NorSIS
NORSK SENTER FOR
INFORMASJONSSIKRING

NSM

ID-tyverirapport 2025

Foto: Ilja Hendel/NSM

Færre klassiske ID-tyverier, men flere andre former for misbruk

Over 170 000 nordmenn over 18 år oppgir at de har opplevd å få sin identitet misbrukt, og ytterligere 340 000 har opplevd forsøk på dette.

Mye tyder mye på at det har vært en reell nedgang av den klassiske formen for ID-tyveri. Samtidig er andre former for tyverier av andres identitet, som overtakelse av andres profiler i sosiale medier, stadig mer vanlig. Med KI-bølgen som skyller over landet, vil også nye former for ID-tyveri komme, og det å sikre at én person kun har én identitet i Norge, som ved bruk av biometri, blir bare viktigere.

Mer enn 680 000 nordmenn over 18 år (15 %) oppgir at de har opplevd at noen har tatt over én eller flere av deres kontoer i sosiale medier, eller opprettet en falsk konto i sosiale medier og utgitt seg for å være dem. Dette er en langt større digital trussel for både den enkelte og samfunnet enn det mange tenker over.

Kan føre til forverret psykisk helse: Skam, skyld, redsel og maktesløshet

Årets undersøkelse er den 15. i rekken og dobbelt så stor i antall respondenter. Spørsmålene er justert for bedre å speile det trusselbildet som NorSIS i NSM ser innenfor identitetsfeltet i dag. Den er derfor ikke direkte sammenlignbar med tidligere år.

Undersøkelsen er blitt utarbeidet i et tett samarbeid med Skatteetaten og prosjektet «Samfunnssikkerhet og digitale identiteter (SODI)» ved Institutt for privatrett ved Universitetet i Oslo, og underbygger viktigheten av identitetsforvaltning. Det å få misbrukt sin identitet har ikke bare en økonomisk kostnad for ofrene og samfunnet, det kan også være en ekstrem belasting for den enkelte. Forskningen tyder på at flere av ofrene får en forverret psykisk helse i etterkant, som sterk følelse av skam, skyld, redsel og maktesløshet. I tillegg kan det være en stor praktisk oppgave å forsøke å rydde opp etter et ID-tyveri, og bevise sin uskyld.

Rammer færre nordmenn, men sårbare grupper er blitt mer utsatt

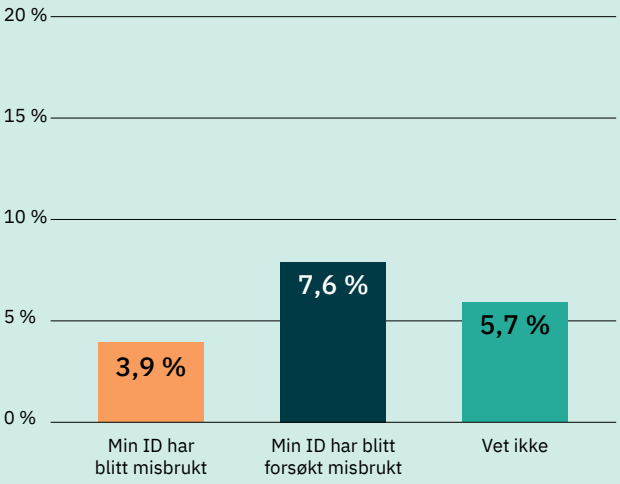
Sammenstilt med andre nyere rapporter over forekomsten av ID-tyveri i Norge tyder imidlertid mye på at spesielt ID-tyveri som innebærer misbruk av andres BankID, pass, førerkort og lignende, har gått ned. Det skyldes trolig både nytt lovverk og strengere krav til bankenes ansvar når dette skjer.

De siste tallene fra Finanstilsynet (Svindelstatistikk H2, 2024)[1] viser at betalingstilbydernes tap som følge av svindel etter sosial manipulering i 2024, til tross for en positiv nedgang i andre halvår, samlet gikk opp hele 42,5 prosent fra 2023. Svindel der svindleren initierer eller modifiserer betalingen, økte med 20,5 prosent fra 2023 til 2024. Sosial manipulering øker med andre ord langt mer enn de «klassiske ID-tyveriene». Bankene stoppet også i andre halvår i fjor svindler for over 1,6 milliarder kroner.

1 Finanstilsynet, https://www.finanstilsynet.no/publikasjoner-og-analyser/svindel-og-svindelstatistikk/2024/h2/svindelstatistikk-andre-halvar-2024

Hvilke typer ID-er har nordmenn benyttet siste to år	
BankID	98,9 %
Pass	35,8 %
Fysisk førerkort	30,9 %
MinID	24,1 %
Nasjonalt ID-kort	15,2 %
Digitalt førerkort	15,1 %
Buypass	7,5 %
Commfides	0,9 %
Annen	1,7 %

Andel misbruk av ID totalt



Selv om den representative undersøkelsen nå inkluderer mer enn 2000 respondenter, er sannsynligvis sårbare grupper som arbeidsinnvandrere, bostedsløse og mennesker i rusmiljø underrepresentert. Blant disse ser vi dessverre at ID-misbruk fremdeles er for vanlig. Det skjer typisk ved at allerede sårbare enkeltpersoner blir lurt, presset, truet og/eller tilbudt betaling for å gi fra seg sin BankID eller annen eID.

Organiserte kriminelle nettverk har i økende grad misbrukt blant annet Skatteetatens systemer ved hjelp av identitetstyveri, noe som har resultert i betydelige økonomiske tap. Skatteetaten har i 2024 alene varslet Oslo politidistrikt om over 100 potensielle lånebedragerisaker knyttet blant annet til dette misbruket.

Må styrke den nasjonale identitetsforvaltningen: Bevissthet og robuste løsninger viktigst

Det at mer enn 1 av 10 nordmenn på et eller annet tidspunkt enten har vært utsatt for et klassisk ID-tyveri, eller har opplevd forsøk på dette, viser at vi fremdeles har en vei å gå i den nasjonale identitetsforvaltningen.

Når en person søker pass eller ID-kort, samler politiet allerede inn biometri (som ansiktsbilde) for å bekrefte hvem det er. Denne biometrien søkes mot alle andre bilder som er tatt, for å sikre at det er rett person og unngå «doble» identiteter. Neste steg er å få opplysningen overført til Folkeregisteret slik at man får status som «UNIK». Dette betyr at ingen andre kan få utstedt pass eller ID-kort i den personens identitet fordi de er biometrisk knyttet til sitt fødselsnummer. På den måten blir alles identiteter sikrere og bedre beskyttet mot ID-tyveri.

Samtidig må alle bli mer bevisste på å beskytte identiteten sin: bruke totrinnspålogging, aldri dele BankID, og være kritisk til forsøk på sosial manipulering. Å miste kontrollen over egen identitet rammer ikke bare en selv, det svekker hele samfunnet. Derfor trengs bedre, sikrere og mer robuste løsninger for ID, og biometri er en viktig del av svaret.

Å miste kontrollen over egen identitet er en belastning vi ikke har råd til – verken som enkeltpersoner eller samfunn. Derfor trengs en tryggere og mer effektiv identitetsforvaltning.

Foto: Andrey K

KAPITTEL 1

ID-tyveri rammer alle: Reell nedgang de siste to årene

ID-tyveri er noe som rammer alle, uavhengig av kjønn, alder, bosted, inntekt eller forhold til egen datasikkerhet. Bare i løpet av de siste to årene har nærmere 70 000 nordmenn blitt utsatt for dette.

Årets undersøkelse tyder likevel på at antall ID-tyverier har gått ned fra 2023 til 2025. Dette til tross for at årets undersøkelse er større og spørsmålsstillingene noe endret, og derfor ikke direkte kan sammenlignes med den som ble gjennomført for to år siden. Mens 3,4 prosent av de spurte i 2023 oppga at de hadde vært utsatt for ID-tyverier i løpet av de to siste årene, var det tilsvarende tallet i 2025 1,5 prosent – tilsvarende rundt 70 000 nordmenn over 18 år.

Reell nedgang etter nye sikkerhetstiltak og lovverk

En Høyesterettsdom i 2022 skjerpet bankenes ansvar ved BankID-svindel, for eksempel de såkalte Olga-svindlene. Her ble det fastslått at banker ikke kan fraskrive seg hele ansvaret når kunder blir lurt av profesjonelle svindlere til å oppgi sikkerhetsinformasjon og får kontoen sin tømt. I etterkant har foretakene økt sitt fokus på sikkerhetstiltak. Den nye finansavtaleloven og flere sikkerhetstiltak har trolig bidratt til en nedgang i lånesvindel basert på misbruk av BankID, og lignende typer svindel. Samtidig har utfordringene med svindel ved bruk av sosial manipulasjon vært økende.

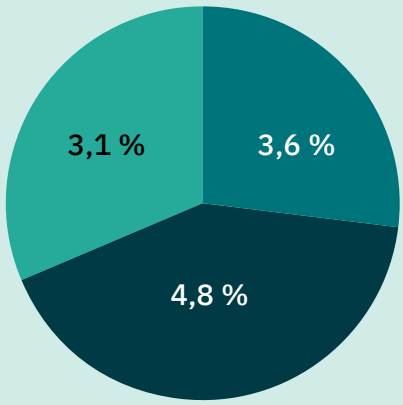
3,9 prosent av de spurte oppgir at de på et eller annet tidspunkt har vært utsatt for ID-tyveri. Flertallet av disse (nærmere 5 av 10) oppgir at dette skjedde for mer enn fem år siden.

På «bekymringstoppen»: 44 prosent er i stor grad bekymret for ID-tyveri

ID-tyveri er blant de negative hendelsene som nordmenn er mest bekymret for å bli utsatt for. Ifølge Politiets Innbyggerundersøkelse for 2024[1] var det bare alvorlige trafikkulykker, tyveri på offentlig sted og skremmende eller plagsom atferd som nordmenn fryktet mer eller like mye som ID-tyveri. Denne undersøkelsen bekrefter langt på vei dette. Hele 44 prosent av de spurte oppgir at de i stor grad er bekymret for å bli utsatt for ID-tyveri/ID-misbruk i fremtiden.

1 Politiet, https://www.politiet.no/om-politiet/tall-og-fakta/innbyggerundersokelsen

Fordeling av de som har fått sin ID misbrukt



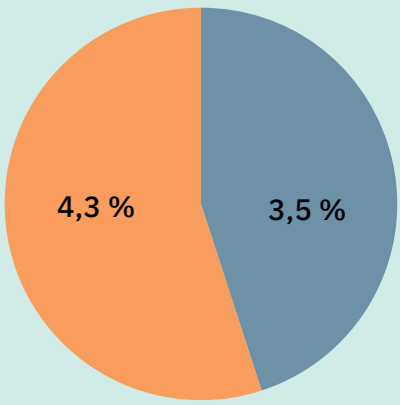
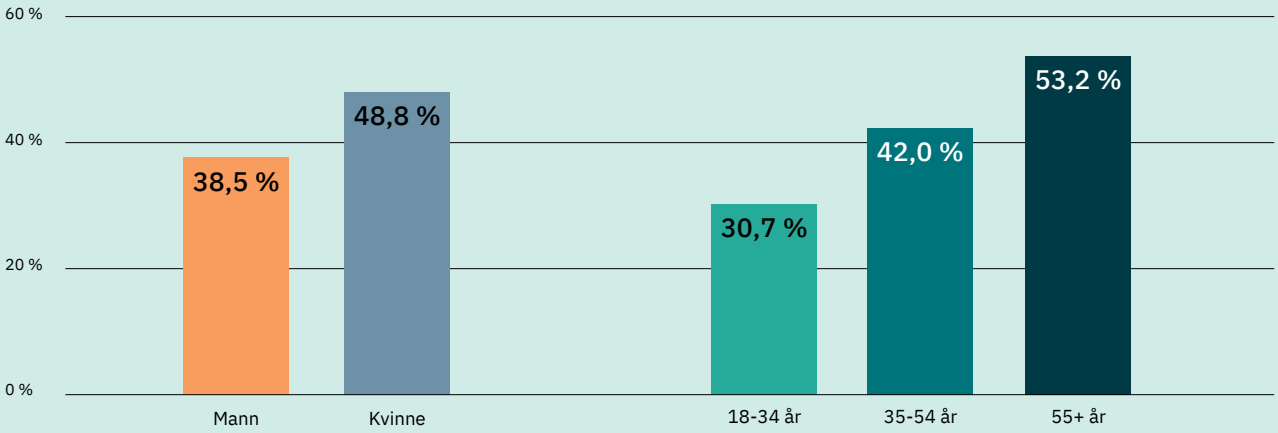


Foto: Ilja Hendel/NSM

Bekymret for ID-tyveri i fremtiden



Misbrukes mest til netthandel i andres navn

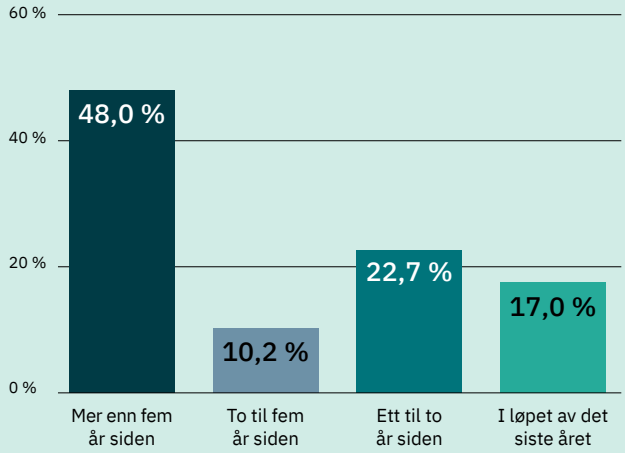
De vanligste formene for misbruk av nordmenns identitet er ifølge undersøkelsen at andre har handlet en vare på nett i offeret sitt navn. Deretter følger at andre får tilgang til en tjeneste, som strømmetjeneste eller mobilabonnement.

I fjor kom det nye regler som krever at man må fremlegge gyldig identitetsbevis for å kjøpe kontantkort eller opprette mobilabonnement – nettopp for å beskytte forbrukere mot ID-tyveri. De fleste ID-misbruk skjer ifølge undersøkelsen med betalingskort/kredittkort. Dette har skjedd i hele 1 av 3 tilfeller. BankID, enten med kodebrikke eller app på mobil, har vært benyttet i 15 prosent av tilfellene.

Flertall positive til opplysninger om ID-tyveri i Folkeregisteret

Nærmere 6 av 10 nordmenn (57 %) oppgir at de i stor grad er positive til at opplysninger om at de har vært utsatt for ID-tyveri burde fremkomme av Folkeregisteret. Slik informasjon kan bidra til å redusere konsekvensene av et ID-tyveri. Bare 1 av 10 (9 %) er i liten grad positive til et slikt tiltak, mens resten er ifølge undersøkelsen usikre.

Når ble din ID misbrukt sist



Hvilke ID-er er misbrukt	
Betalingskort/kredittkort	33,3 %
BankID	15,3 %
Pass	2,9 %
Annet fysisk ID	2,5 %
Førerkort	2,4 %
MinID	1,2 %
Buypass	1,2 %
Commfides	1,2 %
Nasjonalt ID-kort	0,0 %

Dette er ID-tyveri

Identitetsmisbruk, også kalt ID-tyveri, skjer når noen uten samtykke bruker dine person-opplysninger for å utgi seg for å være deg.

Dette kan innebære bruk av fødsels- eller d-nummer, BankID, betalingskort, fysisk legitimasjon eller lignende for å overføre penger fra kontoen din, kjøpe varer, registrere telefonabonnement, søke om kredittkort eller lån, eller endre opplysninger i offentlige registre i ditt navn.

KAPITTEL 2

Misbruk og metoder: 30 000 har fått misbruk sin ID til pengeoverføringer

Mer enn 30 000 nordmenn har opplevd at identiteten deres er misbrukt til å overføre penger fra deres private kontoer.

Selv om de klart vanligste tilfellene av ID-tyveri over tid har skjedd i forbindelse med netthandel (32 % av de som har opplevd ID-tyveri) og abonnement på forskjellige typer tjenester (21 %), er det også et større antall nordmenn som har opplevd at gjerningspersoner har overført penger fra bank-kontoen deres. Ifølge årets ID-tyveriundersøkelse oppgir hele 18 prosent av de som har vært utsatt for ID-tyveri, nettopp dette. Det tilsvarer i overkant av 30 000 nordmenn over 18 år.

Titusener har tapt mer enn 10 000 kroner på ID-tyveri

Mens 21 prosent av de som har opplevd ID-tyveri, har tapt mellom 1000 og 10 000 kroner på det, har 15 prosent tapt mer enn 10 000 kroner. Nærmere halvparten (48 %) av de spurte oppgir at ID-tyveriet ikke har ført til noe økonomisk tap for dem.

I fire prosent av tilfellene har kriminelle misbrukt andres identitet til å endre opplysninger i offentlige registre eller registrert ID-tyveri-ofre som eier/leder eller med styreverv i selskap.

I praksis betyr det at tyven ikke bare stjeler en identitet, men bruker den i systemer som stoler på at man er den man utgir seg for å være – og slik skader både personen og systemets integritet.

1 av 5 ofre for ID-tyveri kjente gjerningspersonen

Selv om gjerningspersonen er ukjent i 65 prosent av ID-tyveriene, oppgir hele 21 prosent av ofrene at de kjente gjerningspersonen.

De fleste beskriver sin relasjon til gjernings-personen(e) som «en bekjent». Deretter følger «en nær venn» og «en person tilknyttet arbeidsplassen (som en kollega, sjef)».

Oppdaget misbruk etter ukjente kontotransaksjoner

33 prosent av ofrene ble først klar over misbruket etter at de selv oppdaget ukjente transaksjoner på kontoen sin. Nærmere 1 av 4 (23 %) ble klar over misbruket etter at banken, politiet eller andre gjorde dem oppmerksom på det. I seks prosent av tilfellene avslørte de som sto bak ID-tyveriet, seg selv, eller de fortalte om det. Omtrent like mange rammede fikk varsel om en kredittvurdering og oppdaget misbruket på denne måten.

ID-tyveriundersøkelsen tyder også på at litt under halvparten (46 %) av de over 170 000 nordmennene som har blitt rammet, anmeldte forholdet til politiet.

Mens 21 prosent tapte fra 1000 til 10 000 kroner på ID-tyveriet, tapte 16 % mer enn 10 000 kroner

Foto: Carlos Torres

8 % er i liten grad eller likegyldig til å være forsiktig med å oppgi sensitive personinformasjon via telefon eller e-post. De under 34 år er overrepresentert blant disse

Vanligste økonomiske metoder for ID-tyveri	
Kjøpe en vare på nett	28,6 %
Få tilgang til en tjeneste, abonnement eller lignende (f.eks. ditt mobil-abonnement, streamingtjeneste)	24,8 %
Overføre penger ut av din konto	12,5 %
Kjøpe en vare eller tjeneste i en fysisk butikk	9,8 %
Inngå en mobilabonnementsavtale i ditt navn	5,3 %
Bestille et kredittkort	2,2 %
Overføre penger ut av en konto du disponerer på vegne av et selskap/ forening	2,1 %
Overføre penger/verdipapirer	2,1 %
Tatt opp et lån	1,7 %
Andre ting	23,0 %

Dette er noen tegn på at du kan være rammet av ID-tyveri

- Du mottar regninger for produkter du ikke har bestilt.
- Du ser bevegelser på konto eller kredittkort, som du ikke kjenner igjen.
- Du mottar bekreftelse på kreditt eller kreditt-ramme uten å ha spurt om dette.
- Du mottar varsel om at adresseendring er mottatt.
- Du mottar telefon eller brev om kjøp du ikke har gjort.
- Du mottar gjenpartsbrev av kredittsjekk uten at du har gjort noe som gjør dette nødvendig.

Foto: Ilja Hendel/NSM

7 av 10

følger i stor grad med på brev om kredittsjekk

Vanligste handlinger for ID-tyveri	
Fått tilgang til dine kontoopplysninger i banken	8,5 %
Fått tilgang til dine helseopplysninger	2,5 %
Registrert deg som eier/styreleder/ styremedlem/daglig leder i et selskap	1,9 %
Endret opplysninger om deg i offentlige registre (f.eks. skatteopplysninger)	1,8 %
Endret eller registrert opplysninger om eiendom du har rettigheter i, for eksempel pantsatt bolig eller fritidseiendom	1,8 %
Søkt om offentlig støtte (f.eks. fra NAV)	0,4 %
Endret kontonummer for utbetaling av offentlig støtte slik at du ikke fikk ytelsene (f.eks. fra NAV)	0,0 %
Andre ting	9,0 %

Kriminelle kan utnytte en stjålet identitet ved at den

- brukes til å åpne bankkontoer, søke om lån eller kredittkort, eller handle varer på avbetaling i andres navn
- brukes til å kapre kontoer i sosiale medier eller til å opprette falske kontoer. Kontoene misbrukes til pengeutpressing, svindel og sosial manipulering
- brukes til å utnytte offentlige støtteordninger eller endre opplysninger i offentlige registre
- selges på kriminelle markedsplasser, som en del av et økosystem der identitetsinformasjon kombineres med skadevare, falske nettsteder og deepfake-teknologi
- brukes til å opprette selskaper som front for økonomisk kriminalitet eller annen arbeidslivskriminalitet
- misbrukes for å skjule annen type kriminalitet, for eksempel ved å føre myndigheter og politi på villspor

KAPITTEL 3

22 % har brukt andres BankID: Sikrest, men høyest risiko når misbruk skjer

Mer enn hver femte nordmann (22 %) oppgir at de i løpet av det siste året har brukt noen andres BankID. De fleste oppgir at de har gjort dette for å hjelpe ektefelle eller foreldre.

Mens de under 20 år primært låner bort sin BankID til foreldre, låner de over 60 år i større grad bort til barna sine. Den viktigste grunnen til at de har tatt i bruk andres BankID oppgis å være nettopp å hjelpe andre (56 %).

Funnene i årets ID-tyveriundersøkelse er i tråd med NorSIS-rapporten «Nordmenn og digital sikkerhetskultur 2024»[1]. Sammenlignet med 2023 tyder mye på at det har vært en signifikant nedgang i antallet som har brukt andres BankID. Da var det 31 prosent som oppga det samme.

BankID er Norges klart mest brukte digitale sikre identifiseringsløsning. Mens 84 prosent foretrekker å bruke BankID på mobil, bruker rundt 15 prosent BankID med kodebrikke. I aldersgruppen over 55 år bruker fortsatt 1 av 4 fysisk BankID med kodebrikke mest.

BankID er personlig og skal aldri deles – på samme måte som man ikke lar andre signere avtaler i sitt navn, eller låner bort passet sitt.

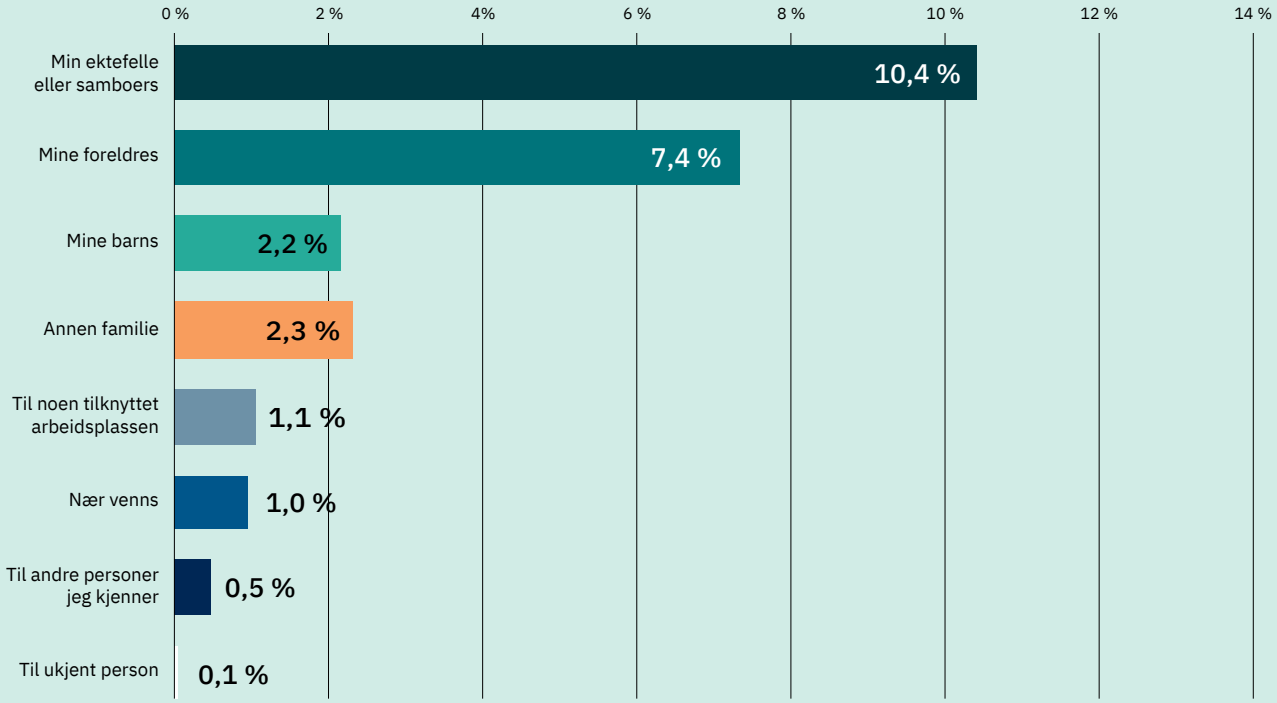
Over 100 000 har brukt venner eller kollegaers BankID

1 av 10 som har brukt andres BankID (tilsvarende nærmere 110 000 nordmenn), har gjort dette på vegne av andre utenfor familien, som nære venner eller kollegaer på jobb. De under 20 år er over-representert blant de som har lånt bort BankID til noen utenfor familien.

1 av 7 ID-tyverier med BankID: Flest blir lurt via lenker i SMS eller e-post

I overkant av 1 av 7 ID-tyverier i Norge (15 %) over tid har ifølge undersøkelsen skjedd ved misbruk av BankID. Det tilsvarer nærmere 30 000 enkelttilfeller. Mer enn 4 av 10 nordmenn som har opplevd dette, har fulgt en lenke fra e-post, SMS eller lignende, som førte til misbruket. Omtrent like mange vet ikke hvordan noen klarte å misbruke deres BankID.

Hvem sin BankID har de brukt



Mindre kritisk sans ved innlogging med BankID

Den fysiske kodebrikken eller appen på telefonen, som i starten ble brukt for å logge inn i banken eller på offentlige tjenester som Altinn eller Skatteetaten, brukes i dag også til alt fra verifisering av identitet ved netthandel, til elektronisk signering.

«Den utstrakte bruken av BankID og ulike innloggingskontekster gir en form for «slitasje» på brukerens kritiske sans ved innlogginger med BankID», skrev Finanstilsynet i sin ROS-analyse for 2024[2].

Høyeste sikkerhetsnivå, men også høyeste risiko ved misbruk

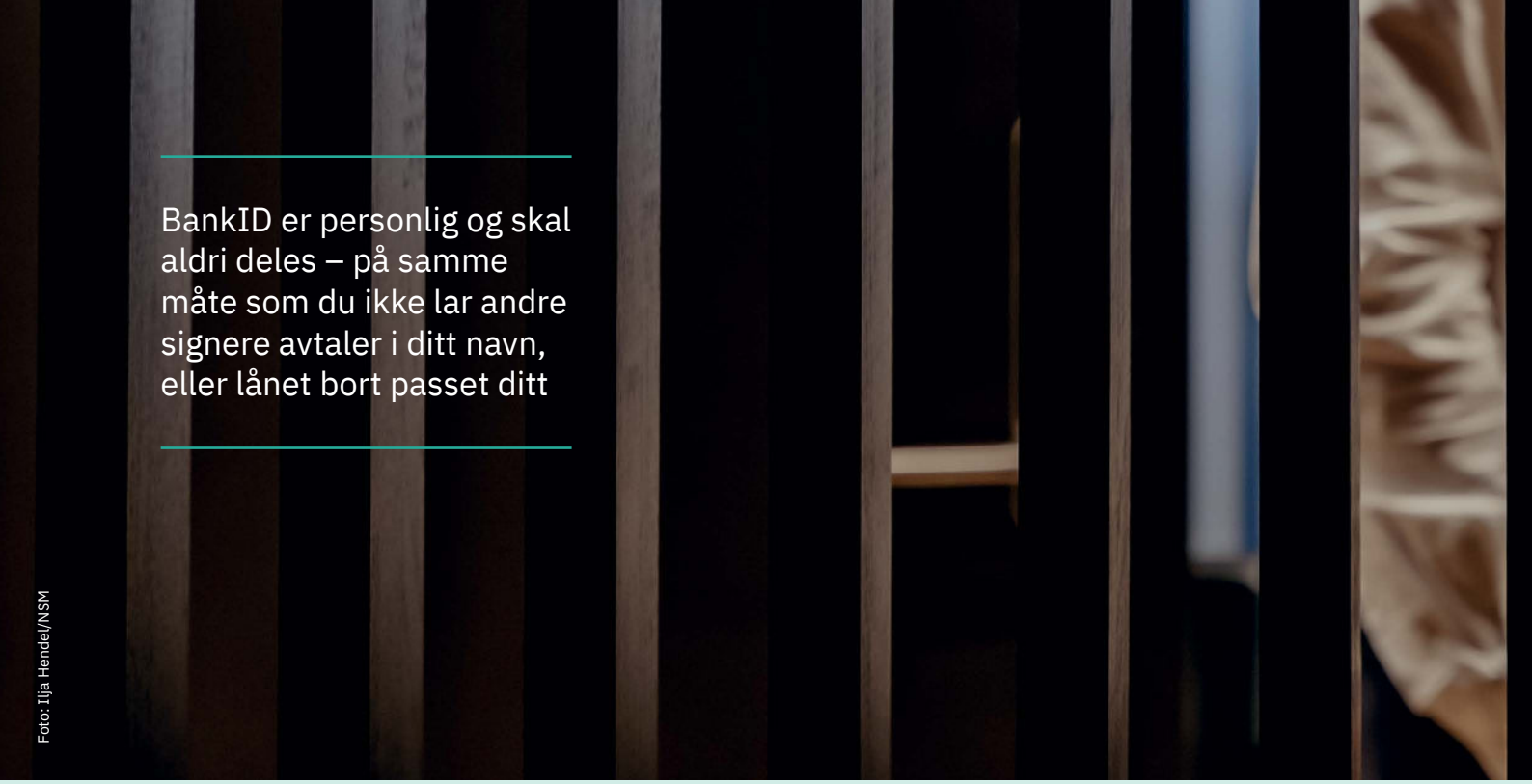
BankID er en digital eID med det høyeste sikkerhetsnivået. Det betyr at man med denne kan få tilgang til de mest sensitive tjenestene, som for eksempel helseopplysninger. Her kreves det både totrinnspålogging og at man tidligere har vist legitimasjon personlig, for å hindre misbruk. Det betyr også at om uvedkommende har tilgang til noens fysiske BankID kodebrikke, fødselsnummer og passord, kan de blant annet ta opp lån, kjøpe varer og overføre penger ut av nettbanken.

99 %

over 18 år har benyttet seg av BankID siste to år

1 NorSIS, https://norsis.no/sikkerhetskultur2024

2 Finanstilsynet, https://www.finanstilsynet.no/publikasjoner-og-analyser/risiko--og-sarbarhetsanalyse



BankID er personlig og skal aldri deles – på samme måte som du ikke lar andre signere avtaler i ditt navn, eller lånet bort passet ditt

Foto: Ilja Hendel/NSM

Elektronisk ID i Norge

Elektronisk ID (eID) er en digital måte å bekrefte en persons identitet på nettet eller i digitale transaksjoner.

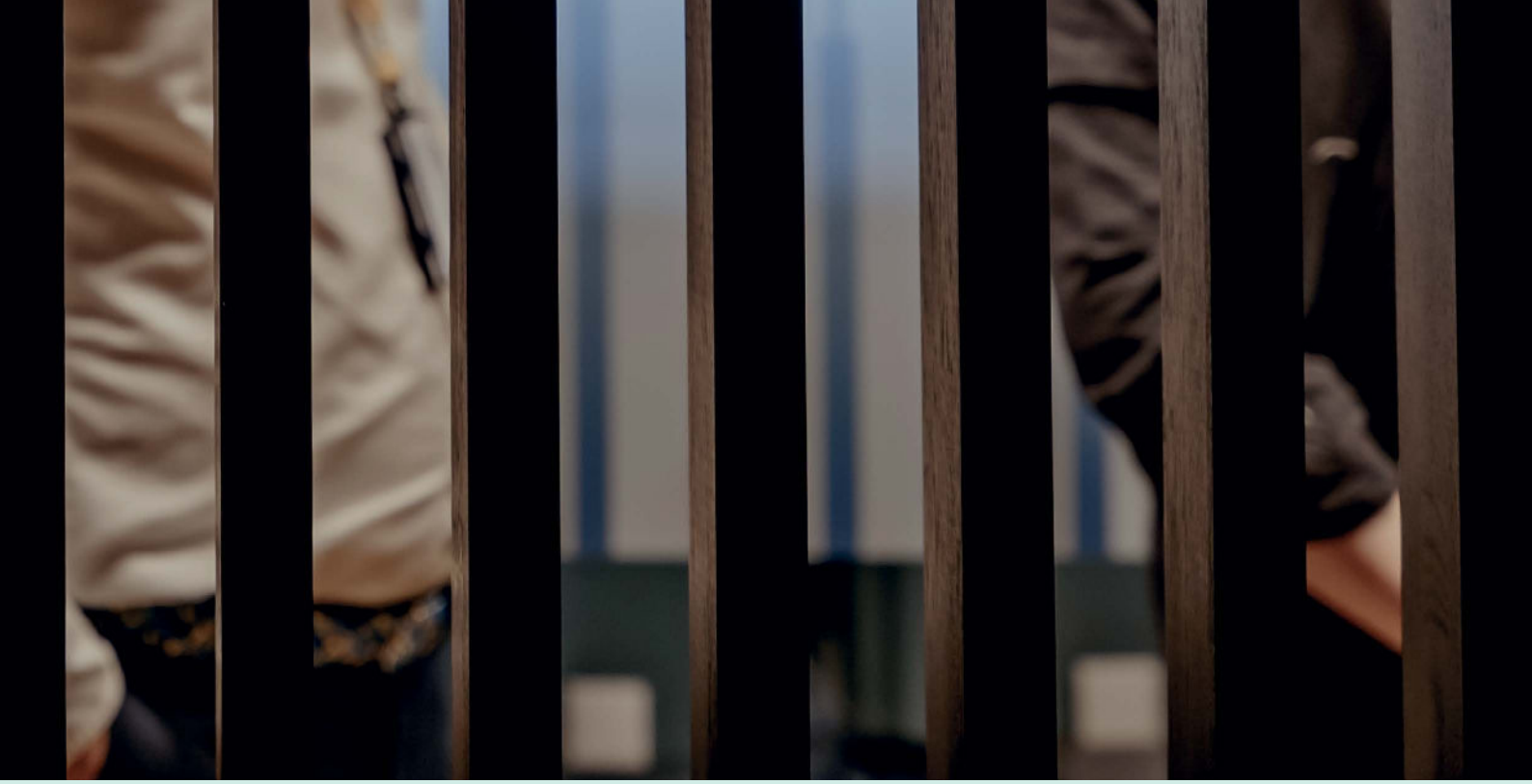
BankID er den mest brukte elektroniske ID-tjenesten i Norge. Sammen med Buypass og Commfides har BankID det høyeste sikkerhetsnivået og gir tilgang til de mest sensitive tjenestene – for eksempel helseopplysninger. Her kreves både totrinnspålogging og at du tidligere har vist legitimasjon personlig, for å hindre misbruk.

MinID brukes til tjenester med middels høye sikkerhetskrav og krever totrinnspålogging: fødselsnummer, passord og en engangskode via SMS eller app.

Viktigste årsak til å bruke andres BankID

Trenger hjelp til å bruke BankID	55,8 %
Stoler på at de kan dele sin BankID	34,7 %
En eller flere tjenester som kun en har tilgang til	18,3 %
Praktisk	15,4 %
Vanskelig å få fullmakt til å bruke egen BankID til å logge inn på vegne av en annen	7,7 %
Ikke har vært klar over at det bryter vilkår	1,1 %
Av andre grunner	9,0 %

Kilde: Digitaliseringsdirektoratet



Slik bruker du BankID sikkert

- Del aldri BankID-informasjon med noen – heller ikke med familie, venner, politi eller banken.
- Oppgi aldri passord eller koder via telefon, e-post eller SMS. Verken banken eller BankID vil be deg om dette.
- Svindlere stresser deg – de spiller på følelser som frykt og hastverk. Avslutt samtalen og kontakt banken direkte.
- Klikk aldri på lenker i SMS eller e-post som utgir seg for å være fra BankID. Det er alltid svindel.
- Bruk et sterkt og unikt passord, gjerne en kort, positiv setning med mellomrom. Det gjør passordet både sikkert og lett å huske.
- Godkjenn kun egne innlogginger.
- Får du en BankID-varsel du ikke forventer, trykk “Nei, det er ikke meg”.
- Er du usikker eller har gjort en feil? Kontakt banken din umiddelbart. Det er alltid bedre å spørre én gang for mye enn én gang for lite.

87 %

av alle nordmenn oppgir at de er svært forsiktig med å logge inn med BankID etter å ha klikket på lenker i e-post, SMS, sosiale medier eller andre kilder

17 %

varslet ikke banken etter at deres BankID hadde vært misbrukt

KAPITTEL 4

1 av 7 nordmenn har opplevd ID-tyveri i sosiale medier: Verre enn mange tror

Nærmere 700 000 nordmenn (16 %) over 18 år har opplevd at noen har tatt over kontoen deres i sosiale medier, eller opprettet en falsk konto i deres navn.

Mens kontokapring i større grad rammer yngre og menn, er kvinner og eldre overrepresentert blant dem som har blitt utsatt for en falsk konto i eget navn.

De to siste årene er det kontokapring aller flest har kontaktet den kostnadsfrie rådgivningstjenesten Slettmeg.no for å få hjelp med. Blant mange tusen årlige henvendelser dreier 14 prosent seg om denne formen for ID-tyveri.

Store konsekvenser – både følelsesmessig og økonomisk

«Jeg har ingenting å skjule, så dette er ikke noen stor krise», er det mange som tenker når noen stjeler deres identitet i sosiale medier. Selv om det der og da ikke har en kostnad, kan imidlertid konsekvensene over tid bli store – både følelses-messig og økonomisk.

Økt troverdighet i svindelforsøk, og tyveri av personopplysninger for videresalg

Når noen kaprer en konto i sosiale medier, eller oppretter en falsk konto i andres navn, er det ikke bare den personen som rammes – det rammer også venner og bekjente. Kriminelle bruker andres identitet for å virke troverdige og forsøker å lure bekjente i nettverket rundt – med alt fra krypto-svindel til forsøk på å få tilgang til BankID eller andre sensitive opplysninger.

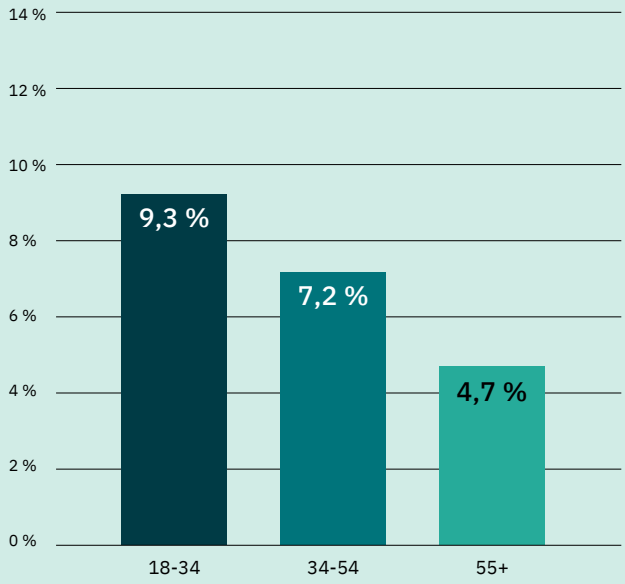
Grunnen til at en konto i sosiale medier er interessant for svindlere kan være enkel: Folk stoler mer på meldinger fra noen de kjenner enn fra en ukjent avsender. Derfor er slike profiler attraktive.

I tillegg selges eller misbrukes ofte bilder og innhold som ligger på profilen. Dette brukes i mange tilfeller til utpressing – en stadig vanligere del av kontokapringer.

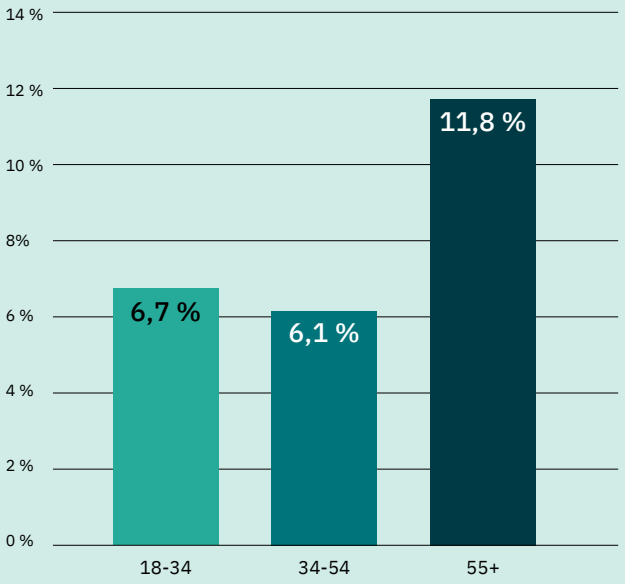
Foto: Charles Deluvio

Konsekvensene over tid kan bli store – både økonomisk og følelsesmessig

Fått sin konto kapret



Utsatt for falsk konto i sitt navn



Unge tar mer sjanser på nett

Hele 87 prosent av nordmenn oppgir at de er svært forsiktige med å logge inn med BankID etter å ha klikket på lenker i e-post, SMS eller i sosiale medier. Omtrent like mange, 79 prosent, oppgir at de i stor grad bare logger inn med BankID på noen få nettsteder som de kjenner godt. Spesielt blant de over 55 år er det mange som oppgir dette (83 %). Blant de under 34 år er andelen lavest (74 %). Langt flere unge enn eldre oppgir at de tar sjanser som de vet er risikable på nett (28 % blant 18-34 åringer mot 5 % i aldersgruppen over 55 år).

Har noen først kapret en konto, har de mest sannsynlig allerede brukernavn og passord til denne. Dette kan igjen også misbrukes andre steder siden nærmere 1 av 4 nordmenn (Nordmenn og Digital sikkerhetskultur 2024)[1] ofte har samme passord på de fleste av sine tjenester.

Totrinnspålogging mer utbredt blant de yngste enn de eldre

Falske profiler fjernes som regel om man rapporterer dette til den plattformen den er opprettet på. Kontokapring meldes også inn på denne måten. For å redusere risikoen for konto-kapring kan man aktivere totrinnspålogging. NorSIS i NSM-undersøkelsen viser at 55 prosent i stor grad bruker totrinnspålogging der det er mulig. Sammenlignet med tidligere undersøkelser tyder dette på at stadig flere får dette på plass. Spesielt blant de unge er andelen høy (64 %). Lavest er den blant de over 55 år (44 %).

1 NorSIS, https://norsis.no/sikkerhetskultur2024

Foto: Ilja Hendel/NSM

Smarte grep for å sikre kontoen din

- **Skru på totrinnspålogging**
  Det er den beste måten å hindre uvedkommende i å få tilgang til kontoen din, selv om passordet ditt skulle komme på avveie.
- **Bruk sterke og unike passord**
  Aldri gjenbruk passord på flere tjenester! Bruk en passordbank hvis du synes det er vanskelig å huske dem.
- **Vær skeptisk til meldinger fra «venner»**
  Hvis noen ber deg om å klikke på en lenke eller oppgi passord, kan kontoen deres være hacket. Sjekk alltid direkte med dem først.
- **Ikke del sensitive opplysninger**
  BankID, passord eller engangskoder skal aldri gis videre, uansett hvem som spør. Seriøse aktører ber deg aldri om dette.

22 %

har i liten grad skrudd på totrinnspålogging på e-post, sosiale medier – der det er mulig

16 %

av de under 34 år er ikke like opptatt av å holde passord for seg selv

KAPITTEL 5

ID-tyveri på «frykttoppen»: Kan være en stor psykisk belastning

Hele 44 prosent av nordmenn er i stor grad bekymret for ID-tyveri. De som er minst opptatt av å ta i bruk sikkerhetstiltakene som skal beskytte mot dette, er også de som er minst bekymret.

Tanken på at andre skal misbruke ens identitet er blant de verst tenkelige negative hendelsene nordmenn frykter kan ramme. Det viser denne og tidligere undersøkelser gjennomført av NorSIS i NSM[1] og Politiet[2].

En segmentanalyse av tallgrunnlaget i undersøkelsen viser at ett segment, som består av rundt 1 av 7 nordmenn (over 600 000), er mindre forsiktige med hva de deler av personlig informasjon enn gjennomsnittet. De låner oftere ut egen BankID, bruker sjeldnere totrinnspålogging, og følger i mindre grad sikkerhetsråd enn folk flest. Likevel oppgir langt færre enn gjennomsnittet i dette segmentet at de i stor grad er bekymret for ID-tyveri – bare 30 prosent.

Denne gruppen er tydelig overrepresentert i aldersgruppen 35 til 54 år, og består av litt flere kvinner enn menn – 53 mot 47 prosent.

De eldre og kvinner mest bekymret for ID-tyveri

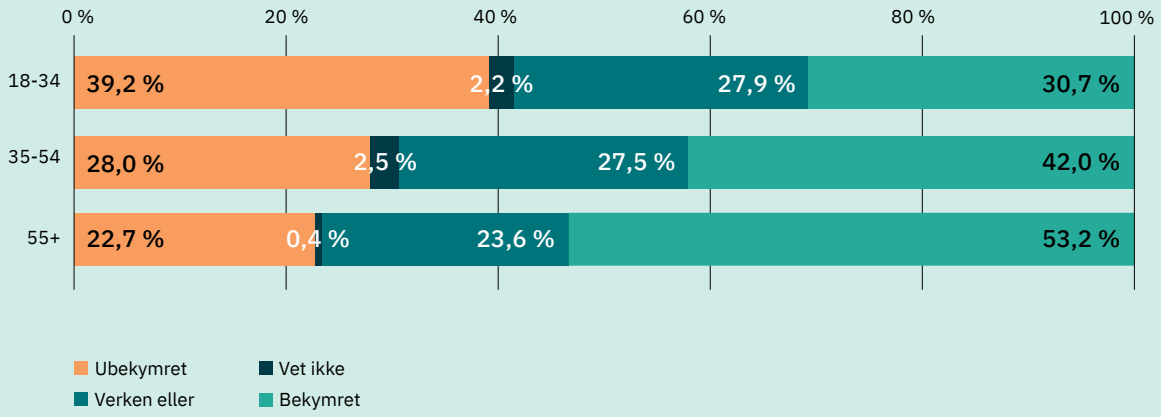
Generelt er bekymringen for ID-tyveri størst i de eldre aldersgruppene (53 % er i stor grad bekymret) og minst iblant de yngste (31 %). Kvinner er også gjennomgående mer bekymret for dette enn menn (henholdsvis 49 % og 39 % er i stor grad bekymret).

NorSIS i NSM-undersøkelsen «Nordmenn og digital sikkerhetskultur» fra 2024 viste at antall nordmenn som var bekymret for at andre skulle utgi seg for å være dem på nett, økte med fire prosentpoeng – fra 50 prosent til 54 prosent – fra året før. Nordmenns bekymringsnivå for uønskede hendelser på nett har økt fra år til år, og folk var mer bekymret i fjor enn noen gang tidligere. Kvinner bekymrer seg jevnt over mer enn menn.

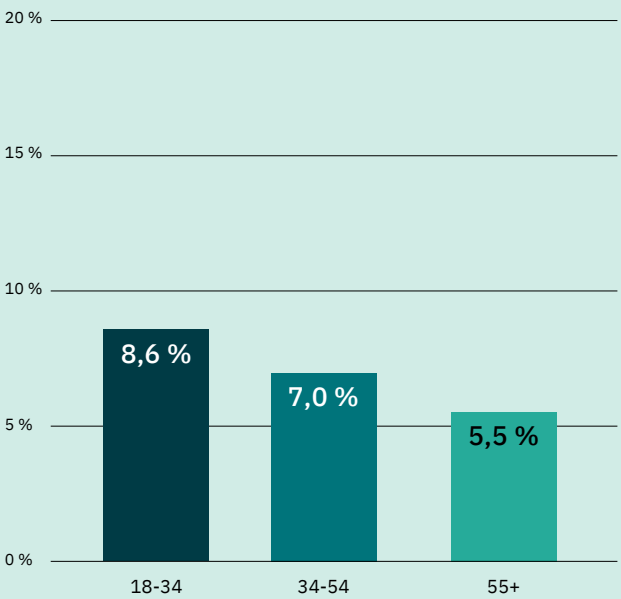
1 NorSIS, https://norsis.no/sikkerhetskultur2024

2 Politiet, https://www.politiet.no/om-politiet/tall-og-fakta

Bekymring for ID-tyveri i fremtiden



Har lånt bort sin BankID



76 %

unngår å bruke enkelte internettjenester i frykt for kriminelle handlinger

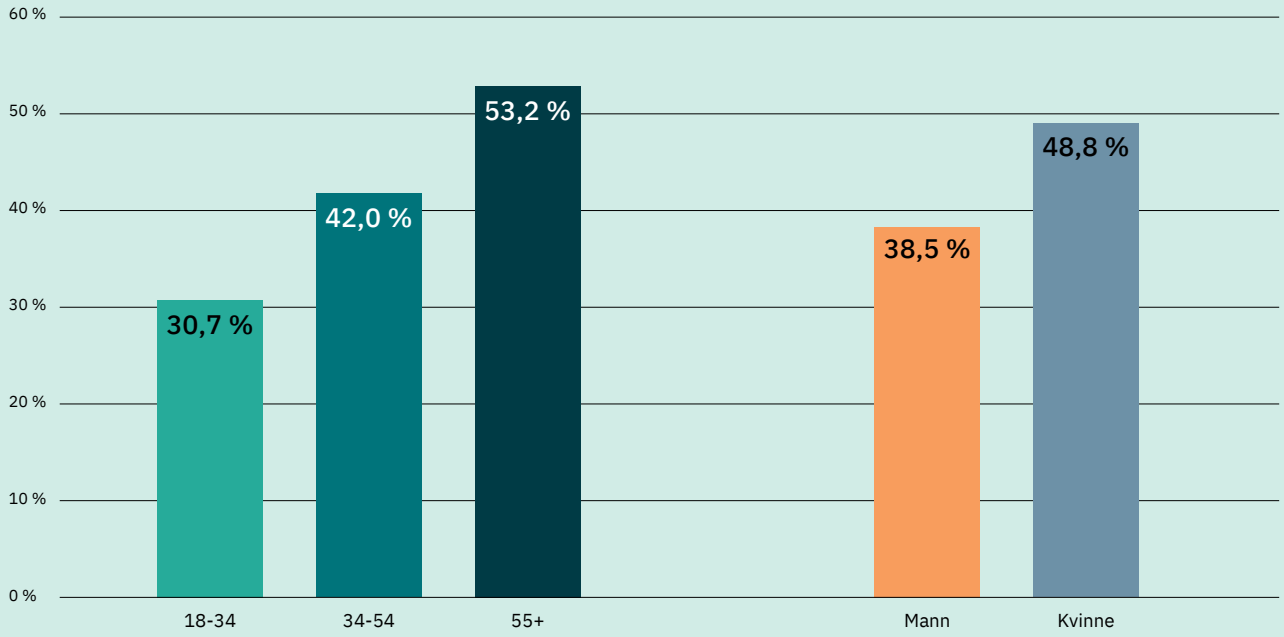
8 %

av de som har blitt utsatt for ID-tyveri, har ikke snakket med noen om dette

Mange av ofrene for ID-tyveri på nett beskriver en sterk følelse av skam, skyld og maktesløshet

Foto: Jonathan Borba

Bekymring for ID-tyveri



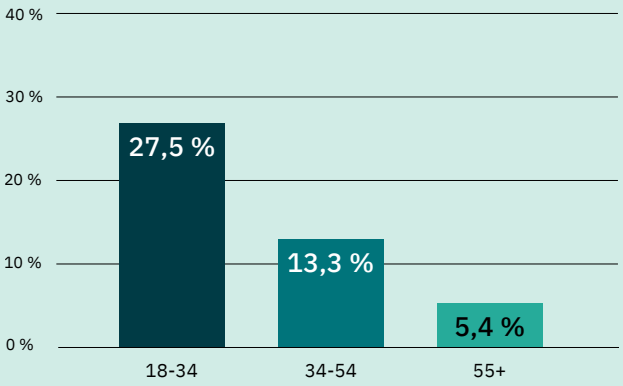
EU-rapport: Mange får en sterk følelse av skam, skyld og maktesløshet

Det finnes flere studier som påpeker sammenhengen mellom ID-tyveri og forverret psykisk helse. I rapporten «Study on online identity theft and identity-related crime» som EU-kommisjonen ga ut i 2022[1], fremgår det at mange av ofrene for ID-tyveri på nett beskriver en sterk følelse av skam, skyld og maktesløshet. Det er heller ikke uvanlig å føle seg sint, redd eller utlevert. Noen ofre for dette trekker seg også unna sosialt – særlig om ID-tyveriet har resultert i at økonomien eller ryktet deres er skadet.

Andre igjen får søvnproblemer, angst eller depressive symptomer. For enkelte påvirker ID-tyveriet, ifølge rapporten fra EU-kommisjonen, hele hverdagen deres. Mange blir også mer usikre når de er på nett. Noen holder helt opp med å bruke flere digitale tjenester.

Når noe så personlig og intimt som ens egen identitet blir misbrukt, er det ikke bare økonomien som kan få seg en knekk – det kan også gjøre noe med den psykiske helsen og den generelle trygghetsfølelsen.

Tar sjanser som de vet er risikable på internett



1 EU-kommisjonen, https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1

KAPITTEL 6

Flertall for biometri: Kan forhindre at en person har mange identiteter

Nærmere 6 av 10 nordmenn er positive til å ta i bruk biometri for sikker identifisering, som fingeravtrykk og ansiktsgjenkjenning.

25 prosent av befolkningen har ikke noe klar mening om dette, mens i underkant av 18 prosent er negative. Skepsisen til bruk av biometriske data for identifisering er marginalt større i aldersgruppen over 55 år, og er like stor blant menn og kvinner. De som er for denne type identifisering, fordeler seg jevnt i alle aldersgrupper og blant begge kjønn.

Noe av utfordringen med den norske identitetsforvaltningen i dag er at vi ikke har et system som knytter én fysisk person til kun én identitet i digitale og fysiske sammenhenger

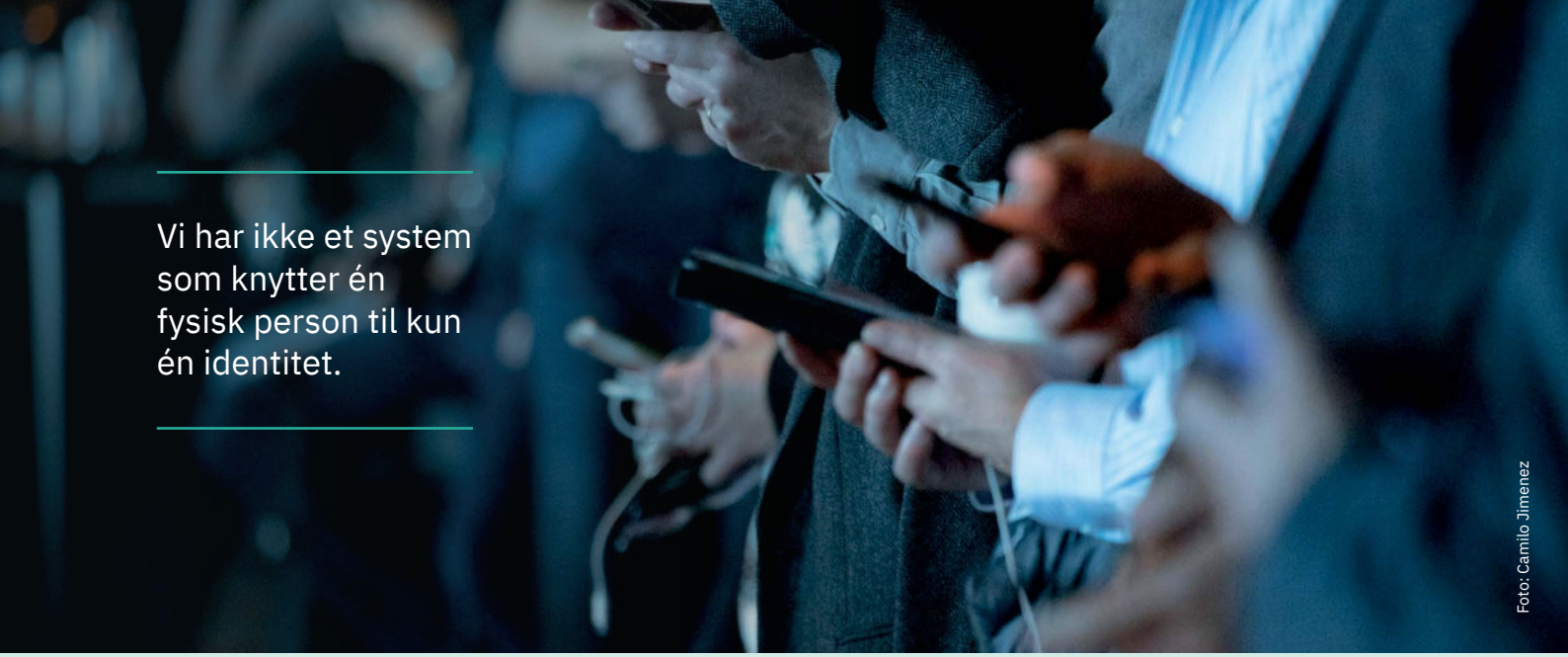
Identitetsforvaltningen i Norge preges av mange aktører med fragmenterte ansvarsområder, og det mangler tiltak som sørger for at identitetene våre er sikre og beskyttet mot misbruk.

Vanskeligere å operere med flere identiteter

Som et resultat av det kan en fysisk person som ønsker å manipulere systemet, opptre med et stort antall identiteter. Det gir vedkommende muligheten til å utnytte statens velferdsgoder, opprette selskaper, ta opp lån eller begå andre former for kriminalitet i andres navn.

Ved å knytte ett unikt fysisk kjennetegn (som ansiktsfoto) til en identitet, og på den måte «låse» en persons tildelte identitetsnummer i Folkeregisteret, blir det langt vanskeligere å operere med flere identiteter.

Samtidig er det personvernutfordringer og risikoer knyttet til denne typen biometriske registre, for eksempel ved datalekkasjer. Skulle biometriske data komme på avveie, kan ikke disse endres.



Vi har ikke et system som knytter én fysisk person til kun én identitet.

Foto: Camilo Jimenez

8 av 10

nordmenn mener KI vil gjøre dem ekstra utsatt for svindel

58 %

er i stor grad positiv til bruk av biometri når de må identifisere seg

Biometri som sikring av identitet – og veien mot UNIK-status i Folkeregisteret

Ved søknad om pass og nasjonale ID-kort samler allerede politiet i dag inn biometriske data i form av ansiktsfoto og fingeravtrykk for å sikre at identiteten til søkeren er korrekt. Siden november 2020 har ansiktsfoto blitt kontrollert gjennom et såkalt «en-til-mange-søk», hvor informasjonen sammenlignes mot hele databasen.

Et «en-til-mange-søk» betyr at biometriske data fra en person sammenlignes mot alle registrerte biometriske profiler i systemet. På den måten kan det sjekkes om samme person allerede finnes under en annen identitet.

Da kan man med høy grad av sikkerhet forhindre at en person får utstedt dokumenter i flere identiteter. Biometrien fungerer dermed som en lås som kobler personen til et bestemt fødselsnummer i Folkeregisteret.

Denne prosessen vil ikke gjelde bare for norske statsborgere, men også for utenlandske borgere med f-nummer, forutsatt at de har godtgjort identitet og lovlig opphold. Utenlandske personer med d-nummer er foreløpig ikke omfattet av muligheten til å kunne få utstedt et nasjonalt ID-kort.

UNIK – det neste steget for entydig identifisering i Folkeregisteret

Neste steg er å registrere i Folkeregisteret at et biometrisk en-til-mange-søk er gjennomført og godkjent. Ikke selve biometrien, men resultatet. Slik er det ikke i dag. Da kan personen merkes der som «UNIK», altså entydig identifisert. Dette kan så deles med banker, offentlige tjenester og andre som trenger sikker ID. Målet er klart: å vite hvem man har med å gjøre og hindre ID-misbruk.

KAPITTEL 7

KI-svindelen øker: Behov for sikker identifisering blir enda viktigere

De tradisjonelle ID-tyveriene har blitt færre, men stadig flere lures nå til selv å overføre penger eller dele sensitiv informasjon med kriminelle. Dette skjer i økende grad ved hjelp av kunstig intelligens.

Avansert sosial manipulasjon benytter seg av kunstig intelligens for å gjøre svindelforsøkene mest mulig realistiske. Dette er både enklere og mer lønnsomt, og det tas i bruk av stadig flere kriminelle miljøer.

Deepfake-teknologi er fortsatt en relativt ny trussel, men vokser raskt. I deler av den europeiske finansnæringen, inklusive Norge[1], rapporteres det at deepfakes nå utgjør rundt 6,5 prosent av alle oppdagede svindelforsøk. Dette er en økning på mer enn 2000 prosent på tre år.

Europol: ID-svindel en katalysator for økonomisk kriminalitet

I Europol-rapporten «Serious and Organised Crime Threat Assessment 2025»[2] advares det om at kunstig intelligens med identitetssvindel som verktøy er en katalysator for økonomisk kriminalitet og destabiliserende hybridoperasjoner.

Kunstig intelligens gjør ID-svindel både mer overbevisende og mer tilgjengelig for kriminelle. Nå kan svindlere bruke deepfakes, målrettede phishing-angrep og KI-genererte identiteter for å utgi seg for å være andre i tekst, bilder, video og lyd.

Vanskeligere å gjennomskue avansert sosial manipulasjon

Et tydelig eksempel på utviklingen er direktør-svindel (CEO-svindel). Tidligere kom den gjerne som en e-post fra «sjefen» med forespørsel til noen på økonomiavdelingen om en pengeoverføring som hastet. Nå kan det utspille seg som en videosamtale der en KI-generert kopi av direktøren ber en ansatt om å overføre penger. Stemmen og ansiktet ser ekte ut. Det gjør svindelen langt mer troverdig.

Kunstig intelligens brukes også for å gi innholdet i phishing-kampanjer et ekte, mer persontilpasset språk, mens generativ KI kan brukes til å opprette brukere i sosiale medier i et høyt tempo.

Verktøyene som skal til for å ta i bruk dette, er også lett tilgjengelig for de kriminelle, og krever ikke spesielt god teknisk kompetanse.

Verktøyene som skal til for å ta i bruk KI, er lett tilgjengelig for de kriminelle

Foto: Tija Hendel/NSM

8 av 10 tror kunstig intelligens vil gjøre dem ekstra utsatt for svindel

I NorSIS i NSM sin rapport «Nordmenn og digital sikkerhetskultur 2024»[3] oppga hele 8 av 10 nordmenn at de mente kunstig intelligens vil gjøre dem ekstra utsatt for svindel*. I aldersgruppen under 35 år er frykten lavest (73 %). Dette er også den aldersgruppen hvor de selv mener de best kan vurdere troverdigheten til en avsender. Mens 72 prosent av nordmenn generelt mener de i stor grad kan dette, oppgir 82 prosent i den yngste aldersgruppen (18-34 år) det samme.

Lavest tro på egne evner til å vurdere troverdigheten til en avsender sees i gruppen over 55 år (62 %).

Avansert analyse av store datastrømmer kan beskytte oss

KI vil gjøre angrepene mer overbevisende, hyppige og skalerbare. Ifølge NSM Risiko 2025[4] er det derfor viktig at ansatte er kjent med trusler og risiko for phishingforsøk og andre forsøk på sosial manipulasjon som bruker KI-generert innhold.

Samtidig vil KI-drevet forsvar forhåpentligvis bli mer sofistikert. KI kan allerede oppdage mistenkelig aktivitet gjennom å finne avvik og trender i store datastrømmer, som at noen plutselig overfører penger klokken 02 på natta, eller til et land de aldri har overført penger til før. Det kan også hjelpe med å avdekke falske dokumenter/identiteter og styrke sikkerheten med biometrisk kontroll.

Nye former for sosial manipulasjon og ID-misbruk vil komme. Det å sikre at én person kun har én identitet i Norge, som ved bruk av biometri, vil bare bli viktigere ettersom digitaliseringen øker og teknologien stadig blir mer avansert.

Syntetisk identitet

En syntetisk identitet er en kunstig konstruert identitet som kombinerer:

- Reelle persondata (som fødselsnummer eller navn) med
- Fiktive eller fabrikerte elementer (som falsk adresse eller e-post)
- Målet er ofte å skape en identitet som er «troverdig nok» til å brukes for økonomisk bedrageri, svindel mot offentlige støtteordninger eller annen ulovlig aktivitet. Det brukes også i pengeflyt for hvitvasking og som del av falske selskapsstrukturer.

Deepfake

En deepfake er en form for syntetisk media som bruker kunstig intelligens (KI) til å generere svært realistiske, men falske bilder, videoer eller lydopptak.

2137 %

økning i svindelforsøk med deepfake på 3 år i europeisk finansnæring

1 Signicat, https://www.signicat.com/no/pressemeldinger/svindelforsøk-med-deepfakes-har-økt-med-2137-i-løpet-av-de-siste-tre-årene

2 Europol, https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime

3 NorSIS, https://norsis.no/sikkerhetskultur2024

4 NSM, https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2025

Foto: Tim Gouw

NorSIS
NORSK SENTER FOR
INFORMASJONSSIKRING

Forsidefoto: Mehdi Lamaaffar
Design: Tank Design

Undersøkelsen er utført av Opinion i januar 2025, og gjort i et landsrepresentativt utvalg av befolkningen 18+ år. 2011 respondenter.

NSM