



# Velkommen til Åpen datakafé

Tema:  
Føl deg tryggere på nettet





**Føl deg tryggere  
på nett**





## Dagens tema

- Introduksjon til en tryggere digital hverdag
- Hva er tofaktorautentisering?
- Passord og lagring av passord
- Hvordan kan du oppdage et svindelforsøk
- Oppsummering og spørsmål

# Introduksjon til en tryggere digital hverdag

- Hvorfor er det viktig å kunne bruke digitale verktøy på en trygg måte?  
Livet vårt blir mer digitalt og det er viktig at vi passer litt ekstra på det.  
Vi bruker mobilen og internett til nesten alt i dag. Bank, helse, e-post, bilder og meldinger.  
Med noen sikkerhetsvaner kan vi unngå svindel, beskytte vår personlig informasjon og føle oss tryggere på nettet.



## Introduksjon til en tryggere digital hverdag

Utforsk ressurser og verktøy for bedre digital sikkerhet.



Passord: <https://nettvett.no/passord/>



Phishing: <https://nettvett.no/phishing/>



Sosiale medier: <https://nettvett.no/sosiale-medier/>



Oppdatering: <https://nettvett.no/oppdatering>

# Introduksjon til en tryggere digital hverdag

- Hvorfor er det viktig å kunne bruke digitale verktøy på en trygg måte?
- Hvordan kan du beskytte deg mot digitale trusler
  - Bruk et sterkt passord
  - Vær skeptisk
  - Ikke klikk på lenker du er usikker om
  - Aldri gi bort/del passord/BankID
  - Spør om hjelp hvis du er usikker



## Introduksjon til en tryggere digital hverdag



Utforsk ressurser og verktøy for bedre digital sikkerhet.



Passord: <https://nettvett.no/passord/>



Phishing: <https://nettvett.no/phishing/>



Sosiale medier: <https://nettvett.no/sosiale-medier/>



Oppdatering: <https://nettvett.no/oppdatering>

# Tofaktor-autentisering og hva det innebærer

- **Hva er tofaktor-autentisering og hvorfor er den viktig? (2FA)**

Tofaktor-autentisering (2FA) er en sikkerhetsmekanisme som krever **to uavhengige faktorer** for å bekrefte identiteten din ved innlogging.

Disse faktorene kommer fra ulike kategorier:

**Noe du vet:** Passord eller PIN.

**Noe du har:** Mobiltelefon, kodebrikke, autentiseringsapp.

**Noe du er:** Biometriske data som fingeravtrykk eller ansiktsgjenkjenning.



# Tofaktor-autentisering og hva det innebærer

- Hva er tofaktor-autentisering og hvorfor er den viktig? (2FA)
- De forskjellige typene av 2FA
  - Godkjenning eller kode på E-post



## Verify it's you

Google wants to make sure it's really you trying to access admin.google.com



# 36

Open the Gmail app on iPhone

Google sent a notification to your iPhone. Open the Gmail app, tap **Yes** on the prompt, then tap **36** on your phone to verify it's you.

[Resend it](#)

[More ways to verify](#)

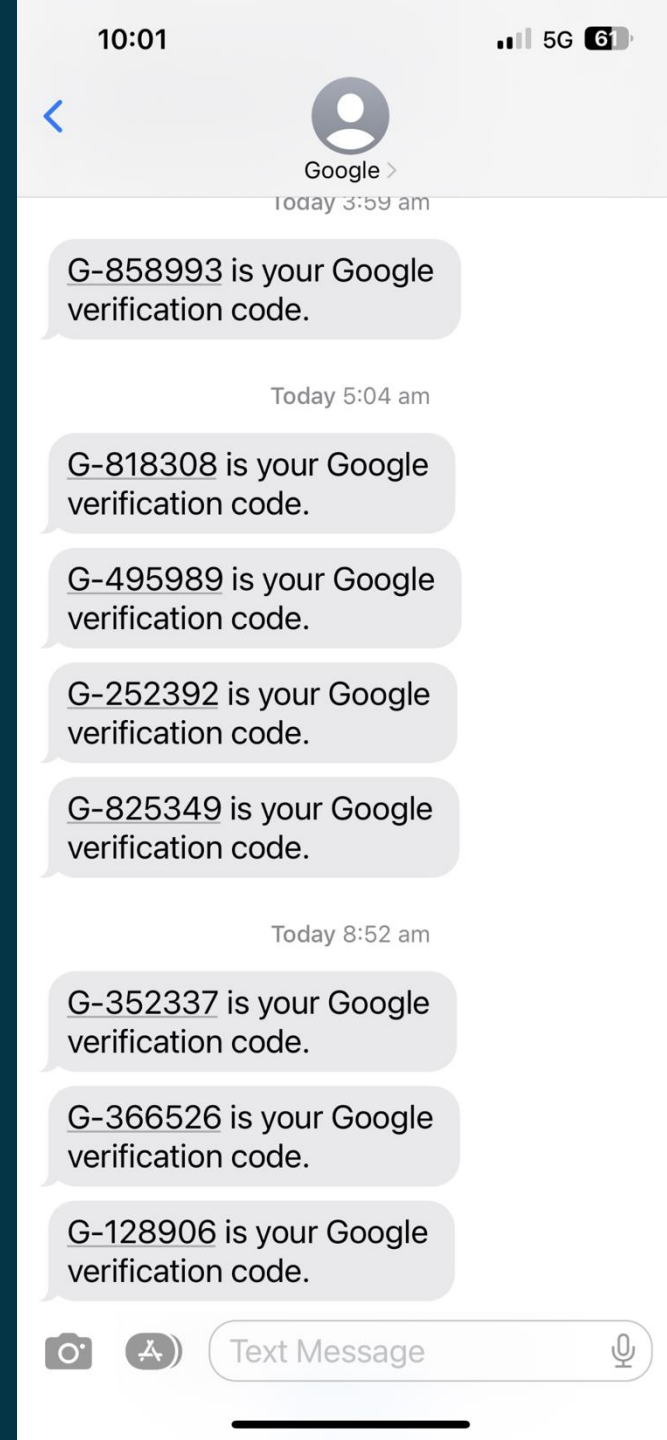
# Tofaktor-autentisering og hva det innebærer

- Hva er tofaktor-autentisering og hvorfor er den viktig? (2FA)
- De forskjellige typene av 2FA
  - Godkjenning eller kode på E-post
  - Kodebrikke



# Tofaktor-autentisering og hva det innebærer

- Hva er tofaktor-autentisering og hvorfor er den viktig? (2FA)
- De forskjellige typene av 2FA
  - Godkjenning eller kode på E-post
  - Kodebrikke
  - SMS kode





# Tofaktor-autentisering og hva det innebærer

- Hva er tofaktor-autentisering og hvorfor er den viktig? (2FA)
- De forskjellige typene av 2FA
  - Godkjenning eller kode på E-post
  - Kodebrikke
  - SMS kode
  - App bekreftelse



TIDSKRITISK  
BankID

nå

Er det du som prøver å bruke BankID hos Sbanken?

Ja, det er meg

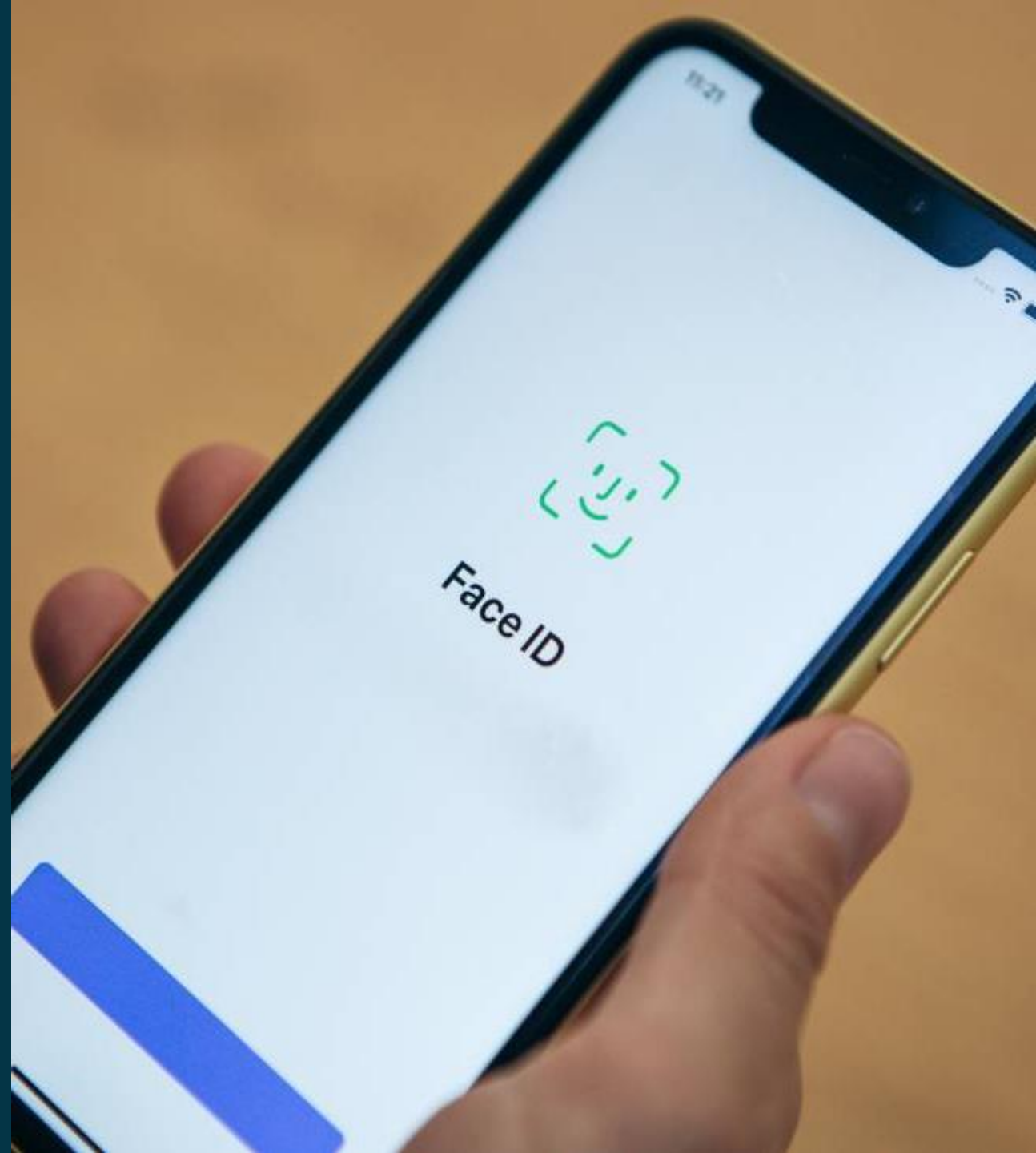


Nei, avbryt



# Tofaktor-autentisering og hva det innebærer

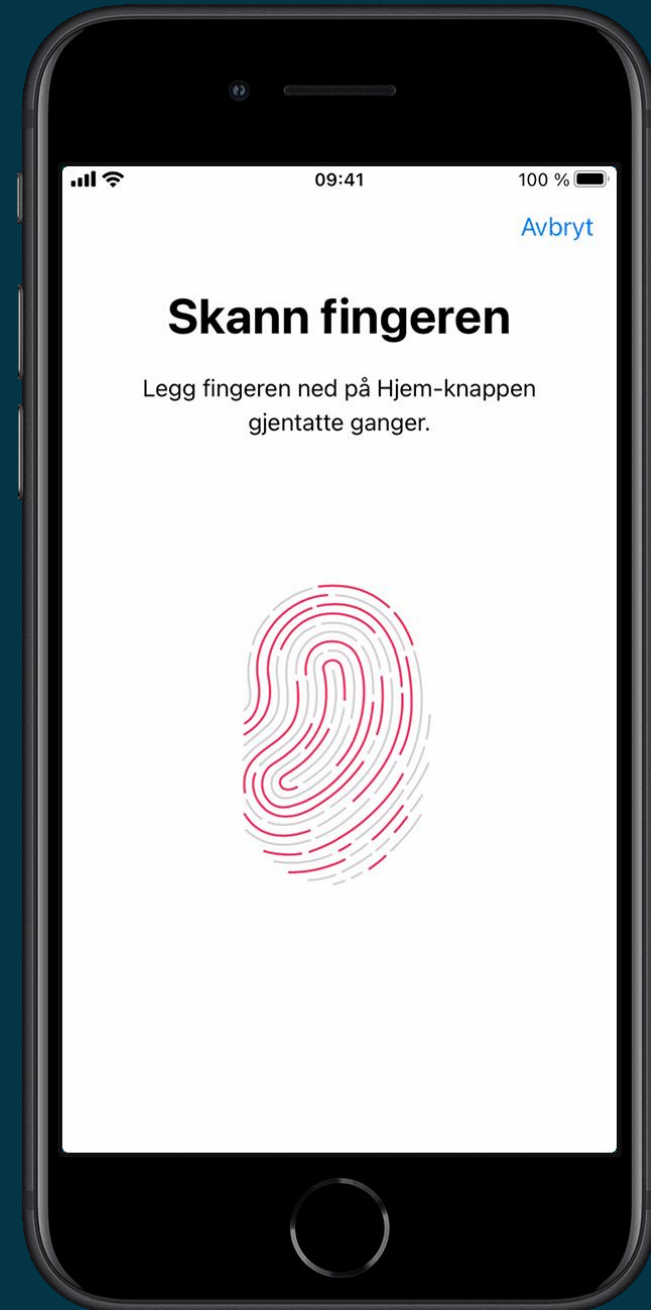
- Hva er tofaktor-autentisering og hvorfor er den viktig? (2FA)
- De forskjellige typene av 2FA
  - Godkjenning eller kode på E-post
  - Kodebrikke
  - SMS kode
  - App bekreftelse
  - FaceID





# Tofaktor-autentisering og hva det innebærer

- Hva er tofaktor-autentisering og hvorfor er den viktig? (2FA)
- De forskjellige typene av 2FA
  - Godkjenning eller kode på E-post
  - Kodebrikke
  - SMS kode
  - App bekreftelse
  - FaceID
  - Touch ID



# Hvordan å opprette et sterkt passord

1. Lengde: Minst 10-16 tegn



# Hvordan å opprette et sterkt passord

1. **Lengde:** Minst 10-16 tegn
2. **Inneholde ulikhet:** Store og små bokstaver, tall og symboler.



# Hvordan å opprette et sterkt passord

1. **Lengde:** Minst 10-16 tegn
2. **Inneholde ulikhet:** Store og små bokstaver, tall og symboler.
3. **Variasjon:** Ikke bruk like passord overalt



# Hvordan å opprette et sterkt passord

1. **Lengde:** Minst 10-16 tegn
2. **Inneholde ulikhet:** Store og små bokstaver, tall og symboler.
3. **Variasjon:** Ikke bruk like passord overalt
4. **Ikke bruk:** navn, fødselsdato eller enkle tall som 1234



# Hvordan å opprette et sterkt passord

1. **Lengde:** Minst 10-16 tegn
2. **Inneholde ulikhet:** Store og små bokstaver, tall og symboler.
3. **Variasjon:** Ikke bruk like passord overalt
4. **Ikke bruk:** navn, fødselsdato eller enkle tall som 1234
5. **Tips:** En setning eller kombinasjon av ord som du husker





# Svake og Sterke passord

## Svake passord

1. 12345678



# Svake og Sterke passord

## Svake passord

1. 12345678
2. navn1234



# Svake og Sterke passord

## Svake passord

1. 12345678
2. navn1234
3. bursdags dato  
(mars1992/201007)



# Svake og Sterke passord

## Svake passord

1. 12345678
2. navn1234
3. bursdags dato  
(mars1992/201007)
4. navn på kjæledyr



# Svake og Sterke passord

## Svake passord

1. 12345678
2. navn1234
3. bursdags dato  
(mars1992/201007)
4. navn på kjæledyr

## Sterk passord

5. AndenesTur09



# Svake og Sterke passord

## Svake passord

1. 12345678
2. navn1234
3. bursdags dato  
(mars1992/201007)
4. navn på kjæledyr

## Sterk passord

5. AndenesTur09
6. HvorforGate89



# Sterkere og Meget sterkt passord

## Sterkere passord

1. #AndenesTur09



# Sterkere og Meget sterkt passord

## Sterkere passord

1. #AndenesTur09
2. Hvorfor?Gate89



# Sterkere og Meget sterkt passord

## Sterkere passord

1. #AndenesTur09
2. Hvorfor?Gate89

## Meget sterkt password

3. #And3n35Tur2009



# Sterkere og Meget sterkt passord

## Sterkere passord

1. #AndenesTur09
2. Hvorfor?Gate89

## Meget sterkt password

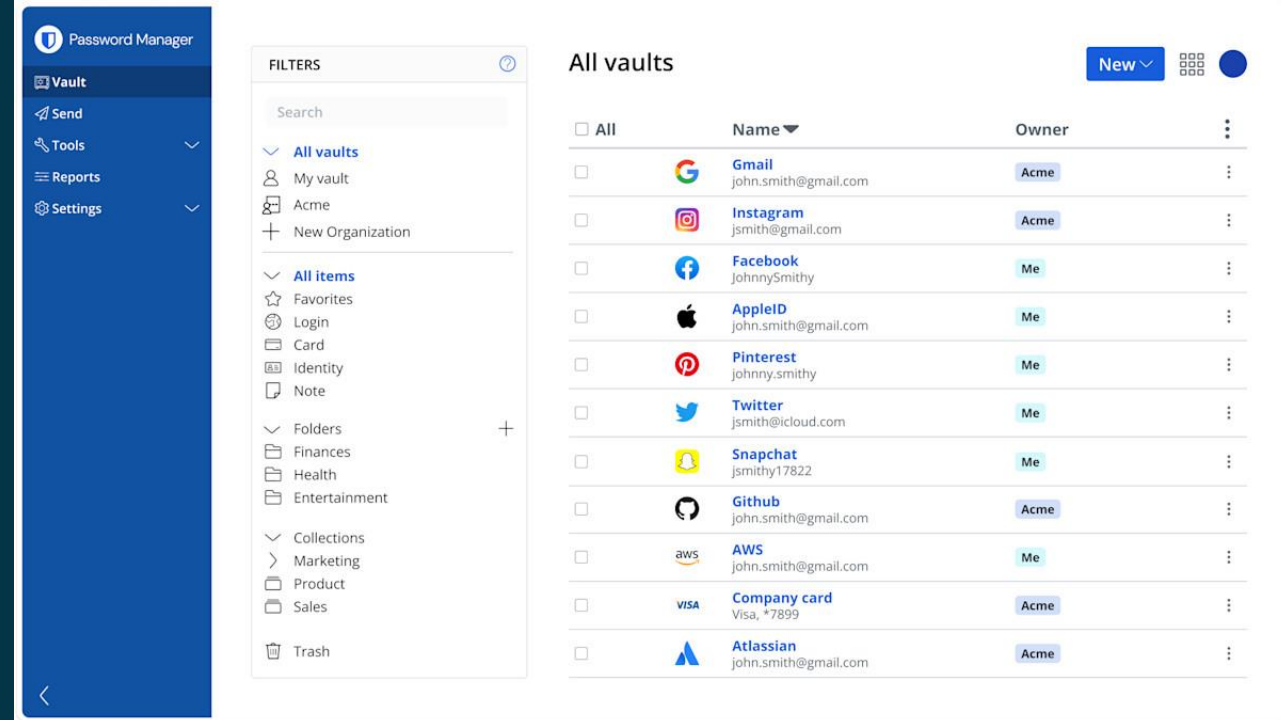
3. #And3n35Tur2009
4. i}Q#eRlFJz6LkbUG

# Hvordan lagre passord

Måter man kan lagre passord på:

## 1. Passordhvelv

Et passordhvelv er som en **digital safe** der du kan lagre alle passordene dine på ett sikkert sted. Du trenger bare å huske **ett hoved passord** for å åpne hvelvet. Apper som **Passwords** og **Samsungpass** for telefoner og **Password Manager** for PC.





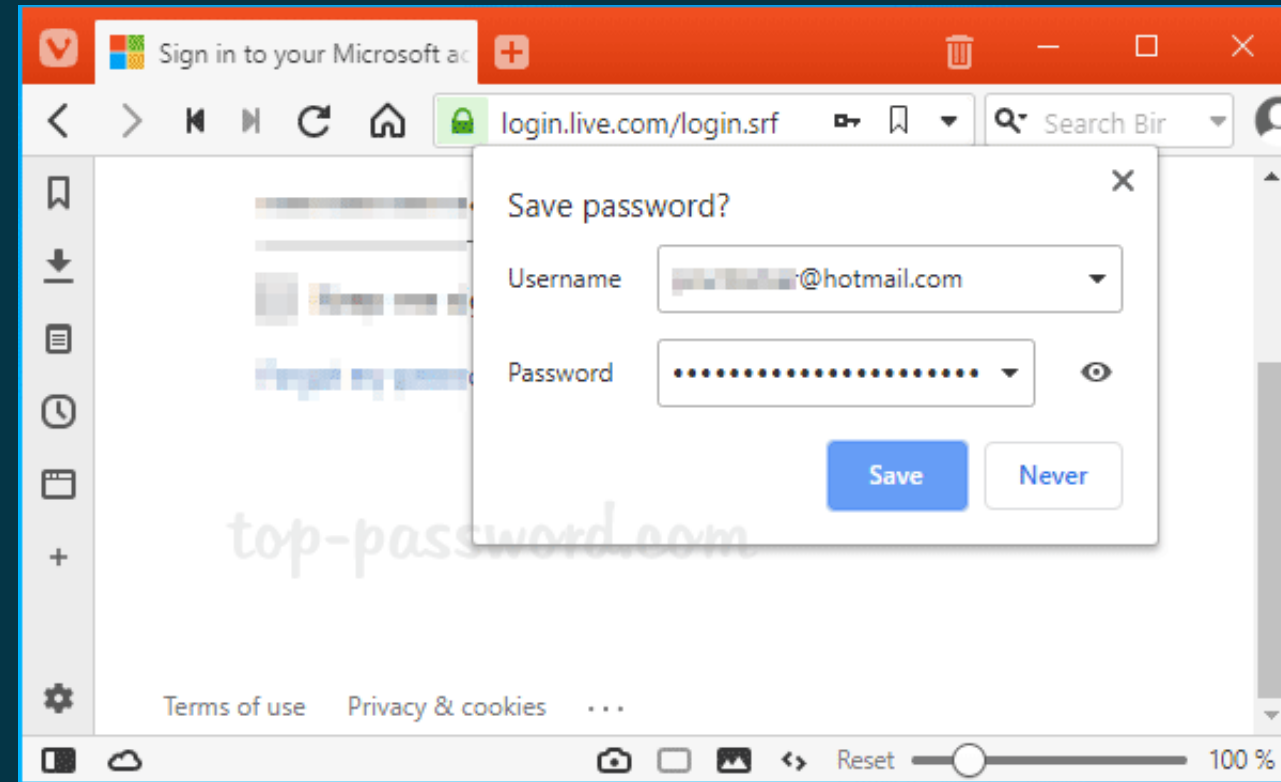
# Hvordan lagre passord

Måter man kan lagre passord på:

## 1. Passordhvelv

## 2. I nettleseren

Man kan velge å lagre passordet og brukernavn til en innlogging ved å trykke **lagre** etter man har logget inn for **første gang**. Dette fører til at alt blir **automatisk ført** inn ved neste innloggings forsøk.

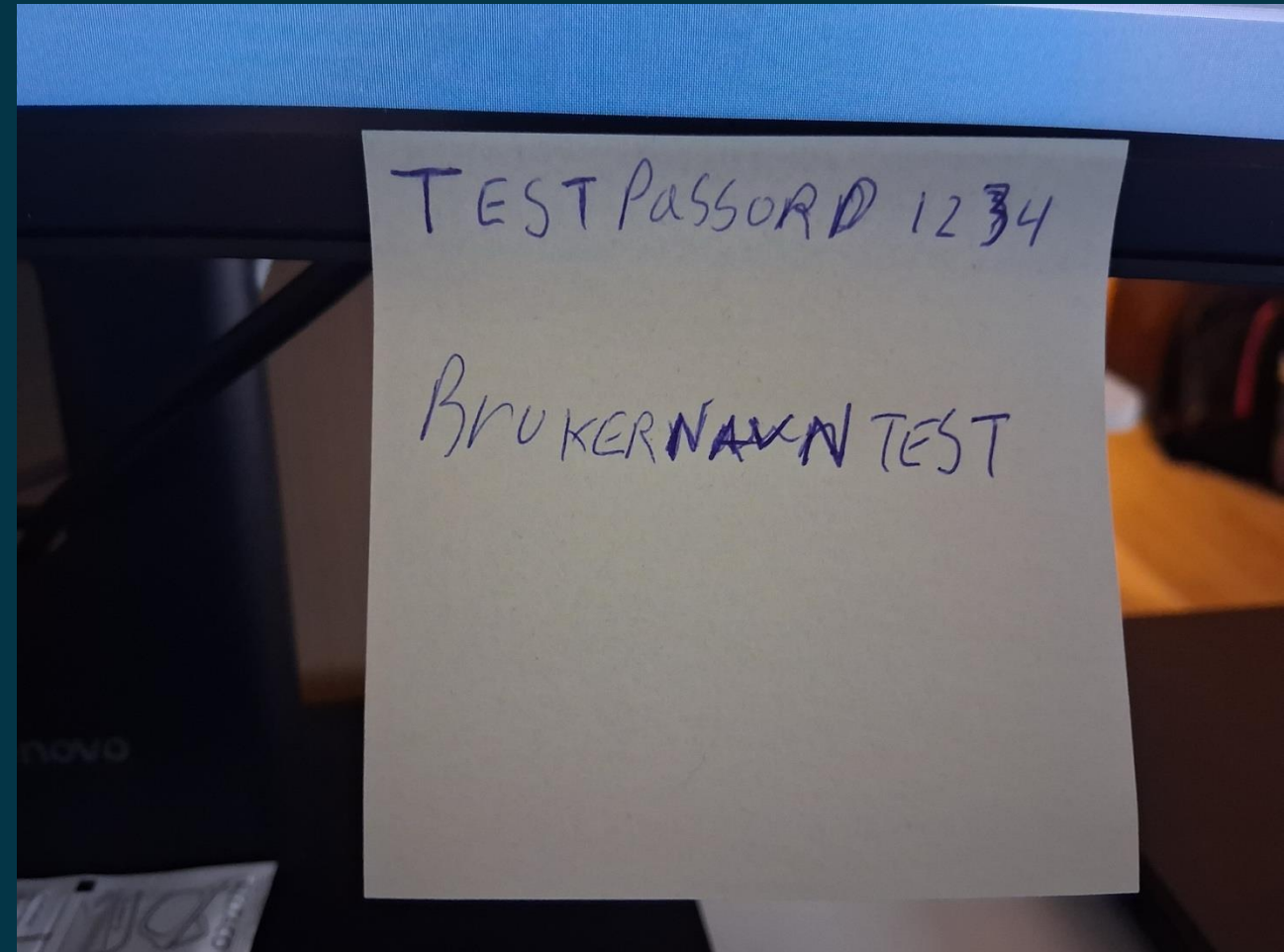




# Hvordan lagre passord

Måter man kan lagre passord på:

1. Passordhvelv
2. I nettleseren
3. **Skrive ned passord på fysisk dokument**  
Bare hvis man kan ta vare på det som en verdi papir.





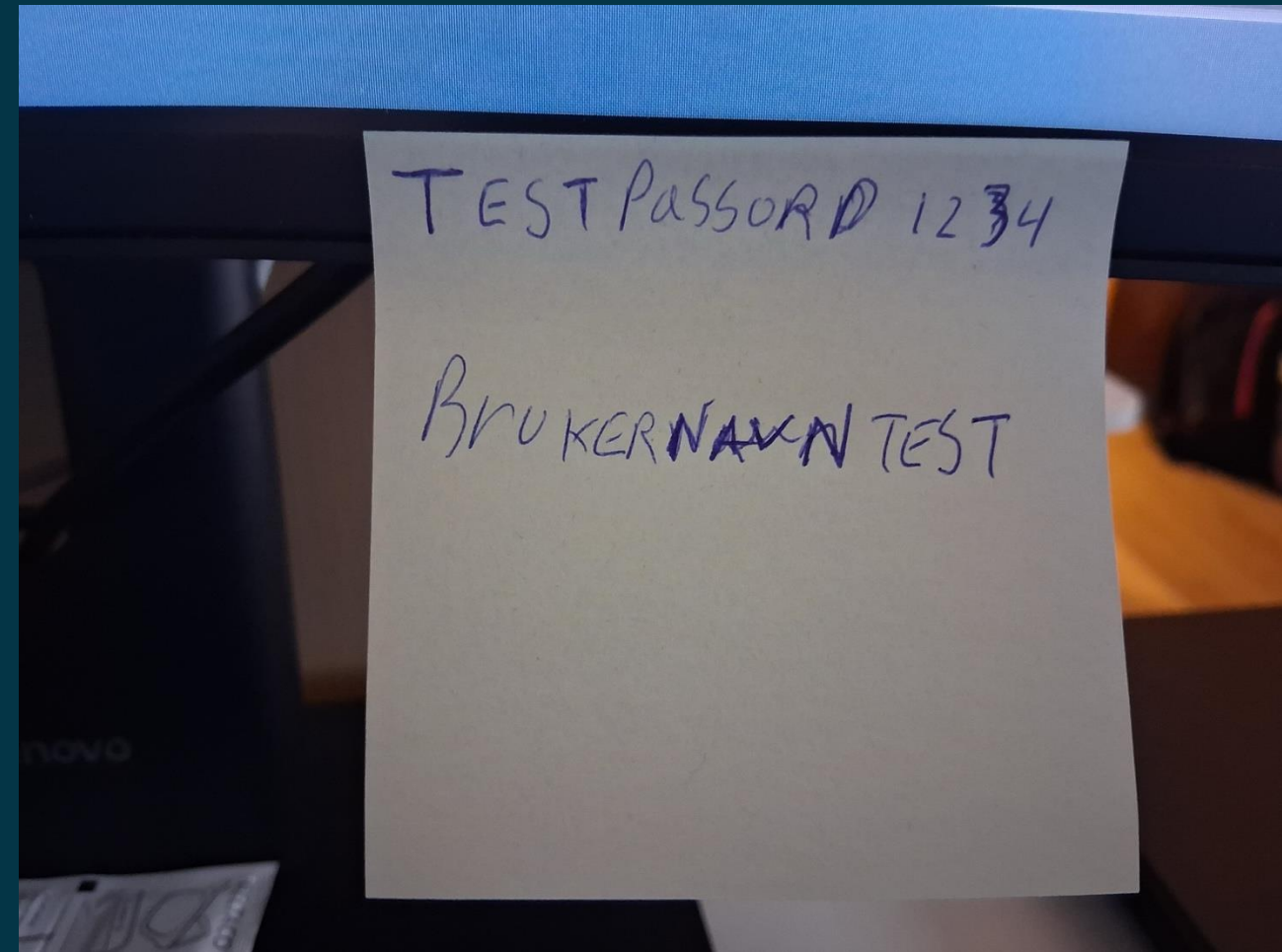
# Hvordan lagre passord

Måter man kan lagre passord på:

1. Passordhvelv
2. I nettleseren
3. Skrive ned passord på fysisk dokument

Hvordan passord ikke bør håndteres:

4. Bilde av passordet





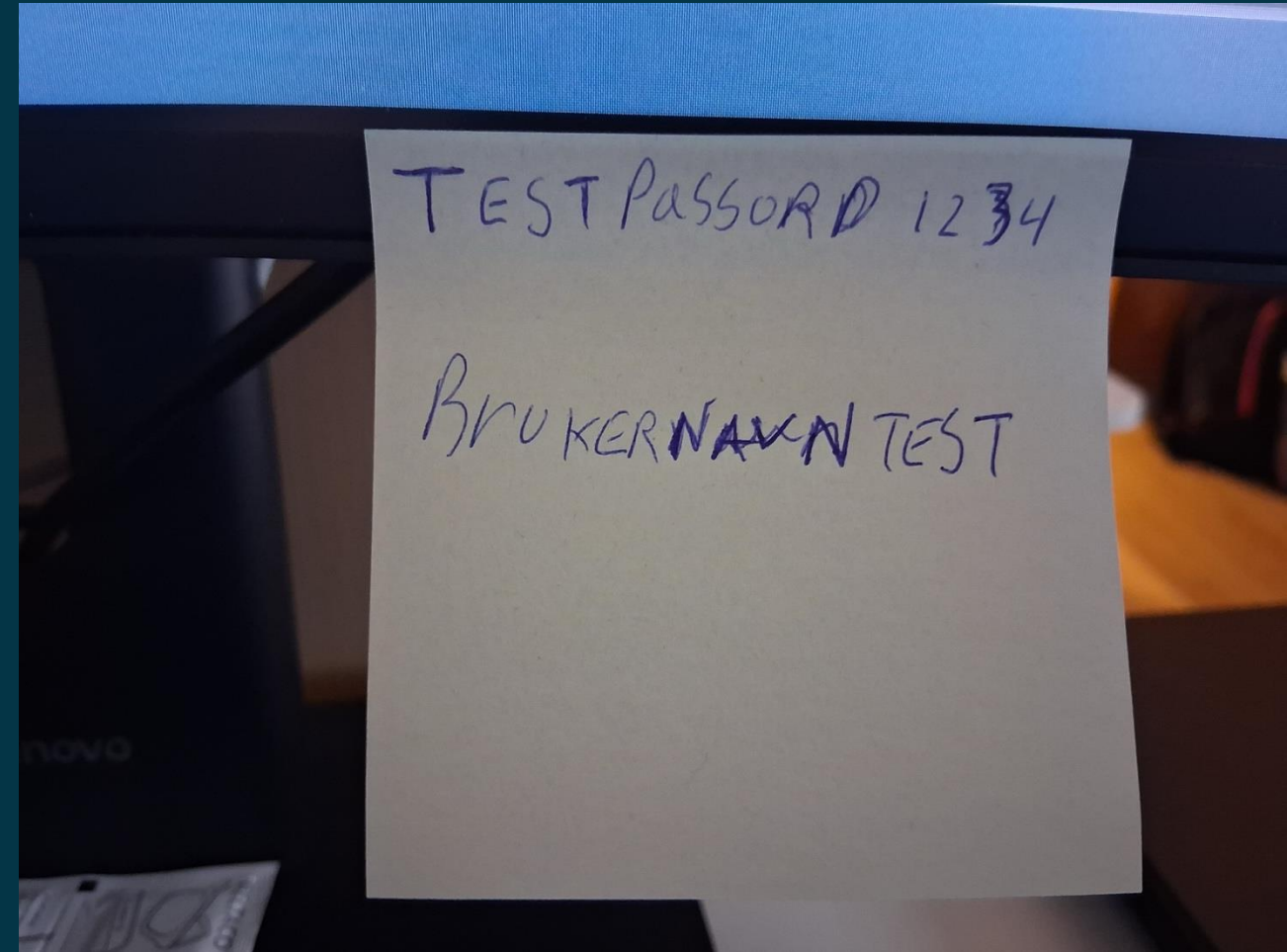
# Hvordan lagre passord

Måter man kan lagre passord på:

1. Passordhvelv
2. I nettleseren
3. Skrive ned passord på fysisk dokument

Hvordan passord ikke bør håndteres:

4. Bilde av passordet
5. Skrive ned passord på fysisk dokumenter





# Hvordan kan du oppdage svindelforsøk

1. Sjekk avsender og innhold  
Svindlere bruker ofte **falske** e-postadresser som ligner på ekte, men har **små feil** (f.eks. ekstra bokstaver eller rare domener). Vær **skeptisk** til e-poster med **dårlig språk**, mange **skrivefeil** eller **uvanlig høflighet**.

**Fra:** DNB Kundeservice <[kundeservice@dnb-login-secure.com](mailto:kundeservice@dnb-login-secure.com)>

**Til:** Christian

**Kjære kunde,**

Vi har oppdaget uvanlig aktivitet på din konto. For å beskytte dine midler må du bekrefte din identitet umiddelbart. Hvis du ikke gjør dette innen 24 timer, vil din BankID bli midlertidig sperret.

Klikk på lenken under for å bekrefte:

👉 <https://dnb.no>

Takk for at du velger DNB.

Med vennlig hilsen,

**DNB Kundeservice**

<https://dnb-login-secure.com>



# Hvordan kan du oppdage svindelforsøk

1. Sjekk avsender og innhold
2. Vær kritisk til ukjente lenker eller vedlegg  
Hvis du får en e-post med en lenke eller et vedlegg du ikke forventet, **ikke åpne det**. Hold musepekeren over lenken for å se den faktiske adressen før du klikker.

Fra: DNB Kundeservice <[kundeservice@dnb-login-secure.com](mailto:kundeservice@dnb-login-secure.com)>

Til: Christian

Kjære kunde,

Vi har oppdaget uvanlig aktivitet på din konto. For å beskytte dine midler må du bekrefte din identitet umiddelbart. Hvis du ikke gjør dette innen 24 timer, vil din BankID bli midlertidig sperret.

Klikk på lenken under for å bekrefte:

👉 <https://dnb.no>

Takk for at du velger DNB.

Med vennlig hilsen,

**DNB Kundeservice**

<https://dnb-login-secure.com>



# Hvordan kan du oppdage svindelforsøk

1. Sjekk avsender og innhold
2. Vær kritisk til ukjente lenker eller vedlegg
3. **Vær oppmerksom på hastverk og trusler**

Svindlere skaper ofte stress: «Svar innen 10 minutter» eller «Kontoen din blir sperret». Seriøse aktører gir deg tid og presser ikke.

Hvis du ikke gjør dette innen 24 timer, vil din BankID bli midlertidig sperret.



# Hvordan kan du oppdage svindelforsøk

1. Sjekk avsender og innhold
2. Vær kritisk til ukjente lenker eller vedlegg
3. Vær oppmerksom på hastverk og trusler
4. Bekreft med en annen kilde (ta kontakt med familie, venner eller direkte med banken)

# Gavekortsvindel

Gavekortsvindel er en form for svindel der kriminelle lurer deg til å **kjøre gavekort** (for eksempel Apple, Google Play, Elkjøp, Coop) og deretter **dele koden** på kortet med dem. Når du har sendt koden, kan svindleren bruke gavekortet eller selge det videre – og pengene er som regel tapt for godt



# Eksempel svindelforsøk fra «politi» «interpol»

- Rare stavelser og skrivefeil



## STEVNING

For en rettslig etterforskning  
(artikkel 331-1-22 i straffeprosessloven)

Jeg er herr Arne Jørgen Olafsen, politidirektør og kriminalpolitimester. I samarbeid med European Police Service (INTERPOL), kontakter jeg deg umiddelbart etter et beslag av cyberinfiltrasjon (autorisert, spesielt innen barnepornografi, pornografiske nettsteder, cyberpornografi) for å informere deg om at du **gjør gjenstand** for flere søksmål. :

- \* **SYBERPORNGRAFI**
- \* **PORNOGRAFISKE NETTSIDER**
- \* **BARNEPORNO**
- \* **TRASSERING AV BARN**

Ta kontakt med oss på e-post med dine begrunnelser slik at de kan undersøkes for å vurdere sanksjonen.

Dette innen en streng frist på 48 timer. Etter dette tidspunkt vil vi være forpliktet til å sende vår rapport til statsadvokat Roaldsøy Atle, slik at han kan utstede en arrestordre mot deg, og vi går videre til din umiddelbare arrest.

Du vil da bli registrert i National Sex Offenders Registry.

Filen din vil også bli publisert i media slik at publikum og din familie vet hva du **gjør** på datamaskinen din.

Vi venter på svaret ditt for å åpne en rapport.

Du er nå advart.



Arne Jørgen Olafsen  
politidirektør og  
kriminalpolitimester.



# Eksempel svindelforsøk fra «politi» «interpol»

- Rare stavelser og skrivefeil
- Hastverk og trusler



POLITIGENERALT

BESKYTTELSESBRIGADE FOR MINJØRIGE

## STEVNING

For en rettslig etterforskning  
(artikkel 331-1-22 i straffeprosessloven)

Jeg er herr Arne Jørgen Olafsen, politidirektør og kriminalpolitimester. I samarbeid med European Police Service (INTERPOL.), kontakter jeg deg umiddelbart etter et beslag av cyberinfiltrasjon (autorisert, spesielt innen barnepornografi, pornografiske nettsteder, cyberpornografi) for å informere deg om at du gjør gjenstand for flere søksmål. :

- \* SYBERPORNGRAFI
- \* PORNOGRAFISKE NETTSIDER
- \* BARNEPORNO
- \* TRASSERING AV BARN

Ta kontakt med oss på e-post med dine begrunnelser slik at de kan undersøkes for å vurdere sanksjonen.

Dette innen en streng frist på 48 timer. Etter dette tidspunkt vil vi være forpliktet til å sende vår rapport til statsadvokat Roaldsøy Atle, slik at han kan utstede en arrestordre mot deg, og vi går videre til din umiddelbare arrest. Du vil da bli registrert i National Sex Offenders Registry. Filen din vil også bli publisert i media slik at publikum og din familie vet hva du gjør på datamaskinen din.

Vi venter på svaret ditt for å åpne en rapport.

Du er nå advart.



Arne Jørgen Olafsen  
politidirektør og  
kriminalpolitimester.



# Eksempel svindelforsøk fra «politi» «interpol»

- Rare stavelser og skrivefeil
- Hastverk og trusler
- Logoer som ser Ekte ut, men som er enkle å kopiere



**JUSTISDEPARTEMENTET**

**POLITI**  
POLITIGENERALT  
BESKYTTELSESBRIGADE FOR MINJØRIGE

**INTERPOL**

## STEVNING

For en rettslig etterforskning  
(artikkel 331-1-22 i straffeprosessloven)

Jeg er herr Arne Jørgen Olafsen, politidirektør og kriminalpolitimester. I samarbeid med European Police Service (INTERPOL), kontakter jeg deg umiddelbart etter et beslag av cyberinfiltrasjon (autorisert, spesielt innen barnepornografi, pornografiske nettsteder, cyberpornografi) for å informere deg om at du gjør gjenstand for flere søksmål. :

- \* SYBERPORNGRAFI
- \* PORNOGRAFISKE NETTSIDER
- \* BARNEPORNO
- \* TRASSERING AV BARN

Ta kontakt med oss på e-post med dine begrunnelser slik at de kan undersøkes for å vurdere sanksjonen.

Dette innen en streng frist på 48 timer. Etter dette tidspunkt vil vi være forpliktet til å sende vår rapport til statsadvokat Roaldsøy Atle, slik at han kan utstede en arrestordre mot deg, og vi går videre til din umiddelbare arrest.

Du vil da bli registrert i National Sex Offenders Registry.

Filen din vil også bli publisert i media slik at publikum og din familie vet hva du gjør på datamaskinen din.

Vi venter på svaret ditt for å åpne en rapport.

Du er nå advart.



Arne Jørgen Olafsen  
politidirektør og  
kriminalpolitimester.



**RETNINGEN**  
Kriminalpolitimester og  
KriminalPOLITI  
Arne Jørgen O.  
POLITIDIREKTØR

# Eksempel melding fra NAV

## 1. Lenken er feil

Den falske meldingen bruker en ukjent adresse (*minid-portalen.vercel.app*), ikke NAVs offisielle domene.

Du har mottatt en ny melding fra NAV.

Logg inn på

<https://minid-portalen.vercel.app>

for å lese meldingen.

Vennlig hilsen

NAV

# Eksempel melding fra NAV

1. Lenken er feil
2. Ser profesjonell ut, men er ikke ekte  
Svindlere lager troverdige meldinger for å lure deg til å klikke.

Hei! Du har fått en ny melding fra NAV. Logg deg inn på [nav.no](http://nav.no) for å lese meldingen. Vennlig hilsen NAV

# Eksempel melding fra NAV


1. Lenken er feil
2. Ser profesjonell ut, men er ikke ekte
3. **Formålet**  
Når du klikker, kan du bli bedt om å oppgi BankID eller personopplysninger – som svindlerne misbruker.

Hei! Du har fått en ny melding fra NAV. Logg deg inn på [nav.no](https://nav.no) for å lese meldingen. Vennlig hilsen NAV


# Eksempel melding fra NAV

1. Lenken er feil
2. Ser profesjonell ut, men er ikke ekte
3. **Formålet**
4. **Sjekk alltid lenken**  
Den skal være *nav.no* eller en kjent offentlig adresse. **Ikke klikk på ukjente lenker.** Hvis du er usikker, gå direkte til **nav.no** via nettleseren – ikke via SMS-lenken.


Hei! Du har fått en ny melding fra NAV. Logg deg inn på [nav.no](https://nav.no) for å lese meldingen. Vennlig hilsen NAV

A woman with blonde hair, wearing a dark blazer over a light-colored top, is sitting at a dark desk in an office. She is smiling slightly and looking towards the camera. Her hands are clasped on the desk. To her right, there is a desk lamp with a long, thin light fixture, a yellow mug, and some papers. The background is a plain, light-colored wall. The lighting is soft and focused on the woman.

Og det er dét vi svindlere spiller på.



Politiet ville aldri spurt deg om BankID.

A woman in a red dress stands in the center of a dark, modern interior space. The room features a large, light-colored rectangular structure in the background, possibly a piece of art or a wall panel, with some faint lights and shadows. The overall atmosphere is mysterious and dramatic.

Svindlere spiller på følelsene dine.



# 5 tips til å unngå å bli svindlet



Del aldri bank-, kort- eller personopplysninger med noen



Vær skeptisk til telefoner, meldinger og e-poster



Trykk ikke på lenker eller vedlegg du ikke stoler på



Bruk sterke passord og aktiver to-faktor autentisering



Be om hjelp fra noen du stoler på dersom du er usikker



# 5 tips hvis du har blitt svindlet



Avbryt all kontakt med svindleren



Informer banken hvis du har gitt fra deg kort- eller kontoinformasjon



Endre passord der du er rammet av svindel



Meld fra til politiet om svindelen



Be om råd fra noen du stoler på



# Oppsummering

- Lag et sterkt passord
- Bruk tofaktorautentisering
- Vær oppmerksom på svindelforsøk