

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over SMS-phishing / smishing-bedrageri

Strafudmåling, sondringen mellem § 279 og § 279 a samt civilretlig hæftelse efter betalingsloven

Version 2 · Opdateret 24. jun. 2026 · 22 afgørelser · 2015-2026

[Læs online](#)

INTRODUKTION

SMS-phishing (smishing) er en af de mest udbredte former for IT-relateret økonomisk kriminalitet i Danmark. Gerningsmanden udsender SMS-beskeder, der efterligner afsendere som PostNord, MobilePay, Skat eller offerets egen bank, med et link til en falsk hjemmeside, hvor offeret narres til at indtaste kortoplysninger og MitID-legitimation. Retligt rejser smishing-bedrageri to hovedspørgsmål: (1) den strafferetlige kvalificering efter straffelovens § 279 (bedrageri) eller § 279 a (databedrageri), herunder strafudmåling og udvisning, og (2) den civilretlige fordeling af tab mellem kunde og bank efter betalingslovens § 100. Praksis viser, at organiserede smishing-operationer med mange ofre og store beløb medfører straffe i intervallet 1½–6 års fængsel, mens Finansielle Ankenævn systematisk anvender en selvrisiko på 8.000 kr. for ofre, der har godkendt transaktioner via MitID efter phishing-SMS.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** SMS-phishing kvalificeres som databedrageri efter straffelovens § 279 a, når offeret narres til at godkende en elektronisk transaktion via MitID, idet den tabsforvoldende disposition sker via elektronisk databehandling.
- 02** Klassisk bedrageri efter § 279 kan dog anvendes, hvor gerningsmanden telefonisk manipulerer offeret til at udlevere betalingskort, kontanter eller smykker – typisk ved vishing-opkald der følger efter SMS-kontakt.
- 03** Ved organiseret smishing med mere end 600 ofre og beløb over 27 mio. kr. udmåles straffen op til 5–6 års fængsel efter § 286, stk. 2 (særlig grov beskaffenhed).
- 04** En chauffør eller medhjælper i en organiseret bedragerigruppe straffes typisk med 1½–2 års fængsel, selv ved begrænset egen andel i bedrageriet.
- 05** Pengemuldyr (money mules), der stiller konti til rådighed for at modtage og videresende udbyttet, straffes selvstændigt for hvidvask efter § 290 a.
- 06** Sager om IT-relateret økonomisk kriminalitet, herunder smishing, behandles af NCIK (Nationalt Center for It-relateret økonomisk Kriminalitet) under NSK.

- 07 Manipulation af SMS-afsendernavne (A-nummer-spoofing) kan afdækkes via teledata, jf. Rigsadvokatmeddelelsen om teledata, afsnit 2.5.5.
- 08 Efter betalingslovens § 100, stk. 4, hæfter kunden med op til 8.000 kr. ved groft uforsvarlig adfærd – typisk godkendelse af MitID-transaktion efter phishing-SMS.
- 09 Kunden hæfter kun med 375 kr. efter § 100, stk. 3, hvis den uautoriserede transaktion skyldes andres uberettigede anvendelse af betalingsinstrumentet, og kunden ikke har handlet groft uforsvarligt.
- 10 Finansielle Ankenævn afviser hyppigt smishing-sager til domstolene, når bevisførelsen om kundens adfærd kræver mundtlige parts- og vidneforklaringer.
- 11 Udvisning af udenlandske gerningsmænd er hovedreglen ved organiseret smishing-bedrageri, medmindre EMRK art. 8 (privat- og familieliv) fører til et andet resultat.
- 12 Identitetsmisbrug i forbindelse med smishing kan tillige straffes efter straffelovens § 264 e, typisk i sammenstød med § 279 a.

Lovgrundlag: Bedrageri, databedrageri og betalingslovens hæftelsesregler

§ 1

SMS-phishing (smishing) rammes strafferetligt af to centrale bestemmelser i straffeloven:

[Straffelovens § 279](#) (bedrageri) kræver, at gerningsmanden ved retsstridigt at fremkalde, bestyrke eller udnytte en *vildfarelse* bestemmer en anden til en handling eller undladelse, hvorved der påføres et formuetab. Bestemmelsen finder typisk anvendelse, når offeret telefonisk manipuleres ("vishing") til fysisk at udlevere betalingskort, kontanter eller smykker, eller til manuelt at foretage en bankoverførsel.

[Straffelovens § 279 a](#) (databedrageri) rammer den, der retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer til elektronisk databehandling, eller i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling. Bestemmelsen er central ved smishing, fordi den tabsforvoldende disposition – selve betalingstransaktionen – sker automatiseret via betalingssystemet, efter at gerningsmanden har fået adgang til offerets kortoplysninger og MitID-legitimation.

Sondringen i praksis afhænger af, hvem eller hvad der foretager den tabsforvoldende disposition. Når offeret narres til at godkende en betaling i MitID-appen uden at forstå, hvad der godkendes, er det betalingssystemet, der disponerer – og forholdet henføres under § 279 a. Når offeret derimod selv overfører penge eller udleverer fysiske genstande, er det offeret, der *bestemmes* til en handling – og forholdet er klassisk bedrageri efter § 279.

Ved grovere forhold anvendes [straffelovens § 286, stk. 2](#), der hæver strafmaksimum til 8 års fængsel for bedrageri og databedrageri af *særlig grov beskaffenhed*. Ifølge [Rigsadvokatmeddelelsen om formueforbrydelser](#) vil forbrydelsen navnlig være af særlig grov beskaffenhed på grund af udførelsesmåden, fordi forbrydelsen er udført af flere i forening, som følge af omfanget af den opnåede eller tilsigtede vinding, eller når et større antal forbrydelser er begået.

På den civilretlige side regulerer [betalingslovens § 100](#) fordelingen af tab ved uautoriserede betalingstransaktioner mellem kunde og betalingstjenesteudbyder (bank). Bestemmelsen opererer med en trinmodel:

- **Stk. 3** (375 kr.): Kunden hæfter med op til 375 kr. for tab som følge af andres uberettigede anvendelse af betalingsinstrumentet, medmindre kunden har handlet groft uforsvarligt.
- **Stk. 4** (8.000 kr.): Kunden hæfter med op til 8.000 kr., hvis den uautoriserede transaktion skyldes, at kunden ved groft uforsvarlig adfærd har muliggjort misbruget.
- **Stk. 5** (ubegrænset): Kunden hæfter uden beløbsbegrænsning, hvis kunden har handlet svigagtigt eller forsætligt undladt at opfylde sine forpligtelser.

LOV

[Betalingsloven § 100, stk. 3-5](#)[Straffeloven § 279](#)[Straffeloven § 279a](#)[Straffeloven § 286, stk. 2](#)

§ 2 NCIK og efterforskning af smishing-sager

Siden 1. januar 2022 er sager om IT-relateret økonomisk kriminalitet, herunder smishing, centraliseret hos **Nationalt Center for It-relateret økonomisk Kriminalitet (NCIK)**, der er forankret i National enhed for Særlig Kriminalitet (NSK). [Rigsadvokatmeddelelsen om formueforbrydelser](#) oplyser, at NCIK's sagsområde dækker syv kategorier, herunder:

- Kontaktbedrageri mod borgere (kategori 3)
- Misbrug af betalingskort (kategori 5)
- Misbrug af adgang til netbank/betalingstjenester (kategori 6)

Smishing falder typisk under kategori 3 (kontaktbedrageri mod borgere) i kombinationen med kategori 5 og 6. Statsadvokaten for Særlig Kriminalitet (SSK) varetager tilsynsopgaver, og klager over centerets afgørelser kan indgives til SSK.

Et centralt teknisk element i smishing-sager er **A-nummer-spoofing** – manipulation af afsendernavnet i SMS-beskeder, så de fremstår som sendt fra fx "PostNord", "MobilePay" eller offerets bank.

[Rigsadvokatmeddelelsen om teledata](#) beskriver, at denne type manipulation kan afdækkes ved at indhente teledata vedrørende A-nummeret, idet det heraf vil fremgå, at nummeret ikke har været anvendt til den pågældende aktivitet.

§ 3 Strafadmåling ved organiseret smishing-bedrageri

Retspraksis viser, at strafudmålingen ved smishing-bedrageri afhænger af tre hovedfaktorer: (1) det samlede omfang (antal ofre og beløb), (2) gerningsmandenes organisationsgrad og rolle, og (3) individuelle formildende eller skærpende omstændigheder.

Hovedmanden i en stor phishing-operation: I [SS-6507/2023-ALB](#) blev en 21-årig mand idømt **5 års fængsel** for at have organiseret et omfattende svindelsystem over halvandet år. Tiltalte sendte SMS'er med links til falske

MitID-sider til mere end 600 personer, og med de stjålne oplysninger foretog gerningsmændene over 2.900 onlinekøb af guld, luksusvarer og gavekort for mindst 27 mio. kr. Retten lagde særlig vægt på:

- Den lange periode (halvandet år)
- Den planlagte og organiserede karakter
- Det meget store antal ofre (over 600)
- Den enorme samlede beløbsstørrelse
- At tiltalte havde udnyttet unge kammerater til at stå for konti og firmaer

Tiltalte blev dømt efter [§ 279](#), [§ 279 a](#) og [§ 263, stk. 1 og 3](#), alle jf. [§ 286, stk. 2](#), samt [§ 21](#) (forsøg). Der skete konfiskation af luksusgenstande (Louis Vuitton, Prada, CELINE mv.) samt 17 sim-kort, og tiltalte blev pålagt erstatning for ca. 4,76 mio. kr.

Chaufføren i en vishing/smishing-gruppe: I [SS-634/2024-SVE](#) blev en 30-årig mand idømt **1 år og 9 måneders fængsel** for sin rolle som chauffør i en organiseret bedragerigruppe, der systematisk ringede ældre borgere op efter SMS-kontakt og fik dem til at udlevere betalingskort, kontanter og smykker. Der var tale om over 200 forhold mod ældre borgere i hele Jylland. Retten udtalte:

Retten har ved udmålingen af fængselsstraffen lagt vægt på kriminalitetens omfang og grovhed, herunder at tiltalte indgik i en veltilrettelagt organisation, der systematisk og målrettet gik efter at franske ældre medborgere deres opsparinger, kontanter, betalingskort, smykker mv.

I formildende retning indgik tiltaltes fulde tilståelse.

[Straffelovrådets betænkning nr. 1581/2023 om strafudmåling – Bind III](#) giver et samlet overblik over strafniveauet for databedrageri og bedrageri. For databedrageri i forbindelse med NemID/MitID-misbrug anføres i den lave ende 1 års fængsel (24 tilfælde af NemID-misbrug, lån for over 400.000 kr.) og i den høje ende 2–2½ års fængsel (systematisk misbrug over længere periode med beløb på 3–5 mio. kr.).

Rolle / omfang	Typisk strafniveau	Eksempel
Hovedmand, 600+ ofre, 27 mio. kr.	5 års fængsel	SS-6507/2023-ALB
Chauffør/medhjælper, 200+ forhold	1 år 9 mdr. fængsel	SS-634/2024-SVE
NemID-misbrug, 24 tilfælde, 400.000 kr.	1 års fængsel	Bet. 1581/2023
Stilling misbrug, systematisk, 3-5 mio. kr.	2–2½ års fængsel	Bet. 1581/2023

LOV	Straffeloven § 21	Straffeloven § 279	Straffeloven § 279a	Straffeloven § 286, stk. 2
PRAKSIS	Byretten · Ung mand idømt fem års fængsel for omfattende phishing og databedrageri for over 27 millioner kroner			07.06.2024
	Byretten · Dom for omfattende bedrageri og databedrageri mod ældre borgere			15.04.2024

§ 4 Modus operandi: Typiske SMS-scenarier og teknisk forløb

Smishing-angreb følger i dansk praksis et genkendeligt mønster. Gerningsmanden udsender en SMS med et link, der efterligner en pålidelig afsender. De hyppigste scenarier i den fundne praksis er:

-

PostNord-SMS: "Din pakke afventer betaling af fragt" med link til falsk PostNord-side, hvor offeret indtaster kortoplysninger.

- **MobilePay/bank-SMS:** "Din Online MitID-betaling er blevet deaktiveret" eller "Din konto er spærret" med link til falsk MitID-login.
- **DBA/handelsplatform-SMS:** I forbindelse med salg af varer sendes et link til en falsk DAO-betalingsside, der ser ud som en legitim fragt-/betalingsside.
- **Skat/Politi-SMS:** "Skat har en restance" eller "Politiet har en bøde" med link til falsk betalingsside.

Det tekniske forløb efter offeret klikker på linket er typisk:

1. **Indtastning af kortoplysninger** på den falske side – kortnummer, udløbsdato, CVC.
2. **MitID-godkendelse:** Gerningsmanden bruger de indtastede oplysninger til at initiere en betaling eller korttilknytning, som udløser en MitID-godkendelsesansøgning i offerets MitID-app.
3. **Aktivering af ny MitID-app:** I mere avancerede tilfælde narres offeret til at godkende oprettelsen af en ny MitID-app på en fremmed enhed, hvorved gerningsmanden får fuld kontrol over offerets digitale identitet.
4. **Udnyttelse:** Med adgang til MitID og kortoplysninger foretager gerningsmanden onlinekøb, bankoverførsler eller tilknytning af offerets kort til Apple Pay/Google Pay.

I sagen [507/2022](#) havde klageren dagen forinden selv ændret sit MitID-bruger-id, hvilket gjorde hende mindre mistænksom over for en SMS om, at hendes "Online MitID-betaling" var deaktiveret. Banken oplyste, at transaktionen blev godkendt via klagerens MitID-app, men IP-adressen var lokaliseret til Marokko.

I [357/2023](#) blev en ny MitID-app aktiveret på en fremmed enhed (iPhone 12 mini) efter validering af en SMS-pinkode sendt til klagerens telefon. Kort efter blev to transaktioner på hver 5.200 kr. gennemført til en kryptovalutabørs i Litauen.

Disse sager illustrerer, at smishing-angrebene i stigende grad udnytter MitID-arkitekturen – særligt funktionen til aktivering af nye MitID-apps – som en central vektor. Se også [praksisoversigten om MitID/NemID-misbrug](#) for den videre udnyttelse efter den initiale phishing.

PRAKSIS	Det finansielle ankenævn · Afvisning af sag om misbrug af MitID og korttransaktioner efter phishing-angreb via dba.dk	18.04.2024
	Det finansielle ankenævn · Afvisning af klage over kortmisbrug efter smishing-SMS grundet behov for bevisførelse	31.05.2023

Civilretlig hæftelse: Betalingslovens § 100 og Finansielle Ankenævns praksis

§ 5

Når en forbruger har lidt tab som følge af smishing, er det centrale civilretlige spørgsmål, hvem der bærer tabet – kunden eller banken. [Betalingslovens § 100](#) regulerer dette med en trinmodel, og Finansielle Ankenævn har udviklet en omfattende praksis for smishing-sager.

Hovedmønsteret i praksis: Bankerne godtgør som udgangspunkt hele tabet *minus* en selvrisiko på 8.000 kr. under henvisning til § 100, stk. 4 (groft uforsvarlig adfærd). Klagerne gør typisk gældende, at de højst bør hæfte med 375 kr. (stk. 3). Ankenævnet afviser hyppigt at tage stilling til dette spørgsmål og henviser sagen

til domstolene, fordi en afklaring af, om kunden ved groft uforsvarlig adfærd har muliggjort misbruget, kræver mundtlige parts- og vidneforklaringer.

I sagen [131/2023](#) – der direkte omhandlede en PostNord-SMS – havde klageren klikket på et link i en SMS, der angav, at en pakke ventede på betaling. Klageren indtastede kortoplysninger på den falske side, og der blev efterfølgende foretaget uautoriserede transaktioner. Banken anerkendte at godtgøre tabet med fradrag af 8.000 kr.

I [533/2023](#) modtog klageren en SMS, der fremstod som fra MobilePay. Hun trykkede på linket, indtastede kortoplysninger og anvendte sit MitID. Tre uautoriserede transaktioner blev gennemført. Banken fastholdt, at klageren hæftede for 8.000 kr. med den begrundelse, at MitID-appen specifikt viste teksten: *"Betal 10000,00 DKK til [B] fra kort xx1623"*, og at klageren ved at godkende en betaling til en ukendt modtager udviste groft uforsvarlig adfærd. Ankenævnet afviste sagen til domstolene.

Samme mønster ses i [304/2023](#), [409/2023](#), [530/2023](#) og [700/2023](#), hvor bankerne konsekvent anvender 8.000 kr.-selvrisikoen, og nævnet hyppigt afviser til domstolene ved bevistvivl.

Oversigt over hæftelsesniveauer:

Betalingslovens § 100	Hæftelsesbeløb	Typisk situation ved smishing
Stk. 3	Op til 375 kr.	Offeret har <i>ikke</i> handlet groft uforsvarligt – typisk rent automatiserede transaktioner uden MitID-godkendelse
Stk. 4	Op til 8.000 kr.	Offeret har godkendt MitID-transaktion efter at have klikket på phishing-link – bankernes standardposition
Stk. 5	Ubegrænset	Offeret har handlet svigagtigt – sjældent relevant ved smishing

LOV

[Betalingsloven § 100, stk. 3-5](#)

PRAKSIS

Det finansielle ankenævn · Hæftelse for 8.000 kr. efter phishing-mail: Groft uforsvarlig adfærd ved godkendelse af MitID-transaktion	19.08.2024
Det finansielle ankenævn · Indsigelse mod hæftelse for 8.000 kr. ved svindel-transaktion godkendt med MitID efter phishing-SMS	18.04.2024
Det finansielle ankenævn · Afvisning af sag om misbrug af MitID og korttransaktioner efter phishing-angreb via dba.dk	18.04.2024
Det finansielle ankenævn · Indsigelse mod hæftelse for phishing-transaktion på 3.726,25 kr. godkendt via MitID	19.03.2024
Det finansielle ankenævn · Indsigelse mod misbrug via Apple Pay efter phishing-SMS afvist grundet behov for bevisførelse	18.01.2024
Det finansielle ankenævn · Indsigelse mod hæftelse for Apple Pay-transaktioner efter indrullering af betalingskort i tredjemands wallet	22.12.2023
Det finansielle ankenævn · Groft uforsvarlig adfærd ved phishing-SMS: Hæftelse for 8.000 kr. efter godkendelse af MitID-anmodning på stort beløb	06.09.2023
Det finansielle ankenævn · Afvisning af klage over kortmisbrug efter smishing-SMS grundet behov for bevisførelse	31.05.2023

§ 6 Landsretspraksis om bankens hæftelse ved phishing

Mens Finansielle Ankenævn ofte afviser smishing-sager til domstolene, har der dannet sig en vis landsretspraksis om fordelingen af tab.

I [BS-2380/2022-VLR](#) behandlede Vestre Landsret spørgsmålet om en banks hæftelse over for en kunde, der var blevet offer for phishing. Sagen illustrerer det centrale bevisspørgsmål: om kunden ved at reagere på en phishing-henvendelse og videregive autentifikationsoplysninger har handlet "groft uforsvarligt" i betalingslovens forstand.

I en anden landsretssag, [BS-28994/2022-OLR](#), tog Østre Landsret stilling til lignende spørgsmål om kundens hæftelse ved uautoriserede transaktioner initieret via phishing.

Praksis viser, at domstolene foretager en konkret vurdering af hændelsesforløbet, herunder:

- Om SMS'en/kommunikationen bar tydelige tegn på svindel, som kunden burde have genkendt
- Om MitID-godkendelsesteksten tydeligt angav modtager og beløb, som afveg fra det forventede
- Om kunden reagerede hurtigt med spærring efter at have fattet mistanke
- Om banken havde opfyldt sine forpligtelser til at levere tilstrækkelig autentifikation og advarsler

Landsretten har i de behandlede sager lagt vægt på, at phishing-angrebene ofte er *professionelt* udført og kan være vanskelige for selv opmærksomme forbrugere at gennemskue. Dette taler mod at skærpe kundens hæftelse til det ubegrænsede niveau i § 100, stk. 5.

LOV

[Betalingsloven § 100, stk. 4](#)

PRAKSIS

Landsretten · Betydelig fællesstraf og udvisning for omfattende bedrageri og databedrageri mod ældre borgere (ca. 42 forhold) 11.04.2025

Landsretten · Bedrageri og medvirken til databedrageri: Frifindelse i Landsretten for lån optaget i andres navn 31.01.2023

§ 7 Udvisning af udenlandske gerningsmænd ved organiseret smishing

Organiseret smishing-bedrageri begås i mange tilfælde af udenlandske gerningsmænd, der indrejser i Danmark som led i en koordineret operation. Udvisningsspørgsmålet vurderes efter udlændingelovens § 22–§ 26, herunder proportionalitetsprincippet i EMRK art. 8 (retten til respekt for privat- og familieliv).

I Højesterets dom [U.2022.4567H](#) blev en udenlandsk statsborger udvist for organiseret databedrageri. Højesteret vurderede, at den organiserede karakter og det store omfang af bedrageriet udgjorde tungtvejende grunde for udvisning, som ikke blev opvejet af tiltaltes tilknytning til Danmark.

I byretsdomme vedrørende smishing-sager, herunder [SS-6507/2023-ALB](#), ses det, at gerningsmændene opererer internationalt – tiltalte i den konkrete sag blev anholdt på et hotel i Madrid, hvor spansk politi fandt 17 sim-kort og computere med phishing-skabeloner. Denne grænseoverskridende karakter er et fast træk ved organiseret smishing og har betydning for vurderingen af udvisning og indrejseforbud.

Praksis viser, at udvisning med indrejseforbud i 6 år er udgangspunktet ved organiseret smishing, medmindre gerningsmanden har så stærk tilknytning til Danmark (børn, langvarigt ophold, sygdom), at det ville være uproportionalt efter EMRK art. 8.

LOV

[Straffeloven § 286, stk. 2](#)

PRAKSIS	Byretten · Mand idømt 6 års fængsel for organiseret 'smishing' og databedrageri for over 23 millioner kroner	26.08.2025
	Byretten · Ung mand idømt fem års fængsel for omfattende phishing og databedrageri for over 27 millioner kroner	07.06.2024

§ 8 Pengemuldyr og hvidvask i forbindelse med smishing

Et fast element i organiserede smishing-operationer er brugen af **pengemuldyr** (money mules) – personer der stiller deres bankkonti til rådighed for at modtage og videreoverføre udbyttet af bedrageriet. Pengemuldyrene rekrutteres ofte via sociale medier med løfter om let fortjeneste og straffes selvstændigt, typisk for hvidvask efter [straffelovens § 290 a](#) eller medvirken til bedrageri.

I den store smishing-sag [SS-6507/2023-ALB](#) havde hovedmanden instrueret flere unge bekendte i at oprette selskaber og bankkonti, som blev brugt til at modtage indbetalinger fra de falske webshops og phishing-operationen. Et af vidnerne forklarede, at han modtog indbetalinger på sin konto uden at vide hvorfra, og overførte dem til tiltalte efter pres.

I [SS-634/2024-SVE](#) fungerede flere navngivne medgerningsmænd som mellemed, der afhentede betalingskort fra ofre og misbrugte dem i hæveautomater og til varekøb.

Forsætsvurderingen for pengemuldyr er ofte et centralt stridspunkt: Anklagemyndigheden skal bevise, at pengemuldyret indså eller fandt det overvejende sandsynligt, at midlerne stammede fra en strafbar handling. I praksis er det afgørende, om der forelå omstændigheder, der burde have vakt mistanke – fx usædvanligt store indbetalinger fra ukendte personer, anmodning om straks at videreoverføre beløbet, eller åbenlys disproportion mellem den lovede betaling og den krævede indsats.

Se [praksisoversigten om databedrageri](#) for en bredere behandling af CEO-fraud og e-mail-baseret phishing mod virksomheder.

LOV [Straffeloven § 279a](#)

PRAKSIS	Byretten · Ung mand idømt fem års fængsel for omfattende phishing og databedrageri for over 27 millioner kroner	07.06.2024
	Byretten · Dom for omfattende bedrageri og databedrageri mod ældre borgere	15.04.2024

§ 9 Identitetsmisbrug og hacking som selvstændige gerningsindhold

Smishing-bedrageri indebærer ofte overtrædelse af flere straffebestemmelser ud over [§ 279/§ 279 a](#). De vigtigste er:

Hacking – [straffelovens § 263, stk. 1](#): Ubertrettiget adgang til en andens oplysninger eller programmer i et informationssystem. Når gerningsmanden bruger de phishede MitID-oplysninger til at logge ind i offerets netbank, foreligger der hacking i sammenstød med databedrageri. I [SS-6507/2023-ALB](#) blev tiltalte dømt efter [§ 263, stk. 1 og 3](#) for at have skaffet sig uberettiget adgang til over 700 personers MitID-oplysninger.

Ulovlig adgang til MitID – [straffelovens § 263 a, stk. 1, nr. 3, litra a](#): Bestemmelsen rammer den, der uberettiget skaffer sig adgang til et andet datasystem. I [SS-634/2024-SVE](#) blev dette forhold medtaget i tiltalen vedrørende uberettiget adgang til ofres MitID.

Identitetsmisbrug – straffelovens § 264 e: Rigsadvokatmeddelelsen om freds- og ærekrænkelser fastslår, at der som udgangspunkt straffes i *sammenstød* i tilfælde, hvor der forud for, samtidigt med eller efter en overtrædelse af § 264 e foreligger en overtrædelse af fx § 279 om bedrageri eller § 279 a om databedrageri. Udgangspunktet for førstegangs bøden er 10.000 kr., men ved groft identitetsmisbrug kan der idømmes fængselsstraf.

LOV	Straffeloven § 263, stk. 1	Straffeloven § 263a, stk. 1	Straffeloven § 264e
PRAKSIS	Byretten · Ung mand idømt fem års fængsel for omfattende phishing og databedrageri for over 27 millioner kroner		07.06.2024
	Byretten · Dom for omfattende bedrageri og databedrageri mod ældre borgere		15.04.2024

§ 10 Sammenfatning og centrale tendenser

SMS-phishing (smishing) er et dynamisk kriminalitetsområde, hvor dansk retspraksis stadig er under udvikling. De centrale tendenser kan opsummeres således:

- **Strafferetligt** kvalificeres smishing som databedrageri (§ 279 a), ofte i sammenstød med hacking (§ 263) og identitetsmisbrug (§ 264 e). Ved grovere organiseret kriminalitet med mange ofre og store beløb henføres forholdene under § 286, stk. 2, med strafmaksimum på 8 år. Praksis viser straffe i intervallet 1½–5 år afhængigt af rolle og omfang.
- **Civilretligt** bærer ofret som udgangspunkt en selvrisiko på 8.000 kr. (betalingslovens § 100, stk. 4), når vedkommende har godkendt en MitID-transaktion efter en phishing-SMS. Finansielle Ankenævn afviser ofte at tage endelig stilling til hæftelsesniveauet og henviser sagen til domstolene, når der er tvivl om omstændighederne ved godkendelsen.
- **Organisatorisk** behandles sagerne centralt af NCIK under NSK, med SSK som tilsynsmyndighed. Den grænseoverskridende karakter af smishing – med gerningsmænd der opererer fra udlandet via spoofede SMS-afsendere – stiller særlige krav til det internationale politisamarbejde.
- **Pengemuldyr** rekrutteres til at vaske udbyttet og straffes selvstændigt for hvidvask. Forsætsvurderingen er central: det afgørende er, om pengemuldyret indså eller burde have indset, at midlerne stammede fra kriminalitet.
- **Udvisning** af udenlandske gerningsmænd er hovedreglen ved organiseret smishing, men proportionalitetsvurderingen efter EMRK art. 8 kan i konkrete tilfælde føre til et andet resultat.

For den bredere kontekst af digital bedrageri, se [praksisoversigten om databedrageri](#) (e-mail-baseret CEO-fraud og virksomhedsbedrageri) og [praksisoversigten om MitID/NemID-misbrug](#) (den videre udnyttelse efter den initiale phishing).

LOV	Betalingsloven § 100, stk. 3-4	Straffeloven § 279a	Straffeloven § 286, stk. 2
PRAKSIS	Byretten · Ung mand idømt fem års fængsel for omfattende phishing og databedrageri for over 27 millioner kroner		07.06.2024
	Byretten · Dom for omfattende bedrageri og databedrageri mod ældre borgere		15.04.2024
	Det finansielle ankenævn · Indsigelse mod hæftelse for 8.000 kr. ved svindel-transaktion godkendt med MitID efter phishing-SMS		18.04.2024
	Det finansielle ankenævn · Groft uforsvarlig adfærd ved phishing-SMS: Hæftelse for 8.000 kr. efter godkendelse af MitID-anmodning på stort beløb		06.09.2023

REFERENCE Lovgrundlag

6 paragraffer

Betalingsloven § 100	stk. 3-4	Straffeloven § 21	
Straffeloven § 263a	stk. 1	Straffeloven § 279	
Straffeloven § 279a		Straffeloven § 286	stk. 2

MATERIALE Citerede afgørelser

22 afgørelser

HØJESTERET · ØVERSTE INSTANS

3

28.06.2023	Højesterets vurdering af varetægtsfængsling ved omfattende databedrageri og påvirkningsrisiko	AM2023.06.28H
29.05.2017	Højesteret stadfæster dom for organiseret menneskehandel og databedrageri: Udnyttelse af identitet kræver ikke kendskab fra ofret	Sag 70/2017
30.06.2015	Højesteret stadfæster ubetinget udvisning i 12 år af serbisk statsborger for organiseret databedrageri af særlig grov beskaffenhed	Sag 85/2015

LANDSRETTE · ANKEINSTANS

3

11.04.2025	Betydelig fællesstraf og udvisning for omfattende bedrageri og databedrageri mod ældre borgere (ca. 42 forhold)	S-0009-25
31.01.2023	Bedrageri og medvirken til databedrageri: Frifindelse i Landsretten for lån optaget i andres navn	S-0930-22
09.12.2022	Afgørelse om hæftelse for tab ved phishing efter Betalingslovens § 100	2941-3487

BYRETTE · FØRSTE INSTANS

5

26.08.2025	Mand idømt 6 års fængsel for organiseret 'smishing' og databedrageri for over 23 millioner kroner	10075-11802
07.06.2024	Ung mand idømt fem års fængsel for omfattende phishing og databedrageri for over 27 millioner kroner	6168-7392
15.04.2024	Omfattende sag om bedrageri mod ældre borgere: Fængselsstraf og erstatningskrav	6568-7891
15.04.2024	Dom for omfattende bedrageri og databedrageri mod ældre borgere	6569-7892
15.12.2023	Omfattende dom for databedrageri: Fire tiltalte idømt lange fængselsstraffe	6497-7797

DET FINANSIELLE ANKENÆVN · NÆVN / KLAGESTANS

10

22.01.2026	Hæftelse for misbrug af betalingskort efter phishing-mail: Groft uforsvarlig adfærd ved godkendelse i MitID	468/2025
17.01.2025	Hæftelse for 8.000 kr. ved phishing-svindel: Klager godkendte EUR-beløb i MitID i troen om fragtbetaling på 39 kr.	233/2024

19.08.2024	Hæftelse for 8.000 kr. efter phishing-mail: Groft uforsvarlig adfærd ved godkendelse af MitID-transaktion	700/2023
18.04.2024	Afvisning af sag om misbrug af MitID og korttransaktioner efter phishing-angreb via dba.dk	357/2023
18.04.2024	Indsigelse mod hæftelse for 8.000 kr. ved svindel-transaktion godkendt med MitID efter phishing-SMS	533/2023
19.03.2024	Indsigelse mod hæftelse for phishing-transaktion på 3.726,25 kr. godkendt via MitID	530/2023
18.01.2024	Indsigelse mod misbrug via Apple Pay efter phishing-SMS afvist grundet behov for bevisførelse	409/2023
22.12.2023	Indsigelse mod hæftelse for Apple Pay-transaktioner efter indrullering af betalingskort i tredjemands wallet	304/2023
06.09.2023	Groft uforsvarlig adfærd ved phishing-SMS: Hæftelse for 8.000 kr. efter godkendelse af MitID-anmodning på stort beløb	131/2023
31.05.2023	Afvisning af klage over kortmisbrug efter smishing-SMS grundet behov for bevisførelse	507/2022

PARKERINGSKLAGENÆVNET · NÆVN / KLAGEINSTANS

1

28.04.2023	Kontrolafgift pålagt knallert for manglende p-tilladelse på privat område	park-3487
------------	---	-----------

FORARBEJDE **Betænkninger**

1 reference

Betænkning om strafudmåling – Bind III

nr. 1581 · 2023 · Justitsministeriet