HACKING

Historier fra den virkelige verden

VÆR MED PÅ TELEFONEN PÅ

MENTI.COM

KODE: 7881 0100

EMIL HØRNING

Dobbelt kandidat (datalogi / cybersikkerhed)

DM I hacking opgaveudvikler

Underviser I Cybersikkerhed

Arbejder som etisk hacker

ET FORORD OM

DE GODE BAD GUYS

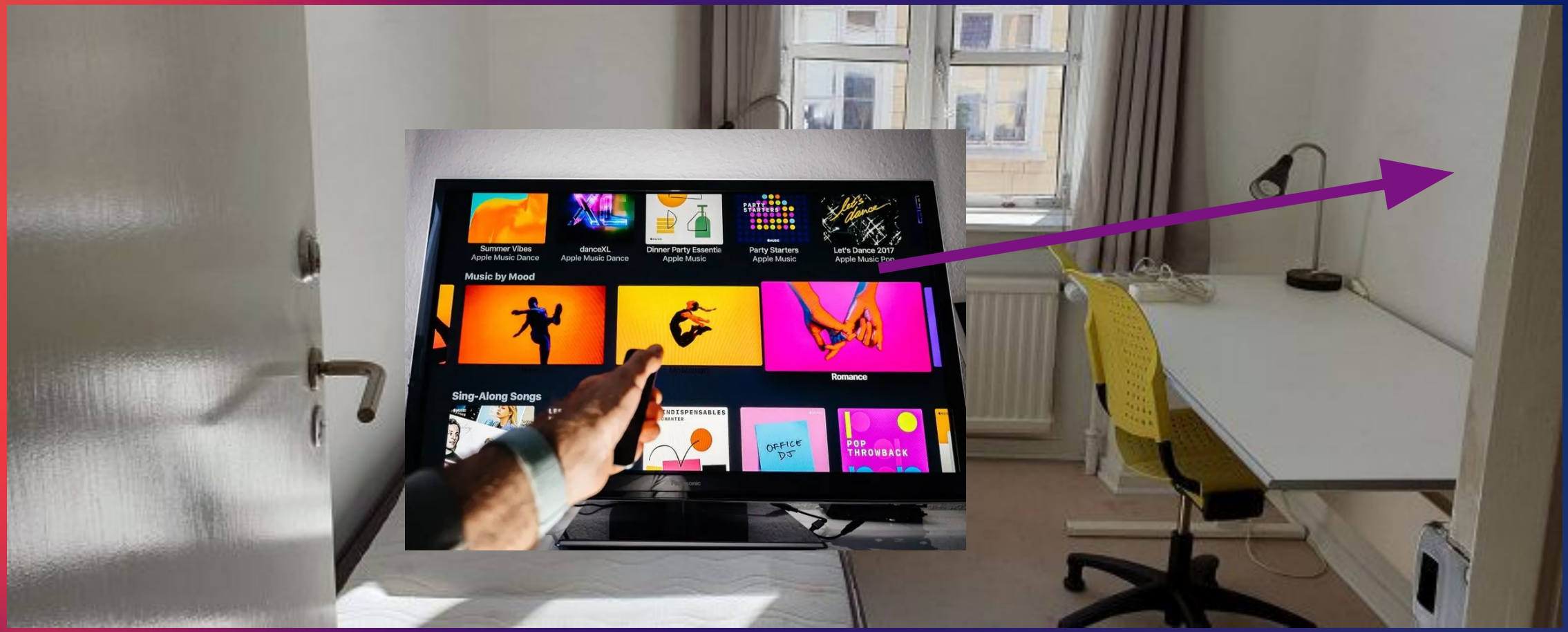
CHROMECASTS & WIFI

Historien om den forfærdelige nabo

LIVET PÅ KOLLEGIEVÆRELSET

LIVET PÅ KOLLEGIEVÆRELSET

LIVET PÅ KOLLEGIEVÆRELSET



LIVET PÅ KOLLEGIEVÆRELSET

WIRELESS NETWORKING » WI FI

How to Hack Wi Fi Using Android

Author Info

Last Updated: January 31, 2023 Approved

Download Article

Do you want to test your network security? It used to be that you needed a desktop OS such as Windows or Linux installed on a computer with a specific wireless network card. Now, however, you can also use certain Android devices to scan and crack wireless networks. These tools are available for free as long as your device is compatible. Hacking routers without permission is illegal. These steps are provided to test the security of your own network.

METHODS

1 WEP Routers

2 WPA2 WPS Routers

OTHER SECTIONS

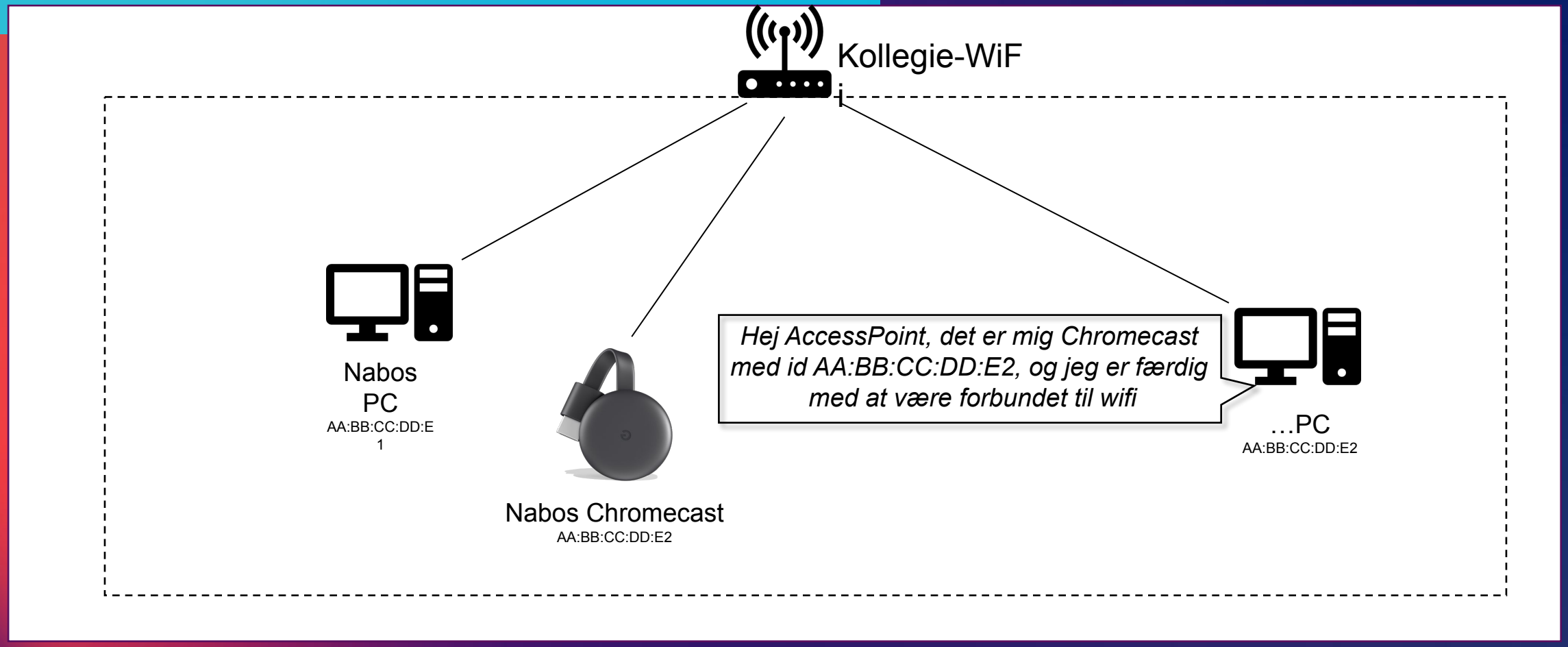
Questions & Answers

Tips and Warnings

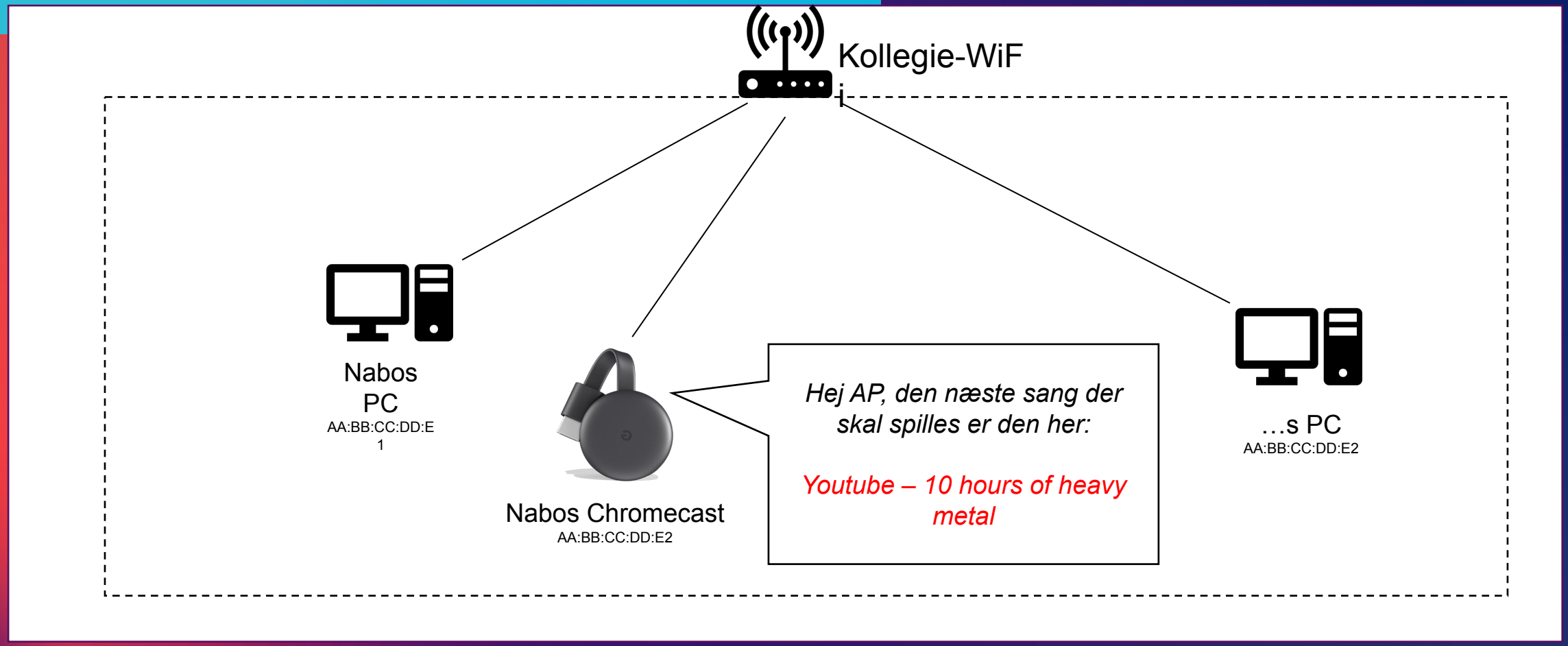
Related Articles

References

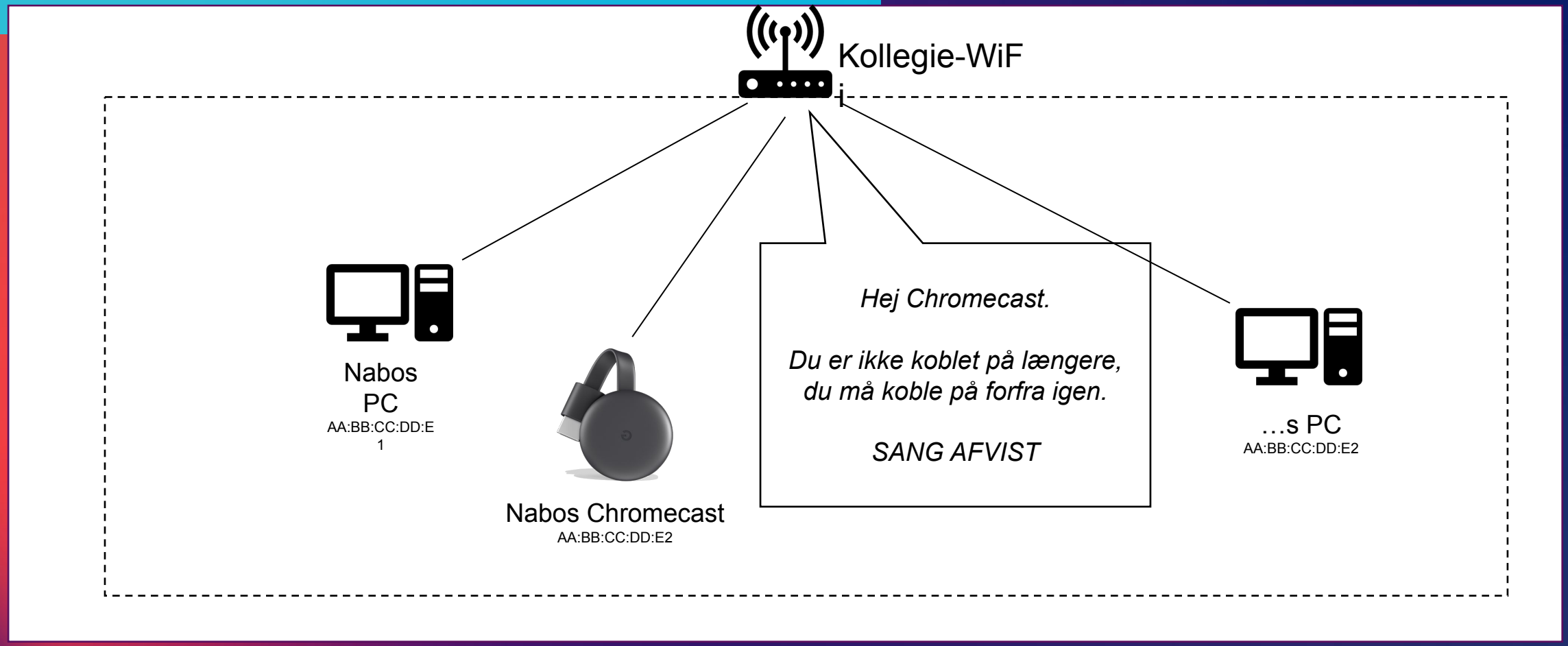
LIVET PÅ KOLLEGIEVÆRELSET



LIVET PÅ KOLLEGIEVÆRELSET



LIVET PÅ KOLLEGIEVÆRELSET



menti.com – Kode: 7881 0100

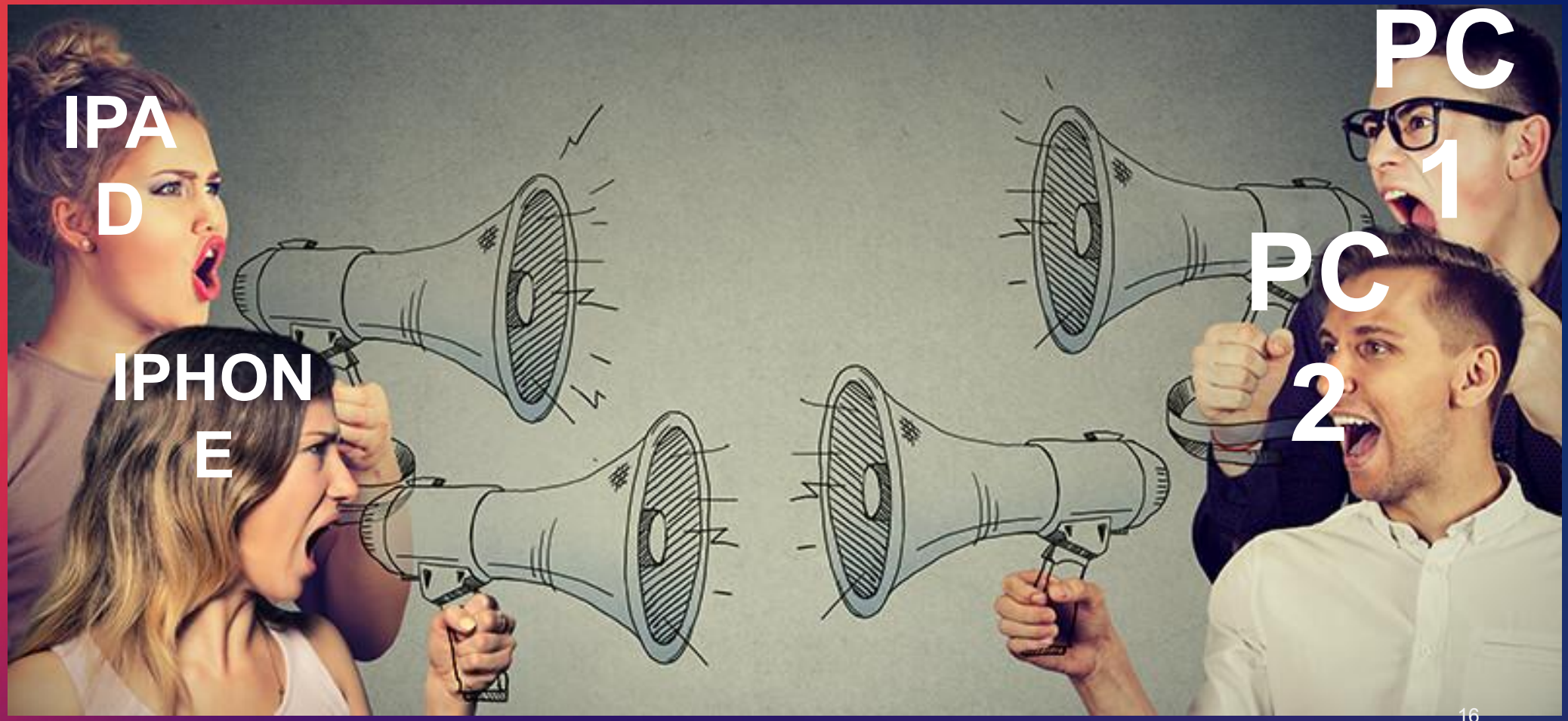
HVAD SKETE DER SÅ?

STEM PÅ MENTI

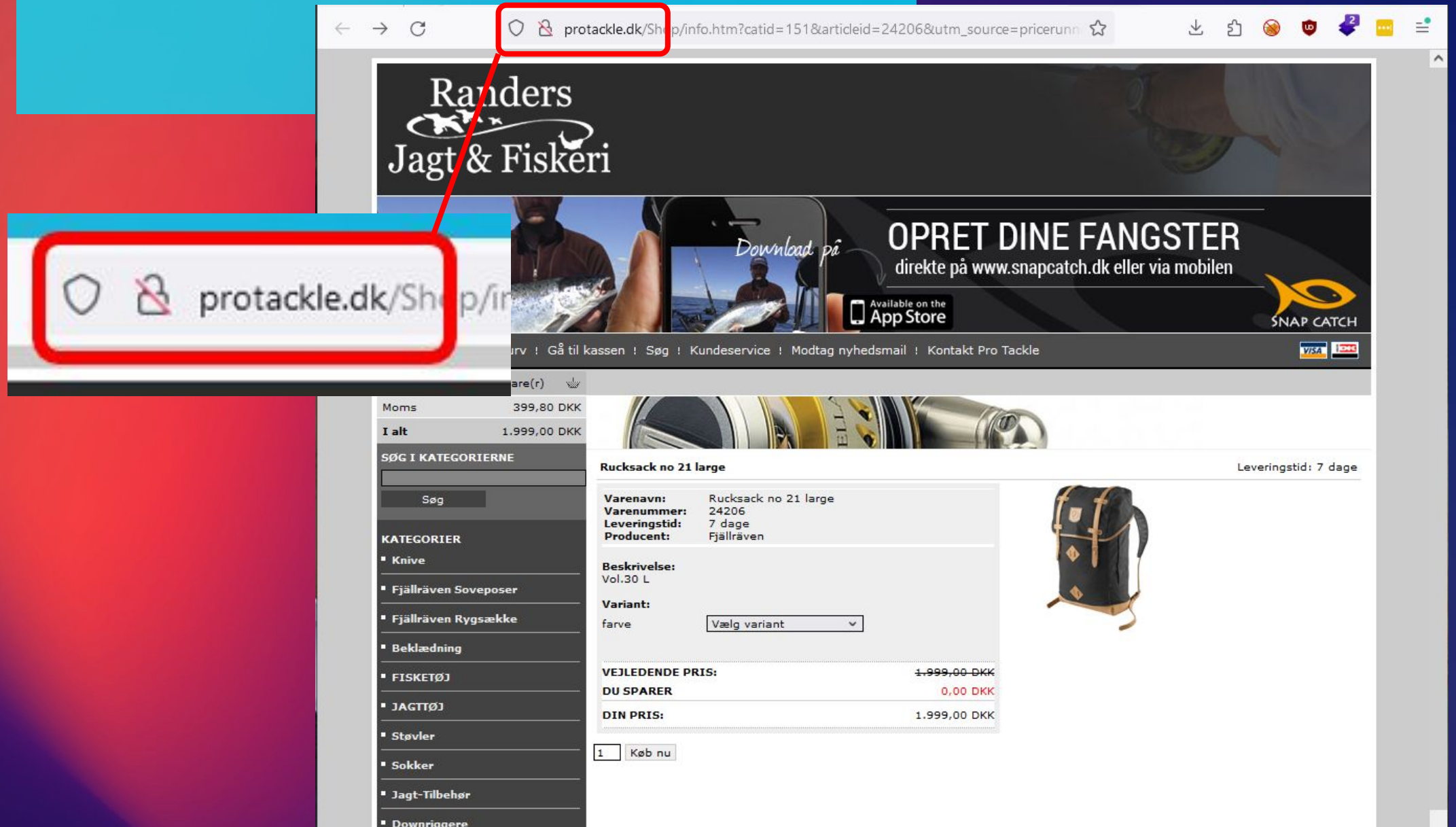
… FIK SIN SØVN

MISFORSTÅELSER OM WIFI

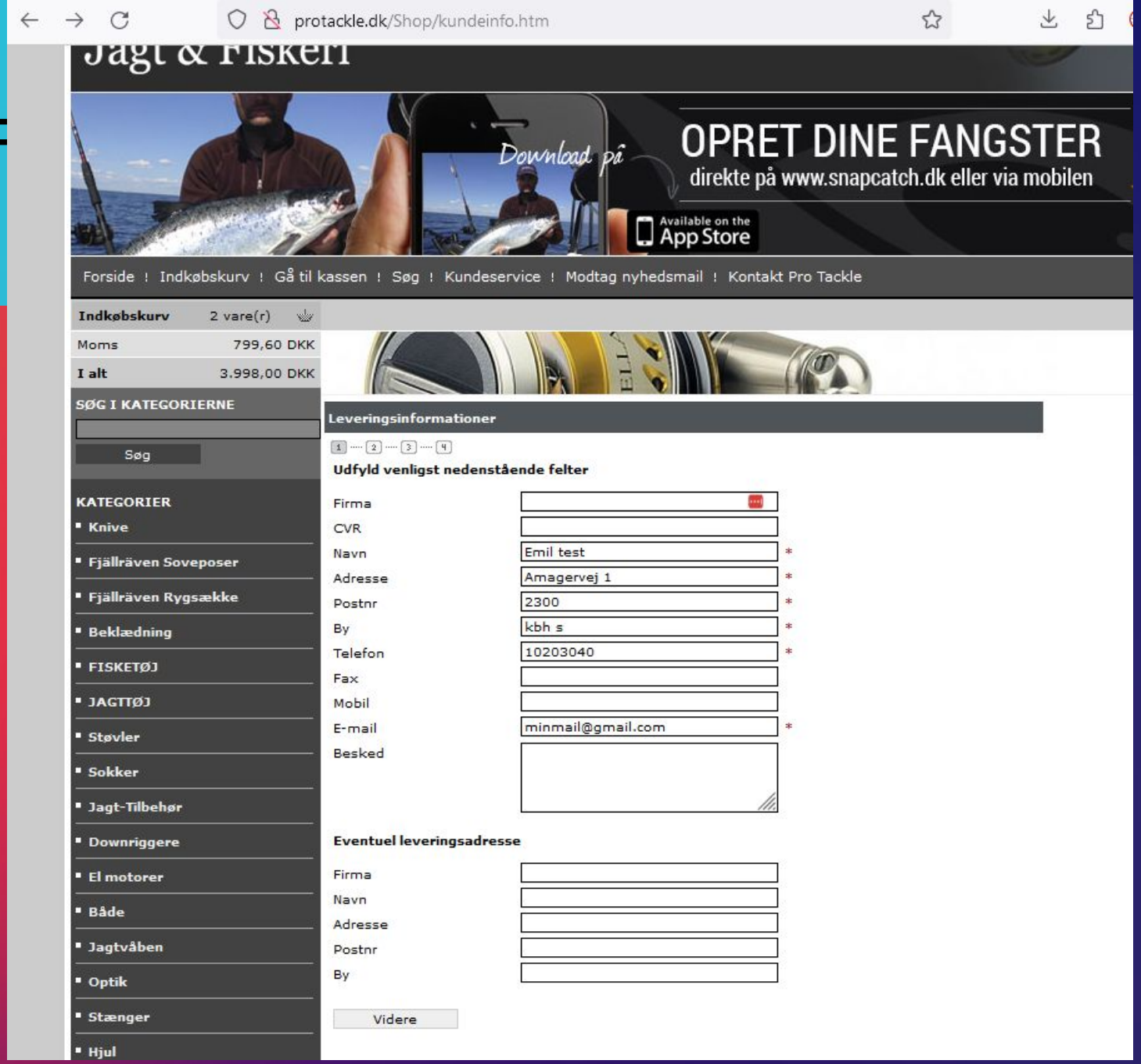
MISFORSTÅELSER OM WIFI



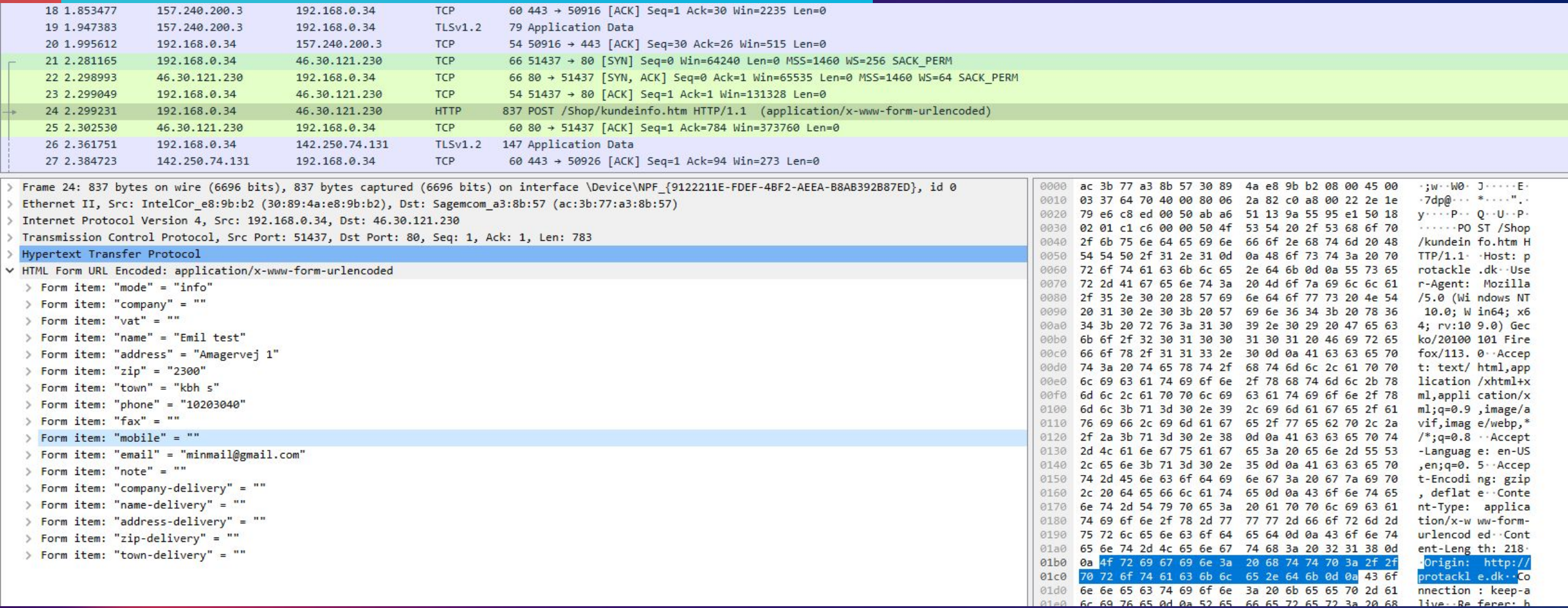
MISFORSTÅELSER OM WIFI



MISF


protackle.dk/Shop/kundeinfo.htm
Jagt & Fiskeri
Download på
OPRET DINE FANGSTER
direkte på www.snapcatch.dk eller via mobilen
Available on the App Store
Forside ! Indkøbskurv ! Gå til kassen ! Søg ! Kundeservice ! Modtag nyhedsmail ! Kontakt Pro Tackle
Indkøbskurv 2 vare(r)
Moms 799,60 DKK
I alt 3.998,00 DKK
SØG I KATEGORIERNE
Søg
KATEGORIER
Knive
Fjällräven Soveposer
Fjällräven Rygsække
Beklædning
FISKETØJ
JAGTTØJ
Støvler
Sokker
Jagt-Tilbehør
Downriggere
El motorer
Både
Jagtvåben
Optik
Stænger
Hjul
Leveringsinformationer
1 2 3 4
Udfyld venligst nedenstående felter
Firma
CVR
Navn Emil test *
Adresse Amagervej 1 *
Postnr 2300 *
By kbh s *
Telefon 10203040 *
Fax
Mobil
E-mail minmail@gmail.com *
Besked
Eventuel leveringsadresse
Firma
Navn
Adresse
Postnr
By
Videre

MISFORSTÅELSER OM WIFI



```
   18 1.853477    157.240.200.3   192.168.0.34    TCP       60 443 → 50916 [ACK] Seq=1 Ack=30 Win=2235 Len=0
   19 1.947383    157.240.200.3   192.168.0.34    TLSv1.2   79 Application Data
   20 1.995612    192.168.0.34    157.240.200.3   TCP       54 50916 → 443 [ACK] Seq=30 Ack=26 Win=515 Len=0
   21 2.281165    192.168.0.34    46.30.121.230   TCP       66 51437 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   22 2.298993    46.30.121.230   192.168.0.34    TCP       66 80 → 51437 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM
   23 2.299049    192.168.0.34    46.30.121.230   TCP       54 51437 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   24 2.299231    192.168.0.34    46.30.121.230   HTTP      837 POST /Shop/kundeinfo.htm HTTP/1.1  (application/x-www-form-urlencoded)
   25 2.302530    46.30.121.230   192.168.0.34    TCP       60 80 → 51437 [ACK] Seq=1 Ack=784 Win=373760 Len=0
   26 2.361751    192.168.0.34    142.250.74.131  TLSv1.2   147 Application Data
   27 2.384723    142.250.74.131  192.168.0.34    TCP       60 443 → 50926 [ACK] Seq=1 Ack=94 Win=273 Len=0

> Frame 24: 837 bytes on wire (6696 bits), 837 bytes captured (6696 bits) on interface \Device\NPF_{9122211E-FDEF-4BF2-AEEA-B8AB392B87ED}, id 0
> Ethernet II, Src: IntelCor_e8:9b:b2 (30:89:4a:e8:9b:b2), Dst: Sagemcom_a3:8b:57 (ac:3b:77:a3:8b:57)
> Internet Protocol Version 4, Src: 192.168.0.34, Dst: 46.30.121.230
> Transmission Control Protocol, Src Port: 51437, Dst Port: 80, Seq: 1, Ack: 1, Len: 783
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "mode" = "info"
  > Form item: "company" = ""
  > Form item: "vat" = ""
  > Form item: "name" = "Emil test"
  > Form item: "address" = "Amagervej 1"
  > Form item: "zip" = "2300"
  > Form item: "town" = "kbh s"
  > Form item: "phone" = "10203040"
  > Form item: "fax" = ""
  > Form item: "mobile" = ""
  > Form item: "email" = "minmail@gmail.com"
  > Form item: "note" = ""
  > Form item: "company-delivery" = ""
  > Form item: "name-delivery" = ""
  > Form item: "address-delivery" = ""
  > Form item: "zip-delivery" = ""
  > Form item: "town-delivery" = ""

0000  ac 3b 77 a3 8b 57 30 89  4a e8 9b b2 08 00 45 00   ·;w··W0· J·····E·
0010  03 37 64 70 40 00 80 06  2a 82 c0 a8 00 22 2e 1e   ·7dp@··· *····"..
0020  79 e6 c8 ed 00 50 ab a6  51 13 9a 55 95 e1 50 18   y····P·· Q··U··P·
0030  02 01 c1 c6 00 00 50 4f  53 54 20 2f 53 68 6f 70   ·····PO ST /Shop
0040  2f 6b 75 6e 64 65 69 6e  66 6f 2e 68 74 6d 20 48   /kundein fo.htm H
0050  54 54 50 2f 31 2e 31 0d  0a 48 6f 73 74 3a 20 70   TTP/1.1· ·Host: p
0060  72 6f 74 61 63 6b 6c 65  2e 64 6b 0d 0a 55 73 65   rotackle .dk··Use
0070  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
0080  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
0090  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00a0  34 3b 20 72 76 3a 31 30  39 2e 30 29 20 47 65 63   4; rv:10 9.0) Gec
00b0  6b 6f 2f 32 30 31 30 30  31 30 31 20 46 69 72 65   ko/20100 101 Fire
00c0  66 6f 78 2f 31 31 33 2e  30 0d 0a 41 63 63 65 70   fox/113. 0··Accep
00d0  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t: text/ html,app
00e0  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
00f0  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
0100  6d 6c 3b 71 3d 30 2e 39  2c 69 6d 61 67 65 2f 61   ml;q=0.9 ,image/a
0110  76 69 66 2c 69 6d 61 67  65 2f 77 65 62 70 2c 2a   vif,imag e/webp,*
0120  2f 2a 3b 71 3d 30 2e 38  0d 0a 41 63 63 65 70 74   /*;q=0.8 ··Accept
0130  2d 4c 61 6e 67 75 61 67  65 3a 20 65 6e 2d 55 53   -Languag e: en-US
0140  2c 65 6e 3b 71 3d 30 2e  35 0d 0a 41 63 63 65 70   ,en;q=0. 5··Accep
0150  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 67 7a 69 70   t-Encodi ng: gzip
0160  2c 20 64 65 66 6c 61 74  65 0d 0a 43 6f 6e 74 65   , deflat e··Conte
0170  6e 74 2d 54 79 70 65 3a  20 61 70 70 6c 69 63 61   nt-Type:  applica
0180  74 69 6f 6e 2f 78 2d 77  77 77 2d 66 6f 72 6d 2d   tion/x-w ww-form-
0190  75 72 6c 65 6e 63 6f 64  65 64 0d 0a 43 6f 6e 74   urlencod ed··Cont
01a0  65 6e 74 2d 4c 65 6e 67  74 68 3a 20 32 31 38 0d   ent-Leng th: 218·
01b0  0a 4f 72 69 67 69 6e 3a  20 68 74 74 70 3a 2f 2f   ·Origin:  http://
01c0  70 72 6f 74 61 63 6b 6c  65 2e 64 6b 0d 0a 43 6f   protackl e.dk··Co
01d0  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
01e0  6c 69 76 65 0d 0a 52 65  66 65 72 65 72 3a 20 68   live··Re ferer: h
```

KEY TAKE AWAYS - CHROMECAST

PÆN OPFØRSEL 1

Lad være med at blaste høj musik om natten så dine naboer ikke kan sove

PÆN OPFØRSEL 2

Snak med din nabo frem for at hacke deres elektroniske devices

USIKKER TEKNOLOGI

Teknologien der understøtter vores samfund har meget få mennesker læst manualen til.

DE KAN LYTTE MED

Andre folk på wifi netværket kan lytte med på alt der bliver ‘råbt’ om. Brug altid sider med HTTPS

BILLIGE BURGERE OG SULTNE HACKERE

Historien om den sårbare burgerbiks

SULTNE HACKERE

Det danske sikkerhedsmarked

security WORLDMARKET.COM

NYHEDER LEVERANDØRER SE

Ændre marked

Global

North America

Middle East

United Kingdom

Sweden

Norway

Denmark

Abonnér på nyhedsbrev

Aktuelle begivenheder

31-05-2023 – 31-05-2023

Bosch Roadshow Luleå – Luleå, Sweden

01-06-2023 – 01-06-2023

11-02-2020

Danmarks fø cybersikkerh

Aalborg Universitet, Campus

Cybertruslen mod dansk været større. Det råder A at uddanne landets komm

general

Mar 31st

jens 9:22 AM

@everyone We would like to remind you that it is not allowed to hack the coffee machine, and especially not when other staff members are around 🙂 Happy weekend.

👀 7 🚀 6 🙇 1 😅 1

👾 2

INPUT

ANMELDELSER ELBILER FREMTIDENS HJEM GADGETS GAMING STREAMING

ANNONCERING DATAPOLITIK KONTAKT

få kandidatgrad i cybersikkerhed i København

å kandidatgrad i cybersikkerhed i

ersikkerhed bliver den første af sin slags i Danmark.

2020 0 Kan læses på 1 minut

ersikkerhed på AAU's campus i København. Universitetet udbyder en helt ny erhed – den første og eneste i Danmark.

SENESTE

1 Selvk mang intelli 30. m

2 Nyt LF Mode 30. m

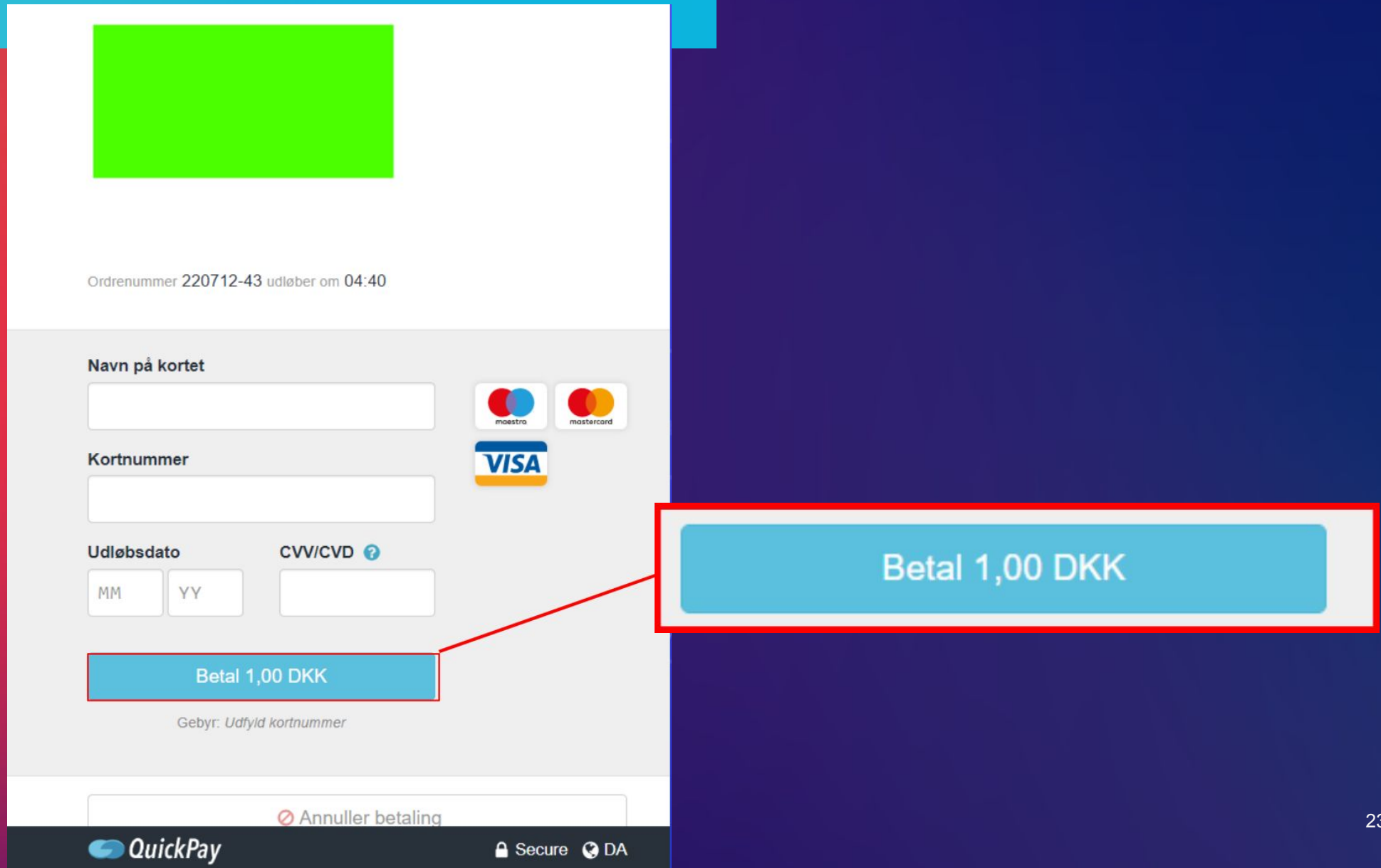
3 Sono over 29. m

4 Volvo kig p 29. m

5 HUAWEI Aftale Huaw sikke 26. m

6 Nothi

SULTNE HACKERE



SULTNE HACKERE

Request

Pretty Raw Hex

```
1  POST /api/v1/orders.php?selfservice_token=                    &cmd=create HTTP/2
2  Host:
3  User-Agent: *****
4  Content-Type: application/json
5  Content-Length: 127
6
7  {
     "Location":"cart",
8    "Items":{
       {
         "FoodItem":"Cheeseburger Menu",
9        "Quantity":1
10     },
11     {
         "FoodItem":"Extra Fries",
12       "Quantity":1
       }
     }
13 }
14
```

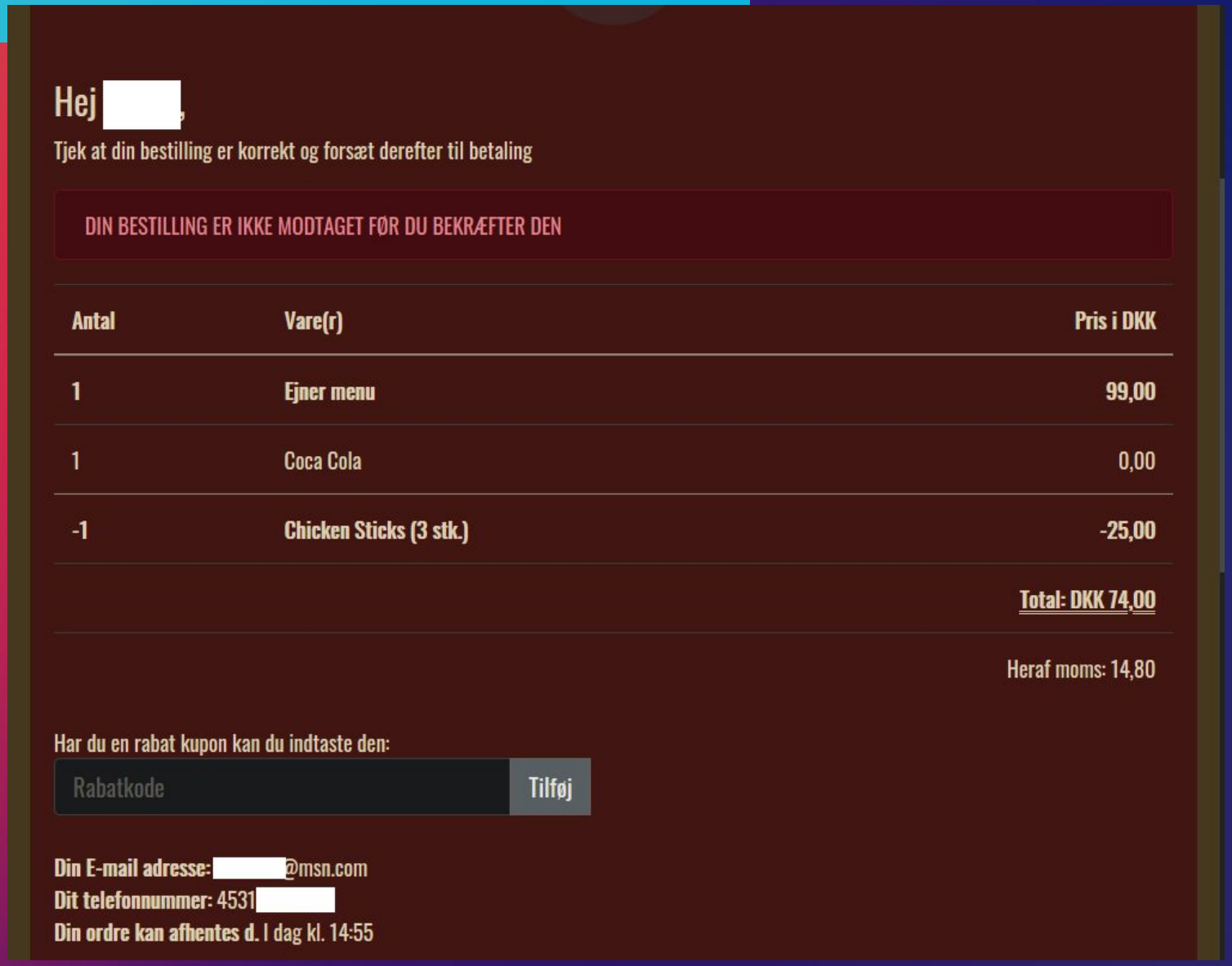
SULTNE HACKERE

Request

Pretty Raw Hex \n

```
1  POST /api/v1/orders.php?selfservice_token=[redacted]&cmd=create HTTP/2
2  Host: [redacted]
3  User-Agent: *****
4  Content-Type: application/json
5  Content-Length: 127
6
7  {
     "Location":"cart",
8    "Items":{
       {
         "FoodItem":"Cheeseburger Menu",
9        "Quantity":1
10     },
11     {
         "FoodItem":"Extra Fries",
12       "Quantity":-1
       }
     }
13 }
14
```

SULTNE HACKERE



SULTNE HACKERE

SULTNE HACKERE

Muligt sikkerhedshul i jeres platform Inbox ×

Emil Hørning <emilhoerning@gmail.com>
to [redacted]

Hej [redacted]

Hvad er jeres politik omkring fund af sikkerhedshuller i jeres produkt?

Jeg vil gerne diskutere et muligt fund med jer, men jeg vil gerne sikre mig at det gøres på ordentlige vilkår.

Hvad er jeres process for responsible disclosure ? (https://conscia.com/dk/blog/responsible-disclosure/)

Vh Emil

SULTNE HACKERE

DISCLOSURE POLITIKER

FULL DISCLOSURE

- Sårbarheden offentliggøres af hackeren uden at underette den ansvarlige virksomhed eller deres kunder
- Tilføjer pres på ansvarlige virksomhed til at fixe sårbarheden ASAP
- Kriminelle får også adgang til denne viden.

RESPONSIBLE DISCLOSURE

- Virksomhed kontaktes først privat af hacker og lærer om sårbarheden
- Sårbarheden offentliggøres af hackeren efter at virksomheden har fået tid til at fikse den.
- I tidsrummet bør ansvarlige virksomhed have et fix klar.

PRIVATE DISCLOSURE

- Virksomheden kontaktes først privat af hacker og lærer om sårbarheden
- Virksomheden har god tid til at fikse sårbarheden, da der ikke er nogen deadline fra hackeren
- Meget få får viden om sårbarheden

menti.com – Kode: 7881 0100

HVAD SKETE DER SÅ?

STEM PÅ MENTI

PRIVATE DISCLOSURE

SULTNE HACKERE

W [redacted] <[redacted]>

to me

Danish > English Translate message

Hej Emil

Det er hermed modtaget. Vi har kunnet genskabe fejlen i vores produktion og udviklingsmiljø og sørger for at få rettet asap.
Forventet rettet i dag.
Vi takker mange gange for indberetningen.

W [redacted] <[redacted]>

to me

Danish > English Translate message

Hej Emil

Blot en sidste note.
Vi har nu sendt et hotfix live.
Min tidligere mail var lidt kortfattet, da vi gik i gang med at gennemgå og rette op på fejlen.

I forhold til hvad restauranten ville se, så vil der stå det bestilte på ordren.
Der vil stå 10 sandwich og -10 fritter.

Endnu en gang takker jeg for din indberetning.

God jul og godt nytår når du kommer dertil.

•••

KEY TAKE AWAYS - BURGERBIKS

STOL IKKE PÅ DATA FRA BRUGERE

Alt data fra en bruger der bliver sendt til dig bør ikke stoles på.

OVERVEJ JERES DISCLOSURE POLITIK

Tag stilling til hvordan I gerne vil arbejde med hackere der kontakter jer omkring sårbarheder

OVERVEJ JERES BOUNTY POLITIK

Nogle hackere, på godt og ondt, er motiveret af belønninger. Overvej hvor jeres virksomhed står på denne front

SÅRBARE ACCESSKORT

Historien om den dårligst sikrede, men mest brugte smartcard teknologi

SÅRBARE ADGANGSKORT

- Mifare Classic er den mest velkendte korttype
- Brugt I utallige rejsekort rundt om I Europa og verden
- Brugt I utallige virksomheder, til adgangs kontrol
- Sikkerhed brudt siden 2010

SÅRBARE ADGANGSKORT

SÅRBARE ADGANGSKORT

icare®

Premium Sikkerhedssoftware og hardware

Start | Produkter | Viden | Shop

HAR DU ET REJSEKORT KAN DU FRIT GÅ IND I 9.000 BOLIGER, TALLET ER FORMENTLIGT MEGET STØRRE

AF MICHAEL RASMUSSEN / ADGANGSKONTROL, ELEKTRONISKE LÅSE, REJSEKORT / ADGANGSKONTROL, ELEKTRONISKE LÅSE, REJSEKORT / 4 MINUTTERS LÆSNING

Version2 kører i øjeblikket en artikel serie om elektroniske låse der kan hackes og give fysisk adgang til mange tusinde hjem. Det vakte opsigt hos beboerne, da Version2 kom forbi med det modificerede rejsekort, der i løbet af få minutter var blevet omdannet til en universalnøgle til flere hundrede lejligheder, kælderrum og fællesrum. Fem mails og flere fysiske breve var ikke nok til at få låseproducenten Scantron til at reagere. Nu kæmper udlejere med tiden for at sikre beboerne.

Ifølge Journalist Mads Lorenzen fra V2, har de opdaget at ca. 9.000 lejligheder står åbne for indbrudstyve.

Hack af digitale låse er forsikringsmareridt for beboere: »Der vil ikke være dækning«

PLUS | It-sikkerhed | 12. december 2022 kl. 06:00 | 47

To af beboerne i de sårbare boliger, Version2 besøgte med rejsekortet. Deres umiddelbare reaktion var, at det er 'fucked up', at ingen har fortalt dem om deres sårbare lås. Illustration: Jakob Carlsen.

Version2's undersøgelse af digitale låse fra selskabet Scantron rejser ifølge forsikringsselskaber en række svære spørgsmål i forhold til, om forsikringen dækker ved digitalt faciliterede indbrud eller ej.

SÅRBARE ADGANGSKORT

- Kortets id
  - Unikt og kan ikke ændres
  - Kan aflæses, ikke skrives
    - *Med mindre man bruger et 'magisk kort'*

- Data på kortet
  - Indeholder information om kortet
  - Kan frit aflæses og skrives

```
$ ./mfdread.py ./dump.mfd
File size: 4096 bytes. Expected 64 sectors

UID:  33bd9d3f
BCC:  2c
SAK:  98
ATQA: 02
```

Key A Access Bits Key B

Sector	Block	Data	Access Bits
0	0	33bd9d3f2c980200648f841441502212	100
	1	090f1808000000000003010000400b	100
	2	00000000400c400c400c000400040005	100
	3	a0a1a2a3a4a5787788c17de02a7f6025	011
1	0	418d50c98d7f962462004c800000ffcc	100
	1	1fa1014100d101c060000000049a2a9f	100
	2	1fa1014100d101c060000000049a2a9f	100
	3	2735fc1818077877880bf23a53c1f63	011
2	0	3065061730077220296012505b74c05d	100
	1	68c701da24c027ece0ee9a99c0caadb1	100
	2	c82591842f0b8304a2a068d1f4e016e7	100
	3	2aba9519f574787788ffcb9a1f2d73b8	011
3	0	6c135ade77c0f7a11f09ad059d45720c	100
	1	3c0dc85010e3ef723bfad584c4ad509d	100
	2	040e821625f14168040ed8ee61a8f635	100
	3	84fd7f7a12b6787788ffc7c0adb3284f	011
4	0	420d53f9dbd3362461004c800000bc18	100
	1	1f51014100d101c0900004240280bdce	100
	2	1f51014100d101c0900004240280bdce	100
	3	73068f118c1378778800 2b7f3253fac5	011
5	0	00000000000000000000000000000000	110
	1	01770000907222029653352020202020	110
	2	00000000000000000000000000000000	110
	3	186d8c4b93f908778f029f131d8c2057	011

SÅRBARE ADGANGSKORT

- Utallige adgangskort I danmark kan aflæses
  - Det kræver bare kort tid (10-20 sekunder) nær (15 cm) kortet
- ‘Magiske’ kort sælges i store mængder online
  - Disse kort bruges til at lave kopier af de aflæste kort

SÅRBARE ADGANGSKORT

https://github.com/mchro/RejsekortReader

README.md

RejsekortReader

Python code and basic Android app to parse the danish Rejsekort Mifare NFC cards.

Currently parsed is: the purse (how much money is on the card), ticket and event log entries (what travels have taken place), card meta information (card number), and customer information (e.g. birth-month).

The card stores the last 15 events, and the last 7 tickets, including locations and timestamps.

We have been working on and off (mostly off) for quite some time, and originally planed to do an app like http://blog.bangbits.com/2014/03/rejsekort-scanner.html But now we are dumping whatever we have, in the hope that it might be useful for Casper Bang (or others).

Code Structure

The Python code is the primary prototyping place. The data is parsed in `rkf/card.py`, with the different data types parsed in `rkf/datatypes.py`.

menti.com – Kode: 7881 0100

HVAD SKETE DER SÅ?

STEM PÅ MENTI

DE VAR SIKRE! (ISH)

SÅRBARE ADGANGSKORT

Mobil-hack af anonyme rejsekort: Fem personer tiltalt for at rejse gratis 1.061 gange

Finans-it | 2. september 2016 kl. 10:54 | 25

En familie er anklaget for via en app at have snydt sig til gratis rejser via rejsekort.

Artiklen er ældre end 30 dage

Manglende links i teksten kan sandsynligvis findes i bunden af artiklen.

Ekstra Bladet kan i dag fortælle, at en fem personer er tiltalt i en sag om hacking af anonyme rejsekort. Det skulle være foregået via en mobil-app hentet fra nettet.

SÅRBARE ADGANGSKORT

Krimi Opdateret: 30. okt. 2016 Gem artikel

Erkender snyd med rejsekort: - Jeg var bare nysgerrig

21-årig svensker fik ideen til at hacke dansk rejsekort - fire medtiltalte nægter, at de også snød

Anklage: Sådan gjorde de

De tiltalte købte ifølge anklagen først et anonymt rejsekort til 80 kroner og satte et mindre beløb ind på kortet, for eksempel 100 kroner.

Herefter rejste de som alle andre.

Når der manglede penge til nye rejser, brugte de det særlige program og en mobiltelefon til at nulstille kortet med en kopi af det oprindelige beløb på 100 kroner.

Flere end 1000 gange gentog de denne kopiering på i alt 15 kort, hvilket i månedsvis gjorde det gratis for dem at rejse.

Samlet blev der rejst for over 18.000 kroner, før politiet i Danmark og Sverige ransagede de nu tiltaltes hjem og anholdt dem

Kilde: Politiets anklageskrift i sagen

KEY TAKE AWAYS - ADGANGSSKORT

MIFARE CLASSIC ER USIKKERT

Det meget omstridt brugte mifare classic access kort har meget dårlig sikkerhed og det kan let klones eller krypteret data kan læses.

NOGLE GANGE ER ANALOGE LØSNINGER BEDRE

Det er ikke altid at det giver mening at løse et problem digitalt, som allerede er løst analogt

DET ER SVÆRT AT SIKRE ADGANGSKORT

Både fra hacking, men også fra tyveri eller efterligning. Det bør indgå I risikovurderinger.

RT MEGET

KKERH

NG

18.01.23 · DI DIGITAL · NYHEDER

Nye tal fra Danmarks Statistik viser, at manglen på it-sikkerhed i de små virksomheder er alt for stor

Over halvdelen af de danske mikrovirksomheder har ingen dokumentation for it-sikkerhedstiltag. Det vækker stor bekymring hos DI Digitals branchedirektør, Rikke Hougaard Zeberg, der efterspørger en helt ny CERT og modernisering af politiet.

Mangel på it-sikkerhedsviden står bag 80 procent af alle sikkerhedsbrister viser ny rapport

29.4.2022 07:10:16 CEST | Fortinet

Del

Ny Fortinet-rapport påpeger en række problemområder vedrørende it-sikkerheden i organisationer: mangel på sikkerhedstalenter, udfordringer med rekruttering- & diversitet samt manglende sikkerhedsårvågenhed

28.01.2020 | 3 min læsetid

It-sikkerheden truet af mangel på kompetencer

de trussel fra it-kriminelle mangler landets heder it-sikkerhedskompetencer

CFCS advarer: Mangel på arbejdskraft er en trussel mod dansk it-sikkerhed

Cybersikkerhed | 27. september 2022 kl. 13:44 | 1

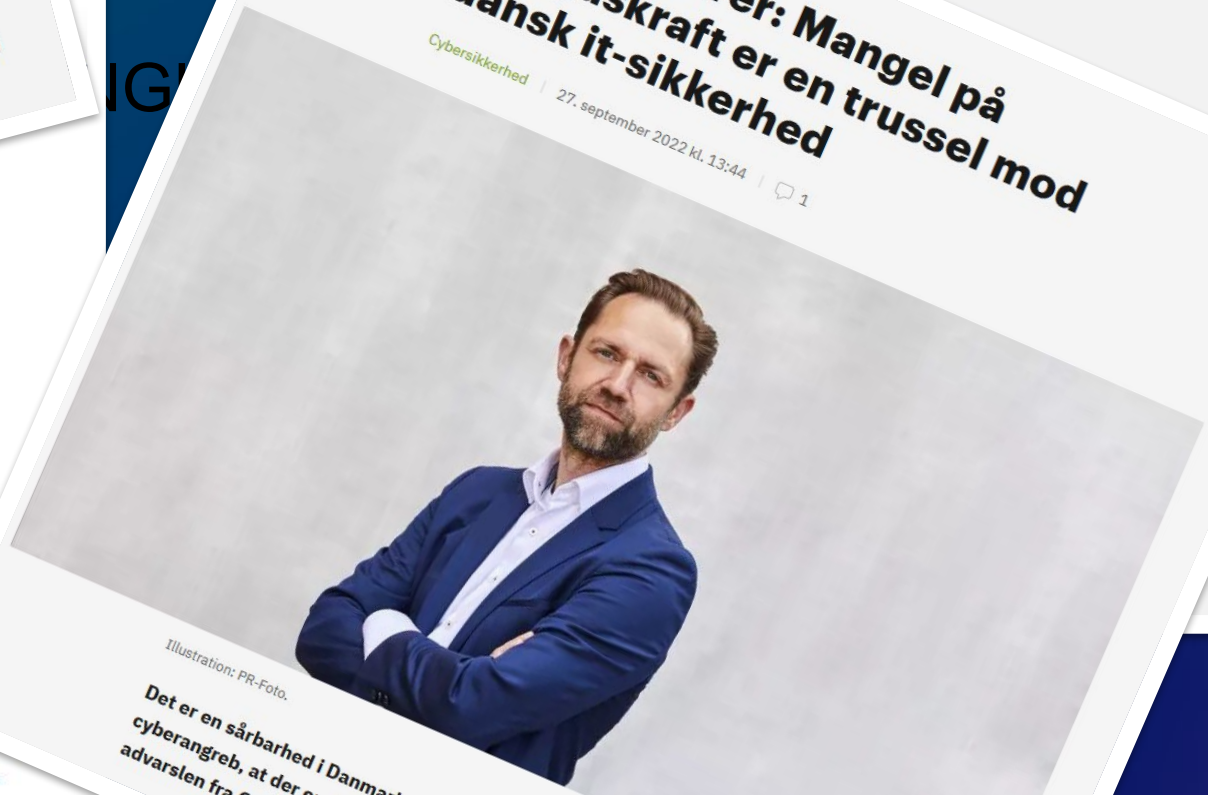


Illustration: PR-Foto.

Det er en sårbarhed i Danmarks evne til at forsvare sig sel
cyberangreb, at der er så massiv mangel på it-med
advarslen fra Center for Cybersikkerhed.

HVO MAN


Aspiring
Security
Professionals
Hacking
Programming
Web
Networking
Systems
imgflip.com

STEP 1
LÆR BASICS

DATA BASICS

- Hvordan er data repræsenteret?
- Hvad er bits og bytes?
- Strings, ints, floats osv.

COMPUTER BASICS

- Hvilke komponenter består en computer af?
- Hvilke komponenter består dit operativ system af?
- Lær at programmere.

NETVÆRKS BASICS

- Hvordan 'snakker' computere sammen over netværk?
- Hvordan virker internettet?
- Hvilke protokoller findes der?

WEB BASICS

- Hvordan virker en browser?
- Hvordan virker en hjemmeside?
- Hvordan virker HTTP protokollen?

./ pwn.college

HACKSPLAINING

FEATURES LESSONS ENTERPRISE OWASP TOP 10 PCI COMPLIANCE THE BOOK LOGIN SIGNUP

SECURITY TRAINING FOR DEVELOPERS

PWNABLE TW

Learn Modern Cryptography

Hack The Box
PEN-TESTING LABS

Try Hack Me

OFFENSIVE security

STEP 2

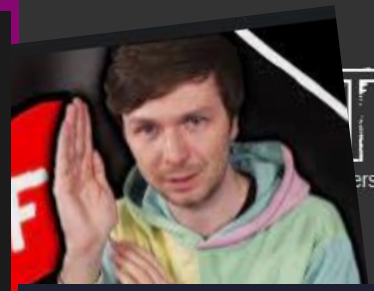
SLÅ DIG LØS

ROP Emporium

Learn return-oriented programming through a series of challenges.

View Beginners' guide

Download all challenges



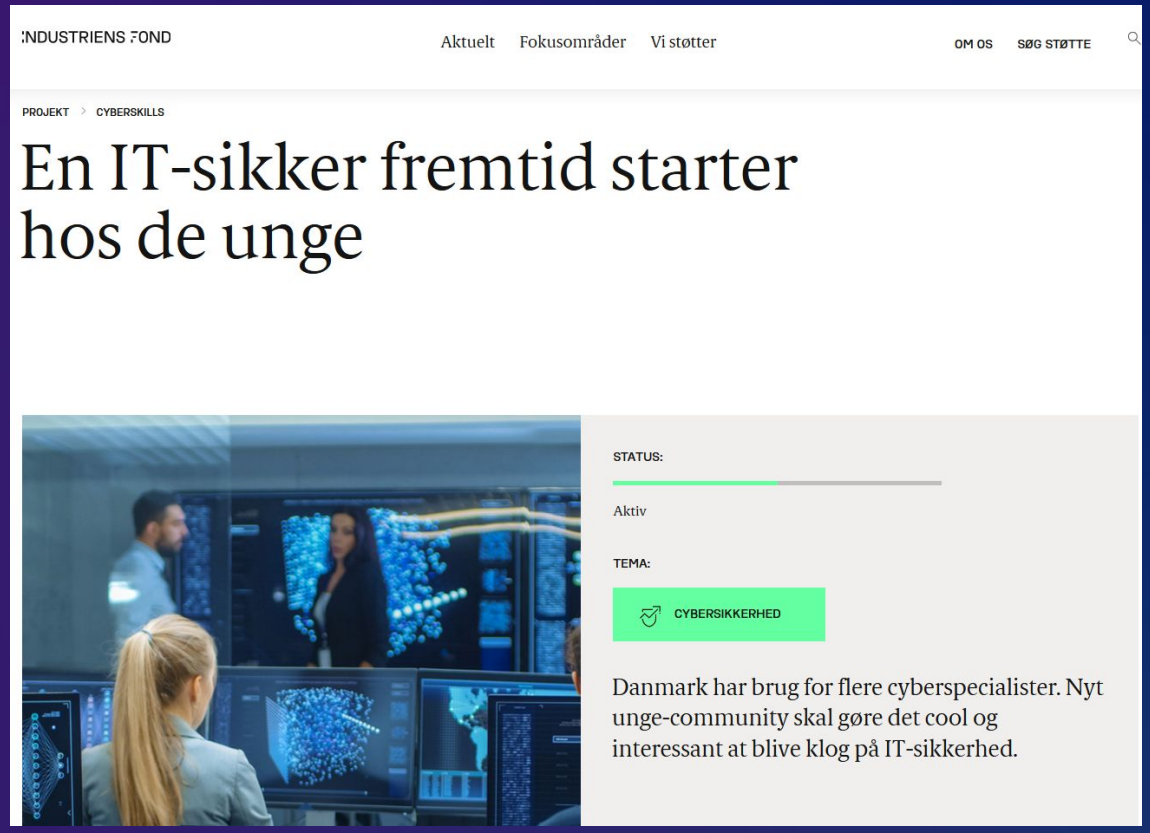
OT be a hacking noob in 2022 ...

picoCTF

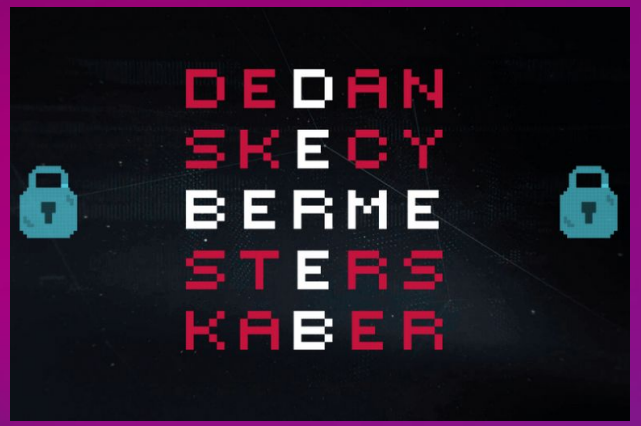
Google CAPTURE the FLAG MOAR

DE UNGE BANER VEJEN

- Industriens fond har støttet et projekt for at få unge interesseret I cybersikkerhed
- De unge (15-25) deltager aktivt I diverse events hostet igennem ***Cyberskills***
- Der er stor deltagelse til diverse it-sikkerheds events og CTF som virksomheder afholder

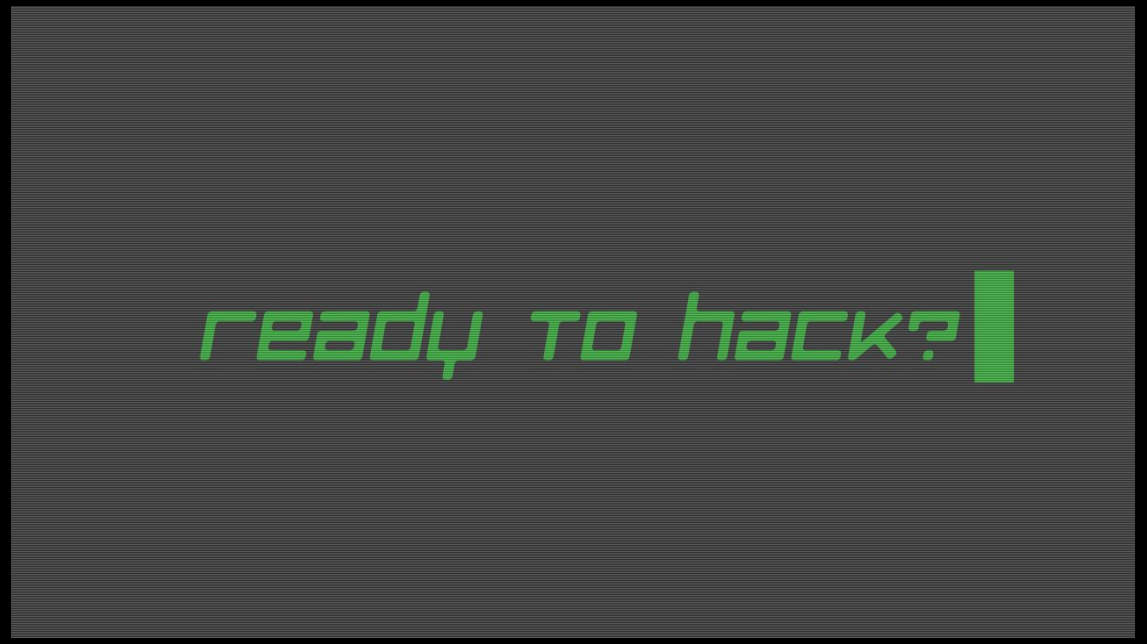


DER ER STOR VÆRDI I LÆRING IGENNEM CTF



HVIS I VIL HOLDE JERES EGEN CTF

- Hvis jeres virksomhed vil afholde en CTF
  - Internt til jeres medarbejdere
  - Eksternt for interesserede
- … og Emil har stor erfaring med planlægning og afholding af CTF
- Events hvor cybersikkerhed og læring er I fokus



…

Emil Hørning – Emilhoerning@...