

Informasjonssikkerhet for seniorer

Svindelmetoder

Svein R. Aarvik



Ikke ute etter deg som person
De kriminelle spiller på følelser

- **Frykt**
- **Fristelser (penger / kjærlighet)**
- **Tillit**
- **Tidspress**
- **Hva andre gjør**
- **Autoriteter**
- **Teknisk informasjon**



Informasjonssikkerhet for seniorer

«**Brukerkontoer**»



Passord og pinkode på PC/nettbrett/mobil

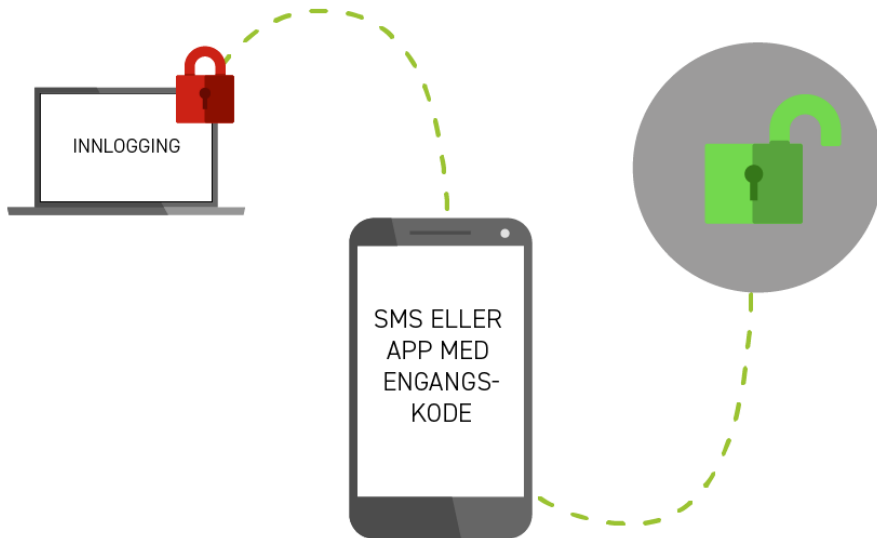
Kommer din PC, nettbrett eller PC over på uvedkommendes hender kan utstyret brukes til å svindle deg.

Det er derfor viktig når du setter opp dette utstyret at **du legger inn passord for å starte opp PC**, og pinkode for å starte nettbrett og mobil.

Skulle du miste eller forlegge utstyret vil det da ikke kunne bli misbrukt om det kommer over på uvedkommendes hender.

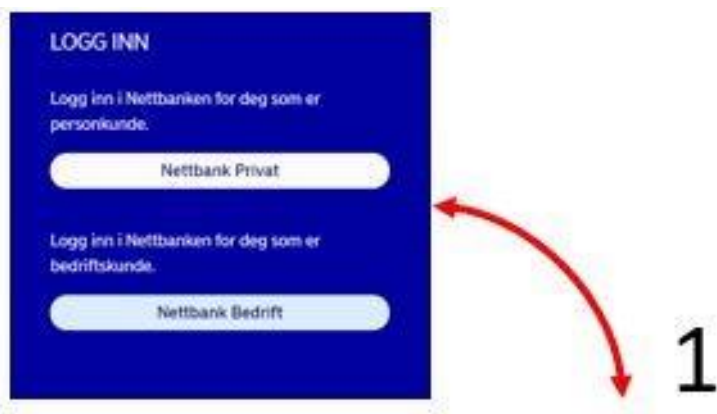
Legger du fra deg PC, nettbrett eller mobil, der andre kan få tilgang til dette utstyret, så husk på å **låse utstyret slik at en kun kan åpne det med passordet eller pinkoden.**

Sikre din brukerkonto med totrinnsbekreftelse



Fordi passord både kan lures fra deg, og at det finnes passordprogram som teknisk sett avslører ditt passord, har leverandører **innført totrinnsbekreftelse for å være sikrere på at det er du som logger deg inn på din tjeneste.**

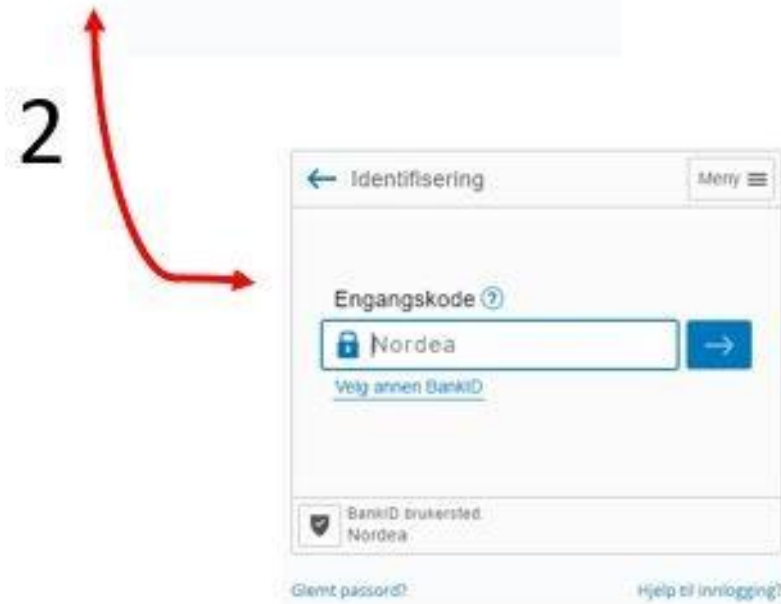
Når du logger deg inn taster du inn ditt brukernavn og passord, da er du ferdig med det første innloggingstrinnet. **Det andre trinnet er at det eks. sendes en kode til din mobil eller kodebrikke som du taster inn i et anvist felt i innloggingen.**



Bank ID er et eksempel på totrinnsbekreftelse

Når du logger seg inn mot din bank bruker bankene BankID for å være helt sikker på at **ingen andre enn deg kan logge seg inn i dine bankkontoer.**

Dette gjøres ved at du på forhånd hos banken har registrert din mobil eller kodebrikke, slik at banken kan sende koden for pålogging til din kodebrikke eller mobilen, som du deretter taster inn i innloggingsbildet.



Banktjenester med BankID er en sikker måte å logge seg inn på.



Informasjonssikkerhet for seniorer

«**Bruk av e-post**»



E-post

E-post er en **enkel og rask** tjeneste for kommunikasjon.

E-post er dessverre også **mye brukt blant svindlere** for å nå potensielle ofre. Spesielt siden det ikke er noen direkte kostnad forbundet med utsendelse, og at sporing av avsender er vanskelig.

Det er heller ikke noen generelle filtrerings- eller sikkerhetsmekanismer bygget inn i e-post.

Forfalskning av avsender

Ang. din konto hos oss



tormod.hansen@dnb.no
Mon 28-Jan-19 15:23

To: ☐ ola.olsen@eksempel.no;

← REPLY

↩ REPLY ALL

→ FORWARD



Mark as unread

Avsender på en e-post er svært lett å forfalske, og det finnes ingen innebygget kontroll eller identifisering.

Du kan altså **aldri stole på at avsender av en e-post er den en gir seg ut for**. Stemmer ikke innholdet med hvordan avsender vanligvis formulerer seg, så gjør en ekstra **kontroll eks. via telefon**. Mao. tenk deg om hvis innholdet i e-posten "skurrer"



Hvorfor får jeg e-postsvindel

Svindlere samler e-postadresser slik som **selgere samler telefonnummer**.

Følgende innhold er svært vanlig i svindler:

- **Lånetilbud**
- **Forretningsmuligheter og investeringsmuligheter**
- **Utdeling av gaver og fristende konkurranser**
- **Arv og kontakt fra påståtte advokater**
- **Jobbtilbud**
- **Kjæresteforhold og pornografisk innhold**
- **Salg av tabubelagte varer** (potensmiddel, helsekost osv.)
- **Gode tilbud på luksusvarer** (Rolex, mobiltelefoner osv.)
- E-post med slikt innhold bør medføre grunnholdningen din om at det kan være en svindel. **Tenk deg om for hva du gjør videre.**



Riktig E-post

- Hei, Svein Ragnar
- Du har fått en ny melding i Digipost:
- - Melding fra det offentlige, «Årsoppgave» fra NAV
- Logg inn i Digipost-appen eller på nett for å lese meldingen.
-
- Med vennlig hilsen
- Digipost
- --
- Du mottar varsler om nye meldinger, og påminnelser om post, basert på innstillingene dine i Digipost.
- Denne e-posten ble sendt 7. januar 2025 19:02.



Informasjonssikkerhet for seniorer

«Sosiale medier»



Sosiale medier

Vi vil i denne kursmodulen ta for oss farer rundt bruk av **Facebook**, ettersom det er tjenesten flest benytter. Rådene og farene gjelder imidlertid også de fleste andre sosiale mediene, slik som Twitter, LinkedIn og Pinterest for å nevne noen.

Følger du våre råd vil du stort sett få en trygg og positiv opplevelse.

De vanligste svindlene i sosiale medier er:

- **Annonsering for varer og tjenester som i bunn og grunn er svindel**
- **Kjærlighetssvindel**
- **Uthenting av privat informasjon som benyttes til målrettede svindel eller utpressing**
- **Deling av falsk informasjon**
- **Falske konkurranser**



Falske kontakter

En vanlig måte svindlere kommer i kontakt med deg er via **falske venneforespørsler**. Ofte **søte unge jenter** for menn, og **personer i uniform** for kvinner.

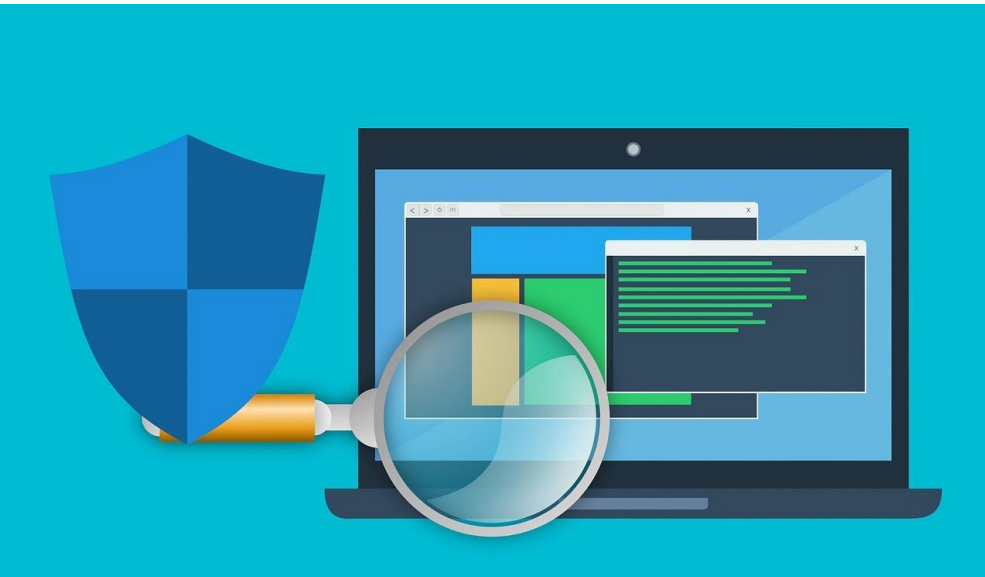




Informasjonssikkerhet for seniorer

«Sikkerhetsverktøy»

Sikkerhetsverktøy



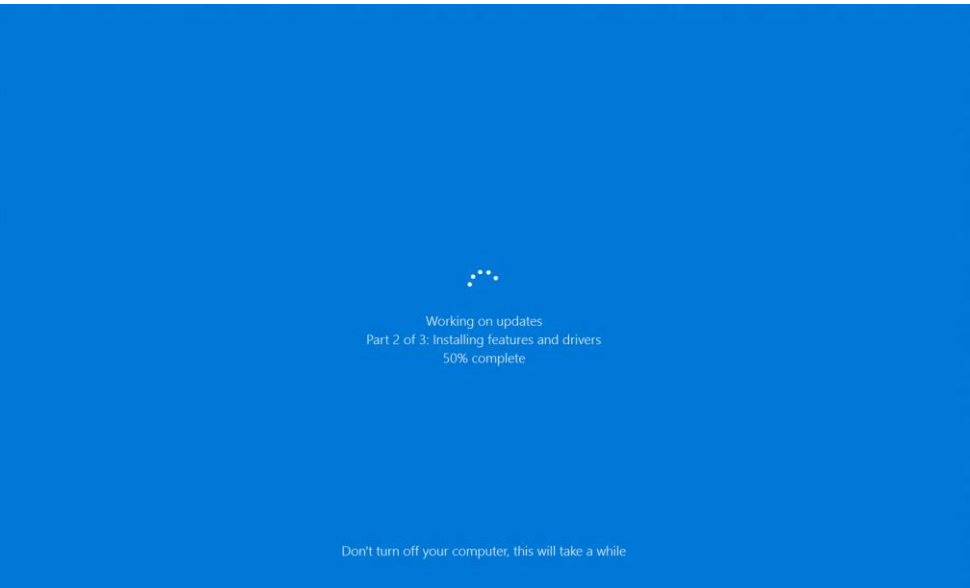
Som nevnt i introduksjonen til dette kurset er de fleste farer i dag basert på **sosial manipulasjon**.

Vi nevnte også at din **egen vurdering** ofte er viktigere og mer effektiv enn tekniske verktøy.

Vi skal likevel ta for oss noen **sikkerhetsverktøy**, for det er jo ikke slik at disse er uten effekt. Vi bør som minimum ha:

- rutiner for **oppdatering** av utstyr og systemer
- gode rutiner for **sikkerhetskopiering (backup)**
- **søppelpostfilter** for din e-post
- **antivirusprogram for din PC**
- Installasjon og oppsett av det som er nevnt over kan være for teknisk for mange, i så fall få hjelp av de du vet kan dette, der er viktig at dette er i orden.

Oppdater maskiner



Programmer og apper til datamaskiner og mobiler kommer stadig i **nye versjoner**. Selvsagt er ny funksjonalitet en del av disse oppdateringene, men **sikkerhetsforbedringer** er et vel så viktig innhold. Når du setter opp din PC/nettbrett/mobil så **svar ja når du får spørsmålet om å få automatiske oppdateringer av produsenten av utstyret**.

Mange er litt engstelige for nye versjoner og oppdateringer ettersom utseende kan endres. Andre tenker at de ikke "trenger alt som er nytt". Dessverre blir man da også sittende med **programmer og apper som inneholder kjente feil**, og som hackere kan utnytte.

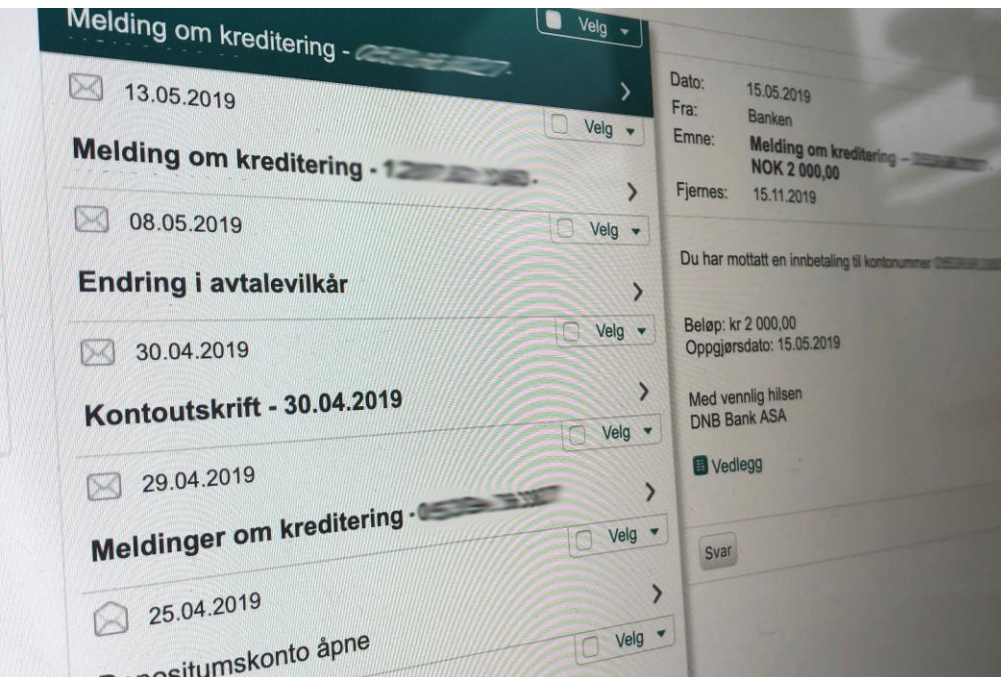
Det er derfor **viktig å holde programvare og apper oppdatert**, så får du **sikkerhetsoppdateringer med på kjøpet!**

A decorative graphic on the right side of the slide features a large, solid green padlock. To its left, several smaller green squares are arranged in a grid-like pattern, with some squares missing, creating a pixelated or mosaic effect. The squares vary in shades of green, from light to dark.

Informasjonssikkerhet for seniorer

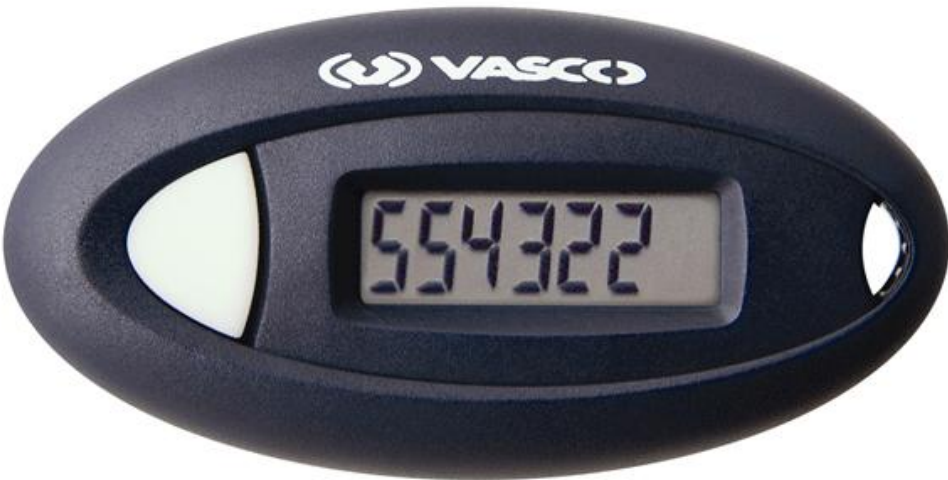
«Banktjenester på nett»

Banktjenester på nett – kommunikasjon med banken



Bankene sender deg derfor sjelden e-post til din private e-postadresse. Om det skjer, så er det for å gi deg beskjed om at du må logge deg inn på nettbanken på vanlig måte for å lese meldinger i din sikre postkasse der.

Det samme gjelder også om du får en tekstmelding (SMS) fra banken. Da vil de be deg om å logge inn på nettbanken på vanlig måte. **Ikke svar direkte på meldingen eller klikk på lenker i meldingen.** Det kan nemlig være svindlere som utgir seg for å være banken.



Banktjenester på nett - BankID

Når du logger deg på nettbanken bruker norske banker en **metode for å være sikker på at du er den du er**, så noen ikke kan gi seg ut for å være deg. Metoden kalles BankID, og du må logge deg på i to trinn.

Det fungerer slik dersom du har en kodebrikke fra banken:

- **Trinn 1:** Du logger deg på med bruker-ID (kontonummer eller personnummer) og passord
- **Trinn 2:** Du taster inn en engangskode fra din kodebrikke.

Informasjonssikkerhet for seniorer

Handle på nett



Betalingskort - Kredittkort

Kredittkort, slik som Mastercard, er faktisk det beste betalingsmiddelet å benytte på nett.

Dersom du blir svindlet eller lurt, og har betalt med et kredittkort, kan du **rette erstatningskravet ditt mot banken i stedet for svindleren**. Så må banken ta dette videre for å forsøke få tilbake pengene.

Det lønner seg å ikke ha **for høy kredittgrense** på kort som benyttes til netthandel. Tilbyr banken det, kan du også be om at du får **varsel på tekstmelding** hver gang det foretas en betaling.

Men pass på: Ulempen med kredittkort er at man fort kan handle for mer penger enn det man kan betale når regningen kommer.



Get it first. Pay later.

Pay later with Klarna.

Klarna.

Betalingsaktører

I tillegg til at nettbutikkene selv kan håndtere betalingen, er det også dukket opp en del **tredjepartsaktører** som butikkene samarbeider med.

De mest kjente av disse er **PayPal** og **Klarna**. Disse forenkler betalingen, og er kjent som trygge aktører.

Kjære ,

10 kunder fra hele landet har blitt valgt ut i vår mest sjenerøse promotering i 2016. **Og du er en av disse 10 utvalgte.**

Vi gir bort 10 x Samsung 55" Smart LED-TV for kun 1 kr*

* Hvorfor ikke gratis? Hvorfor én krone?
Vi tar kun 1 kr for frakt og forsendelse.

De 10 utvalgte heldige kundene er:

BEKREFT NÅ

DanielNilsen2@gmail.com

bekreftet 15 sekunder siden

Oliverlund1@hotmail.com

bekreftet 27 minutter siden

Isabsk2@private.no

bekreftet 42 minutter siden

Williak@sam.com

bekreftet 1 time 40 minutter siden

Nilshåkan0@hotmail.com

bekreftet 2 timer 08 minutter siden

Amandagirl2@gmail.com

bekreftet 3 timer 34 minutter siden

Hedi213453@norge.no

bekreftet 4 timer 15 minutter siden

Ikke bekreftet



00:58:55

FÅ DIN SAMSUNG TV NÅ

DETTE ER ELKJØP

Du visste kanskje at Elkjøp av Nordens største elektronikkforhandlere. Visste du at vi har vedtekter som sier at vi skal ha det gøy på jobb? At vi har egen skole? At lageret vårt har egen toglinje? Elektronikkeventyret startet i Norge med 33 handlere i 1962, og teller nå 10 000 engasjerte mennesker i Norden.

JOBB OG KARRIERE

"Vi skal ha det gøy", sier vår kulturplakat. Og det har vi! Hverdagen som elkjøper byr på sterk bedriftskultur, stor innsatsvilje og hardt arbeid. Vi er opptatt av å ta vare på hverandre som kolleger og dyrke talentene våre. Vi har en egen skole og bruker rundt 50 millioner kroner på opplæring årlig.

VI ELSKER TEKNOLOGI!

Elkjøpere er nok over gjennomsnittlig interesserte i teknologi. Vi har tusenvis av produkter i butikkene våre, egne messer, opplæring med de store leverandørene,

Svindelbutikker

Når du får e-post eller tekstmelding fra tilsynelatende kjente butikker, kan disse være **forfalsket**. Linker vil derfor kunne føre deg til **svindelbutikker**.

Sjekk derfor alltid at nettadressen er korrekt. For eksempel er **www.elkjop.no** korrekt, mens **www.butikk-elkjop.no** ikke tilhører Elkjøp, og kunne dermed vært en falsk nettside.

Sikrest er du dersom du alltid **selv taster inn nettadressen** til nettbutikker du ønsker å handle i.

nikebutikks

 All  Images  Maps  Videos  News  More  St

Page 2 of about 137 results (0.24 seconds)

Forbrukertilsynet advarer: Ikke bestill noe fra disse falske ... - On
<https://www.onlinenytt.com/forbrukertilsynet-advarer-ikke-bestill-n...> ▼ [Translate this page](#)
nikebutikks.com. nikefreerun.cc. nikefreerunnorge.com. nikefreerunsko.eu. nikefreesko.r
nikegono.com. nikeigo.com. nikemax.cf. nikenorge.com. nikeskomall.

www.nikebutikks.com: Nike Free kjøre online salg fra Norge Air r
<archive.is/www.nikebutikks.com> - [Translate this page](#)
Aug 8, 2015 - www.nikebutikks.com: Beste stedet å kjøpe Billige Nike Running sko onlin
høy kvalitet Nike Free Run sko på salg.

Forbrukertilsynets falske nettbutikker
<https://datawrapper.dwcdn.net/vFh0O/2/> ▼ [Translate this page](#)
1, adamaruiz.org. 2, adidasenergyboost.com. 3, adidasko.com. 4, adidasoutletnorge.com.
adidasoutletnorway.eu. 6, adidassuperstarnorge.com. 7, afshirtsno.

hmkshop rabattkoder - Få rabattkode hos rabattkoderogkuponge
<https://rabattkoderogkuponger.info/.../rabattkode-hmkshop.html> ▼ [Translate this page](#)
... klimashop ≡ bbs ≡ multiplication ≡ bigdipper ≡ vidcomshop ≡ skiens antikvariat ≡ r
nikebutikks ≡ mc butikken ≡ gluxe ≡ barnashus ≡ notatboken ...

Falske nettbutikker - Numedalsnett
www.numedal.net/default.aspx?ArticleID=119001&MenuID... ▼ [Translate this page](#)
Jul 20, 2015 - nikebutikks.com. nikefreerun.cc. nikefreerunnorge.com. nikefreerunsko.eu
nikegono.com. nikeigo.com. nikenorge.com. nikeskomall.com.

Pass på når du handler på nett - Supernytt - NRK Super
twens.no/link.php?id=2375 - [Translate this page](#)
nikebutikks.com. nikefreerunnorge.com. P. parajumperjakke.net. parajumperjakkerno.coi
parajumpersoutlet.no. R. rabattprissko.com. S. sko-norgebutikk.com.

Avsløre svindelbutikker

Mer aktivt kan det være lurt å **ta kontakt med nettbutikken** med spørsmål om produkter. Gode og raske svar er et godt tegn.

Du bør også **søke opp bedriftsnavnet** i en søkemotor slik som Google, og lese omtaler av bedriften.

Pass også på å **ikke tillegge omtaler på sidene til selve nettbutikken særlig stor vekt**. Disse er lett å skrive selv. At ulike personer tilsynelatende anbefaler butikken og produktene er lite til hjelp dersom det er falsk informasjon.

HTTPS



Når man handler på nett er det viktig å **kontrollere at nettadressen starter med https://** og ikke bare http://. De fleste nettlesere indikerer også dette med et hengelåssymbol.

Den ekstra s-en forteller oss at informasjon vi oppgir (betalingskortinformasjon, navn, kontaktinformasjon osv.) **sendes kryptert** til mottakeren, slik at den ikke kan avlyttes.

Pass også på at du fortsatt er på en HTTPS-side når du utfører selve betalingen.

HTTPS



Det er imidlertid svært viktig å huske på at HTTPS ikke sier noe om nettsiden vi besøker. Det kan fortsatt være svindlere som opererer denne. Det kan også være at nettbutikken er dårlig drevet.

HTTPS er altså **ingen "godkjenningsordning"** for nettsiden, slik mange tror.



Råd for når uhellet først er skjedd

- Ring banken eller kredittkortselskapet med en gang dersom du mistenker at du er blitt utsatt for svindel.
- Sperr bankkortet slik at det ikke kan benyttes mer av svindleren.
- Har du handlet i utlandet kontakt forbrukerrådet.
- Svindel skal meldes politiet.



Informasjonssikkerhet for seniorer «Offentlige tjenester»

Skatt

Spesielt i tiden rundt skatteoppgjøret er det mye svindler. E-poster som forteller deg at du får penger igjen på skatten gjør de fleste så oppglødde at de uten å tenke spesielt kritisk klikker videre på linker.



Igjen er det viktig å huske på at denne typen informasjon kun kommer i de offentlige kommunikasjonskanalene (Altinn).



Altinn

Mye av informasjon og samhandling med det offentlige gjøres gjennom portalen **Altinn**. Dette er en **sikker portal** både for å motta brev, men også for å sende inn skjemaer og meldinger.

Blant annet vil alt som har med skattemeldingen (tidligere selvangivelsen) og skatteoppgjøret finnes i Altinn.

Det er viktig å huske på at det offentlige vil bruke slike kanaler for all digital kommunikasjon. I tillegg til Altinn er de digitale postkassene **Digipost** og **E-boks** mye brukt.



Informasjonssikkerhet for seniorer «Tabubelagt nettsurfing»



Tabubelagt nettsurfing

Internett gir mange nye aspekter og muligheter. Også informasjon og tilgang til tjenester vi blir litt bluferdige av, og som vi i første omgang ikke innrømmer å bruke. Vi tenker da på **datingsider, annonsering vedr. intimitet, porno etc.** Alt dette er noe tabubelagt, men enkelt å gå inn på, det er noen klikk unna. Når vi er inne på disse tjenestene blir vi lett **emosjonelle** og dermed også **lett lurt**.



Datingsider - falske nettsider

En type svindel vedr. dating er at det opprettes falske nettsider. Dette er nettsider som tilsynelatende er opprettet for å gi deg et håp om at her kan du treffe en livsledsager, men i realiteten er den opprettet for å få deg som medlem ved at **du oppretter en profil og betaler** en innmelding via kredittkortet ditt.

Når du under tiden kommer til at siden er tull og tøys eller at du ikke finner noen interessante personer der, og vil melde deg ut, kan det ofte være **problemer med å melde seg ut**. Medlemskapet ruller videre **uten din vilje** også med nye trekk i kredittkortet.

Informasjonssikkerhet for seniorer

«ID-tyveri»





Hva er ID-tyveri?

Identitetstyveri oppstår når noen skaffer seg personlig informasjon om andre på en uautorisert måte, og bruker denne informasjonen ved å **utgi seg for denne personen og begå bedrageri eller annen kriminalitet.**

Identitetssvindel er ervervelse av penger, varer, tjenester og andre fordeler eller unngåelse av økonomiske eller andre forpliktelser ved å **utgi seg for å være en annen ved bruk av falsk identitet.**



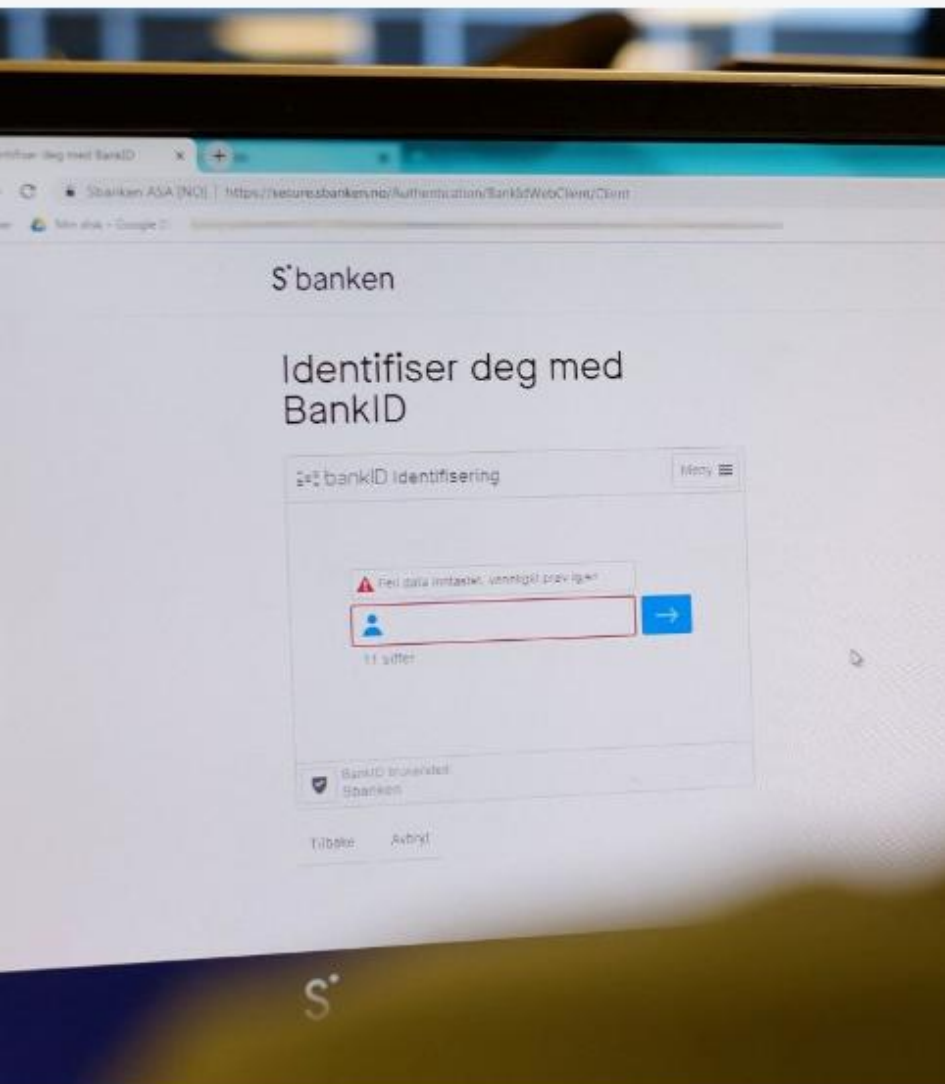
Hvilke opplysninger om deg kan misbrukes?

Personlige opplysninger kan for eksempel være:

- Fødselsnummeret ditt
- Brukernavn du har på internett-tjenester
- Bilder der du er med
- Telefonnummeret ditt
- E-postadressen din
- Bolig- og hjemmeadressen din
- Passord og pinkoder

Dette er eksempler på informasjon som kan knyttes til deg som person som kan bli misbrukt for å identifisere seg som deg.

kan koste deg dy



Forebygging – Tekniske tiltak forts...

- Er du på reise så **skru av trådløst nettverk** når du ikke bruker det.
- I alle moderne mobiltelefoner er det mulighet for tjenester som lar deg **spore mobilen eller nettbrettet ditt om det blir borte**, og også **mulighet for fjernsletting**. Dersom du skal ut å reise kan det være lurt å sette seg inn i disse tjenestene i forkant.
- Ikke last ned apper **ukritisk**. Det finnes falske virusapper gjemt blant de ekte i appbutikken.
- Bruk mobilen din som om det var et **bankkort**. Ikke gi den bort og ikke fortell PIN-koden eller passord til noen.

Ikke la deg lure av svindlere som prøver å få tak i informasjon.

[Sjekk Forbrukertilsynet](#)

[Sjekk Nettvett.no](#)



Jeg er blitt utsatt for ID-tyveri

Ta kontakt med banken. Gi de informasjon om hva som er skjedd og **spør hva som er best å gjøre.** Sperr gjerne bank konto, men da kan du få problemer med andre betalinger mot denne kontoen, banken vet best hva du skal gjøre.

Sørg for å påpeke urettmessige transaksjoner.

Be om frivillig sperring av kreditt sjekk hos kredittopplysningsbyråene. Bisnode har [en elektronisk løsning](#), det samme har [Experian](#) (krever innlogging).

- De fleste som yter kreditt vil verifisere din kredittverdighet hos disse selskapene. En telefon/epost til disse vil kunne verne deg mot ytterligere skade.
- Det er viktig å se på et eventuelt gjenpartsbrief som sendes deg hvem som ber om kredittvurdering. Inkassobyråer vil få innsyn selv om du har satt på frivillig sperring av kreditt, da vil du også få gjenpartsbrief i posten.



Informasjonssikkerhet for seniorer

«Vanlige svindler»

Facebook-konkurranser

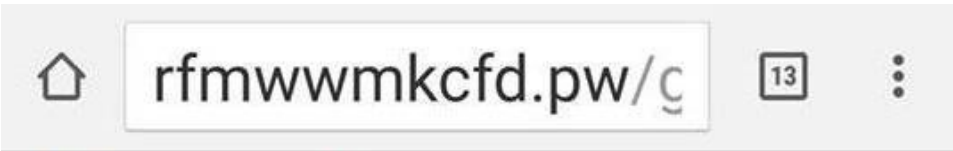
For å unngå denne typen svindler er det enkleste rådet:
Aldri delta i konkurranser på nett.

Dette er selvsagt ikke alle enige i, men det er
overraskende mye svindler knyttet til konkurranser.

Du bør i hvert fall sjekke Facebook-siden som arrangerer konkurransen nøye. **Hvor mange følgere** har den? **Når ble den opprettet?** **Hvilke andre innlegg** har den? Det er lite sannsynlig at et stort firma nylig har opprettet sin Facebook-side og kun har et par hundre følgere.

Sist men ikke minst: Når du ser venner og bekjente deltar, ikke stol på at de har gjort en grundig nok kontroll.
Gjør kontrollen selv.





Systemet er sterkt skadet av fire virus!

At vi oppdage din Samsung Galaxy S5 er 28,1% SKADET oven grunn av skadelige virus fra nyere voksne nettsteder. Snart vil det skade telefonens SIM-kort og vil ødelegge din kontakter, bilder, data, programmer, etc.



Hvis du ikke fjerner viruset nå, vil det forårsaker alvorlig skade på telefonen. Her er hva du trenger å gjøre (trinn for trinn):

Advarsler om feil på datamaskinen

Det er ikke rart man blir engstelig dersom det plutselig dukker opp **advarsler om alvorlige feil** på datamaskin eller mobiltelefon.

Dessverre er dette en teknikk mange svindlere benytter for å få din oppmerksomhet. Enten for å lure deg til å **betale for produkter og tjenester** du egentlig ikke trenger, **ringe dyre spesialnummer** eller laste ned **skadelig programvare** (virus).

SAMSUNG GALAXY

Få en Samsung Galaxy Tab S + S6 Edge for bare 41 kr inkl. 7 dagers strømming av film og serier hos THRILLERSTREAM.COM

TOTAL 41 KR.

Vi aksepterer:
VISA VISA Electron Mastercard

Kortnr.

Utløpsdato:

Kontrollsfre:
 [HJELP](#)

KJØP NÅ

Tab S
Kapasitiv touchscreen
Android OS, v4.4.2 (KitKat)
2 Kameraer

S6 edge
Super AMOLED-skjerm
Trådløs lading
Raskt 16MP kamera

Gevinster

Det finnes et utall ulike versjoner av svindler der du blir kontaktet som **vinneren i en konkurranse**. I andre tilfeller inviteres du til en konkurranse, der du etter noen få enkle spørsmål blir "vinneren".

Nettsidene ser **profesjonelle** ut, og gleden er selvsagt stor når man tilsynelatende vinner dyre fine premier. Når sidene så spør om **leveringsadresse** og deretter krever at du **betaler småpenger for frakt**, legger mange også inn sitt **betalingskort**.

Og det er her svindelen finner sted. Med liten skrift står det nemlig at du ikke er en vinner, men har **muligheten til å vinne**. Samtidig står det at du **tegner deg til et dyrt månedlig abonnement** på en digital tjeneste som typisk koster 799 kr/mnd.

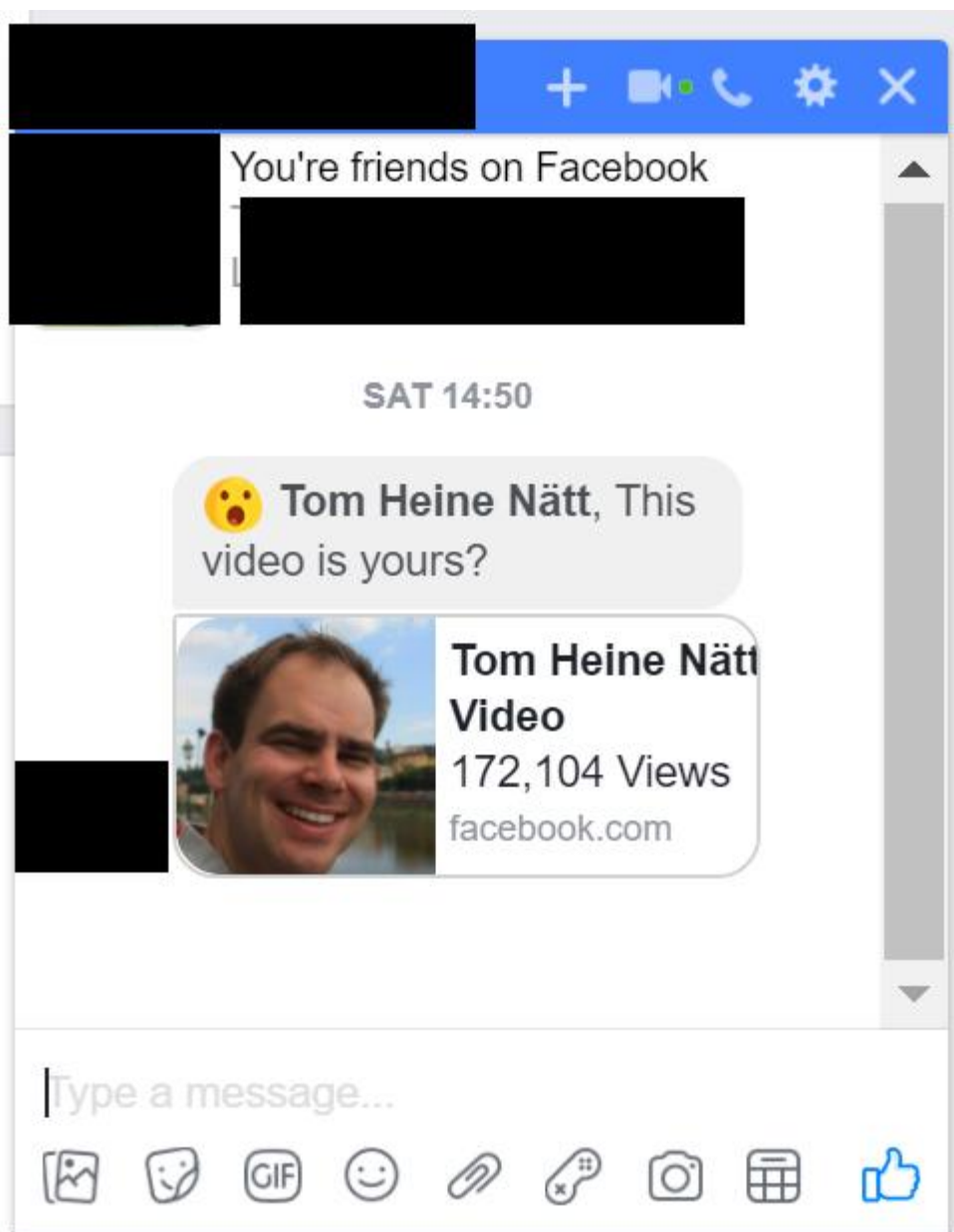


Telefonsvindel

Typisk for disse telefonnumrene er at de er 9- eller 10-sifret. Noen ganger starter de med +47, men på grunn av nummerlengden er det ikke et norsk nummer.

Generelt vil rådet være å **ikke ringe tilbake** til utenlandske nummer du ikke kjenner.

Om du uheldigvis skulle ringe tilbake til slike nummer vil de som svarer forsøke dra ut samtalens lengde med mye **forvirring og spørsmål**. Dette er også et tegn på denne svindelen.



Kontokapring

Spesielt Facebook er utsatt for en mengde forsøk på **kontokapring**.

Det starter med at du får en spennende melding fra en av dine kontakter. Klikker du på meldingen kommer du til en **falsk innloggingsside** for Facebook. Og dersom du forsøker logger inn på denne, **stjeler bakkmennene passordet ditt**.

I sin tur benytter de din Facebook-konto til å **svindle dine kontakter** i ditt navn.

Noen ganger en kontroll over Facebook-kontoen det de ønsker seg. Andre ganger håper de at det samme passordet også skal være brukt i andre tjenester.

Og til slutt...



Selv om vi her kun har presentert noen få svindler, har de forhåpentligvis gitt deg noen hint om hva det kan være lurt å se etter.

Vi gjentar igjen fra innledningen at du bør være spesielt skeptisk til alt som har følgende tema å gjøre:

- Lån eller investeringsmuligheter
- Jobbmuligheter
- Dating
- Helse og helsekost
- Donasjoner
- PC-problemer
- Utpressing
- Konkurranser



Informasjonssikkerhet for seniorer

Gode råd - holdninger

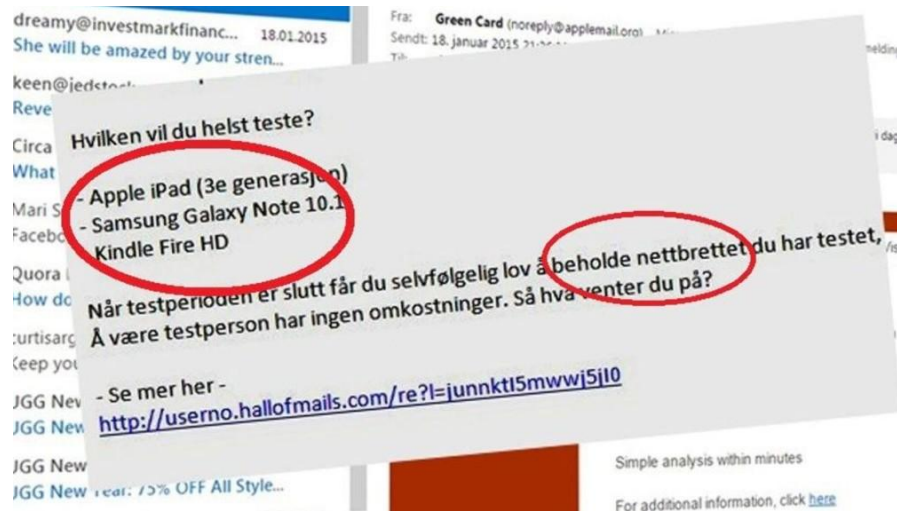
Er det for godt til å være sant, så....

Svært mange svindler burde vært enkle å avsløre basert på frasen "er det for godt til å være sant, så er det nok det".

Unormalt gode tilbud på produkter, **uoppfordret kontakt** fra potensielle fremtidige partnere eller svært gunstige muligheter for å tjene **kjappe penger**.

Alle disse tingene er **kjennetegn på svindler**, men samtidig noe vi svært gjerne ønsket var sant. Derfor overbeviser vi oss ofte selv om at det er det, selv om alle alarmklokker burde ringe.

Vær derfor **ekstra skeptisk** til det som har med disse tre temaene å gjøre. En svært stor andel er nemlig svindel.





Ikke la følelsene styre

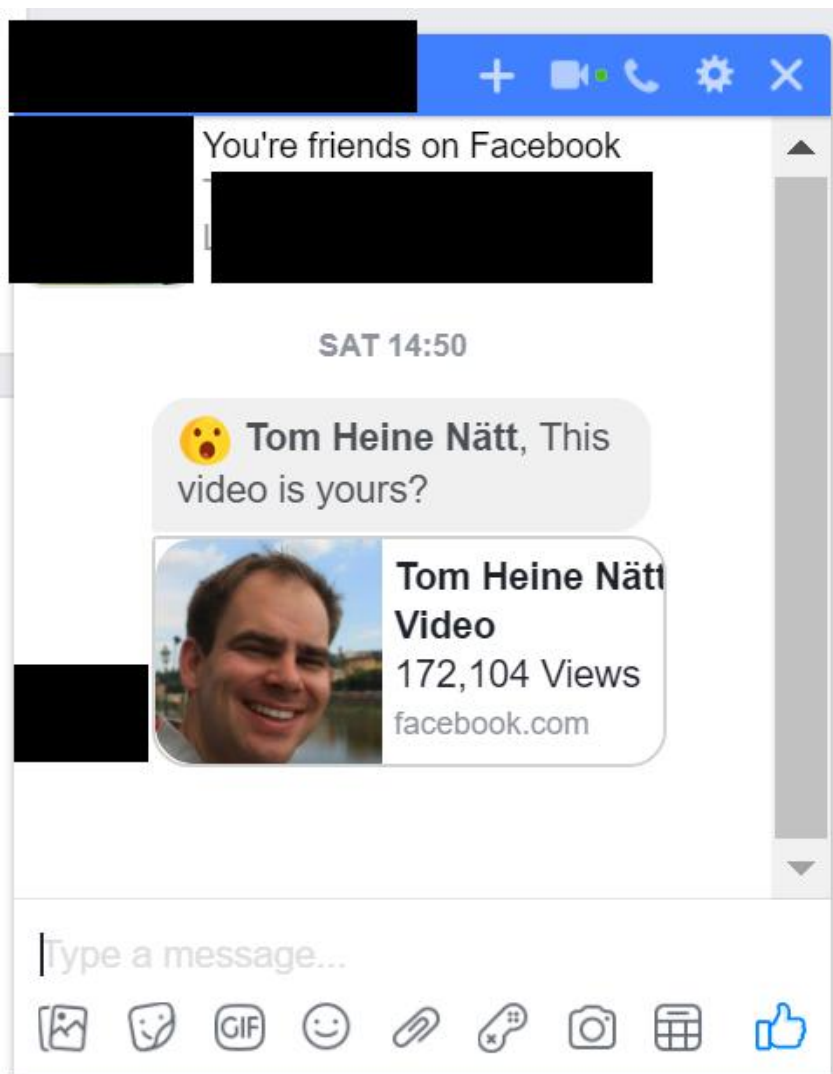
Vi **styres av følelser** i langt større grad enn vi selv vil innse. De fleste valg vi tar er ikke nøye overveide og rasjonelle, men derimot ganske hurtig tatt basert på en **magefølelse**.

Denne magesfølelsen fungerer som regel godt. Unntatt når noen bevisst **misbruker følelsene våre til svindel**.

På nett bør du derfor alltid bli litt **ekstra skeptisk** når du føler stor lykke, nysgjerrighet, tillit, frykt og lignende.

For å sikre rasjonelle avgjørelser er det viktig å la slike ting ligge litt før vi gjør noe med de. Magesfølelsen er nemlig **mest aktiv i de raske beslutningene**.

Ingenting haster så mye at det må ordnes med en gang. Får du inntrykk av at noe går galt eller at du går glipp av noe dersom du ikke handler snarest, er sannsynligheten for at det er en svindel høy.



Ikke stol på kjente

Ikke stol på kjente! Dette kan jo høres ut som en dårlig holdning. Selvsagt skal vi ikke være skeptiske til alle vi kjenner.

Men det er to faktorer vi alltid bør ta høyde for på nett:

1. Det er enkelt for svindlere å **utgi seg for å være personer du kjenner** via e-post, SMS, Facebook osv. Vi bør derfor alltid dobbeltsjekke rare og litt uvanlige meldinger.
2. Vi kan ikke ta for gitt at kjente som deler linker, konkurranser, nyheter, tjenester, apper osv. har gjort en god nok kontroll av hva de tilsynelatende **går god for**. Vi må derfor **alltid gjøre denne vurderingen selv**.

Informasjonssikkerhet for seniorer

Når uhellet er ute

Har du blitt utsatt for svindel?

Det er viktig at du anmelder forholdet til politiet så fort som mulig. På internett forsvinner spor fort. En god start på etterforskningen kan bety mye for saken din. Du kan ikke anmelde på nett. Kontakt lokalt politi.

Når uhellet er ute

Hvis du blir svindlet på nett må du anmelde det til politiet.

Mange synes det å ta kontakt med politiet er et stort skritt å ta, men din anmeldelse av en faktisk svindel hjelper ikke bare deg i å få mulighet til å få refundert tapte verdier, men det gir politiet informasjon om din sak og om metoder svindlere bruker på nett. Det er viktig at du kan gi en så detaljert beskrivelse som mulig.



Når uhellet er ute - økonomisk tap

Dersom svindel på nett fører til at f.eks. kontoen din tappes for penger, eller at du betaler for en vare du ikke har mottatt, er det viktig at **du kontakter banken din så fort som mulig.**

Du vil få råd fra banken om hva du skal gjøre, det kan også være at du har en sjanse til å få refundert noe. Banken kan også hjelpe deg med å sperre betalingskort eller BankID for å hindre mer misbruk.

Følg nøye med på transaksjoner på kontoen din framover og meld fra til banken om du finner noe unormalt.

Når uhellet er ute - økonomisk tap



Noen forsikringsselskaper har refundering av tap ved nettsvindel i innboforsikringen. **Er du svindlet på nett så sjekk med ditt forsikringsselskap** om dette er dekket i din forsikringsavtale. I prosessen med å rydde opp etter en svindel vil dette hjelpe deg betraktelig.

Mange forsikringsselskaper har også egen forsikring for ID-tyveri.

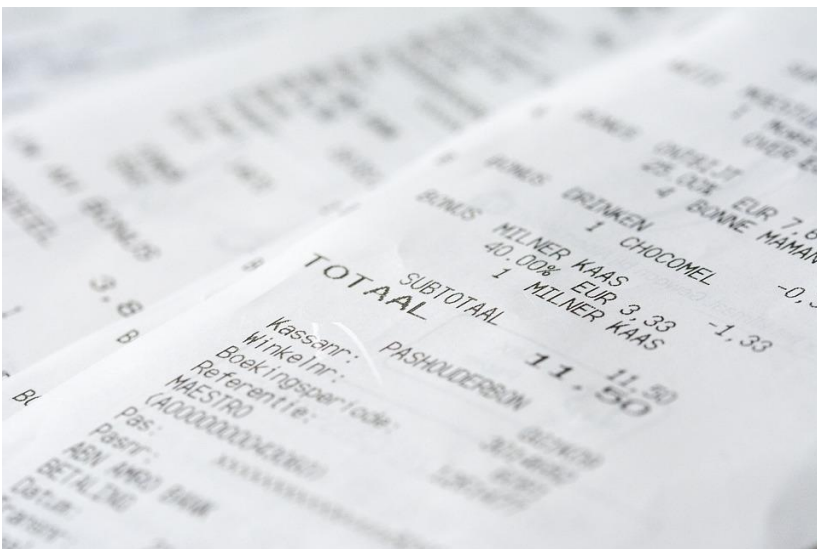


Når uhellet er ute - fjerning av din informasjon på nett

Noen som melder seg inn i nettsamfunn som f.eks. Facebook, eller registrerer seg på tjenester som f.eks. datingsider, kan komme til å angre seg og ville ut av tjenesten, eller ønske å få fjernet informasjon om seg.

I mange tilfeller er ikke dette så lett å gjøre selv. **Prøv først å ta kontakt med tjenesten det gjelder. Er dette vanskelig, ta kontakt med [Slettmeg.no](https://slettmeg.no)** som har veiledninger og kontakter mot nettsamfunn slik at de kan forklare deg hvordan du går frem for å slette.

[Slettmeg.no](https://slettmeg.no) er en gratis tjeneste, med mange års erfaring, og din sak behandles konfidensielt.



Når uhellet er ute - hacket

Hva skal du gjøre om noen har kapret brukerkontoen din på nett, eller du har fått et ondsinnet virus på din PC/nettbrett/Mobil?

Dersom det er snakk om et virus, kan det være vanskelig å fjerne på egenhånd. Da kan du **ta med deg utstyret dit du kjøpte det**, for å få hjelp til å sette det tilbake til fabrikkinnstillinger. Da vil skadelig programvare bli slettet.

Dersom det er snakk om en kapret brukerkonto på nett, kan du få hjelp av [Slettmeg.no](https://slettmeg.no).

Når uhellet er ute - passord ditt er på avveier

Det er svært viktig at **bare du vet passordet** til dine forskjellige tjenester. Har du mistanke om at noen vet det og kan ha brukt din brukerkonto må du gjøre følgende:

1. Hvis du ikke har **totrinnsbekreftelse ved pålogging** **må du legge inn det der det er mulig**. Se hvordan du gjør det for forskjellige tjenester på nettrett.no
2. Hvis tjenesten det gjelder ikke har mulighet for totrinnsbekreftelse må du **endre passordet umiddelbart**. Se hvordan du velger gode passord på nettrett.no

[Her finner du flere tips om sikker pålogging.](#)





Når uhellet er ute - snakk med andre

Når uhellet er ute kan en ofte føle seg dum, føle seg lur, eller tenke “hvordan kunne jeg gå på det som jeg egentlig visste om...”

Men alle kan gå på en utspekulert svindel, og det er viktig å ikke stå alene når i en vanskelig tid.

Selv om det er en terskel å fortelle dette til andre, kan det likevel være en fordel å **benytte seg av sitt nettverk** for bistand. [Seniornett](#) er et eksempel på mange seniorer som sitter med bred erfaring og som kan være til hjelp.

Tirsdag 28. januar kommer oppfølging; «Populære bedragerier»