prosent, opplever at de har kontroll over egne personopplysninger på internett.

Samtidig gjør kunstig intelligens og automatisert datainnsamling det enklere å hente inn, sammenstille og misbruke store mengder informasjon om enkeltpersoner.

Dataskraping er et eksempel på dette. Det betyr at programvare automatisk samler inn informasjon som ligger åpent tilgjengelig på nettet – som innlegg, bilder, kommentarer og profiler som ikke er skjermet, i sosiale medier eller andre digitale tjenester. Sammen med KI kan slike data brukes til å bygge detaljerte og innholdsrike profiler av personer og målgrupper.

Når små spor får verdi

Digitale avtrykk er sporene vi legger igjen når vi bruker nettet. Noe deler vi bevisst, som feriebilder, innlegg i sosiale medier, jobbhistorikk og informasjon i nettbutikker og apper. Andre spor legger vi igjen uten å tenke over det. Informasjonskapsler registrerer hvilke sider vi besøker og hva vi klikker på, mens mobilapper kan samle inn informasjon om hvor vi befinner oss.

I tillegg finnes det opplysninger andre legger ut om oss, informasjon som ligger i åpne registre og data fra tidligere lekkasjer. Flere milliarder kompromitterte kontoer, ofte med både e-postadresse og passord, ligger tilgjengelig for salg.

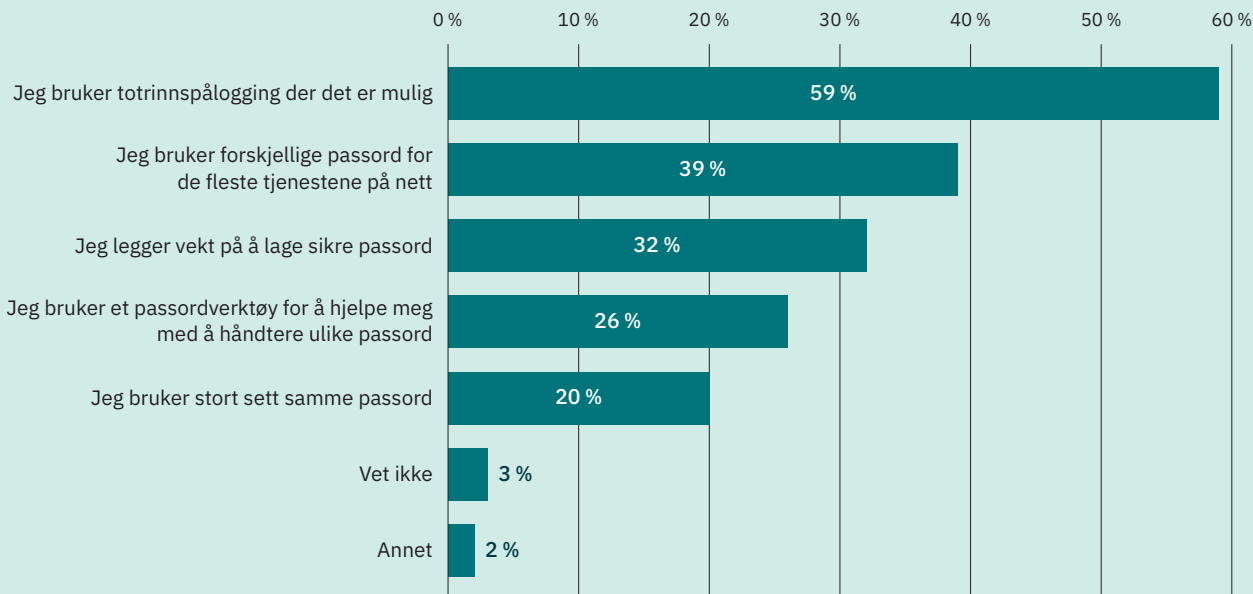
Hver for seg kan opplysningene virke ubetydelige. Samlet kan de brukes til målrettet svindel, utpressing og ID-tyveri.

Når språkbruk, våre venner og familie, arbeidssted og kontaktinformasjon kobles sammen, blir det enklere å bygge detaljerte profiler som kan brukes mot oss.

Ifølge Europol er nettbasert svindel i dag en sentral del av organisert kriminalitet, der stjalne

Passordbruk

Hvordan bruker du passord i privat sammenheng?



data selges og deles videre mellom ulike kriminelle miljøer. Angrepene blir stadig mer målrettede og bygger ofte på informasjon vi selv har gjort tilgjengelig på nett – både hjemme og på jobb.

Ett passord kan være nok

Et konkret eksempel er e-postadresser og passord. 1 av 5 nordmenn oppgir at de stort sett bruker samme passord på de fleste tjenester. Hvis e-postadresse og passord først er lekket, kan automatiserte verktøy teste den samme innloggingen på tvers av tjenester.

Det betyr også at en privat hendelse kan få konsekvenser langt utenfor privatlivet. Mange bruker de samme enhetene, vanene og noen ganger også de samme passordene hjemme og på jobb.

Nesten hver fjerde yrkesaktive nordmann (24 prosent) vet ikke om arbeidsplassen deres har regler for digital sikkerhet – eller oppgir at slike regler ikke finnes.

Brukes passordet flere steder, vil en lekkasje kunne bli inngangen til flere kontoer.

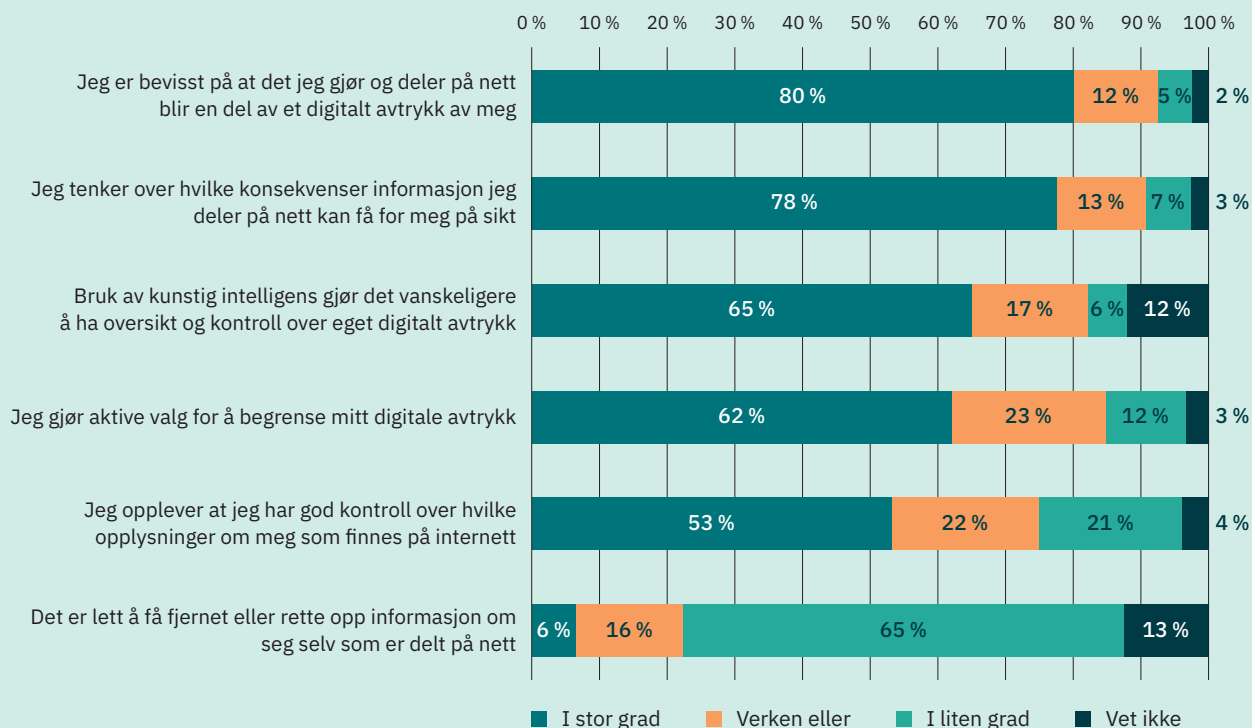
1 av 5

nordmenn oppgir at de stort sett bruker samme passord på de fleste tjenester

Jeg vet at jeg ikke bør bruke samme passord overalt. Men du mister jo helt oversikten når alle skal ha forskjellige passord med tall, store bokstaver og spesialtegn.

Digitale avtrykk

Hvor enig eller uenig er du i følgende påstander?



Mange er bevisste – men få føler kontroll

Årets undersøkelse viser at 8 av 10 nordmenn er bevisste på hva de deler på nett. Likevel opplever bare litt over halvparten at de har kontroll over egne personopplysninger.

Flere (21 prosent) opplever at de har begrenset oversikt over hvilke opplysninger som er samlet inn, hvem som har tilgang til dem og hvordan informasjonen brukes videre.

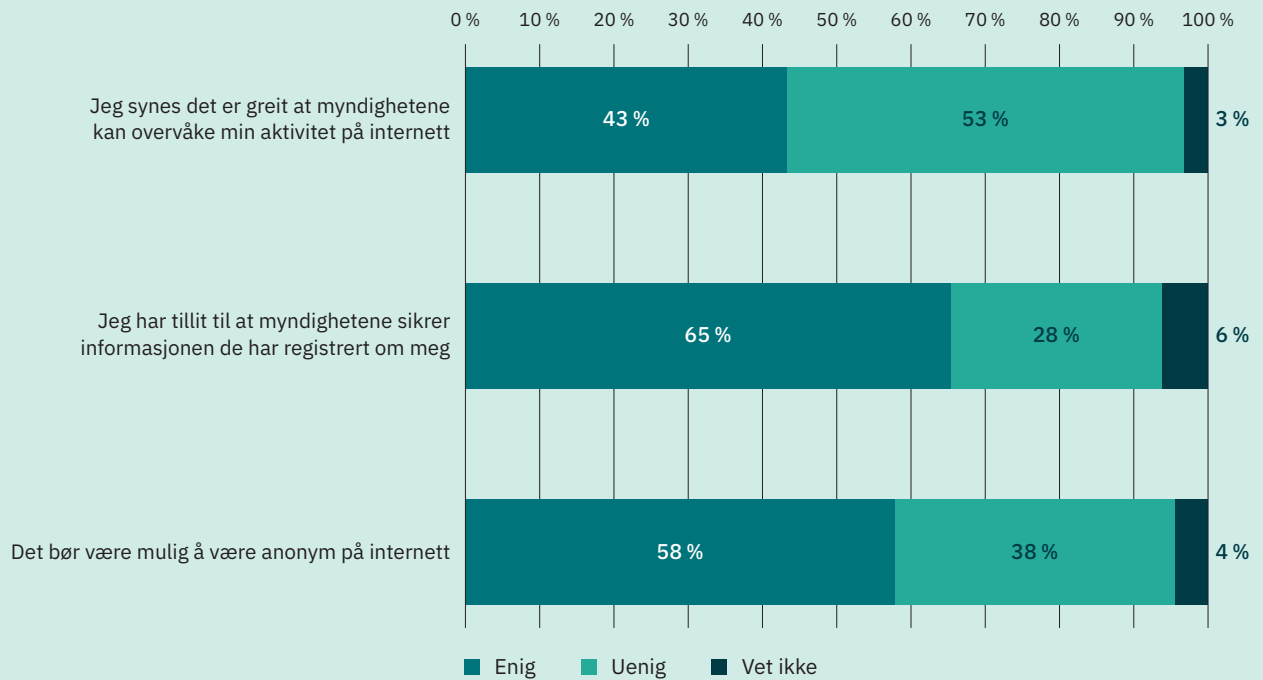
49 prosent er i stor grad bekymret for at andre skal utgi seg for å være dem på nett. Frykten er tydeligst blant personer over 55 år, der 58 prosent oppgir at de er bekymret for ID-tyveri.

Nærmere 4 av 10 nordmenn frykter også at de skal bli lurt til å gi fra seg sensitiv informasjon som passord, kortinformasjon, betalingsopplysninger eller BankID. Samtidig har 28 prosent liten eller ingen tillit til at myndighetene beskytter informasjonen som er registrert om dem.

Tallene viser at bekymringen ikke bare handler om datainnsamling, men også om hvor vanskelig det er å ha oversikt når informasjon først er delt og spredt mellom ulike tjenester.

Myndigheter

Hvor enig eller uenig er du i følgende påstander?

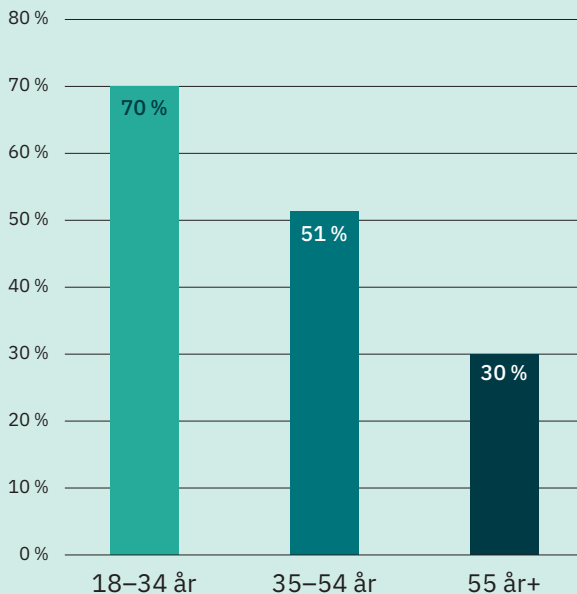


58 %

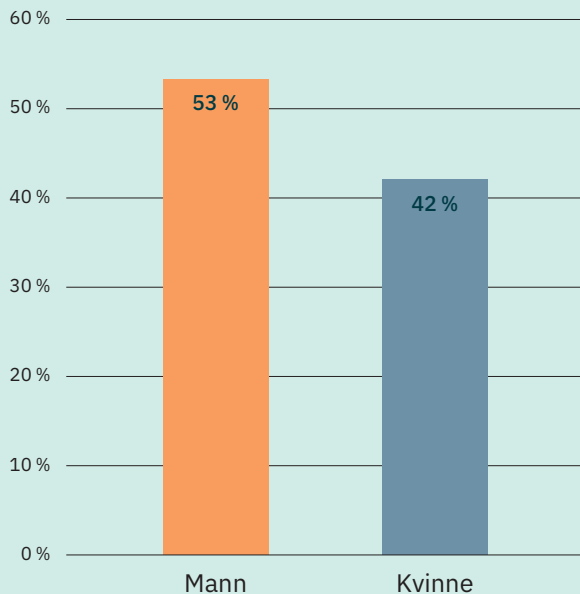
av nordmenn er bekymret
for at virksomheter samler inn
informasjon om hva de gjør på nett

Bruker tekstbaserte KI-tjenester ukentlig eller oftere

Alder



Kjønn



KI gjør svindel mer personlig

Kunstig intelligens forsterker behovet for å ha oversikt over egne digitale avtrykk. Teknologien kan tilpasse språk, tone og innhold slik at meldinger og henvendelser fremstår mer troverdige for mottakeren.

Nærmere 8 av 10 nordmenn tror KI gjør dem ekstra utsatt for svindelforsøk.

8 av 10

nordmenn tror KI gjør dem
ekstra utsatt for svindelforsøk

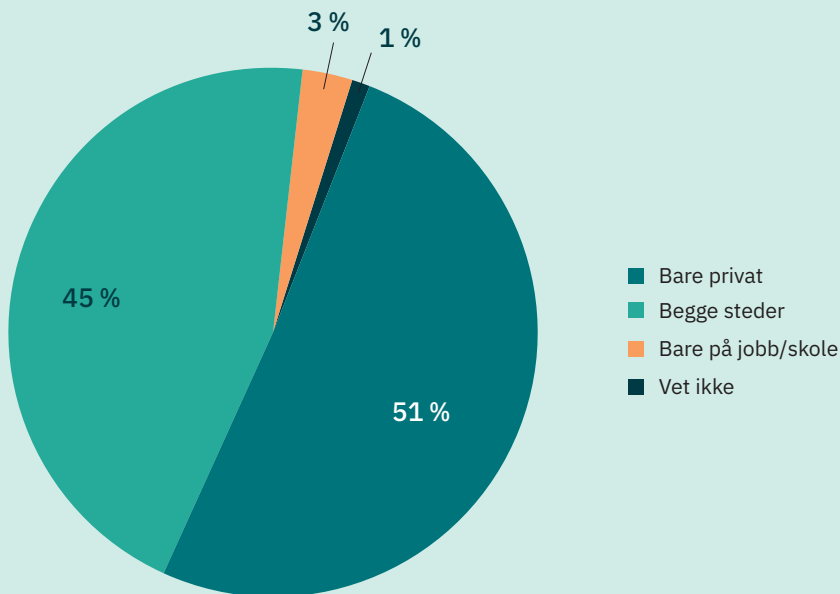
Flere bruker KI – og flere deler informasjon

48 prosent av nordmenn bruker tekstbaserte KI-tjenester som ChatGPT, Copilot, Gemini eller lignende ukentlig eller oftere. Bruken er klart høyest blant dem mellom 18 og 34 år, der 70 prosent bruker slike tjenester ukentlig. Blant dem over 55 år er andelen 30 prosent.

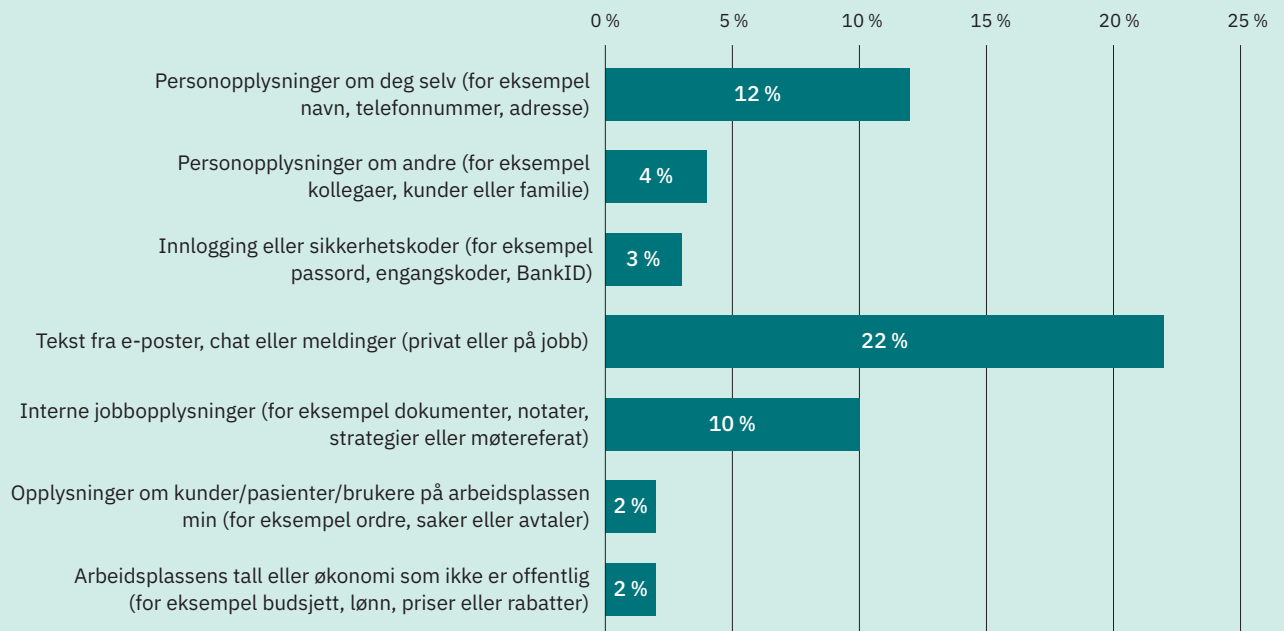
Rundt halvparten av KI-brukerne bruker tjenestene bare privat, mens omtrent like mange også bruker dem på jobb eller skole.

Blant dem som bruker tekstbaserte KI-tjenester eller KI-svar i søkemotorer ukentlig eller oftere, oppgir 12 prosent at de har delt personopplysninger om seg selv. 10 prosent har delt interne jobbopplysninger. Rundt 3 prosent har delt innlogging eller sikkerhetskoder, 2 prosent har delt arbeidsplassens interne økonomitall, og 2 prosent har delt opplysninger om kunder, pasienter, eller brukere på arbeidsplassen.

Hvor brukes KI

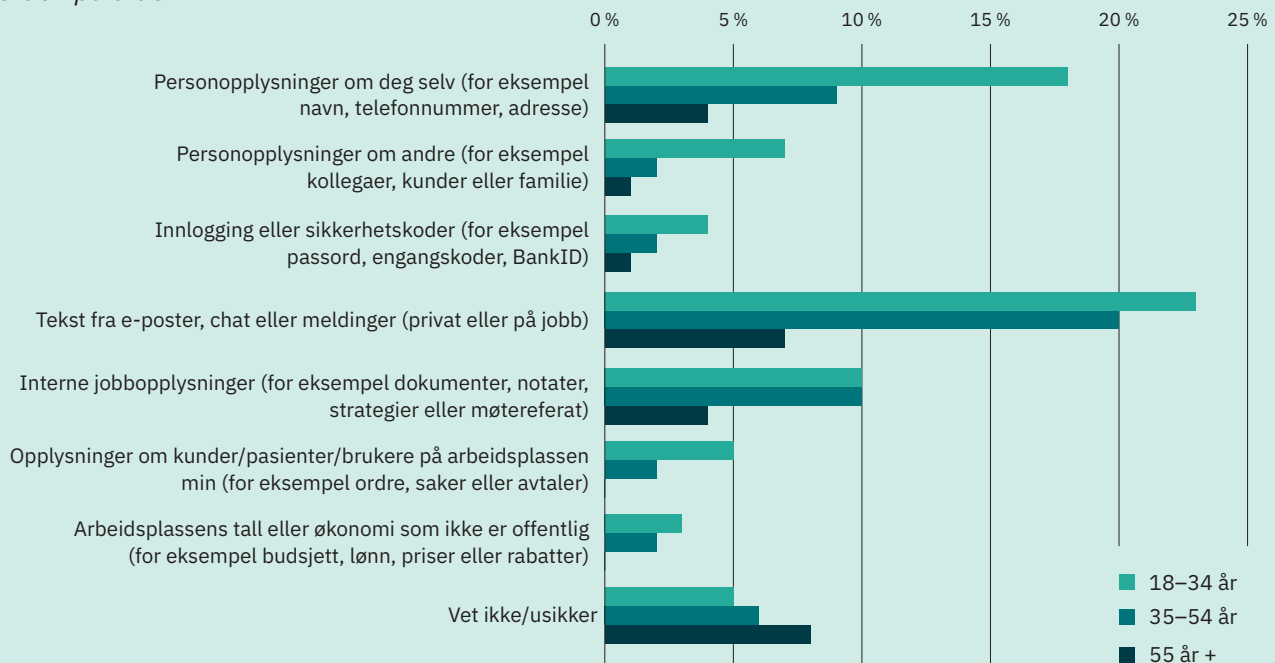


Opplysninger de som bruker tekstbaserte KI verktøy eller KI søkemotorsvar har lagt inn



Opplysninger lagt inn i KI-verktøy

Fordelt på alder



Andelen av de unge deler gjennomgående mer informasjon med KI-tjenester enn andre aldersgrupper.

Samtidig forbinder 65 prosent av nordmenn det å legge inn personlig informasjon i KI-verktøy med høy risiko. Foruten å dele passord eller BankID med andre er dette blant aktivitetene nordmenn vurderer som mest risikable på nett. 37 prosent oppgir også at de har latt være å bruke KI-verktøy som ChatGPT, Copilot eller lignende av frykt for kriminalitet eller andre ubehageligheter.

Del mindre enn du kan

Utfordringen handler ikke bare om hvordan KI-modellene fungerer, men om hva som skjer med informasjonen etter at den er delt. Tekst, dokumenter, bilder og personopplysninger kan lagres, analyseres og brukes videre uten at brukeren har full oversikt.

For privatpersoner kan det handle om helseopplysninger eller private meldinger. For virksomheter kan det være interne vurderinger, økonomitall og kunde- eller pasientinformasjon.

Når du ikke vet sikkert hvor informasjonen havner, bør terskelen være lav for å la være. En enkel hovedregel er å ikke legge inn informasjon i åpne KI-tjenester, som du ikke ville delt i en åpen digital kanal.

Resultatet er et risikobilde som er mindre synlig, men mer personlig. Det handler ikke lenger bare om virus eller hacking, men om hvem du er, hva du har delt og hvordan informasjonen kan brukes mot deg.

Når du ikke vet sikkert hvor informasjonen havner, bør terskelen være lav for å la være. En enkel hovedregel er å ikke legge inn informasjon i åpne KI-tjenester, som du ikke ville delt i en åpen digital kanal.

Hjernespesialist: Øvelse gjør fremdeles mester

Hvorfor gjør vi ting på nett, som vi vet kan være risikable? Ifølge hjernespesialist Marte Roa Syvertsen skyldes det ikke først og fremst mangel på kunnskap, men at hjernen vår er utviklet for en annen virkelighet enn den digitale.

– Vi er ikke biologisk rustet for å håndtere det samfunnet vi lever i nå. Hjernen vår er tilpasset mammutjakt-verden, samtidig som vi har utviklet et samfunn som er langt mer komplisert. Det gapet blir bare større jo mer vi finner på med våre egne hjerner. Siste skudd på stammen er kunstig intelligens, sier hun.

Syvertsen er lege med doktorgrad i nevrologi og forskningssjef ved Drammen sykehus, Vestre Viken. Hun har en særlig interesse for hjernen, hjerneutvikling, beslutninger og læring, og hun har skrevet flere bøker om temaet.

Hvorfor gjør vi ting vi vet er risikable?

– Veldig mye av det vi gjør, er ubevisst. Vi bare gjør det. Etterpå rasjonaliserer vi lynkjapt og finner på en grunn for å rettferdiggjøre valget. Veldig ofte tror vi at vi har tatt et informert og bevisst valg, mens vi egentlig har vært instinktstyrt. Kunnskap om risiko fører derfor ikke automatisk til en tryggere handling, sier Syvertsen.

Samtidig mangler digital kommunikasjon ofte signalene hjernen bruker for å vurdere andre mennesker – for eksempel om noen forsøker å lure oss.

– Hjernen vår er et relasjonsorgan. Vi er laget for nærkontakt. Vi leser ansiktsuttrykk, tonefall, øyekontakt og små trekninger i ansiktsmuskulaturen. Alle disse inntrykkene er viktige for beslutningsgrunnlaget vårt.

På nett må vi vurdere mer med færre holdepunkter. Det utnytter svindlere når en melding haster, virker personlig, kommer fra noen vi stoler på eller krever at vi godkjenner noe med en gang.

– Det er bare en bitte liten del av atferden vår som vi faktisk har kontroll på med bevisst vilje. Instinktene styrer nesten alt, og når det gjelder digital sikkerhet, er de instinktene akterutseilt, for å si det mildt.

Er det nok å vite hva som er trygt?

– Nei. En ting er det teoretiske: at man hører foredrag, leser bøker eller tar kurs. Men så er det den praktiske gjøredelen, den som bygger ferdighet og atferdsmønstre, sier Syvertsen.

Kunnskapen må ligge i bunn. Folk må vite hva svindel er, hvilke situasjoner som bør få dem til å stoppe opp, hvorfor tottrinnslogging virker, og hvorfor BankID og passord må beskyttes og aldri deles med andre.



Kunnskapen må først på plass.
Deretter må den trenes på,
brukes og repeteres til tryggere
reaksjonsmønstre får bedre feste.

– Marte Roa Syvertsen

Øvelse bygger nye hjernebaner

– Hvis vi aktiverer bestemte nettverk i hjernen, blir de automatiske og mer effektive. Gjennom bruk kan vi lage nye baner i hjernens mønster og atferdsmønstre. Når vi bruker dem mye nok, blir de en del av det ubevisste.

Derfor mener hun at «øvelse gjør mester» også gjelder digital sikkerhet. Hun sammenligner det med å lære å kjøre bil. I starten er alt nytt, bevisst og krevende. Etter hvert tar automatiserte mønstre over fordi hjernen har gjort oppgaven mange nok ganger. Litt som når en erfaren sjåfør kommer fram uten å huske særlig mye av selve kjøreturen.

– Hvis man har opplevd å bli lurt, er det vondt. Men det er også en praktisk erfaring du lærer mye av. Da har du vært i det landskapet før, og hjernen er bedre forberedt neste gang.

Hvordan skal vi unngå å bli lurt av KI?

– Kunstig intelligens gjør svindel vanskeligere å avsløre fordi flere gamle faresignaler viskes ut. Språket blir bedre, bildene mer troverdige, og lyd og video kan etterligne mennesker og situasjoner på måter som tidligere var langt mindre tilgjengelige.

Syvertsen mener erfaring med bruk av KI-verktøy gir hjernen trening i rytmen, setningsstrukturen, bildespråket og de små avvikene som ofte følger med kunstig generert innhold.

– Det er mer som å lære språk. Du skal høre, lese og eksponere deg masse. Gradvis lager du koblinger, så du vet at dette hører sammen, og dette hører ikke sammen.

Hva er det viktigste rådet?

– Dette er unaturlig for oss. Det er ikke automatisk. Vi må lære det inn. Men det kan vi jo gjøre, for vi klarer å lære oss bilkjøring. Vi klarer å lære oss veldig komplekse ting, men da må man eksponeres for det og gjøre det.

Kunnskapen må først på plass. Deretter må den trenes på, brukes og repeteres til tryggere reaksjonsmønstre får bedre feste.

– Vi får ikke forandret DNA-et vårt. Vi får ikke evolusjonert oss ut av dette. Men vi kan bygge nye mønstre. Vi kan øve opp reaksjoner. Og vi kan gjøre tryggere valg mer automatiske.

Digital dømmekraft: Når kunnskap ikke er nok

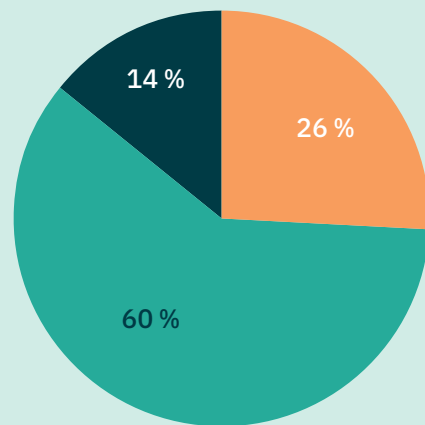
Selv om de fleste nordmenn har god kunnskap om digitale trusler og hvordan de skal beskytte seg, oppgir mer enn 1 av 4 at de bevisst tar risiko på nett.

Dette skjer i et trusselbilde der svindelforsøkene allerede er blitt mer målrettede, mer troverdige og vanskeligere å avsløre.

Når svindelen blir mer troverdig, blir også digital dømmekraft viktigere og vanskeligere. Årets undersøkelse viser at mange mener de har denne kompetansen. I underkant av 70 prosent oppgir at de vet hvordan de skal beskytte seg på nett. Mellom 67 og 74 prosent sier de kan bruke grunnleggende tiltak, som å vurdere avsender, sjekke lenker og vedlegg og ta i bruk tottrinnspålogging.

Tar sjanser

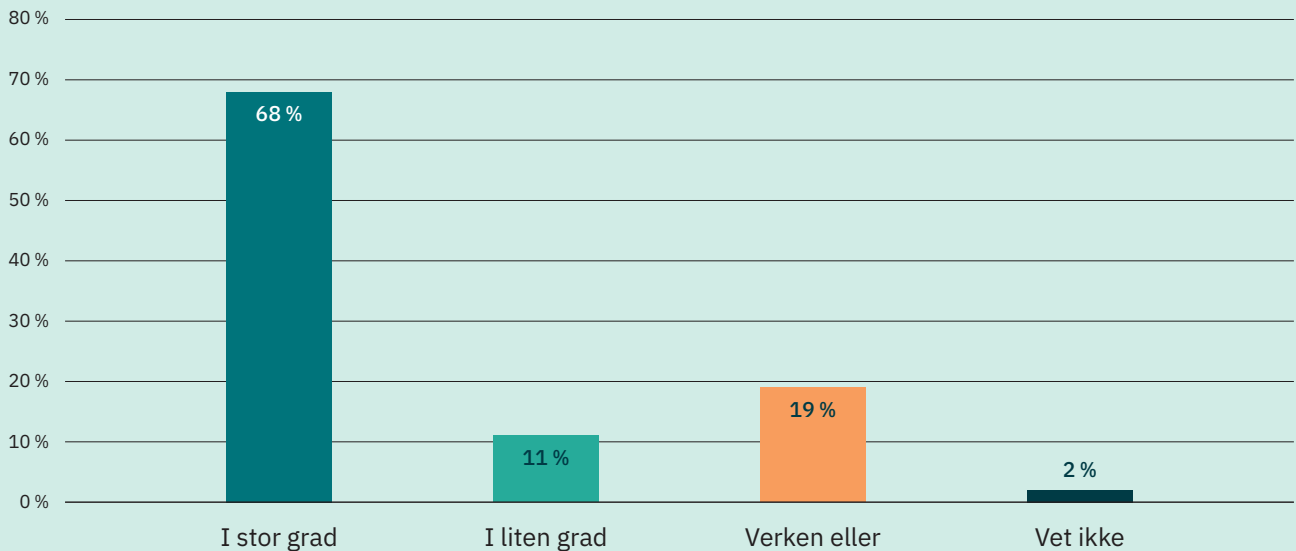
Det hender jeg tar sjanser som jeg vet er risikable på internett



Ja Nei Vet ikke

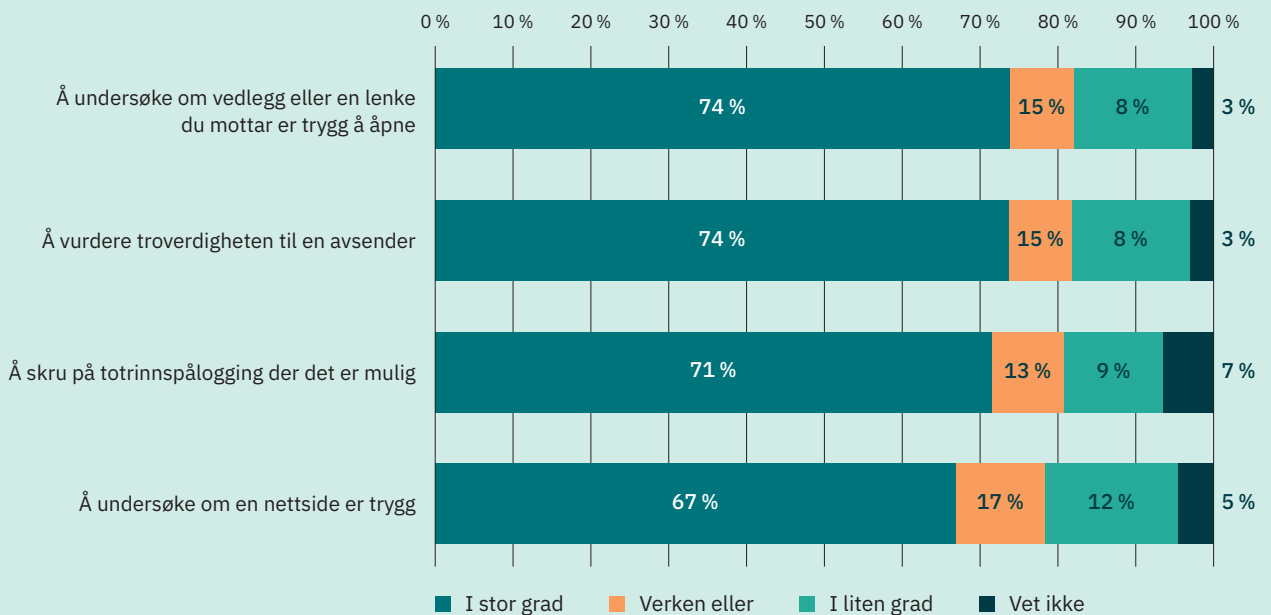
Evne til generell sikkerhetsvurdering

I hvilken grad vil du si du er i stand til å vurdere hva som er trygt eller utrygt å gjøre på internett generelt?



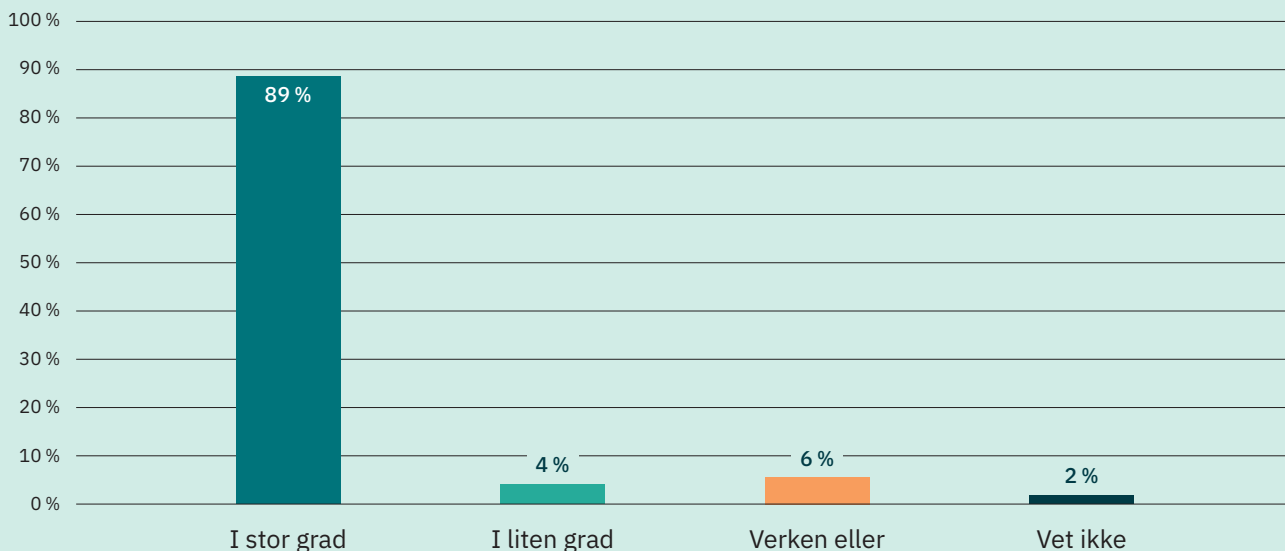
Evne til sikkerhetstiltak

I hvilken grad mener du at du vil klare å gjøre følgende?



Dele BankID med andre

I hvilken grad forbinder du å dele BankID med andre med høy risiko?



Angrepene går via mennesker

Digitale angrep handler i dag sjelden bare om å bryte seg inn i systemer. I stedet forsøker angripere ofte å få oss til å gjøre noe selv: klikke på en lenke, godkjenne en innlogging, dele informasjon eller gjennomføre en betaling. Når angrep lykkes, er det sjelden bare fordi teknologien svikter. Det er fordi vurderingen i øyeblikket gjør det.

Helt vanlige situasjoner får dermed større betydning: en SMS fra banken, en e-post som haster, eller en forespørsel fra noen vi stoler på.

Den klassiske «Hei mamma»-svindelen illustrerer hvordan slike angrep utvikler seg. Tidligere kunne svindelen bestå av en enkel tekstmelding om at barnet hadde mistet mobilen og trengte penger raskt. Med KI kan den samme svindelen bli langt mer troverdig og personlig. Meldingen kan vise til konkrete hendelser, steder eller personer hentet fra sosiale medier, og følges opp av lyd eller video som etterligner noen mottaker kjenner.

Svindelen blir ikke nødvendigvis ny. Det som endrer seg, er at den blir mer troverdig og vanskeligere å gjennomskue.

Vet hva som er risikofyllt – men gjør det likevel

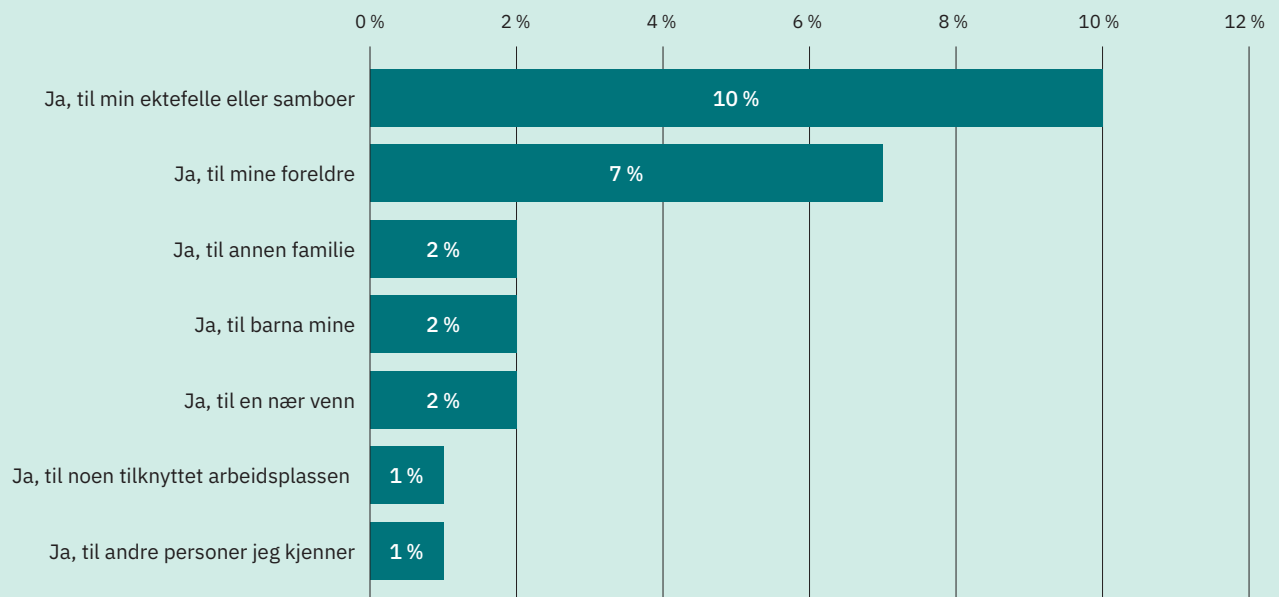
Det som i liten grad har endret seg, er avstanden mellom hva nordmenn vet er risikabelt – og hva de rent faktisk gjør.

- 89 prosent vurderer det som høy risiko å dele BankID. Likevel har 10 prosent latt andre bruke sin BankID det siste året, og 26 prosent har brukt andres.
- 69 prosent mener det er risikabelt å bruke samme passord flere steder, men 20 prosent gjør det likevel.
- 55 prosent mener det er risikabelt å ikke bruke tottrinnslogging. Likevel oppgir 41 prosent at de ikke bruker tottrinnslogging der det er mulig.
- 17 prosent av ansatte i mindre bedrifter som bruker KI-verktøy på jobb, oppgir at de har brukt dem på en måte som ikke er tillatt i bedriften.¹
- 26 prosent oppgir at de tar sjanser på nett de vet er risikable.

Risikoadferd er ikke lenger et unntak – det er en del av den digitale hverdagen.

¹ NorSIS i NSM sin bedriftsundersøkelse, 722 heltidsansatte i virksomheter med 11–50 ansatte. 214 av de spurte har ledende roller, mens 508 har vanlige stillinger.

Har brukt andres BankID



Når gevinsten frister mer enn risikoen bremser

Risiko er ikke en fast størrelse – den er situasjons- og personbetinget. Når gevinsten oppleves som konkret og nær, mens konsekvensene virker mindre sannsynlige og ligger lenger frem i tid, tar vi oftere sjansen.

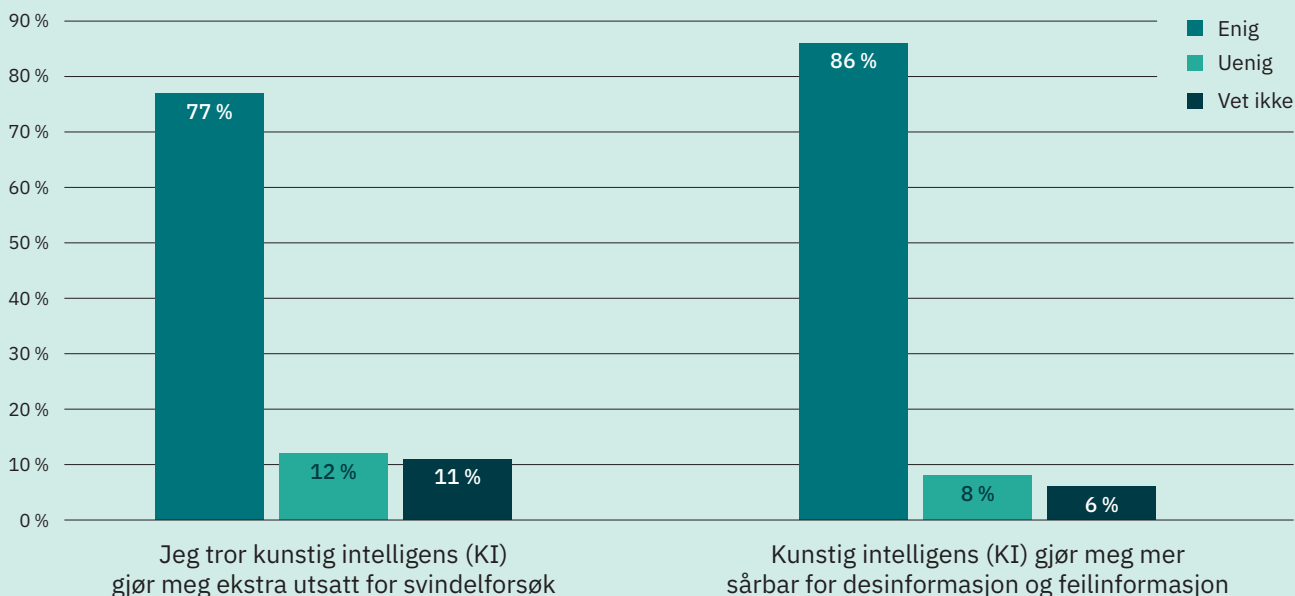
En Instagram-annonse viser joggesko til halv pris, siste dag. Vi tenker at det kan være en falsk nettbutikk. Samtidig er tilbudet godt, og risikoen fremstår som liten: Det verste som kan skje, er at varen aldri kommer.

Det som ofte undervurderes, er hvor lett informasjon som deles i én situasjon, kan brukes videre i nye svindelforsøk. Kortinformasjon, kontaktopplysninger eller innloggingsdata kan raskt få verdi for kriminelle aktører.

Dette gapet mellom hva vi vet og hva vi gjør blir mer alvorlig i et trusselbilde som i økende grad retter seg mot mennesker, ikke teknologi.

Datteren min sier bare: «Ser du ikke at det er KI?» Jeg tror faktisk man ser det lettere jo mer man bruker KI selv.

Påstander om KI



Klar over KI-risikoen – men må handle langsommere

Utviklingen innen kunstig intelligens forsterker dette bildet. Teknologien gjør det enklere å lage meldinger, bilder, lyd og henvendelser som er vanskelige å skille fra ekte.

77 prosent mener KI gjør dem mer utsatt for svindelforsøk, og 86 prosent mener teknologien gjør de mer sårbare for desinformasjon. Over halvparten er bekymret for å bli utsatt for KI-basert svindel.

Når falske henvendelser blir mer troverdige, holder det ikke alltid å vite at risikoen finnes. Flere situasjoner vil kreve at folk bruker mer tid før de klikker, svarer, godkjenner eller deler informasjon.

Det kan oppleves både tungvint og frustrerende å måtte dobbelt- og trippelsjekke det som før virket enkelt. Samtidig er det nettopp dette digital dømmekraft handler om: å stoppe opp, sjekke avsender og bruke noen ekstra sekunder før man handler.





Foto: KucherAV / Getty Images

Det samme mønsteret går igjen for kunstig intelligens. Blant 18–34-åringer oppgir 18 prosent at de deler personopplysninger om seg selv i KI-verktøy som ChatGPT og Copilot. I befolkningen samlet er andelen 9 prosent.

Samtidig er eldre mer bekymret for digital svindel og ID-tyveri enn yngre. Forskjellene peker på et tydelig generasjonsskille: yngre opplever i større grad mestring og tar flere sjanser, mens eldre oftere opplever større usikkerhet på nett.

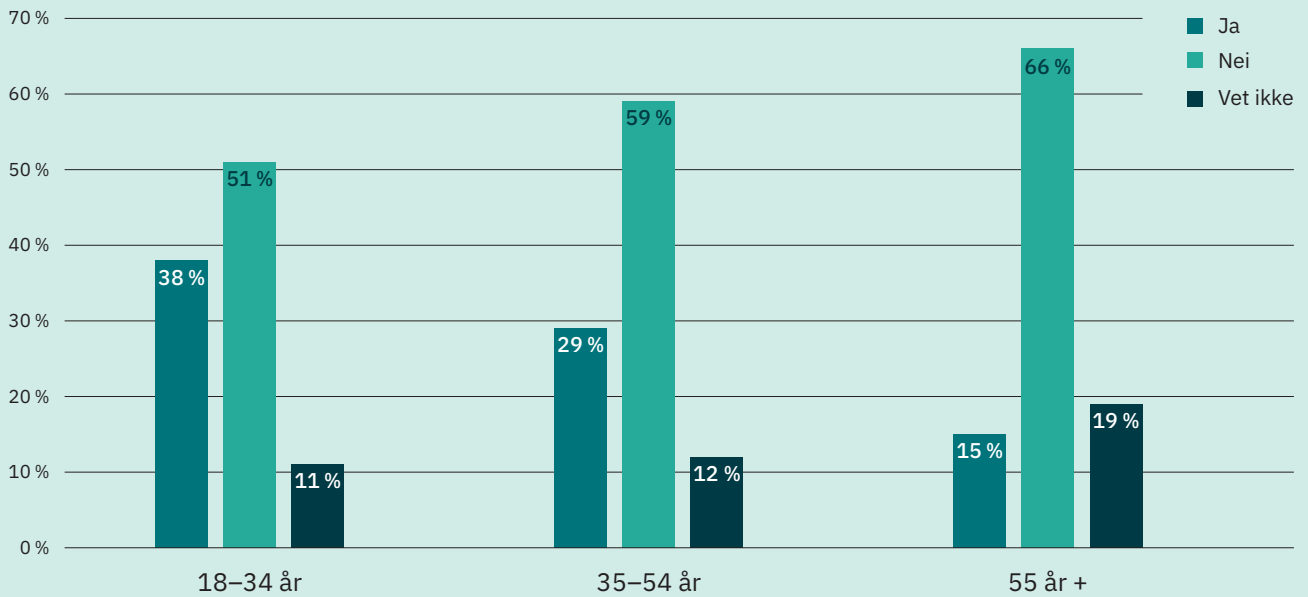
Unge tar flest sjanser – eldre er mest utrygge på nett

Det er de yngste som tar klart mest risiko på nett. I 2026 oppgir 38 prosent av nordmenn mellom 18 og 34 år at de tar bevisste sjanser på nett, mot 15 prosent blant dem over 55 år.

Menn tar også oftere risiko enn kvinner: 30 prosent mot 21 prosent.

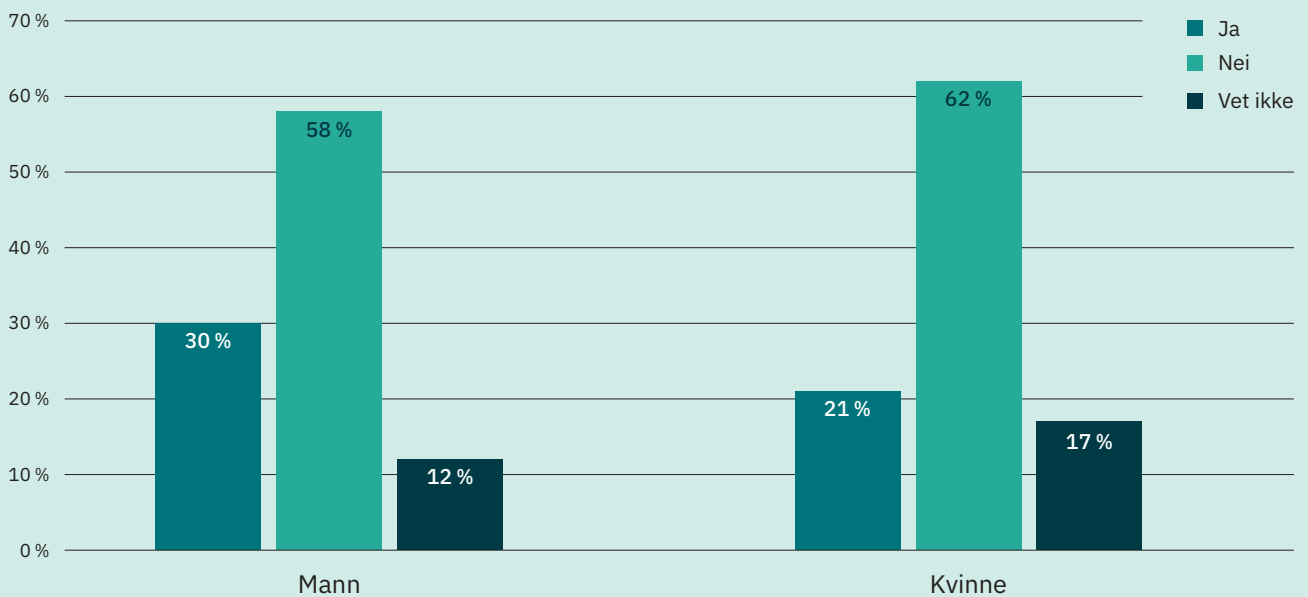
Tar sjanser, fordelt på alder

Det hender jeg tar sjanser som jeg vet er risikable på nett



Tar sjanser, fordelt på kjønn

Det hender jeg tar sjanser som jeg vet er risikable på nett



Digital trygghet – hvem kan vi stole på?

Samtidig som et flertall av nordmenn mener myndighetene gjør for lite for å beskytte dem mot datakriminalitet, tror også under halvparten at politiet vil hjelpe dersom de selv blir rammet.

54 prosent vet ikke eller er uenige i at politiet vil hjelpe dem dersom de blir utsatt for datakriminalitet. Skepsisen er klart størst blant menn. Dette har vært et relativt stabilt bilde gjennom de ti årene nordmenns digitale sikkerhetskultur er kartlagt.

Samtidig viser Politiets innbyggerundersøkelse¹ for 2025 at 73 prosent har høy tillit til politiet generelt: Nordmenn har høy tillit til politiet som institusjon, men lavere tillit til at de får hjelp når kriminaliteten skjer digitalt.

Mange vil ha sterkere beskyttelse mot digital kriminalitet, men ikke nødvendigvis mer statlig kontroll.

Flere åpner for private aktører – færre vil ha overvåkning

Synet på myndighetenes innsats har også holdt seg stabilt de siste årene. 43 prosent er helt eller delvis uenige i at myndighetene gjør nok for å beskytte dem mot kriminalitet på nett. Ytterligere 17 prosent svarer «vet ikke».

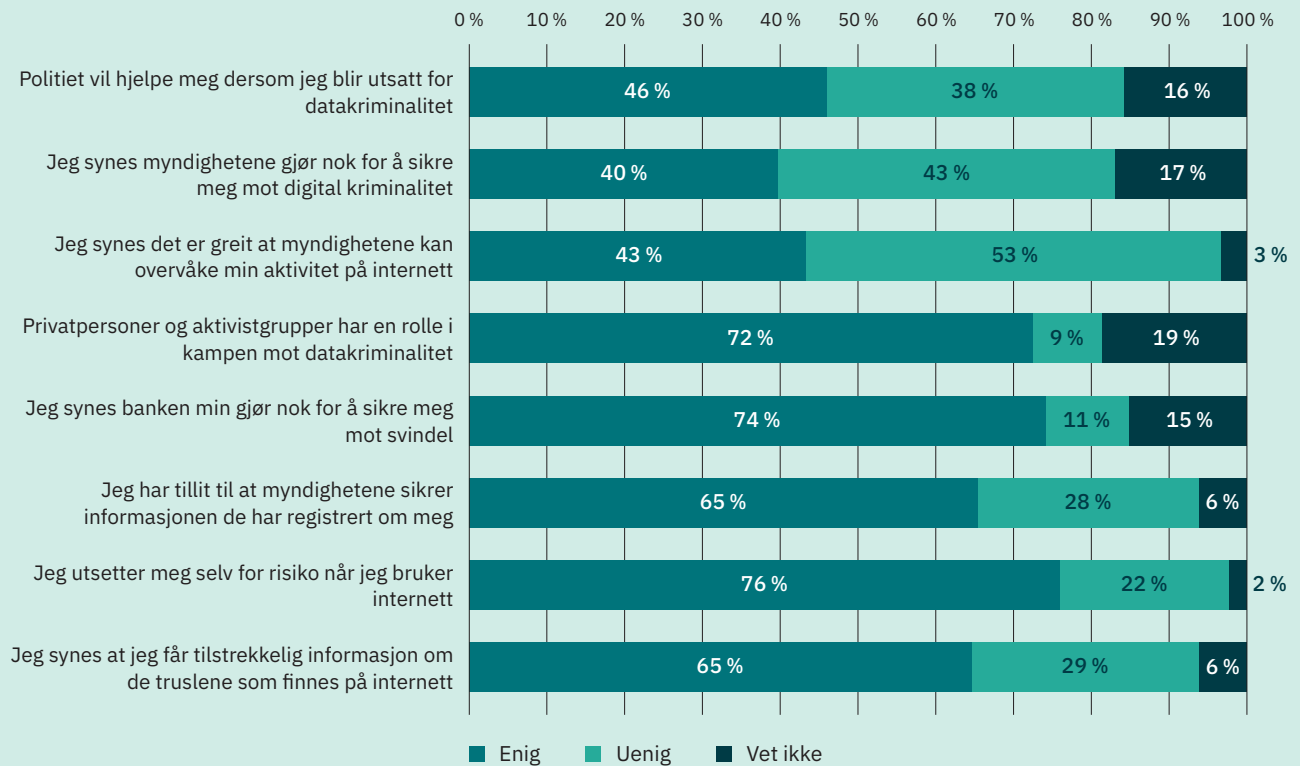
Mange etterlyser sterkere beskyttelse, men befolkningen er delt i synet på hvilke virkemidler som er akseptable. 43 prosent mener det er greit at myndighetene kan overvåke aktiviteten deres på nett, mens 53 prosent er imot. Over tid har andelen som er positive til slik overvåkning, gått ned.

I samme periode har støtten til at andre enn politi og myndigheter skal ha en rolle i kampen mot datakriminalitet, økt. I 2017 var 62 prosent helt eller delvis enige i at privatpersoner og aktivistgrupper har en rolle i kampen mot datakriminalitet. Nå er andelen 72 prosent, relativt likt fordelt på kjønn og alder. Bare ni prosent er helt eller delvis uenige.

¹ Politiets innbyggerundersøkelse 2025

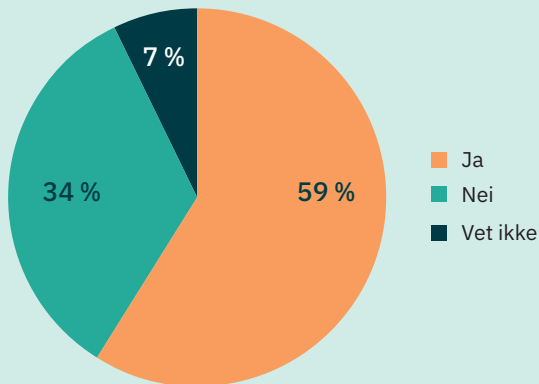
Påstander

Hvor enig eller uenig er du i følgende påstander?

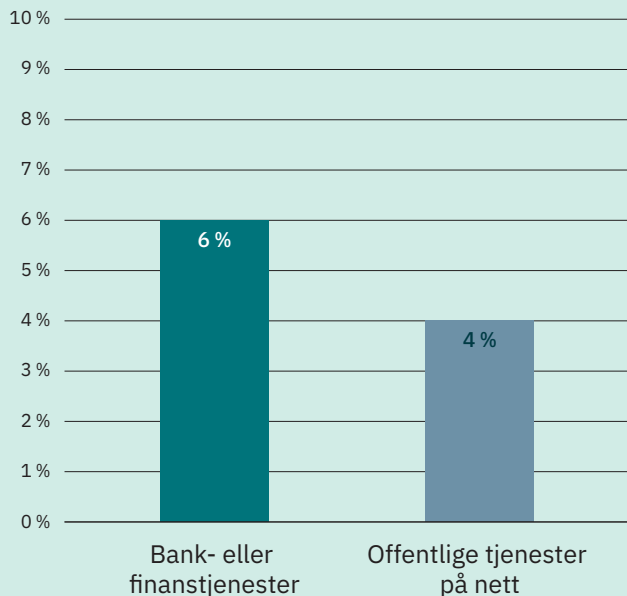


Unngå bruk av tjeneste

Hender det du lar være å bruke en tjeneste på internett fordi du er redd for å bli utsatt for noe kriminelt eller ubehagelig?



Type tjeneste unngått



Bruk betyr ikke trygghet

Tillit til myndigheter, banker og andre sentrale instanser er også viktig.

Tilliten til at bankene beskytter nordmenn mot svindel er høyere enn tilliten til at myndighetene beskytter opplysningene de har registrert om dem. 74 prosent oppgir at banken deres gjør nok for å sikre dem mot svindel. 65 prosent oppgir at de er helt eller delvis enig i at de har tillit til at myndighetene sikrer informasjon de har registrert om dem.

Tilliten til både bankene og offentlige myndigheter på disse punktene er høyere desto eldre respondentene er.

Selv om 59 prosent har sluttet å bruke en netjtjeneste for å unngå kriminalitet eller andre ubehageligheter, er det bare et fåtall som har sluttet å bruke bank- og finanstjenester (6 prosent) eller offentlige tjenester på nett (4 prosent).

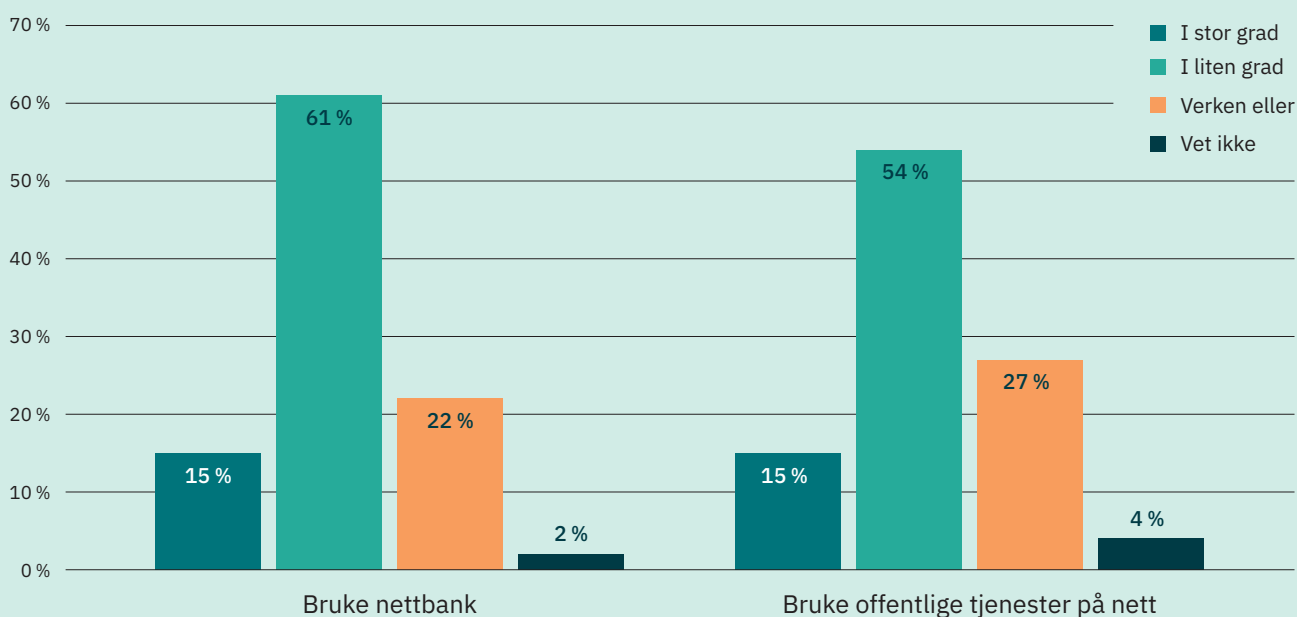
Rundt 15 prosent forbinder allikevel bruk av nettbank med høy risiko. Like mange mener det samme om offentlige tjenester på nett. Det tilsvarer nærmere 700 000 nordmenn over 18 år.

Digitale tjenester som oppleves nødvendige i hverdagen, brukes videre selv når mange forbinder dem med risiko. Det er noe vi er nødt til å forholde oss til da det ikke alltid finnes alternativer. Det gjør tillit til sentrale digitale tjenester stadig viktigere for hvordan samfunnet fungerer.

Digitale tjenester som oppleves nødvendige i hverdagen, brukes videre selv når mange forbinder dem med risiko.

Aktiviteter med høy risiko

I hvilken grad forbinder du følgende aktiviteter med høy risiko?



Hovedsakelig er det meg selv som har ansvaret, men myndighetene og selskapene må også gjøre sitt.

Truslene endrer seg raskt – holdningene saktere

Det digitale trusselbildet har endret seg raskt, og det vokser i omfang. Svindel, sosial manipulering og KI-generert innhold gjør det stadig vanskeligere å skille ekte fra falskt. Angrepene handler ikke lenger bare om tekniske svakheter, men om tillit, dømmekraft og små valg i hverdagen – hjemme eller på jobb – som kan få store konsekvenser.

Likevel viser den tiende årlige undersøkelsen om nordmenns digitale sikkerhetskultur at holdninger og vaner ikke endrer seg i samme tempo. Flere er bekymret, og mange forstår at risikoen finnes. Men det betyr ikke nødvendigvis at vi opptrer tryggere.

Fortsatt mener 7 av 10 at den største risikoen på nett er at noen andre skal gjøre noe mot dem – ikke at de selv skal gjøre en feil. Det er et stabilt mønster: Mange ser fortsatt digital risiko først og fremst som noe som kommer utenfra.

Andelen som oppfatter at de utsetter seg for risiko når de bruker internett, har vært nærmest uendret de siste ti årene. I dag mener 76 prosent at de gjør dette.

Også opplevelsen av informasjon har endret seg lite. 65 prosent mener de får tilstrekkelig informasjon om truslene på internett.

Til sammen peker funnene i samme retning: Nordmenn kjenner igjen risikoen, men holdningene og sikkerhetsvanene flytter seg saktere enn trusselbildet. Å vite at noe er risikabelt er ikke det samme som å handle trygt.

Derfor handler digital sikkerhetskultur ikke bare om mer kunnskap, men om å gjøre den kunnskapen enklere å bruke i hverdagen. Når truslene blir mer troverdige, må trygg digital atferd bli mer praktisk, mer forståelig og lettere å velge – hver gang vi klikker, svarer, deler eller godkjenner.

Det er hver og en av oss sitt ansvar, arbeidsgiveres ansvar, myndighetenes ansvar – og ikke minst plattformeiere og andre store digitale aktørers ansvar.



NorSIS
NORSK SENTER FOR
INFORMASJONSSIKRING

Forsidefoto: Daniel Canibano / Unsplash
Design: Tank Design

Undersøkelsen er utført av Opinion
i februar 2026, 1010 respondenter.

