Hacking a bank using a paper form.

Per Thorsheim
CISA, CISM, CRISC
Security & Governance Manager BankID

Twitter: @thorsheim

vipps

20:46

Tweet

Per Thorsheim @thorsheim · 19 m

Got a reputation to maintain.

I have it verbally from @CormacHerley, with a witness present, that he's interested in passwords while I'm obsessed with it.

Cormac: please confirm statement? :-D

2

Cormac Herley
@CormacHerley

Svar til @thorsheim og @spazef0rze

Confirm. I have a healthy curiosity, while @thorsheim is pathologically obsessed.

Oversett fra engelsk

02.01.2018, 20:42

Background

1. «Everyone» does online banking in Norway
2. Vast majority uses mobile banking (dedicated apps)
3. BankID is used by «everyone» for authentication & electronic signatures

- And not just for banking, but in contact with government, insurance, health & much more

Situation: Not everyone is online

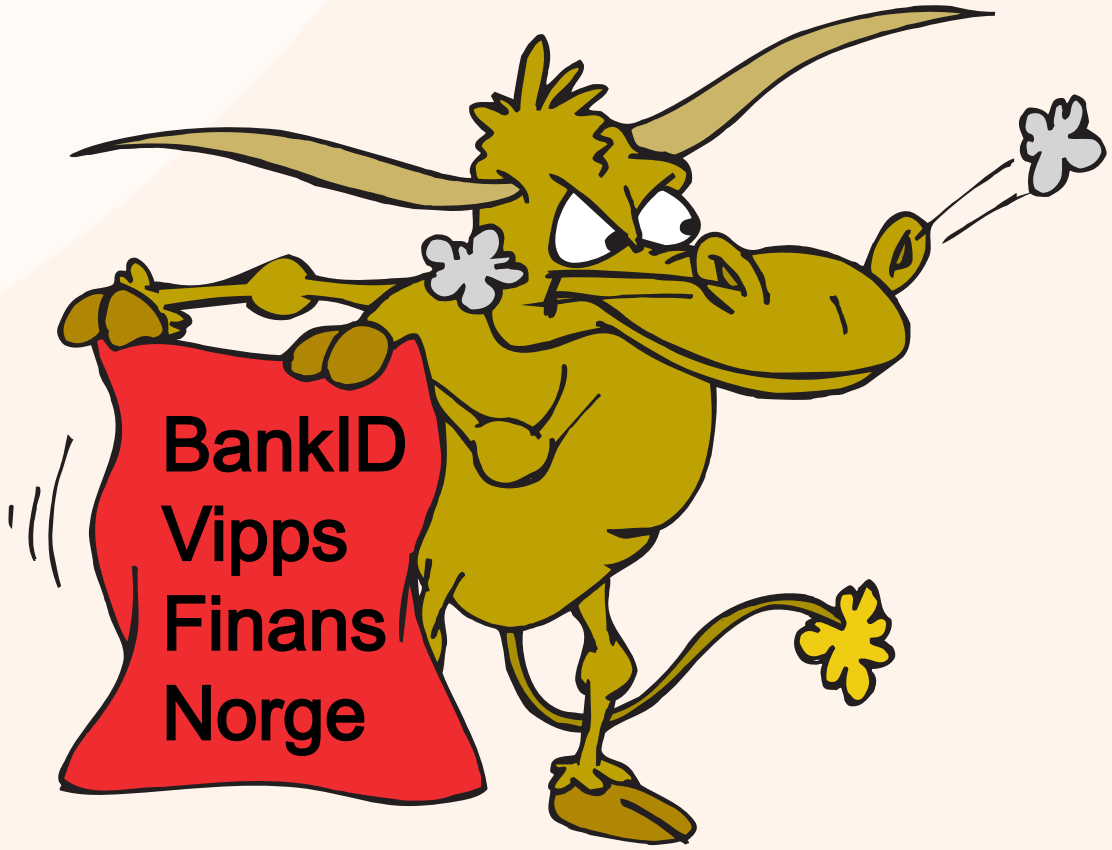
Do not share your BankID.
Use «disposisjonsrett» instead.

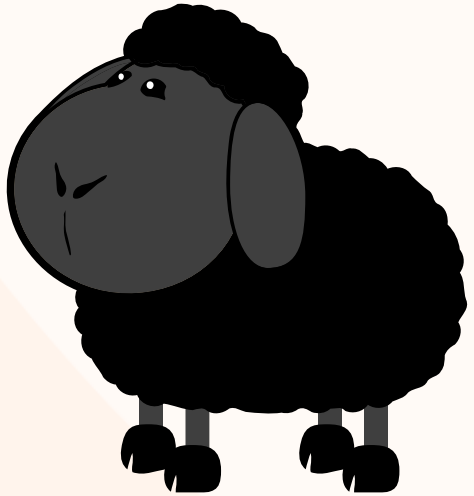
Danish: Fuldmakt
English: Power of attorney

Never share your OTP.

Never share your password.

And to me this was like…





Per

The person you give access to must already be a customer of DNB. (?)

DNB

Dagligbank og lån | Pensjon og forsikring | Sparing og investering | Innstillinger

Registrere ny disponent

Til informasjon

- Dersom ny disponent allerede er kunde hos oss, vil personen automatisk få tilgang til kontoen din i sin egen nettbank.
- Dersom ny disponent ikke er kunde i DNB, må personen først bli det via dnb.no eller på et av våre bankkontor.
- Er du under 18 år kan du ikke legge til disponenter i nettbanken.

Skriv ut

1 Ny disponent | 2 Oppsummering | 3 Kvittering

Kvittering 21.08.2020 kl 18:36

Kontonummer:	0540
Fødselsnummer:	0510
Disposisjonsforhold:	Hver for seg

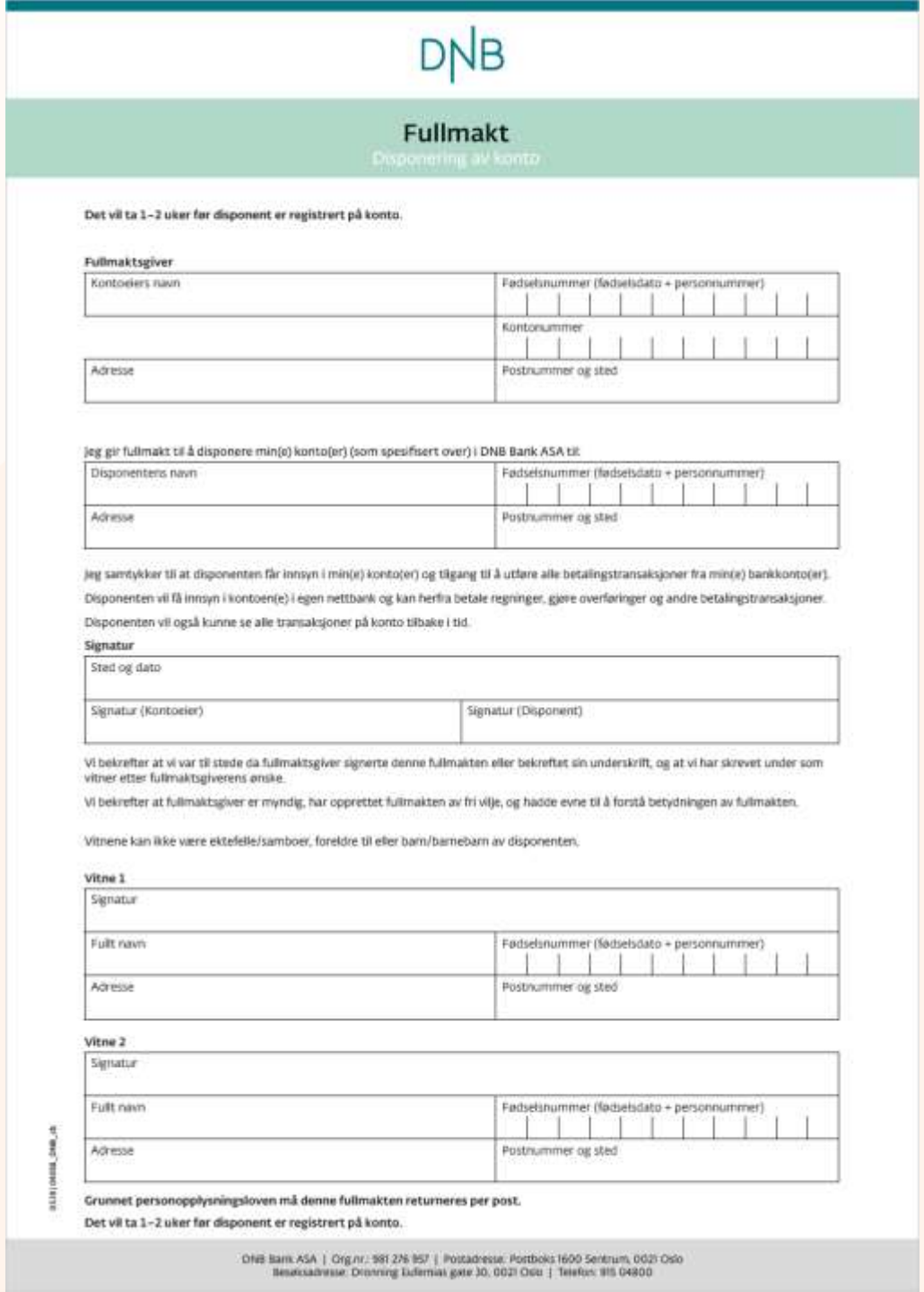
Til Disponenter

Tips

Disposisjonsforhold - Hver for seg:
Kontoeier og disponent kan disponere kontoen uavhengig av hverandre.

Configuring «Power of Attorney»

1. Login & assign access using BankID
2. Fill out paper form & send by postal mail



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

Grunnet personopplysningsloven må denne fullmakten returneres per post.

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

DNB Bank ASA | Org.nr.: 981 276 857 | Postadresse: Postboks 1600 Sentrum, 0021 Oslo
Besøksadresse: Dronning Eufemias gate 30, 0021 Oslo | Telefon: 915 04800

Name, address, social security number & bank account number? Not really a secret. <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?)

Obtaining your Norwegian social security number

1. Never ment to be a secret
2. Public algorithm, 11 digits, DOB + 5
3. 100971XXXXX
   Gender indicator
   Men: Odd
   Women: Even
4. Find victim DOB, generate possible numbers, find a service that will validate number candidates.

HOWTO: validate Norwegian social security numbers

This space contains no names or logos, in order to protect those who didn’t do proper rate limiting, allowed unauthenticated verification & data enrichment of random norwegian social security numbers. Let’s just refer to them as:

Obtaining your bank account number

1) Finanstilsynet: it is not a secret
2) Postoppkrav (cash on delivery)
3) Social engineering

2 types of security questions

«Static» Security Questions

- Mothers maiden name
- Name of first pet
- Name of first school

- **Doesn’t change**
- **Google it!**

«Dynamic» Security Questions

- Name someone you made a payment to during last few days
- How much money do you have in account X?

- **Answers are not fixed**
- **But is the entropy good enough?**

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 ovenfor)

Disponentens navn	
Adresse	

	Fødselsnummer (fødselsdato + personnummer)
	Postnummer og sted

Grunnet personopplysningsloven må denne fullmakten returneres per post.

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

DNB Bank ASA | Org.nr.: 981 276 857 | Postadresse: Postboks 1600 Sentrum, 0021 Oslo
Besøksadresse: Dronning Eufemias gate 30, 0021 Oslo | Telefon: 915 04800

So we completed the form and sent it to the bank on Tuesday afternoon, and then we waited.

Name

...sses 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?)

1. Insufficient controls
2. Nobody got notified
3. Full access

«Disposisjonsrett» is not standardized

- Legal agreement
- Order process, overview, changes, use, logging, alerting & removal of access
- End of agreement: 31.12.9999
- Other persons access not visible in main screen of web/app bank

HOWTO FIX

vopps

TIME

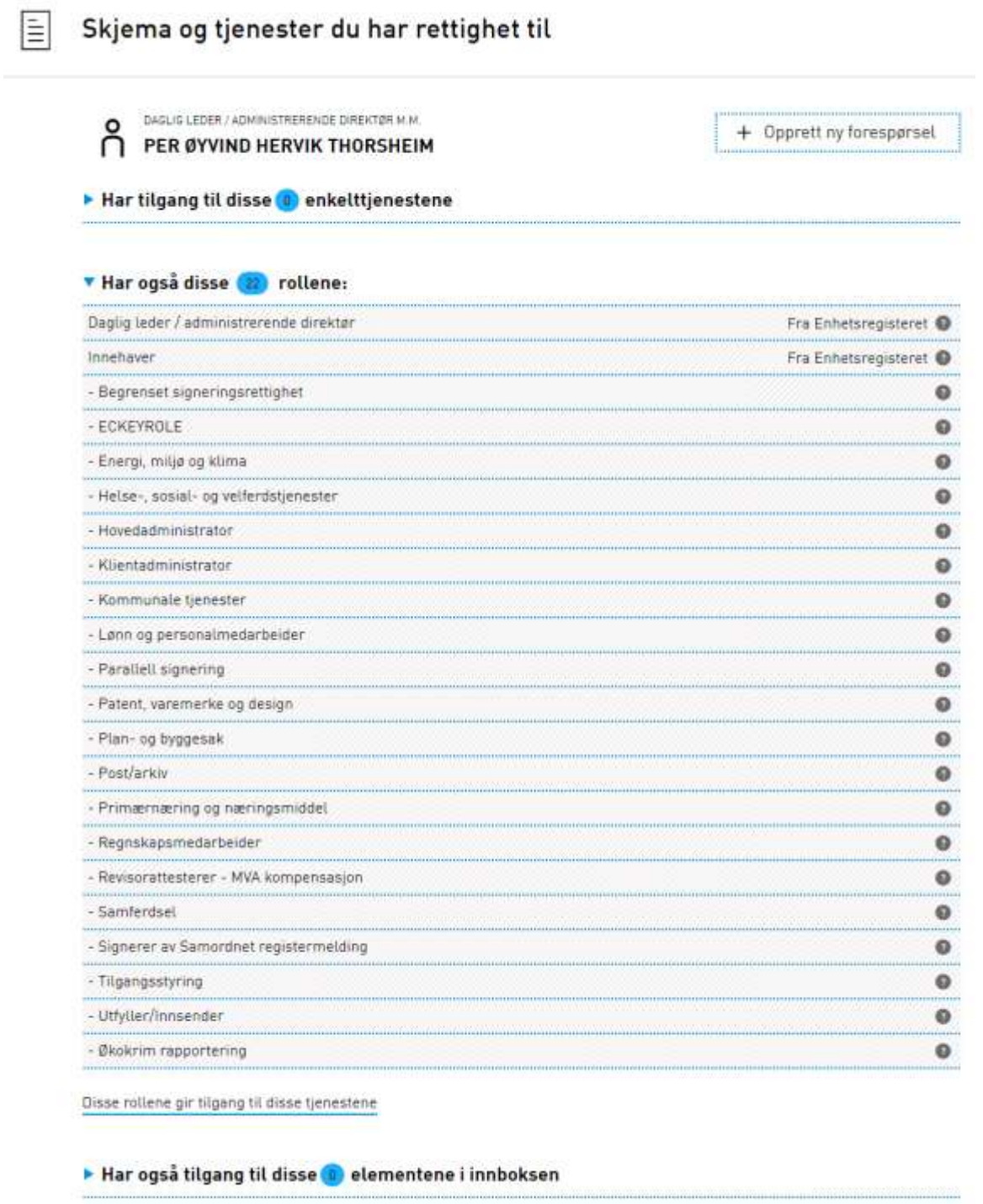
Using time to our advantage, and
to the disadvantage for criminals.

Granularity

«Disposisjonsrett» currently offers no granularity at all.

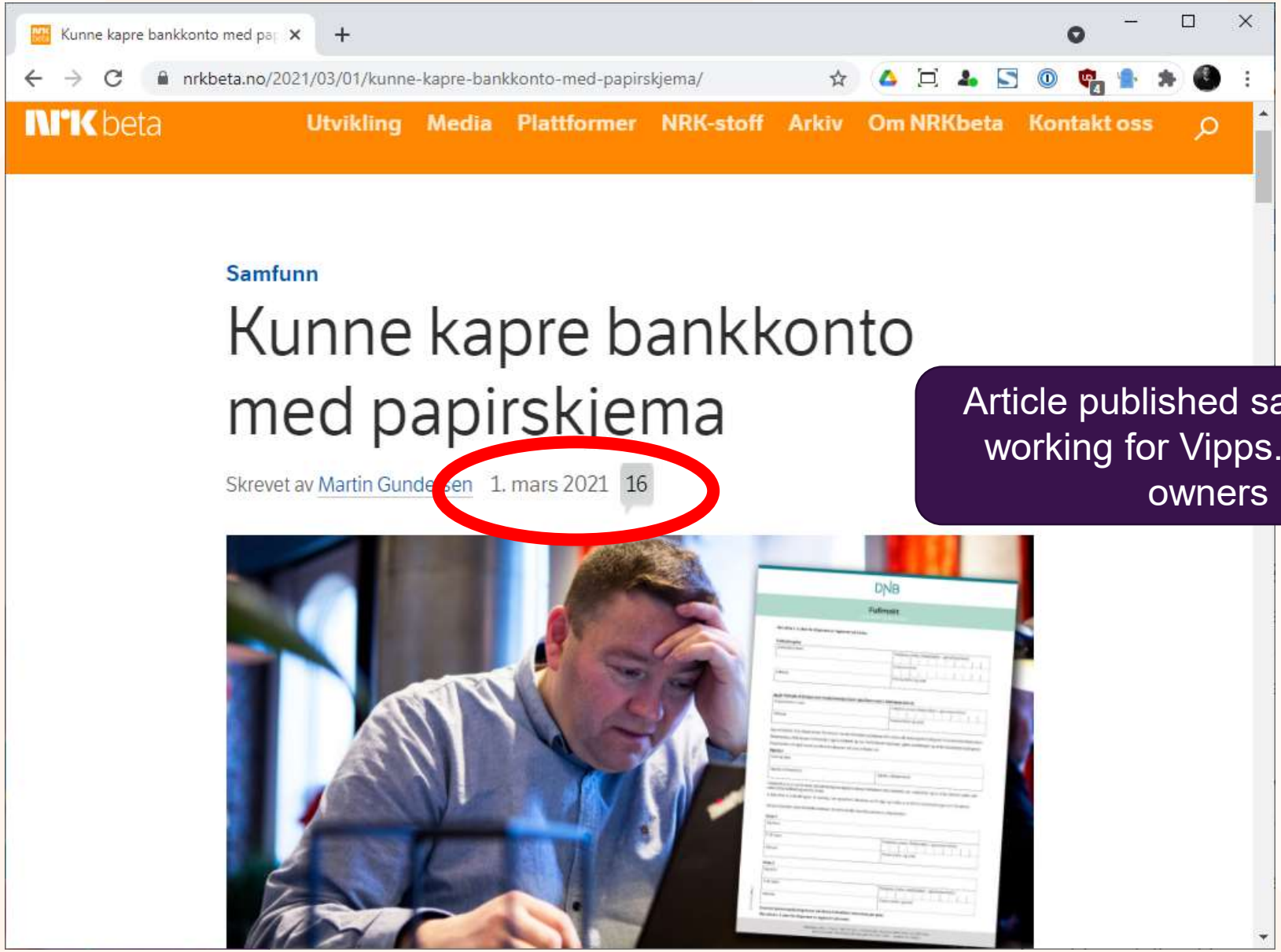
Either you give full access, or no access.

(Finans Norge is – afaik – working on something)



Responsible (coordinated) Disclosure

(Don’t be evil)



Article published same day as I started working for Vipps. DNB is one of the owners of Vipps.

https://nrkbeta.no/2021/03/01/kunne-kapre-bankkonto-med-papirskjema/

A question nobody asked:

«Why did you go to the media with this?»

Additional takeaways:

1. 90 days to fix (Google) + 30 days before details are released
2. Growing industry: bug bounty programs
3. ISO 29147 – Vulnerability Disclosure
4. ISO 30111 – Vulnerability handling processes

Security

Vipps.no/security

vipps

Vipps Mobil | Produkter og tjenester | Hjelp | Logg inn

Vipps and security

We are continually working with the security in our solutions. Input and reports from our users and security specialists are important contributions in our work. Thank you for being a team player.

If you think you have found a vulnerability in any of our products or services, we encourage you to report it to us so we can solve the problem. Before you report a vulnerability, please read through our Responsible Disclosure Policy. Our Responsible Disclosure Policy provides guidelines for how to report vulnerabilities in Vipps' products or services in a responsible manner. The purpose is to make it easy to report any vulnerabilities and give clear guidelines for what is allowed to do to our systems.

Read our responsible disclosure policy

So, what’s next then?

PAPER FORM VERSION 2 (2021 edition) ☺

vipps

THANK YOU! (Questions?)

If you want to test this with your bank wherever you are, do it responsibly and let me know the results.

@thorsheim or Signal: +47 90 99 92 59

vipps