

Sikkerhet og Svindel på nett



**Hva bør du vite om Sikkerhet og
Svindel på nett**

3. sept. 2025

AGENDA

- **Mobiltilf/nettbrett – enkle sikkerhetstiltak og råd for å unngå svindel**
- **ID-tyveri. Hva er ID-tyveri, hvordan kan det oppdages og unngås**
- **Nettsvindel, vi skal se på flere typer som Phising, Whaling, Wangiri, Spoofing**
- **Svindel på sosiale medier**
- **Eksempler på svindel-epost**
- **Oppsummering**

I følge Telenor:

- I løpet av 2024 stoppet Telenor til sammen 2,2 milliarder hendelser knyttet til digital kriminalitet, inkludert 2,1 milliarder blokkeringer fra sikkerhetsfiltre, 54,5 millioner svindelforsøk via anrop, og 64,1 millioner svindelforsøk via SMS. I første halvår av 2025 har Telenor stoppet totalt 938 millioner digitale trusler, noe som inkluderer 515 millioner blokkerte nettsider, 24,1 millioner svindel-SMS, og 24,1 millioner svindelanrop.
- Nordmenn ble svindlet for 2 milliarder kr. i 2024, opp med 150 % siste 4 år
- Flesteparten av svindelen er gjort ved at det er klikket på falske linker
- Mye er «kjærlighetssvindel»
- Store mørketall (skam)

SIKKERHET OG SVINDEL PÅ NETT

- Sikkerhet og svindel på nett er et vidt begrep og omfatter mye, vi skal se på noe...
- Svindlerne blir stadig mer avanserte og opptrer på stadig flere områder i vår digitale verden
- Svindlere har blitt mer profesjonelle og er kyniske
- Du kan gjøre mye selv for å minimalisere risikoen for å bli neste offer...
- Mange råd for å unngå svindel er enkle
- Statistikk viser at mange ikke følger slike råd, selv om de kan virke opplagte
- Enkle råd kan sørge for at du unngår økonomiske tap og timevis med "oppryddingsarbeid"
- Sikkerhet og svindel på nett innebærer også at du sikrer dine egne data, det vil si bilder, dokumenter, videoer, musikk, osv.
 - **Svindlere spiller ofte på FRYKT, TILLIT, FRISTELSE OG TID**

Beskytt mobilen



- Mobiltelefon må sikres slik at ikke andre kan misbruke den
- Fire enkle råd:
 - Lås
 - Hold den oppdatert
 - Ha en plan for hva du gjør hvis den blir borte
 - Bruk skytjenester

Lås

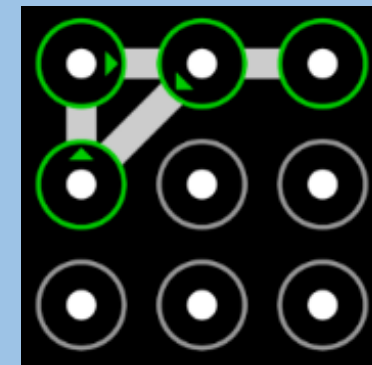
- Mange har ikke lås på mobilen for å slippe det ekstra bryderiet det er å låse den opp hver gang du skal bruke den. Det er en risikabel strategi. Alle kan bli utsatt for svindel. Du kan miste telefonen eller den kan bli stjålet.
 - Det er flere ulike typer låser:
 - Pin-kode (både på tlf. og SIM-kort)
 - Mønster
 - Ansiktsgjenkjenning
 - Fingeravtrykk

Lås

- Det enkleste er ansiktsgjenkjenning. Da behøver du bare å se på mobilen, så låser den seg opp
- For fingeravtrykk kan du registrere flere fingre, slik at den også kan brukes hvis du har fått et sår på fingeren
- Vil du ha ansiktsgjenkjenning eller fingeravtrykk må du også ha en pin-kode

Lås

- Mønster betyr at du, i en ramme med 9 prikker, skal tegne et mønster (gjelde Android)
- Du velger altså et mønster som du klarer å huske, du holder en finger nede på skjermen mens du tegner mønsteret



Hold nettbrett og tlf. oppdatert

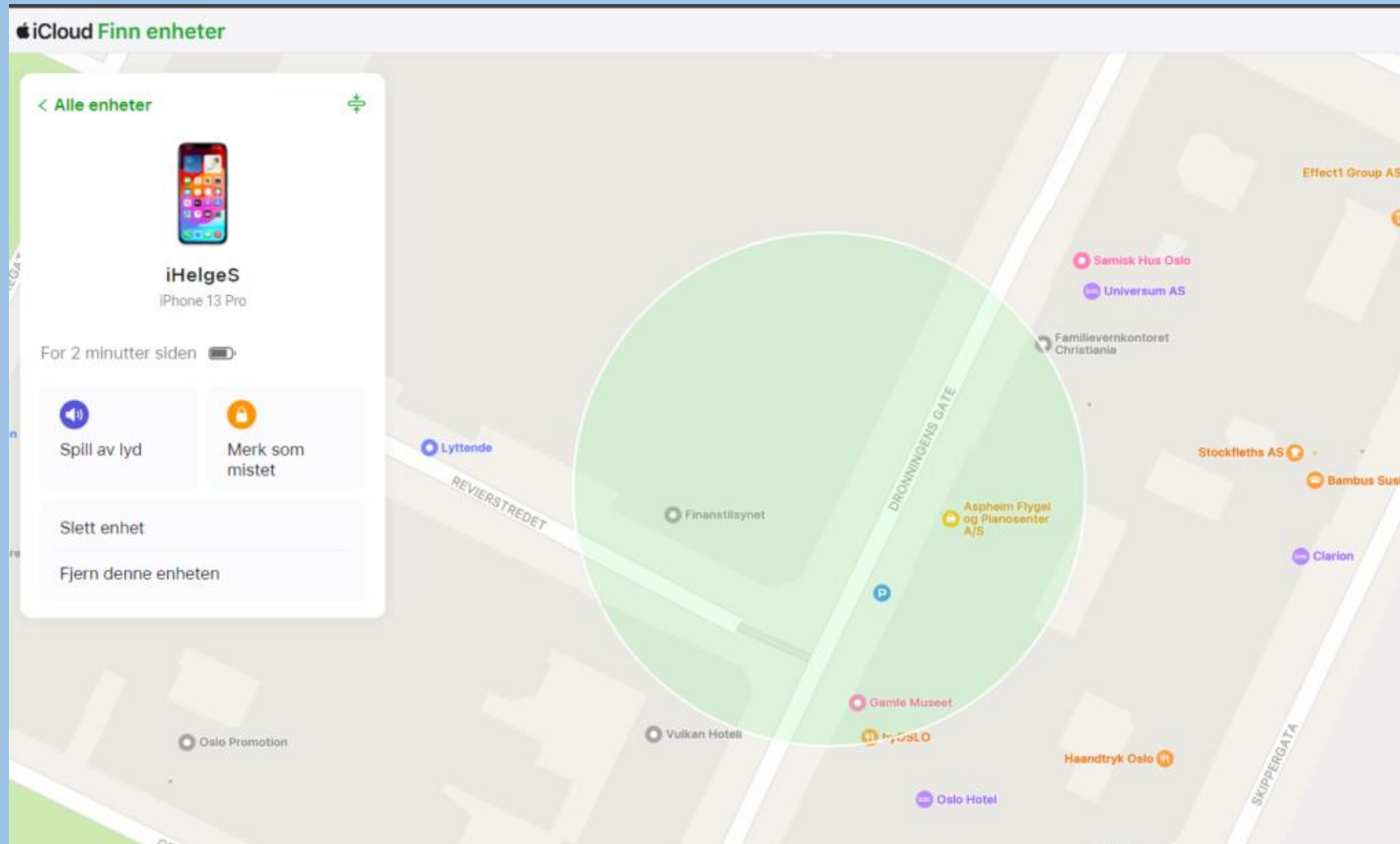
- Det å holde nettbrett og tlf. oppdatert, dvs. både system/programvareoppdateringer, og oppdatering av de apper du bruker, er en av de beste sikkerhetstiltak du kan gjøre selv
- I hver oppdatering ligger det sikkerhetsoppdateringer, det vil si funksjoner som skal unngå at nettbrett og tlf. blir «infisert» av skadelig programvare (gjelder også PC)
- Kan også bidra til bedre ytelse – lavere batteriforbruk

Ha en plan for hva du gjør dersom mobiltlf. blir stjålet eller mistet - sporing

- Undersøk på forhånd hvordan du sporer din mobil
- Dersom den er på og er koblet til internett, kan du fra en annen enhet/PC se hvor mobilen din er
- For android-telefon gjør du dette ved å gå inn på:
- <https://www.google.com/android/find>
- For iPhone logger du deg inn på iCloud og går inn på:
<https://www.icloud.com/find/> («Finn enhet» må være slått på)

Ved sporing

- **Man ser hvor telefonen er i kart, og det er 3 ulike ting man kan gjøre:**
- **Spill av lyd:** Da vil telefonen «ule» i 5 minutter
- **Beskytt enheten:** Da blir den låst og avlogget slik at andre ikke kan bruke den
- **Tøm enheten:** Da fjernes alt på telefonen og den tilbakestilles til fabrikkinnstillinger (kan ikke reinstallerer uten apple-id passord)
- **Dersom du har slått av mobildata vil ikke dette virke. Derfor er det lurt å alltid ha mobiltilf. påslått**



Skytjenester

- Hva er Skytjenester?



Benytt skytjenester

- Er skytjenester trygt?
- Det er enkelt å ta mange bilder. Men det er risikabelt å kun lagre dem på telefonen
- Du kan miste telefonen, eller noe kan gå i stykker slik at den ikke lenger virker. Da er det veldig dumt å miste bildene dine
- Hvis du bruker skytjeneste på bildene så vil de automatisk bli lagret «i skyen». Da kan du også se dem fra andre enheter (f.eks. på PC eller nettbrett)
- Hvis du har aktivert en skytjeneste på din mobil og du bytter mobil, så vil alt fra den gamle telefonen automatisk bli overført til den nye tlf.

ID-tyveri



Definisjon av ID-tyveri:

«uberettiget bruk av både stjålet og fiktiv identitet, med forsett å oppnå en økonomisk vinning for seg selv eller andre, eller å påføre tap eller ulempe for andre»

Poenget her er at noen er ute etter dine (sensitive) opplysninger for at de skal utgi seg for å være deg

Flere ulike måter å bli svindlet på ved ID-tyveri

- **Netthandel:** En falsk nettbutikk. Du «kjøper» noe der, men de har ingen varer. Du oppgir kredittkortnummer når du «betaler»
- **Sosiale medier:** Noen har opprettet en falsk profil og sender melding til dine «venner» og ber dem om å bli med på noe som gir økonomisk gevinst. Den som mottar, tror det er fra deg og går på limpinnen
- **Oppgi personopplysninger i telefon:** Det ringer en person fra feks. «politiet» som sier han skal stoppe noen som holder på å stjele penger fra din konto. Han ber deg oppgi fødselsnr. og bankid-koder. Han er selvfølgelig ikke fra politiet (selv om telefonnr. du ser tilsynelatende er fra politiet)
- Haster alltid

- **Papirer på avveie:** Papirer med sensitive opplysninger bør makuleres eller brennes (påloggingsinfo, PIN/PUK-koder etc.)
- **Falske linker:** Dette er kanskje den vanligste årsaken til å bli utsatt for ID-tyveri. Du får en epost som frister med penger eller lykke. Du skal bare trykke på en link og fylle ut et skjema, og ID-tyveriet er i gang...

Hvordan forhindre at du blir rammet av id-tyveri

- Aldri oppgi sensitive data i telefon fra bedrifter eller offentlige etater
- Ingen seriøse organisasjoner vil spørre om dette
- De mest avanserte svindlere opptrer som om de er seriøse aktører
- Er det en melding som inneholder en link («trykk her») så er det sannsynligvis svindlere
- Får du en melding på sosiale medier som tilsynelatende er fra en du kjenner, så skal du heller ikke oppgi noen kode

Symptomer på at du er rammet av id-tyveri

- Du mottar regninger for produkter du ikke har bestilt eller ikke kjenner til
- Du oppdager ukjente transaksjoner eller kjøp på kredittkortregningen din
- Du mottar bekreftelse på kreditt eller endring av kredittrammen din uten at du har spurt om dette
- Du får varsel fra posten eller andre om at adresseendring er mottatt
- Du blir kontaktet på telefon eller brev om kjøp du ikke har gjort eller kjenner til
- Du mottar gjenpartsbrev etter *kredittsjekk* uten å forstå hvorfor
- Du mottar post du ikke forstår hvorfor du får, for eksempel en faktura, et avtaleforslag eller hentemelding for noe du ikke har bestilt

Nettsvindel

- Svindel er et forsøk på å lure noen til å gi bort informasjon eller gjøre en handling som fører til tap av penger
- Svindel og bedrageri har eksistert i alle år. Men i den moderne tid har gjerne svindelmetodene gått over til å bli digitale, ved bruk av stadig mer avanserte teknologiske metoder
- Ved å kunne gjenkjenne de forskjellige metoder, ved å bruke sunn fornuft og ved å «holde hodet kaldt» kan man være bedre forberedt for å unngå svindel

Nettsvindel

Det er 3 hovedmetoder du kan bli svindlet på:

- **Frykt**: Du har mange trusler på din maskin, eller du må gjøre noe veldig raskt (du må gjøre noe NÅ, ellers er det for sent) Hva gjør du? Stopp opp – ta det med ro – ta deg tid til å tenke deg om
- **Tillit**: Du får melding fra en du kjenner som ber deg om å gjøre noe. Men er det naturlig at du får denne meldingen? Ber den deg om å gjøre noe uventet? Er det virkelig en du kjenner som har sendt deg denne meldingen?
- **Fristelse**: Eksempel «Du er den heldig vinner av» - Hva gjør du? Slett meldingen uten å gjøre noe mer med den. Du vinner nemlig ingenting

Phishing

- Dette er den mest brukte form for svindel. Phishing er det engelsk ord for «fiske». Dette er en form for internettbedrageri, som er basert på å «fiske ut» personlig informasjon fra den som skal svindles
- Det kommer som regel i form av en e-post, en SMS eller et telefonanrop. Disse e-poster eller SMS-er inneholder da ofte et falskt vedlegg eller lenke
- Lenken fører til nettsiden som tilsynelatende er nettsiden til en pålitelig bank eller nettbutikk, men som er en falsk nettside
- Det handler ofte om at du har vunnet noe eller at du for eksempel kan løse et problem med bankkontoen din

Whaling

- Eksempel: en såkalt bekjent kontakter deg i form av en e-post, en SMS eller en melding på Messenger fordi han eller hun er i nød og ikke lenger har tilgang til pengene sine
- Typisk at den såkalt bekjente er på ferie i utlandet og har blitt frastjålet både bankkort og pass
- Han/hun trenger penger for å komme seg tilbake til Norge og ber deg om hjelp. (Dette er såkalte tigge-e-poster eller tigge-meldinger)

Wangiri

- Betyr at det kommer et anrop fra et utenlandsk nummer som ringer kun én gang. (Kan også være skjult nr.) Målet er at du skal ringe tilbake. Du ringer nemlig tilbake til et telefonnummer med veldig høy takst
- Ofte er det en telefonsvarer eller lydfil i enden av det utenlandske høytakst-nummeret som skal holde samtalen i gang lengst mulig
- Jo lenger du lytter desto større blir telefonregningen din og desto mere tjener svindlerne

Spoofing

- Er en teknikk som gjør at svindlere kan utgi seg for å kontakte deg fra et norsk nummer (eller trygg IP-adresse)
- For å utføre spoofing på telefon bruker svindlerne en programvare som viser et annet nummer enn det originale nummeret de ringer fra
- Dermed kan samtalen se ut som at den kommer fra et norsk nummer, noe som ofte vekker mer tillit enn et utenlandsk nr.x

Facebook, Instagram, Snap, Tik-Tok



Facebook, Instagram, Snap, Tik-Tok

- **Falske venneforespørsler**
- **Kontokapring**
- **Falske profiler**
- **Falske lenker**
- **Falske annonser for varer du aldri mottar**
- **Henvendelser som utgir seg for å være fra Meta**
- **Trusler om å dele bildene dine...**
- **«Lær å bli rik fort...»**

Facebook, Instagram, Snap, Tik-Tok

- **Falske venneforespørsler.** Noen sender deg en venneforesp. i en annens navn. Du får aldri venneforesp. fra en du allerede er venn med
- **Konto-kapring** - svindlere kan kapre en eksisterende Facebook-konto for å sende ut spam, svindelforsøk eller lenker med skadelig programvare til dine kontakter
- **Falske profiler og sponsoravtaler** - svindlere oppretter profiler som ligner på ekte merker eller influencere for å tilby sponsoravtaler eller samarbeid, spesielt rettet mot unge mennesker
- **Falske lenker** – du blir linket til sider som er falske, for eksempel noe som er gratis, billig, fristende osv
- **Falske annonser for varer du aldri mottar**
- **Henvendelser som utgir seg for å være fra Meta**
- **Trusler om å dele bildene din.** Bilder som du ikke vil dele med andre blir et pressmiddel
- **«Lær å bli rik fort...»** En oppskrift på hvordan du kan gjøre store penger på å følge enkle råd..

Enkle råd for å unngå svindel

- Bruk sunn fornuft og ikke foreta deg noe før du har tenkt deg godt om. Ikke la deg lure til å handle for raskt!
- Ikke ring tilbake hvis du ser at et ukjent nummer har ringt deg
- Ikke klikk på lenker du har mottatt fra ukjente nummer eller ukjent avsender
- Slett e-poster og SMS-er som kommer fra totalt ukjente eller som ikke virker legitime

Enkle råd for å unngå svindel

- Ikke last ned apper fra andre steder enn Google Play og App Store
- Oppgi aldri BankID-koden din til noen, selv ikke til politiet. Det er ingen andre enn deg som skal bruke den
- Vær veldig kritisk – husk at ingen profesjonelle aktører spør etter personlige opplysninger
- Vær kritisk til QR-koder, det kan være svindel
- Hvis det plutselig dukker opp en ny app som er ukjent for deg, slett den

Benytt totrinns verifisering



- I tillegg til brukernavn og passord, er det sterkt å anbefale at du bruker en ekstra sikkerhet ved innlogging
- Dette kalles totrinnsverifisering, totrinnsbekreftelse eller tofaktorautentisering
- Det gjør kontoen din sikrere fordi det hindrer andre å logge inn på din konto selv om uvedkommende kjenner til ditt passord

Har du blitt offer av svindel

- Anmeld svindel til politi
- Ta kontakt med banken din
- Ta evt. kontakt med din teleoperatør om du har oppgitt ditt mobilnr. til svindlerne
- Bytt **passordet umiddelbart** dersom du har oppgitt innloggingsdetaljer

Eksempler på svindelforsøk



Frode Alnæs

22. apr. · 🌐

Stadig vekk prøver noen seg i mitt navn... Jeg har kun en artistside på Facebook, og sender aldri ut venneforespørsler eller kommenterer. Slett evt venneforespørsler (og kommentater) og rapporter gjerne slike sider!



Frode Alnæs har sendt deg en venneforespørsel.

3 t

Bekreft

Slett



Frode Alnæs liker ditt bilde: "Pasjon 2025 Stavanger domkirke. Jeg har ..."

3 t



Kontakt@vegvesen kjendli@online.no <foerdeshop8285477-jbfop... 22:39

Til: Per Harald Kjendlie >

Svar til: noreply >

Forny førerkortet ditt NÅ 66292313,-29/05/2025 02:34:32p



Statens vegvesen

Hei, kjendli@online.no

Vivil minne deg om at det er på tide å fornyeførerkortet ditt. Vi vil minne deg om at det er på tide å fornye førerkortet ditt.

For å starte fornyelsesprosessen, vennligst logg inn på vår nettside ved å klikke på knappen nedenfor.

Vennligst fullfør fornyelsen innen fristen for å unngå eventuelle problemer med gyldigheten av ditt førerkort. Har du spørsmål, kan du finne mer informasjon på våre nettsider eller kontakte vårt kundesenter.

[logg inn](#)



SpareBank /Contact

Til: Per Harald Kjendlie >

Contacts



Kjære klient,

Vi beklager å informere deg om at din BankID-tilgang er utløpt. Du vil ikke kunne bruke BankID for noen tjenester med din bank før du aktiverer den igjen.

For å aktivere din BankID-tilgang, klikk på knappen nedenfor og bekreft din sikre enhet.

Oppdater nå

Takk for din oppmerksomhet.

Kundeinformasjon fra deg for ditt SpareBank1

[Åpne i nettleser](#)

Viktig beskjed – Vi mangler informasjon om deg

Hei! Vi viser til tidligere varsel om at vi mangler oppdatert informasjon om deg.

Siste påminnelse: For å unngå at dine kontoer blir sperret må du oppdatere kundeinformasjon innen 17/07/2025

Oppdatering av kundeinformasjon innebærer at du må besvare noen spørsmål knyttet til din bruk av banken. Du kan besvare spørsmålene på én av følgende måter:

[Logg Inn](#)

Hva skjer dersom du ikke oppdaterer kundeinformasjon?

Dersom vi ikke mottar oppdatert kundeinformasjon innen fristen vil ditt kundeforhold i banken bli midlertidig sperret. Så snart vi mottar oppdatert informasjon vil kundeforholdet bli åpnet igjen.

Vi beklager de ulemper dette medfører, men lov om hvitvasking krever at banken skal ha oppdatert informasjon om alle kunder.

NB: Oppdatering av kundeinformasjon må gjennomføres selv om du eventuelt har vært innom banken for å vise legitimasjon tidligere i år.

Hilsen



Skattekortet for 2025 er klart

Du har fått endret skattekort med skattetrekk for 2025.

Vi varsler arbeidsgivere og andre utbetalere om at du har fått nytt skattekort som de skal ta i bruk.

Sjekk skattekortet, så blir det riktig. Arbeidsgiver og andre utbetalere henter skattekortet elektronisk.

[Logg Inn](#)

Hilsen Skatteetaten



Altinn

Til: Per Harald Kjendlie >

20

Contacts

Hei,

Velkommen som Altinn kunde Vi må nå foreta en sikker ID-kontroll av deg. For å gjennomføre identifiseringen trykker du på lenken i denne eposten:

[Logg inn på kontoer](#)

Altinn



Varsel: Mistenkelig aktivitet oppdaget

Kjære Telenor-kunde,

Vi har registrert mulig ondsinnet aktivitet på enheten din som kan påvirke både personvernet og ytelsen.

For din sikkerhet anbefaler vi å installere et verktøy som er testet og anbefalt for å fjerne slike trusler.

Last ned beskyttelse nå

Viktig: Hvis du ikke iverksetter tiltak innen 48 timer, kan vi bli nødt til å midlertidig suspendere kontoen din for å hindre at potensielle trusler sprer seg gjennom e-posten din.

Kontoinformasjon	
Kunde-ID:	TLN-83921-NO
Bruker:	kjendli
Status:	Trussel oppdaget
Siste sjekk:	2025-07-23

Med vennlig hilsen,
Telenor Sikkerhetsteam



VanMoof S3 <info@rpc.pixibeauty.com>

FÅ EN HELT NY VANMOOF S3

I kjendli@online.no

Klikk her for å laste ned bilder. Outlook forhindrer automatisk nedlasting av noen bilder i denne meldingen for å bidra til å verne din private informasjon.

Velg **Internett -tjenesten** Tilbyderne
får sjansen til å **VINNE!**

Helt ny **VanMoof S3**



Du er valgt til å delta i lojalitetsprogrammet vårt – helt **GRATIS!** Det tar bare ett minutt å motta denne fantastiske premien.

SE TILGJENGELIGE PLANER

Elkjop.no <meetic@meetic.com>

Vi feirer jubileet til Elkjop-med-iPhone14-Pro.

wanadoo.fr

oblemer med hvordan denne meldingen vises, kan du klikke her for å vise den i en nettleser.



gratulerer kjendli

Du har blitt valgt til å teste en iPhone 14 Pro for oss, og du kan beholde den GRATIS! Fyll ut informasjonen din så snart som mulig



*******SPAM***** Donation of \$1,500,000.00 USD from the Azim Premji Philanthropies Foundation**

Dear Sir/Ma'am,

We are pleased to inform you that you have been selected to receive a donation of \$1,500,000.00 USD from the Azim Premji Philanthropies Foundation-India. Our foundation, guided by the principles of "giving while living," is committed to making a positive impact in our society.

If this is a valid email address, kindly reply to this message for further details on how to proceed.

Contact E-mail: azimpremjifoyndatiion@gmail.com

For more information about Azim Premji and our philanthropic initiatives, please visit https://en.wikipedia.org/wiki/Azim_Premji

Lyt til hjertets stemme

Det er svært at finde nogen, man kan stole på i disse dage.
Hvad tænker du, hvis vi kan overbevise dig om, at vores fællesskab er præcis, hvad du har brug for?

Vælg mellem over 30.000 profiler af kvinder i dit område og andre lande.
Vores samfund består hovedsageligt af ukrainske kvinder og andre nationaliteter.

Du kan kontakte disse tre skønheder med det samme, tilmeld dig!



Aleksandra 31



Victoria 50



Lilia 35

Registrering er gratis, hurtigt og sikkert.
Stol på vores samfund, vi lover, at du vil være glad for os.

Benyt lejligheden, og hvem ved, måske møder du nogen i dag:

MeetYourLove

Vi bruger et avanceret anti-svigsystem og online shopping systembeskyttet af verdens førende certificeringsorganer - GoDaddy og McAfee.



30000+ Members



Tested and secured



Free Signup

Hvis du ikke længere ønsker at modtage vores tilbud, [afmeld her](#).

Meldingen inneholder bilder som ikke er lastet inn.

[Last inn alle bilder](#)

Meldingen er fra en e-postliste.

[Avslutt abonnement](#)



FlørtPortalen

Til: Per Harald Kjendlie >

Svar til: FlørtPortalen >



Du har fått et frekt bilde... Klar for å se?



Du har fått et nytt bilde!

Et frekt bilde venter på deg... nysgjerrig?

Se bildet

Ikke interessert? [Meld deg av](#)

*******SPAM***** Vi har spart denne invitasjonen kun for deg**

En Invitasjon Kun til Deg

Du har blitt personlig valgt ut til å oppdage noe nytt – noe spennende. Vi lanserer en ny plattform for menn som ønsker å møte ekte, vakre ukrainske kvinner som nå bor i Europa. Hvis du leter etter flørt, moro og kanskje noe mer – dette er din sjanse.

Medlemmene våre er ekte, verifiserte og klare til å chatte. Ingen apper, ingen kompliserte steg – bare et sted hvor ærlige samtaler kan begynne. Det er enkelt å registrere seg: bare brukernavn og e-post. Det er gratis, anonymt og umiddelbart. I en travel verden kan dette være det mest ekte du ser i dag.

[Start din Ukraina Date nå](#)

Møt noen av medlemmene som allerede er online:

Oppsummering

- **Bruk sunn fornuft, ta deg litt ekstra tid til å sjekke**
- Dersom det dukker opp noe du er i det minste tvil om er svindel eller ikke, vil blant annet et raskt søk på nett etter deler av teksten i meldingen kunne avsløre svindelen
- **Er det for godt til å være sant, så er det gjerne det.** Med dette ordtaket vil man i utgangspunktet kunne avsløre mange type svindel
- **Du vinner ikke noe** «*Du kan vinne en gratis iPhone, om du bare svarer på noen spørsmål*». Eller du får en melding eller e-post om at du allerede er trukket ut som vinner av en premie

Oppsummering

Hold alle enheter oppdatert

Oppdatering av alle enheter du bruker er en av de beste sikkerhetstiltak du kan gjøre selv. Oppdateringer tetter hullene i sikkerhetsnettet, som gjør at det er mer sikkert å bruke enheten

- **Bruk totrinns pålogging**
- **Ikke skam deg om du blir svindlet**
- **Vær skeptisk men ikke engstelig**
- **Kommer dette fra den jeg tror det kommer fra?**
- **Ikke si: «det vil aldri skje meg»**
- **Passord er en utfordring – bruk tid på å finne deg gode passordrutiner**

Takk for oppmerksomheten

Håper du har hatt nytte av dette, og bruk gjerne litt tid på å tenke igjennom hva *du* kan forbedre i forhold til:

- *sikkerhet og svindel på nett* -

