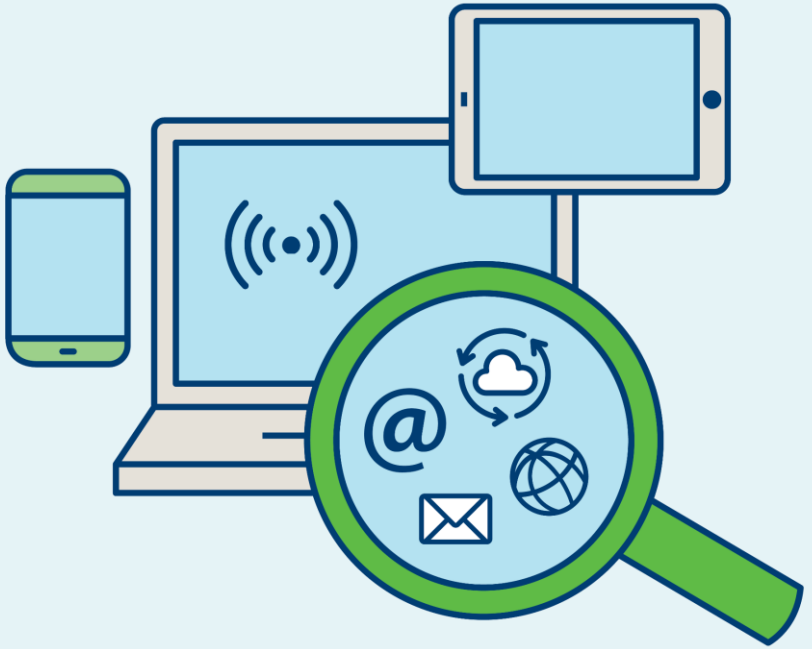
Velkommen til Åpen datakafé

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

- 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

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:

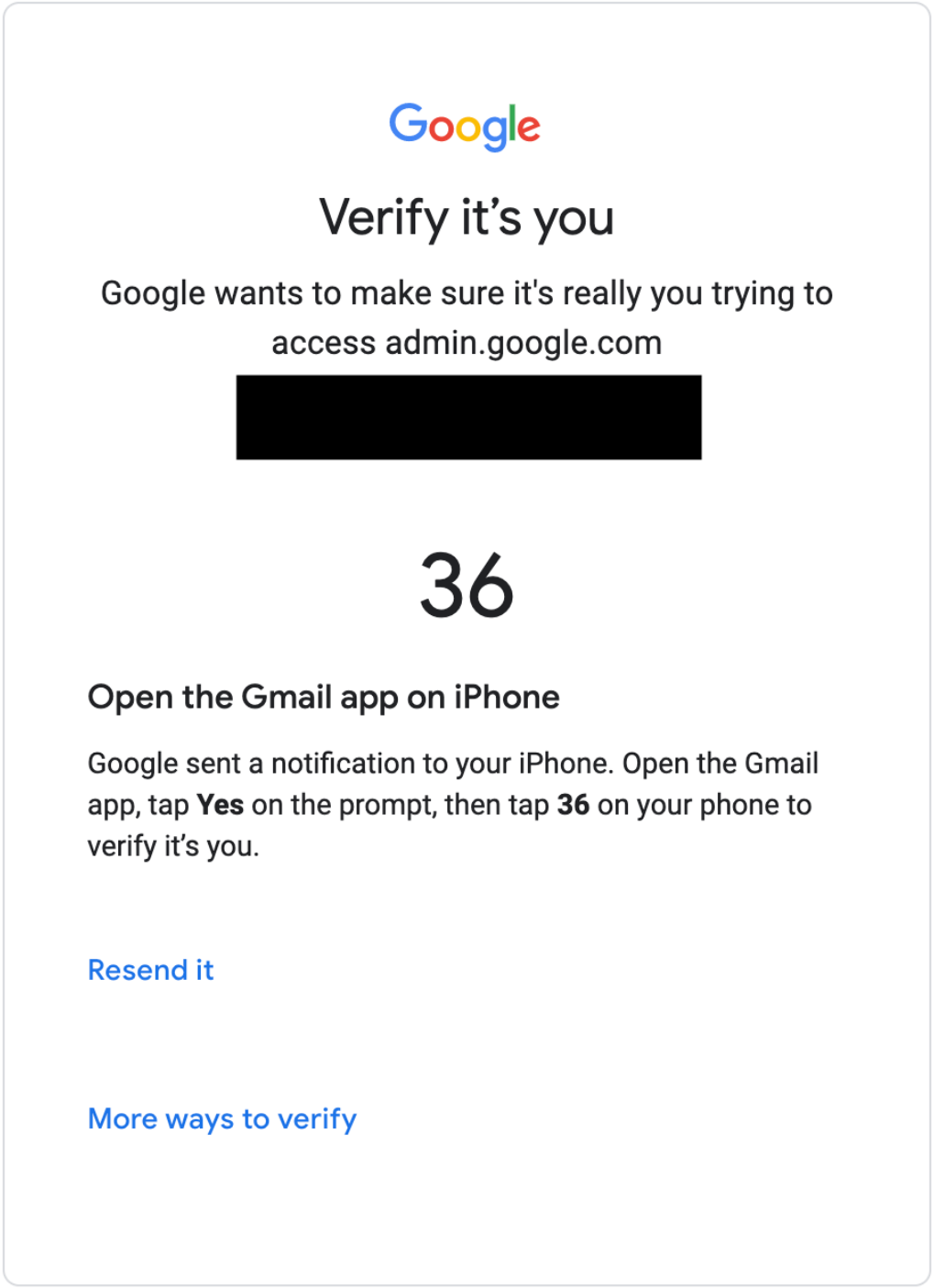
  Noe du vet: Passord eller PIN.

  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

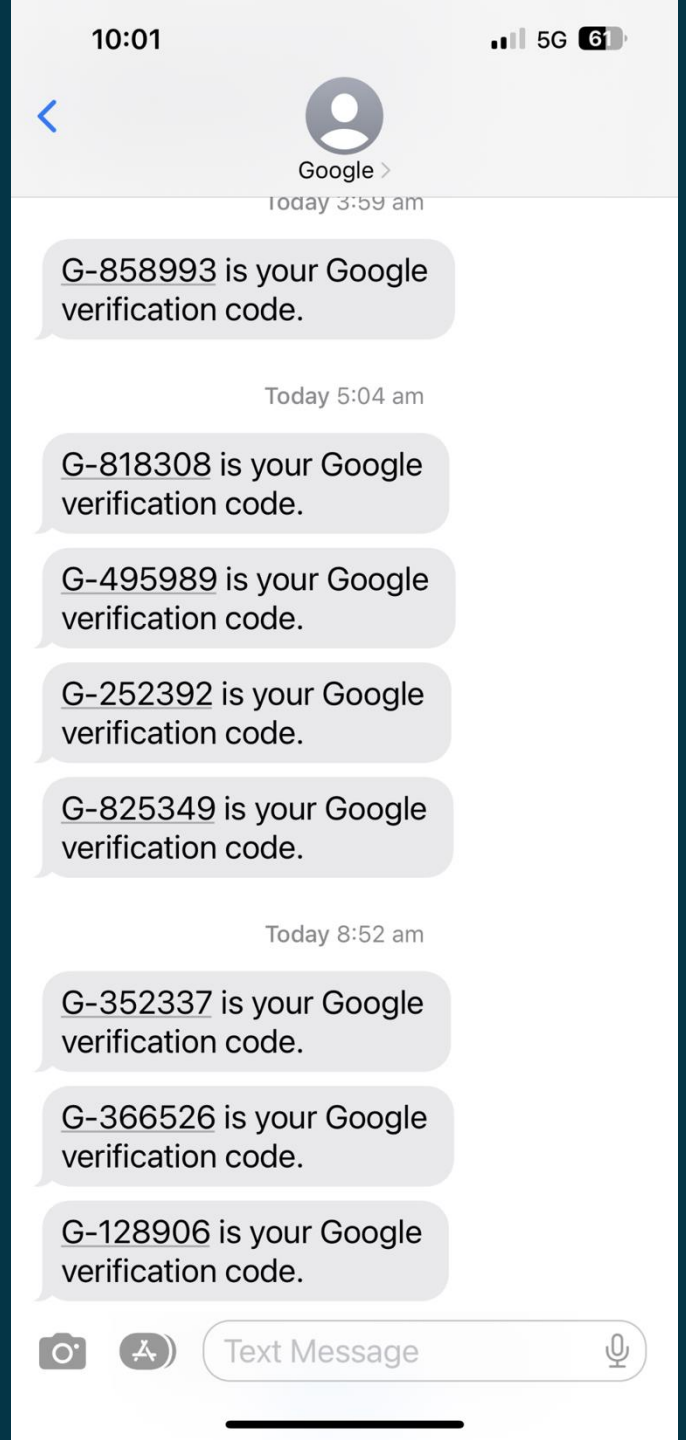


Tofaktor-autentisering og hva det innebærer

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

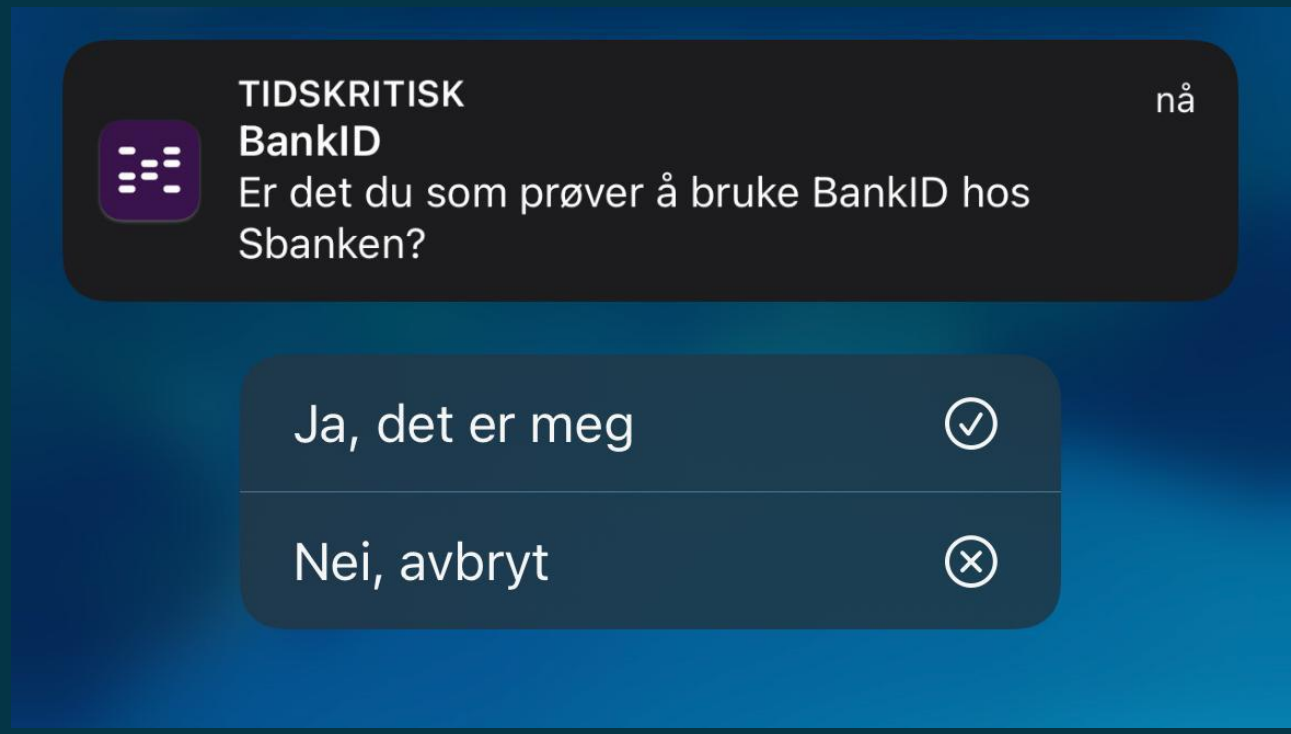
Tofaktor-autentisering og hva det innebærer

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



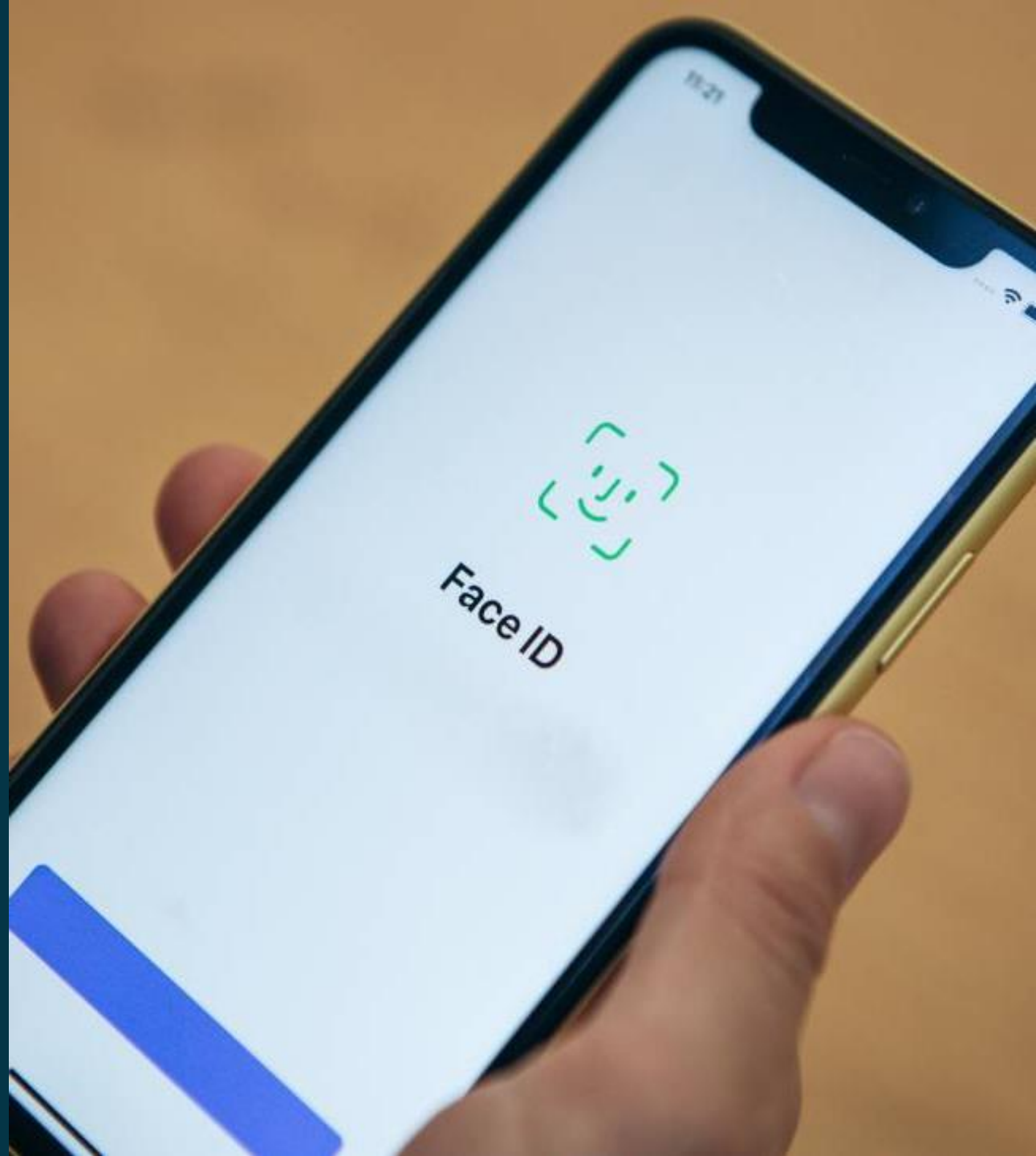
Tofaktor-autentisering og hva det innebærer

- 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



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

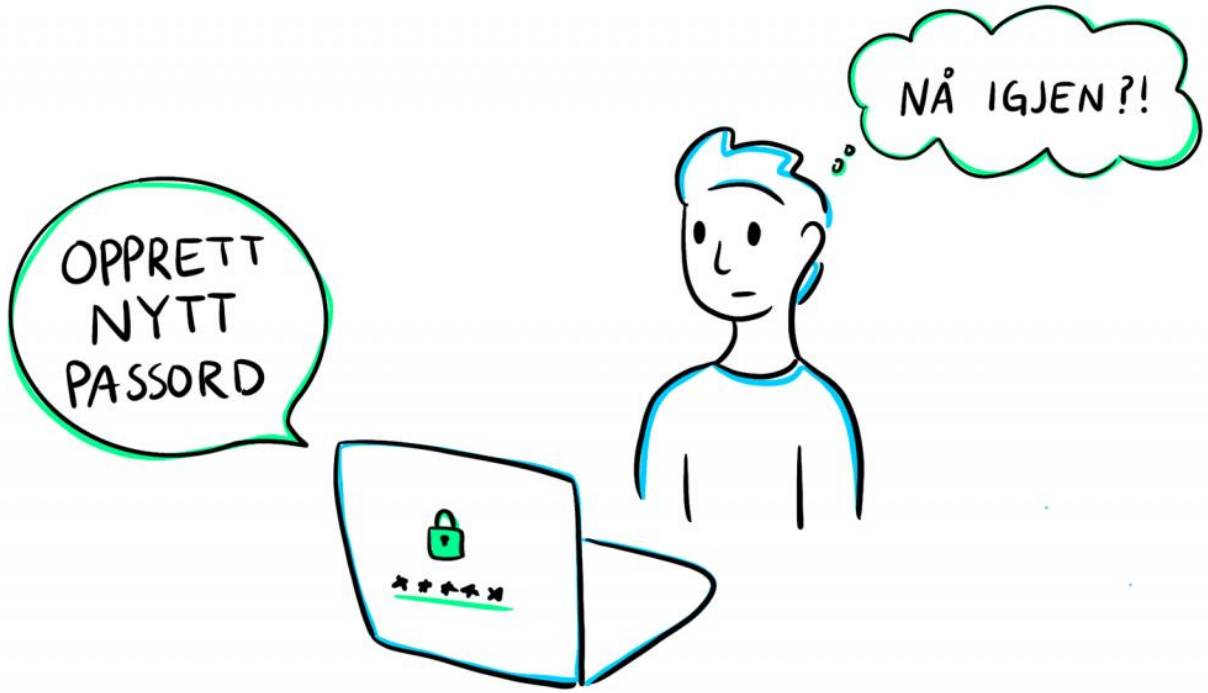


Tofaktor-autentisering og hva det innebærer

- 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

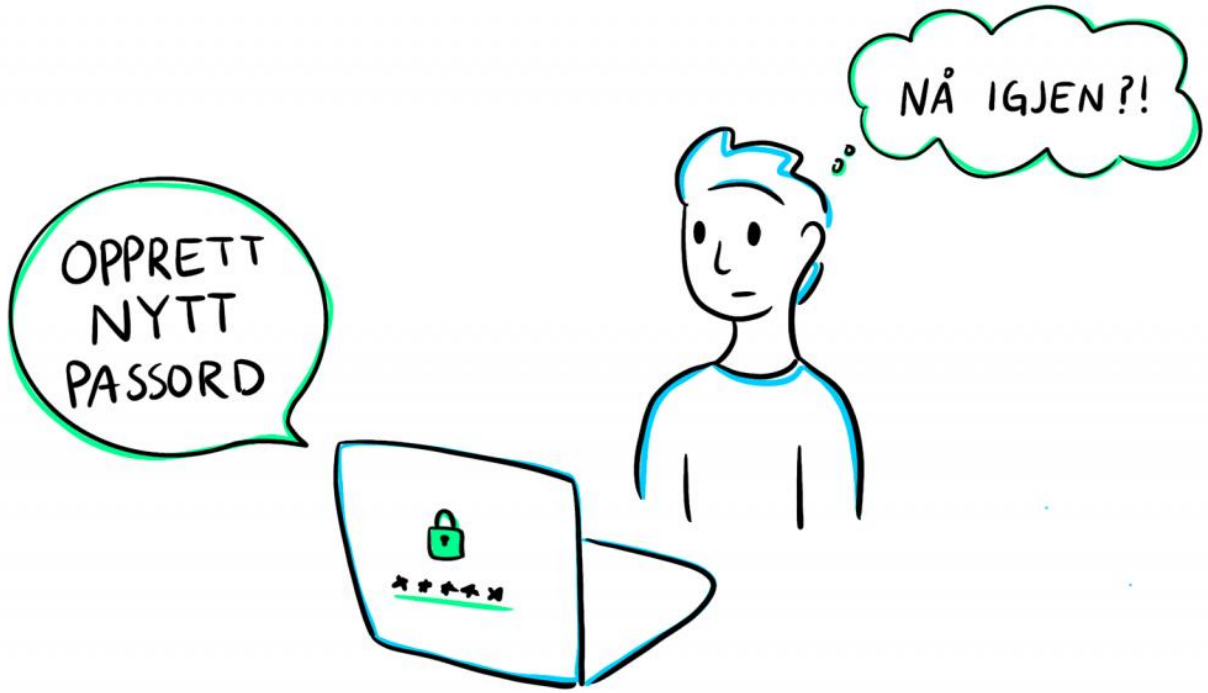
Hvordan å opprette et sterkt passord

1. **Lengde:** Minst 10-16 tegn



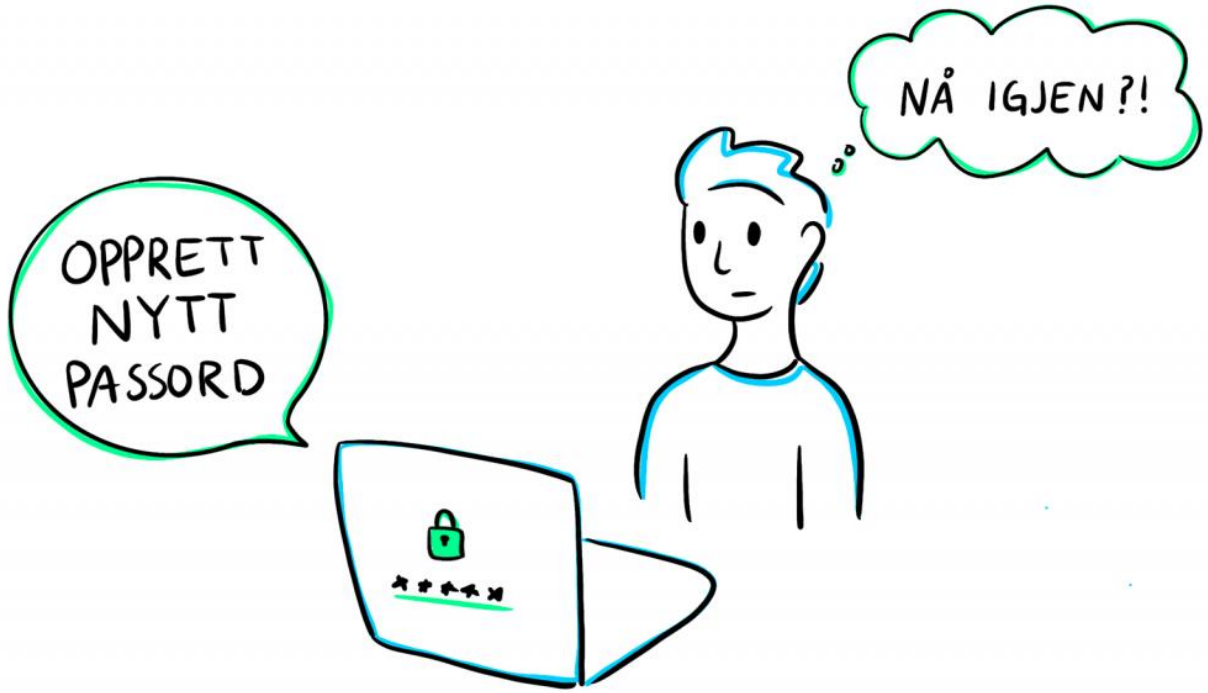
Hvordan å opprette et sterkt passord

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



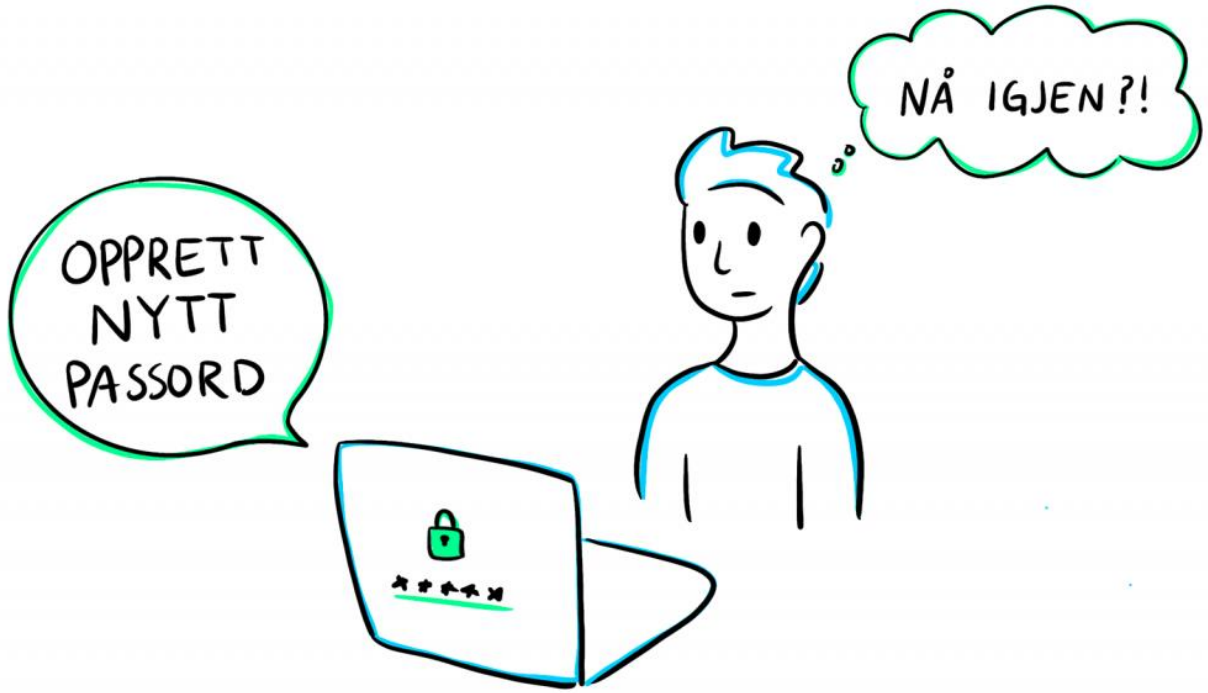
Hvordan å opprette et sterkt passord

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



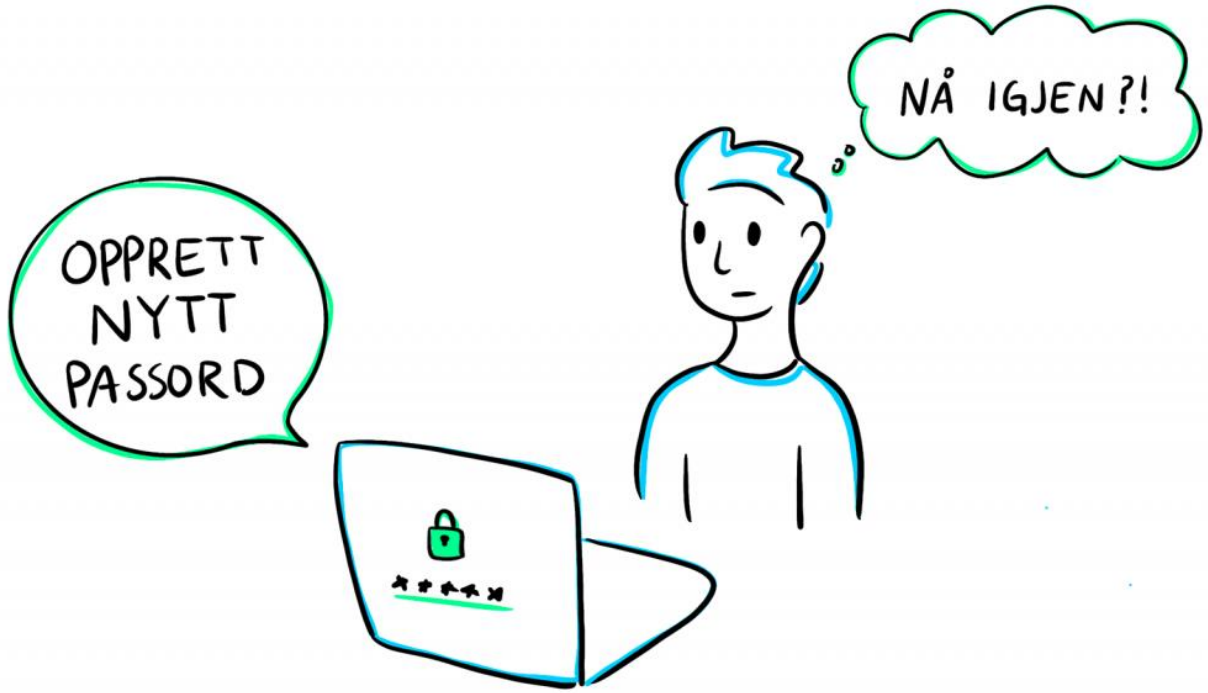
Hvordan å opprette et sterkt passord

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

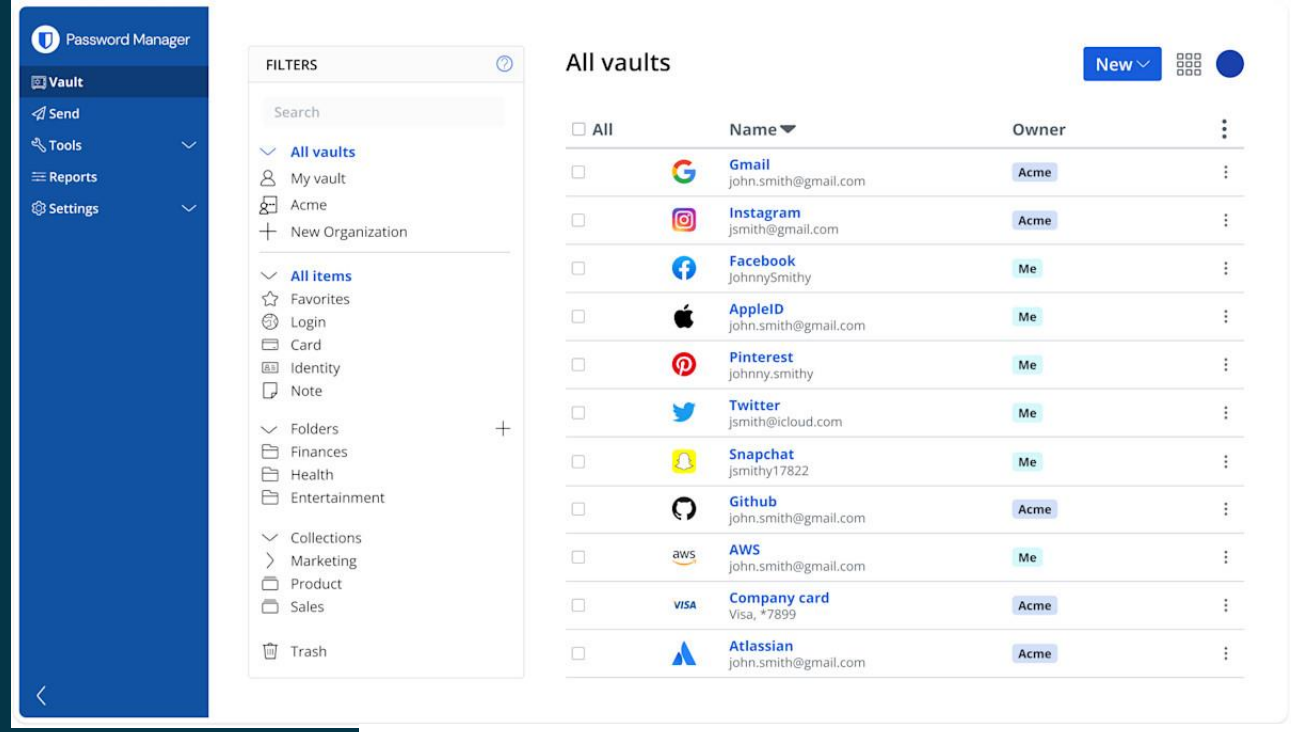
Meget sterkt password

3. #And3n35Tur2009
4. i}Q#eRlFJz6LkbUG

Hvordan lagre passord

Måter man kan lagre passord på:

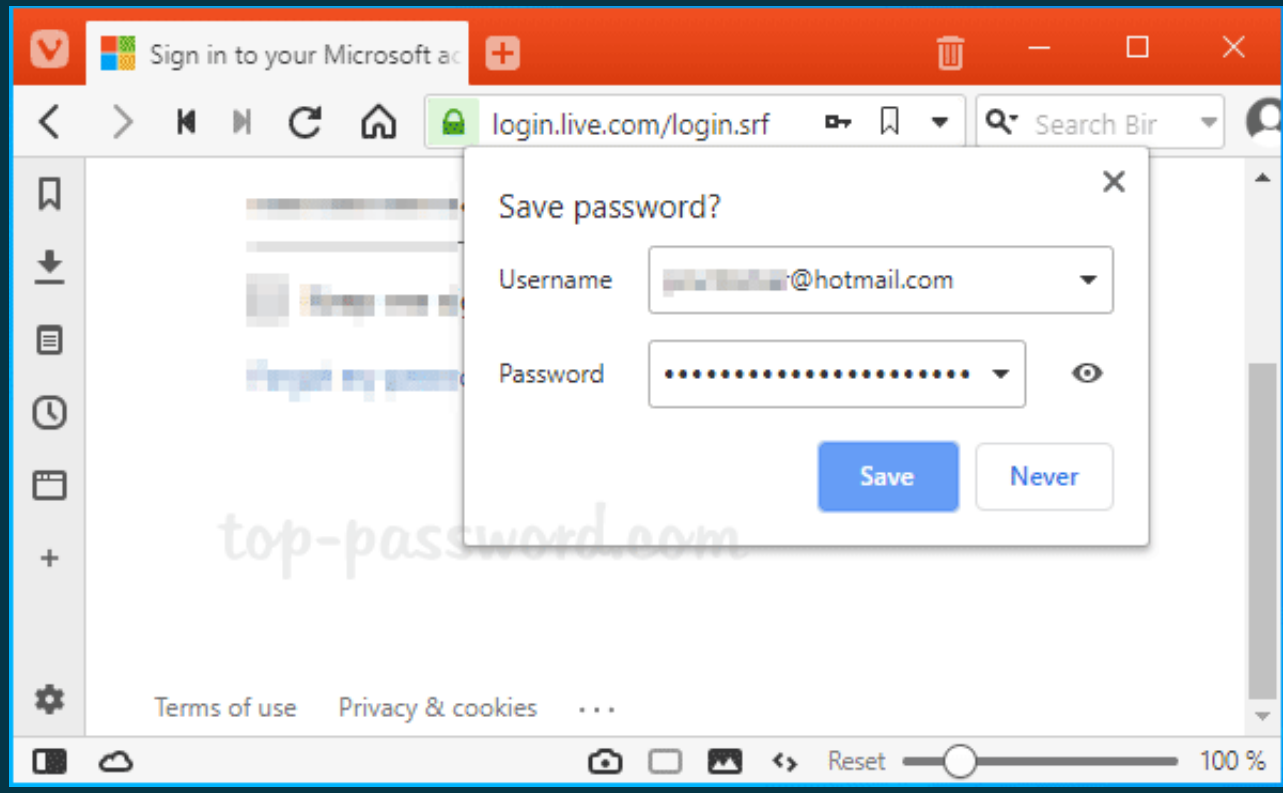
1. **Passordhvelv**
   Et passordhvelv er som en **digital safe** der du kan lagre alle passordene dine på ett sikkert sted. Du trenger bare å huske **ett hoved passord** for å åpne hvelvet. Apper som **Passwords** og **Samsungpass** for telefoner og **Password Manager** for PC.



Hvordan lagre passord

Måter man kan lagre passord på:

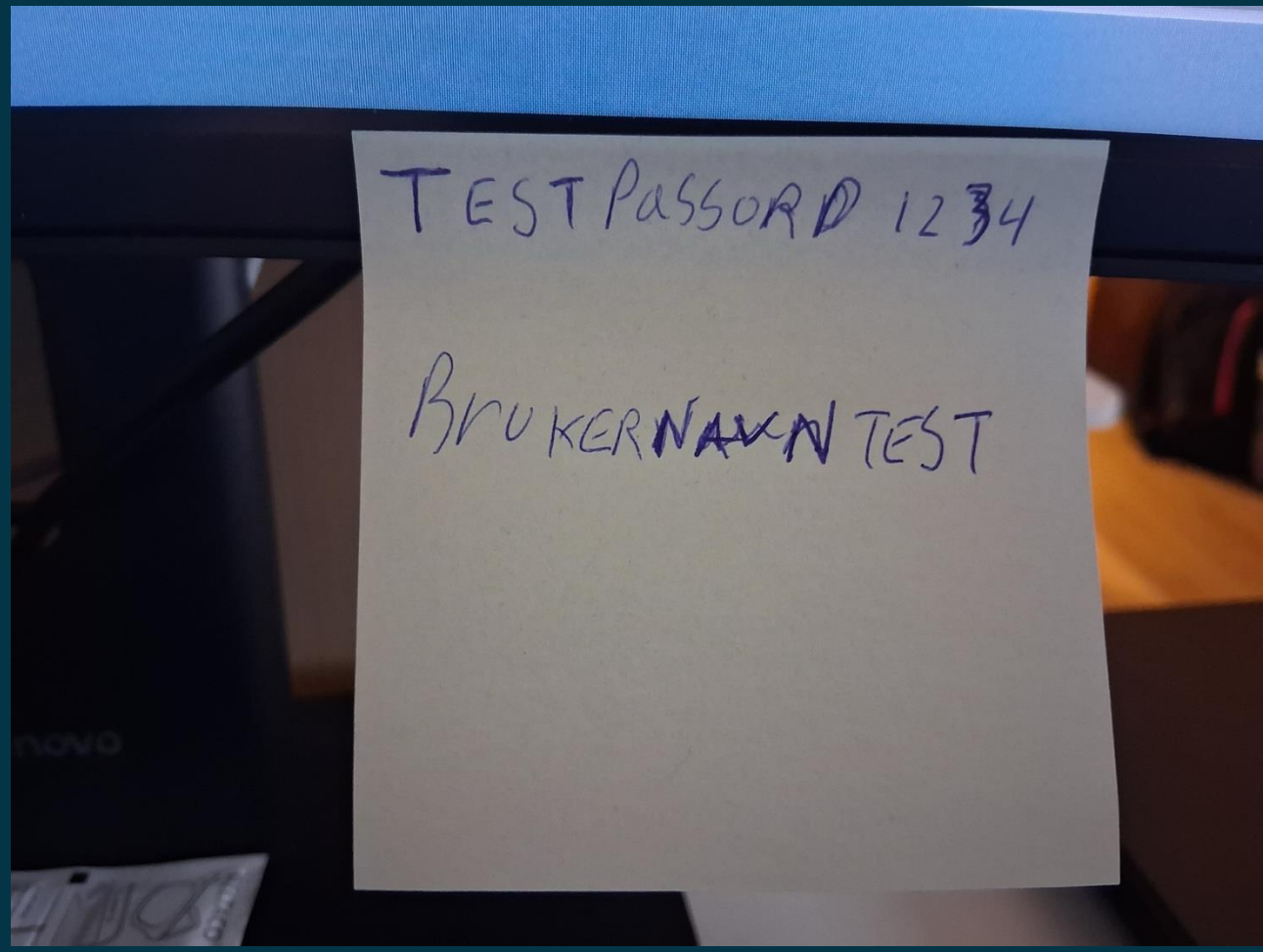
1. **Passordhvelv**
2. **I nettleseren**
   Man kan velge å lagre passordet og brukernavn til en innlogging ved å trykke **lagre** etter man har logget inn for **første gang**. Dette fører til at alt blir **automatisk ført** inn ved neste innloggings forsøk.



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.



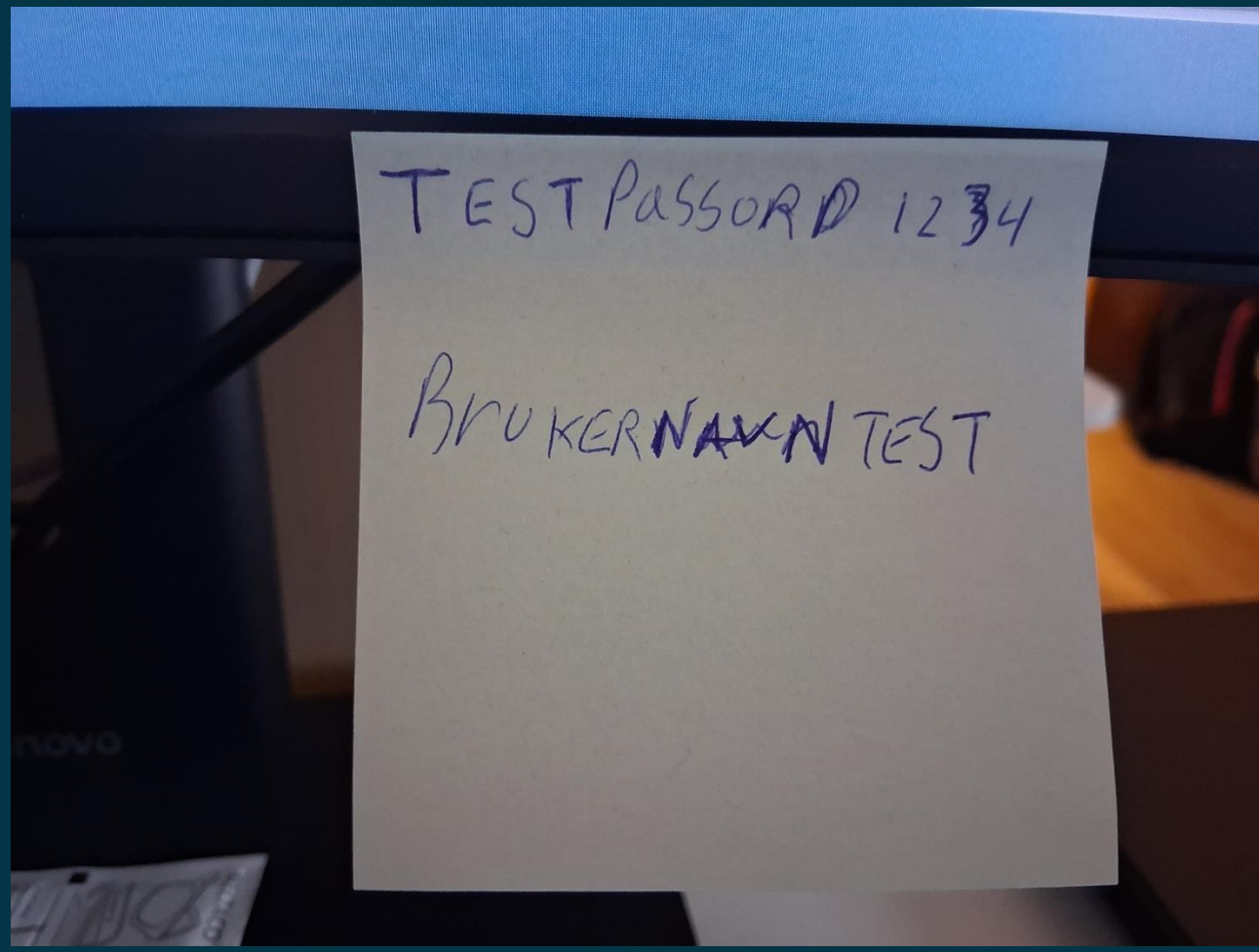
Hvordan lagre passord

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



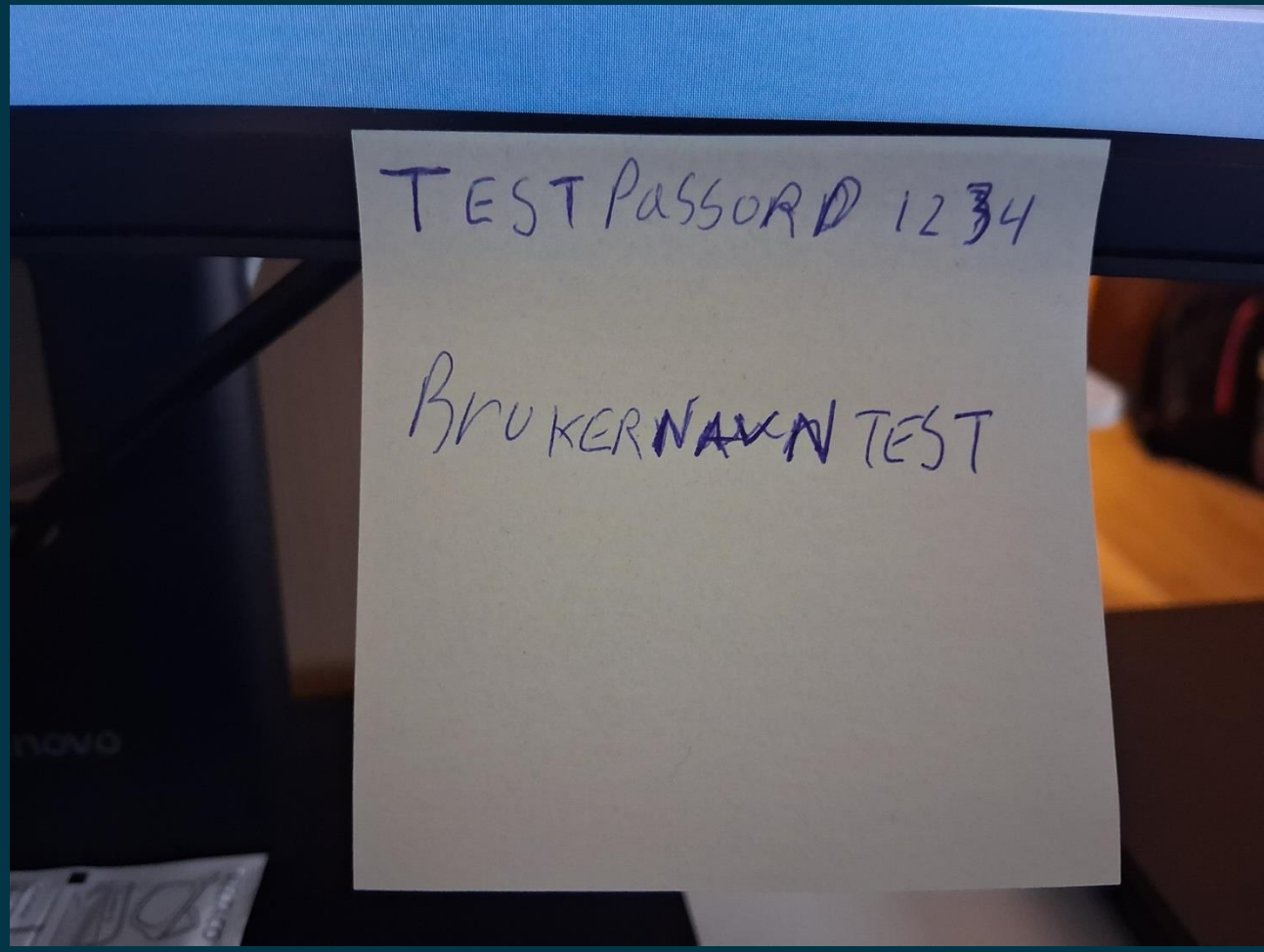
Hvordan lagre passord

Måter man kan lagre passord på:

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

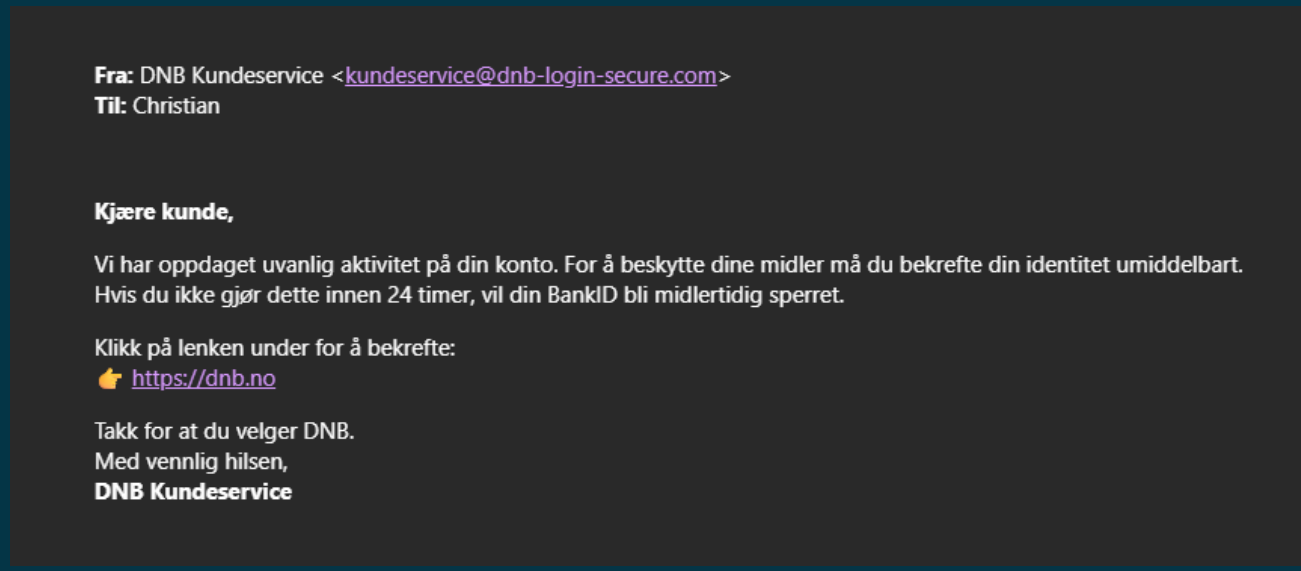
Hvordan passord ikke bør håndteres:

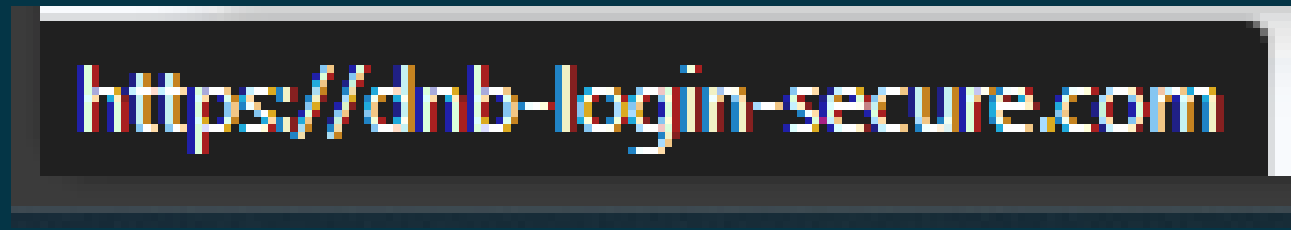
4. Bilde av passordet
5. Skrive ned passord på fysisk dokumenter



Hvordan kan du oppdage svindelforsøk

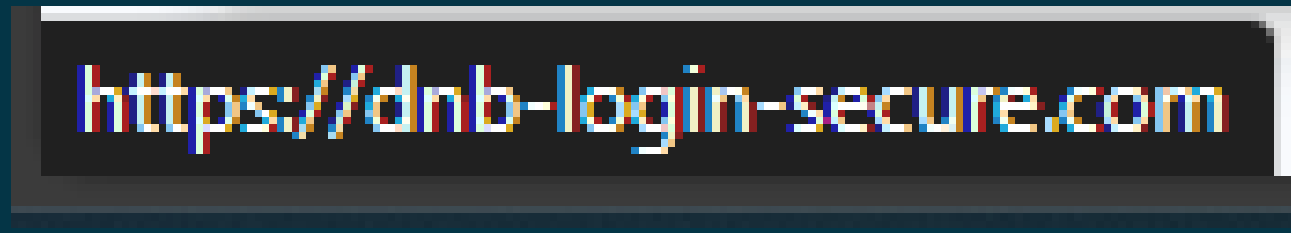
1. **Sjekk avsender og innhold**
   Svindlere bruker ofte **falske** e-postadresser som ligner på ekte, men har **små feil** (f.eks. ekstra bokstaver eller rare domener).
   Vær **skeptisk** til e-poster med **dårlig språk**, mange **skrivefeil** eller **uvanlig høflighet**.





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.



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.

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 **kjøpe 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

JUSTISDEPARTEMENTET

INTERPOL

POLITI

POLITIGENERALT

BESKYTTELSESBRIGADE FO[illegible] MINJORIGE

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.

RETNINGEN

Arne Jørgen Olafsen
politidirektør og
kriminalpolitimester.

KRIMINALPOLITI

Arne Jørgen. O

POLITIDIREKTØRATET

Eksempel svindelforsøk fra «politi» «interpol»

- Rare stavelser og skrivefeil
- Hastverk og trusler

JUSTISDEPARTEMENTET

INTERPOL

POLITI

POLITIGENERALT

BESKYTTELSESBRIGADE FOR MINJORIGE

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.

RETNINGEN

Arne Jørgen Olafsen
politidirektør og
kriminalpolitimester.

KRIMINALPOLITI

Arne Jørgen. O

POLITIDIREKTORATET

Eksempel svindelforsøk fra «politi» «interpol»

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

JUSTISDEPARTEMENTET

INTERPOL

POLITI

POLITIGENERALT

BESKYTTELSESBRIGADE FOR MINDRE ORIGE

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.

RETNINGEN

Arne Jørgen Olafsen
politidirektør og
kriminalpolitimester.

KRIMINALPOLITI

Arne Jørgen. O

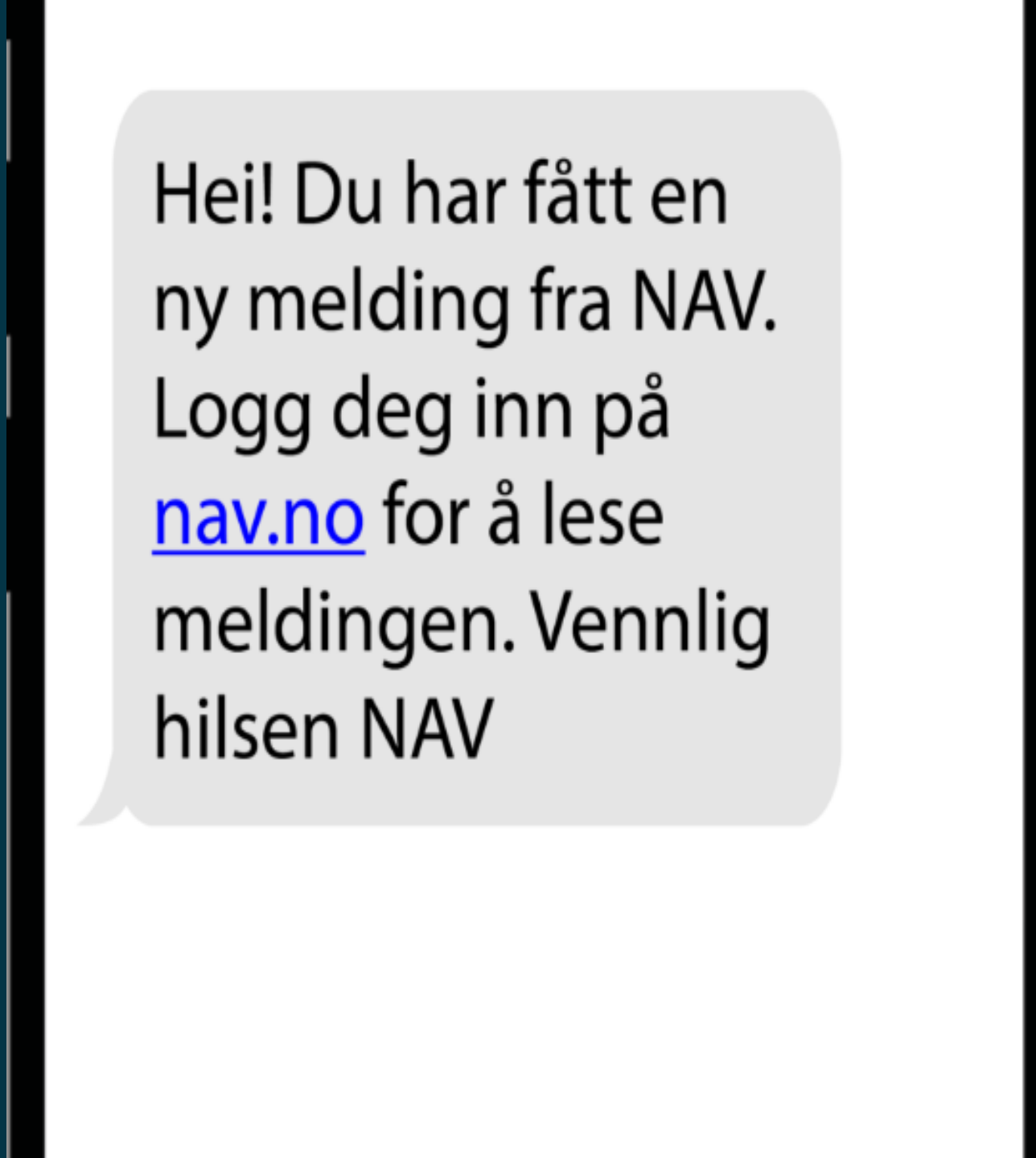
POLITIDIREKTORATET

Eksempel melding fra NAV

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

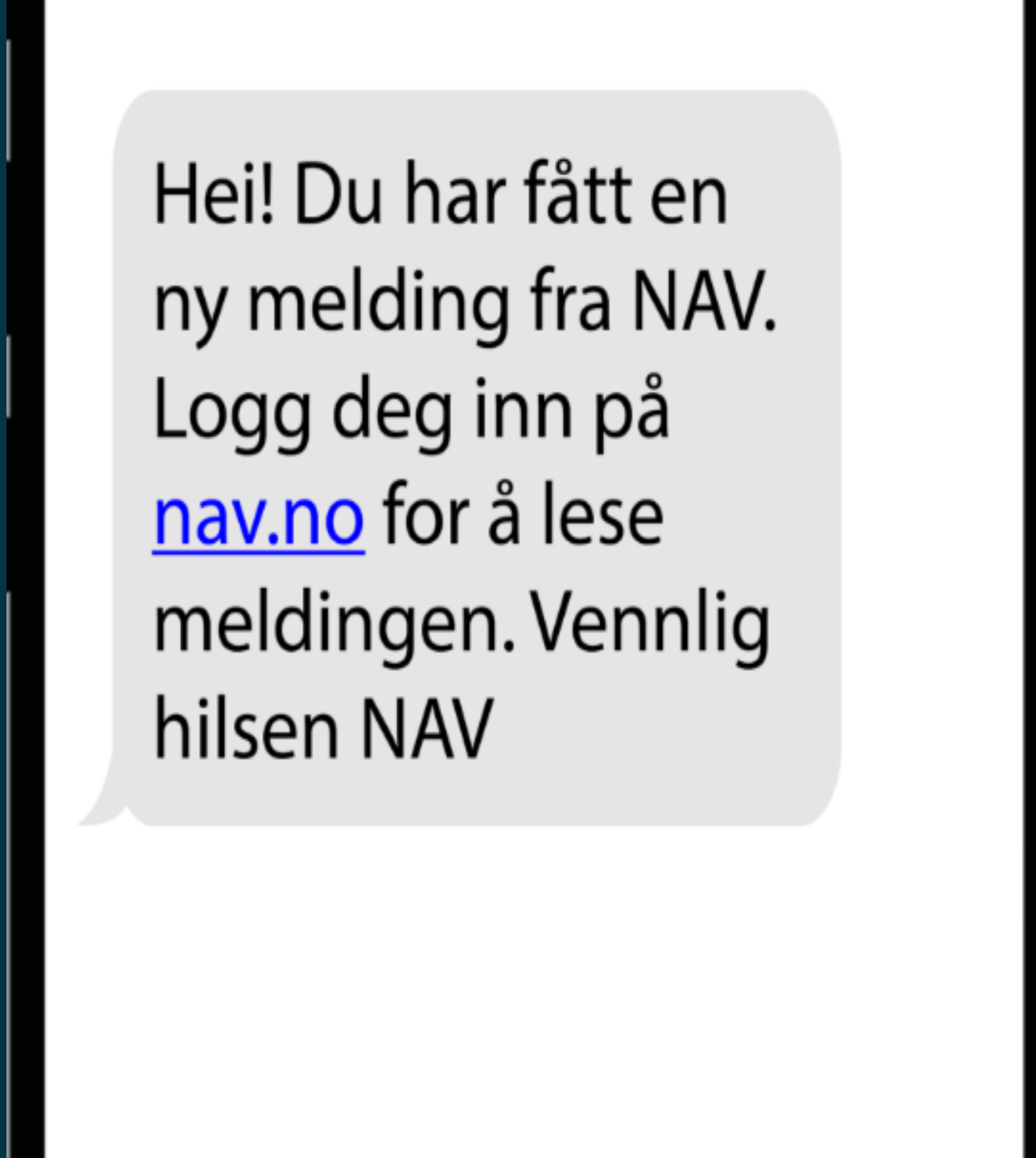
Eksempel melding fra NAV

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



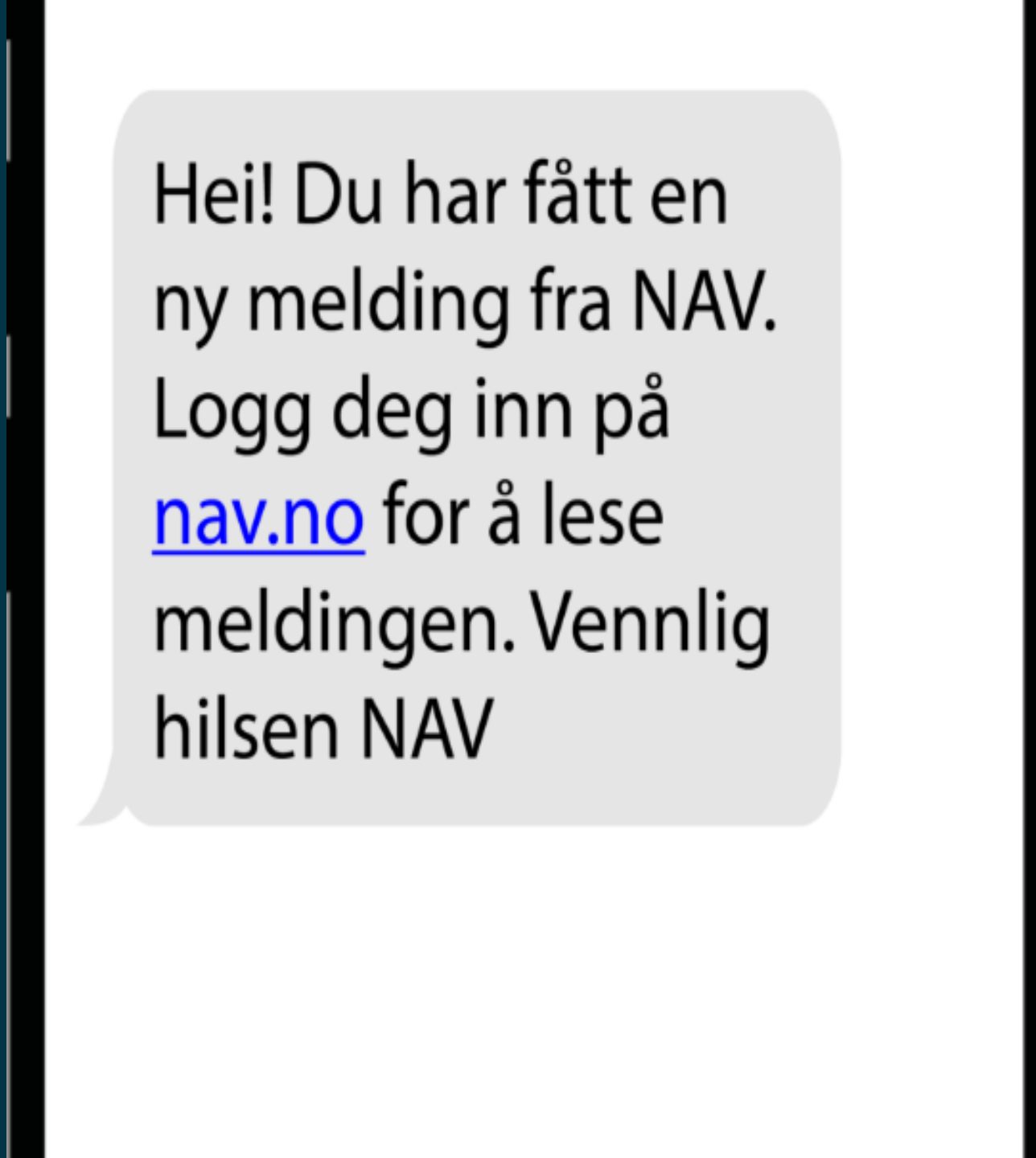
Eksempel melding fra NAV

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.



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.




Og det er dét vi svindlere spiller på.


Politiet ville aldri spurt deg om BankID.


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 kontoinform-asjon

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