JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 5. december 2019
Kontor: Strafferetskontoret
Sagsbeh: Camilla Nielsen
Sagsnr.: 2019-0030-3014
Dok.: 1293255

Hermed sendes besvarelse af spørgsmål nr. 248 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 7. november 2019. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Mette Johansen

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 248 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren redegøre for, hvordan spoofing er kriminaliseret, og om der er hjemmel til at lukke for de hjemmesider, der tilbyder denne form for SMS-service, og vil ministeren redegøre for, hvilke initiativer ministeren vil tage til at bekæmpe denne form for snyd, jf. artiklen: ”Erik advarer mod trick: Svindlerne sender SMS'er fra dit telefonnummer” fra bt.dk den 5. november 2019?”

Svar:

1. Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Rigsadvokaten, der har oplyst følgende:

> ”Spoofing er ikke selvstændigt kriminaliseret men kan bruges som middel til at begå forskellige former for kriminalitet, herunder navnlig berigelseskriminalitet som eksempelvis bedrageri.
>
> Det følger af straffelovens § 279, at for bedrageri straffes den, som, for derigennem at skaffe sig eller andre uberettiget vinding, ved retsstridigt at fremkalde, bestyrke eller udnytte en vildfarelse bestemmer en anden til en handling eller undladelse, hvorved der påføres denne eller nogen, for hvem handlingen eller undladelsen bliver afgørende, et formuetab.
>
> Strafudmålingen i sager, der involverer spoofing, vil afhænge af strafniveauet for den pågældende lovovertrædelse. Det betyder, at hvis en person via digital kommunikation får afsenderen af en sms til at fremstå som hidrørende fra en anden end den reelle afsender, og dermed får en anden person til at overføre penge til sig, og som følge heraf opnår en uberettiget økonomisk gevinst, vil straffen blive udmålt i overensstemmelse med strafniveauet for bedragerisager af tilsvarende grovhed.
>
> Strafferammen for bedrageri er fra bøde op til 8 års fængsel, jf. straffelovens §§ 285-287.”

Justitsministeriet har til brug for besvarelsen af spørgsmålet endvidere indhentet en udtalelse fra Rigspolitiet, som bl.a. har oplyst følgende:

> ”Indledningsvist kan Rigspolitiet oplyse, at det er sædvanligt i f.eks. arbejdsmæssige sammenhænge i såvel den offentlige som private sektor at anvende hjemmesider eller apps til at afsende SMS mv. Dette vil typisk være tilfældet, når virksomheden mv. vil sende en SMS mv. til mange modtagere på én gang, og hvor beskeden skal fremstå som afsendt fra selve virksomheden og ikke fra en bestemt medarbejders telefon.

Teknologien kan imidlertid misbruges til kriminelle formål, idet en SMS mv. kan manipuleres til at fremstå som en aktivitet, der er udgået fra f.eks. et bestemt telefonnummer, selv om aktiviteten reelt er udgået fra en app eller lignende. Derved er det muligt for kriminelle at vildlede og derigennem eventuelt opnå et kriminelt forehavende. Modtageren af en manipuleret SMS kan således f.eks. vildledes til at overføre penge til et kontonummer, der er oplyst i den manipulerede SMS.

Rigspolitiet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Københavns Politi, Landsdækkende Center for IT-relateret økonomisk Kriminalitet (LCIK), der bl.a. har oplyst, at LCIK siden centerets opstart i december 2018 løbende har modtaget anmeldelser af forhold, hvor modus er, at gerningsmanden som led i gerningen har benyttet sig af "spoofed" SMS'er. Disse sager registreres ikke på en særskilt gerningskode i politiets sagsstyringssystem (POLSAS), og det er derfor ikke muligt at oplyse, hvor mange sager det drejer sig om. Det er dog Københavns Politis vurdering, at der er tale om et større antal sager.

Anmeldelserne omhandler primært bedrageri i forbindelse med køb mellem private parter, hvor gerningsmanden har formået at få den forurettede til at udlevere en vare ved fremvisning af en "spoofed" SMS, hvoraf det fremgår, at gerningsmandens bank har bekræftet, at der er overført penge til den forurettedes bankkonto. I disse tilfælde har den forurettede først efterfølgende opdaget, at gerningsmanden ikke har overført betalingen til den forurettede.

LCIK har løbende forebyggende indsatser, hvor LCIK oplyser borgerne om denne type af svindel og giver borgerne konkret rådgivning om, hvordan man undgår at blive udsat herfor. Den forebyggende indsats sker bl.a. i forbindelse med pressehenvendelser, ligesom LCIK i anledning af "Cyber Security Month" i oktober 2019 sendte forebyggelsespakker ud til politikredsene, således at politiet lokalt kan oplyse og rådgive borgerne om at undgå svindel i forbindelse med samhandel. LCIK har endvidere i forbindelse med "Cyber Security Month" sammen med Rigspolitiet deltaget i en live chat via Facebook, hvor borgerne kunne stille spørgsmål om, hvordan de kan undgå at blive udsat for IT-relateret økonomisk kriminalitet.

I forbindelse med de forebyggende indsatser rådgiver LCIK bl.a. borgerne om, at man ikke har modtaget penge i forbindelse med en bankoverførsel, førend beløbet fremstår som indestående på ens egen bankkonto. LCIK oplyser endvidere borgerne om, at banker og pengeinstitutter ikke sender SMS-beskeder som dem, der er beskrevet ovenfor, hvor banken mv. bekræfter pengeoverførslen.

> Københavns Politi har desuden oplyst, at LCIK har været med til at udvikle og levere indhold til Forbrugerrådet Tænks app "Mit Digitale Selvforsvar". Via app'en kan borgere holde sig opdateret om digitale trusler, udviklingen på kriminalitetsområdet og generelt læse om sikkerhed på nettet. I app'en kan man blandt andet læse om "spoofing". LCIK henviser altid borgerne til at downloade app'en "Mit Digitale Selvforsvar", hvor man kan holde sig orienteret om udviklingen på kriminalitetsområdet. Når en borger har foretaget en anmeldelse til LCIK via politi.dk, får de en anmeldelseskvittering, hvor der ligeledes fremgår oplysninger om app'en "Mit Digitale Selvforsvar".
>
> Både LCIK og Rigspolitiets Nationale Cyber Crime Center (NC3) har siden efteråret 2018 endvidere arbejdet tæt sammen med Digitaliseringsstyrelsen og Erhvervsstyrelsen om hjemmesiden www.sikkerdigtal.dk, hvor såvel borgere som virksomheder kan hente gode råd til en mere sikker digital adfærd. Både LCIK og NC3 leverer løbende input til hjemmesiden, når der opstår nye trends på it-kriminalitetsområdet.
>
> Rigspolitiet kan supplerende oplyse, at i forbindelse med politiets efterforskning vil det ofte være muligt at afdække, hvorvidt en SMS mv. er manipuleret. Den manipulerede SMS'en mv. vil således ikke – modsat en normal SMS – blive registreret i teledata vedrørende det telefonnummer mv., der fremstår som afsender af SMS'en.
>
> Afslutningsvist kan Rigspolitiet oplyse, at der er etableret et samarbejdsforum mellem Rigspolitiet og teleudbyderne, der bl.a. skal sikre fornøden informationsudveksling om fremtidige tiltag, der vil kunne påvirke partnernes virksomhed direkte eller indirekte. Rigspolitiet vil sikre, at behovet for eventuelle særlige indsatser i forhold til "spoofing"-tjenester bliver drøftet i dette samarbejdsforum."

2. Om adgangen til at lukke hjemmesider kan Justitsministeriet generelt oplyse, at i tilfælde, hvor en hjemmeside anvendes til mulige strafbare forhold, vil der efter omstændighederne og som udgangspunkt efter forudgående retskendelse kunne ske beslaglæggelse i henhold til reglerne i retsplejelovens kapitel 74.

Reglerne om beslaglæggelse suppleres af bestemmelsen i retsplejelovens § 791 d om blokering af hjemmesider. Denne bestemmelse finder dog alene anvendelse, hvis der er grund til at antage, at der fra hjemmesiden begås en overtrædelse af straffelovens bestemmelser om terrorisme eller bestemmelserne om trusler og chikane vedrørende offentligt ansatte.

3. Jeg har noteret mig, at Rigspolitiet har oplyst, at der kan være legitime formål med anvendelsen af hjemmesider og apps, som kan ændre visningen af et telefonnummer. Hvis "spoofing" derimod bruges som middel til at begå kriminalitet, f.eks. bedrageri, vil det kunne straffes efter de relevante bestemmelser i straffeloven.

Jeg har endvidere noteret mig, at Rigspolitiet har oplyst, at politiets Landsdækkende Center for IT-relateret økonomisk Kriminalitet løbende har forbyggende indsatser vedrørende "spoofing", hvor politiet bl.a. rådgiver borgere og indgår i relevante samarbejdsfora.

Jeg er derfor tilfreds med, at der allerede er taget en række initiativer til at bekæmpe denne type svindel, og at Rigspolitiet løbende følger området.