

Uppdrag till PTS att motverka tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier

Nummerforum , 17 oktober 2024

Stor uppmärksamhet i media

Polisen varnar för spoofing

Äldre kvinna lurad av telefonbedragare
100 000 kronor

Efter upprepade

bedrägeriförsök – nu g

**Falskt VMA utskick
Strängnäs**

Äldre paret lurades på 1,8 miljoner av
telefonbedragare

Banken varnar
närområdet: "F

Post- och telestyrelsen



geric
2023 var rekordår för
telefonbedrägerier

telefonbedragare har lurat till
sig 225 miljoner

ökning av bedrägerier mot
årt att komma åt

retagare på Orust utsattes
spoofing

ör telefonbedrägeri –
a dig inte med bank-id

ri i **Kraftig ökning av
telefonbedrägerier – upp 132
procent på ett halvår**

PTS arbete

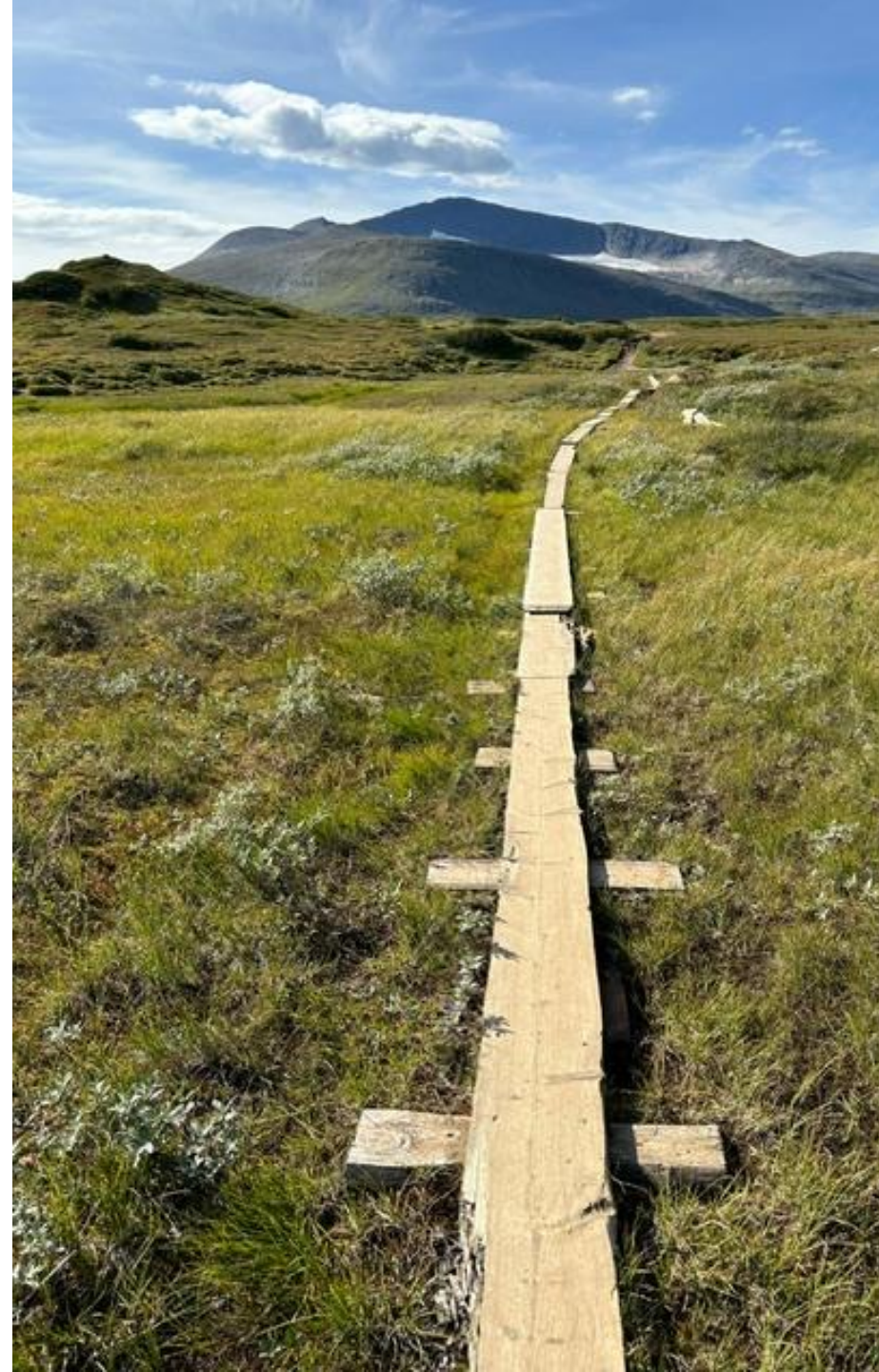
Vad gör PTS inom området

Det här har vi gjort

- Vägledning för tillhandahållare
- Nya föreskrifter mot spoofing
- Delrapport av regeringsuppdraget

Det här pågår

- Slutrapport av regeringsuppdraget
- Internationell utblick



Föreskrifter och allmänna råd för att förhindra samtal med manipulerade anropande telefonnummer (16 september)

Vad är problemet?

- Vid telefonbedrägerier används ofta manipulerade nummer
- För mottagaren kan det se ut som att samtalet kommer från någon annan än det faktiskt gör t.ex. från banken
- Syftet är att vilseleda mottagaren att logga in på sin bank eller lämna ut kortuppgifter

Föreskrifterna

- Föreskrifterna bygger på vägledningen som tidigare tagits fram
- Utgår från att svenska nummer ska användas i Sverige
- Kontroll ska göras för att säkerställa att det originerande samtalet kommer från ett nummer som är tilldelat en tillhandahållare
- Samtal från svenska nummer som kommer in från utlandet ska som huvudregel spärras
 - För mobilnummer måste kontroll göras om abonnenten befinner sig utomlands (roamar)
- Möjlighet till speciella lösningar för t.ex. call centers i utlandet

Föreskrifterna

Ikraftträdande:

- 4 november 2024 (Fast telefoni)
- 3 mars 2025 (Mobilt)



Regeringsuppdrag –

Att motverka tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier

Regeringsuppdraget

Kartläggning

Kartlägga och redovisa användningen av elektroniska kommunikationstjänster vid bedrägerier

Analys – bef. föreskriftsrätt

Analysera PTS bef. föreskriftsrätt för att motverka dessa bedrägerityper

Internationell utblick

Beakta int. utvecklingen användning av elektroniska kommunikationer vid bedrägerier, andra länders åtgärder, t.ex. stöd och nya regelverk

Föreslå åtgärder

Föreslå åtgärder för att motverka bedrägerityperna i Sverige, inkl. nödvändiga författningsförslag

Redovisa konsekvenser av föreslagna åtgärder

Redovisa konsekvenser, inkl. kostnadsuppskattningar och förslag till finansiering av åtgärdsförslagen

Redovisa effektiviteten av föreslagna åtgärder

Redovisning av åtgärdsförslagets kostnadseffektivitet och samhällsekonomiska effektivitet

Verka för informations spridning

Se till att information om bedrägerityper i Sverige och åtgärder som kan vidtas sprids till allmänheten



Post- och telestyrelsen

Regeringen
2023-12-14
P2023/02206

Finansdepartementet
I N K O M
PTS
2023-12-21
Aktörlista
Dnr:

Post- och telestyrelsen
Box 610
102 32 Stockholm

Uppdrag till Post- och telestyrelsen att motverka tillvägagångsätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier.

Regeringens beslut
Regeringen ger Post- och telestyrelsen (PTS) i uppdrag att lämna förslag till åtgärder för att förhindra missbruk av telefonnummer, s.k. spoofing, och andra tillvägagångsätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier.

PTS ska, utifrån myndighetens kunskap och ansvar inom området för elektronisk kommunikation,

- kartlägga och redovisa användningen av elektroniska kommunikationstjänster vid bedrägerier, t.ex. i form av spoofing och SMS-bedrägerier,
- analysera om myndighetens befintliga föreskriftsrätt möjliggör för den att meddela föreskrifter för att motverka sådana bedrägerier,
- lämna förslag till åtgärder för att motverka identifierade problem, t.ex. i form av nödvändiga författningsförslag, och

Exemplifierade aktörer i uppdraget vi ska inhämta synpunkter ifrån

Polisen | TechSverige

Svenska Bankföreningen
Swedish Bankers Association

Konsumentverket · KO

Andra NRA:er/andra länder

Andra aktörer PTS ev. samverkar med

bra | TELEKOMRÅDGIVARNA | SVERIGES KONSUMENTER

Ekobrottsmyndigheten | MSE | Myndigheten för samhällsskydd och beredskap | BankID

INTERNET STIFTELSEN | SKPF: pensionärerna

Digitalidag | Leissner Data | Teknikföretagen

elegitimation.se | Om ditt digitala id-kort | BROTTSOFFER JOURNEN | PRO

Brottsförebyggande Myndigheten | HANDISAM

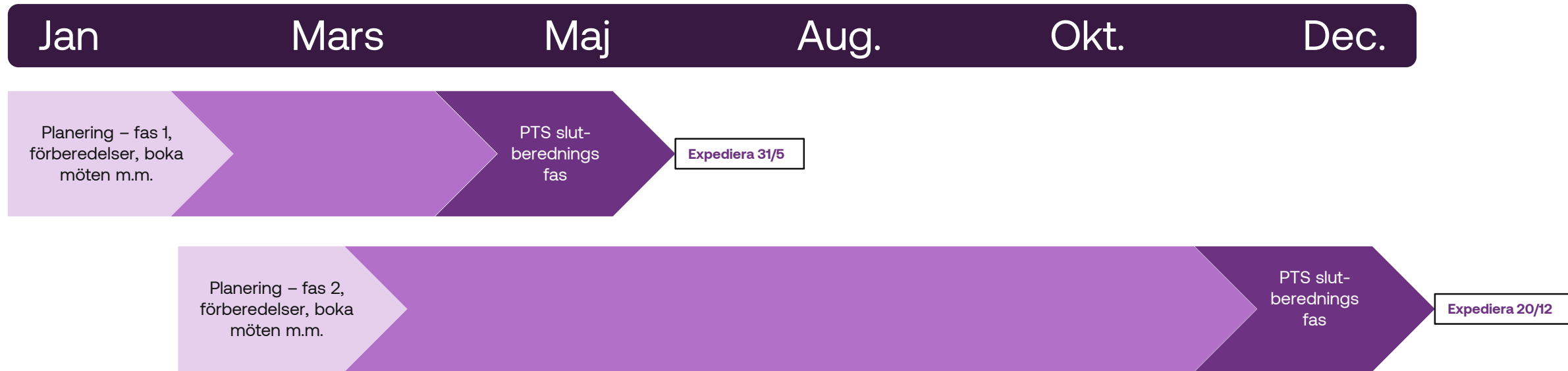
SVERIGES KONSUMENTER | Skatteverket | SENIORERNA | SH Svensk Handel

EUROPOL | INTERPOL | FRA

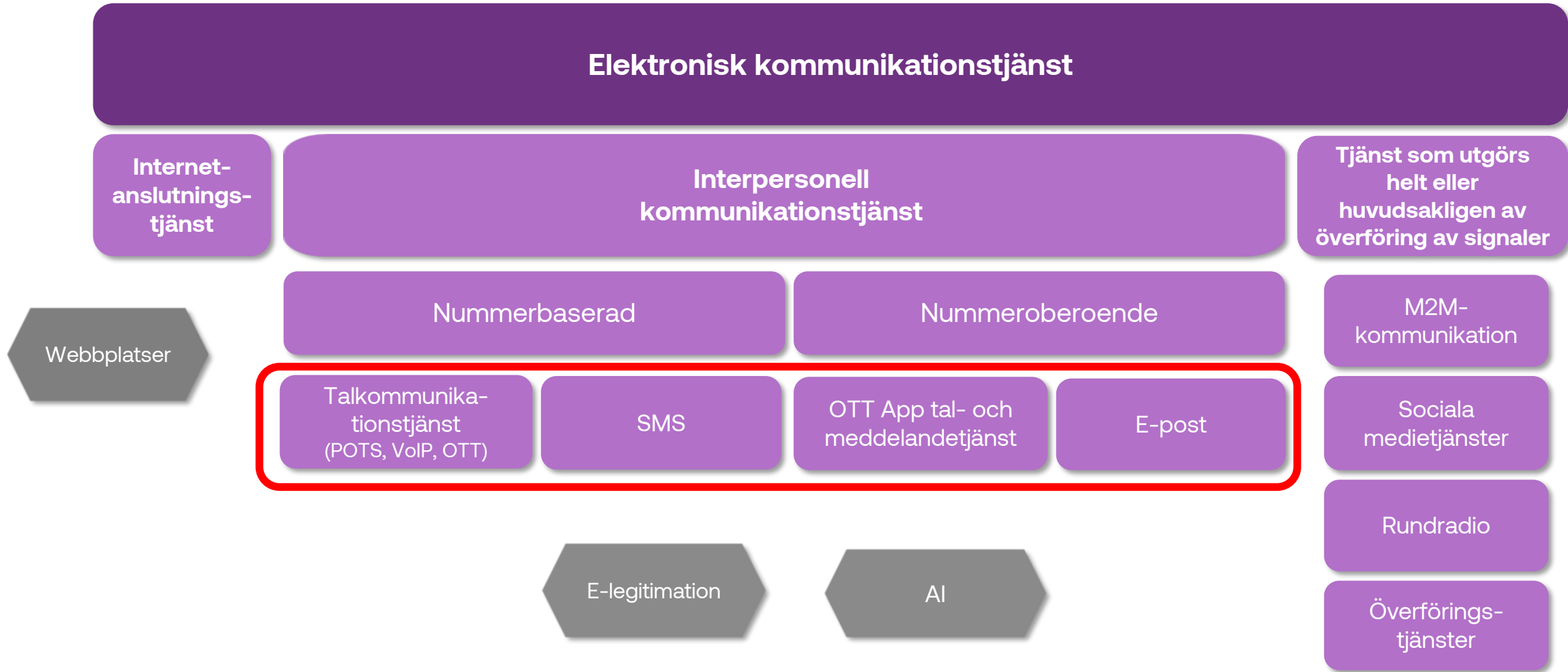
BRANSCH-ORGANISATIONEN MORGAN | GSMA | CFCA | enisa

Operatörer/aggregatörer
OTT-aktörer i Sverige

Tidplanen som styr uppdraget – med PTS hålltider



Elektroniska kommunikationstjänster – ett brett område

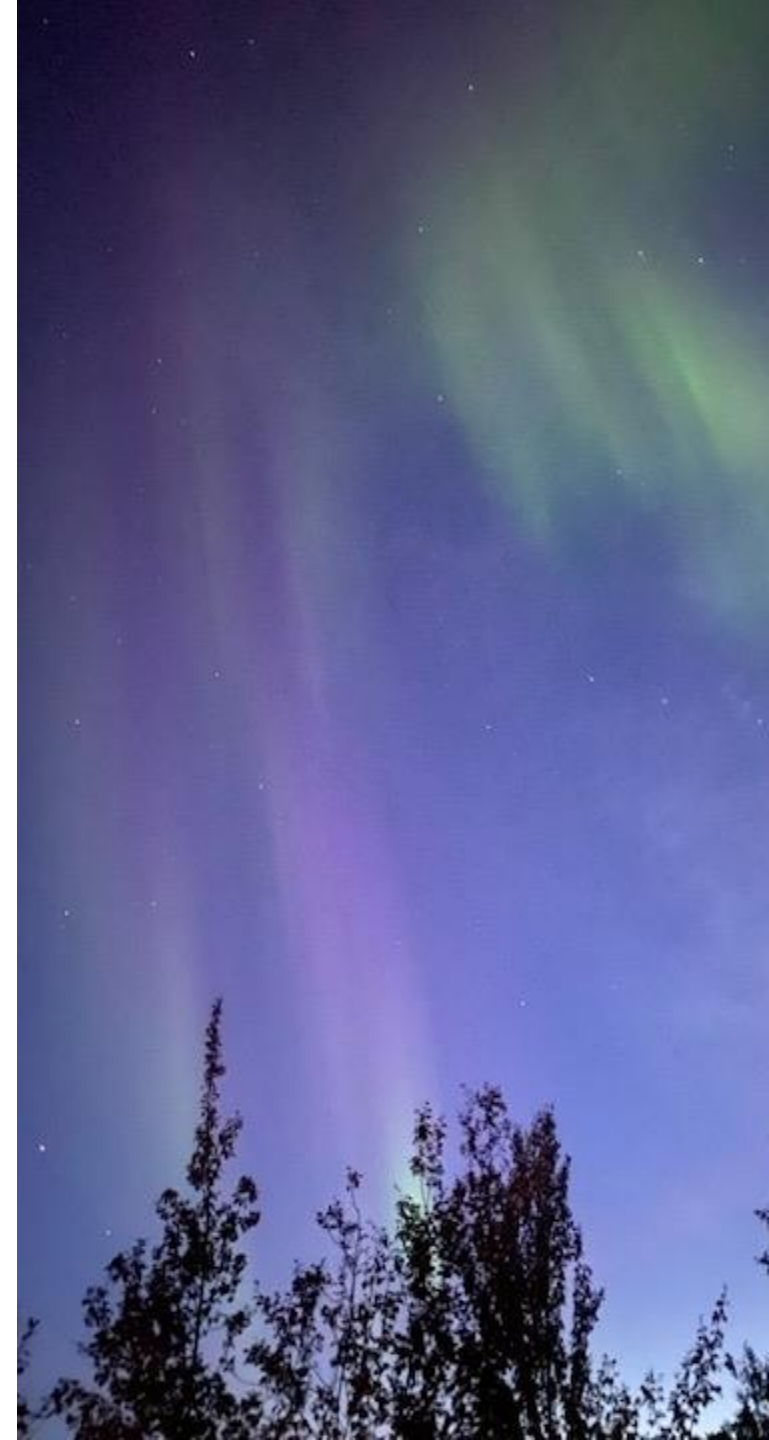


Övergripande slutsatser vid delredovisningen

- Telefonsamtal, sms och e-post är vanligast förekommande elektroniska kommunikationstjänster som används i samband med bedrägerier
- Även e-legitimation, sociala medietjänster och falska webbplatser används i samband med bedrägerier
- Personlig information som finns tillgänglig publikt på internet är ett problem då bedragare utnyttjar det vid kartläggning av brottsoffer
- Problem med bedrägerier via nummeroberoende OTT-tjänster ökar
- Användning av AI som ett verktyg i samband med bedrägerier ökar
- Informationsspridning om bedrägerier och hur slutanvändare skyddar sig kan behöva samordnas.

Andra iakttagelser/fortsatt arbete

- Teknikutvecklingen är positiv men kan ha en baksida
- Snabbrörligt – när en dörr stängs så öppnas en annan
- Sms i fokus
- Skydd mot bedrägerier vs personlig integritet
- AI både som bov och sheriff



Vad görs internationellt?

Vad görs i andra länder?

Norden

- **NaN2** – Europeisk arbetsgrupp inom CEPT som bl.a. arbetar med bedrägerifrågor
- **Norge** – tillåtet att skanna/läsa sms för att hitta länkar. Man har samlat operatörer, banker, polis för att gemensamt lösa problemen. Proxylösning på plats i höst. Mycket på frivillig basis.
- **Danmark** – håller på att ta fram lösning för registrering av SenderID, lagstiftning saknas för detta.
- **Finland** – reglering finns på plats för samtal och sms. Trots det fortsätter bedrägerier att ske.

Vad andra länder gör Europa

- **Belgien** – tillåtet att skanna/läsa sms för att hitta bedrägligt innehåll. Det finns undantag för detta i lagstiftningen. Till lagstiftaren har man påpekat att detta är enda sättet att stoppa bedrägerierna likt filtrering av e-post.
- **Nederländerna** – har infört DNO-listor på frivillig basis, ungefär samma lösning som svenska operatörer har infört.
- **Irland** – har infört DNO-listor för banker m.m.

DNO: Do Not Originate

Vad görs i andra länder?

Övriga länder

- **Singapore** – delat ansvar bank/telekomföretag. Operatörer tvingas lämna statistik om blockerade samtal. Registrering av SMS Sender ID tvingande.
- **Indien** – har lösning med central proxy för samtal.
- **USA** – kan bötfälla bolag som genererar robocalls. Databas för nummer som operatörer kan göra uppslag mot. Dåliga aktörer kan förbjudas. STIR/SHAKEN inte haft önskad effekt.
- **Japan** – har drabbats hårt med en åldrande befolkning. Minskat bedrägerierna med 97%, dock med stora intrång i den personliga integriteten.