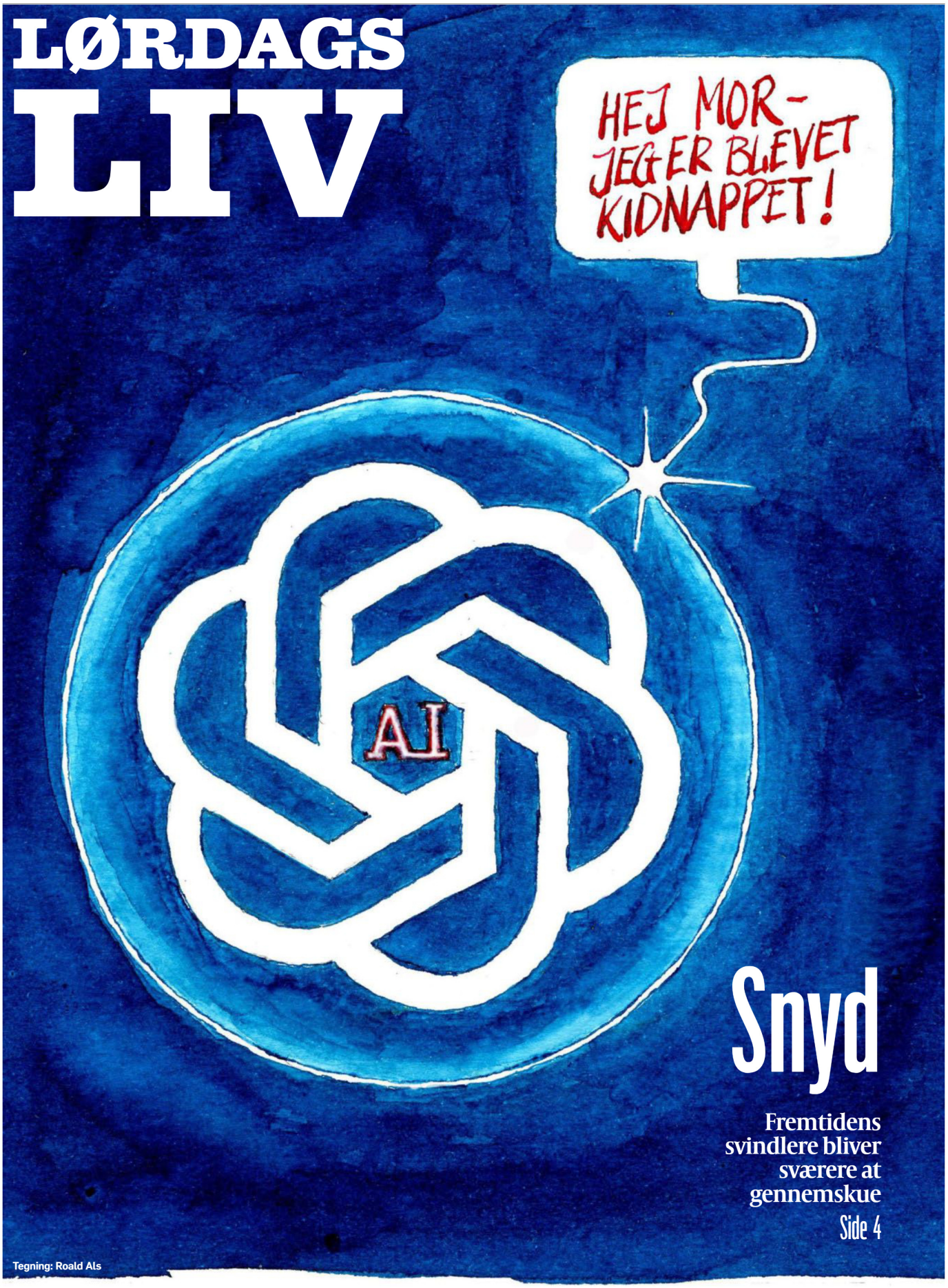
POLITIKEN 5 Lørdag 13. januar 2024

LØRDAGS LIV



Snyd

Fremtidens svindlere bliver sværere at gennemskue

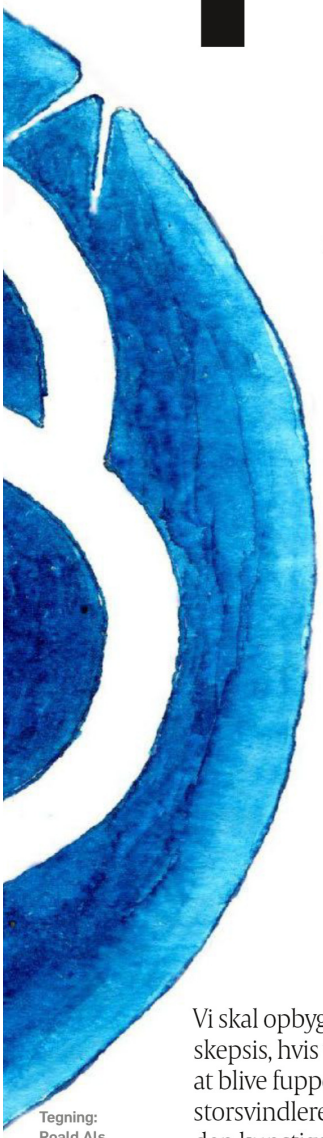
Side 4

Tegning: Roald Als

Pas på!

AI har givet digitale svindlere helt nye

redskaber



Tegning: Roald Als

Vi skal opbygge en ny skepsis, hvis vi vil undgå at blive fuppet af digitale storsvindlere, der udnytter den kunstige intelligens, mener formanden for bankernes nye taskforce mod svindel.

MICHAEL OLSEN

Ann-Lis Hake var begyndt at tænke tanken: om der kunne være tale om svindel, da hun få dage før nytår fik en sms fra datteren Kerstin.

Kerstin fortalte, at hendes mobiltelefon var gået i smadder, og at hun derfor havde været tvunget til at købe en ny.

Slet det gamle nummer og gem det nye, lød opfordringen fra datteren, der kort tid efter sendte en ny sms, hvor hun bad om hjælp med at betale nogle regninger, fordi hendes bank-id endnu ikke var koblet op på det nye telefonnummer.

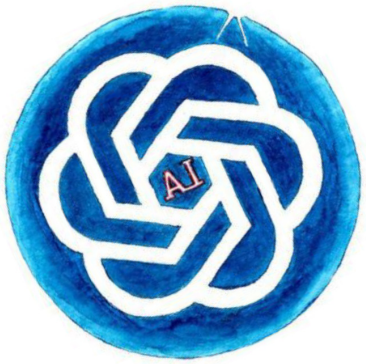
Ann-Lis Hake ville være sikker på, at hun ikke blev snydt, så hun ringede på det nye nummer. Et øjeblik efter havde hun datteren i røret, og så var der ikke længere grund til at tvivle på arrangementet. Ann-Lis Hake sendte sine bankoplysninger videre til datteren.

»Jeg var helt overbevist om, at det var min datter. De havde ramt tonefaldet, og stemmen lød præcis som min datter«, fortæller Ann-Lis Hake fra bopælen i Malmø til den svenske avis Sydsvenskan, der slog historien stort op i sidste uge.

Det var nemlig ikke datteren, der tog telefonen. It-kriminelle havde kopieret, genskabt eller efterlignet datterens stemme så præcist, at Ann-Lis Hake gik lige i fælden i et af de raffinerede svindelforsøg, der ifølge eksperterne vil komme mange flere af i fremtiden.

Nyt svindeltaskforce

Med ny teknologi, stemmemaskiner, sprogrobotter og kunstig intelligens kan stemmesekvenser, hentet ud af en telefonsvarer eller en video på de sociale medier, omsættes i troværdige samtaler.



Og selv om den slags svindelsager stadig er sjældne i Danmark, er det en ny normal lige om lidt, når de økonomisk kriminelle for alvor lærer at styre de maskiner, der er i stand til at efterligne den menneskelige intelligens, stemme og fremtoning.

Det er budskabet fra Christiane Vejlø, en af landets førende eksperter i digitale trends og kunstig intelligens, og formand for Finans Danmarks nye taskforce mod svindel, der er sat i verden for at finde nye våben og værktøjer i kampen mod de digitale storsvindlere. Det er der brug for, forsikrer Christiane Vejlø:

»Vi er kommet til det punkt, hvor det er muligt teknologisk at genskabe både det menneskelige ansigt og den menneskelige stemme med så stor overbevisning, at selv forældrene bliver narret, når falske børn beder om penge«.

Og det er bare et hjørne af det, vi har i vente:

»I USA har vi set flere sager, hvor børn ringer deres forældre op og fortæller, at de er blevet kidnappet, hvorefter forældrene bliver afkrævet enorme løsesummer, hvis de vil have deres børn tilbage. Det er ren svindel, men så overbevisende og skræmmende skruet sammen, at forældrene slet ikke tænker tanken, at det kan være svindel«, siger Christiane Vejlø.

Det gør topchefen heller ikke, når han bliver ringet op af en falsk regnskabschef på FaceTime, der beder ham om at godkende en pengeoverførsel til et datterselskab eller en filial.

»Vi er slet ikke som mennesker gearede til at være mistroiske, når noget er meget genkendeligt. Så falder vores panser. Så betaler vi uden rigtig at tænke tanken, at der kunne være tale om svindel«, siger Christiane Vejlø.

Men den går bare ikke længere.

Det er slut med at stole på det, vi ser og hører. Vi er nødt til at lære at være meget mere kritiske, når vi bruger penge, hvis vi skal have en chance for at slippe forbi det nye filter af sofistikeret svindel, mener Vejlø.

> **Når de kriminelle både kan forfalske dit ansigt og din stemme og skabe falske samtaler, så bliver det rigtig farligt**
> Emil Gade, Nets

»Det er ikke længere nok at bruge den sunde fornuft«.

Nets slår igen i våbenkapløb

Meldingen er den samme fra betalingstjenesten Nets, der hvert år håndterer milliarder af transaktioner med betalingskort.

Den kunstige intelligens har accelereret kapløbet mellem nettets økonomisk kriminelle og de finansielle virksomheder, banker og betalingsformidlere, der både skal beskytte kunderne og sig selv mod nye angreb.

»Når de kriminelle både kan forfalske dit ansigt og din stemme og skabe falske samtaler, så bliver det rigtig farligt; for hvem er det så egentlig, du taler med, når du tror, det er din søn eller din datter«, siger Emil Gade, markedsanalytiker i Nets med speciale i digitale svindelsager.

Engang var falske mails, beskeder og hjemmesider præget af dårligt sprog, elendige oversættelser, skæve logoer og mærkelige mailadresser. Nu er stadig flere af dem formfuldendte i udtrykket og udstyret med tekster, der matcher afsenderens signatur og kendetegn i en sådan grad, at en falsk hjemmeside næsten kan se mere ægte ud end de ægte, fortæller Emil Gade.

Vil det sige, at der i dag er større risiko for, at vi som forbrugere bliver snydt, når vi handler på nettet?

»Det er noget, både vi og andre finansielle virksomheder bruger mange kræfter på at imødegå, men der er store udfordringer, og der er mere misbrug, end der har været før«.

For at slå angriberne tilbage bruger Nets' egne eksperter også den kunstige intelligens – blandt andet undersøger selskabet mulighederne for at udvikle og bruge sofistikerede stemmegenkendelsesværktøjer.

Samtidig overvåger Nets' eksperter de mørke hjørner af nettet, det såkaldte dark web, hvor kriminelle udveksler informationer om nye og gamle svindelmetoder.

»Vi ser hele callcentre bygget op omkring særlige svindelkoncepter, hvor folk får udleveret drejebøger og manualer, der fortæller, hvordan de skal snyde folk over telefonen eller via falske mails og beskeder, der med den nye teknologi kan fabrikeres i høj kvalitet på alle sprog«, siger Emil Gade.

Ny rekord i digital svindel

I 2022 blev der ikke begået et eneste fysisk bankrøveri i Danmark. Til gengæld slog den digitale svindel nye rekorder. I 2022 lykkedes det kriminelle at slippe af sted med 425 millioner kroner med alle typer af betalingssvindel.

Det er knap 100 millioner kroner mere end i 2021 og en stigning på 27 procent. Og stigningen er fortsat ind i 2023, fastslår Finans Danmark i sin nyeste rapport om digital svindel, der blev offentliggjort i december sidste år. Og så er det langtfra al svindel, der bliver opdaget, understreger Christiane Vejlø:

> **Vi er slet ikke som mennesker gearede til at være mistroiske på forhånd, når nogen beder os om penge**
> Christiane Vejlø, formand for Finans Danmarks taskforce mod svindel

»Der er et meget stort mørketal på det her område. For der er også stor skam forbundet med at blive svindlet og snydt. Mange vælger at holde det for sig selv. De føler, at de har dummet sig, og derfor går de ikke til politiet. Vi skal al den skam til livs, så folk tør tale mere frit om det her – og dermed også kan advare andre«.

Selv om den digitale svindel vokser, lykkedes det i 2022 de danske banker at stoppe 60 procent af de kendte svindelsager. Sådan endte det også for Ann-Lis Hake i Malmø. Hendes bank anede uråd og stoppede overførslen af hendes bankoplysninger.

Nu har mor og datter ifølge Sydsvenskan aftalt et kodeord, der gør det muligt for dem altid at kontrollere, om de rent faktisk taler med hinanden – og ikke med en svindler.

michael.olsen@pol.dk

FAKTA

Kendte digitale svindelmetoder

Betalingskortsvindel: Typisk misbrug på falske hjemmesider, hvor man lokkes til at handle efterfølgende får ens kortoplysninger misbrugt.

Eller falske sms'er fra f.eks. et pakkefirma, der får ofrene til at klikke på et link og godkende en betaling.

Eller at den kriminelle, efter et identitetstyveri, tilmelder ofrenes betalingskort til en app-løsning.

Netbanksvindel: Offeret overtales til at overføre penge til den kriminelle eller afgiver id, password, MitID-brugernavn til it-kriminelle på baggrund af falske hjemmesider, mails, sms eller telefonopkald.

Kærlighedssvindel: Man får frarøvet sine penge af kriminelle, der f.eks. bruger falske profiler på datingsider. Offeret overtales til at overføre penge.

Investeringssvindel: Svindelsager, hvor man får frarøvet sine penge af kriminelle, der lokker med lukrative investeringsmuligheder.

Direktørsvindel: Hvor en medarbejder typisk bliver narret til at foretage en 'fuldt autoriseret' overførsel fra virksomhedskontoen, ved at en bedrager ringer eller mailer og udgiver sig for at være en højtplaceret person i virksomheden (f.eks. direktøren).

Fakturasvindel: Omfatter svindel med bankoplysninger på leverandører og falske fakturaer. Omfatter også den form for fakturabedrageri, hvor en svindler beder om, at fremtidige fakturaer betales til en ny bankkonto – som svindleren kontrollerer.

Kilde: Finans Danmark

Ekspert: Sådan er du stillet, hvis du bliver snydt på MobilePay

Hvis du bliver svindlet på MobilePay, er det afgørende, hvem du har handlet med, og hvilken betalingsform du har brugt. Her er en guide til, hvordan du er stillet, hvis uheldet er ude.

JONAS PRÖSCHOLD

MobilePay oplyste i denne uge, at de vil indføre nye tiltag for at bekæmpe svindel. Over årene har selskabet i stigende grad set kriminelle gemme sig bag opfundne navne i app'en. Det har kunnet lade sig gøre, fordi man i MobilePay har mulighed for at ændre sit navn, når man sender eller modtager penge – men det skal være slut nu, lyder det.

»Dit fulde juridiske navn vil altid fremgå i appen – både når du swiper og modtager penge. Derfor er det ikke længere muligt at bruge et alias«, siger Anette Bøje, dansk landechef for Vipps MobilePay, der står bag appen, til Ritzau.

Og der er god grund til at være opmærksom på, hvordan og hvem du betaler, når du bruger MobilePay, mener Forbrugerrådet Tænk. For selv om alle transaktioner slutter af med, at du stryger din finger hen over skærmen, så er der stor forskel på, hvordan du er beskyttet.

»Du skal særligt være opmærksom, hvis du sender penge til en privatperson ved at indtaste deres telefonnummer. Her er der som udgangspunkt ikke mulighed for, at du kan få dine penge igen, selv om du er blevet svindlet«, siger Uffe Rabe Krag, politisk chef i Forbrugerrådet Tænk.

Han fortæller, at en betaling til en privatperson på MobilePay rent teknisk svarer til en kontooverførsel. Og her er det meget vanskeligt at få tilbageført penge, selv hvis man er blevet svindlet. Derfor skal man generelt være påpasselig og tænke sig godt om, når man overfører penge til private, da både kontantbetaling, kontooverførsel og private MobilePay-betalinger er en type af betalinger, hvor det er svært – grænsende til umuligt – at få sine penge igen.

> **Man kan ikke gøre så meget andet end at bede om sine penge igen, men det har næppe nogen effekt**
> Uffe Rabe Krag, politisk chef, Forbrugerrådet Tænk

»Man kan ikke gøre så meget andet end at bede om sine penge igen, men det har næppe nogen effekt på en svindler. Derfor er den eneste reelle mulighed at melde sagen til politiet eller rejse et betalingspåkrav ved fogedretten«, siger Uffe Rabe Krag.

Han opfordrer derfor til, at man altid mødes med den person, man vil give penge, og bruger sin sunde fornuft – det gælder især, hvis der er tale om store beløb. Hvis man derimod er ved at købe en varer til 50 kroner på Den Blå Avis, kan man slække lidt på sine forholdsregler.

Høj sikkerhed i butikker

Det er derimod en helt anden verden, hvis du bruger MobilePay til at betale virksomheder eller butikker. Denne type betalinger adskiller sig ved, at du ikke indtaster et telefonnummer, men derimod fem tal eller bogstaver i app'en. Det kan også være, når du bruger MobilePay til kortbetalinger på nettet.

»I denne type betalinger fungerer MobilePay som et bindeled mellem dit betalingskort og virksomheden, og her er det i teknisk forstand en kortbetaling. Det betyder, at du kan benytte dig af de klagemuligheder, der eksisterer hos din bank eller udbyderen af betalingskortet«, siger Uffe Rabe Krag.

Han henviser til, at hvis du har betalt med et betalingskort for en vare eller ydelse, som du ikke har modtaget, har du mulighed for at gøre indsigelse mod betalingen. Betingelserne for at få dine penge igen er, at du kan dokumentere, at du har gjort dit krav gældende over for butikken – eksempelvis ved at sende dem en mail, hvor du har bedt om at få dine penge igen.

Hvis virksomheden nægter eller ikke svarer inden for rimelig tid – det vil typisk være en uge eller to – kan du lave en indsigelse i banken.

Det er dog vigtigt, at du ikke venter for længe, da det også er et krav, at du har handlet inden for rimelig tid. Det vil typisk være seks måneder fra, at du med rimelighed burde have vidst, at du ikke ville modtage varen eller ydelsen.

Er du i tvivl om, hvorvidt en betaling med MobilePay i teknisk forstand er foretaget som en kontooverførsel eller en kortbetaling, kan du altid tjekke dit kontoudtog. Hvis der er tale om en kontooverførsel, vil betalingen have beskrivelsen 'MobilePay' i din netbank.

jonas.proschold@pol.dk