Forstærket kamp mod digital svindel

Det handler om tillid

Fokusområder for indsatsen mod svindel med betalingskort

Nets er Danmarks største udbyder af digitale betalingsløsninger, og vi har derfor en del af ansvaret for at beskytte danskerne mod digital svindel. Vores indsats er fokuseret på at undersøge og analysere omfanget, årsagerne og konsekvenserne af digital svindel – **og anvende den viden til at forebygge fremtidens svindel.**

Her præsenterer vi nogle af de vigtigste tendenser inden for digital svindel, viser omfanget af svindlen og identificerer de mest udsatte områder. Vi fremhæver også danskernes tillid til digitale løsninger – fordi systemerne omkring digital betaling i høj grad er tillidsbaserede.

Omfanget af digital svindel er stigende. Og i takt med fremkomsten og udbredelsen af nye teknologier bliver bekæmpelsen af det endnu mere kompleks. Det er derfor nødvendigt, at alle aktører på området arbejder endnu tættere sammen. Vi deler her nogle af vores indsigter om digital svindel for at bidrage til en del af det arbejde – og til en informeret debat om, hvordan alle aktører kan samarbejde endnu mere om at beskytte samfundet mod svindel.

Nets ser behov for et **specialiseret og mere operationelt beredskab mod digital svindel** bestående af både offentlige og private aktører med indsigt i svindlernes metoder. Det skal sikre en stærk, koordineret indsats mod digitale svindelforsøg gennem nye tiltag.

Udgivelsen er baseret på data, som vi i Nets har særlig indsigt i, interviews med eksterne og interne eksperter, offentligt tilgængeligt data, samt en undersøgelse fortaget i april 2024 i samarbejde med analysevirksomheden Norstat.

I Nets håber vi, at dette kan bidrage til en bredere debat om, hvordan vi kan styrke tilliden i det danske samfund – og forebygge den digitale svindel, som truer med at underminere den.

Udvikling og tendenser inden for digital svindel

Digital svindel giver danske virksomheder sværere kår

Anbefalinger

Digital svindel i et af verdens mest tillidsfulde – og digitaliserede – samfund

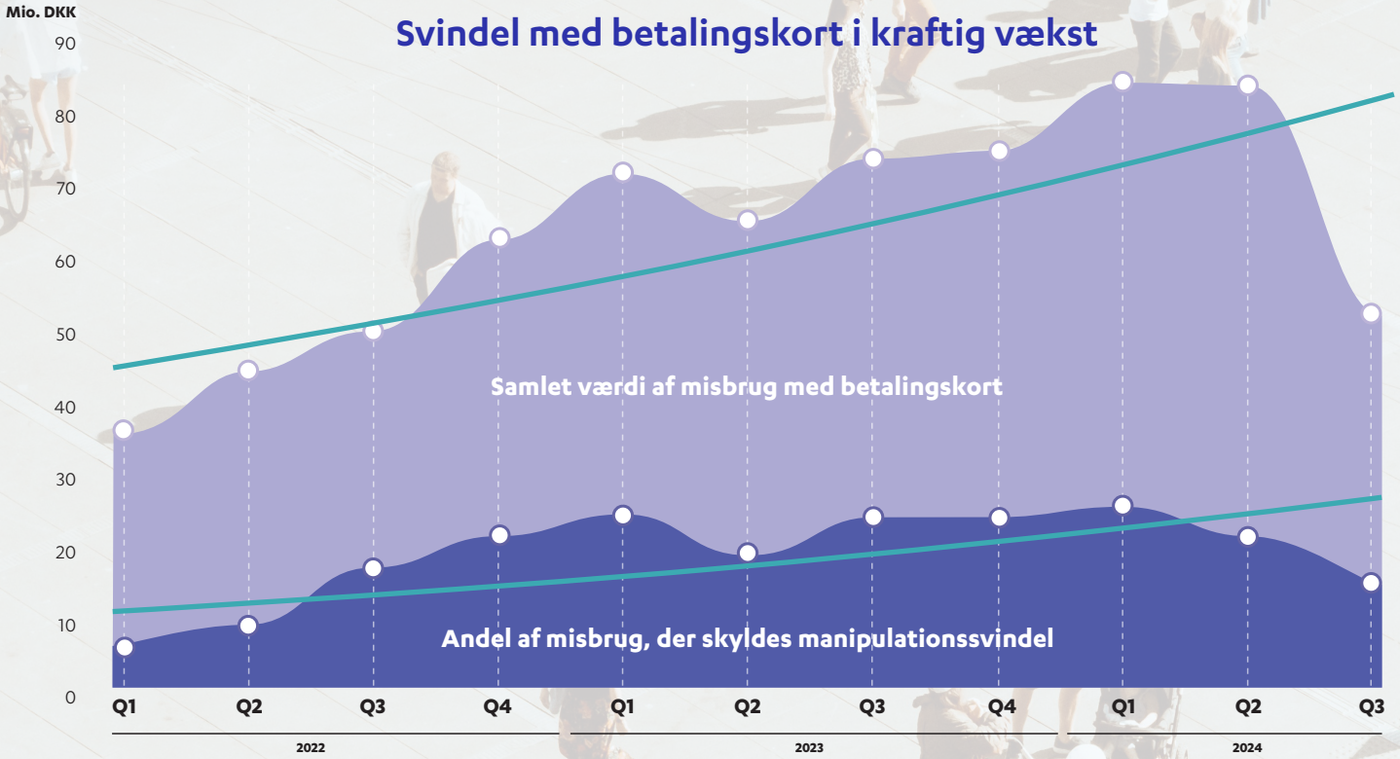
Danmark er kendt som et af de lande, hvor tilliden mellem mennesker og institutioner er højest i verden – og det afspejler sig i vores stadig mere digitaliserede samfund.

Tillid er en central værdi i samfundet og er grundlæggende for vores model for betalingsløsninger. Men digital svindel truer med at erodere tilliden til de løsninger – og mellem borgere, til virksomheder og til myndigheder.

Det er vigtigt, at den enkelte borger er opmærksom på den øgede risiko for svindel. Men det er måske endnu vigtigere, at vi som samfund – på både virksomheds- og myndighedsniveau – i endnu højere grad samarbejder for at kunne opretholde vores tillidsfulde samfund, som er afgørende for den økonomiske og sociale udvikling i Danmark.

Antallet af misbrugssager med betalingskort viser periodiske udsving. Selvom tredje kvartal 2024 viser en nedgang, ser vi en tydelig vækst i det digitale misbrug over tid. De seneste tiltag har haft en positiv effekt på kort sigt, men erfaring viser, at svindlerne konstant tilpasser sig og følger med udviklingen – og at vi i fællesskab må holde fast og fortsætte indsatsen for at værne om tillidsbaserede samfund.

Svindel med betalingskort i kraftig vækst



Samlet værdi af misbrug med danskudstedte betalingskort i Danmark i perioden 2022-2024.
Datagrundlag: Kunder hos Nets og inkluderer både fysisk og digitalt misbrug.
Kilde: Nets

Manipulationssvindel udgør i dag en betydelig – og stadig stigende – andel af det samlede svindelomfang. En af de nyere metoder involverer brugen af social engeneering. Et eksempel herpå er falske kampagner på sociale medier, hvor kendte personers ansigter og stemmer bliver manipuleret og udnyttet for at lokke intetanende individer til at investere større summer i eksempelvis kryptovaluta, hvor man lokkes til at reinvestere efter hurtige gevinster.

Manipulation driver udviklingen

En af de væsentligste årsager til den stigende svindel er manipulation. Kriminelle manipulerer ofre gennem sofistikeret social *engineering* til at udlevere oplysninger eller overføre penge.

Sikkerhedsforanstaltningerne omkring digitale betalinger er de seneste år blevet styrket i høj grad – med øget regulering, 2-faktor-godkendelse ved betalinger på nettet, indførsel af QR-kode i MitID-appen – og andre, lignende tiltag. Paradoksalt er det, at svindlen ikke er faldet, men tværtimod steget i samme tidsperiode.

Det skyldes, at kriminelle også forbedrer deres evner og metoder. Især fremkomsten og brugen af generativ AI har styrket de kriminelle. Det gør det nemmere eksempelvis at lave falske stemmer, billeder, tekster og særligt hjemmesider, som virker troværdige og autentiske.

Teknologiens fremskridt kan dermed udnyttes både til gavn og skade, og vi ser et våbenkapløb mellem de kriminelle – og dem, der forsøger at beskytte vores systemer og tilliden til vores betalingsløsninger.

Social engineering

Social engineering er en måde at udnytte menneskers psykologi, følelser og tillid – og er de seneste år blevet et mere udbredt fænomen inden for digital svindel.

Kriminelle udgiver sig for at være pålidelige personer, virksomheder eller myndigheder for at vinde offerets tillid. De bruger taktikker som efterligning og overtalelse til at få adgang til følsomme oplysninger som adgangskoder, økonomiske data og bestemte systemer. De kriminelle vil i højere grad end tidligere involvere sig og investere tid i bedrageriet, f.eks. ved længere telefonopkald, hvor de skaber et bånd til offeret gennem en opdigtet historie.

Alle kan blive ofre for digital svindel. Det er ikke kun ældre eller uerfarne, men også unge og digitalt kompetente personer, som bliver snydt. Svindlerne tilpasser nemlig deres angreb til forskellige målgrupper, situationer og platforme. De udnytter ofrenes følelse af hast, frygt eller nysgerrighed til at få dem til at handle impulsivt eller uforsigtigt.

Der er mange årsager til, at forskellige mennesker bliver snydt. Ældre kan være mere tilbøjelige til at stole på falske henvendelser, der udgiver sig for at være fra myndigheder, banker og lignende. Yngre og digitalt indfødte er til gengæld ofte så vant til konstant at swipe, at de kan overse små advarselstegn i farten. En ny tendens er, at unge i højere grad end tidligere er i de kriminelles søgelys. Vi ser, at især aldersgruppen 15-24 år ser ud til at være i højere risiko for at komme på afveje – f.eks. lokket af udsigten til store gevinster på kryptovaluta.

NETS HAR SPURGT DANSKERNE:

41%
af danskerne angiver, at de har mindre tillid til sikkerheden omkring betalinger og digital færden, end de havde for tre år siden.

Kun
14%
mener at have mere tillid i dag.

45%
angiver, at de hverken er mere eller mindre tillidsfulde i dag, end de var for tre år siden.

Nets har med hjælp fra analyseinstituttet Norstat undersøgt befolkningens tillid til betalingsløsninger og erfaring med svindel. Undersøgelsen er foretaget i april 2024.

Phishing, smisching, vishing og spoofing
Det er nemt at blive lokket af et godt tilbud, en falsk e-mail eller en venlig stemme i telefonen. Men digital svindel kan have store konsekvenser for både pengepungen og privatlivet.

E-mails, sms'er og opkald – de fleste borgere er efterhånden bekendt med disse svindelmetoder, især phishing, som er blevet et almindeligt begreb. Phishing involverer falske e-mails, der ligner beskeder fra betroede kilder, såsom banker eller myndigheder – hvormed de kriminelle fisker efter borgernes fortrolige oplysninger. Smishing er den samme taktik via sms-beskeder, og vishing sker gennem telefonopkald, hvor kriminelle udgiver sig for at være nogen, de ikke er.

Mens phishing, smishing og vishing har til formål at få folk til at videregive information, handler spoofing om at skabe en troværdig facade for svindleren. Her manipulerer vedkommende sin egen identitet eller placering for at fremstå troværdig. Eksempler kan være:

- **Telefonspoofing:** Her ser det ud som om, opkaldet kommer fra et almindeligt dansk nummer. Det nummer er ofte "lånt" af en intetanende borger. Hvis du forsøger at ringe tilbage, vil opkaldet gå til denne person, som den kriminelle har "lånt" nummeret af og ikke til svindleren selv.
- **E-mail- og hjemmesidespoofing:** Svindleren manipulerer e-mailadresser eller domænenavne, så de ligner officielle kilder, hvilket kan få beskeder til at ligne interne e-mails eller beskeder fra familiemedlemmer.
- **GPS- og IP-spoofing:** Svindleren skjuler sin placering eller identitet ved at manipulere tekniske data, hvilket gør dem sværere at spore.

Tidligere krævede det både betydelig teknisk viden og god sproglig forståelse at udføre disse angreb. Men adgangen til avancerede værktøjer og generativ AI har gjort svindelforsøgene mere sofistikerede og sværere at opdage.

Der er nu luget ud i de sproglige fejl, der før kunne afsløre et svindelforsøg, hvilket gør det vanskeligt selv for digitalt kompetente personer at gennemskue.

Samtidig er omfanget af disse angreb vokset betydeligt. Det er blevet muligt i et hidtil uset omfang at automatisere og skalere svindelforsøgene – og dermed producere og udsende store mængder af falske beskeder og opkald, hvilket gør det sværere for den enkelte borger at forblive opmærksom og at skelne mellem sandt eller falsk.

Falske hjemmesider
Ifølge certificeringsordningen E-mærket eksisterer der over 200.000 falske hjemmesider, der retter sig mod Danmark. Kriminelle efterligner legitime sider for at narre forbrugere til at indtaste deres personlige og finansielle oplysninger. Det kan være en tro kopi af den originale hjemmeside med samme produkter og billeder, men med en lille bevidst tastefejl i forretningens navn eller URL. Her bestiller forbrugerne varer, som de er vant til, men modtager aldrig noget.

På samme måde opretter svindlerne sider, der skal ligne Nets eller MitID for at franarre ofre deres betalingskortoplysninger og andre fortrolige informationer. Nets lukker i gennemsnit 100 hjemmesider om måneden, som er forsøg på at kopiere Nets-sider.

NETS HAR SPURGT DANSKERNE:

66%
af danskerne svarer, at de er bekymrede for, at kunstig intelligens kan bruges til økonomisk svindel eller misbrug ved f.eks. at lede dem til falske hjemmesider, der udgiver sig for at være nogen, som brugeren normalvis har tillid til.

26%
svarer neutralt, mens 9 % er ubekymrede.

CASE: **Digital svindel udfordrer tilliden – politiet kæmper imod for at sikre trygheden**

Digital svindel har en markant indvirkning på tilliden i samfundet. Det handler ikke kun om de økonomiske tab, men om noget langt dybere – borgernes tillid til at kunne navigere sikkert i det daglige liv. Som Kresten Munksgaard bemærker, kan svindel rykke ved den grundlæggende tillid, hvilket kan have en samfundsskadelig effekt, selv når de enkelte beløb ikke er store: "Tillid og tryghed hænger sammen. Det giver tryghed, når vi har tillid til hinanden. Samtidig er det ikke nødvendigvis dem, der føler sig mest utrygge, som er mest udsatte for digital svindel.

Vi taler inden for forebyggelse om funktionel utryghed. Du låser din cykel og din hoveddør, selvom det ikke er din skyld, hvis noget bliver stjålet. Målet er at finde løsninger, der ikke koster for meget eller begrænser borgernes personlige frihed, men som stadig har stor effekt, når det kommer til at skabe tryghed. For politiet handler det om at give borgerne mulighed for at finde den rette balance mellem beskyttelse og frihed. Og for en pris, der er til at betale."

Hvem er i fare for at blive snydt?

Ældre borgere er særligt udsatte for investerings- og datingsvindel, fordi de ofte har større opsparinger, hvilket er med til at gøre dem til et mere attraktivt mål for svindlerne. Selvom de føler sig mere utrygge online, er deres forsigtighed en beskyttelse mod de mindre, men hyppigere former for svindel. Unge derimod falder oftere for billet- og handelssvindel. Deres store tillid til egne digitale evner gør dem mindre opmærksomme på faresignaler, fordi de hurtigt swiper og træffer beslutninger på autopilot. Selvom svindlen ofte involverer mindre beløb, sker det hyppigere, fordi de overser advarselstegnene i farten:

"Det løbende fokus på at forklare om svindel og indsatsen imod den har gjort en forskel for de ældre, der gerne vil lære og er villige til at lytte. Ældre er blevet mere påpasselige og stiller spørgsmål. Når de falder i fælden, er det ofte fordi autoritetstroen tager over. Omvendt kan vi se, at de unge har travlt og føler sig beskyttet af, at de har styr på teknologien. Men at være digitalt indfødt betyder ikke nødvendigvis, at man kan gennemskue svindel – Vi ser også mange unge falde i svindlernes fælder."

Svindelmetoderne udvikler sig – og politiet må følge med

Social manipulation er seneste skud på stammen for de digitale svindlere: Den digitale svindel har gennemgået en markant udvikling over de seneste år. Svindlerne opererede tidligere med at stjæle papkort og koder til netbanker. Da MitID blev indført, blev det betydeligt sværere for svindlere at overtage personers identitet. Men med hver ny sikkerhedsforanstaltning opstår nye svindelmetoder. Derfor er indsatsen mod digital svindel en evig kamp, hvor teknologiske løsninger og kriminelle teknikker udvikler sig side om side. Seneste skud på den kriminelle stamme er avanceret social manipulation.

"Det, vi ser nu, er en stigning i sociale svindelmetoder. De kriminelle udnytter folks tillid til nære relationer, såsom familiemedlemmer eller venner. En typisk fremgangsmåde kan være, at svindleren udgiver sig for at være en ven eller et familiemedlem, der har fået et nyt telefonnummer og beder om økonomisk hjælp via sms eller en platform som Snapchat. Særtegnet ved svindel er i dag skalerbarheden af svindlen, og at det ikke kender geografiske grænser. En svindler kan udføre sin kriminalitet over alt alene ved hjælp af en computer og en mobiltelefon. De kan snyde flere hundrede mennesker på en enkelt dag. Politiet bliver bedre, men det gør de kriminelle altså også – og de leder konstant efter huller i sikkerheden," forklarer Munksgaard.

Nye teknologier skaber kræver nye og større indsatser

Deepfakes er begyndt at dukke op som ny trussel. Selvom det ikke er udbredt i Danmark endnu, er det noget, Kresten og hans team forbereder sig på. I udlandet ses eksempler på

Om interviewpersonen: Kresten Morten Munksgaard er leder af forebyggelse og analyse i Nationalt Center for It-Kriminalitet (NCIK) som er en del af National enhed for Særlig Kriminalitet (NSK). Kresten og hans kolleger følger med i trends og tendenser inden for udviklingen af it-kriminalitet. Og de udvikler forebyggelsesindsatser, der skal bekæmpe kriminaliteten – både selv og i samarbejde med politikredsene og eksterne samarbejdspartnere. Målet er at gøre politiet og resten af samfundet bedre til både at forebygge og opklare kriminaliteten.

deepfakes, hvor kriminelle fx kopierer lydbidder fra et barn og bruger det til at narre forældre.

Samtidig er det blevet både billigere og nemmere for kriminelle at forsøge at svindle mange mennesker. Et nyere eksempel på dette fænomen er Crime as a Service (CaaS), hvor kriminelle grupper tilbyder for eksempel phishing og smishing som svindelydelser, man direkte kan købe. Det betyder, at enhver med økonomiske midler og kriminelle intentioner kan købe såkaldte 'svindelkits' gennem internettets mørke afkroge – og bruge det til at svindle andre, uden selv at besidde den tekniske ekspertise, som tidligere var nødvendig.

Dette skift i kriminalitetens natur betyder, at efterforskningen også må ændre sig. Det kræver en helt ny tilgang og større ressourcer for at kunne håndtere den store mængde af data og de sofistikerede metoder, kriminelle bruger:

"Efterforskning har ændret sig markant de sidste 30 år. Engang handlede det om at gå fra at være på var bund til at finde det ene vigtige bevis. I dag handler det om at sortere. Vi får tonsvis af information hele tiden. Der er milliarder af transaktioner – og vi skal finde den ene transaktion, der skiller sig ud. Det er vitterligt nålen i høstakken. Vi bruger flere ressourcer end tidligere, men vi er nødt til at acceptere, at vi ikke kan opklare alt. Det er en konstant balancegang, hvor vi prioriterer mellem økonomisk kriminalitet og fx mere personfarlige sager."

Samarbejde som det vigtigste middel mod digital svindel

For at kunne imødegå de komplekse og stadigt mere sofistikerede svindelmetoder, arbejder politiet tæt sammen med en lang række aktører – både offentlige og private. Dette inkluderer blandt andet Nets, banker, Erhvervsministeriet og statslige institutioner. Et centralt forum for disse samarbejder er Forum mod IT-relateret økonomisk kriminalitet (FIK). Her sidder op mod 70 forskellige aktører i arbejdsgrupper for at udveksle viden, dele erfaringer og koordinere indsatsen mod digital svindel.

Samarbejdet med Nets er et godt eksempel på, hvordan politiet og private aktører i fællesskab kan styrke indsatsen mod digital svindel. Politiet modtager løbende oplysninger fra Nets, som hjælper med at identificere svindel, finde gerningsmænd og opklare sager. I juni 2024 faldt der dom i en sag, der lev afdækket på baggrund af godt samarbejde. Her blev en ung mand fra Nordjylland idømt fem års fængsel for svindel for mere end 36 mio. kroner.

Men på trods af det omfattende samarbejde, er der stadig en række udfordringer, særligt når det gælder deling af data. Politiet kan ikke altid dele oplysninger, de ønsker at bringe i spil i samarbejdet med private aktører – og det samme gælder den anden vej. Det hæmmer muligheden for hurtige og effektive løsninger i sager, hvor tid er en afgørende faktor. Selv når der er vilje til at handle hurtigt, kan de tekniske og juridiske rammer gøre det svært at dele data i realtid.

"Kampen mod digital svindel skal først og fremmest bekæmpes i samarbejde med andre aktører. Vi er i politiet i vid udstrækning afhængige af et tæt samarbejde med eksempelvis banker, teleudbydere og techvirksomheder. Vi er ikke herre over de platforme, hvor svindlen foregår, og derfor bruger vi mange ressourcer på at drive og udvikle samarbejder med både offentlige og private aktører. Det kræver en vedvarende indsats fra alle parter for at følge med de kriminelle," slutter Kresten Munksgaard.

FEM GODE RÅD TIL BORGERNE FRA POLITIET OG NETS

1. **Tænk en ekstra gang ved uopfordrede henvendelser om penge**
   Modtager du en besked om, at du skal indbetale penge eller betale et gebyr, bør du tjekke, om henvendelsen er reel ved at kontakte virksomheden bag. Svindlere vil ofte forsøge at presse dig til at handle hurtigt. Undgå at lade dig rive med – også selvom der er tale om små beløb..

2. **Tal med andre, før du handler – også selvom du føler dig sikker**
   Spørg andre til råds, når du eksempelvis bliver tilbudt en investeringsmulighed, eller hvis en fremmed tager kontakt til dig via sociale medier – de kan hjælpe dig med at gennemskue, hvorvidt der er tale om svindel. Tal altid med familie og venner, før du overfører penge til personer, du ikke kender.

3. **Vær opmærksom på, hvilken kanal du bliver kontaktet på**
   Svindlere bruger mange forskellige kanaler til at kontakte dig – telefonopkald, sms eller e-mail. Vær ekstra på vagt, hvis du bliver kontaktet på en kanal, du normalt ikke bruger til at modtage sådanne beskeder. Vær altid skeptisk over for uopfordrede henvendelser om betalinger, lån og overførsler.

4. **Vær kritisk over for online annoncer**
   Svindel gennem online annoncer er udbredt, især på sociale medier. Vær derfor på vagt over for annoncer og tilbud, der virker for billige eller for lukrative.

5. **Del aldrig dine personlige oplysninger**
   Hverken Nets, din bank, politiet eller andre myndigheder vil bede dig om dine loginoplysninger til netbank eller koden til dit MitID. Banken sender heller aldrig nogen hjem til dig. Slå koldt vand i blodet og afvis henvendelsen.

Svindelforsøg bliver målrettet den enkelte

Kriminelle udnytter kunstig intelligens til at udvælge ofre for kortsvindel med en hidtil uset præcision. Ved hjælp af generativ AI kan de identificere og målrette deres angreb mod specifikke grupper af mennesker, hvilket gør svindlen både mere effektiv og sværere at opdage.

For eksempel kan de målrette deres angreb mod ældre kvinder i et bestemt område, sende dem en overbevisende besked, og derefter fysisk hente deres kort, måske endda ved at udgive sig for at være en betroet person.

Eksempler på hvad kriminelle får hjælp af generativ AI til at besvare

- Hvad er de mest almindelige danske navne for kvinder født i 1945?
- Hvilke interesser har den gennemsnitlige ældre, danske kvinde?
- Hvilke typer af e-mails eller SMS'er eller breve modtager denne gruppe ofte?

Med få simple spørgsmål kan svindlere skabe meget målrettede angreb.

De kan på baggrund af svarerne sende personlige beskeder eller e-mails, der appellerer til ofrenes interesser eller livserfaringer. De kan udforme beskeder, der ser ud som om de kommer fra velkendte organisationer eller endda venner og familie. Og de kan bruge sprog og terminologi, der virker troværdig for den specifikke målgruppe. Derfra kræver det blot at identificere potentielle ofre i specifikke områder og kontakte dem.

Ved at forstå hvordan generativ AI bliver brugt til at skærpe svindlernes præcision, bliver det tydeligt, hvorfor det er så vigtigt at styrke vores forsvar mod digital svindel. Generativ AI har accelereret kapløbet mellem de kriminelle og bl.a. Nets, der på vegne af banker og forretninger arbejder på at bremse forsøg på kortsvindel.

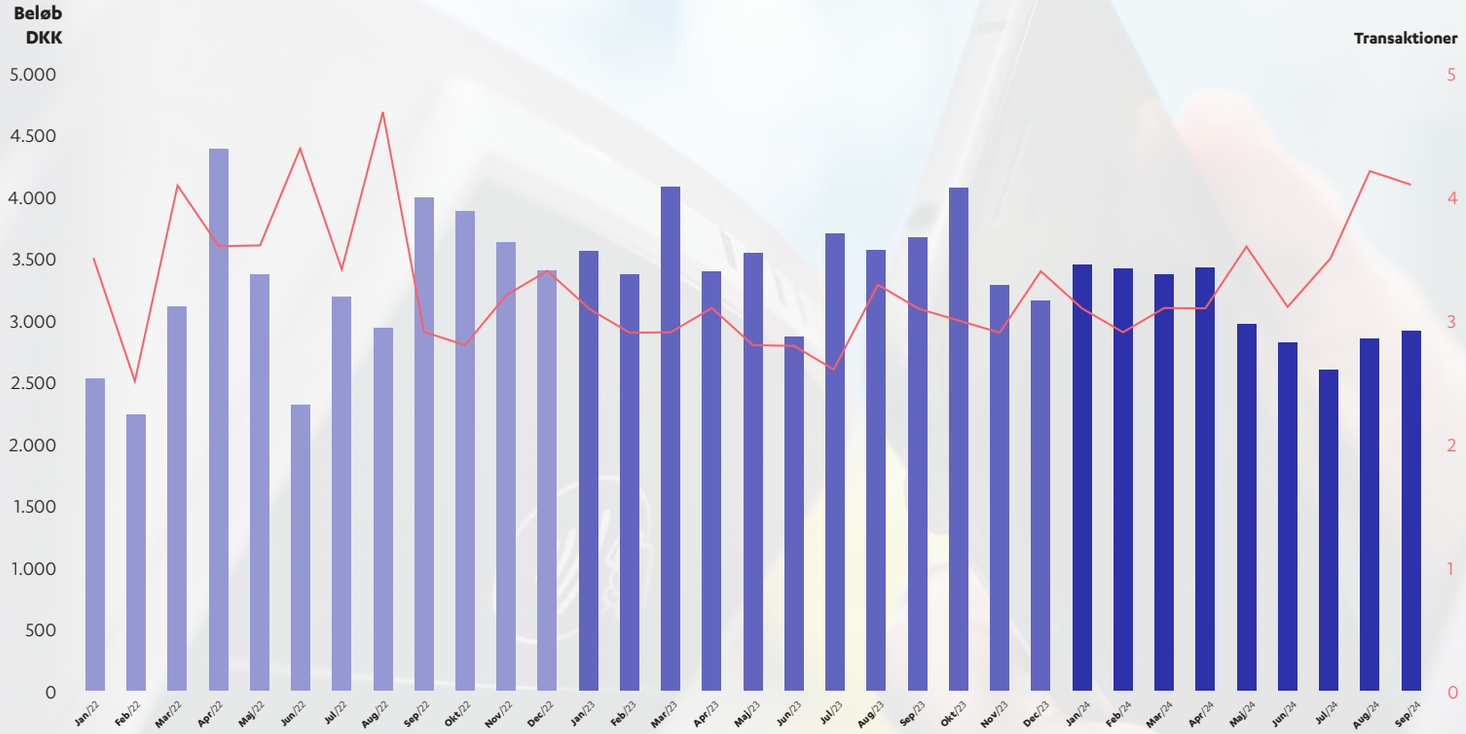
Hvad er på vej?
I takt med den teknologiske udvikling ser vi nye og mere avancerede svindelmetoder dukke op. Her er nogle af de metoder, vi kan forvente at se mere til i fremtiden:

SVINDEL SOM EN SERVICE: Vi ser en øget professionalisering og organisering af kriminelle netværk, der flere steder opererer som helt almindelige virksomheder. Netværkene sælger "svindelpakker" til betalende kunder, der dermed får adgang til målrettede svindelmanualer og brugsanvisninger til eksempelvis phishing.

DEEPFAKES: Udviklingen af deepfakes går også stærkt. Allerede i dag ser vi, at teknologien kan skabe billeder og videoer af kendte personer, der ser ud til at opfordre til bestemte køb eller handlinger. Videoerne og billederne bruges til at narre folk til at tro, at de modtager legitime beskeder fra troværdige mennesker, de stoler på, og gør det endnu sværere at skelne mellem ægte og falsk information.

Med fremkomsten af AI-drevne stemmegeneratorer kan kriminelle efterligne stemmer fra kendte personer – eller endda nogen, ofrene kender personligt. Det kan bruges til at lave telefonopkald, der lyder autentiske, og overbevise folk om at udlevere følsomme oplysninger eller overføre penge.

De kriminelle svindler færre gange per stjålet betalingskort – **men for større beløb**



Gennemsnitligt misbrugsbeløb pr. anmeldt svindelsag og gennemsnitligt antal transaktioner pr. anmeldt svindelsag på danskudstedte betalingskort.
Datagrundlaget udgøres af kunder hos Nets.
Kilde: Nets

Vi ser en tendens til, at svindlere i dag foretager færre, men større transaktioner end tidligere med et stjålet betalingskort.

Tendensen er især tydelig inden for køb af kryptovaluta, rejser og elektronik, hvor store beløb er almindelige – og dermed er sværere for sikkerhedssystemerne at opdage, hvilket giver svindlere mulighed for at maksimere deres udbytte.

Skiftet fra flere små til få store transaktioner tyder på en mere strategisk tilgang fra svindlernes side. Tidligere brugte kriminelle ofte det stjålne betalingskort til at foretage mange små køb, da transaktioner under en vis beløbsgrænse ikke kræver pinkode. Men vores sikkerhedsforanstaltninger i Nets kan fange dette mønster, f.eks. når der sker mange ens, små transaktioner på betalingskortet.

Vi begynder nu at se en ændring i de kriminelles adfærd. De gør i højere grad end tidligere en indsats for at anskaffe koden til betalingskortet – eller indruller det stjålne betalingskort i deres egen digitale wallet, hvis de f.eks. har fået adgang til offerets MitID – for derefter at foretage enkelte, større transaktioner, inden kortet bliver meldt stjålet.

Falske webshops og smishing-svindel for 36 mio. kr. afsløret

Nets' efterforskningsenhed arbejder målrettet på at identificere, forhindre og opklare tilfælde af digital svindel ved at analysere store mængder betalingsdata. I modsætning til den enkelte butik eller bank der kun kan se sine egne transaktioner, har Nets mulighed for at analysere data på tværs. Det gør det muligt at opdage mønstre og sammenhænge, som ellers ville være usynlige. Samarbejdet med politiet, bankerne og teleindustrien sikrer, at disse indsigter hurtigt kan omsættes til konkrete handlinger, der kan hjælpe med at stoppe eller opklare kriminalitet.

En af de største sager om digital svindel i nyere tid

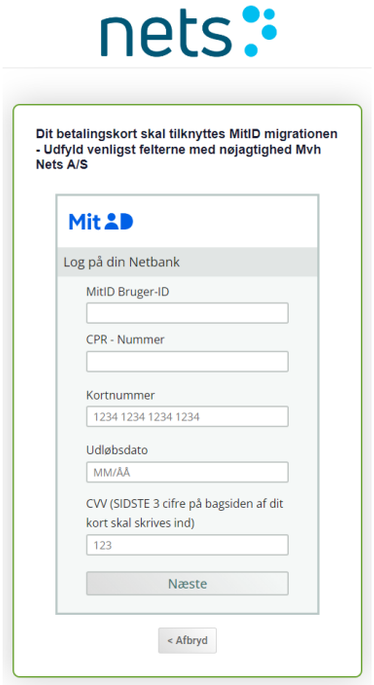
En person havde oprettet falske hjemmesider uden reelle varer og indgået aftaler om betalinger. I 2022 begyndte vedkommende også at misbruge betalingskortoplysninger, som var blevet opsnappet gennem smishing, der blev sendt til borgere over hele Danmark. Det gjorde det muligt for ham at foretage ulovlige internetbetalinger med de kompromitterede kort.

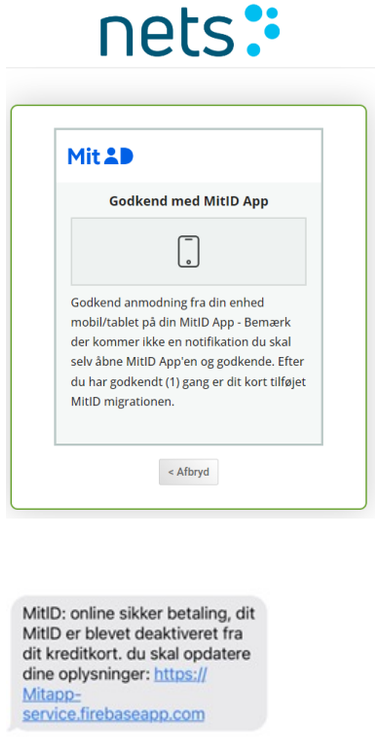
Fra september 2022 til februar 2023 brugte personen over 700 danske betalingskort i mere end 3.200 onlinebetalinger eller forsøg på betalinger til en samlet værdi af omkring 28 millioner kroner.

Når der er tale om så mange betalinger med mange forskellige kortoplysninger, kan det være svært at opdage et mønster. Det skete dog, da efterforsker i Nets genkendte en e-mailadresse, der var blevet brugt i forbindelse med både fiktive webshop-ordrer og oprettelsen af falske betalingsaftaler tilbage i 2021. Den kobling blev afgørende for Nets' videre arbejde med sagen – og for at kunne binde de forskellige svindelforsøg sammen – og bidrage med beviser til politiets sag.

Sagen kort:

- Over 1.000 personer blev ramt af svindlen, og sagen omfattede i alt 5.300 forhold.
- Den dømte stod bag bedrageri for over fem millioner kroner via falske hjemmesider med navne som Po1wer, Elgigantan og Elgigantenn, hvor kunder blev lokket til at købe fiktive varer som elektronik, der aldrig blev leveret.
- Samtidig stod han bag svindel gennem 'smishing' for over 30 millioner kroner ved at sende falske sms'er om opdatering af NemID til MitID, hvor ofre uforvarende udleverede deres MitID-koder og kortoplysninger. Oplysningerne blev derefter brugt til at foretage dyre køb af blandt andet modegenstande, hotelophold og guldbarrer. Over 500 personer vågnede op til tomme bankkonti.
- Den omfattende retssag krævede 18 retsdage, og 80 vidner blev afhørt.
- Nets bidrog med store mængder data, der blev fremlagt i retten.
- En mand blev den 7. juni 2024 idømt 5 års ubetinget fængsel for groft bedrageri og databedrageri til en samlet værdi af cirka 36 millioner kroner. Sagen blev i første omgang anket, men efter betænkningstid accepteret. Personen afsoner nu sin dom.





NETS HAR SPURGT DANSKERNE:

Danskernes har tillid til de sikkerhedsforanstaltninger, der beskytter deres transaktioner, når de foretager betalinger onlinef.eks. verifikation af transaktioner via SMS eller MitID.

53% af danskerne har tillid til, at sikkerhedsforanstaltningerne virker.

30 % vurderer deres tillid til sikkerhedsforanstaltningerne som neutral

Kun 8 % angiver, at de ikke har tillid.

Proaktive tiltag mod digital svindel hos Nets og Dankort

Sådan arbejder Nets med AI og machine learning for at bekæmpe svindel
Nets har i en årrække anvendt machine learning til at styrke misbrugsovervågningen i takt med, at de kriminelle også konstant ændrer fremgangsmåder. Og vi bliver ved med at udvikle vores systemer for at kunne være et skridt foran.

I samarbejde med KPMG byggede vi i Nets den oprindelige model, der udnyttede machine learning til i realtid at identificere usædvanlige mønstre, som mennesker måske overser eller ikke kan nå at reagere på. Den første version af modellen kunne identificere svindel på cirka 20 millisekunder – seks gange hurtigere end et blink med øjet. Modellen udvikles løbende og er trænet til at identificere normal adfærd i stedet for svindelkarakteristika. I stedet for at fokusere på specifikke svindelmønstre, lærer vores model, hvad der er normalt, og reagerer på adfærd, der falder udenfor denne norm.

Dette gør det muligt at opdage svindel, selv når de kriminelle ændrer deres metoder. Med modellen har vi i Nets reduceret svigagtige transaktioner med 40%. Dette, oveni vores eksisterende svindelbekæmpelsesforanstaltninger. Alle data om kortholdere, som benyttes i modellen, er anonymiserede. Nets bruger udelukkende dataene til at genkende mønstre og stoppe svindel.

Sådan arbejder Dankort med sikkerhedsforanstaltninger i kampen mod digital svindel
I en tid hvor digital svindel udgør en stadig større trussel mod både private og virksomheder, er det afgørende at implementere effektive sikkerhedsforanstaltninger.

Dankort har udviklet systemet Dankort Advarselsservice for at imødegå udfordringen. Denne service er et vigtigt værktøj til at beskytte økonomiske transaktioner og sikre, at både forbrugere og virksomheder kan handle trygt online.

Dankort Advarselsservice er en innovativ løsning, der automatisk sender en advarsel til webshops, hvis et misbrugt Dankort er blevet anvendt på deres hjemmeside inden for de seneste 96 timer.

Når banken bekræfter misbruget, modtager webshopejere straks en advarsel fra Nets' misbrugsovervågning. Det giver webshopsene mulighed for at tilbageholde varer eller overvåge specifikke betalingskort – og dermed undgå økonomiske tab, der ville være forbundet med transaktionen.

Svindelens andel i forhold til den samlede omsætning, der behandles gennem Nets' betalingssystemer for den pågældende type af betalingskort, målt i basispoint (misbrug divideret med omsætning gange 10.000).
Datagrundlag: Transaktioner fra Nets' kunder.

Der svindles mindre med Dankortet end andre betalingskort. En mulig forklaring på dette er, at Dankortet er mindre attraktivt for kriminelle, da det ikke kan bruges i udlandet. Samtidig udstedes der væsentligt færre Dankort end f.eks. Visa/Dankort.

CASE: Troværdighed er et værktøj for svindlerne

Sydbank

Hos Sydbank er bekæmpelse af digital svindel en afgørende prioritet. Banken står som en af de førende på området og har opbygget en hel enhed dedikeret til at håndtere denne komplekse kriminalitet. Digital svindel vokser støt, og det gælder både antallet af sager og de beløb, der er involveret. "Vi ser en klar opadgående tendens," siger Louise Schøning, der hver dag arbejder for at forhindre svindel i Sydbanks afdeling i Aabenraa. "Der er flere sager, og svindlerne går efter større summer."

Selvom Sydbank løbende investerer i avancerede sikkerhedssystemer og skærper deres overvågning, bliver metoderne hos de kriminelle mere sofistikerede. Hvor der tidligere var tale om uautoriserede betalinger foretaget af tredjemand er det gået til at være uautoriserede betalinger foretaget af kunden selv, fordi vedkommende manipuleres til det. Derudover udgør svindel via køb uden 3D Secure og phishing i dag en stor del af sagerne. Også sager, hvor kunder bestiller varer fra falske sider og dermed ikke modtager noget, er blevet en hyppig problematik.

Mange sager involverer social manipulation, hvor svindlerne formår at udnytte kundernes tillid. Derfor arbejder Sydbank konstant på at forbedre både de teknologiske løsninger og på at øge og forbedre kommunikationen til kunderne. "Vi må hele tiden være på forkant, og samtidig er det blevet klart for os, at det kræver en samlet indsats på tværs, hvis vi skal kunne matche svindlerne," fortæller Malene Morsing.

Svindlernes troværdige metoder udfordrer kunderne

Hos Sydbank bemærker man, at selvom kunderne ved, at de bør være påpasselige, virker svindlerne så tillidsvækkende, at det ikke altid er muligt. De kriminelle grupper investerer meget tid, når udbyttet kan vise sig at være højt. Ved at bruge oplysninger, de har skrabet fra nettet, skaber de en relation til ofrene. Og til tider opbygger de en så detaljeret historie, at kunderne har svært ved at skelne bedrag fra virkelighed, forklarer Malene Morsing:

"De er blevet enormt dygtige til at opbygge tillid, og det gør, at alle kan falde i. Også dem, der normalt er forsigtige. Vi har for eksempel haft en sag, hvor svindlerne manipulerede en familie en hel weekend og fik familien selv til at tømme deres konti til såkaldte "sikrede konti". Og vi har haft en sag, hvor svindlere udgav sig for at være en konkret rådgiver fra vores bank. De henviste til rådgiverens rigtige profil på LinkedIn – og de ringede fra et nummer, der meget vel kunne ligne et af vores."

I dag kan alle altså være i fare, uanset alder eller digitale færdigheder, siger Malene og forklarer, at unge oftere rammes af småsvindel som billethandelssvindel og agerer mulddyr, mens ældre i højere grad er udsat for eksempelvis falske investeringstilbud. Den bredde i målgrupper og svindelmetoder skaber udfordringer i bankens kommunikationen til kunderne:

"Hvordan kan vi fortælle det klart til alle – uden at skabe forvirring for alle? Det er blevet svært, for svindelmetoderne er både flere og mere sofistikerede. Det er alle kundetyper, alle aldersgrupper, alle typer af svindel. Alle kan falde i nu."

Machine learning og regelbasere koder er blevet en del af hverdagen i banken

Sydbank og Nets arbejder med regelbaserede monitoreringssystemer, som flager mistænkelige transaktioner. Det betyder, at hvis Sydbank ser en række sager med samme mønster – måske med de samme forretningsnumre eller svindelmønstre – kan de samle denne information og dele den med deres kontaktperson i Nets. I

Louise Schøning (tv), Product Owner for Fraud-teamet Malene Morsing (th), Afdelingsdirektør, Sydbank Aabenraa

de tilfælde kan Nets opsætte en række koder eller regler, der blokerer alle typer at den slags transaktioner.

I andre alvorlige tilfælde kan Nets stoppe muligheden for at bruge bankens kort hos specifikke og mistænkelige hjemmesider. Louise Schøning forklarer, at der er tale om en konstant justering af overvågningssystemerne, hvor de hele tiden tilpasses nye svindelmetoder, men at man i Sydbank også må arbejde med at holde en balance:

"Machine learning hjælper os med at identificere mønstre, men det er hele tiden en balancegang – hvis vi stopper noget, en bestemt slags betalinger, risikerer vi også at stoppe alle de gode transaktioner. Dem, der ikke er svindel og som kunderne gerne vil gennemføre. Det bliver en hårfin balance mellem at beskytte kunden og sikre, at brugeroplevelsen stadig er god. Vi vil ikke gøre betalingsoplevelsen besværlig, men vi må aldrig gå på kompromis med sikkerheden."

Samarbejdet er afgørende

I kampen mod svindel er samarbejde på tværs af sektoren afgørende, og Sydbank deler derfor jævnligt erfaringer med både andre banker, betalingsudbydere og myndigheder. Når nye svindlere hopper fra bank til bank, kan de prøve at undgå overvågning, men et samarbejde, der også inkluderer myndigheder og private aktører, vil kunne minimere risikoen.

"Vi ser ofte, at svindel går på tværs af bankerne. Det er helt nødvendigt at skabe en stærk front, så vi kan dele de erfaringer og data, der kan forhindre svindel."

Sydbank arbejder også på at informere alle kundetyper om sikkerhed, uanset digitale færdigheder og alder. Banken afholder blandt andet arrangementer sammen med Ældresagen og deltager i Pengeugen, hvor de rådgiver unge om svindelrisici.

"Kommunikation er helt afgørende – alle skal forstå, hvad de skal være opmærksomme på, uanset alder og digitale færdigheder," slutter Malene Morsing.

Digital svindel giver danske virksomheder sværere kår

Når forbrugerne handler online, forventer de at kunne betale sikkert og nemt med deres betalingskort. Desværre udnytter kriminelle denne tillid og forsøger at svindle med falske eller stjålne kortoplysninger. Det skader samtidig de mange virksomheder, som risikerer økonomiske tab både gennem tilbageførsler af svindeltransaktioner og tab af solgte varer. Håndteringen af svindelsager kræver betydelige ressourcer og kan tynge driften i virksomhederne.

Kriminelle kan få fat i betalingskortoplysninger på flere måder, f.eks. ved at:

- hacke en webshop og stjæle kundedata
- installere skadelig software på en forbrugers computer eller mobil
- købe stjålne kortoplysninger på det sorte marked
- lokke oplysningerne ud af kortholder ved hjælp af phishing og lignende

Regningen ender ofte hos virksomheden: Når en forbruger opdager svindlen på sin konto og gør indsigelse, fører det til en såkaldt chargeback, hvor banken tilbagefører beløbet fra virksomheden til forbrugeren. Virksomheden mister således både mulig indtjening – og varer.

En anden indirekte måde hvorpå virksomheder mister omsætning, er gennem markedet for kopivarer, som kriminelle sælger på falske hjemmesider. Forbrugere, der måske ellers ville have købt en original vare fra en dansk virksomhed, ender i stedet med at købe en kopi på en svindelside. Dermed mister de lovlige virksomheder potentielle salg, som kunne løbe op i betydelige beløb over tid.

Hvor bruger de kriminelle andres penge?
Når kriminelle får adgang til stjålne kortoplysninger, bruger de dem steder, hvor de hurtigt kan omsætte de stjålne midler til penge eller værdifulde varer. Disse brancher har det til fælles, at de tilbyder let omsættelige varer og tjenester, der enten kan bruges direkte af svindlerne eller hurtigt sælges videre.

Kontanter og pengeoverførsler

Favoritten blandt kriminelle er kontanter og pengeoverførsler. Det omfatter også køb af såkaldt Quasi Cash, f.eks. gavekort, spillechips eller forudbetalte taletidskort. Quasi cash er en storfavorit, da det hurtigt kan omsættes til andre varer eller kontanter – og nemt kan købes i både butikker og online.

Rejser – fly og transport, hoteller og restauranter

Rejse- og transportsektoren, herunder hoteller og restauranter, er hårdt ramt. Kriminelle bruger stjålne kortoplysninger til at booke flybilletter og hotelværelser, som enten bruges af kriminelle selv eller sælges videre til intetanende tredjeparter. Rejser er en af de kriminelles foretrukne kategorier, da der kan gå længe, før offeret opdager, at deres kort er blevet misbrugt.

Detailhandel og stormagasiner

En anden betydelig kategori er detailhandel og stormagasiner. Kriminelle bruger kreditkort til at købe højværdigenstande, som let kan videresælges på det sorte marked. Det omfatter alt fra elektronik og smykker til luksusvarer, der opretholder høj efterspørgsel og værdi.

Telekommunikation, IT og elektronik

Inden for telekommunikation, IT og elektronik, køber de kriminelle dyre gadgets som smartphones, computere og andre højteknologiske enheder. Produkterne har både høj værdi og er lette at sælge videre.

Underholdning, sport og fritid

Underholdning, sport og fritid er ligeledes et attraktivt område for svindlere. Her købes billetter til events, abonnementer og medlemskaber, som derefter sælges videre. Dertil kommer forlystelsesparker og sportsanlæg, hvor svindlere kan købe adgang og tjenester.

Services

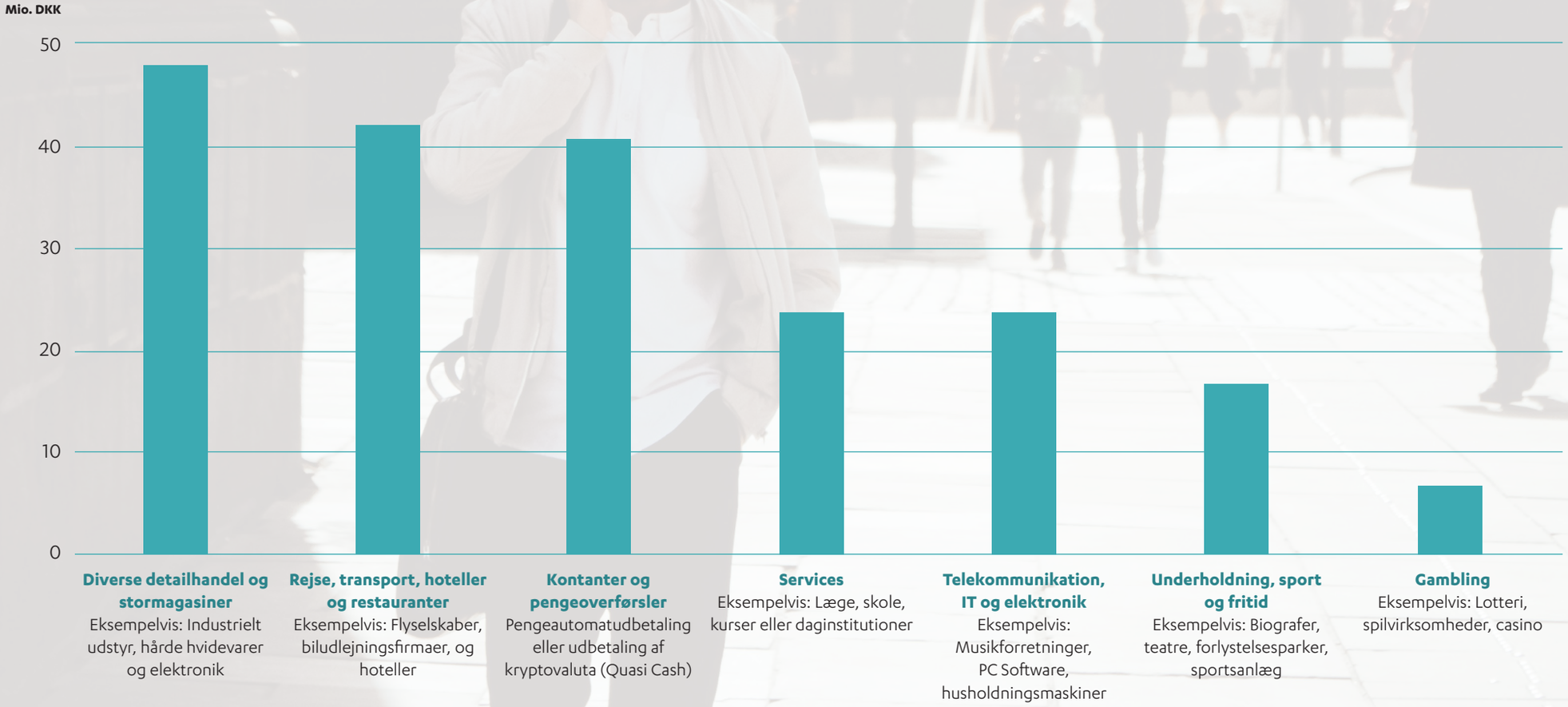
Services dækker over en bred vifte af tjenester, hvor kriminelle kan udnytte stjålne kortoplysninger, såsom privatlæger, skoler eller kurser. Selvom det kan virke som et overraskende mål, udgør de en attraktiv mulighed for svindlere. For eksempel kan tilmeldingsgebyrer til kurser betales med et stjålent kort, hvorefter adgangen sælges billigere til andre. Det skaber økonomiske og administrative udfordringer for de berørte institutioner og tjenesteudbydere, der må håndtere konsekvenserne af svindelen.

Gambling

I forhold til gambling anvender de kriminelle de stjålne kreditkortoplysninger til f.eks. at finansiere spilleaktiviteter, både online og i fysiske casinoer, hvor det kan være svært at spore oprindelsen af midlerne.

De kriminelles foretrukne brancher og butikstyper for brug af stjålne kortoplysninger viser, hvor omfattende og tværgående svindel er. For at beskytte både forbrugere og virksomheder er det afgørende, at både finansielle institutioner, virksomheder og serviceudbydere implementerer solide sikkerhedsforanstaltninger.

Særligt detailhandlen og rejsebranchen er **hårdt ramt af misbrug**



Samlet værdi af misbrug med danskudstedte betalingskort i perioden januar-september 2024 fordelt på branchekategorier. Datagrundlag: Kunder hos Nets.
Kilde: Nets

CASE: **Stigning i digital svindel truer danske virksomheder**

Kriminelles gruppers svindelmetoder er blevet mere sofistikerede. De har fået adgang til avancerede værktøjer, som gør det nemmere at ramme både store og små virksomheder. Dansk Erhverv ser konsekvenserne. Organisationen oplever en markant stigning i henvendelser fra medlemmer, der er ramt af svindel. Problemet er omfattende, og løsningerne kræver indsats fra både virksomhederne – og samfundet omkring dem.

Fra phishing til falske hjemmesider: En bred palet af svindeltyper

Tidligere var det især store virksomheder, der blev ramt af digital svindel. Sådan er det ifølge Dansk Erhverv ikke længere. Særligt AI-værktøjer gjort det nemmere for svindlere at kopiere hjemmesider én-til-én. Det skaber problemer for både forbrugere og virksomheder.

"Vi oplever en markant stigning i digital svindel, særligt de seneste år. Klassisk phishing er stadigvæk den største synder, men de kriminelle bliver mere sofistikerede, især med brugen af AI," forklarer Jens Wedenborg, der er chefkonsulent i Dansk Erhverv og til daglig arbejder med at analysere digital handel.

De mest udbredte former for digital svindel inkluderer phishing, såkaldt CEO-fraud og kopiering af online platforme, hvor kriminelle via falske hjemmesider udgiver sig for at være velkendte virksomheder. Det kan være svært for forbrugere at gennemskue svindel, fordi mange af de falske hjemmesider fremstår næsten identiske med de originale.

Dansk Erhverv oplever, at flere små virksomheder udsættes for kopiering af deres hjemmesider – samtidig med at de store også fortsat bliver ramt. Det skaber udfordringer for forbrugerne, som ofte ikke opdager svindlen før sent i købsprocessen, hvis overhovedet. Det skaber problemer for den enkelte og udfordringer for virksomhederne, som går glip af salget. De store virksomheder har flere ressourcer til at kæmpe imod problemet, mens små og mellemstore virksomheder desværre ofte har oplevelsen af at stå mere alene med problemet.

"De kriminelle er egentlig ligeglade med, om det er Bauhaus eller Bentes Blomsterbinderi – de går efter sårbarheder, hvor end de kan finde dem," fortæller Henrik Lundgaard Sedenmark, der er fagchef for betalinger og detailhandelssikkerhed i Dansk Erhverv.

Svindlen spænder fra hurtigt og dårligt udførte angreb – til målrettede, avancerede metoder som fx infiltration af rigtige mailkorrespondancer mellem virksomheder. De kriminelle kan arbejde meget sofistikeret og ændrer kontooplysninger på forskellige online platforme for at kanalisere reelle betalinger over på deres egne konti. "Denne form for svindel kræver en større indsats fra de kriminelle, men gevinsten kan være enorm, når der pludselig overføres en million euro til den forkerte konto," fortæller Henrik Sedenmark.

Erosion af tillid

Digital svindel har ikke kun konsekvenser for virksomhederne – det påvirker forbrugernes tillid til e-handel som sådan. I årene siden coronapandemien har flere oplevet et skred i forbrugernes adfærd, hvor mistillid til digitale platforme er vokset med en stigende skepsis over for online shopping til følge.

"Tilliden er under pres, og det kan på sigt erodere det samfund, vi er glade for med mange frie muligheder for den enkle. Det er en alvorlig konsekvens af den stigende digitale svindel. Det rammer på den måde ikke kun den enkelte virksomhed og forbruger, men også hele den måde vi handler og interagerer på," fortæller Henrik Sedenmark.

Henrik Lundgaard Sedenmark, Fagchef for betalinger og detailhandelssikkerhed

Jens Wedenborg, chefkonsulent

Virksomheder skal udpege en sikkerhedsansvarlig
En undersøgelse fra Dansk Erhverv viser, at 38 procent af de adspurgte virksomheder har oplevet svindel. Alligevel er det kun 20 procent af disse sager, der bliver anmeldt til politiet. Det efterlader et enormt mørketal. Mange virksomheder undlader at anmelde denne form for kriminalitet, fordi de ikke har ressourcerne til at forfølge sagen – eller mangler de fornødne sikkerhedsrutiner til at håndtere både udfordringerne og anmeldelserne. Dertil kommer, at man i nogle virksomheder kan opleve en svækket tillid til, at myndighederne har ressourcerne til at gribe ind i forbindelse med svindelsagerne. De kan skabe en opfattelse af, at anmeldelser ikke nødvendigvis fører til konkret hjælp eller resultater.

De større virksomheder har i stigende grad implementeret avancerede sikkerhedsforanstaltninger, mens mindre virksomheder ofte ikke har de samme muligheder. Det er vigtigt, at virksomheder – uanset størrelse – udvikler stærkere tilgange til at tage ansvar for deres digitale sikkerhed. En klar anbefaling fra Dansk Erhverv er derfor, at alle virksomheder bør have en ansvarlig, der kan håndtere digitale trusler og hurtigt reagere, hvis der sker et angreb:

"Uanset virksomhedens størrelse er det essentielt, at én person har ansvaret og kan sikre, der bliver reageret hurtigt, hvis der er behov for det. Mange små og mellemstore virksomheder har endnu ikke en klar sikkerhedsprocedure, og det kan koste dyrt," lyder det fra Henrik Lundgaard Sedenmark.

For små og mellemstore virksomheder kan det være særligt udfordrende at identificere og forhindre svindel. Mange mindre virksomhedsejere er ikke bevidste om, at de i praksis også er IT-chefer og sikkerhedsansvarlige i deres egen forretning. Det gør de mindre virksomheder særligt sårbare over for digitale angreb.

Det er også vigtigt, at virksomheder anmelder svindel, selvom det kan virke tidskrævende. På den måde kan politiet få et bedre overblik over problemets omfang og sætte ind over for mønstre i udviklingen.

En nødvendig indsats på tværs af sektorer
Dansk Erhverv samarbejder med flere aktører, herunder bankerne, Nets og politiet, for at bekæmpe digital svindel. En del af det gode samarbejde sker i regi af Forum mod IT-relateret økonomisk kriminalitet (FIT), hvor politiet er tovholder.

"Sammen har vi en fælles interesse i at bekæmpe digital svindel. Jo mere vi kan samarbejde og dele information, jo stærkere står vi mod svindel. FIT fungerer, fordi alle i samarbejdet selv har forpligtet sig til fællesskabet, og fordi politiet sidder for bordenden. Politiet sætter holdet, og det giver samarbejdet den nødvendige legitimitet," fortæller Henrik Lundgaard Sedenmark.

Med de rette initiativer og samarbejder minimeres risikoen for at blive ramt af de kriminelle. Og det øger sikkerhed for, at både virksomheder og forbrugere kan navigere trygt i det digitale landskab. Det er afgørende, at alle – fra små virksomheder til store koncerner sammen med myndighederne – tager ansvar og handler hurtigt, når der er angreb fra svindlere. Det er helt nødvendigt, hvis vi skal stå imod de kriminelle og kæmpe for at opretholde den tillid, der er så vigtig for vores samfund.

"Uanset hvilke tekniske løsninger vi udvikler, vil kriminelle finde nye veje. Det er et fælles ansvar at bidrage til at skabe en mere sikker digital fremtid. Kriminaliteten er mangefacetteret, og derfor skal løsningerne også være det," slutter Henrik Lundgaard Sedenmark.

FEM GODE RÅD FRA DANSK ERHVER OG NETS

1. **Udpeg en sikkerhedsansvarlig i virksomheden**
For at kunne reagere hurtigt og effektivt på digital svindel er det vigtigt, at én person har et klart ansvar for sikkerheden. Denne person bør være fortrolig med virksomhedens IT-sikkerhedsprotokoller og handle hurtigt i tilfælde af trusler.

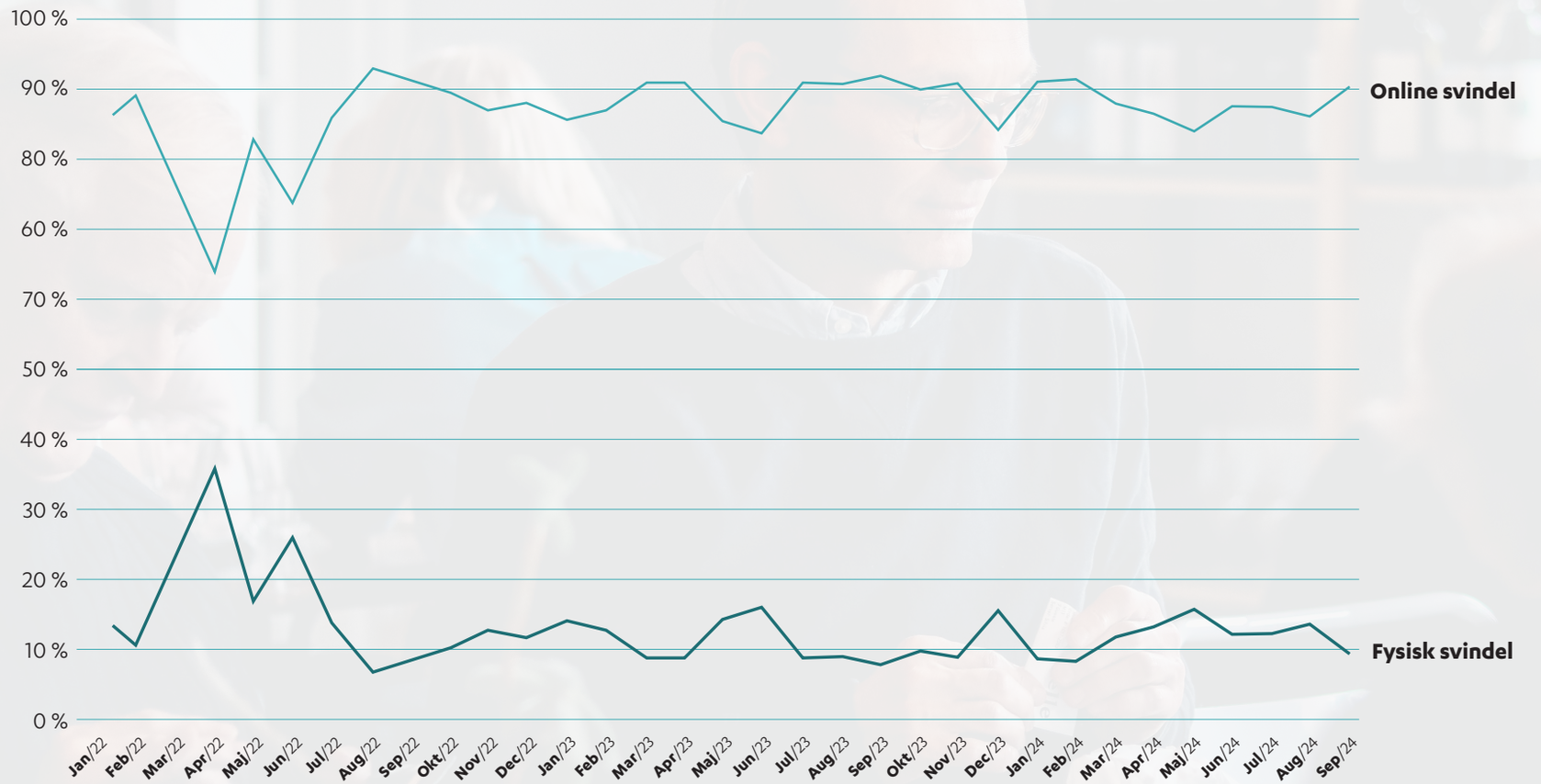
2. **Opbyg rutiner for sikkerhedsanmeldelse og dokumentation**
Sørg for at anmelde al svindel – også svindelforsøg – til politiet og eventuelle relevante myndigheder. Anmeldelser bidrager til, at myndighederne får et bedre overblik over problemets omfang. Dokumentér desuden alle hændelser, så virksomheden kan lære af dem og forbedre sine sikkerhedsprocedurer løbende.

3. **Undervurder ikke phishing – lav rutiner for sikkerhed i e-mails**
Phishing er fortsat en af de mest udbredte svindelmetoder, så opret rutiner, der gør medarbejderne i stand til at identificere mistænkelige e-mails og links.

4. **Tilpas sikkerheden til virksomhedens behov og svindelmønstre**
Virksomheder har forskellige udfordringer, og derfor er det vigtigt at skræddersy sikkerhedsprocedurerne. Overvej fx at automatisere visse tjek eller integrere et system, der flagger ordrer med usædvanlige leveringsadresser, browserindstillinger eller IP-adresser, så virksomheden kan reagere hurtigt på mulige svindelforsøg.

5. **Tjek for risikofaktorer – adresser, IP'er og sprogmønstre kan afsløre svindel**
Indfør en kontrolrutine for bestillinger med høj værdi eller usædvanlige forhold, så potentielle svindelforsøg opdages tidligt. Vær særligt opmærksom på bestillinger, hvor leveringsadressen fx er en udenlandsk postboks i et for virksomheden atypisk land. Kombinér dette tjek med fx oplysninger om browserens sprogindstillinger og land.

Dynamikken mellem **fysisk** og **online** svindel



Misbrug med danskudstedte betalingskort i tidsperioden januar 2022- september 2024 fordelt på hhv. online og fysisk handel i butikker. Datagrundlaget udgøres af kunder hos Nets. Data er eksklusive Dankort og Visa/Dankort, da sammenlignelige data ikke har været mulige at frembringe.
Kilde: Nets

I dag er online svindel den mest udbredte form for svindel. For de kriminelle er der mindre risiko forbundet med at operere online. De kan for eksempel bestille varer til anonyme postbokse eller adresser og arbejde fra enhver lokation i verden.

En nyere metode er, at de kriminelle stjæler eller køber kortoplysninger på dark web og tilføjer oplysningerne til deres egen digitale wallet på telefonen – og har dermed et digitalt betalingskort på telefonen. Det gør det muligt for dem at gennemføre transaktioner uden at have det fysiske kort.

Historisk set har svindelmetoder ændret sig i takt med, at nye sikkerhedsforanstaltninger er blevet implementeret. Det betyder også, at når der strammes op på den digitale sikkerhed, kan svindlere skifte fokus tilbage til fysiske metoder. Denne skiftende dynamik kan komme i bølger, hvor online og fysisk svindel veksler i hyppighed.

Forbrugernes tillid til både digitale og fysiske betalingssystemer er afgørende. Derfor er det vigtigt at fortsætte med at udvikle og forbedre sikkerhedsforanstaltninger på begge fronter for at beskytte mod svindel og opretholde tilliden.

Den løbende indsats mod svindel i Danmark viser sig også at have en positiv effekt. Tal fra Den Europæiske Centralbank og Den Europæiske Banktilsynsmyndighed indikerer, at vi i Danmark har et lavere svindelniveau sammenlignet med EU-gennemsnittet (2024 Report on Payment Fraud).

NETS HAR SPURGT DANSKERNE:

Mens mange er bekymrede for online sikkerhed, viser undersøgelsen, at kun **7%** er bekymrede for at blive udsat for svindel eller misbrug, når de foretager betalinger i fysiske butikker.

Nets’ svindelbekæmpelse

Teamet bag svindelbekæmpelsen i Nets består af 20 nordiske ansatte, der arbejder døgnet rundt på at minimere svindel ved at monitorere transaktioner og identificere potentielle svindelmønstre for vores bank- og virksomhedskunder.

Værn

- **24/7 transaktionsmonitorering**
- **Regelbaseret overvågning baseret på kunstig intelligens og machine learning**
- **Consumer protection service, der hindrer autorisationer fra butikker, som fremmer f.eks. abonnementsfælder og distribution af kopivarer**
- **Identifikation af misbrugte betalingskort, spærring samt kommunikation med banker og kortholdere**
- **Monitorering af mistænkelige butikker og hjemmesider**
- **Konstant opdatering af svindellister**

Analyse

- **Implementering af værn mod alle kendte svindelmønstre, hvor mistænkelige køb, som afviger fra etablerede betalingsvaner, bremses hurtigt**
- **Analyse af mistænkelig kortholderadfærd, som opfanges og flages**
- **Analyse af seneste svindeltendenser**

Efterforskning

- **Løbende samarbejde med politiet for at forhindre og opklare svindelsager**
- **Samarbejde med internationale efterforskningsenheder for at bekæmpe og forhindre svindel**
- **Deltagelse i nationale, regionale og internationale fora om svindelbekæmpelse**

Træning og uddannelse

- **Løbende kundemøder og vejledninger om bedre svindelbeskyttelse**
- **Fokus på kampagner og samarbejde med myndigheder**
- **Orientering til bank- og butikskunder om seneste svindeltendenser**

Nets arbejder hver dag for at beskytte samfundet mod digital svindel

I Nets er vi bevidste om vores særlige rolle i forhold til det danske betalingssystem og i kampen mod digital svindel – dette som både samarbejdspartner for bankerne og leverandør af betalingsløsninger for virksomhederne.

I begge henseender arbejder medarbejderne i Nets hver dag proaktivt for at beskytte samfundet mod digital svindel, som har enorme økonomiske og sociale konsekvenser – for den enkelte person, der rammes af svindel, for den lille eller store virksomhed samt for den generelle sammenhængskraft og tillid i Danmark.

Nets vil gerne bidrage til at forsvare samfundet og vores kunder mod de kriminelle – både inden, under og efter et muligt svindelforsøg:

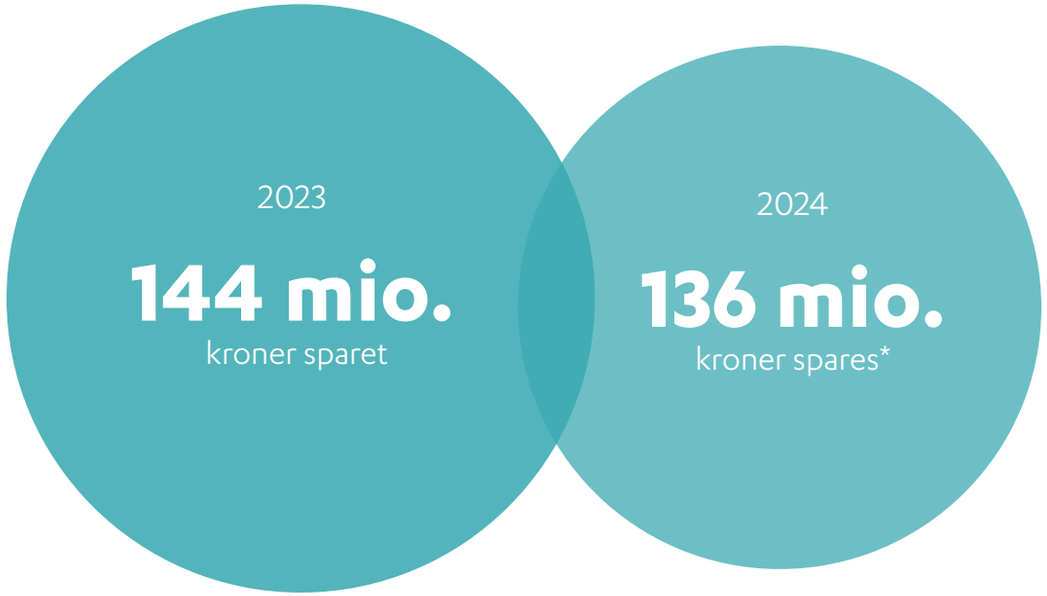
Før
Nets arbejder mod at forebygge mest mulig svindel ved at overvåge transaktioner og identificere mistænkelige betalingsforsøg. Vores systemer er designet til hurtigt at identificere mulig svindel, og vi samarbejder tæt med danske banker for løbende at opdatere sikkerhedskoderne baseret på de nyeste svindeltyper. Derudover gennemfører vi en grundig introduktion for og kontrol af nye virksomhedskunder for at sikre, at de er legitime og ikke involveret i ulovlige aktiviteter som f.eks. salg af ulovlige varer eller hvidvaskning af penge.

Under
Når mistænkelige aktiviteter opdages mens de sker, kan vi hurtigt gribe ind. For eksempel kan vi advisere butikker og forretninger, inden de sender varer, der er købt på mistænkelige kort. Det daglige samarbejde med forretninger hjælper med at forhindre svindel, inden det sker. Samtidig arbejder vi tæt sammen med både bankerne og politiet, når vores systemer opdager mistænkelige mønstre.

Efter
Efter en svindelsag hjælper vores efterforskningsenhed politiet med at opspore gerningsmænd. Vi undersøger, hvordan kortoplysninger er havnet hos kriminelle, f.eks. ved at identificere datalæk, så vi kan forhindre misbrug af andre kort, der kan være berørt. Gennem analyse af data og mønstre fra svindelsager forbedrer vi løbende vores systemer, så vi kan opdage og reagere endnu hurtigere på nye svindelmetoder.

I 2023 og 2024 har Nets forhindret op mod en million forsøg på svindel med danskudstedte betalingskort

Det har og vil spare bankerne mere for omtrent 280 millioner kroner i perioden.



*Estimat baseret på faktisk tabsbesparelse frem til rapportens tilblivelse i oktober 2024

Øget sikkerhed for forbrugere og forretninger med Nets' consumer protection service

Nets' consumer protection service hjælper med at beskytte banker og deres kunder mod økonomiske tab og besvær. Med denne service har vi det seneste år stoppet **995.367 misbrugsforsøg, hvilket har resulteret i en samlet besparelse på over 500 millioner kroner.**

Servicen reducerer risikoen for, at forbrugere selv foretager risikofyldte transaktioner, som kan være svigefulde eller uigennemsigtige – herunder f.eks. dating-sites, kopivarer og abonnementsfælder. Mange af disse transaktioner præsenteres som attraktive tilbud eller "gode handler," der i virkeligheden er designet til at narre forbrugeren. Ved at analysere advarselsmønstre og opdage potentielt skadelige transaktioner og misbrug, beskytter Nets kortholderen mod at blive fanget i økonomiske fælder, der ofte er dyre og besværlige at komme ud af.

Det kan for eksempel være datingsider, hvor man lokker forbrugeren til at chatte med profiler, der er automatiserede chatbots – for derefter at opkræve betaling for yderligere "kommunikation." Vi ser også varer, som sælges til en brøkdel af den oprindelige pris, men hvor produktet enten er af en kopi af ringe kvalitet – eller slet ikke eksisterer. Abonnementsfælder er en anden hyppig svigefælde, hvor et tilsyneladende billigt tilbud fører til dyre aftaler.

Med denne service beskytter vi kortholderen mod faldgruber, hvor et tilbud, der ser for godt ud til at være sandt, viser sig at være netop det – en fælde.

Denne indsats er en del af vores kontinuerlige arbejde – og samarbejde med bankerne – for at styrke beskyttelsen mod svindel. Hos Nets er vi dedikerede i arbejdet med at gøre det stadig sværere for kriminelle at lykkes med deres svindelnumre og leder konstant efter nye måder at forbedre sikkerheden og tilliden til betalingssystemerne.

Hvad er abonnementsfælder?
Abonnementsfælder er vildledende tilbud, der lokker forbrugere til at tilmelde sig tjenester, der virker gratis eller meget billige, men reelt medfører dyre abonnementer. Typiske produkter omfatter hudplejeprodukter, fitnessabonnementer og populære goodie-bokse, som ofte reklameres på sociale medier. Brugerne accepterer vilkår, der med småt skjuler komplicerede afmeldingsprocedurer, høje gebyrer og urimelige priser.

Anbefalinger

Digital svindel er ikke kun er en trussel mod den enkelte borger eller virksomhed – men også mod det danske samfunds fundamentale værdier som tillid og økonomisk sammenhængskraft.

Vi skal som samfund gør vores yderste for at være foran de kriminelle. Det er en permanent oprustningskamp, der kræver vi kan agere hurtigere og mere fleksibelt. Enkeltstående tiltag og traditionelle regulatoriske processer kan ikke længere følge med. Der er brug for en mere agil tilgang, hvor offentlige og private i samarbejde kan agere på nye trusselsbilleder, så snart vi ser dem. Og som foregangsland for digitalisering bør vi anse det som vores pligt at skubbe resten af Europa i samme retning under EU-formandskabet i 2025.

Vi håber, at politiske beslutningstagere, virksomheder og offentligheden vil tage imod dem som en invitation til yderligere dialog. Vi lytter også meget gerne til andre forslag, der kan bidrage til en styrket indsats.

1. **Etablér et operationelt beredskab til styrket offentligt-privat samarbejde i kampen mod digital svindel**
2. **Styrk det offentlige Danmarks modstandskraft mod digital svindel**
3. **Forstærk de juridiske rammer**

1. Etablér et operationelt beredskab til styrket offentligt-privat samarbejde i kampen mod digital svindel

Vi foreslår, at erhvervsministeren tager initiativ til at nedsætte et operationelt beredskab mod digital svindel med beslutningsmyndighed til at igangsætte tiltag, dele data og implementere teknologiske løsninger i kampen mod digital svindel. Beredskabet bør arbejde tæt sammen med både nationale og internationale aktører for at styrke indsatsen. Medlemmerne bør bestå af både offentlige og private aktører, der har ekspertise og ressourcer til at bekæmpe svindel effektivt. Betalingsudbydere, banker, teleindustrien, sociale medieplatforme og andre relevante aktører – med myndighederne for bordenden. Det er essentielt, at beredskabets medlemmer har mandat til at implementere løsninger i egne organisationer.

Konkrete initiativer, beredskabet kan igangsætte for at styrke indsatsen mod digital svindel:

a. Udvikling og brug af kunstig intelligens

- Udvikle et fælles forsvar mod digital svindel ved at anvende mønstergenkendelses-teknologi, der kan analysere og genkende mønstre i store mængder transaktions-data. Systemet skal kunne samle data, som aktørerne i dag er forhindret i at dele med hinanden og på den baggrund dele anbefalinger med de enkelte aktører.
- Udvikle en hjemmeside, app eller anden teknologi, der ved hjælp af kunstig intelligens kan hjælpe borgere med at vurdere, om konkrete hjemmesider, links, SMS'er eller e-mails er svindel. Dette vil også sænke borgernes reaktionstid og forhindre forhastede klik.

b. Vidensudveksling og vurdering af trusselsbillede

- Etablering af sikre kanaler for dataudveksling mellem alle deltagende aktører. I dag er berettigede hensyn til datasikkerhed og konkurrence med til at forhindre en effektiv indsats mod svindel. En afgrænset gruppe bør have muligheder for at dele svindelrelateret viden med relevante aktører for bedre og hurtigere at kunne forhindre svindel.
- Regelmæssige møder for at drøfte det aktuelle trusselsbillede og dele indsigt om nye svindelmetoder, diskutere og implementere nye tiltag i kampen mod svindel..

2. Styrk det offentlige Danmarks modstandskraft mod digital svindel

For effektivt at bekæmpe digital svindel – og værne om tilliden til det offentlige – er det nødvendigt med en styrket indsats inden for uddannelse, ressourcer og kompetencer i det offentlige Danmark.

a. Uddannelse og forskning

Udviklingen og brugen af AI er essentiel i kampen mod digital svindel. Det kræver, at vi uddanner flere med de nødvendige kompetencer at forberede fremtidige generationer til at bekæmpe digital svindel. Vi foreslår, at uddannelses- og forskningsministeren tager initiativ til at inkludere cybersikkerhed og AI som vigtige emner i kommende gymnasie- og universitetsreformer. Der bør ligeledes sikres større støtte til forskning og udvikling inden for digital sikkerhed og AI.

b. Ressourcer og kompetencer

Indsatsen mod digital svindel – og brugen af AI – kræver både bedre ressourcer og stærkere kompetencer i det offentlige Danmark. Trods, vi også mangler nødvendige kompetencer i virksomhederne, er det offentliges rolle i kampen mod svindel essentiel – og der er i dag et substantielt løngab mellem den private og den offentlige sektor, som vi anbefaler, at regeringen tager initiativ til at udligne for at tiltrække kvalificerede medarbejdere til det offentlige.

c. Øget samarbejde og koordinering

Vi opfordrer justitsministeren til at allokere tilstrækkelige ressourcer til NSK og andre relevante myndigheder for effektivt at bekæmpe digital svindel. Forbedret koordinering mellem NSK og SKAT er afgørende for at adressere tværgående svindelmetoder. Øget internationalt samarbejde gennem Interpol er nødvendigt, da digital svindel opererer globalt og kræver en koordineret indsats.

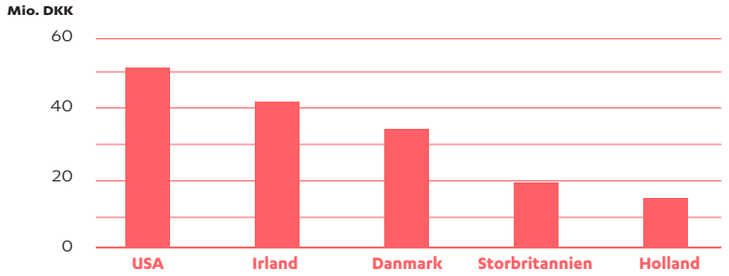
Anbefalinger

3. Forstærk de juridiske rammer

a. Regulering af sociale medier

En stor del af digital svindel sker gennem brugen af sociale medier. Vi foreslår, at digitaliseringsministeren tager initiativ til at etablere klare lovgivningsmæssige rammer, der muliggør mere effektiv bekæmpelse af digital svindel på sociale medier. Der bør herunder indføres krav om, at aktører som META bør reagere inden for en bestemt varselstid, såfremt der er begrundet mistanke om svindel på deres platform. I Nets er vi er klar til at understøtte dette arbejde ved at hjælpe META og andre platforme med at identificere svindel.

Danske betalingskort misbruges på sociale medieplatforme



Værdi af misbrug med danskudstedte betalingskort i tidsperioden oktober 2023 – september 2024 fordelt på de fem mest eksponerede lande. Datagrundlaget udgøres af kunder hos Nets.
Kilde: Nets

Den primære del af misbruget på danske betalingskort kan henføres til USA og Irland. Her har mange store teknologi- og sociale medievirksomheder hovedsæde. Misbrugte danske kort bruges ofte til at finansiere annoncer på disse platforme med det formål at udføre phishing-angreb og promovere falske hjemmesider eller produkter. Samtidig kan man på mange amerikanske hjemmesider handle ved at udfylde kortoplysninger uden ekstra sikkerhed som 2-faktor godkendelse.

b. Regler for tilbageholdelse af betalinger

I dag er Nets forpligtet til at gennemføre en betaling senest 1 arbejdsdag efter købstidspunktet, hvilket er reguleret i betalingsloven og EU's PDS2 direktiv. Nets foreslår, at i tilfælde, hvor der er berettiget mistanke om svindel, at Nets og øvrige betalingsudbydere da får 3-4 dage til at undersøge, hvorvidt mistanken om svindel er berettiget inden betalingen gennemføres.

For at styrke bekæmpelsen af digital svindel bør reglerne for, hvor længe betalingsudbydere må tilbageholde betalinger ved rimelig mistanke om svindel, justeres. De nuværende korte tilbageholdelsesperioder er ofte utilstrækkelige til at gennemføre en grundig undersøgelse, hvilket øger risikoen for, at svindeltransaktioner gennemføres og resulterer i økonomi-ske tab.

c. Brug af interne data i kunstig intelligens

I dag findes der mange forskellige regelsæt vedrørende brugen af data i teknologiske løsninger baseret på kunstig intelligens. Mens Nets forstår samfundets berettigede ønske om at beskytte borgers persondatarettigheder, vil øget brug af personlige købsmønstre i vores machine learning overvågning af transaktioner styrke kampen mod digital svindel.

Vi foreslår, at regeringen indfører lovgivningsmæssige ændringer, der tillader betalingsudbydere at bruge personlige data i deres AI-baserede svindelbekæmpelsesmetoder på en forsvarlig måde. Dette inkluderer strenge retningslinjer og sikkerhedsforanstaltninger for at beskytte brugernes privatliv og sikre, at data kun anvendes til svindelbekæmpelse.

d. Nye produkter og teknologier skal indeholde en obligatorisk svindelkonsekvensanalyse

For at beskytte imod svindel, bør alle nye produkter og services indeholde krav om svindelkonsekvensanalyser. Fx er introduktionen af deepfake og stemmegenkendelser i høj grad anvendt af kriminelle til at begå svindel, men hverken EU's forordning om digitale tjenester (DSA) eller forordningen om kunstig intelligens har fokus på svindel.

Den danske regering bør arbejde for indførelse af tiltag i EU-lovgivning, der sikrer produkters potentielle misbrug i forhold til digital svindel.