

Digital beredskap og trygghet

"Når mobilen blir nøkkelen til alt"





Hvorfor dette er viktig



- Mobilen brukes til bank, helse, kommunikasjon og identifikasjon
- Økende digital avhengighet
- Eldre er særlig utsatt for svindel og tekniske problemer



Sikker bruk av mobilen



- Bruk skjermlås (PIN, mønster, fingeravtrykk)
- Oppdater telefon og apper
- Installer kun apper fra sikre kilder
- Ikke del passord med andre



Vanlige digitale trusler



- Svindeltelefoner og SMS
- Falske lenker og e-poster
- Identitetstyveri
- Tap av mobil eller passord



Gjenkjenne svindel



- Vær skeptisk til uventede henvendelser
- Ikke trykk på ukjente lenker
- Bank, politi og offentlige tjenester ber aldri om passord



Hva gjør du hvis noe skjer?



- Sperr SIM-kort og banktjenester
- Endre passord
- Kontakt familie eller noen du stoler på
- Meld fra til banken eller politiet ved svindel

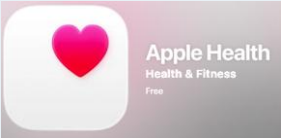
Nyttige verktøy

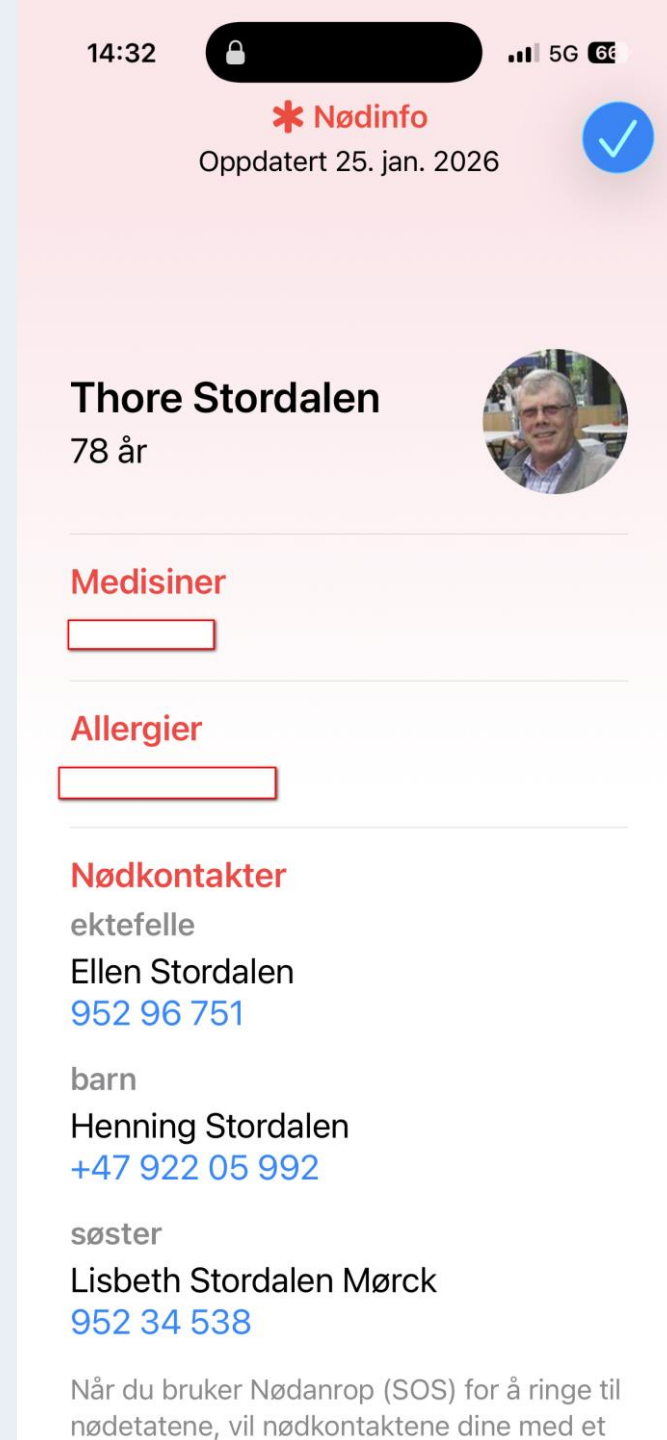
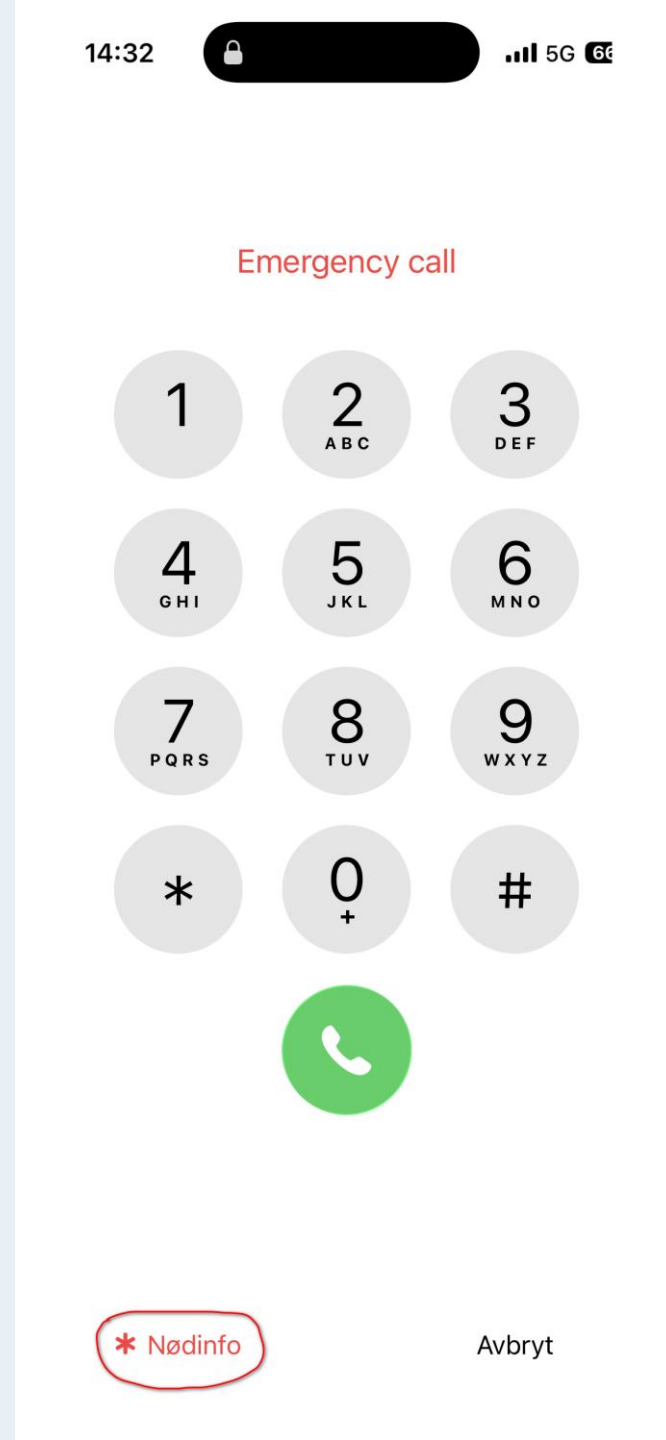
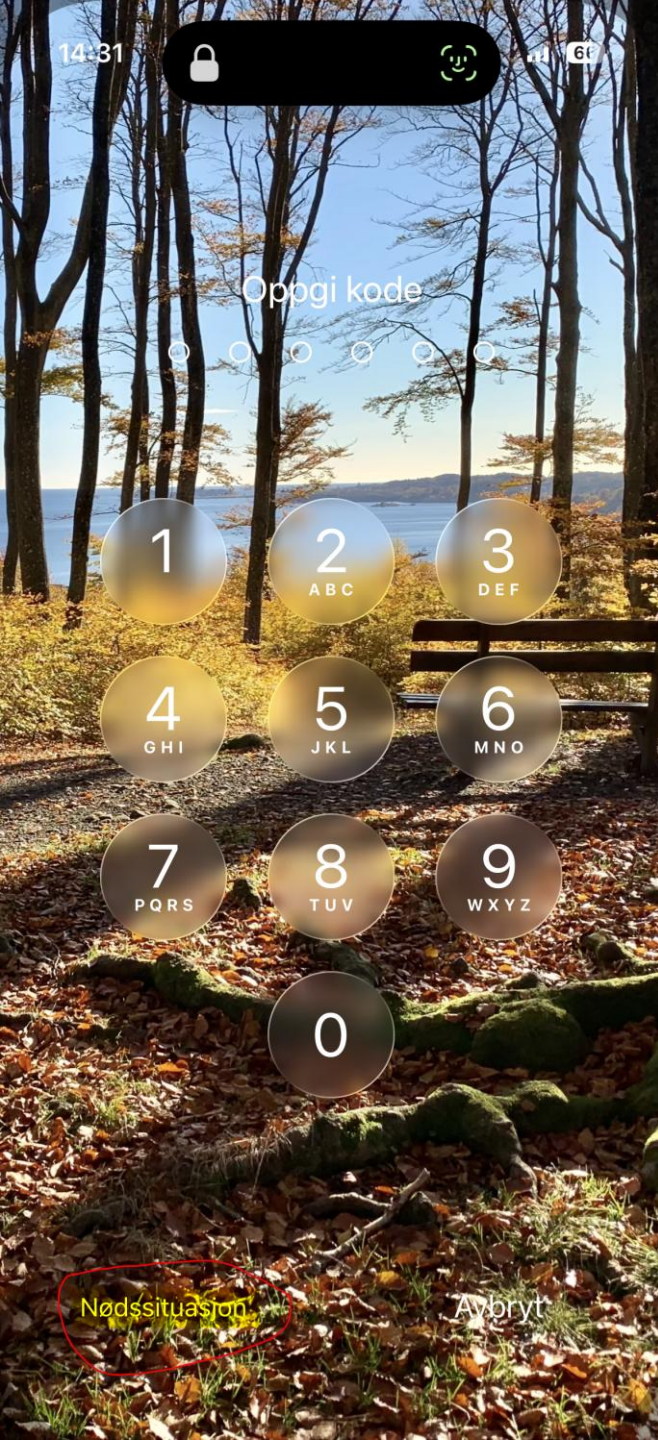
- BankID-app
- Sikkerhetskopi i skyen
- Sporing av tapt mobil
- Nødmodus på mobilen



Hva er nødmodus/nødanrop?



- Nødmodus på mobilen er en sikkerhets-funksjon som raskt lar deg ringe nødetatene (110, 112, 113) og varsle dine forhåndsdefinerte nød-kontakter.
- Du legger inn nød-kontakter i appen «Helse» 
- **iPhone (Nød-SOS): For å ringe:** Trykk og hold sideknappen og en av volumknappene, *eller* trykk sideknappen raskt 5 ganger.
- Telefonen kan dele posisjonen din, sende nød-SMS, eller bruke satellitt (på nyere iPhones) uten at du må låse opp skjermen.
- Eller:



Hva er nødmodus/nødanrop?



- **Samsung/Android:** Gå til Innstillinger > Sikkerhet og nødsituasjoner > Nødanrop SOS for oppsett.
- Telefonen kan dele posisjonen din, sende nød-SMS, eller bruke satellitt (på nyere iPhones) uten at du må låse opp skjermen.



BankID – trygg bruk

- BankID brukes til innlogging, betaling og signering
- Bruk helst BankID-appen
- Ha skjermlås på mobilen
- Ikke godkjenn noe du ikke selv har startet
- BankID skal aldri brukes etter telefon fra "banken"



BankID – vanlige svindelforsøk

- Telefon fra "banken" som ber deg logge inn
- SMS som ber deg oppdatere BankID
- E-post som sier at BankID er sperret
- Svindlere prøver å få deg til å godkjenne noe du ikke forstår



Passord – slik lager du sterke og enkle passord

- Bruk en setning du husker godt
- Ikke bruk samme passord flere steder
- Ikke bruk navn, fødselsdato eller enkle tallrekker
- Bytt passord hvis du mistenker misbruk

Passord – hjelpemidler

- Bruk gjerne en passordhåndterer
- Skriv aldri passord på lapper som ligger fremme
- Ikke del passord med familie – bruk delt tilgang der det finnes



Noen eksempler på svindel





Svindeleksempel 1

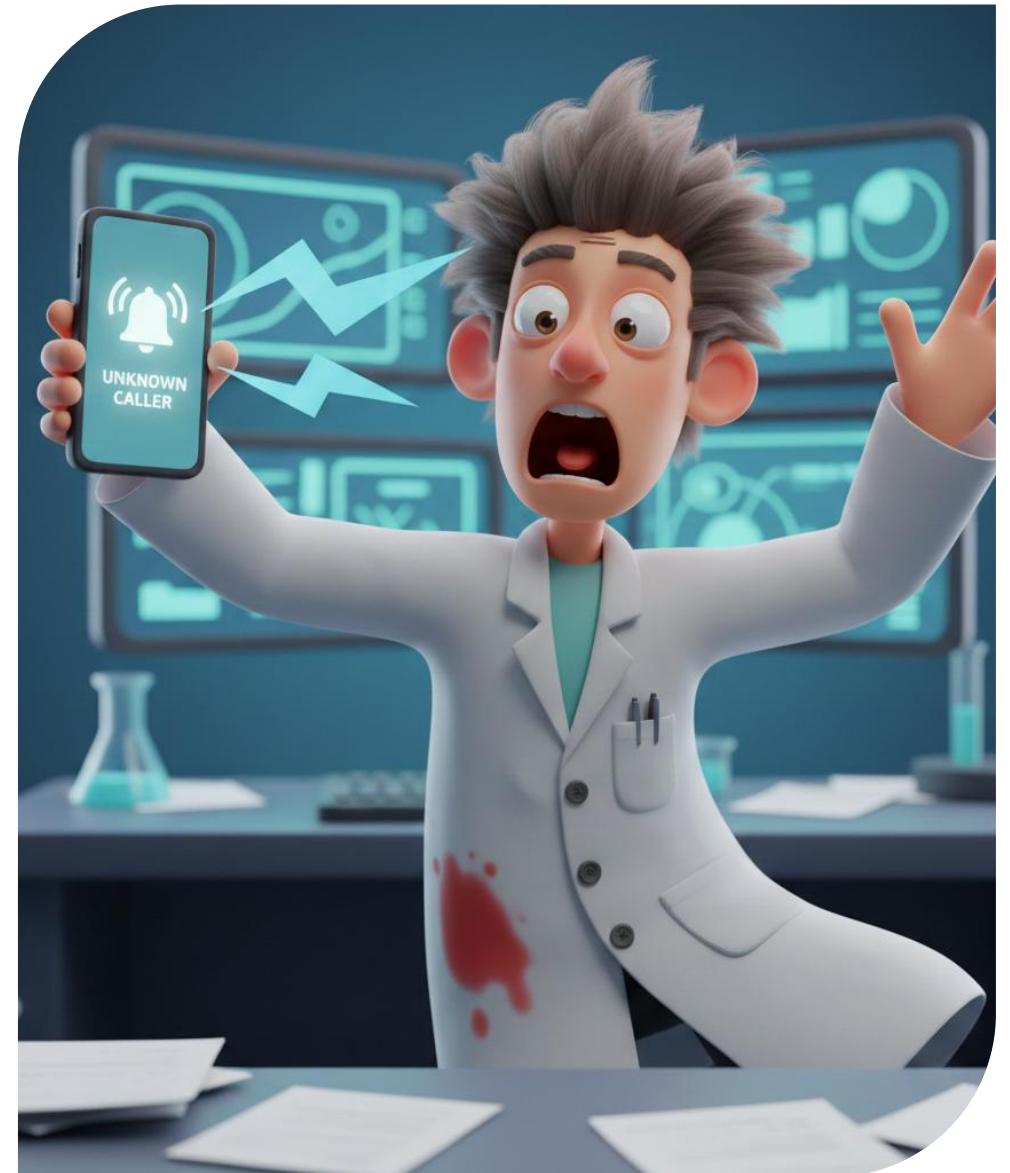
– Falsk SMS fra "Posten"

- Eksempel: "Pakken din kan ikke leveres. Betal 29 kr i frakt: [lenke]"
- Hvordan avsløre det:
 - Posten ber aldri om betaling via SMS
 - Lenken går ofte til en falsk side
 - Små beløp brukes for å lure deg til å skrive inn kortinformasjon

```
mirror_mod = modifier_ob.  
set mirror object to mirror  
mirror_mod.mirror_object  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True  
  
selection at the end -add  
mirror_ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier  
mirror_ob.select = 0  
= bpy.context.selected_ob  
data.objects[one.name].sel  
  
print("please select exactl  
  
-- OPERATOR CLASSES ----  
  
types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
mirror X"  
  
context):  
context.active_object is not
```

Svindeleksempel 2 – Telefon fra "banken"

- Eksempel: "Det er mistenkelig aktivitet på kontoen din. Logg inn med BankID nå!"
- Hvordan avsløre det:
 - Banken ringer aldri og ber deg logge inn
 - De ber aldri om fødselsnummer eller engangskoder
 - Legg på og ring banken selv





Svindeleksempel 3 – Falsk e-post

- Eksempel: "Du må oppdatere kontoen din. Klikk her."
- Hvordan avsløre det:
 - Dårlig språk
 - Uvanlig avsenderadresse
 - Lenker som ikke går til ekte nettsider
 - Ekte tjenester ber deg logge inn via egen app

Sjekkliste

– trygg digital hverdag

- Oppdater PC, telefon og apper
- Ha skjermlås på mobilen
- Ikke trykk på ukjente lenker
- Bruk sterke passord
- Bruk BankID kun når du selv har startet handlingen
- Ta sikkerhetskopi
- Be om hjelp når du er usikker

