DANMARKS NATIONALBANK

DIGITALISERING

ANALYSE | Betalinger
29. april 2024 | Nr. 7

Svindel og misbrug med digitale betalinger i Danmark

Skrevet af

Marcus Clausen Brock
Senior Retail Payments Economist

mcb@nationalbanken.dk
+45 3363 6072

Tidsforbrug

23 sider

Digitale betalinger er blevet meget udbredt, og det har givet nye muligheder for, at kriminelle kan foretage svindel. Det gælder også i Danmark, som på betalingsområdet er blandt de mest digitaliserede lande i verden. De danske betalingssystemer er sikre og svære at misbruge. Derfor bruger svindlerne i højere grad metoder, hvor borgere og medarbejdere i virksomhederne manipuleres til at foretage og godkende de svindelrelaterede betalinger.

Misbruget med danske betalingskort er på et lavt, men stigende niveau

Kortmisbruget har i en årrække været faldende, men er de sidste par år steget. Stigningen skyldes bl.a., at svindlerne har fundet nye metoder til at tilegne sig borgernes betalingskort. Sammenlignet med Europa er kortmisbruget i Danmark lavt.

Det meste af kortmisbruget sker i udenlandsk e-handel og i større grad uden for Europa

Nye sikkerhedsforanstaltninger og europæisk krav om tofaktor-godkendelse kan have medvirket til, at kortmisbruget i større grad sker uden for Europa. Det vurderes, at bredere anvendelse af kortspærring i geografiske områder eller betalingssituationer kan begrænse misbrug med danske betalingskort i udenlandsk e-handel.

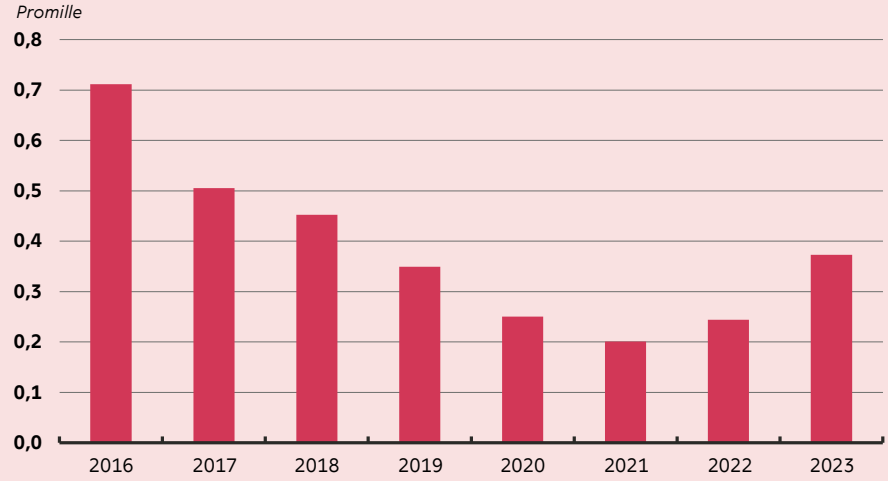
Svindel med kreditoverførsler skyldes særligt tilfælde, hvor borgerne selv overfører penge til svindleren

Det er vigtigt, at både borgere og medarbejdere er opmærksomme på, at de i stigende grad er i risiko for at blive manipuleret til selv at godkende svindelrelaterede betalinger. Når en borger eller medarbejder selv har godkendt betalingerne, hæfter de eller virksomheden i de fleste tilfælde for det økonomiske tab.

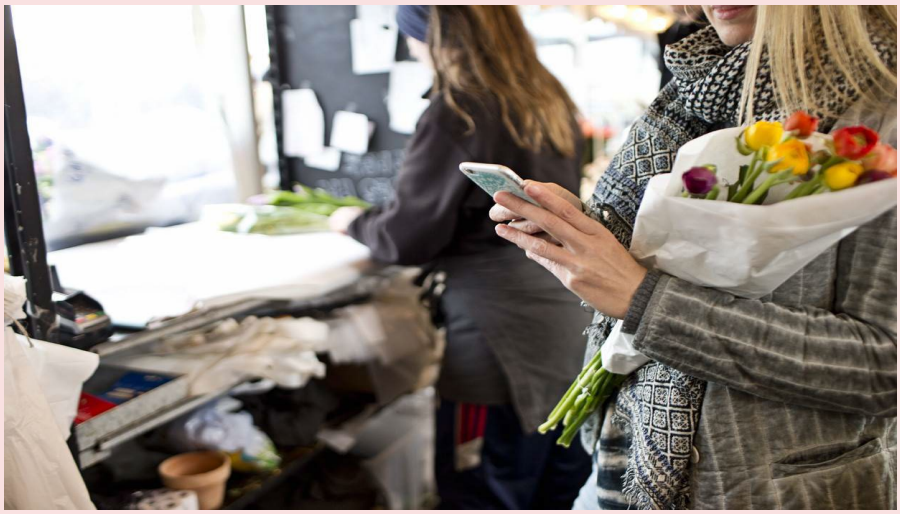
Hvorfor er det vigtigt?

Et af Nationalbankens hovedformål er at understøtte sikre og effektive betalinger i Danmark. Svindel kan ramme alle i befolkningen, og i takt med at danskerne i stigende grad anvender nye digitale betalingsløsninger, ændrer de kriminelles muligheder sig også for at foretage digital svindel. Det er derfor vigtigt, at borgere og virksomheder er opmærksomme på, hvordan de risikerer at blive udsat for digital svindel, så de fortsat har tillid til, at deres betalinger kan gennemføres sikkert.

Hovedfigur: Misbrug med betalingskort er på et lavt, men stigende niveau



Anm.: Samlet misbrug med dansk udstedte betalingskort i forhold til den samlede kortomsætning.
Kilde: Danmarks Nationalbank.



Emner

Betalinger

Digitalisering

Finansiel regulering

Statistik

01
Introduktion

I Danmark bruger borgerne digitale betalingsløsninger til over 92 pct. af den samlede værdi af alle betalinger. Det skyldes i høj grad, at borgerne foretrækker digitale betalingsløsninger, og at det danske samfund løbende digitaliseres.[1] Den digitale betalingsinfrastruktur er sikker og effektiv, og digitaliseringen har medvirket til, at det er blevet hurtigere og nemmere for de fleste borgere at foretage betalinger.

Den øgede brug af digitale betalingsløsninger betyder dog også, at borgerne og virksomhederne er mere eksponerede over for digital svindel. I 2023 var den samlede svindel og misbrug med digitale betalingsløsninger i Danmark ca. 627 mio. kr. Knap halvdelen af værdien vedrørte misbrug med betalingskort, som primært misbruges på udenlandske hjemmesider, fx ved betaling på en falsk netbutik. Svindel med overførsler fra bankkonti, også kaldet kreditoverførsler, er steget de seneste år og var i 2023 på niveau med kortmisbruget. I modsætning hertil er antallet af fysiske røverier mere end halveret i løbet de sidste 10 år, og der blev hverken i 2022 eller 2023 registreret bankrøverier i Danmark.[2] Disse tal understreger, at de kriminelle i høj grad er blevet digitale og følger udviklingen i samfundet.

Nye teknologier, sikkerhedsforanstaltninger og europæiske regler for tofaktor-godkendelse af digitale betalinger har gjort det vanskeligt for de kriminelle at gennemføre digitale betalinger og kreditoverførsler fra netbanken, uden at borgere eller medarbejdere skal godkende transaktionen. Svindel og misbrug med digitale betalingsløsninger sker derfor i stigende grad, ved at det lykkes de kriminelle at manipulere borgere eller medarbejdere i virksomhederne til at betale eller overføre penge til de kriminelle.

Udviklingen i svindelmønstrene vidner om, at de kriminelle løbende har tilpasset deres metoder til nye teknologier og regler. Det er derfor vigtigt, at borgere og virksomheder i et digitalt samfund er opmærksomme på, at de i stigende grad risikerer at blive manipuleret til at godkende svindelrelaterede betalinger.

Ud over svindel, hvor det lykkes at manipulere borgere eller medarbejdere til at foretage betalingerne, så er der ved digitale betalinger også risiko for misbrug af betalingsoplysninger til at gennemføre betalinger uden borgernes godkendelse. Det sker fx ved misbrug af betalingskort, hvor det lykkes de kriminelle at tilegne sig et betalingskort og den tilhørende pinkode.

I denne analyse defineres *svindel* med betalingsløsninger som de tilfælde, hvor det lykkes svindlerne at bedrage og manipulere borgere eller medarbejdere til selv at foretage betalinger eller kreditoverførsler til de kriminelle. *Misbrug* med betalingsløsninger defineres som svindlerens brug af betalingsløsninger uden direkte involvering af den svindelramte.

[1] Se Danmarks Nationalbank, Kontanters rolle i et samfund med lavt brug af kontanter, *Danmarks Nationalbank Analyse*, nr. 21, november 2023 (*link*).
[2] Se Danmarks Statistik, *Kriminalitet 2022,* december 2023 (*link*), og Finans Danmark, *Et år uden bankrøverier – for andet år i træk,* januar 2024 *(link).*

Det er første gang, at Nationalbanken har mulighed for at belyse udviklingen i svindel og misbrug med både betalingskort og kreditoverførsler. Det skyldes nye data vedrørende kreditoverførsler.[3] Derudover anvendes data for kortmisbruget, som Nationalbanken offentliggør kvartalsvis.

[3] Data for svindel og misbrug med kreditoverførsler er baseret på pengeinstitutternes indberetninger til Finanstilsynet i medfør af Den Europæiske Banktilsynsmyndighed, *EBA guidelines on fraud reporting under PSD2*, se tabelbilag. Finanstilsynet har desuden bidraget til analysen med gode kommentarer.

02

Misbrug med betalingskort er på et lavt, men stigende niveau

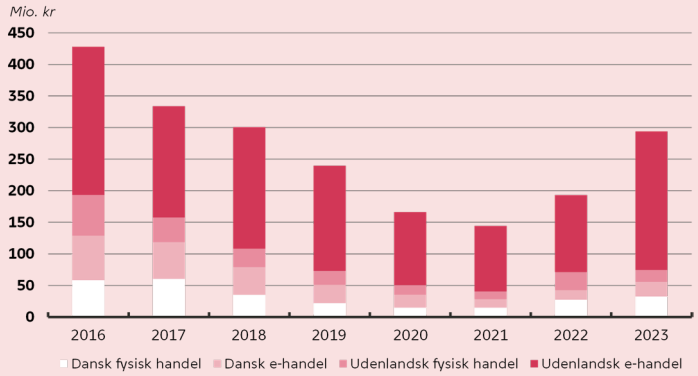
Når danske borgere eller virksomheder køber varer og tjenester i en butik eller på internettet, så sker det i stigende grad med digitale betalingsløsninger som betalingskort og mobiltelefonen. Det er både sikkert og nemt at betale med betalingskort, men indimellem lykkes det svindlere at foretage betalinger uden kortholderens godkendelse. Det kan fx skyldes, at kortholderen har fået stjålet sit betalingskort, efter at svindleren har afluret pinkoden, eller at svindleren har tilegnet sig kortoplysningerne, fx ved at franarre kortholderen dem via betalingslink på SMS eller ved betaling på en falsk netbutik.

Det samlede registrerede misbrug med betalingskort udstedt af danske pengeinstitutter var i 2023 ca. 294 mio. kr., se figur 1.[4] Misbruget var fordelt på ca. 232.000 misbrugsrelaterede kortbetalinger. Det giver en gennemsnitlig misbrugsværdi pr. betaling på knap 1.300 kr. Den samlede misbrugsværdi skal ses i sammenhæng med, at den totale kortomsætning i 2023 var ca. 800 mia. kr. Dermed var kortmisbruget i gennemsnit 369 kr. pr. omsat mio. kr.

FIGUR 1

Misbrug med betalingskort er steget det seneste par år

Samlet værdi af misbrug med betalingskort i fysisk handel og på internettet

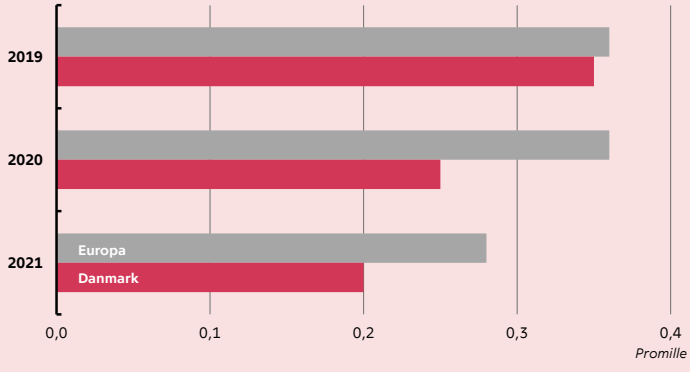


Anm.: Misbrug med dansk udstedte betalingskort. Fysisk handel indeholder også misbrug med betalingskort i hæveautomater.
Kilde: Danmarks Nationalbank.

FIGUR 2

Misbrug med betalingskort er lavere i Danmark sammenlignet med resten af Europa

Samlet misbrug med betalingskort i forhold til den samlede kortomsætning



Anm.: Data for Europa er kun tilgængeligt frem til og med 2021. Europa omfatter det såkaldte SEPA-område, som består af alle EU- og EØS-lande, Andorra, Monaco, San Marino, Schweiz, UK og Vatikanstaten.
Kilde: Danmarks Nationalbank og Den Europæiske Centralbank (*link*).

[4] Dansk udstedte betalingskort er typisk Dankort, Mastercard og Visakort udstedt af danske pengeinstitutter.

Misbruget med betalingskort har i en længere årrække været faldende. Det hænger i høj grad sammen med nye sikkerhedsforanstaltninger og nye europæiske regler for godkendelse af betalinger, se boks 1. Derudover var både 2020 og 2021 præget af omfattende nedlukninger af samfundet som følge af corona-pandemien, hvilket gjorde det svært for svindlere at aflure pinkoder og stjæle fysiske betalingskort. Siden 2021 er kortmisbruget dog steget, hvilket både kan skyldes, at borgerne handler mere på udenlandske hjemmesider, og at svindlerne har fundet nye metoder til at få adgang til borgernes betalingskort.

I en international sammenhæng er det relative kortmisbrug lavere i Danmark end i resten af Europa. I 2021, hvor misbruget for betalingskort senest blev opgjort på tværs af Europa, var den danske misbrugsandel 0,20 promille, mens det europæiske gennemsnit var 0,26 promille, se figur 2. Det relative kortmisbrug er dog steget i Danmark siden 2021. En lignende tendens er observeret i Sverige.[5]

BOKS 1

Europæiske regler for godkendelse af betalinger

Siden januar 2021 har alle digitale betalinger i Europa, herunder også betalinger med betalingskort og mobilbetalinger, skullet godkendes ved hjælp af mindst to forskellige faktorer - den såkaldte tofaktor-godkendelse. Det gælder både i fysisk handel, hvor reglerne trådte i kraft 1. januar 2018, og ved betalinger på internettet fra 1. januar 2021.

De to faktorer skal enten være noget, som kun betaleren ved (fx en pinkode); noget, som kun betaleren er (fx ansigtsgodkendelse); eller noget, som kun betaleren har (fx betalingskort eller mobiltelefon).

Betalingstjenesteudbyderen, dvs. typisk betalerens bank, har mulighed for at undtage bestemte transaktioner for tofaktor-godkendelse, hvor risikoen for svindel og misbrug vurderes lav. Det gælder fx kontaktløse betalinger i fysiske forretninger op til 350 kr. og internetbetalinger op til 225 kr.[1]

[1] Se Europa-Kommissionens delegerede forordning (EU) 2018/389 af 27. november 2017 (*link*).

Størstedelen af misbrug med danske betalingskort sker i udenlandsk e-handel

Misbrug med danske betalingskort sker hovedsageligt på udenlandske hjemmesider, se figur 3. I 2023 var det samlede misbrug med dansk udstedte betalingskort i udenlandsk e-handel 219 mio. kr., svarende til ca. 75 pct. af det samlede kortmisbrug.

Der kan være flere årsager til, at betalingskort i højere grad bliver misbrugt på udenlandske hjemmesider. En af årsagerne er, at kravene om tofaktor-godkendelse ved betalinger ikke gælder uden for EØS.[6] Det muliggør misbrug af danske betalingskort uden kortholderens godkendelse, hvis svindlerne har fået kendskab til betalingskortoplysningerne og den udenlandske hjemmeside ikke har indført lignende sikkerhedsforanstaltninger til godkendelse af betalingen.

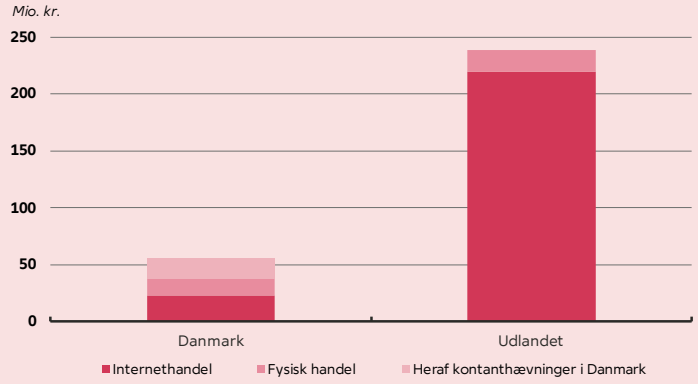
I 1. halvår 2023 foregik knap halvdelen af det samlede kortmisbrug i udlandet uden for EØS, selvom mindre end en femtedel af den samlede udenlandske omsætning med danske betalingskort blev foretaget i området. Dermed er det relative kortmisbrug med danske betalingskort markant højere uden for Europa end i Europa og især i forhold til Danmark, se figur 4.

[5] Se Sveriges Riksbank, *Betalningsrapport 2024*, marts 2024 (*link*).
[6] Det Europæiske Økonomiske Samarbejdsområde, EØS, dækker EU-landene, Norge, Island og Liechtenstein.

FIGUR 3

Størstedelen af misbrug med betalingskort sker i udlandet

Fordeling af det samlede misbrug med betalingskort i 2023

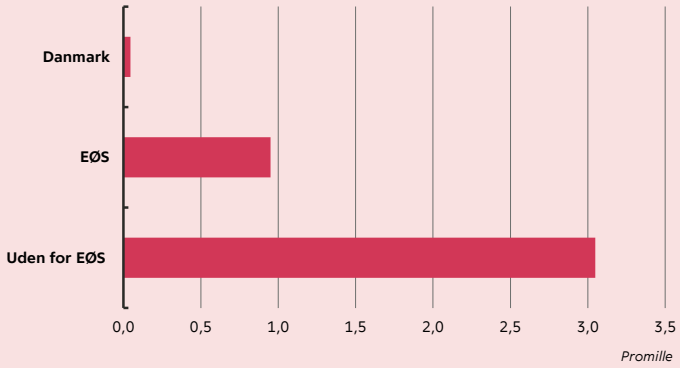


Anm.: Misbrug med dansk udstedte betalingskort. Fysisk handel i udlandet indeholder også kontanthævninger, da opdeling ikke er mulig.
Kilde: Danmarks Nationalbank.

FIGUR 4

Det relative kortmisbrug er størst uden for Europa

Samlet misbrug med betalingskort i forhold til den samlede kortomsætning



Anm.: Misbrug med dansk udstedte betalingskort. Opgørelsen dækker 1. halvår 2023. Det Europæiske Økonomiske Samarbejdsområde, EØS, dækker EU-landene, Norge, Island og Liechtenstein.
Kilde: Pengeinstitutternes indberetninger til Finanstilsynet i medfør af Den Europæiske Banktilsynsmyndighed, *EBA guidelines on fraud reporting under PSD2,* og Danmarks Nationalbank.

Svindlernes metoder til at franarre betalingskortoplysninger

Svindlerne benytter bl.a. falske netbutikker til at få adgang til borgernes eller virksomhedernes kortoplysninger. Det sker fx, ved betaling på en falsk netbutik i forventning om at modtage en vare eller ved kortbetalinger i forbindelse med falske investeringsmuligheder. Se flere eksempler i boks 2.

Svindlerne bruger også i høj grad såkaldt phishing og smishing, hvor svindlerne ved hjælp af henholdsvis e-mail eller SMS franarrer betalingskort- og personoplysninger. Det sker fx, ved at svindlerne udgiver sig for at være fra banken eller danske myndigheder.[7]

Svindlernes metoder gør det vanskeligt at bekæmpe svindlen og kortmisbruget, idet borgerne selv oplyser kortoplysningerne og i nogle tilfælde også godkender betalingen. Svindlerne har dermed mulighed for både at modtage den oprindelige betaling og anvende kortoplysningerne til at foretage andre køb eller transaktioner. Reglerne for tofaktor-godkendelse begrænser dog umiddelbart svindlernes mulighed for at foretage yderligere opkrævninger inden for EØS, hvilket kan være med til at forklare, hvorfor den relative svindelværdi er større uden for EØS, se figur 4.

[7] Se Finans Danmark, *Netbanksvindel* (*link*).

BOKS 2

Eksempler på svindel og misbrug med betalingskort og kreditoverførsler

Falske netbutikker: Misbrug med betalingskort sker primært på internettet. Det kan fx være i tilfælde, hvor betaleren i god tro foretager betalinger på falske netbutikker og kortoplysningerne efterfølgende misbruges. Derfor anbefaler bl.a. Digitaliseringsstyrelsen og Center for Cybersikkerhed, at man kontrollerer netbutikkens ægthed, hvis den virker mistænkelig.[1]

Svindel ved privat samhandel: Ifølge bankernes interesseorganisation, Finans Danmark, involverer en stor del af den digitale svindel sociale medier og handelsplatforme som Facebook Marketplace og DBA.[2] Det kan fx være falske annoncer for koncertbilletter eller boligudlejning, hvor der typisk er mange interesserede købere, hvilket får borgerne til hurtigt at overføre penge i forventningen om at sikre sig varen. Politiet opfordrer derfor til, at borgerne mødes fysisk for derved at sikre, at man modtager den vare, man betaler for.[3] Derudover tilbyder flere billetformidlere en løsning til videresalg af billetter, så billetten er verificeret og garanteret, hvilket sker mod betaling gennem billetudstederen.

Phishing og smishing: I flere tilfælde forsøger svindlerne at franarre betalingskort- og personoplysninger, fx MitID, ved hjælp af e-mail (phishing) eller SMS (smishing). Det sker fx, ved at svindlerne udgiver sig for at være fra en dansk myndighed eller virksomhed og får overbevist modtageren om at åbne et link og efterfølgende foretage en betaling. Digitaliseringsstyrelsen og Center for Cybersikkerhed advarer om, at man ikke skal svare på sådanne henvendelser, da ingen reelle virksomheder eller myndigheder vil anmode om betalingskortoplysninger, MitID eller andre login-informationer via e-mail eller sms.[4]

Netbanksvindel: Svindel med netbanken kan skyldes, at det er lykkedes de kriminelle at bryde ind i borgernes eller virksomhedernes netbank, fx efter at have franarret brugerne deres login-oplysninger. I langt de fleste tilfælde skyldes netbanksvindel dog tilfælde, hvor det lykkes de kriminelle at manipulere borgere eller medarbejdere til selv at overføre penge til svindlerne, såkaldt social engineering.[5]

Investeringssvindel: Ved at tilbyde attraktive afkast i falske investeringsmuligheder, fx aktier, eller kryptoaktiver lykkes det de kriminelle at overtale ofrene til at betale eller overføre penge for en falsk investering.

Svindel mod virksomheder: Når de kriminelle forsøger at franarre virksomhederne penge, sker det bl.a., ved at svindlerne sender fakturaer på varer eller services, som virksomheden ikke har købt. I andre tilfælde udgiver svindlerne sig for at være en allerede anvendt leverandør og informerer virksomheden om, at den fremover ønsker betalinger på en anden bankkonto.[6]

Fem gode råd til at undgå digital svindel
Ifølge Det Kriminalpræventive Råd er it-kriminalitet en af de mest udbredte former for kriminalitet, og det rammer alle aldersgrupper. Det er derfor vigtigt at være påpasselig og kritisk, når man begår sig på internettet, eller hvis man bliver ringet op eller kontaktet på SMS af en afsender, som man ikke forventer at blive kontaktet af. Det Kriminalpræventive Råd angiver fem gode råd til at undgå digital svindel:[7]

1) **Stop op og tag dig god tid**, inden du klikker, betaler eller deler personlige oplysninger. Det er vigtigt at undgå forhastede beslutninger.
2) **Lyt til din mavefornemmelse.** Ofte vil du fornemme, at noget er galt.
3) **Vær opmærksom på faresignalerne**, hvis kommunikationen ændrer sig pludseligt eller virker anderledes end normalt, og hvis du føler dig presset til at handle hurtigt.
4) **Bekræft identiteten på den, du er i kontakt med**. Brug myndighedernes officielle kanaler, fx hovednummeret, og hvis det er en person, du kender, så ring selv op på det nummer, personen normalt bruger.
5) **Del aldrig personlige oplysninger** som fx mit MitID eller personlige koder – heller ikke til familie og venner.

[1] Digitaliseringsstyrelsen og Center for Cybersikkerhed m.fl. har udarbejdet en guide til at afsløre digital svindel (*link*). Ligeledes har en række virksomheder og organisationer lanceret en hjemmeside, hvor borgere og virksomheder kan tjekke, om en hjemmeside er troværdig eller et svindelforsøg *(link)*.
[2] Se Finans Danmark, *Kampen mod digital svindel,* december 2023 *(link)*.
[3] Se Politiet, *Undgå at blive snydt, når du handler med andre på nettet (link)*.
[4] Se Digitaliseringsstyrelsen og Center for Cybersikkerhed mfl, *sikkerdigital.dk (link)*.
[5] Se figur 8 og Finans Danmark, *Netbanksvindel (link)*.
[6] Se Finans Danmark, *Virksomhedssvindel (link)*.
[7] Se Det Kriminalpræventive Råd, *Stop op og undgå digital svindel (link)*.

Geografisk sikkerhed kan begrænse misbrug med betalingskort i udlandet

Nogle betalingskort tillader såkaldt geografisk sikkerhed. Det betyder, at borgerne og virksomhederne kan vælge, at kortet ikke kan anvendes til betalinger i specifikke geografiske områder eller bestemte betalingssituationer som fx internethandel eller kontanthævninger. Dermed hindres muligheden for misbrug med betalingskortet i bestemte geografiske områder eller betalingssituationer, hvor borgerne typisk ikke anvender kortet. Det gælder fx internethandel uden for Europa. Hvis en borger eller virksomhed på et senere tidspunkt alligevel har behov for at kunne betale i et spærret område eller i en spærret betalingssituation, kan spærringen typisk hæves midlertidigt eller permanent via net- eller mobilbank.

Det er imidlertid ikke alle korttyper, som understøtter geografisk sikkerhed. Det skyldes bl.a., at flere kortudstedere ikke tilbyder spærringsmuligheden, og at kendskabet til geografisk sikkerhed blandt befolkningen er begrænset. Øget brug af geografisk sikkerhed vurderes at kunne reducere misbruget med betalingskort, men det kræver en bredere udbredelse af løsningen på tværs af både korttyper og kortudstedere.

Kortmisbruget i Danmark er lavt, både i fysisk handel og på internettet

Omfanget af misbrug med betalingskort i Danmark er relativt lavt. I 2023 var den samlede misbrugsværdi i Danmark 56 mio. kr. Heraf blev ca. 40 pct. foretaget på internettet, mens den resterende del foregik i fysisk handel og i hæveautomater, se figur 3. Dermed adskiller misbruget med betalingskort i Danmark sig særligt fra udlandet, ved at misbrugsværdien i dansk internethandel er på et lige så lavt niveau som fysisk handel. I 2023 var den relative misbrugsandel for både internethandel og fysisk handel ca. 0,1 promille. Den lave andel understreger, at betalinger i Danmark er meget sikre.

Den høje grad af sikkerhed skyldes både, at betalingskort er sikre og svære at forfalske, og at kortselskaberne og pengeinstitutterne løbende har udviklet og implementeret effektive realtidsmekanismer til at identificere mistænkelige transaktioner. Som følge heraf skyldes stort set alle misbrugstransaktioner i fysisk handel i Danmark, at borgerne har tabt eller fået stjålet deres betalingskort.[8]

Kortbetalinger med mobiltelefonen har givet svindlerne nye muligheder

Danmark er et af de mest digitaliserede lande i verden på betalingsområdet, hvor ca. 9 ud af 10 betalinger i fysisk handel sker digitalt.[9] Den høje grad af digitalisering giver dog også svindlere nye betalingsmuligheder, som ikke nødvendigvis er lige så udbredte i andre lande. Det gælder fx kortbetalinger via mobilen, de såkaldte wallet-betalinger som Apple Pay eller Google Pay, der er udbredte i Danmark.

Wallet-betalinger har gjort det muligt, at de kriminelle kan digitalisere stjålne betalingskortoplysninger på deres egne mobiltelefoner. Derudover er en særlig udfordring med wallet-betalingerne, at hvis det lykkes svindlerne at få digitaliseret et stjålet betalingskort, giver det adgang til at trække penge på den tilhørende betalingskonto uden kendskab til pinkoden. Det skyldes, at svindlerne selv kan godkende betalingerne med egen mobilkode eller ansigtsgodkendelse frem for kortets tilhørende pinkode.[10]

[8] I 2023 var den samlede misbrugsværdi med falske betalingskort i Danmark ca. 124.000 kr. ud af et samlet kortmisbrug i fysisk handel i Danmark på ca. 14,3 mio. kr.
[9] Se Danmarks Nationalbank, Danmark er blandt de mest digitaliserede lande på betalingsområdet, *Danmarks Nationalbank Analyse*, nr. 2, februar 2022 (*link*).
[10] Ved brug af wallet-betalinger som fx Apple Pay og Google Pay bruger kortudstederne såkaldt delegeret autentifikation, hvor tofaktor-godkendelse gennemføres i wallet-udbyderens miljø. Det kan fx være en talkode eller biometrisk løsning, som anvendes, se Finanstilsynet, *Temaundersøgelse om brugen af stærk kundeautentifikation i e-handlen,* 2021 *(link).*

Digitalisering af et stjålet betalingskort er dog vanskelig, fordi det også kræver godkendelse fra kortejeren med MitID. Derudover forhindrer både pengeinstitutterne og kortselskaberne en stor del af de forsøg, som svindlerne foretager. Misbrug med wallet-betalinger skyldes derfor typisk, at borgerne har været udsat for identitetstyveri[11], eller at svindleren har manipuleret borgeren til at godkende digitaliseringen af betalingskortet på svindlerens mobiltelefon.

Siden 2021 er værdien af kortmisbruget i dansk fysisk handel fordoblet til godt 14 mio. kr. Det skyldes i høj grad, at den gennemsnitlige transaktionsværdi er steget, og at svindlerne i stigende grad lykkes med at betale uden brug af pinkode, fx ved brug af wallet-betalinger, se figur 5 og figur 6.

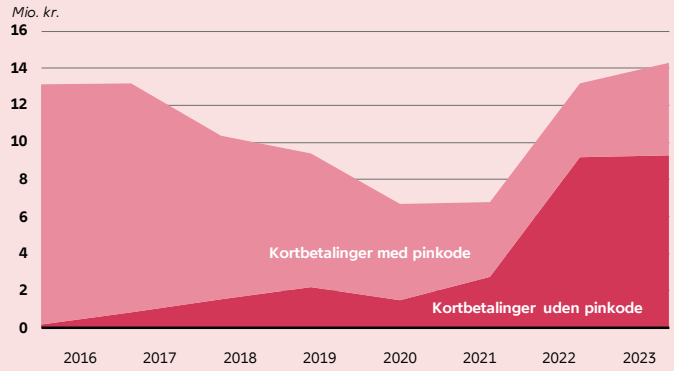
Stigningen i misbrugsværdien uden brug af pinkode skal særligt ses i lyset af, at det før introduktionen af mobile wallet-betalinger ikke var muligt at foretage kortbetalinger i fysisk handel over 350 kr. uden brug af pinkode, se boks 1. Wallet-betalingerne har dermed isoleret set muliggjort, at svindlerne kan misbruge stjålne betalingskortoplysninger til større transaktionsværdier uden kendskab til pinkoden, hvis de får digitaliseret betalingskortet.

Misbrug med wallet-betalinger kan desuden være vanskelig at opdage for både borgerne og pengeinstitutterne, da betalingerne typisk ligner almindelige hverdagstransaktioner, når de fremgår i netbanken. Derudover mister borgerne ikke et fysisk betalingskort, hvilket betyder, at der i nogle tilfælde kan gå lang tid, før misbruget bliver opdaget.

FIGUR 5

Misbrugsværdi af kortbetalinger i Danmark i fysisk handel

Fordeling af misbrugsværdi med betalingskort i dansk fysisk handel opdelt efter, om pinkoden har været anvendt ved betalingen

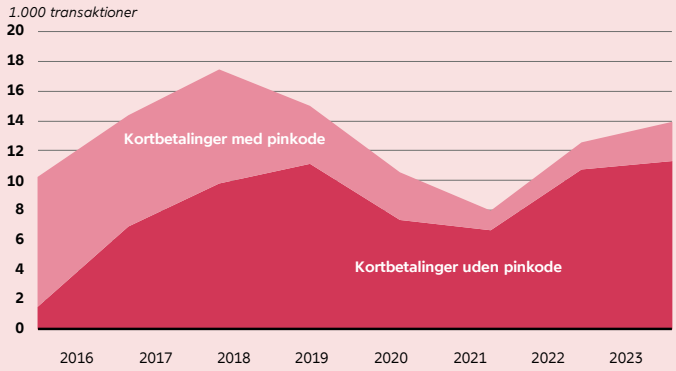


Anm.: Kortbetalinger uden pinkode er typisk kontaktløse betalinger eller mobile wallet-betalinger. Opgørelsen dækker dansk udstedte betalingskort.
Kilde: Danmarks Nationalbank.

FIGUR 6

Antallet af misbrugstransaktioner i Danmark i fysisk handel

Fordeling af misbrugstransaktioner med betalingskort i dansk fysisk handel opdelt efter, om pinkoden har været anvendt ved betalingen



Anm.: Kortbetalinger uden pinkode er typisk kontaktløse betalinger eller mobile wallet-betalinger. Opgørelsen dækker dansk udstedte betalingskort.
Kilde: Danmarks Nationalbank.

[11] Identitetstyveri dækker bl.a., når nogen ulovligt tilegner sig en andens oplysninger og misbruger disse oplysninger til fx at optage lån eller købe ting. De personlige oplysninger kan fx være CPR-nummer, adgangskoder eller MitID. Det er ikke identitetstyveri, hvis en svindler får adgang til kreditkortoplysninger og misbruger dem, se Borger.dk (*link*).

03
Svindel med kredit-overførsler er stigende

Svindlernes muligheder for svindel og misbrug med overførsler fra bankkonti har ændret sig de senere år. Det skyldes dels, at borgere og virksomheder i større grad selv foretager overførsler uden direkte involvering af banken, fx ved hjælp af mobil- eller netbank, dels at befolkningen i større grad benytter digitale betalingsløsninger, som anvender kreditoverførsler til at gennemføre betalingerne, fx MobilePay.

Til forskel fra misbrug med kortbetalinger er økonomisk kriminalitet forbundet med kreditoverførsler typisk relateret til økonomisk svindel, hvor borgere eller medarbejdere manipuleres til at gennemføre overførslen. Det betyder også, at svindel med kreditoverførsler ikke nødvendigvis er forbundet med en betalingssituation.

Derudover adskiller svindel med kreditoverførsler via mobil- eller netbank sig også fra betalingskort, ved at betalingskort kun er knyttet til én specifik konto, samtidig med at både kontanthævninger og løbende forbrug med betalingskort typisk er beløbsbegrænset. Lykkes det derimod svindleren at få adgang til netbanken, evt. med manipuleret godkendelse fra den svindelramte, er det muligt at gennemføre kreditoverførsler fra flere konti og samtidig tømme dem eller foretage overtræk, hvis kontoen tillader det.

Bankerne lykkes i de fleste tilfælde med at forhindre svindlen. Alligevel har den samlede værdi af svindel gennemført med kreditoverførsler været stigende og var i 2023 ca. 333 mio. kr., se figur 7. Det er stort set på niveau med værdien for kortmisbrug, som i samme periode var ca. 294 mio. kr. Til forskel fra kortmisbrug blev der dog registeret markant færre, men gennemsnitligt større svindeltransaktioner. I 2023 blev der registreret ca. 9.400 svindelrelaterede kreditoverførsler med en gennemsnitlig værdi på ca. 35.300 kr. Til sammenligning var den gennemsnitlige misbrugsværdi med kortbetalinger knap 1.300 kr. i 2023, se kapitel 2.

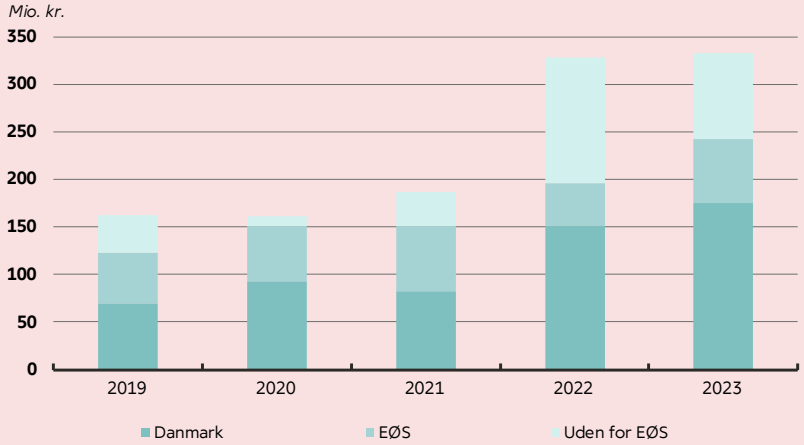
Ifølge tal fra bankernes interesseorganisation, Finans Danmark, er det særligt borgerne, som bliver ofre for svindel med kreditoverførsler: I første halvår 2023 udgjorde svindel relateret til borgerne ca. 80 pct af den samlede svindelværdi, mens virksomhedssvindel udgjorde knap 20 pct.[12] Det har bl.a. givet anledning til, at flere myndigheder og organisationer har haft en kommunikationsindsats over for borgerne ift. at undgå digital svindel, se boks 2.

[12] Se Finans Danmark, *Virksomhedssvindel* (*link*).

FIGUR 7

Svindel med kreditoverførsler er stigende

Samlet svindel og misbrug med kreditoverførsler opdelt efter modtagerkontoens oprindelse



Anm.: Omfanget dækker den fulde svindelværdi, som er gennemført med kreditoverførsler. I flere tilfælde lykkes det bankerne at få tilbageført hele eller en del af den svindelrealterede overførsel, hvorfor det samlede tab er mindre, se figur 10. Bankerne forhindrer desuden størstedelen af de svindelrelaterede overførsler inden de gennemføres. Databrud mellem 1. og 2. halvår 2020.
Kilde: Pengeinstitutternes indberetninger til Finanstilsynet i medfør af Den Europæiske Banktilsynsmyndighed, *EBA guidelines on fraud reporting under PSD2*, og Danmarks Nationalbank.

Svindel og misbrug med kreditoverførsler skyldes særligt tilfælde, hvor borgerne eller medarbejderne gennemfører betalingen til svindleren

Reglerne for tofaktor-godkendelse bevirker, at adgang til netbanken og gennemførsel af betalinger kræver godkendelse med fx MitID. Det har i stigende grad gjort det nødvendigt for svindlerne at involvere borgere og medarbejdere i virksomhederne til at gennemføre og godkende de svindelrelaterede betalinger.

Svindel og misbrug med kreditoverførsler er derfor i stigende grad kendetegnet ved, at borgere og medarbejdere manipuleres til at overføre penge til svindlerne, fx under dække af en påstand om, at borgernes netbank er blevet hacket, og derfor bør overføre deres opsparing til en "sikret konto".

I 2023 var ca. 81 pct. af den samlede svindel- og misbrugsværdi med kreditoverførsler tilfælde, hvor de svindelramte borgere eller virksomheder selv overførte penge, se figur 8. Det sker fx, når de kriminelle kontakter borgere eller medarbejdere telefonisk og udgiver sig for at være fra banken eller danske myndigheder eller når en borger ser en falsk annonce på sociale medier eller handelsplatforme og foretager en betaling, fx med mobilen.[13]

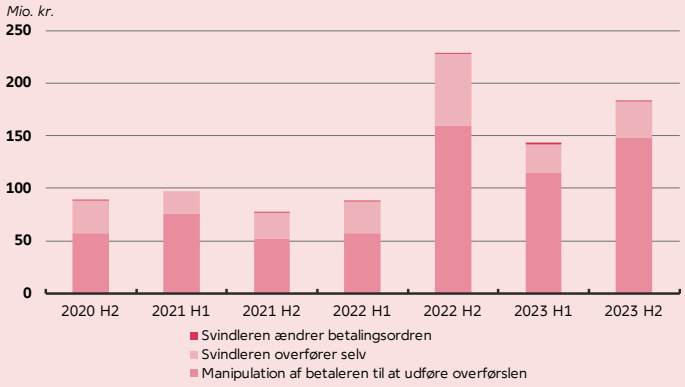
Siden indførslen af tofaktor-godkendelse har langt størstedelen af svindelrelaterede kreditoverførsler været godkendt med tofaktor-godkendelse, se figur 9. Det understreger, at svindlerne løbende ændrer og tilpasser deres svindelmetoder, når der indføres nye sikkerhedsforanstaltninger.

[13] Se Finans Danmark, *Netbanksvindel* (*link*), og *Kampen mod digital svindel* (*link*).

FIGUR 8

Svindel med kreditoverførsler skyldes særligt tilfælde, hvor borgere eller medarbejdere overfører penge til svindleren

Samlet svindel og misbrug med kreditoverførsler opdelt efter, hvem der har overført pengene til svindleren

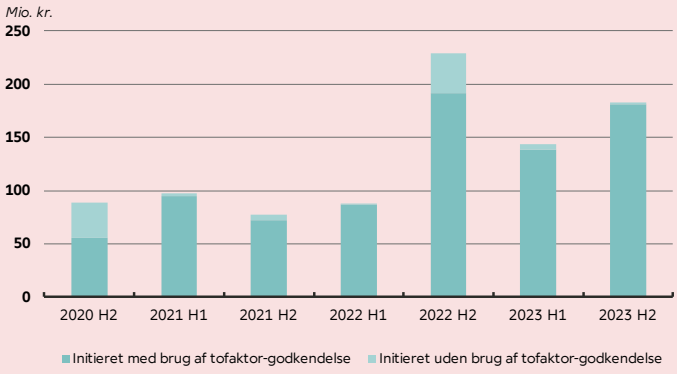


Anm.: Omfanget af svindel, hvor svindlerne ændrer en betalingsordre, er begrænset, og kan derfor være vanskeligt at aflæse i figuren.
Kilde: Pengeinstitutternes indberetninger til Finanstilsynet i medfør af Den Europæiske Banktilsynsmyndighed, *EBA guidelines on fraud reporting under PSD2,* og Danmarks Nationalbank.

FIGUR 9

Størstedelen af svindel og misbrug med kreditoverførsler godkendes med tofaktor-godkendelse

Samlet svindel og misbrug med kreditoverførsler opdelt efter, om der ved overførslen har været anvendt tofaktor-godkendelse



Anm.: Reglerne for tofaktor-godkendelse ved kreditoverførsler trådte i kraft 1. januar 2018. Den høje værdi af svindel med kreditoverførsler initieret uden tofaktor-godkendelse i 2. halvår 2022 skyldes nogle få virksomhedstransaktioner med høje værdier, som blev undtaget kravet om tofaktor-godkendelse i medfør af artikel 17 i KOM/2018/389.
Kilde: Pengeinstitutternes indberetninger til Finanstilsynet i medfør af Den Europæiske Banktilsynsmyndighed, *EBA guidelines on fraud reporting under PSD2,* og Danmarks Nationalbank.

De resterende svindeltilfælde, som ikke direkte involverer borgere eller medarbejdere, skyldes primært, at svindleren har fået adgang til en borgers eller virksomheds netbank og derigennem selv foretager overførslen. Det kan skyldes såkaldt phishing, hvor det lykkes svindlerne at få oplyst loginoplysningerne, eller at svindleren på anden vis lykkes med at stjæle oplysningerne, fx ved at installere skadelig software, også kaldet *malware*. For at svindlerne selv kan gennemføre overførslen, kræver det desuden, at de har mulighed for at få godkendt overførslen med MitID.

Kun i få tilfælde lykkes det svindlerne at ændre på en eksisterende betalingsordre, hvilket understreger, at betalingsinfrastrukturen i sig selv er meget sikker.

Hovedparten af svindelforsøg med kreditoverførsler bliver stoppet af bankerne

I de fleste tilfælde lykkes det bankerne at stoppe svindlen med kreditoverførsler, inden den finder sted. Ifølge tal fra Finans Danmark forhindrede bankerne i 2022 ca. 60 pct. af den samlede svindelværdi, som blev forsøgt gennemført.[14]

Derudover lykkes det også bankerne at få tilbageført en del af den svindelværdi, som i første omgang løber igennem betalingssystemerne. Ud af den samlede misbrugsværdi med kreditoverførsler i 2023, på ca. 333 mio. kr., lykkedes det bankerne at få tilbageført ca. 67 mio. kr. Det samlede tab i perioden var dermed ca. 266 mio. kr.

Svindel med kreditoverførsler, hvor borgere eller medarbejdere manipuleres til at overføre penge, kan være vanskelig for bankerne at forhindre, da transaktionerne kan ligne almindelige kreditoverførsler foretaget af borgerne

[14] Se Finans Danmark, *Kampen mod digital svindel,* december 2023 (*link*).

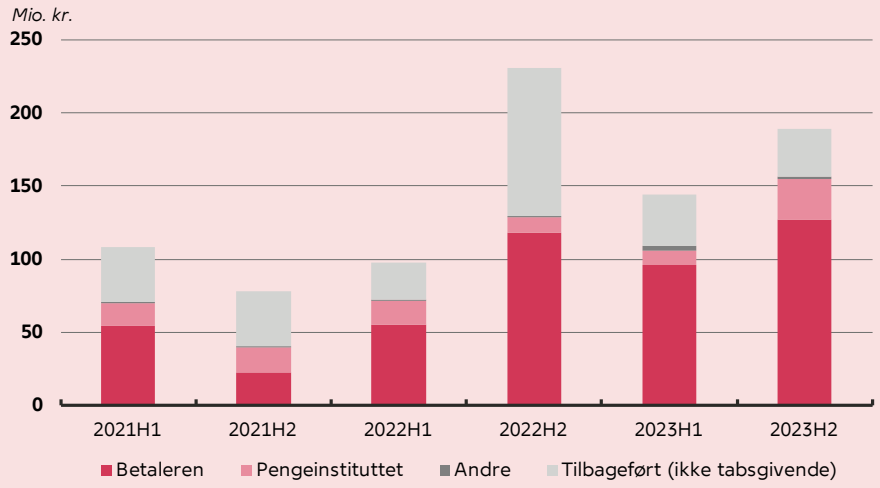
eller virksomhederne. Desuden forhindrer tofaktor-godkendelsen ikke betalingen, da betaleren selv godkender transaktionen.

Når borgere eller medarbejdere har været udsat for svindel med kreditoverførsler, og selv har gennemført og godkendt betalingerne, hæfter de i de fleste tilfælde for det økonomiske tab, se boks 3. Ud af det samlede tab i 2023 hæftede de svindelramte betalere for ca. 223 mio. kr., svarende til ca. 84 pct. af det samlede tab, se figur 10.

FIGUR 10

Betaleren hæfter i høj grad for tabet ved svindel med kreditoverførsler

Samlet svindel og misbrug med kreditoverførsler opdelt efter, hvilken part der hæfter for tabet



Anm.: Betaleren er den borger eller virksomhed, som har foretaget betalingen.
Kilde: Pengeinstitutternes indberetninger til Finanstilsynet i medfør af Den Europæiske Banktilsynsmyndighed, *EBA guidelines on fraud reporting under PSD2*, og Danmarks Nationalbank.

For at dæmme op for digital svindel har Erhvervsministeriet i samarbejde med Finans Danmark, Forbrugerrådet Tænk, Teleindustrien og Ældresagen i efteråret 2023 lanceret fire initiativer. De omfatter bl.a. en reduceret daglig beløbsgrænse for straksbetalinger på 50.000 kr. uden først at have kontaktet banken og informationskampagner mod digital svindel. Derudover etableres en løsning, som muliggør, at afsendere af SMS'er kan få beskyttet deres afsendernavn, så svindlerne ikke kan udgive sig for at være fra en bank eller en myndighed.[15] Senest har Finans Danmark lanceret kampagnen *Sikker bank – sammen* og i december 2023 nedsat en svindeltaskforce til at identificere nye tiltag og anbefalinger, som kan mindske digital svindel.[16]

[15] Se Erhvervsministeriet, *Kampen mod digital svindel styrkes*, november 2023 (*link*).
[16] Se Finans Danmark, *Sikker bank – sammen* (*link*), og *Ny Svindel Task Force tager kampen op mod de kriminelle*, december 2023 (*link*).

BOKS 3

Lovgivning vedrørende misbrug og svindel med betalinger og kreditoverførsler

Det er i udgangspunktet udbyderen af betalingstjenester, dvs. typisk betalerens bank, som hæfter for misbrug med betalingskort eller kreditoverførsler via netbanken, men typen af misbrug og mangel på forsigtighed kan øge betalerens grad af hæftelse.

Betalingstjenesteudbyderen hæfter for betalerens tab, hvis udbyderen af betalingstjenesten har valgt at undtage den konkrete betaling fra kravet om tofaktor-godkendelse, se boks 1. Det gælder fx ved kontaktløse kortbetalinger, hvor betaleren ikke anvender pinkode. Modsat skal betaleren dække 375 kr. af det samlede misbrug, hvis udbyderen af betalingstjenesten kan godtgøre, at den personlige sikkerhedsforanstaltning som fx pinkode eller MitID-appen har været anvendt til godkendelse af betalingen. Det gælder også, selvom betaleren ikke har oplyst sin pinkode eller MitID-oplysninger til nogen.

Betaleren hæfter med op til 8.000 kr. i tilfælde, hvor udbyderen af betalingstjenesten kan godtgøre, at den personlige sikkerhedsforanstaltning har været anvendt, og betaleren på anden vis har opført sig uansvarligt, fx ved at oplyse sin pinkode eller give adgang til MitID. De samme regler gælder, hvis betaleren ikke har givet besked til banken, snarest muligt efter at betaleren har opdaget at have mistet sit betalingskort eller sin mobiltelefon, hvis den kan foretage mobilbetalinger.

Betaleren hæfter ubegrænset, hvis udstederen af betalingstjenesten godtgør, at betaleren har givet den personlige sikkerhedsforanstaltning til svindleren, og at betaleren var eller burde være klar over, at det ville indebære en risiko for svindel.

Betaleren hæfter i udgangspunktet også ubegrænset, hvis betaleren selv gennemfører betalingen med tofaktor-godkendelse. Det gælder fx, når der betales på falske netbutikker, eller når det lykkes svindlerne at overtale betaleren til at overføre penge. I nogle tilfælde har banken dog mulighed for at stoppe betalingen og evt. tilbageføre hele eller dele af betalingen.

Svindel og misbrug med betalingskort eller kreditoverførsler straffes i flere tilfælde efter straffelovens bedrageribestemmelse.[1] Overtrædelse af bedrageribestemmelsen straffes i udgangspunktet med fængsel indtil 1 år og 6 måneder, men straffen kan i særligt grove tilfælde stige til fængsel indtil 8 år.

Kilde: *Bekendtgørelse af lov om betalinger* (*link*) og *bekendtgørelse af straffeloven*, 28. kapitel (*link*).

[1] Se fx Syd- og Sønderjyllands Politi, juni 2020 (*link*).

En stor del af svindel med kreditoverførsler sker til danske konti

I modsætning til svindel og misbrug med betalingskort sker en stor del af den samlede svindel med kreditoverførsler til danske konti, se figur 7.

Som en del af afdækningen af svindel og misbrug med digitale betalinger i Danmark har Nationalbanken været i dialog med nogle af de største betalings- og pengeinstitutter i Danmark for bl.a. at få indblik i de svindelmønstre, som typisk rammer deres kunder, og hvorfor svindelrelaterede kreditoverførsler særligt overføres til danske konti.

Institutterne anfører flere mulige forklaringer. En årsag er, at betalingsinfrastrukturen til indenlandske kreditoverførsler er bedre forbundet end til udenlandske konti. Det skyldes bl.a., at de fleste kreditoverførsler til udlandet kræver flere oplysninger, for at overførslen kan gennemføres. Derudover tager kreditoverførsler til udlandet typisk længere tid, hvilket giver

både institutterne, borgerne og virksomhederne mere tid til at forhindre de svindelrelaterede overførsler.

En anden årsag til er ifølge institutterne, at svindel med kreditoverførsler ofte sker, ved at svindlerne manipulerer borgere eller medarbejdere til at overføre penge til svindlerne: Her vil betalerne formentligt opfatte en overførsel til en udenlandsk konto mere mistænkelig end til en dansk bankkonto.

Endelig bør svindelmønsteret, ifølge pengeinstitutterne, ses i sammenhæng med, at svindlerne ofte anvender en kombination af svindel med betalingskort og kreditoverførsler. Det indebærer, at svindlerne bl.a. anvender en stjålet modtagerkonto, hvortil de også har kendskab til betalingskortoplysninger. Det muliggør kreditoverførsler fra andre borgere eller virksomheder, hvorefter svindlerne kan betale, hæve, sløre eller overføre pengene til udlandet.

04

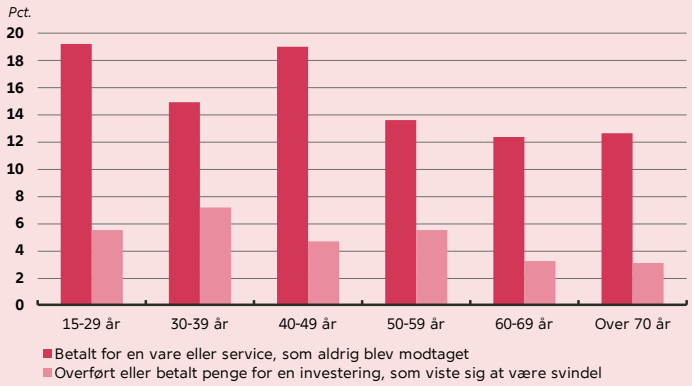
Digital svindel rammer alle dele af befolkningen

Nationalbanken undersøgte i foråret 2023 borgernes betalingsvaner med en spørgeskemaundersøgelse. Undersøgelsen gav bl.a. indblik i, hvilke typer af svindel som borgerne udsættes for, og hvorvidt digital svindel i større omfang rammer bestemte dele af befolkningen. Respondenterne blev bl.a. spurgt, om de inden for det seneste år havde foretaget en betaling i forbindelse med et køb eller en investeringsmulighed, som viste sig at være svindel.[17]

Ifølge undersøgelsen havde 16 pct. af befolkningen betalt for en vare eller tjeneste, som de aldrig modtog. Ligeledes tilkendegav knap 5 pct. af de adspurgte borgere i undersøgelsen, at de havde betalt penge for en investering, som viste sig at være svindel.[18] Resultaterne indikerer dermed, at en større del af befolkningen har oplevet betalingssituationer, som potentielt havde svindel til formål, men det betyder ikke nødvendigvis, at borgerne har oplevet et økonomisk tab.[19]

FIGUR 11

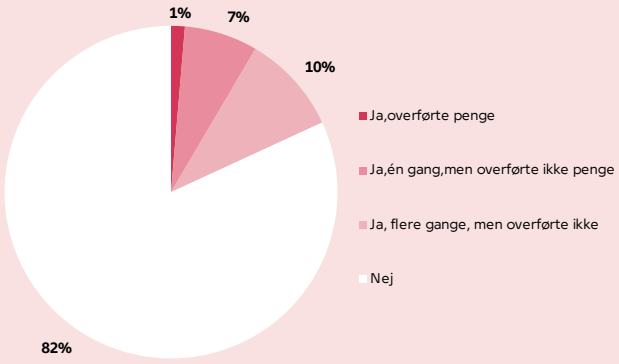
Digital svindel rammer alle dele af befolkningen



Anm.: Baseret på 2.737 besvarelser. Respondenterne blev spurgt, om de inden for det seneste år havde betalt for en vare eller service, som de aldrig modtog, eller om de havde været udsat for investeringssvindel.
Kilde: Danmarks Nationalbank, *Husholdningsundersøgelse 2023*.

FIGUR 12

Ca. 1 pct. af befolkningen har overført penge til en svindler, som kontaktede dem telefonisk



Anm.: Baseret på 2.737 besvarelser. Respondenterne blev spurgt, om de inden for det seneste år var blevet kontaktet telefonisk af en svindler og efterfølgende havde overført penge.
Kilde: Danmarks Nationalbank, *Husholdningsundersøgelse 2023*.

[17] Dataindsamlingen blev foretaget af analyseinstituttet Epinion og er baseret på besvarelser fra 2.737 repræsentativt udvalgte borgere over 15 år.
[18] Undersøgelsens usikkerhed er +/- 1,3 procentpoint ved spørgsmålet om køb af vare eller tjenester som borgeren ikke modtog og +/- 0,8 procentpoint ved spørgsmålet om investeringer. Omfanget i Nationalbankens undersøgelse indikerer, at de *registrerede* sager med misbrug af betalingskort og svindel med kreditoverførsler formentlig er behæftet med mørketal. Det skal bl.a. ses i lyset af, at betaleren i visse tilfælde hæfter helt eller delvist for det samlede svindelbeløb, se boks 3. I de tilfælde har borgerne ikke et økonomisk incitament til at anmelde tabet.
[19] Ved internethandel gælder fx særlige "charge back regler", som sikrer tilbagebetaling i situationer, hvor betaleren ikke modtager den bestilte vare eller tjeneste, se *Betalingsloven* §112 (link).

På tværs af befolkningen var det særligt dem under 50 år, der oplevede at betale for en vare eller service, som de aldrig modtog. Resultaterne skal dog ses i lyset af, at de samme befolkningsgrupper ofte handler mere på internettet. Ligeledes viste undersøgelsen, at det typisk var borgerne under 60 år, som overførte eller betalte penge for en investering, som viste sig at være svindel. Resultaterne indikerer dermed, at digital svindel rammer alle dele af befolkningen, se figur 11.[20]

I Nationalbankens undersøgelse blev borgerne også spurgt om, hvorvidt de inden for det seneste år var blevet kontaktet telefonisk af en person, som fx udgav sig for at være fra en bank eller myndighed, men viste sig at være en svindler. Ifølge undersøgelsen havde ca. 18 pct. af befolkningen mindst én gang i løbet af det seneste år oplevet at blive ringet op eller modtage en SMS fra en svindler. Langt de fleste borgere, som blev kontaktet, gennemskuede dog svindlen og overførte derfor ingen penge. Det lykkedes dog alligevel svindlerne at manipulere ca. 1 pct. af befolkningen til at overføre penge, se figur 12.[21]

[20] Lignende resultater findes i den seneste opgørelse vedrørende it-anvendelsen i befolkningen, som konkluderer, at særligt den yngre del af befolkningen har haft økonomiske tab som følge af svindel på internettet. Se Danmarks Statistik, *IT-anvendelse i befolkningen 2023 (link)*.
[21] Undersøgelsens usikkerhed er +/- 0,4 procentpoint ved spørgsmålet om telefonisk kontaktsvindel. Digitaliseringsstyrelsen finder ligeledes, at ca. 1 pct. af borgerne udleverer de oplysninger, som svindlerne efterspørger, se Digitaliseringsstyrelsen, *Danskernes informationssikkerhed 2022 (link)*.

05
Tabelbilag

Svindel og misbrug med kreditoverførsler opdelt efter modtagerkontoens oprindelse Tabel A1

Mio. kr.	2019	2020	2021	2022	2023*
Samlet værdi af svindel og misbrug med kreditoverførsler	162,3	161,2	186,2	328,6	333,2
Danmark	69,1	92,8	82,9	150,7	175,5
EØS	53,8	58,0	68,1	45,8	67,3
Uden for EØS	39,3	10,3	35,2	132,1	90,4

Anm.: Databrud mellem 1. og 2. halvår 2020. *Data for 2023 er foreløbige værdier.
Kilde: Pengeinstitutternes indberetninger til Finanstilsynet i medfør af Den Europæiske Banktilsynsmyndighed, *EBA guidelines on fraud reporting under PSD2,* og Danmarks Nationalbank.

Svindel og misbrug med kreditoverførsler opdelt efter type Tabel A2

Mio. kr.	2020H2	2021H1	2021H2	2022H1	2022H2	2023H1	2023H2*
Svindleren overfører selv	30,6	21,4	24,8	30,9	68,2	26,5	34,7
Manipulation af betaleren	57,6	76,0	51,9	56,9	159,6	115,4	149,5
Svindleren ændrer betalingsordren	0,2	0,0	0,4	0,0	1,5	1,7	0,3
Initieret med tofaktor-godkendelse	55,7	95,1	72,2	87,3	191,9	138,4	182,9
Initieret uden tofaktor-godkendelse	32,7	2,3	4,8	0,6	37,4	5,2	1,7

Anm.: *Data for 2. halvår 2023 er foreløbige værdier.
Kilde: Pengeinstitutternes indberetninger til Finanstilsynet i medfør af Den Europæiske Banktilsynsmyndighed, *EBA guidelines on fraud reporting under PSD2,* og Danmarks Nationalbank.

Svindel og misbrug med kreditoverførsler opdelt efter hæftelse

Tabel A3

Mio. kr.	2021H1	2021H2	2022H1	2022H2	2023H1	2023H2*
Betaleren	54,1	22,4	54,7	118,0	96,1	127,2
Pengeinstituttet	15,8	17,5	26,5	10,4	9,8	27,8
Andre	0,6	0,4	0,6	0,8	3,3	1,8
Tilbageført (ikke tabsgivende)	37,6	37,7	25,6	101,9	34,8	32,4
Total	108,2	78,0	97,4	231.1	144,0	189,2

Anm.: Betaleren er den borger eller virksomhed, som har foretaget betalingen. *Data for 2. halvår 2023 er foreløbige værdier.
Kilde: Pengeinstitutternes indberetninger til Finanstilsynet i medfør af Den Europæiske Banktilsynsmyndighed, *EBA guidelines on fraud reporting under PSD2,* og Danmarks Nationalbank.

Må vi sende dig *nyheder* fra Nationalbanken?

Få besked om vores nyeste udgivelser direkte i din indbakke.

Læs mere om vores nyhedsservice
og tilmeld dig på *nationalbanken.dk/da/nyhedsservice,*
eller *scan QR-koden.*

Du kan også få vores nyheder som RSS-feeds.
Læs mere på nationalbanken.dk/da/rss-feeds.

Publikationer

NYT

Nyt er en appetitvækker, der giver et hurtigt indblik i en af Nationalbankens længere publikationer. Nyt er for dig, der har brug for et let overblik og godt kan lide en tydelig vinkling.

STATISTIKNYHED

Statistiknyheder sætter fokus på de nyeste tal og tendenser i Nationalbankens statistikker. Statistiknyheder henvender sig til dig, der vil have hurtig indsigt i aktuelle finansielle data.

RAPPORT

Rapporter er en tilbagevendende beretning om Nationalbankens arbejdsområder og virksomhed. Her finder du bl.a. Nationalbankens årsrapport. Rapporter er for dig, der har brug for en status og opdatering på den forgangne periode.

ANALYSE

Analyser fokuserer på aktuelle emner, som er særligt relevante for Nationalbankens formål. Analyser kan også indeholde Nationalbankens anbefalinger. Her finder du bl.a. vores prognose for dansk økonomi og vores vurdering af den finansielle stabilitet. Analyser henvender sig til dig, der har en bred interesse for økonomiske og finansielle forhold.

ECONOMIC MEMO

Economic Memo giver indblik i det analysearbejde, som Nationalbankens ansatte er i gang med. Economic Memo indeholder fx baggrundsanalyser og metodebeskrivelser. Economic Memo henvender sig primært til dig, der i forvejen har kendskab til økonomiske og finansielle analyser.

WORKING PAPER

Working Paper præsenterer forskningsarbejde fra både ansatte i Nationalbanken og vores samarbejdspartnere. Working Paper henvender sig primært til dig, som er fagperson, og til dig med interesse for forskning inden for centralbankvirksomhed samt økonomi og finans i bredere forstand.

Analysen består af en dansk og engelsk version. I tilfælde af tvivl om oversættelsens korrekthed gælder den danske version.

Danmarks Nationalbank
Langelinie Allé 47
2100 København Ø
+45 3363 6363

Redaktionen er afsluttet 22. april 2024

DANMARKS NATIONALBANK