

Fool Us Once, Fool Us Twice..

Hacking banks using paper forms

Cecilie Wian
Per Thorsheim

Intro

- Hacking
- Abusability
- Responsible disclosure

12.07.2024

Agenda

01

2020

02

2024

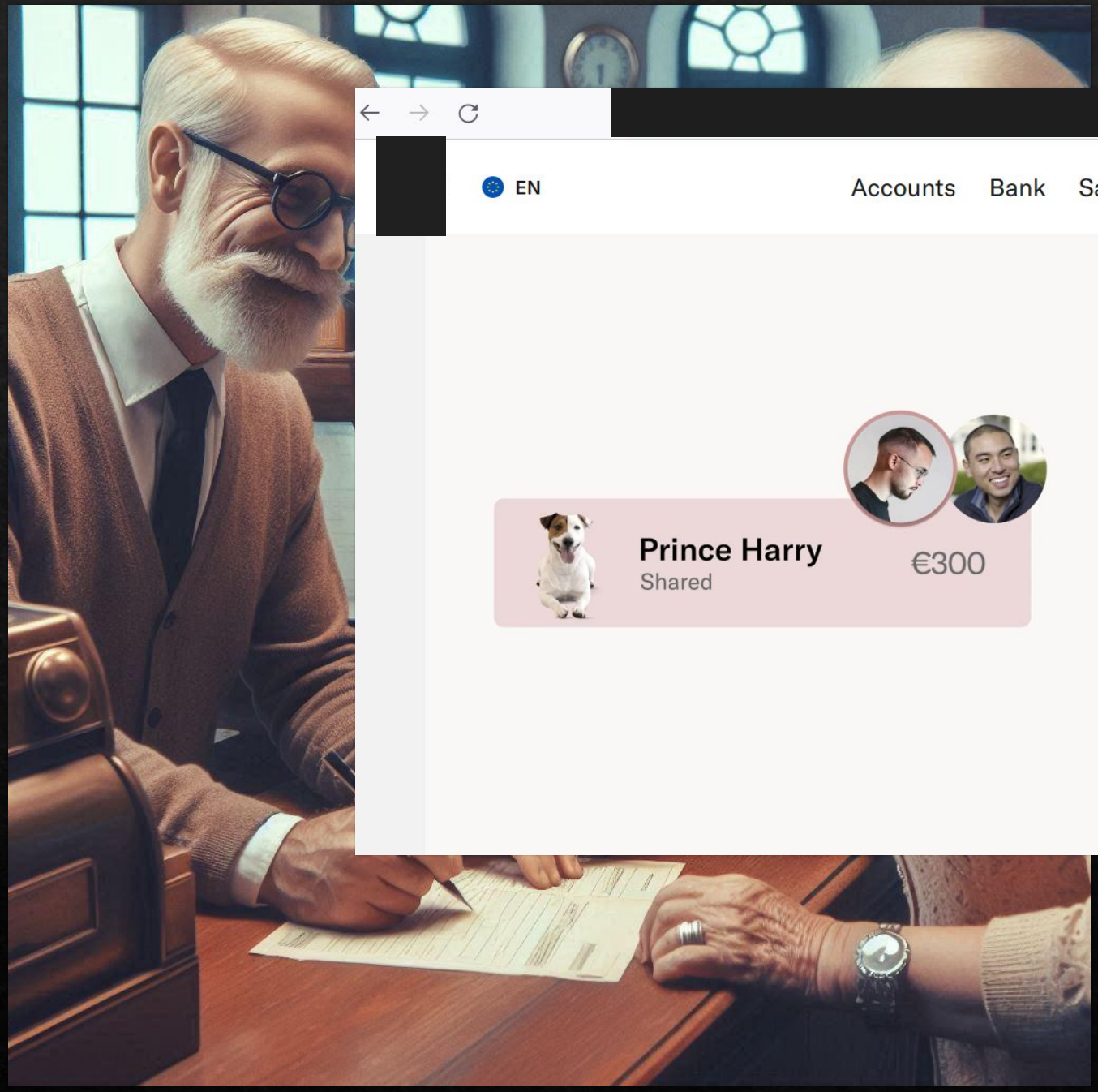
03

THE BIG PICTURE


pie
big



12.07.2024



EN

Accounts Bank Save Invest More Blog

Open Bank Account

Saving and budgeting with others, made easy

Managing household bills and everyday expenses, or simply saving up together for that dream purchase? Invite up to 10 participants to your shared sub-account, and enjoy a hassle-free way to organize money with partners, family or friends.

12.07.2024

”Do not share your BankID. Use Power of Attorney!”



TRENGER NOEN DIN HJELP? Få disposisjonsfullmakt. Da kan du i egen mobil- eller nettbank hjelpe den som har gitt deg fullmakt. Foto: DNB

Skal du hjelpe en eldre med å få utført banktjenester, få disposisjonsfullmakt.

12.07.2024

DNB 2020 - 2021

12.07.2024

DNB

Fullmakt

Disponering av konto

Det vil ta 1–2 uker før disponent er registrert på konto.

Fullmaktsgiver

Kontoeiers navn	Fødselsnummer (fødselsdato + personnummer)
	Kontonummer
Adresse	Postnummer og sted

Jeg gir fullmakt til å disponere min(e) konto(er) (som spesifisert over) i DNB Bank ASA til:

Disponentens navn	Fødselsnummer (fødselsdato + personnummer)
Adresse	Postnummer og sted

Jeg samtykker til at disponenten får innsyn i min(e) konto(er) og tilgang til å utføre alle betalingstransaksjoner fra min(e) bankkonto(er).

Disponenten vil få innsyn i kontoen(e) i egen nettbank og kan herfra betale regninger, gjøre overføringer og andre betalingstransaksjoner.

Disponenten vil også kunne se alle transaksjoner på konto tilbake i tid.

Signatur

Sted og dato	
Signatur (Kontoeier)	Signatur (Disponent)

Vi bekrefter at vi var til stede da fullmaktsgiver signerte denne fullmakten eller bekreftet sin underskrift, og at vi har skrevet under som vitner etter fullmaktsgiverens ønske.

Vi bekrefter at fullmaktsgiver er myndig, har opprettet fullmakten av fri vilje, og hadde evne til å forstå betydningen av fullmakten.

Vitnene kan ikke være ektefelle/samboer, foreldre til eller barn/barnebarn av disponenten.

Vitne 1

Signatur	
Fullt navn	Fødselsnummer (fødselsdato + personnummer)
Adresse	Postnummer og sted

Vitne 2

Signatur	
Fullt navn	Fødselsnummer (fødselsdato + personnummer)
Adresse	Postnummer og sted

0518 | 04058_DNB_cb

Grunnet personopplysningsloven må denne fullmakten returneres per post.

Det vil ta 1–2 uker før disponent er registrert på konto.

Name, address,
social security number & bank account number

Name, address & social security number of person you want to allow access to your bank account.

Signature

2 witnesses confirm the validity of the document in accordance with the wishes of the account owner. Witnesses cannot be spouse/partner, parents, kids or grandchildren of the account owner.

Fall 2020

- Name, address & pone number is usually public information
- Date of birth (6 digits) not that hard to find
- Social security number is a known algorithm, with date 6 digits + 5 digits including gender indicator (M/F)
  - Approximately 100 available for each gender per day
- Problem 1: people *STILL* believe it is a secret
- Problem 2: it is still used as a secret (!)

But is it really a secret?





Obtaining the bank account number

- Financial Supervisory Authority of Norway: *it is not a secret*
- Postoppkrav (pay on delivery)
- Social engineering

DNB

Fullmakt

Disponering av konto

Det vil ta 1–2 uker før disponent er registrert på konto.

Fullmaktsgiver

Kontoeiers navn	Fødselsnummer (fødselsdato + personnummer)
	Kontonummer
Adresse	Postnummer og sted

Jeg gir fullmakt til å disponere min(e) konto(er) (som spesifisert over) i DNB Bank ASA til:

Disponentens navn	Fødselsnummer (fødselsdato + personnummer)
Adresse	Postnummer og sted

Jeg samtykker til at disponenten får innsyn i min(e) konto(er) og tilgang til å utføre alle betalingstransaksjoner fra min(e) bankkonto(er).

Disponenten vil få innsyn i kontoen(e) i egen nettbank og kan herfra betale regninger, gjøre overføringer og andre betalingstransaksjoner.

Disponenten vil også kunne se alle transaksjoner på konto tilbake i tid.

Signatur

Sted og dato	
Signatur (Kontoeier)	Signatur (Disponent)

Vi bekrefter at vi var til stede da fullmaktsgiver signerte denne fullmakten eller bekreftet sin underskrift, og at vi har skrevet under som vitner etter fullmaktsgiverens ønske.

Vi bekrefter at fullmaktsgiver er myndig, har opprettet fullmakten av fri vilje, og hadde evne til å forstå betydningen av fullmakten.

Vitnene kan ikke være ektefelle/samboer, foreldre til eller barn/barnebarn av disponenten.

Vitne 1

Signatur	
Fullt navn	Fødselsnummer (fødselsdato + personnummer)
Adresse	Postnummer og sted

Vitne 2

Signatur	
Fullt navn	Fødselsnummer (fødselsdato + personnummer)
Adresse	Postnummer og sted

0518 | 04058_DNB_cb

Grunnet personopplysningsloven må denne fullmakten returneres per post.

Det vil ta 1–2 uker før disponent er registrert på konto.

Name, address,
social security number & bank account number?
<insert victim here>

Name, address & social security number of person you want to allow access to your bank account.
<insert money mule here>

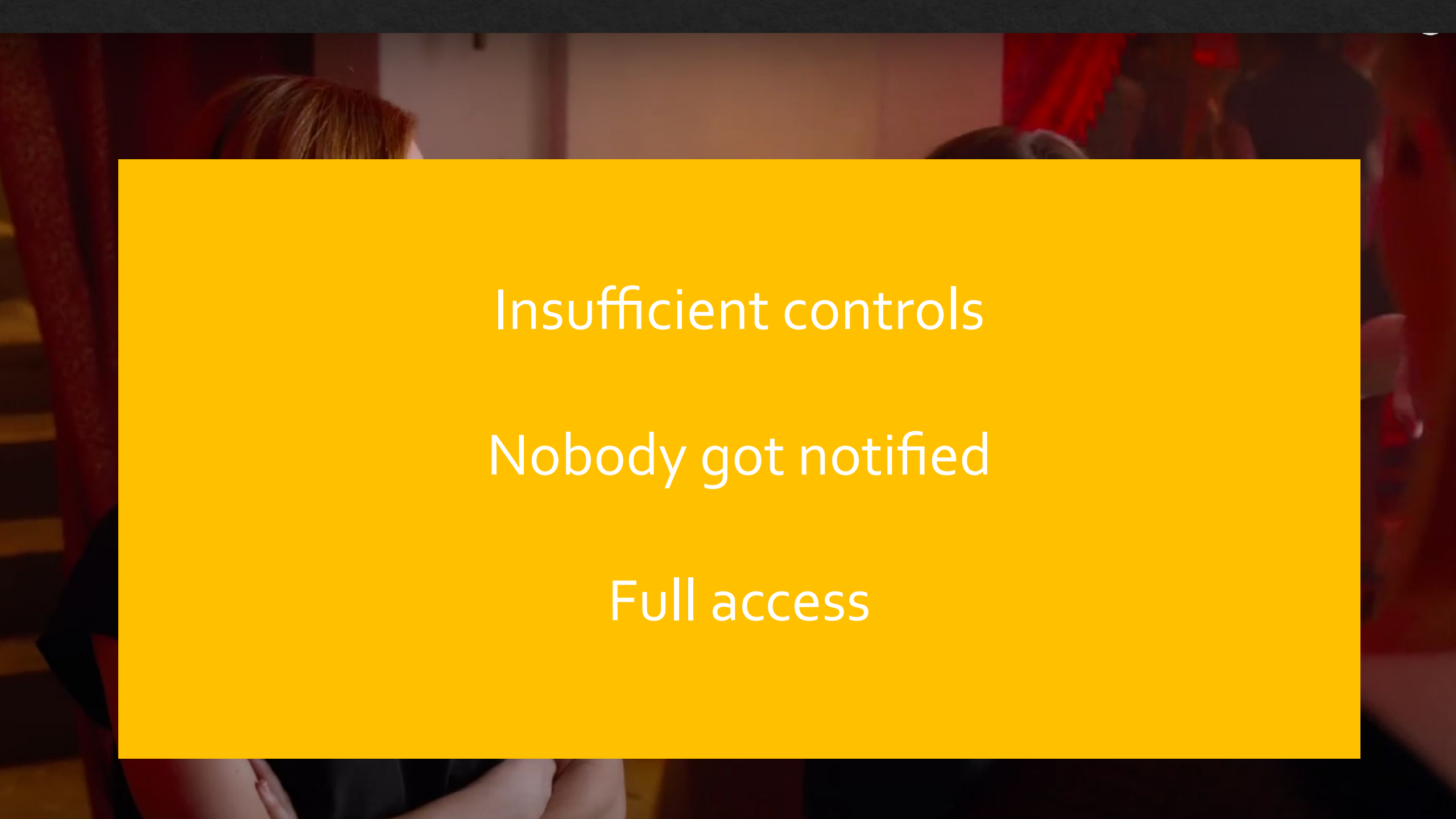
Signature on paper?
Uh, ok, but does anyone check them anymore?

2 witnesses confirm the validity of the document in accordance with the wishes of the account owner. Witnesses cannot be spouse/partner, parents, kids or grandchildren of the account owner.
(Can witnesses be held accountable?)

Fill out, and (slow)mail it

12.07.2024




Insufficient controls
Nobody got notified
Full access


JACKPOT!

DNB

Dagligbank og lån | Pensjon og forsikring | Sparing og investering | Innstillinger | 18 | Logg ut

Min totaloversikt

Eiendeler

Skjul alle

Innskudd 9

Kontonavn	Kontonummer	Disponibel saldo	Bokført saldo
Regningskonto		3	3
		8	8
		8	8
		2	2
		8	8
Brukskonto		0	0

Sum eiendeler 9

Lån og kreditter

Skjul alle

Kreditter

Kredittkort	Kortnummer	Kredittgrense	Saldo
Pluss Mastercard	**** **** ***		

Sum lån og kreditter

Andre oppføringer

Skjul alle

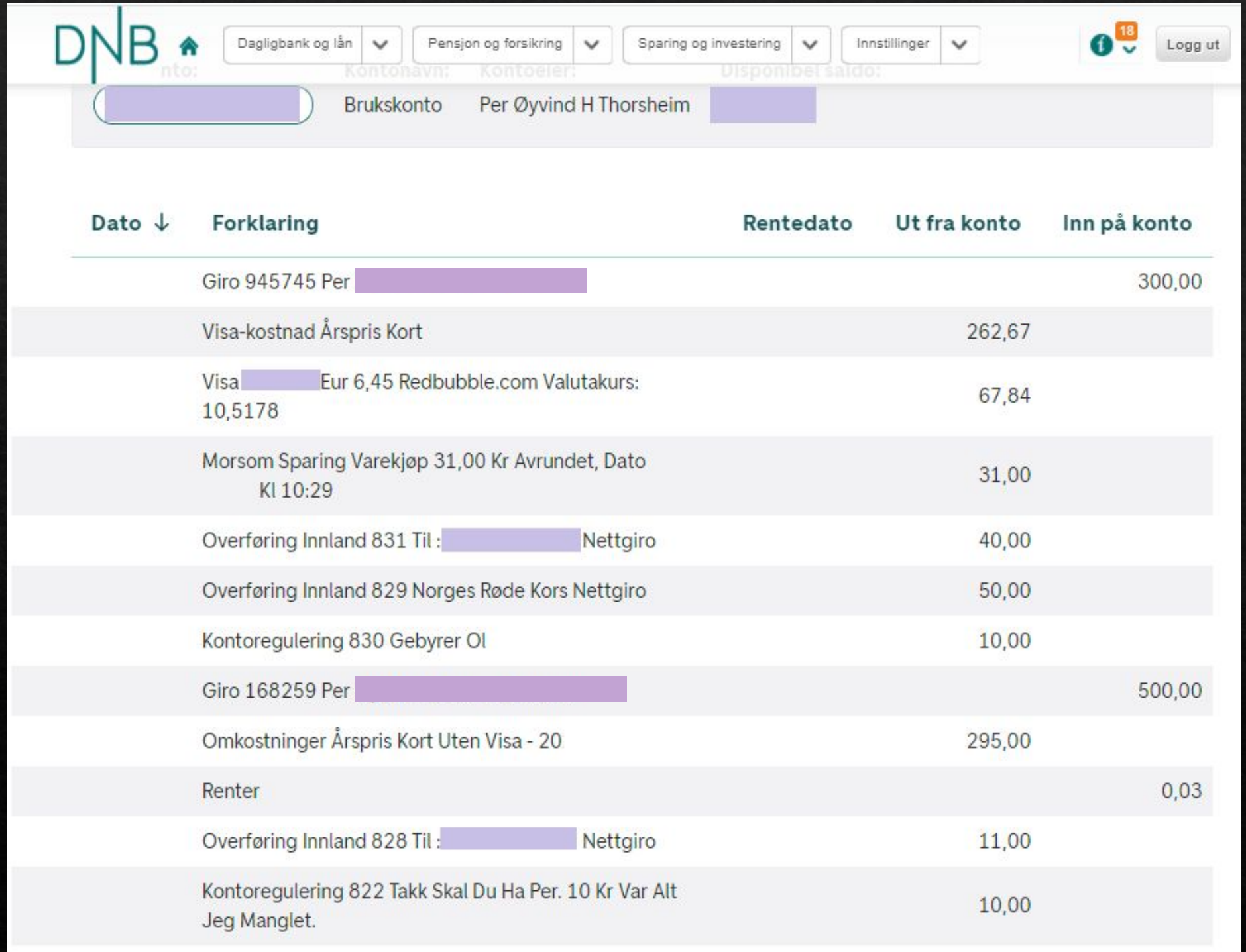
Kontoer du disponerer 43,59

Kontonavn (eier)	Kontonummer	Disponibel saldo	Bokført saldo
Brukskonto (Per Thorsheim)	0540.5	43,59	43,59

Innlogget som

Linn Cecilie Wian

Det er **1 uke og 12 t** siden siste besøk



Hvilke av disse transaksjonen har jeg gjort?

Ser du forskjellen mellom meg, eier og banken?

”What did the manager do?!”

DNB (2020)

- Any and all transactions is made to look like the account owner did them
- Customer service said they could not help / see any difference

10 years of transaction history

What did you spend money on over the past 10 years?

Think about it.

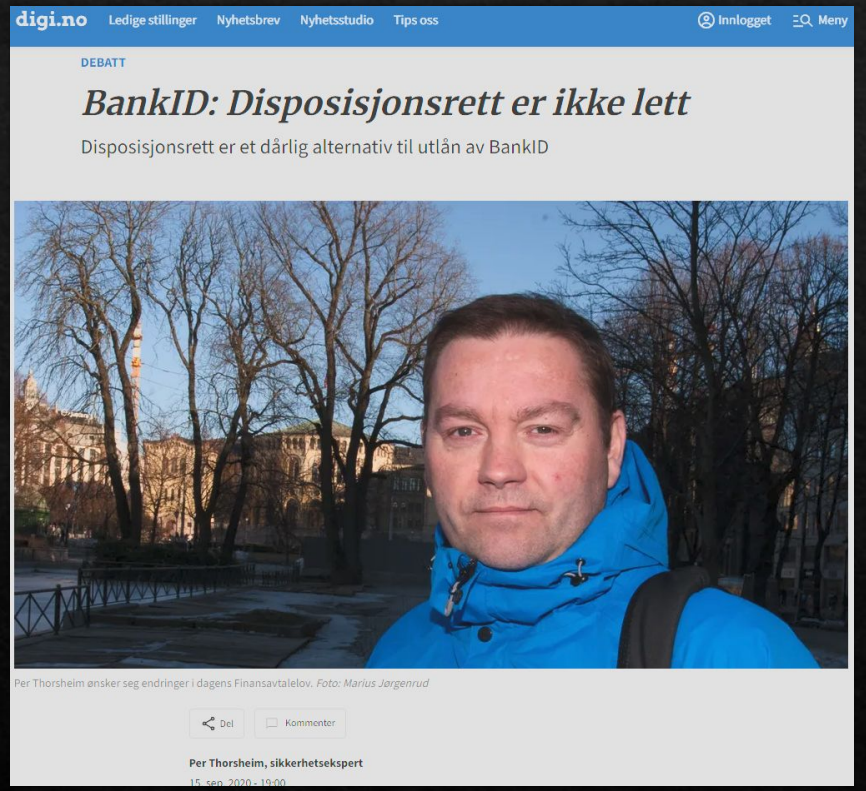
12.07.2024

What did the account manager do?

DNB (2020)

- All transactions are shown as they were carried out by the account owner, not the manager
- Customer service said they couldn't help, and they couldn't see anything else then we did

Letter to the editor at digi.no, Sep 15, 2020



digi.no Ledige stillinger Nyhetsbrev Nyhetsstudio Tips oss Innlogget Meny

DEBATT

BankID: Disposisjonsrett er ikke lett

Disposisjonsrett er et dårlig alternativ til utlån av BankID

Per Thorsheim ønsker seg endringer i dagens Finansavtalelov. *Foto: Marius Jørgenrud*

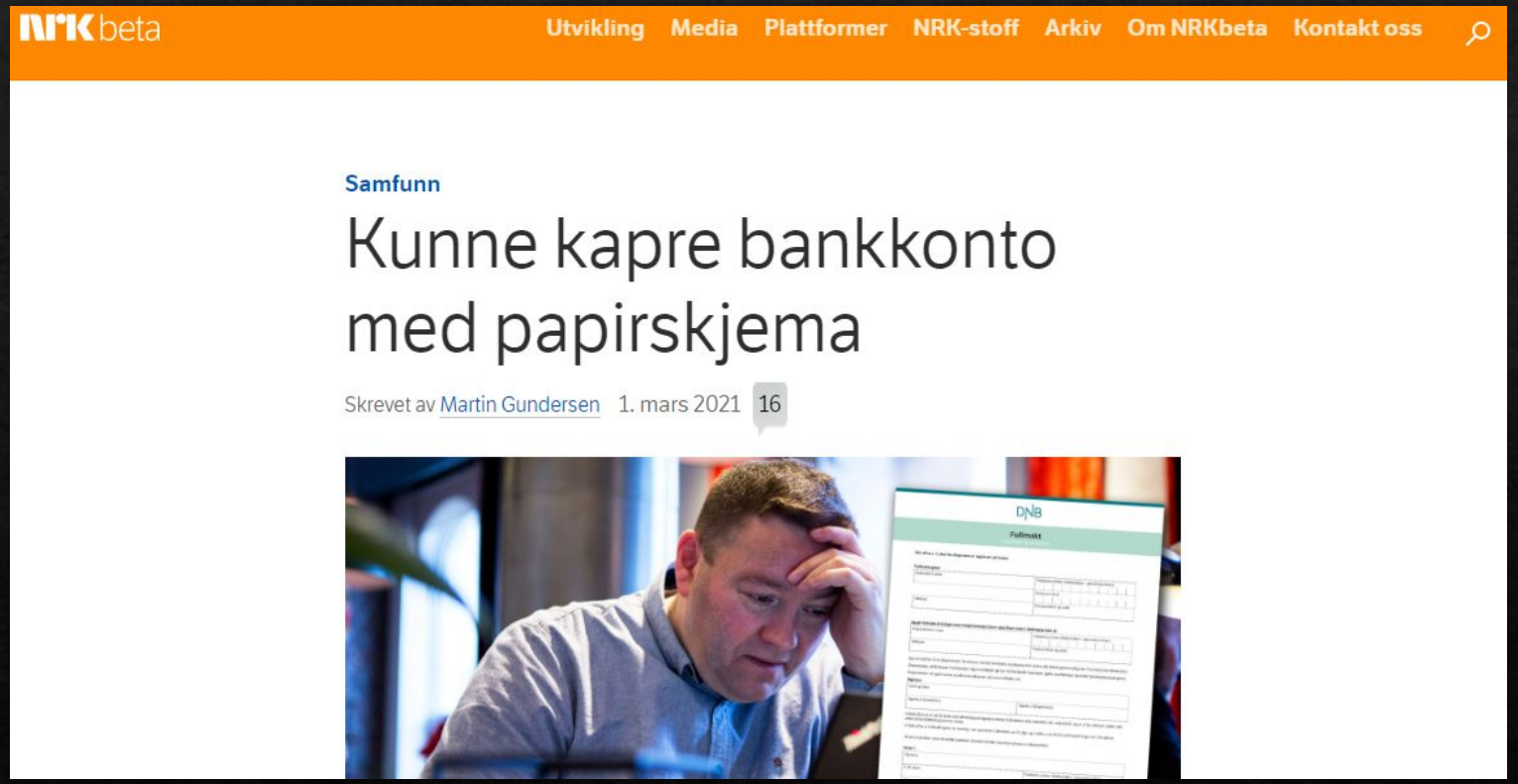
Del Kommenter

Per Thorsheim, sikkerhetsekspert

15. sep. 2020 - 19:00

12.07.2024

News article March 1st, 2021



Storebrand bank - 2024

12.07.2024



More paper!
Terrible paperforms – obvious afterthought
No control

- So we tried again



Bevegelser

NOK - Bufferkonto

Siste 6 måneder | eller dato fra | til

Dato	Type	Tekst	Beløp	Saldo
01.02.2024		*Årsgebyr*	-10,00	18,67
01.02.2024			-30,00	28,67

Tekst: Girobetaling 50100547500. Betalingsdato 01-02-2024
Beløp: -30,00 NOK
Fra konto: NOK - Bufferkonto
Mottakerkonto:
Opprettet den: 01.02.2024
Bokført den: 01.02.2024
Rentedato: 02.02.2024
Disposisjonsdato: 01.02.2024
Bankens referanse: 9699074277
Beskjed fra betaler: takk
Avsender/Mottaker: Per Øyvind Hervik Thorsheim
Løvåsbakken 37
5145 Fyllingsdalen
Signert av brukernavn: Linn Cecilie Wian
Signert av brukernummer:
Serviceavtale:

12.07.2024

What did the manager do?

DNB (2020)

- Any and all transactions is made to look like the account owner did them
- Customer service said they could not help / see any difference

Storebrand bank (2024)

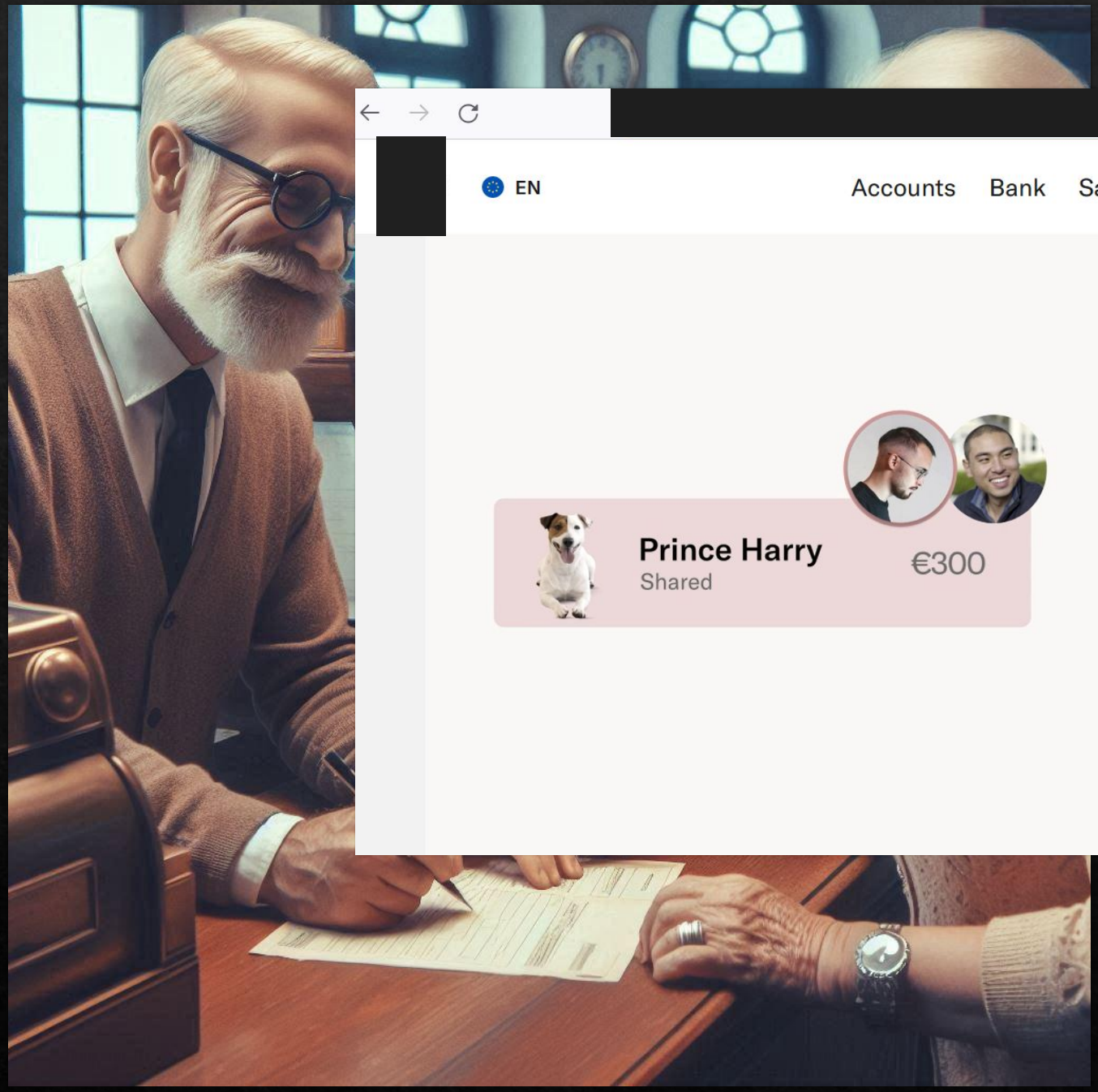
- Transaction logs shows activity from account owner and manager

The good:

The name of who did the transaction is visible for the owner of the account! <3

The bad:

This is the only bank we have seen showing the name of who did the transaction.



EN

Accounts Bank Save Invest More Blog

Open Bank Account

Saving and budgeting with others, made easy

Managing household bills and everyday expenses, or simply saving up together for that dream purchase? Invite up to 10 participants to your shared sub-account, and enjoy a hassle-free way to organize money with partners, family or friends.

12.07.2024

The really bad:

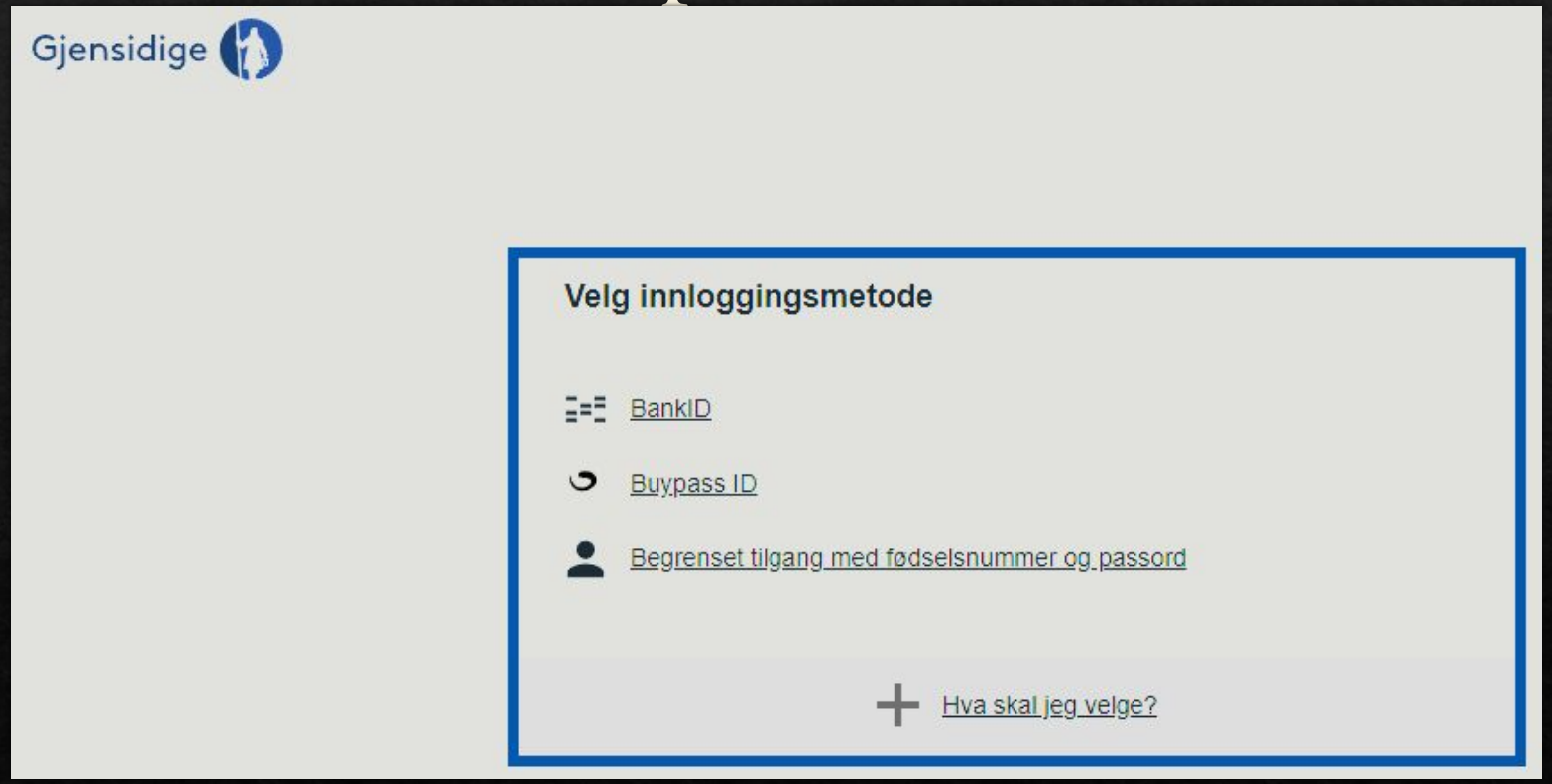
Protecting yourself from fraud of this type, or scams from trusted close ones, is pretty much impossible

How to prevent fraud of this kind?

Power of attorney or joint account:

- Notify me ahead of granting anyone access to my account!
- Who did what is minimum of information that should be available
- Transaction limits and co-signing for bigger amounts

Diversity is good!
Bank/Insurance corp provide several ID options



Thank you!

Q&A

cecilie.wian@bouvet.no

per@thorsheim.net