NCIK | NATIONALT CENTER FOR IT-KRIMINALITET

FAQ om telefonsvindel

Juni, 2023

POLITI

I denne FAQ finder du en række ofte stillede spørgsmål og svar om telefonsvindel. Under hvert spørgsmål kan du finde politiets anbefalinger og gode råd.

I dette dokument kan du finde svar på følgende spørgsmål:

- Hvad er phishing og smishing?
- Hvad er telefonsvindel/vishing – og hvordan foregår det
- Hvad betyder spoofing?
- Hvordan finder de kriminelle mine oplysninger?
- Må jeg godt bare smække røret på, hvis det nu er den rigtige bank eller politiet, der ringer?
- Hvilke konsekvenser har telefonsvindel for ældre?
- Kan de kriminelle møde op på min adresse?
- Hvad er politiets råd til at undgå telefonsvindel?
  Hvordan skal jeg forholde mig, hvis jeg er blevet udsat for telefonsvindel?
- Hvem kan jeg kontakte for at få hjælp?

Q- Hvad er phishing og smishing?

Phishing er falske e-mails, mens *smishing* er falske sms'er.

Svindlen sker typisk ved, at du modtager en e-mail eller en sms, hvor afsenderen forsøger at få dig til at udlevere dine personlige oplysninger som eksempelvis betalingsoplysninger eller MitID-oplysninger via et link i mailen eller sms'en.

Vær opmærksom på, at du også kan modtage falske beskeder på andre platforme som eksempelvis Facebooks Messenger eller WhatsApp, hvor kriminelle kan udgive sig for at være dine venner eller familiemedlemmer.

Politiets anbefaling:

Klik aldrig på links tilsendt via e-mails eller sms'er. Søg selv hjemmesiden frem via din internetbrowser, så du kan se, om siden er ægte eller ej. På den måde undgår du falske links og falske hjemmesider.

Q- Hvad er telefonsvindel/vishing – og hvordan foregår det?

Telefonsvindel kaldes også for *vishing*, og er telefonopkald, hvor kriminelle udgiver sig for at være fra eksempelvis banken, politiet eller en anden myndighed.

Ofte ringer den kriminelle til ældre borgere og udgiver sig for at være eksempelvis fra borgerens pengeinstitut. Den kriminelle vil i dette tilfælde eventuelt fortælle borgeren, at dennes konto er blevet hacket, eller at der har været uregelmæssig aktivitet, eksempelvis i form af udenlandske køb eller optagede lån. Herefter vil den kriminelle ofte prøve at lokke de ældres personlige oplysninger ud af dem, eller overtale dem til at overføre deres penge til en "sikker" konto, som den kriminelle har adgang til.

Vær opmærksom på, at den kriminelle kan arbejde sammen med andre og dermed viderestille den ældre til "kolleger" i banken, politiet, SKAT eller andre myndigheder. Dette sker for at øge troværdigheden af opkaldet, som ofte bærer præg af hast, så borgeren ikke får tid til at tænke sig om.

Politiets anbefaling:

Pengeinstitutter og myndigheder vil **ALDRIG** bede dig om at overføre dine penge. Smæk derfor røret på, hvis nogen ringer og beder dig om betalingsoplysninger, overførsel af penge eller udlevering af personlige oplysninger som eksempelvis personlige koder. Hvis du er det mindste i tvivl, så smæk røret på eller sig, at du ringer tilbage. Kontakt derefter den pågældende virksomhed, bank eller myndighed via hovednummeret og spørg om henvendelsen er ægte og reel.

Q- Hvad betyder spoofing?

Spoofing er betegnelsen for den teknik, kriminelle benytter for at få det til at se ud som om, at opkaldet kommer fra et autoriseret telefonnummer, eksempelvis fra banker, politiet eller andre myndigheder

Politiets anbefaling:

Hvis du er i tvivl om, hvorvidt opkaldet er ægte, så smæk røret på og find efterfølgende myndighedens eller bankens hovednummer. Ring op og spørg om opkaldet er ægte.

Q- Hvordan finder de kriminelle mine oplysninger?

Mange ældre borgere har deres telefonnummer tilgængeligt på Krak.dk, De Gule Sider eller på 118. Her vil de kriminelle søge efter almindelige navne hos de ældre generationer som eksempelvis Else, Grethe og Gerda.

Vær opmærksom på, at de kriminelle kan benytte ældres sociale medier til at samle viden, der kan gøre henvendelsen mere personlig og troværdig.

Alle disse informationer kan bidrage til at gøre henvendelsen mere troværdig og personlig, hvilket kan gøre det sværere for den ældre at gennemskue svindlen.

Politiets anbefaling:

Gå ind på dit telefonselskabs hjemmeside og slå **udeladt nummer** til. Du kan også ringe til dit telefonselskab og bede dem gøre det for dig. På den måde har de kriminelle ikke direkte adgang til dit telefonnummer.

Gør derudover din Facebook-profil privat, så det kun er dig og dine venner, der har adgang til personlige oplysninger om dig.

Q- Må jeg godt bare smække røret på, hvis det nu er den rigtige bank eller politiet, der ringer?

Du skal altid smække røret på, hvis du bliver bedt om at udlevere personlige oplysninger såsom brugernavn til MitID eller bliver fortalt, at din konto er i fare.

Hvis du er i tvivl, om opkaldet er ægte, så kan du altid ringe tilbage på hovednummeret.

Både banken, politiet og andre myndigheder har forståelse for, at du udviser forsigtighed og selv ringer tilbage til dem på deres hovednummer.

Q- Hvilke konsekvenser har telefonsvindel for ældre?

Telefonsvindel har ikke kun store økonomiske konsekvenser – der kan også følge en stor grad af skyld og skam over, at man "lod sig narre" af en kriminel. Derudover kan ældre blive utrygge ved at tage telefonen i fremtiden, ligesom de også kan blive bange for at blive opsøgt og truet af de kriminelle.

Politiets anbefaling:

Hvis du bliver kontaktet af en telefonsvindler, er det meget vigtigt, at du taler om oplevelsen – uanset om du er blevet svindlet eller ej. Nogle oplever at få skældud af børn eller ægtefælle, men det er vigtigt at understrege, at ingen er dumme – ud over de kriminelle, der forsøger at franarre folk deres penge. Denne form for svindel kan være meget svær at gennemskue, og vi kan alle blive ofre for den. Derfor er det vigtigt, at du deler dine erfaringer med andre, og taler om din oplevelse. På den måde kan vi forhåbentlig være med til at minimere risikoen for, at andre udsættes for telefonsvindel.

Q- Kan de kriminelle møde op på min adresse?

De kriminelle møder i nogle tilfælde fysisk op på den ældres adresse og udgiver sig for at være fra banken eller politiet. Dette sker ofte i forbindelse med et telefonopkald, hvor den ældre yderligere bliver narret til at udlevere enten kontanter eller sit dankort med PIN-kode. Det sker under påskud af, at dankortet eller kontanterne skal sikres.

Politiets anbefaling:

Politiet, banken eller andre myndigheder vil **ALDRIG** møde op på din adresse og bede dig om at udlevere kontanter eller dit betalingskort. Dit betalingskort og PIN-koden hertil er personlig, og du skal ikke udlevere det eller dele koden med andre.

Hvad er politiets råd til at undgå telefonsvindel?

SMÆK RØRET PÅ – tre gode råd:

- Vær på vagt - det er svindel, hvis nogen ringer og beder dig overføre penge.
- Smæk røret på - hellere et nej for meget!
- Hvis du er i tvivl, så ring til banken, politiet (på 114) eller en nærtstående.

Hvordan skal jeg forholde mig, hvis jeg er blevet udsat for telefonsvindel?
Hvis du er blevet narret til at overføre penge eller udlevere dine personlige oplysninger over telefonen, er det vigtigt, at du meget hurtigt kontakter din bank på deres hovednummer og får spærret din konto og dit betalingskort.

Hvem kan jeg kontakte for at få hjælp?
Digitaliseringsstyrelsens har to rådgivningslinjer, hvor du blandt andet kan få hjælp til at lære at spotte svindel og blive mere digital sikker. Du kan også få hjælp til, hvad du skal gøre, hvis du har været udsat for svindel.

Cyberhotline til rådgivning om, hvordan du bliver mere sikker digital: **33 37 00 37**

Vejledning til, hvad du skal gøre, hvis du har været udsat for svindel**: 33 98 00 98**