

Nr. 1, mai 2025, 26. årgang

Seniornett

– får seniorene på nett



Digital trygghet og sikkerhet
Ikke la svindlerne vinne
Når uhellet er ute

Utgiver: Seniornett**Ansvarlig redaktør:** Hanni W. Petersen**Magasinredaktør:** Siri Kessel**Redaksjon:**

Elisabeth Farstad

Siri Kessel

Tore Langemyr Larsen

Gunnar Tveiten

Journalistiske bidragsytere:

Jan W. Brill

Elisabeth Farstad

Ove Gundersen

Marthe Eidsand Kjørven

Tore Langemyr Larsen

Gry Nergård

Hanni W. Petersen

Tarja Marita Tamminen

Gunnar Tveiten

Foto:

Mina Elisabeth Albertsen, Svein Brimi,

Øyvind Ganesh Eknes, Ronald Johansen,

A. Lundesgaard, Kirsten Moe, Daniel

Nygård, John Trygve Tollefsen,

Universitetet i Oslo, Økokrim

Grafisk formgivning og trykk:

Flisa Trykkeri AS

www.flisatrykkeri.no**Opplag:** 14 000

Seniornett

www.seniornett.no

Postboks 1002 Sentrum, 0104 Oslo

Tlf. 22 42 96 26

Besøksadresse: Dronningens gate 6, Oslo**E-post:** kontor@seniornett.no**Redaksjon e-post:**redaksjonen@seniornett.no**ISSN 2464-4358 (papirutgave)****ISSN 2535-4361 (webutgave)**

Innhold

Leder	3
Digital trygghet og sikkerhet i hverdagen	4
Min digitale hverdag – Lise Fjeldstad	7
Økokrims rolle	9
Når uhellet er ute – hva gjør jeg?	11
Bankenes arbeid mot svindel	15
Innspill: Behov for basiskunnskaper	18
Seniornett Hønefoss	19
BankID-appen	21
Felles offentlig elektronisk identifikasjon på vei	25
IKT-Norge: Etiske retningslinjer for digital inkludering	27
Ikke la svindlerne vinne – kjenn dine rettigheter!	29
Nyttig å vite om domenenavn	31
Quiz: Ti strake	33
En datahjelpers hverdag	35
Tips & triks: Hold mobilen oppdatert	37
Generalsekretærens hjørne	39



Leder

Dette nummeret av magasinet retter søkelyset spesielt mot *Digital svindel*. Vi har bidrag både fra Finans Norge, Forbrukerrådet, Økokrim og Det juridiske fakultet ved Universitetet i Oslo. Her kan det være mye å lære både om bankenes ansvar ved svindel, om forbrukerrettigheter og fakta om svindel, og ikke minst om hva vi selv bør være oppmerksomme på.

En annen artikkel gir råd om hva vi kan gjøre når svindlerne har lurt oss, og du får også et innblikk i hvordan svindel kan oppleves.

I spalten «Min digitale hverdag» er det skuespiller Lise Fjeldstad som deler sine erfaringer og tanker med oss.

Som vanlig får vi et innblikk i hvordan en lokalforening av Seniornett driver sitt arbeid, denne gangen Hønefoss, som har et nært samarbeid med Ringerike kommune. Vi har også fått inn synspunkter fra et aktivt Seniornett-medlem i Østfold.

At BankID er utfordrende for mange eldre, er velkjent for Seniornett. I dette magasinet har vi en artikkel om BankID

og BankID-appen, og en om myndighetenes arbeid med en eID for alle norske borgere.

Videre presenterer IKT-Norge sine etiske retningslinjer for digital inkludering.

Er du glad i quiz? Da får du også i dette nummeret noe å bryne deg på som også gjør at du kan lære mer om data og teknologi.

Generalsekretæren har sin faste spalte. I tillegg skriver hun om de frivilliges store innsats i Datahjelpen, og om at Datahjelpen trenger flere frivillige.

Som nyslått redaktør vil jeg rette en stor takk til de tre medlemmene av redaksjonsgruppen som har sluttet siden sist, for god og langvarig innsats, også som redaktører: Bodil Brøgger, Annette Hannestad og Tarja Marita Tamminen. Dessverre døde Sølvi Kristiansen fra oss høsten 2024. Hun var aktivt med nesten til det siste og fortjener også stor takk for viktige bidrag gjennom mange år. Uten frivillig innsats – intet Seniornett-magasin, så stor takk også til gamle og nye frivillige redaksjonsmedlemmer.

Siri Kessel, redaktør



Digital trygghet og sikkerhet i hverdagen

Seniornett-magasinet har intervjuet forbrukerdirektør Inger Lise Blyverket om digitaliseringen og den eksplosive økningen av svindel og bedragerier.

Vi er alle enige om at digitaliseringen bringer med seg gevinster som vi ikke ville ha vært foruten, både som brukere og forbrukere. Likevel, når vi ser den griper om seg i stadig mer eksplosiv fart, har digitaliseringen blitt et mål i seg selv?

– Det er i alle fall en fare for at man ser seg blind på teknologien og mister noe på veien. Dette gjelder for eksempel ved automatisering av kundebehand-

ling, hvor kravet om effektivitet og selvhjelp ofte går på tvers av kvaliteten og den hjelpen vi får.

Sett fra ditt ståsted som forbrukerdirektør, er det på plass tilstrekkelige juridiske rammeverk og sikkerhets- og kontrolltiltak for å håndtere at denne utviklingen skjer på en trygg, pålitelig og rettferdig måte?

– Det er ikke nødvendigvis mangel på

regelverk, men oppfølging og etterlevelse av regelverket. For eksempel når det kommer til personvern, hvor vi i utgangspunktet har et robust regelverk, men hvor tilsynsmyndighetene rundt om i Europa sliter med å holde tritt og sanksjonere lovbrudd.

Kan det være noe i en påstand om at 'hodeløs' tro på digitale løsninger er i ferd med å undergrave tilliten til offentlig forvaltning og saksbehandling og vårt tillitsbaserte samfunnssystem?

– Det har vi ikke forutsetning for å svare på.

Etter hvert som generative KI-systemer også blir integrert i ulike digitale plattformen og verktøy, kommer teknologien bare til å bli brukt mer og mer. Trenger vi at noen trekker i bremsen? Eventuelt, hvem skal gjøre det?

– Vi må sikre at utvikling og bruk av kunstig intelligens er trygg, pålitelig og rettferdig. Dessverre har historien vist oss at vi ikke kan ha tiltro til at teknologigigantene ordner dette selv, og at det er behov for regulering og håndheving av lover som sikrer at våre rettigheter blir ivaretatt. Her er det viktig at norske myndigheter ikke blir sittende på gjerdet, og engasjerer seg aktivt i de internasjonale prosessene som pågår. I noen tilfeller virker det også som bruk av kunstig intelligens er viktigere enn hvilken oppgave som skal løses.

Mange eldre gir opp og faller fra og blir avhengige av familie og venner for å håndtere den digitale hverdagen. Hva tenker du om det?

– I debatter om hvordan vi kan løse utfordringene med digitalt utenforskap, mener mange at forbrukerne må få hjelp til å mestre sin digitale hverdag. Forbrukere som mangler kompetanse eller føler seg utrygge digitalt, skal selvsagt få hjelp når de trenger det.

Samtidig vil et ensidig fokus på å gi hjelp bidra til at vi gjør for lite for å sikre alle forbrukere retten til helt grunnleggende varer og tjenester – uten hjelp. Vi vet allerede nok til å fastslå at et stort mindretall forbrukere er utestengt fra å handle digitalt, og at dette kanskje vil være tilfelle i all fremtid. Vi må derfor sikre at det finnes alternative måter å handle på når den digitale tilgangen svikter, for eksempel at forbrukerne kan handle med kontanter og bankkort – av selvhjulpne forbrukere.

Vi er vitne til en drastisk økning av digital svindel som skaper frykt og usikkerhet blant mange eldre. Kriminelle nettvettverk spesialiserer seg på å stjele identiteten og pengene våre. Hvem sitter med ansvaret når først uhellet er ute, bankene eller den enkelte bankkunde?

– Omfanget av svindelsakene øker. Framover vil forbrukerne bli svindlet på flere og mer avanserte måter. Tenk bare på hvilken risiko som kan ligge i bruken av kunstig intelligens.

Høyesterett har slått fast at bankene skal ta ansvaret for tapet. Ifølge loven skal bankene ha de beste forutsetningene og ressursene for å iverksette tiltak som reduserer risikoen for svindel.

Som forbruker og bankkunde vet vi lite om hva slags regler som gjelder. Vi stoler på banken, men i mange tilfeller havner svindelofre i en juridisk uklar situasjon når de “godkjenner” betalinger som senere viser seg å være svindel. Hvilke regler gjelder, og er de klare nok?

– Det er mange varianter av svindel. Ansvarsfordelingen mellom banken og kunden reguleres av finansavtaleloven. Hovedregelen etter loven er at banken er ansvarlig for tap som skyldes en ikke godkjent betalingstransaksjon. Men hva om kunden trykker raskt på godkjenn-knappen, for eksempel for å sjekke årets skatteoppgjør og isteden kommer inn på en falsk nettside? Da har kunden rent teknisk “bekreftet” betalingen, som går til en svindler. Kunden er ofte uvitende om at han bidrar til en betalingstransaksjon. Svindlerne utgir seg ofte å være fra banken selv. Er det et “samtykke” til betaling i slike tilfeller? Dette er kompliserte vurderinger, men det er mange som mener at kunden må forstå at han utfører og samtykker til en betalingstransaksjon. Finansklagenemnda har i slike saker kommet til at kunden ikke har samtykket til transaksjonen. Dersom kunden bestrider å ha ansvar for en slik transaksjon, skal banken som hovedregel tilbakeføre pengene til kundens konto.

Fra flere hold etterlyses en sikrere og mer funksjonell nasjonal fellesløsning til å logge seg inn på offentlige tjenester og banker. Vil ikke det være fornuftig å satse på?

– BankID løser behovene til mange, men ikke mange nok. Våre undersøkelser blant nordmenn over 16 år viser at omtrent 200 000 personer ikke disponerer BankID. Alderen på disse er jevnt fordelt, og årsakene kan være mange. Forbrukerrådet mener at vi trenger en offentlig eID på høyeste sikkerhetsnivå for å sikre at alle forbrukere har digital tilgang til de offentlige tjenestene de har rett til. Utstedelsen må skje under demokratisk kontroll.

På den positive siden ser vi i dag en rekke produkter på markedet som kan gjøre hverdagen enklere og trygge- re både hjemme og ute. Mange er basert på datateknologi og kopling til internett, som for eksempel mobil-telefoner, robotstøvsugere m.m. Har forbrukermyndighetene en rolle for å gi bedre informasjon om hva som finnes av produkter som kan kjøpes i vanlige butikker og på internett?

– Forbrukerrådet har som regel ikke mulighet til å teste og følge opp enkeltprodukter på markedet, så her må man nok se andre steder for veiledning og tips, for eksempel nettaviser og tilbakemeldinger fra andre brukere. Her er det også flere tilsyn som må se til at produktene er trygge og sikre og etterlever krav til for eksempel personvern og informasjonssikkerhet.



Min digitale hverdag

Seniornett-magasinet har intervjuet skuespiller Lise Fjeldstad (85)

Hva er ditt første digitale minne?

– På begynnelsen av 90-tallet var jeg med å starte Briskeby Vel. Styret kommuniserte via faks og stensilerte opp dokumenter. Men da barna fikk hver sin nydelige kremfargede PC, som de fort lærte seg å bruke, da fikk jeg hjelp. Selv våget jeg ikke å røre disse vakre «uhyrene».

Først på midten av 90-tallet lærte jeg å bruke en PC gjennom et kurs i regi av Uranienborg menighet. Kurset var for pensjonister, men jeg tryglet meg til å få være med. Da lærte jeg å ikke være helt gal av redsel for å trykke på knottene! Jeg lærte å gå inn og ut av PC-en og kom så langt at jeg fikk min egen e-postadresse og kunne ta imot og sende meldinger. Etter den andre kursdagen bestemte jeg meg for å skaffe en egen stasjonær Windows PC.

På en skala fra 1 til 10, vurderer du deg selv som teknologisinke (1) eller teknologinerd (10)?

– Uten tvil som teknologisinke; 3 kanskje på skalaen. Jeg begynte ganske tidlig, men utviklet meg jo ikke, for jeg hadde så mye annet å gjøre. Rollene sto i kø på den tiden.

Hvilke digitale plattformer er du på, og hvor mye tid bruker du på disse til daglig?



Lise Fjeldstad. Foto Svein Brimi

– Ofte starter jeg dagen med å sjekke e-poster og meldinger på telefonen.

Under frokosten leser jeg litt nyheter på telefonen. Etterpå bruker jeg min stasjonære PC til å sende og motta e-poster. Dette går helt fint så lenge de er uten vedlegg. Nettbank mestrer jeg.

Jeg søker på internett og bruker nettbutikker, for det er så deilig å få ting levert på døren eller posten. Jeg klarer å returnere et kjøp, om det er såpass dyrt at jeg syns at jeg gidder.

Facebook titter jeg litt på og sender ofte en hilsen, gratulasjon eller noe, men legger ikke ut noe.

Snapchat skjønner jeg ikke, men mottar ting fra barnebarna.

Jeg har både PC, smarttelefon og iPad, men den siste bruker jeg lite.

Hvis jeg har tid, bruker jeg 1–3 timer fordelt på formiddag og ettermiddag.

Hva behersker du godt? Hva er utfordringene?

– Nettpanken behersker jeg ganske godt. Jeg føler meg trygg.

Utfordringer er å kunne sende vedlegg i e-poster, eller å kunne skrive litt raskere på PC-tastaturet og å flytte rundt på teksten i et foredrag eller en tale.

Kanskje det å kunne legge ut mine meninger om noe på sosiale medier, men det har jeg en dobbelthet på.

Hvem henvender du deg til for å få hjelp?

– Sønnen min er til kjempestor hjelp. Han er utrolig snill og tålmodig. Det blir mest han som hjelper meg selv om min datter også er flink. Han kan komme inn på PC-en min, også på avstand. Ting jeg lurer på, sender jeg til ham, og er jeg i tvil om en e-post, kan han svare: «Dette er tøv». Men for å være ærlig må jeg innrømme at jeg mangler digital nysgjerrighet. Jeg er digitalt lat.

Hva er ditt forhold til kunstig intelligens (KI), og har du prøvd ChatGPT?

– Det er jo fantastisk, men samtidig syns jeg det er skremmende, hvordan det etter hvert kan brukes.

Jeg merker at dette engasjerer meg ikke i. Det kommer kastende over oss, og jeg kan ikke gjøre noe med det.

Jeg har ikke prøvd KI selv, men sett det i bruk. Ble kjempeimponert. Men jeg er nå 85 år, så dette får mine barn og barnebarn ta seg av.

Hva kan være til velsignelse, og hva frykter du ved den raske digitaliseringen?

– Det er tidsbesparende på alle mulige måter. Samtidig tror jeg at menneskets følelsesliv blir mer og mer avstumpet.

Samfunnet blir mer og mer effektivt, men også mer brutalt, hardt og kaldt. Intelletet blir skjerpet og utviklet, vil jeg tro, og følelseslivet blir neglisjert og visner.

Teatersalen og konsertsalen er snart de eneste stedene hvor man kan møtes ansikt til ansikt og kommunisere direkte med hverandre.

På telefon møter du ikke lenger en menneskelig stemme, og skal du i en bank, treffer du ikke et menneske, men maskiner. Jeg blir litt redd når jeg kommer inn i et rom med maskiner.

Økokrim's rolle

Seniornett-magasinet har stilt noen spørsmål til Økokrim om hvilken rolle de har når det gjelder digital kriminalitet og svindel overfor eldre spesielt. Her er svarene fra fungerende Økokrim-sjef, Inge Svae-Grotli.

Hvilken statlig etat har det overordnede ansvaret for digital svindel i Norge?

– Økokrim har et nasjonalt ansvar for å bekjempe bedragerier. Vi kan imidlertid ikke bekjempe denne samfunnstrusselen alene. Økokrim er opptatt av totalforsvaret mot økonomisk kriminalitet og jobber tett med både offentlige instanser og private aktører, som eksempelvis bankene og teletilbyderne, for å bekjempe digitale bedragerier. Samarbeid mellom relevante aktører er viktig i arbeidet mot denne samfunnstrusselen. For at vi skal få stoppet svindel fra å skje, må vi blant annet lukke sårbarheter som gjør det mulig å begå svindel.

*Fungerende Økokrim-sjef
Inge Svae-Grotli.
Foto: Økokrim*



I 2024 åpnet Økokrim en egen bedragerienhet på Gjøvik. Bedragerienheten jobber målrettet med å forebygge og bekjempe bedragerier som rammer innbyggere på tvers av politidistrikt og/eller har internasjonale forgreininger.

Hvordan følger Økokrim opp sine trusselvurderinger generelt og når det gjelder digital svindel overfor eldre spesielt?

– Økokrim jobber hver dag aktivt med å forebygge svindel. Opprettelsen av bedragerienheten på Gjøvik har styrket arbeidet betraktelig. Bedragerienheten ser anmeldelser på tvers av politidistrikt i sammenheng. På denne måten klarer vi å identifisere, pågripe og straffeforfølge bakmenn i store svindelsaker. I fjor ble to rumenske menn dømt for å ha svindlet over 400 nordmenn. Dette var en av de første sakene der svindelanmeldelser på tvers av politidistrikt ble sett i sammenheng.

Tidligere var det ofte eldre som ble utsatt for svindel. Slik er det ikke lenger. I dag kan alle bli lurt. Svindlere benytter kunstig intelligens og sosial manipulasjon i svindelforsøkene sine. Dette gjør at svindelen oppfattes som svært trover-

dig. Det er blitt vanskelig å skille ekte og falske henvendelser fra hverandre.

Har Økokrim en rolle når det gjelder å forebygge at eldre utsettes for svindel?

– Økokrim har en viktig rolle når det gjelder å forebygge og bekjempe svindel generelt, også svindel rettet mot eldre.

Vi er kjent med at Økokrim anbefaler at alle svindelforsøk anmeldes. Hvordan prioriteres slike saker, og hvilken forventning kan den som anmelder, ha til at en anmeldelse vil bli fulgt opp?

– Økokrim oppfordrer til å alltid anmelde bedragerier. Informasjonsinnhenting gjennom anmeldelser er viktig for politiets arbeid i kampen mot svindel, både for potensielle etterforskninger og for det forebyggende arbeidet i politiet. Alle anmeldelser vil kunne inneholde viktige spor som kan gi politiet informasjon om hvem som utfører bedrageriet og hvordan det gjennomføres.

Om du oppdager å ha blitt svindlet, ta umiddelbart kontakt med banken din og anmeld saken til politiet. I mange tilfeller klarer bankene å stoppe transaksjoner som er på vei til svindlerens bankkonto.



ØKOKRIM



Når uhellet er ute – hva gjør jeg?

Alle kan bli utsatt for digital svindel, for eksempel ved at personlige opplysninger blir stjålet og brukt til netthandel eller til å opprette nye bankkonti og lån i vårt navn. Dessverre er det blitt vanskeligere for oss å gjennomskue svindlerne, blant annet fordi mange har tatt i bruk kunstig intelligens (KI/AI).

Av Siri Kessel

Vi må legge vekk skammen over å ha blitt lurt og isteden raskest mulig trykke på alarmknappen. Det finnes gode råd om hvordan vi kan håndtere svindel!

Noen av dem som kan hjelpe oss med å stoppe svindeltransaksjoner, hindre at skadeomfanget øker eller hjelpe

oss med å få refundert noe av tapet, er politi, banker og forsikringsselskap. I tillegg er det flere, både private og offentlige instanser, som kan gi gode råd og hjelp.

Her presenterer vi hva disse instansene sier vi kan og bør gjøre.

Politiet¹

Anbefaler å:

- kontakte banken din for om mulig å stoppe overføringer
- anmelde forholdet til politiet
- kontakte forsikringsselskapet ditt for å sjekke om de dekker svindel

På politiets nettside finnes [skjemaet for anmeldelse av bedrageri](#)². Se nettsidene i fotnote 2 nederst på siden.

Ditt lokale politi kan gi veiledning og råd hvis du lurer på om du skal anmelde.

Bankene

Også bankene vil at vi skal melde fra om svindel. Videre ber de oss om å sperre aktuelle konti, bankkort og kredittkort.

Mange av bankene har gått sammen om å lage nettstedet [svindel.no](#)³, hvor vi kan lære oss selvforsvar mot svindel.

Bankene har et ansvar for å hjelpe oss om vi utsettes for svindel. Dette kan du lese om i artikkelen *Bankenes arbeid* mot svindel på side 15 i dette magasinet.

Forsikringsselskapene

Som politiet anbefaler, er det viktig å

sjekke om forsikringen vår dekker tap ved svindel.

Norsk senter for informasjons-sikring (NorSIS)

Senteret arbeider for at alle skal ha en trygg digital hverdag med særlig søke-lys på allmennheten og små og mellomstore bedrifter. NorSIS utgjør en del av arbeidet til Nasjonal sikkerhetsmyndighet (NSM).

På nettsidene til NorSIS finnes mye nyttig informasjon om svindel⁴. Deres råd til personer som utsettes for svindel eller svindelforsøk, er:

- **Få oversikt.** Skriv ned det som har skjedd så detaljert som mulig.
- **Anmeld forholdet til politiet.** Dette er viktig for deres arbeid. En kvittering på at forholdet er anmeldt, kan legges fram for eventuelle kreditorer.
- **Kontakt banken og sperr kort.** Meld fra til banken eller kontoutsteder om du oppdager nye, ikke gjenkjennbare konti eller transaksjoner.
- **Sperr kreditt.** De fleste som yter kreditt, vil verifisere din kredittver-

1 <https://www.politiet.no/tjenester/anmelde/anmelde-svindel-og-id-tyveri/>

2 <https://www.politiet.no/globalassets/tjenester-admin/anmelde/bedrageri---forenklet-anmeldelse.pdf>

3 <https://www.svindel.no>

4 <https://norsis.no/veiledninger/utsatt-for-id-tyveri/>

dighet hos et kredittopplysnings-selskap. Om du ber om frivillig sperring av din kreditt hos disse virksomhetene, vil det kunne verne deg mot ytterligere skade. Se kontaktopplysninger til kreditt-opplysningsselskapene på NorSIS' nettside (fotnote 4).

- **Følg med på posten.** Ved mistanke om urettmessig endring av adressen din, bør du snarest kontakte Posten.
- **Søk hjelp hos forsikringsselskapet ditt.** Finn ut om forsikringen din kanskje dekker ID-tyveri.
- **ID-tyveri på internett.** Får du kjennskap til at nye konti er opprettet i navnet ditt, eller at brukerrettigheter er endret eller konti er overtatt av andre, må du reagere umiddelbart. Følg punktene over. Om du ser at noen har gjennomført netthandel i ditt navn, bør du kontakte nettbutikken.
- **Andre du bør vurdere å kontakte.** Ved tap eller tyveri av ID-dokumenter, som pass, førerkort, Mastercard, VISA, NETS og Posten, må du melde fra. Kontaktinfo til instanser

hvor tap av ID-dokumenter kan meldes, finnes på NorSIS' nettside (fotnote 4).

Finanstilsynet

Råd ved svindel med kryptovaluta⁵ er utarbeidet av Finanstilsynet og er beregnet for investorer.

Seniornett – Datahjelpen

Er du medlem av Seniornett, kan Datahjelpen gi deg råd om hva du skal gjøre dersom du utsettes for svindelforsøk. Du kan ringe Datahjelpen på telefon 22 42 96 26, mandag–fredag fra kl. 9.00 til 15.30.

Jussbuss, Universitetet i Oslo (UiO)

Studenter ved juridisk fakultet kan gi råd ved svindel. De har utarbeidet skrevet «Informasjon til personer utsatt for svindel»⁶. I tillegg til de rådene vi allerede har nevnt, anbefaler de også å endre alle passord, sperre BankID-brikken og å sjekke gjeldsregisteret.

Du kan ta kontakt med Jussbuss via telefon 22 84 29 00, personlig oppmøte i Oslo eller ved å fylle ut [nettskjemaet til Jussbuss](#)⁷.

5 <https://www.finanstilsynet.no/forbrukerinformasjon/svindell-med-kryptovaluta/#Hvab%C3%B8rdugj%C3%B8rehvisduerutsattforkryptosvindell>

6 https://foreninger.uio.no/jussbuss/saksomrader/gjeldsrett/brosjyrer/informasjonskriv_svindell.pdf

7 <https://foreninger.uio.no/jussbuss/elektronisk-saksmottak/>

Astrid (77) forteller

“Jeg kjente at jeg ble dårlig.”

Astrid Holm, som er medlem av Seniornett i Tromsø, ble forsøkt svindlet i mai 2024. I et oppslag i avisa Tromsø fortalte hun om en oppringning som førte til at hun slo på PC-en og gjorde det vedkommende ba henne om. Dermed fikk svindlerne tilgang til banken hennes. Videre sa hun: *“Da jeg kom til meg selv, ringte jeg politiet. Der fikk jeg bekreftet at jeg var blitt lurt.”*

Siden det var kveld, var det ikke mer hun kunne gjøre enn å sperre kortene sine. Dagen etter ringte hun banken.

“De sa at det lå en overføring klar til å sendes til Thailand på 450.000 kroner. Da kjente jeg at jeg ble dårlig.”

Heldigvis fikk banken stoppet transaksjonen, så svindlerne fikk ikke tatt pengene fra Astrid! Hun forteller sin historie for å advare andre mot svindel og for å vise at det er mulig å få hjelp.



Astrid Holm. Foto: Ronald Johansen, Avisen Tromsø.

Bankenes arbeid mot svindel

Banknæringen arbeider aktivt for å forebygge, avdekke og stoppe svindel.

Av Gry Nergård, forbrukerpolitisk direktør for digital robusthet i Finans Norge

Svindel mot norske bankkunder er dessverre omfattende. Eldre med god økonomi og som har en viss digital utrygghet, ser ut til å være blant favorittene for svindlerne. De som blir utsatt for svindel, kan tape mye penger. I tillegg kan svindel skape betydelig usikkerhet, redsel, mistillit og i verste fall store psykiske påkjenninger for ofrene.

Banken er i stor grad forpliktet til å betale tilbake penger som kundene deres er blitt svindlet for; i første halvår 2024 måtte norske banker tilbakebetale 607 millioner kroner til svindelofre. Likevel er det mange som opplever å måtte dekke tapene selv fordi de selv har bidratt aktivt – gjerne over lengre tid – til den svindelen som rammet dem selv. Det gjelder for eksempel investerings-svindel og kjærlighetssvindel. Hvor mye penger folk taper, har vi dessverre ingen god oversikt over.

Selv om tapstallene er forholdsvis høye, betyr ikke det at bankene ikke gjør noe for å hindre denne svindelen. I første halvår 2024 stoppet også norske banker svindel for 1,3 milliarder kroner.



Gry Nergård, Finans Norge.

Foto: Daniel Nygård, Finans Norge

Bankene jobber sammen

Da vi sammen med bankene talte opp de mest vanlige svindeltypene før jul, kom vi frem til hele 16 ulike metoder.

For å motvirke disse 16 ulike svindel-metodene har bankene foreslått 20 tiltak som det må jobbes med i 2025. Det er dels tiltak som bankene selv må

jobbe med, men det er også tiltak hvor vi må samarbeide med andre, eller der vi må få andre til å iverksette tiltak.

Bankenes tiltak for å forebygge, avdekke og stoppe svindel

Noen av de viktigste tiltakene som bankene selv bør innføre, er listet opp i «Antisvindelhåndboken», som bankene har utviklet i fellesskap:

1. **Varsel:** Banken gir kunden varsel om mistenkelig aktivitet i mobil- og nettbank slik at kunden kan reagere i tide.
2. **Kontekst:** Kundene får mer informasjon om hva de er i ferd med å gjøre, bekrefte eller signere slik at de kan avsløre svindel.
3. **Tidsbegrensninger:** Banken og kunden får ekstra tid til å oppdage, undersøke og stoppe forsøk på svindel.
4. **Forsterket bekreftelse (step-up):** Ved høyrisikoaktivitet blir kunden bedt om å gi ekstra bekreftelse på identitet eller hensikt.
5. **Antisvindelsystem:** Banken overvåker transaksjoner for å oppdage mistenkelig aktivitet og kan innføre sperrer ved behov.
6. **Periodisk kontroll:** Banken oppfordrer kontoeier til jevnlig å gjennomgå innstillinger som kan påvirke svindelrisiko.

Noen av tiltakene vil føre til at det tar lengre tid å gjennomføre enkelte bankoppdrag. For eksempel, hvis det innføres tidsbegrensninger med hensyn til hvor lang tid en betalingstransaksjon tar, vil betalingen ta lengre tid enn tidligere. Og hvis banken sender varsel til kunden ved det banken oppfatter som en mistenkelig transaksjon og ber kunden bekrefte eller avkrefte om betalingen skal skje, vil det innebære handlinger fra kunden som denne kanskje synes er vanskelige.

Det har vært diskusjoner i bankene om hvor mye forsinkelser og ekstrarunder kundene vil tolerere for å få mer sikkerhet. Finans Norge fikk derfor utført en kundeundersøkelse som viste at 92 prosent av de spurte var ganske eller meget positive til en forsinkelse i betalingsoverføringer dersom det kan føre til bedre sikkerhet, og 72 prosent var positive til at banken kan sette begrensninger som gjør det vanskeligere å gjennomføre en svindel. Jo eldre man er, jo mer vil man akseptere av inngripende tiltak, mens de yngre var litt mer skeptiske.

Forbrukerinformasjon

Ettersom det er en stor påkjenning å bli utsatt for svindel, mener bankene at det også må være i kundenes interesse å lære seg selvforsvar mot svindel.

Bankene lagde derfor i fellesskap en forbruker-informasjonskampanje som ble sendt på radio, TV, i sosiale medier og på utendørsreklame sist sommer og



litt utover høsten. Kampanjen fokuserte på å lære forbrukerne å kjenne igjen ulike svindelmetoder, og hvordan man kan beskytte seg mot disse.

Samtidig ble nettsiden [svindel.no](https://www.svindel.no) etablert¹. Her legger vi fortløpende ut informasjon om aktuelle typer svindel, og der kan man også finne all informasjonen fra informasjonskampanjen.

Totalforsvar mot svindel

Økokrim har beskrevet svindel og bedragerier som et samfunnsproblem som alle har et felles ansvar for å bekjempe.

Bankene i Norge jobber derfor sammen med politiet, teleselskapene, BankID og offentlige myndigheter for å finne stadig flere og bedre tiltak i bekjempelse av økonomisk kriminalitet.



¹ <https://www.svindel.no/>

Behov for basiskunnskaper

Gjennom mitt arbeid som veileder i Seniornett Sarpsborg Øst har jeg hatt gleden av å møte mange seniorer som ønsker å mestre den digitale hverdagen. Med utgangspunkt i deres ønsker og behov ser jeg tydelige mønstre som kan være nyttige å dele.

Av Ove Gundersen, veileder i Seniornett Sarpsborg Øst



Ove Gundersen.
Foto: Mina Elisabeth
Albertsen.

Utfordringer i møte med det digitale

En av de største utfordringene er manglende basisforståelse for operativsystemer som Windows, MacOS, Android og iOS.

Mange seniorer opplever at det å

vite «hva som styrer hva» er en nøkkel til å få bedre flyt i bruken av mobilen, nettbrettet eller datamaskinen.

Eksempler på nyttig bruk

Når denne basisforståelsen kommer på plass, opplever flere en aha-opplevelse. De kan lettere håndtere nettbank, finne frem på offentlige tjenester

som HelseNorge, og bruke sosiale medier tryggere. Enkel innsikt, som hvordan oppdatere apper eller justere innstillinger, gir økt selvtillit.

Veien videre

Det kunne vært nyttig om Seniornett vurderte mer spesifikke kurs eller materiell som forklarer operativsystemene på en enkel og brukervennlig måte. Slike initiativ ville bidra til at flere seniorer føler seg inkludert i den digitale verden.

Jeg vil gjerne rose Seniornett for innsatsen dere gjør. Det å gi seniorer en plattform for læring og mestring er utrolig verdifullt. Sammen kan vi skape et miljø hvor flere våger å ta steget inn i den digitale verden med trygghet.

Seniornett Hønefoss

– hånd i hånd med kommunen

Av Jan W. Brill, leder Seniornett Hønefoss

Å mestre den stadig voksende digitale verden er ikke alltid like enkelt, spesielt for eldre som ikke er oppvokst med moderne teknologi. Seniornett Hønefoss har, i godt samarbeid med Ringerike kommune, viet seg til å styrke eldres digitale kompetanse gjennom en rekke kurs og aktiviteter. Kursene er gratis. Alle kursutgifter dekkes av kommunen. Våre frivillige er vanlige data- og mobilbrukere med forskjellig kunnskap og erfaring. Vi er i skrivende stund cirka 20 veiledere inklusive 6 kursledere. Vi hjelper hverandre når vi står fast. Felles for oss er at vi synes det er moro og meningsfullt å hjelpe andre.

Grunnkurset “Digital Hverdag”

I samarbeid med Ringerike kommune har Seniornett Hønefoss funnet en plattform for å nå ut til flest mulig eldre innbyggere. Vi startet vårt samarbeid i 2021 og har høsten 2024 hatt hele syv kurssteder: Hønefoss (to steder), Tyristrand, Sokna, Hallingby, Haugsbygd og Nes i Ådal. I 2024 har vi hatt cirka 70 deltakere hver sesong. Kurset er åpent for alle og er på cirka åtte kursdager à to timer. Vi fokuserer på bruk av smarttelefon. Kurset består derfor av grunnleggende telefonkunnskap og sikkerhet, samt viktige og nyttige apper som Vipps,

HelseNorge, 113, bankID, reise og parkering. På den siste kursdagen tar vi også for oss svindel. Kursdeltakerne får utdelt et kurshefte som vi selv har utviklet.

I tillegg til vårt eget grunnkurs har vi samarbeidet med Sparebank1 Ringerike Hadeland. Banken har holdt et totimers kurs om sine digitale tjenester flere steder i kommunen med størst fokus på svindel.

Torsdagstreff med en-til-en-veiledning

I tillegg til de omtalte kursene, tilbyr Seniornett Hønefoss en-til-en-veiledning hver torsdag på Ringerike bibliotek. Det ligger meget sentralt i Hønefoss, har gode parkeringsmuligheter og er meget positive til vår virksomhet.

For å øke bevisstheten om den digitale verden og dens utallige muligheter arrangerer Seniornett Hønefoss også foredrag om forskjellige aspekter av digital teknologi.

Annonsering

For å nå ut til potensielle deltakere og interesserte annonserer Seniornett Hønefoss og kommunen sine kurs og aktiviteter i Ringerikes Blad. I tillegg

til betalte annonser bruker vi avisens gratisspalte «Det skjer». Kursinformasjon spres fysisk og digitalt også på andre plattformer, som via lokale foreninger og Facebook-grupper. Ifølge svarene fra kursevalueringene er dog «jungeltelegrafen» den mest vanlige grunnen til at kursene blir kjent, og lokalavisa Ringerikes Blad er en god nummer to.

Kommentarer fra kommunen

Initiativtager til samarbeidet, Astrid Lundesgaard, som er rådgiver i Ringerike kommune, uttaler følgende:

– Bakgrunn for inngåelse av samarbeidet mellom Seniornett Hønefoss og Ringerike kommune, var at Helsedirektoratet under koronapandemien utlyste midler. Hensikten med tildeling av midler var å:

- Motvirke ensomhet, etablere møteplasser og heve grunnleggende digitale ferdigheter hos eldre.
- Bedre helsekompetansen, tilegne seg helseinformasjon på nett og gjøre eldre bedre i stand til å motta digitale helsetjenester som videokonsultasjon.
- Tilrettelegge for digital opplæring i kommunens lokasjoner sentralt i Hønefoss og ute i distriktene.
- Sammen rekruttere flere frivillige instruktører til Seniornett Hønefoss.

– Det gode samarbeidet med Seniornett Hønefoss er politisk forankret i kommunestyret. Eldrerådet følger med på arbeidet og etterspør resultatene. Et viktig resultat er at flere eldre ikke lenger kjenner på det digitale utenforskapet.



*13 av våre cirka 20 veiledere under en workshop på Ringerike rådhus i 2024.
Foto: A. Lundesgaard*

BankID-appen

Det begynner å bli en god stund siden vi betalte våre regninger i banken. Vi fikk en post- eller brevgiro i posten, og så tuslet vi til banken eller postkontoret for å betale denne. Det var i grunnen veldig greit, men ikke særlig effektivt. I dag er det ikke lenger så mange banker å besøke.

Av Tore Langemyr Larsen

Det finnes fortsatt en overlevning etter denne «enkle» verden i dagens Brevgiro. Bankene har flere ganger varslet at denne tjenesten snart blir borte – og det skjer nok – før eller senere. Og den er ganske dyr for deg i dag.

Og så ble BankID og BankID-appen født

BankID er nå den sikreste måten å utføre banktjenester på. Noen av de store bankene har i tillegg sin egen spesielle bank-app, for eksempel NordealID, men BankID-appen fungerer nå hos alle sammen. Det er alt du trenger!

Offentligheten har godtatt at BankID benyttes for å få tilgang til alle tjenestene som tilbys. Det gjelder for eksempel Skatteteaten, Altinn, Folkeregisteret, HelseNorge, stemme ved kommune- og stortingsvalg, adresseendring hos Posten, gi bud på bolig, signere lånesøknad, tinglyse dokumenter med mer. BankID har et sikkerhetsnivå som er på nivå fire, som er det høyeste.



De nye reglene for BankID, inkludert utviklingen av BankID på mobil, trådte i kraft 1. september 2024. Dette markerte overgangen til BankID-appen som den primære løsningen for digital identifikasjon og signering. Kodebrikken kan riktignok fortsatt brukes.

Før du tar i bruk appen, må du skaffe deg BankID om du ikke har det fra før. Bankene har alle litt forskjellige måter å tilby kundene BankID på, så følg oppskriftene på nettet for de ulike bankene.

Da går vi over til BankID-appen

BankID-app er en mobil løsning for å bruke BankID uten kodebrikke.

Appen kan lastes ned til din mobiltelefon fra **App Store** og **Google Play** avhengig om du har en iPhone/iPad eller en Android-telefon. Se etter symbolet eller ikonet over.

Før denne appen kan tas i bruk, må den “aktiviseres” av banken din. Dette kan virke noe tungvint, men sikkerheten sitter i førersetet her: *Det skal slås fast uten tvil at du er deg!* Dette er både for din egen sikkerhet samt at bankene i det siste har fått et skjerpet ansvar for å passe på pengene dine.

Avtale med banken

Du kan be om et møte i banken din for å få fullført aktiveringen av appen. Nå er det sånn at bankene ikke vanligvis er åpne slik at du bare kan stikke innom. Og det kan være langt til nærmeste bank. Det er nødvendig at du ringer og setter opp en avtale. Husk at du må ha med deg mobilen din samt noe som du identifiserer deg med med bilde, som pass, nasjonalt ID-kort, førerkort eller lignende.

Når du ringer banken, vil de sannsynligvis foreslå at du foretar aktiveringen over telefonen med deres hjelp. Slik at du slipper å møte opp. Det kan alle parter spare tid på. Da gjelder stegene som er beskrevet under. Med

hjelpen under, vil du også fint klare jobben selv.

Igjen litt forvirrende siden de ulike bankene har valgt litt forskjellige metoder for denne aktiviseringen, men mist ikke motet!

Det er bare de følgende måter bankene kan velge blant

1. **Aktivisering med kodebrikke**
2. **Aktivisering med aktiviseringskoder på sms og e-post**
3. **Aktivisering med pass**
4. **Aktivisering med nasjonalt ID-kort**

Bankene kan så velge én eller flere av disse metodene.

Alle metodene begynner med at du åpner BankID-appen, som du lastet ned på mobilen din. Gjør så hva du blir bedt om: Tast inn fødselsnummer (11 siffer) og ditt telefonnummer. Deretter får du en kode på sms som du også må skrive inn. Og så skiller de fire ulike metodene lag.

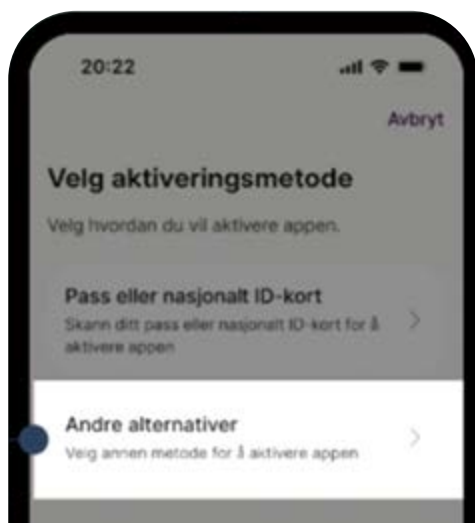
Og her er fremgangsmåtene:

Første metode: Kodebrikke

Du blir bedt om å velge aktiviseringsmetode:

Der velger du **Andre alternativer** og så **Kodebrikke eller app**.

Så logger du deg inn på vanlig måte med BankID, kodebrikkenummer og personlig passord.



Skjerm bilde av første metode for kodebrikke.

På grunn av sikkerheten så vil systemet få deg til å *vente én time* før du kan gå videre. Igjen for å forhindre svindel og ID-tyveri. Du bør også tillate at BankID sender deg en melding når tiden er ute.

Du logger deg så inn igjen med BankID, kodebrikke og personlig passord, og plutselig så er du nå den lykkelige bruker av BankID-appen!

Andre metode: Aktiveringskoder på sms og e-post

Denne metoden kan brukes om du ikke har kodebrikke fra banken din. Du logger deg inn som beskrevet over og velger igjen **Andre alternativer** og så **Aktiveringskoder**.

Nå blir du bedt om e-postadressen din. Her vil du nå få tilsendt koder istedenfor at du bruker kodebrikken. Koden du mottar, skriver du så inn. Og deretter logger du deg inn på BankID igjen, med personlig passord denne gangen.

Da er du ferdig, og den er nå aktivert.

De to siste metodene: Pass og nasjonalt ID-kort

Metode tre og fire er mer krevende. Fremgangsmåten er lik de andre til å begynne med, men du velger **Pass eller nasjonalt ID-kort** under **Velg aktiveringsmetode**. Så følg instruksjonene på skjermen. Som sagt litt krevende, og disse metodene er vel bedre egnet for brukere som:

- ikke har verken kodebrikke eller e-post
- ønsker å bruke Apples FaceID for å logge seg på BankID-appen

Dersom du har vanlig BankID og enten kodebrikke eller e-post, så vil nok metodene en og to anbefales. De er ganske greie metoder. Vil du bruke tre eller fire, så anbefaler vi at du tar kontakt med banken din for hjelp. Men for all del: prøv selv!

Hvis det er uaktuelt for deg å besøke banken, så er det [en web-side som](#)

har veldig gode beskrivelser av disse metodene¹, se under punktet «Guider». Denne siden er faktisk meget brukbar! Der kan du selv i eget tempo klikke deg igjennom alle stegene.

Lykke til!

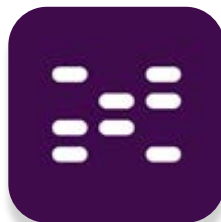
Så hvordan fungerer nå BankID-appen?

Når du har installert – og aktivert! – BankID-appen på din mobil, er du i gang. La oss si at du vil logge deg inn på banken din og velger **Logg inn** på bankens sider. Du skriver så inn ditt **Fødselsnummer** (11 siffer). Det som skjer nå, er at det sendes en melding til BankID-appen på din mobil. Meldingen vises på skjermen som: *Er det du som bruker BankID hos ...?*

Da har du to muligheter til å svare, enten **Ja, det er meg** eller **Nei, avbryt**. Dersom du ikke prøver å logge deg inn nå, så velger du **Nei**.

Så går det en beskjed tilbake til bankens sider der du prøver å logge inn og du skriver inn Personlig passord. Så er du logget inn!

Det kan være at du ikke finner meldingen fra BankID som du skal svare på, da finner du den hvis du trykker på ikonet for BankID-appen:



¹ <https://bankid.no/hjelp-bankid-app>

Felles offentlig elektronisk identifikasjon på vei



Digitaliseringsmyndighetene ønsker å etablere en ny eID – ja, under navnet «eID», altså elektronisk ID. BankID er eiet og drevet av et privat selskap og er knyttet til din bankkonto. Så har du pengene dine i madrassen – eller ikke kvalifiserer for BankID – så kan du vente på eID eller bruke noen andre systemer. Danmark har hatt dette i bruk i 15 år, MitID.

Av Tore Langemyr Larsen

BankID forutsetter at du har en konto i banken. Dette kan være veldig begrensende for utbredelsen av tjenesten. Bankene har (nedre) aldersgrenser for tildeling, du må ha et gyldig fødselsnummer og du må sannsynligvis ha et greit forhold til banken. Du kan eventuelt bruke noen andre systemer som finnes: Bypass ID eller Commfides. Disse må du riktignok betale for. Nå er det mulig å ha BankID i flere banker – som kan være viktig siden bankene har ulike aldersgrenser. Men mange er bekymret over det faktum at tjenesten er eiet av et privat selskap.

Det finnes en offentlig tjeneste, MinID, som har relativt stor utbredelse, men som har for lavt sikkerhetsnivå: nivå tre. Nivå tre betyr at systemet benytter to-nivå autentisering. Dette nivået vurderes noe for lavt for følsom informasjon, slik som helse- og skatteinformasjon, banktjenester, forsikringer, stemmegiving ved valg og annet. BankID har sikkerhetsnivå fire, det høyeste. Når det gjelder e-post, har e-Boks og Digipost sikkerhetsnivå fire.

Regjeringen har utarbeidet en nasjonal strategi for eID i offentlig sektor med

den hensikt å oppgradere MinID. Dette er drevet av en EU-forordning, [revidert eIDAS-forordning](#) (eIDAS 2.0)¹, med krav om offentlig ansvar for utstedelse av eID på høyt sikkerhetsnivå som en del av en digital lommebok (som Apple Pay, Google Pay, Samsung Pay). Under første mål i strategiens handlingsplan; [Alle relevante brukergrupper skal enkelt kunne skaffe seg en eID på det sikkerhetsnivået de har behov for](#)², er det syv tiltak av særlig betydning for seniorer:

- **Tiltak 1:** Regjeringen vil videreutvikle MinID for å bli mer robust og brukervennlig
- **Tiltak 2:** Regjeringen vil utrede hvordan eID på høyt sikkerhetsnivå kan gjøres tilgjengelig for flere
- **Tiltak 3:** Regjeringen vil vurdere utbredelse av en offentlig utstedt eID på sikkerhetsnivå høyt blant brukergruppene som ikke har en eID på sikkerhetsnivå høyt i dag
- **Tiltak 4:** Regjeringen vil at alle brukergrupper skal ha kunnskap om hvordan de får og bruker en eID
- **Tiltak 5:** Regjeringen vil utrede beste praksis og behov for sikker kommunikasjon mellom ulike sektorer og unge brukere, primært under 12 år

- **Tiltak 6:** Regjeringen vil utrede hvordan løsning for sikre og brukervennlige digitale fullmaktløsninger som muliggjør tilgang til offentlige tjenester på vegne av en annen bruker kan realiseres
- **Tiltak 7:** Regjeringen vil utrede brukervennlig eID til brukere uten fødsels- eller d-nummer

Vel og bra. Mesteparten av disse punktene er planlagt gjennomført i løpet av 2025.

Vi seniorer er opptatt at verden ikke skal bli eller være for komplisert. Det er så mye vi skal kunne, huske og lære oss, så:

Å nei, ikke nok et system som vi må forholde oss til! Det sies ikke noe om forholdet til BankID; om vi kan bruke eID overalt eller om vi må “slite” med to systemer i fremtiden.

Men siste ord er vel ikke sagt, om den ene eller den andre vil overta, eller om begge blir aktuelle. Vi får se når eID blir ferdig og tilgjengelig.

Du kan lese mer her:

[Nasjonal strategi for eID i offentlig sektor](#)³. Her finner du alle målene, med foreslåtte tiltak, i kapittel 3.

1 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651

2 <https://www.digdir.no/digital-identitet/mal-1-alle-relevante-brukergrupper-skal-enkelt-kunne-skafe-seg-en-eid-pa-det-sikkerhetsnivaet-de/5514>

3 https://www.regjeringen.no/contentassets/f3f51d0207f04296b8192636cf4a4521/h-2540_nasjonal-strategi-for-eid-i-offentlig-sektor.pdf

IKT-Norge: Etiske retningslinjer for digital inkludering

Øystein Husby, administrerende direktør i IKT-Norge, svarer på spørsmål fra Seniornett-magasinet

Kan du si litt om hensikten med IKT-Norges etiske retningslinjer for digital inkludering?

– Retningslinjene har som mål å sikre et inkluderende digitalt samfunn ved å gjøre digitale løsninger tilgjengelige for alle, uavhengig av barrierer som alder, språk eller funksjonsvariasjoner.

Hvem retter de seg mot?

– De retter seg mot premissleverandører, beslutningstakere, designere, utviklere og alle involverte i digitaliseringsprosesser.

Hvordan markedsføres de?

– Retningslinjene ble overlevert statsråden på området under Arendalsuka 2024 og blir ellers kommunisert i møter i bransjen der dette er tema. Mange av våre 300 medlemsbedrifter jobber direkte med design og utvikling, og er svært opptatt av å hindre digitalt utenforskap.

Hvem har ansvar for at utviklere og designere følger retningslinjene?

– Ansvar ligger hos alle involverte i digitaliseringen, inkludert beslutningstakere og utviklere, for å følge retningslinjene.



Digitaliseringsminister Karianne Tung og administrerende direktør i IKT-Norge Øyvind Husby. Foto: Øyvind Ganesh Eknes

Hva er kostnadene, og hvem betaler?

– Det er ikke dyrere å lage inkluderende løsninger så lenge det tas med i arbeidet fra starten av. Men å gjøre digitale tjenester brukbare for alle i etterkant, er selvsagt noe eierne av tjenestene må bekoste.

Om de etiske retningslinjene følges, hvordan kan de være til hjelp for eldre i deres digitale hverdag?

– Retningslinjene kan hjelpe eldre ved å gjøre digitale løsninger enklere å bruke, mer tilgjengelige og tilpasset deres behov.

Hvordan vil IKT-Norges etiske retningslinjer for digital inkludering kunne bidra til å skape mer sosial likhet og rettferdighet?

– Ved å fjerne barrierer kan retningslinjene bidra til et digitalt samfunn, der alle har like muligheter til å delta og dra nytte av digitale tjenester.

Etiske retningslinjer:

1 Blindsoner

1.1 Vi har alle blindsoner. Forsøk å ta rede på det du ikke vet. Utforsk hva som kan gjøre det vanskelig å bruke dine digitale tjenester.

1.2 Skaff informasjon om brukernes utfordringer og hvordan disse utfordringene påvirker deres behov.

1.3 Lær av andre som allerede har utviklet gode løsninger. Følg konvensjoner for oppbygging av digitale tjenester og produkter.

2 Prosess

2.1 Vi har alle ulike forutsetninger. Benytt barrierene og brukerbehov som en kilde til inspirasjon for innovasjon og nytenkning.

2.2 Planlegg for inkludering i alle ledd. Diskrimineringsvern må være en integrert del av alle utviklingsprosesser.

2.3 Fokuser på spillet mellom den fysiske hverdagen og den digitale tjenesten. Brukerne er hele mennesker, din digitale tjeneste er kun en liten del av deres liv.

3 Brukerinvolvering og testing

3.1 Søk innsikt fra brukere med demografisk spredning og forskjellige barrierer for digital deltakelse og bruk. Gjør dette så tidlig, og ofte som mulig.

3.2 Kartlegg hvilke grupper som kan være sårbare i møte med din digitale løsning, med utgangspunkt i barrierene.

2.3 Test hvordan tjenesten fungerer, så tidlig som mulig og med reelle brukere som opplever de største utfordringene.

4 Forankring i organisasjonen

4.1 Bidra til at alle beslutningstakere kjenner lovpålagte krav til likestilling og inkludering.

4.2 Sørg for at disse kravene måles gjennom utviklingsprosessen, samt i styringsverktøy som risiko- og sårbarhetsanalyser, eller tilsvarende.

4.3 Gi beskjed dersom avgjørelser tas på manglende kunnskapsgrunnlag. Del innsikt om barrierene brukere kan oppleve for å gi en mer komplett forståelse før avgjørelser tas.

5 Tverrfaglighet

5.1 Involver forskjellige faglige perspektiver gjennom hele utviklingsprosessen. Alle involverte er ansvarlige for å bidra til utviklingen av inkluderende digitale løsninger, og alle fagfelt deler ansvaret for å ikke diskriminere.

5.2 Tenk nytt og løs utfordringer tverrfaglig. Å skape inkluderende, digitale løsninger er komplekst. Med bevissthet og kunnskap om inkludering kan alle involverte samle seg rundt en felles rettesnor.

Ikke la svindlerne vinne – kjenn dine rettigheter!

Svindel har blitt mer sofistisert enn noensinne. Profesjonelle svindlere utnytter ny teknologi, psykologiske triks og manipulerende metoder for å lure folk til å gi fra seg penger, personopplysninger eller sikkerhetsinformasjon.

Av Marte Eidsand Kjørven, professor i rettsvitenskap ved Universitetet i Oslo

Mange eldre har blitt utsatt for svindel, og dessverre opplever mange også skam og skyldfølelse i etterkant. Det er viktig å forstå at svindel kan ramme hvem som helst – og at du har rettigheter hvis du blir utsatt for det!

Hovedregel: Banken skal dekke tapet

Hovedregelen er at banken skal dekke tapet dersom en svindeltransaksjon er «ikke godkjent» i lovens forstand. Hva som utgjør en «ikke godkjent» transaksjon, er et ganske komplisert juridisk spørsmål. Transaksjonen kan være «ikke godkjent» selv om du har trykket «godkjenn» i BankID-appen. Mange har for eksempel blitt lurt til å godkjenne transaksjoner etter å ha blitt oppringt av en svindler som utgir seg for å være fra banken eller politiet, og som sier at pengene må flyttes til en «sikker konto» (som selvsagt ikke er sikker i det hele tatt). I mange slike saker har Finansklagenemnda kommet til at transaksjonen ikke er godkjent i finansavtalelovens forstand, og at banken må bære tapet.



Marte Eidsand Kjørven, Foto: Universitetet i Oslo.

Dersom du har brutt pliktene dine i finansavtaleloven med vilje (forsett), må du dekke tapet selv. Men også dette er et komplisert juridisk spørsmål. At du har gitt fra deg BankID-informasjon til en betrodd person, for eksempel for å få hjelp til å betale regninger, betyr ikke nødvendigvis at lovens vilkår om forsett er oppfylt.

Loven beskytter deg også i tilfeller der noen har tatt opp et lån eller kjøpt varer eller tjenester i ditt navn.



Få en uavhengig vurdering

Men det er ikke alltid banken vil gi deg pengene tilbake uten videre. Flere opplever at banken hevder de selv er ansvarlige for tapet. Banken kan for eksempel prøve å argumentere for at en transaksjon er «godkjent», eller at du har handlet med «forsett» fordi du har gitt fra deg BankID- eller sikkerhetsinformasjon.

Hvis banken nekter å tilbakebetale pengene dine, kan det være lurt å få en uavhengig vurdering av saken. Finansklagenemnda eller juridiske eksperter kan hjelpe deg med å vurdere om bankens beslutning er i tråd med loven. Noen har rettshjelp- eller svindelforsikring uten å vite om det, for eksempel som del av innboforsikringen, gjennom en fagforening eller via telefonabonnementet. Sjekk om det gjelder for deg.

Da kan du også få hjelp til å klage til Finansklagenemnda.

Svindel kan ramme hvem som helst

Ikke la skam hindre deg i å kreve dine rettigheter! Svindelrammede er ofre for avanserte bedrag, ikke personer som har gjort noe galt. Dersom du eller noen du kjenner har blitt utsatt for svindel, husk at det finnes veier videre – og at du ikke nødvendigvis må bære tapet alene.

Vær kritisk, vær trygg og kjenn dine rettigheter!

Marthe Eidsand Kjørven fikk
[Rettssikkerhetsprisen i 2024.](#)¹

1 <https://www.juristforbundet.no/globalassets/dokumenter/arrangement/rettssikkerhetsskonferansen/juryens-begrunnelse-2024.pdf>

Nyttig å vite om domenenavn

Et domenenavn er en adresse som brukes til nettsider og e-post. Seniornett har domenenavnet seniornett.no. Nettstedet har adressen <https://seniornett.no>, og en e-postadresse kan være kontor@seniornett.no. Her gir vi en oversikt over hvordan du kan bruke digitale tjenester på en tryggere måte med litt kunnskap om domenenavn.

Av Elisabeth Farstad

Domenenavnet er viktig for sikker navigering

Hvert eneste domenenavn er unikt; det finnes bare ett av hvert. Det betyr at en liten feilskrivning kan lede til en annen nettside. Se på seniornet.no og seniornett.no. De to uttales likt, men en t for lite betyr et annet domenenavn. Du risikerer dermed å havne et annet sted enn du tenkte eller at en e-post ikke kommer fra Seniornett, men fra noen som har onde hensikter.

Hvis du mistenker ugler i mosen

Hvis du er i tvil om hvorvidt en e-post kommer fra riktig avsender:

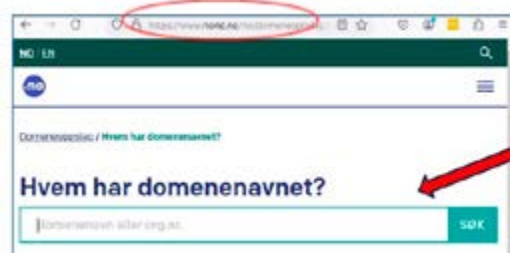
- Gå inn i avsendernavnet og sjekk e-postadressen. Trykk på avsendernavnet og se hvilket domenenavn e-posten er sendt fra.



Hvis Seniornett er avsender, skal e-postadressen være fra en avsender under domenenavnet *seniornett.no*

Hvis du er i tvil om hvorvidt en nettside er den du mente å besøke:

- Hvis det gjelder en nettbutikk eller annen kommersiell virksomhet der du skal betale noe, og du er i tvil om hvem avsenderen er: Hvis adressen slutter på .no, kan du gå inn i [det norske domeneregisteret](https://www.norid.no/no/)¹ og sjekke hvem som har domenenavnet. Registeret er åpent tilgjengelig for alle. Du ser hvem som står bak domenenavnet, og du finner kontaktinformasjon til vedkommende.



¹ <https://www.norid.no/no/>

Det kan være en god idé å sende en e-post eller ringe for å sjekke om dette virkelig er den avsenderen de gir seg ut for å være.

- Hvis domenenavnet slutter på noe annet enn .no, er det litt mer omstendelig. Da går du via en oversikt over [alle verdens toppdomener](https://www.iana.org/domains/root/db)². Her finner du ut hvem som administrerer toppdomenet og kan sjekke selve domenenavnet hos dem.

Noen tips

1. **Skriv inn domenenavnet selv.** Hvis du er i tvil når du får en lenke: Skriv inn domenenavnet (adressen) selv istedenfor å trykke på lenken. Vær pinlig nøyaktig når du skriver!
2. **Vær obs når du bruker en søkemotor.** Du kan gå direkte til den siden du skal besøke istedenfor å gå via en søkemotor. Da er det mindre risiko for å havne på villstrå.
3. **Se etter «https://» og hengelåsen.** Sjekk at det står «https://» og en liten hengelås foran domenenavnet. Da er siden sikrere enn om det bare står "http" uten "s".



4. **Lag bokmerker.** Lag bokmerker i nettleseren for sider du bruker ofte, som banken din, NRK eller NAV. Med

bokmerker navigerer du raskere og tryggere. Hvordan du lager bokmerker, varierer litt mellom ulike nettlesere, men ofte trykker du på en stjerne i adressefeltet.



Fakta

Et domenenavn er en nettsadresse, for eksempel seniornett.no. Det siste leddet – «etternavnet» – viser typen adresse. Alle land i verden har sin egen landkode på to bokstaver, i Norge er landkoden .no, i Sverige .se osv.

Det finnes også andre såkalte toppdomener, som for eksempel .com og .org., og en virksomhet kan også ha sitt eget, som for eksempel .gucci eller .pizza.

I 2024 eksisterte det om lag 350 millioner domenenavn i verden; under den norske landkoden er det registrert i overkant av 850 000. Hvert domenenavn er unikt, det finnes bare ett av hvert.

Under et domenenavn kan det registreres et uendelig antall e-postadresser. Det er ikke mulig å ha oversikt over antallet, og det finnes dermed ikke noe register over e-postadresser.

² <https://www.iana.org/domains/root/db>



QUIZ: Ti strake

Spørsmål

1. Hva står forkortelsen “CPU” for?

- A. Central Processing Unit
- B. Computer Power Unit
- C. Central Programming Utility
- D. Core Processing Unit

2. Hva er en nettleser?

- A. En enhet som lagrer filer
- B. En type virus
- C. En brannmur
- D. Et program for å surfe på internett

3. Hva betyr det å “lagre i skyen”?

- A. Å lagre filer på en CD
- B. Å sende filer til en ekstern server via internett
- C. Å kopiere filer til en USB-pinne
- D. Å skrive ut dokumenter

4. Hva gjør et antivirusprogram?

- A. Forhindrer reklame på nettet
- B. Gjør datamaskinen raskere
- C. Beskytter mot skadelige programmer og virus
- D. Fjerner gamle filer

5. Hva er en e-post?

- A. Et fysisk brev sendt via posten
- B. En digital melding sendt via internett
- C. En type virus
- D. En nettside

6. Hva betyr “kopier og lim inn” (copy & paste)?

- A. Å lage en sikkerhetskopi av alle filer
- B. Å flytte en fil fra én datamaskin til en annen
- C. Å duplisere tekst eller filer og plassere dem et annet sted
- D. Å skrive ut et dokument

7. Hva brukes et passord til?

- A. Å logge inn på tjenester og beskytte informasjon
- B. Å forbedre internetthastigheten
- C. Å blokkere reklame på nettet
- D. Å oppdatere datamaskinen

8. Hva skjer hvis du klikker på en lenke i en e-post fra en ukjent avsender?

- A. Ingenting, det er helt trygt
- B. Du kan bli omdirigert til en skadelig nettside
- C. Du laster automatisk ned et nytt program
- D. Datamaskinen din blir raskere

9. Hva bør du gjøre hvis datamaskinen din blir veldig treg?

- A. Slå den av og aldri bruke den igjen
- B. Knuse tastaturet i frustrasjon
- C. Kjøpe en ny skjerm
- D. Slette unødvendige filer og programmer

10. Hva skjer hvis du trykker og holder inne av/på-knappen på smarttelefonen i flere sekunder?

- A. Telefonen tar et skjermbilde
- B. Telefonen åpner en ny app
- C. Telefonen sender en nødmelding
- D. Telefonen skruer seg av eller gir mulighet til omstart



Svar

1: A) Central Processing Unit. CPU, eller prosessoren, er hjernen i datamaskinen og utfører beregninger og instruksjoner.

2: D) Et program for å surfe på internett. En nettleser (for eksempel Edge, Safari, Chrome, Firefox) brukes til å besøke nettsider og søke på internett.

3: B) Å sende filer til en ekstern server via internett. Skylagring (for eksempel OneDrive, Google Drive) lar deg lagre filer på internett slik at du får tilgang til dem fra ulike enheter.

4: C) Beskytter mot skadelige programmer og virus. Antivirusprogrammer skanner datamaskinen for virus og skadelig programvare, og hjelper med å holde den sikker.

5: B) En digital melding sendt via internett. E-post (elektronisk post) brukes til å sende og motta meldinger over internett (f.eks. Gmail, Outlook).

6: C) Å duplisere tekst eller filer og plassere dem et annet sted. “Kopier og

lim inn” lar deg raskt duplisere tekst eller filer uten å skrive dem inn manuelt på nytt.

7: A) Å logge inn på tjenester og beskytte informasjon. Et sterkt passord hjelper med å beskytte kontoer og personlige data mot uautorisert tilgang.

8: B) Du kan bli omdirigert til en skadelig nettside. Vær forsiktig med e-poster fra ukjente avsendere. De kan inneholde såkalte «phishing»-lenker som prøver å stjele informasjon fra deg.

9: D) Slette unødvendige filer og programmer. Overflødige programmer og filer kan gjøre datamaskinen treg. Å rydde opp kan forbedre ytelsen.

10: D) Telefonen skruer seg av eller gir mulighet til omstart. Hvis telefonen ikke fungerer som den skal, kan det hjelpe å skru den av og på igjen. På de fleste smarttelefoner holder du inne av/på-knappen i noen sekunder for å få opp en meny der du kan velge å skru av eller starte telefonen på nytt.

En datahjelpers hverdag

– Så mange takknemlige tilbakemeldinger!

– Å hjelpe folk til å bli selv-hjulpne digitalt gir meg masse glede, sier Jan Fredrik Gunvaldsen, en av Seniornetts mange populære datahjelpere på telefon. Han oppfordrer alle som har lyst på en positiv opplevelse, om å prøve seg.

Av Hanni W. Petersen

– Å hjelpe andre er morsomt, og det gir energi. Mye mer enn det tar, sier Jan Fredrik smilende, og legger til at man slett ikke må kunne alt for å være datahjelper i Seniornett.

– Du trenger ikke å være mangeårig dataekspert. Det holder med grunnleggende kunnskaper. Du vil lære etter hvert og utvikle deg faglig. Som datahjelper kommer du borti så mange ulike problemstillinger, og det er jo en av tingene som gjør det så morsomt.

For egen del kom Jan Fredrik inn i Seniornett da han i 2022 pensjonerte seg etter mer enn 40 år i IKT-bransjen. Han trengte noe å gjøre og ønsket å bidra med noe meningsfullt. Han tok kontakt med den lokale Seniornett-foreningen i Hønefoss og meldte seg til tjeneste. Siden har han vært aktiv veileder og kursholder på Ringerike og fast datahjelper i Seniornett.



Jan Fredrik Gunvaldsen. Foto: Kirsten Moe

Møte med respekt

I 2024 hadde Jan Fredrik nær 250 datahjelpesamtaler på telefon. En god del av dem er gjentatte samtaler med samme person. Jan Fredrik får ofte høre at de som ringer inn på nytt, vil snakke med nettopp ham.

– Jeg møter så mange takknemlige mennesker som datahjelper i Seniornett. Det er utrolig givende, og det bekrefter at jeg lykkes med det som er viktig for meg.

Jan Fredrik har høy bevissthet rundt hvordan han møter menneskene i den andre enden av telefonen, eller i kursrommet eller i en veiledningsseanse, for den sakens skyld.

– Du må hjelpe folk der de er og ha respekt for nivået de er på, ikke snakke over hodet på dem, sier han engasjert. Og legger til at det ofte handler om å ta bort usikkerhet og skamfølelsen de kommer inn med fordi de ikke kan og får til disse tingene.

– Jeg bruker gjerne litt humor, og beroligende ord, da er det lett å bryte ned dette ubehaget. Du må rett og slett legge litt sjel i det, gi den andre en opplevelse av at dette er viktig for deg også. Da blir det en glede for alle.

Seniornett-familien

Det er sent i januar, og Jan Fredrik har vært på vinterens pizzatreff i Dronningens gate i Oslo, sammen med resten av Seniornetts datahjelpere. Han er blitt både inspirert og motivert av de gode diskusjonene og erfaringsutvekslingene som disse samlingene byr på.

– Det er veldig hyggelige folk å samarbeide med her. Og skulle du komme borti en problemstilling du ikke kan svare på eller hjelpe til med, er det bare å spørre de andre i gruppa, vi finner alltid ut av det. Det er dessuten helt ufarlig ikke å kunne svare på alle spørsmål du får. Bare vær ærlig på at dette skal du finne ut av og at du ringer dem tilbake, sier Jan Fredrik og avslutter med å gjenta hvor meningsfull denne oppgaven er!

Seniornetts datahjelp på telefon

- Datahjelpen på telefon er åpen fem dager i uken, i kontorets åpningstid fra klokken 09.00 til 15.30.

- Vi har cirka 18 datahjelpere, de fleste er frivillige, noen er ansatt. Datahjelperne er på et par timer, halve dager eller hele dager, dette tilpasses den enkeltes ønsker og muligheter.
- I 2024 var det 4545 registrerte henvendelser på datahjelpen, en økning på ti prosent fra året før.
- Rådgivningen og veiledning på datahjelp dreier seg om e-post, nettlelere, programvare, nettbrett, mobil, pc og Mac, sosiale medier, sikkerhet osv.
- Datahjelperne i Seniornett har signert taushetserklæring og får oppfølging og opplæring



Drømmer du om å bli en digital livredder?

Har du lyst til å hjelpe andre?
Liker du å snakke med mennesker?
Kunne du tenke deg å utvikle deg datafaglig og lære nye ting?

Ta kontakt med **Roar Kristiansen**
på tlf. **22 42 96 26** eller
datahjelp@seniornett.no,
og meld deg som datahjelper på telefon i Seniornett.

Seniornetts medlemmer trenger deg!



TIPS & TRIKS

Hold mobilen oppdatert!



Vi er etter hvert blitt avhengige av mobiltelefonen vår. For å oppnå en tryggere og mer effektiv digital hverdag er det viktig å holde mobilens operativsystem oppdatert. Operativsystemet, ofte forkortet OS, er et dataprogram som startes opp før alle andre programmer og som lar deg installere og kjøre annen programvare. Gjennom å holde operativsystemet oppdatert sikrer du at mobilen din har de nyeste funksjonene, de siste sikkerhetsoppdateringene og forbedringer som gir bedre ytelse.

Før du starter oppdateringen

- Sørg for at telefonen har minst 50 prosent batteri eller er koblet til en lader
- Sørg for at telefonen har nettilgang (Wifi eller 4G/5G)

Slik oppdaterer du operativsystemet

Dette varierer avhengig av hva slags operativsystem mobilen din bruker. De mest vanlige er Android og iOS. Her er oppskrift for begge typer:

Android (for Samsung og andre)

1. Koble til et stabilt **Wifi-nettverk**
2. Da unngår du ekstra kostnader for mobildata
3. Åpne **Innstillinger**
4. Trykk på **System** eller **Om telefonen** ved å rulle nedover (dette kan variere avhengig av telefonmodell) og finn **Oppdateringer**
5. Trykk på **Programvareoppdatering** eller **Systemoppdatering** for å sjekke om det finnes nye oppdateringer. Hvis en oppdatering er tilgjengelig: **Last ned** og **Installer**. Dette kan ta noen minutter. Telefonen vil vanligvis starte på nytt etterpå.



iOS (for iPhone)

1. Koble til et stabilt **Wifi-nettverk**. Da unngår du ekstra kostnader for mobildata
2. Åpne **Innstillinger**
3. Gå til **Generelt**
4. Trykk på **Programvareoppdatering**. iPhone vil automatisk søke etter oppdateringer. Hvis en oppdatering er tilgjengelig:

5. Trykk på **Last ned** og **Installer**. Du kan bli bedt om å oppgi Apple-passordet ditt. Du kan velge å installere oppdateringen med én gang eller senere. iPhone vil starte på nytt når oppdateringen er installert.

Viktige tips

- Det er lurt å ta en sikkerhetskopi (til en skytjeneste, PC/Mac eller en ekstern harddisk) av mobilen før du oppdaterer operativsystemet. Dette bør gjøres i tilfelle noe skulle gå galt under prosessen.

Slik tar du sikkerhetskopi til en skylagringstjeneste

- **Android – Google.** Åpne appen *Innstillinger* og velg *Google > Sikkerhetskopiering*. Rull ned til *Detaljer om sikkerhetskopien*
- **iPhone – iCloud.** Åpne appen *Innstillinger* og klikk der navnet ditt står > *iCloud > iCloud-sikkerhetskopi*. Slå deretter på *Sikkerhetskopier iPhone*



Slik kan du ta sikkerhetskopi til en PC/Mac

- **Android.** Koble telefonen din til PC-en via USB kabelen. Da vil varselet: «*Lader denne enheten via USB*» dukke opp på telefonen. Trykk på dette varselet. En ny melding dukker da opp: «*Bruk USB til*». Trykk denne og velg *Overfør filer eller Filoverføring*. Trykk på varselet på PC-en for å få opp en melding. Velg *Åpne enheten* for å vise filer, fra denne meldingen. Herfra kan du kopiere filene til PC-en din.
- **iPhone.** Koble iPhone din til Mac-en din med en kabel. Åpne *Finder* på Mac-en og marker *iPhone* i sidepanelet i *Finder*. Merk at for å kunne sikkerhetskopiere via *Finder* må Mac-ens operativsystem være macOS 10.15 eller nyere. (Hvis det er eldre kan du bruke *iTunes* for å sikkerhetskopiere iPhone din). Trykk på *Generelt* øverst i *Finder*. Marker «*Sikkerhetskopier alle dataene på iPhone til denne Macen*». Hvis du ønsker å kryptere sikkerhetskopidataene og beskytte dem med et passord, markerer du «*Krypter lokal sikkerhetskopi*». Trykk deretter på *Sikkerhetskopier nå*.

Etter oppdateringen bør du sjekke at alle appene dine fungerer med det nye operativsystemet, eller om noen apper også må oppdateres.



Generalsekretærens hjørne

Alle skal med – også i den tredje alder

Hvordan kan Norge bli verdens mest digitaliserte land innen 2030 når en av fem er digitalt sårbare og faller utenfor, de fleste i livets tredje alder?

Regjeringen la i fjor høst fram en ambisiøs digitaliseringsstrategi, Fremtidens digitale Norge. Den handler om digital infrastruktur, digitale systemer og digital innovasjon. Norge skal bli verdens mest digitaliserte land innen 2030, hevder strategien, som sier mindre om menneskene som skal ha nytte av digitaliseringen.

850 000 i Norge har svake digitale ferdigheter og er digitalt sårbare. Svært mange er eldre og allerede i fare for å falle utenfor. Fra håndtering av eget liv, fra å kunne delta i demokratiet og fra å ha glede av den teknologiske og digitale utviklingen.

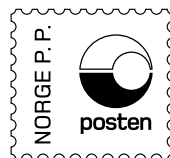
Digitaliseringsstrategien angir videre at 95 prosent av innbyggerne i Norge skal ha grunnleggende digitale ferdigheter

innen 2030. Innsatsområdene ellers sier lite om hvordan dette skal gjøres i praksis eller hvordan eldre og digitalt sårbare kan ivaretas.

Seniornett har i snart 30 år bidratt med opplæring og veiledning av seniorer i digitale ferdigheter. Vi har hatt titusener av eldre innom våre tilpassede opplæringsaktiviteter i lokale foreninger landet rundt, og vi svarer ukentlig på over 100 datahjelpetelefoner fra medlemmer med behov for digital veiledning og støtte. Vi vet hvor mange som trenger hjelp og hvor vondt det er å falle utenfor. Vi vet også hvor lite ressurser som settes av til dette viktige inkluderingsarbeidet.

Norge kan bli verdens mest digitaliserte land – hvis alle er med. Vi mener det nå må settes tall og handling bak de flotte planene og strategiene. Det trengs et solid løft og en digital opplæringsdugnad og inkluderingspott. For å få alle med; både i den første, andre og ikke minst tredje alder!

Hanni W. Petersen, generalsekretær



Medlemsfordeler

For kr 400,- pr år får du:

- Fri datahjelp på telefon eller via nettet
- Datahjelp hos lokale foreninger eller etter avtale ved hovedkontoret
- Seniornettmagasinet to ganger årlig i posten
- Ukentlige nyhetsbrev på e-post
- Tilgang til en av 225 lokale foreninger



Melder du deg inn etter 1. september, gjelder kontingenten også for påfølgende år.



Ja! Jeg vil bli medlem i  **Seniornett**

*Fornavn: _____

*Etternavn: _____

*Adresse: _____

*Postnr.: _____ *Poststed: _____

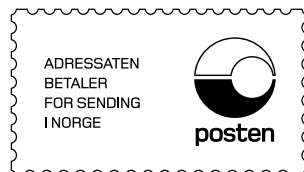
Telefon: _____

E-post: _____

Lokalforening: _____

Andre kommentarer: _____

*Må fylles ut (BRUK BLOKKBOKSTAVER)



Seniornett Norge
Svarsending 3324
0092 Oslo