2023-05-15

Justitiedepartementet
Finansdepartementet
103 33 Stockholm
fi.registrator@regeringskansliet.se
ju.registrator@regeringskansliet.se

Hemställan

Svenska Bankföreningen hemställer om att det tas fram reglering i syfte att motverka och försvåra så kallad spoofing av telefonnummer för samtal och sms för att minska antalet telefonbedrägerier. Regleringen bör rikta sig till teleoperatörer verksamma i Sverige.

Inledning och bakgrund

Brottsvinsterna från bedrägerier har ökat med 38 procent på två år, enligt Polisen (från 4,2 miljarder kronor 2020 till 5,8 miljarder kronor 2022). Denna dystra utveckling kan förklaras av att bedrägerier med inslag av social manipulering, exempelvis telefonbedrägerier, har ökat markant.

Kortbedrägerierna har däremot blivit färre. Det är ett resultat av de politiska krav som införts genom det andra betaltjänstdirektivet (PSD2) på att e-handeln i större utsträckning ska använda bankens säkerhetslösningar. En konsekvens av dessa ökade autentiseringskrav för e-handeln är att brottsligheten drivits mot tillvägagångssätt med större inslag av social manipulering, genom exempelvis telefonbedrägerier, som på senare år har ökat kraftigt. Brottsutvecklingen är liknande i andra europeiska länder. Brottsligheten har på så sätt blivit mer riktad mot individen och därmed mer personlig. Konsumenter och företag har blivit mer utsatta för brottslighet i form av bedrägerier som får större konsekvenser för dem, vilket även påverkar bankerna.

Historiskt sett har bankerna haft förmåga att kunna parera bedrägeribrott, men digitaliseringen i samhället och det andra betaltjänstdirektivet (PSD2) har förändrat förutsättningarna. Bedömningen är att telefonbedrägerier påverkar förtroendet negativt för både bankerna och samhället i betydligt högre utsträckning än

Besök (Visit):
Blasieholmsgatan 4B
Stockholm
Sverige (Sweden)

Post:
Box 7603
SE-103 94 Stockholm
Sverige (Sweden)

t: +46 (0)8 453 44 00

e: info@swedishbankers.se
www.swedishbankers.se

kortbedrägerier. Äldre personer är extra utsatta för telefonbedrägerier, där medelåldern för brottsoffren är 80 år, enligt Polisen.

Digitaliseringen har förändrat hotbilden och då behöver de förebyggande åtgärderna anpassas. För telefonbedrägerier ligger flera viktiga motåtgärder utanför bankernas kontroll.

Tillvägagångssätt vid telefonbedrägerier

Tillvägagångssätt vid telefonbedrägerier är att en konsument blir uppringd av en bedragare med spoofat (maskerat) nummer och under telefonsamtalet blir lurad att antingen lämna ifrån sig koder från sin säkerhetsdosa eller att identifiera sig och signera uppdrag med sin e-legitimation. I det senare fallet luras kunderna att själva utföra transaktionerna, exempelvis under förevändning att pengar behöver skickas till ett ”säkert konto”.

Telefonbedrägerier kan också inledas med ett falskt sms och avsändaren av meddelandet kan se ut att komma från banken, annat företag eller myndighet. Innehållet i falska sms kan till exempel handla om misstänkta ”transaktioner på ditt kort och konto” eller ”händelser med ditt BankID”. Bedragarnas avsikt är att skapa en stressad situation där kunden måste agera snabbt. Ofta uppmanas kunden att klicka på en länk som leder till en falsk hemsida eller att kunden ska ringa upp ett angivet nummer som i själva verket går till bedragarna.

Från bedragarens perspektiv kan ett tillvägagagångssätt se ut så här:

- Bedragare registrerar falska webbsidor som ser ut att vara från ”banken”. Tjänsten ”phishing as a service”, säljer metoden på forum eller handelsplatser på Darknet (det icke-indexerade internet).
- Bedragare använder ofta ”typosquatting” som renommé-snyltar på den äkta hemsidan (man vänder på enstaka bokstäver för att efterlikna bankens hemsida).
- Bedragare använder ofta ”spoofat” telefonnummer i SMS-utskick (samma som den riktiga banken använder).
- Bedragare upprättar falsk infrastruktur i mitten av veckan och startar den falska webbsidan under fredag eftermiddag; ofta är det mer aktivitet runt lönehelger.

Vad gör bankerna?

Telefonbedrägerier är ett exempel på att hotbilden blir alltmer komplex och att kombinerande tillvägagångssätt används i samma brottsupplägg.

För att motverka detta anpassar bankerna de tekniska verktygen som letar efter falska webbsidor innehållande information kring bankens varumärke, företagsnamn med mera. Bankerna analyserar också tekniken bakom de falska webbsidorna, anpassar sin transaktionsövervakning och stänger ned de falska webbsidorna. Bankerna följer hela tiden bedragarna för att identifiera om dessa byter teknik i sitt utförande, med tillhörande justering av transaktionsövervakningen.

Vad behöver göras ytterligare?

Det finns ett antal komponenter som möjliggör telefonbedrägerier och samtliga delar i tillvägagångssättet presenteras nedan. Eftersom delarna i sig förenklar upplägg genom tillgänglighet till uppgifter och brister i skydd kan de var för sig adresseras genom olika infrastruktur- och lagstiftningsåtgärder.

Denna framställning handlar enbart om punkt 2 nedan, men samtliga modus-delar återges för orientering.

1. Mycket information om oss medborgare publiceras på internet med stöd av utgivningsbevis. Bedragare använder den informationen för att till exempel kartlägga ensamstående äldre med god ekonomi.

2. **Bedragare är skickliga på att framstå som att det är banken som kontaktar kunden genom att gömma sig bakom så kallade ”spoofade” telefonnummer vid samtal och sms. Spoofing är när någon maskerar sin nummerpresentation så att det ser ut att komma från ett annat nummer, exempelvis banken.**

3. Kontrollmöjligheterna mot utfärdarna av ID-handlingar är begränsade för banken. Om bankerna får bättre möjligheter att kontrollera id-handlingar på bankkontor och på distans stärks säkerheten i Sverige och antalet obehöriga transaktioner kan minska.

4. Begränsningarna i informationsutbytet påverkar konsumentskyddet negativt. Det är enkelt för kriminella att dela information, men svårt för samhällets goda krafter att dela information. Om lagstiftningen skulle tillåta mer datadelning med syftet att motverka bedrägerier mellan aktörer i samhället skulle det bidra till bättre riskbedömningar i både det preventiva arbetet och i bankernas monitorering.

Eftersom maskering av telefonnummer är en integrerad del av bedragarnas modus för telefonbedrägerier bör Post- och Telestyrelsen se till att teleoperatörer verksamma i Sverige gör mer för att skydda sina kunder från bedrägliga samtal och falska sms.

Att försvåra spoofing av telefonnummer och sms är en effektiv metod som stör bedragarnas möjligheter att agera mot nya bedrägerioffer. En reglering mot spoofing som riktar sig till de svenska telefonoperatörerna skulle avsevärt störa bedragarnas verksamhet.

Trots att Sverige sedan 2019 har en spärrlista för specifika telefonnummer som inte ska kunna spoofas förekommer fortfarande spoofade telefonnummer vid telefonbedrägerier. Förklaringen till det är att nummer ofta byts ut och att användningen av virtuella nummer har ökat samt att spärrlistan idag endast omfattar röstsamtal men inte SMS.

Som en del i att vända utvecklingen av telefonbedrägerier, där spoofade samtal är en komponent i tillvägagångssättet beskrivet ovan, bör det tas fram reglering som motverkar och försvårar detta. Det kan vara lämpligt att Post- och Telestyrelsen genom föreskrifter implementerar en anti-spoofing-infrastruktur för telefon och sms.

Föreskrifterna bör rikta sig till teleoperatörer verksamma i Sverige. Syftet med regleringen skulle vara att försvåra och helst omöjliggöra maskering av telefonnummer och sms. En sådan typ av reglering finns redan för telefon i Finland och de planerar en liknande reglering för sms (se bilaga).

Teleoperatörer bör även utveckla och implementera funktionalitet för att identifiera misstänkt innehåll på samma sätt som e-postleverantörer har satt upp lösningar för att upptäcka potentiellt skadligt innehåll.

Om telefonnummerserier hyrs ut till underleverantörer behöver kontroller finnas, liknande bankens kundkännedom.

Slutligen bör inte online-telekataloger verksamma i Sverige innehålla overifierade telefonnummer till företag, myndigheter och andra verksamheter.

Något om brottsvinsterna

Baserat på finska brottsanmälningar förlorade finländarna cirka 75 miljoner kronor (7,1 miljoner euro) till följd av bedrägerisamtal 2020–2021.

Även om en exakt jämförelse mellan Finland och Sverige är svår att göra indikerar ändå antalet brottsanmälningar i Sverige och storleken på brottsvinsterna från specifikt telefonbedrägerier (som var 157 miljoner kronor 2020, 340 miljoner kronor 2021 och 620 miljoner kronor 2022 i Sverige) att brottsvinsterna i Sverige under samma period vida överstiger de i Finland.

Bild 1: Antal polisanmälda telefon-, romans- och investeringsbedrägerier i Sverige 2019–2022.

	2019	2020	2021	2022
Telefonbedrägeri	5 285	7 026	11 582	21 582
Romansbedrägeri	917	1 024	1 143	1 311
Investeringsbedrägeri	1 610	1 622	1 800	2 535

Källa: Polismyndigheten.

Bild 2: Brottsvinsterna för bedrägeribrottsligheten 2020–2022.

	Total brottsvinst						Variation
	2022	%	2021	%	2020	%	2022-2021
Romansbedrägeri	609 467 976	10%	395 003 655	9%	350 136 570	8%	54%
Investeringsbedrägeri	1 239 495 438	21%	759 269 120	16%	872 472 787	21%	63%
BEC–bedrägeri	236 871 054	4%	386 298 329	8%	207 482 772	5%	-39%
Vishing–bedrägeri	619 361 382	11%	339 187 827	7%	156 674 932	4%	83%
Annonsbedrägeri	180 475 344	3%	123 650 319	3%	123 596 493	3%	46%
Identitetsbedrägeri–köp	93 709 728	2%	139 785 840	3%	63 529 102	2%	-33%
Identitetsbedrägeri–lån	413 646 618	7%	457 506 029	10%	494 199 992	12%	-10%
Identitetsbedrägeri–övrig	313 124 088	5%	130 657 373	3%	100 589 417	2%	140%
Faktura med kontakt	102 872 222	2%	113 224 487	2%	72 515 411	2%	-9%
Faktura utan kontakt	7 633 076	0,1%	40 027 291	1%	85 429 380	2%	-81%
CP–bedrägeri	63 963 042	1%	62 598 390	1%	121 633 744	3%	2%
CNP–bedrägeri	252 663 516	4%	229 288 035	5%	238 768 460	6%	10%
Försäkringsbedrägeri	15 243 040	0,3%	24 274 517	1%	15 614 676	0,4%	-37%
Snyltningsbrott	6 879 600	0,1%	6 067 044	0,1%	4 090 042	0,1%	13%
Grov fordringsbedrägeri	128 534 212	2%	65 270 633	1%	675 000	0,02%	97%
Övrig bedrägeri	1 545 946 142	27%	1 342 854 714	29%	1 314 831 011	31%	15%
Totalt	**5 829 886 478**	100%	**4 614 963 602**	100%	**4 222 239 789**	100%	26%

Källa: Polismyndigheten, *Brottsvinsterna för bedrägeribrottsligheten 2022*, 2023-04-21, diarienr. A232.846/2023, sid. 7.

Inför finska spärr- och blockeringsregler i Sverige

De spärr- och blockeringsåtgärder som infördes i den finska föreskriften från maj 2022 antas ha försvårat telefonbedrägerier, minskat medborgarnas risk att bli offer för ett brott och minskat de kriminellas brottsvinster.

Om en sådan reglering skulle införas i Sverige skulle den medföra både engångskostnader och driftskostnader för teleoperatörerna. Det kan noteras att den finländska motsvarigheten till PTS (Transport- och kommunikationsverket Traficom) inte bedömde att kostnaderna för de finska teleoperatörerna var oskäliga när regleringen infördes i Finland. Kostnaderna och implementeringskomplexiteten torde vara liknande för teleoperatörer verksamma i Sverige.

Med anledning av att telefonbedrägerier ökar i allt snabbare takt bör det ligga i allas intresse att bryta denna negativa utveckling. Bankföreningen ser därför starka behov av att lagstiftningsförändringar och andra nödvändiga åtgärder inom området vidtas omgående.

Bankföreningen hemställer att det tas fram reglering i syfte att motverka och försvåra så kallad spoofing av telefonnummer för samtal och sms för att minska antalet telefonbedrägerier. Regleringen bör rikta sig till teleoperatörer verksamma i Sverige.

SVENSKA BANKFÖRENINGEN

Hans Lindberg

Bilaga:
Transport och kommunikationsverket: *Föreskrift 28 om interoperabilitet av kommunikationsnät och kommunikationstjänster*
https://www.traficom.fi/sv/search?limit=20&offset=0&query=F%C3%B6reskrift%2028%20om%20interoperabilitet%20av%20kommunikationsn%C3%A4t%20och%20kommunikationstj%C3%A4nster&toggle=F%C3%B6reskrift%2028%20om%20interoperabilitet%20av%20kommunikationsn%C3%A4t%20och%20kommunikationstj%C3%A4nster