

Sådan sikrer du dig bedst muligt i tilfælde af svindel

Nedenfor guider vi dig til, hvad du bør gøre, hvis du har været udsat for svindel, eller andre har fået adgang til din personlige oplysninger.

1. Få et nyt MitID

Hvis der er risiko for, at dit MitID kan blive misbrugt, skal det spærres. Herefter skal du have oprettet et nyt MitID. Det kan du selv gøre på www.mitid.dk, eller du kan kontakte Borgerservice.

Du kan læse mere om spærring af dit MitID [her](#) eller kontakte support på tlf. 33 98 00 10.

2. Opret nye adgangskoder, hvis du bruger samme koder flere steder

Bruger du den samme adgangskode flere steder, og er der risiko for, at andre har fået kendskab til en eller flere af dine koder, skal du oprette nye.

Du er bedre sikret, hvis den samme kode ikke kan give en svindler adgang til flere af de digitale løsninger, du bruger. Opret derfor en forskellig adgangskode til hver løsning, du bruger (f.eks. Facebook, e-mail mm.).

3. Spær eventuelt dit betalingskort

Hvis andre har fået kendskab til dine kortoplysninger, skal du spærre dit kort og bestille et nyt. Det gør du her <https://www.spardjurs.dk/Selvbetjening/Betalingskort/Spær-kort> eller ved at kontakte din rådgiver.

Hold også øje med din konto. Hvis der bliver hævet et beløb, du ikke kender til, skal du gøre indsigelse. Det gør du på <https://www.spardjurs.dk/Selvbetjening/Spærring-eller-indsigelse-betalingskort>.

4. Opret en kreditadvarsel

Vi anbefaler dig at oprette en kreditadvarsel, så andre f.eks. ikke kan optage et lån i dit navn. Det gør du ved at logge på www.borger.dk, når du har fået dit nye MitID.

5. Tjek, om der er oprettet kviklån i dit navn

En svindler kan forsøge at oprette kviklån i dit navn. Derfor anbefaler vi dig at undersøge, om der er blevet forespurgt på dine skatteoplysninger. Sådan gør du:

1. Log på www.skat.dk (når du har fået dit nye MitID)
2. Klik på "Profil" i øverste højre hjørne
3. Vælg "Oversigt over hændelser"
4. Vælg "Alle hændelser"
5. I listen kan du se, hvis et kviklånselskab eller lignende har spurgt på dine skatteoplysninger

Derudover kan du på www.kreditstatus.dk se, om der er blevet optaget lån i dit navn. Er dette tilfældet, skal du kontakte de pågældende selskaber direkte.

6. Få rensed din computer

Hvis en svindler har haft adgang til din computer – f.eks. i forbindelse med misbrug af din Netbank – anbefaler vi, at du får den rensed hos en professionel. Dog bør du først spørge politiet, om de skal undersøge din computer i forbindelse med efterforskningen.

7. Lav en politianmeldelse

Vi anbefaler, at du anmelder sagen til politiet. Det kan du gøre på politiets hjemmeside under [anmeld økonomisk kriminalitet på nettet](#).

8. Hent app'en "Mit digitale selvforsvar"

Svindlerne ændrer hele tiden metoder, og det kan være svært at følge med. Derfor anbefaler vi dig, at du henter appen "Mit digitale selvforsvar", hvor du løbende bliver informeret om aktuelle og nye svindelmetoder, som du skal være opmærksom på.

Hjælp andre, så de ikke bliver udsat for svindel

Vi ved, at det føles meget ubehageligt at blive udsat for svindel eller svindelforsøg, men du skal vide, at det desværre ofte sker – du er altså ikke alene.

Måske du kan hjælpe til med at undgå, at det sker for andre. Tal derfor med din familie, venner og bekendte om din oplevelse, så de kan være på vagt, hvis de oplever noget lignende.

Husk, at hverken Sparekassen Djursland, offentlige myndigheder eller private virksomheder vil bede dig om at oplyse din adgangskode, dine oplysninger til MitID eller din kode til en betalingsløsning (f.eks. PIN-koden til din telefon). Det gælder både på telefon, sms og mail.

Har du spørgsmål eller brug for hjælp?

Du er altid velkommen til at kontakte din rådgiver eller lokale filial, hvis du har spørgsmål eller brug for hjælp. Du kan også kontakte Digitaliseringsstyrelsens hotline for identitetstyveri døgnet rund på tlf. 33 98 00 98.