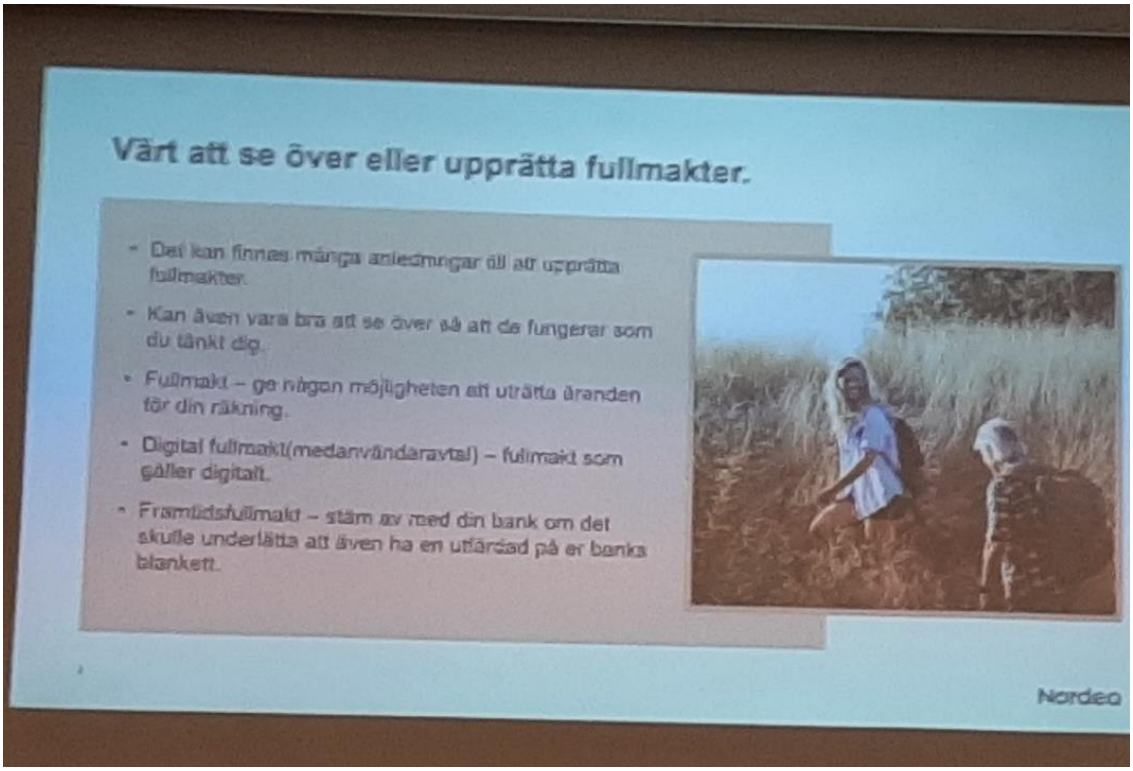
Öppen träff om säkerhet på nätet 12 september 2024

”Trygg i din digitala vardag” var rubriken på dagens träff och många samlades för att ta del av den viktiga informationen.

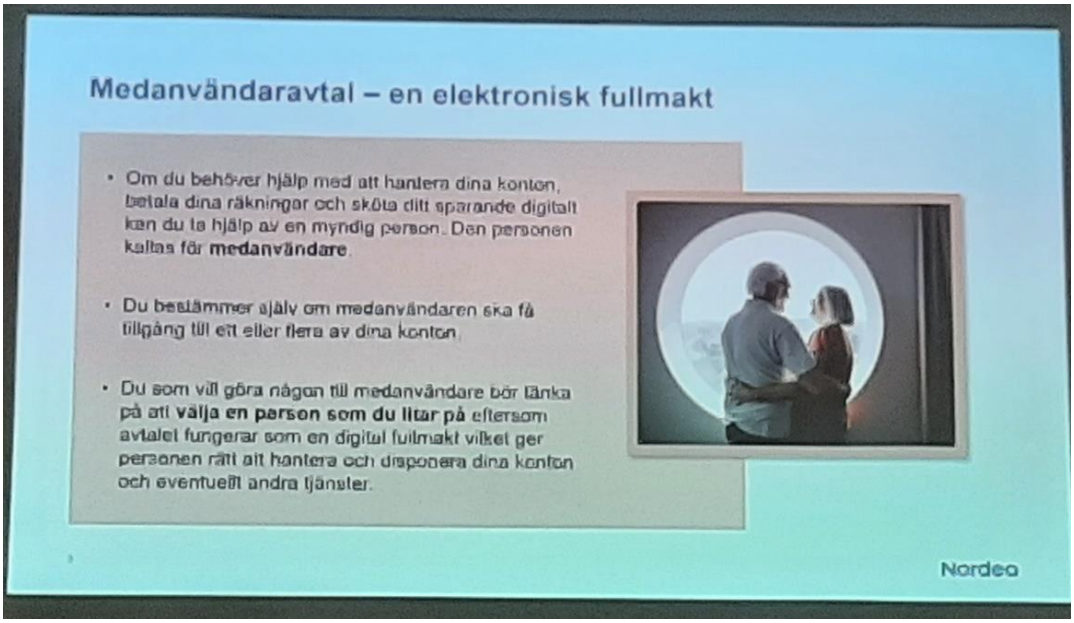
Fredrik Almberger från Nordea hade tagit med sig Nordeas säkerhetsexpert Amalia Krantz för att ge oss matnyttiga tips.

Men Fredrik ville passa på tillfället att uppmana oss att se över våra fullmakter.



De olika bankerna har sina egna blanketter.

Ofta krävs det att man använder dessa för att det ska fungera smidigt och för att man inte ska behöva komma in på banken personligen varje gång.

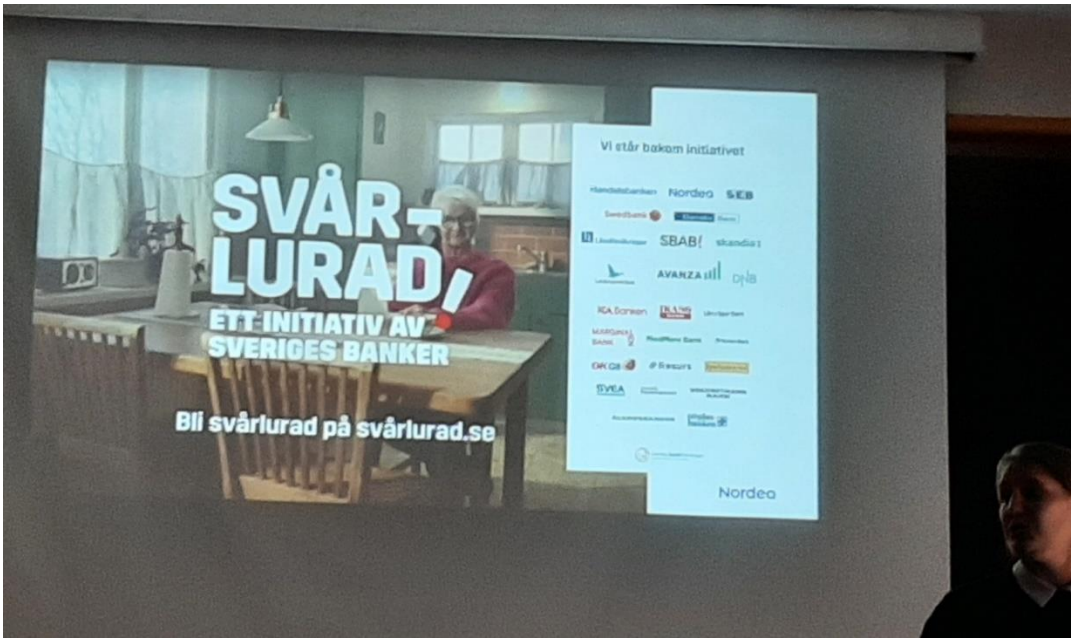


Ett s.k. medanvändatavtal kan vara praktiskt att upprätta, om du vill ge en betrodd anhörig möjlighet att hjälpa till att hantera dina konton på nätet.

Så kontakta din bank och prata igenom hur du vill ha det, var Fredriks budskap.

Så var det Amalias tur.

Med klar och tydlig röst klarade hon sig bra utan mikrofon.



Hon berättade om den hemsida som bankerna i samarbete har tagit fram: www.svårlurad.se

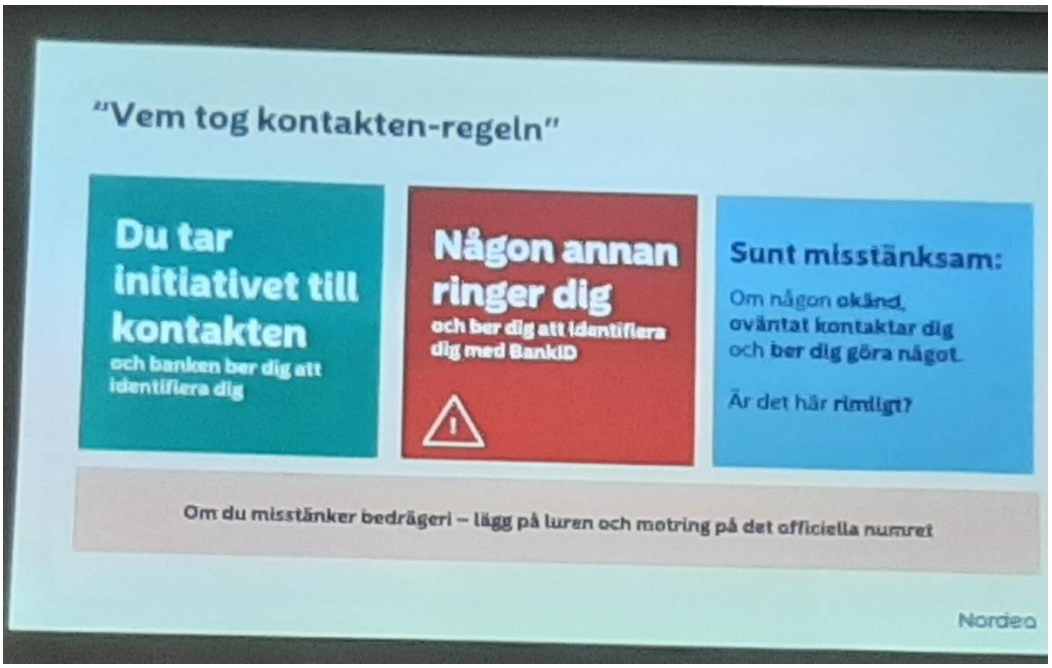
Där kan man i lugn och ro gå igenom många tips.

Amalia beskrev mobilt bankID som säkert, om man bara inte lämnar ut koden till någon annan.

BankID har blivit nästan omöjligt att klara sig utan i dagens samhälle.

Körkort är inte längre godtaget som resehandling inte ens i Europa.

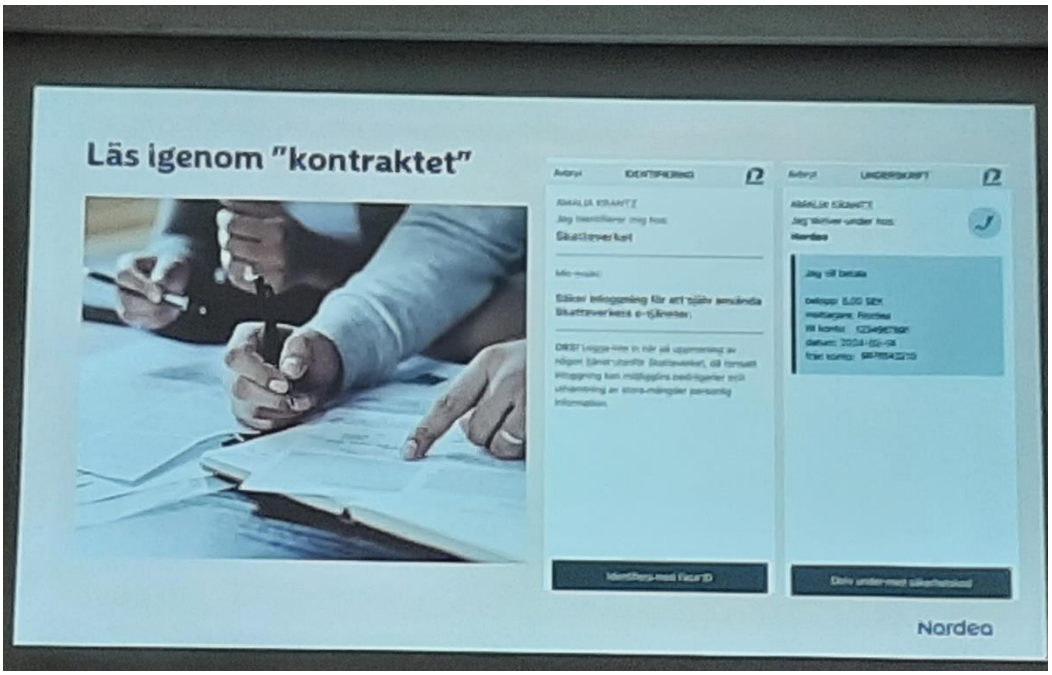
Man måste ha pass eller nationellt ID-kort vid resa.



Sen gick hon in på vad vi måste tänka på vid kontakter med främmande människor på telefon.

Man ska vara sunt misstänksam och inte dra sig för att lägga på luren om varningsklockorna ringer.

Motring gärna men inte till det nummer som de ringer utan till bankens/myndighetens officiella nummer.



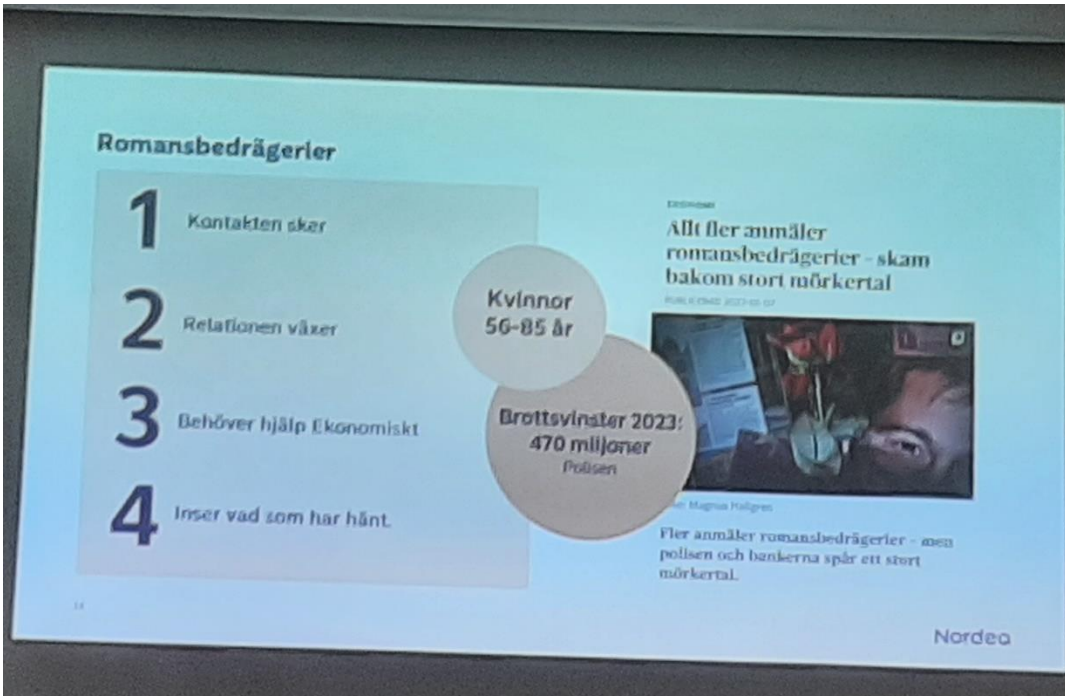
Innan man signerar en utbetalning med sitt bank-ID ska man kontrollera att man verkligen betalar till den man vill betala till.

Det står i klartext till höger på skärmen när man ska signera:

”Jag vill betala xxx kr till XXX.” Det ska stämma.

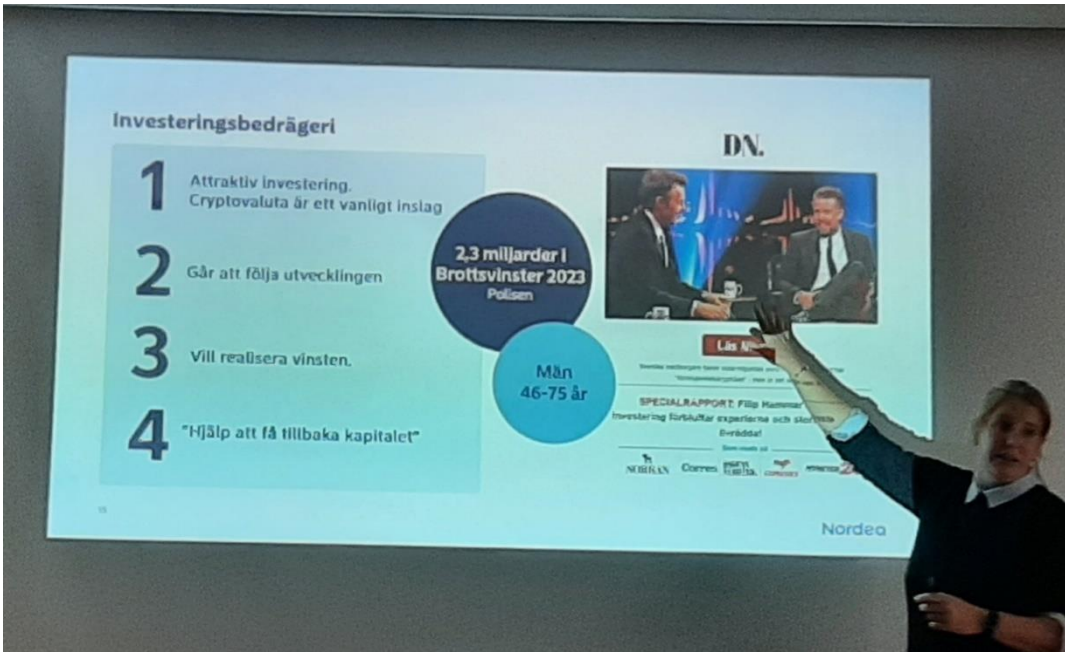
Bedrägerier visar verkligen upp skrämmande siffror.

Mångmiljardbelopp omsätts i den internationella ”bedrägeriindustrin” av cyniska utförare, som är snabba att anpassa sig till aktuella situationer för att lura så många som möjligt.



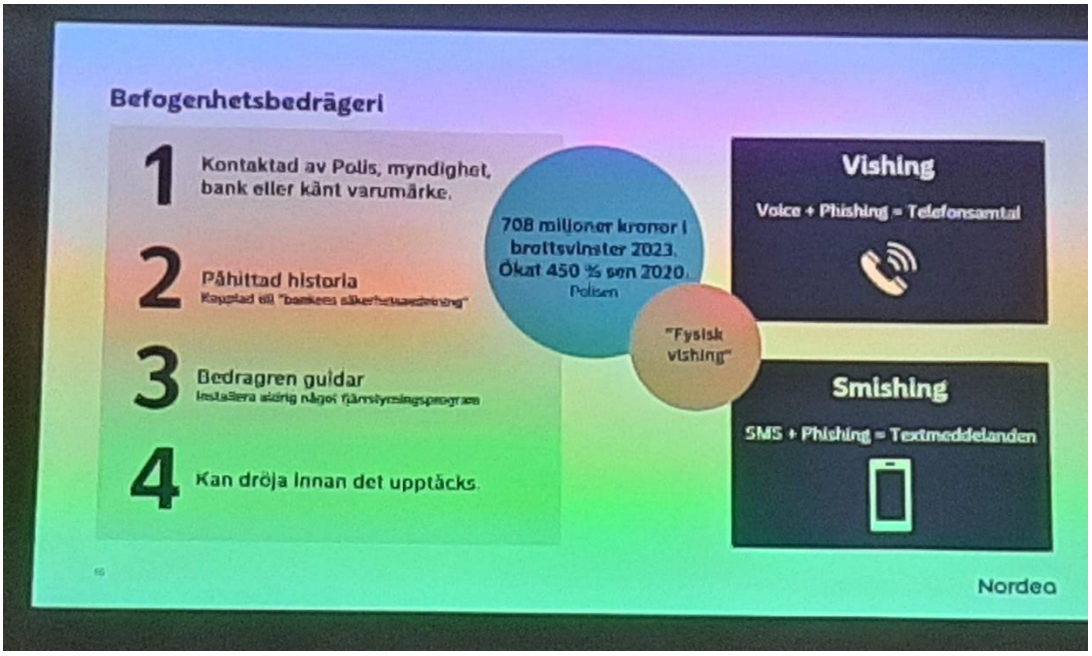
Det finns olika typer av bedrägerier.

Romansbedrägerierna är kanske extra kränkande, eftersom de inbegriper känslor och de orsakar mycket skam och skuld hos de drabbade.



Investeringsbedrägerierna använder sig skamlöst av kändisars namn och bilder för att inge förtroende.

Filip Hammar är en av dem som har blivit utnyttjade.

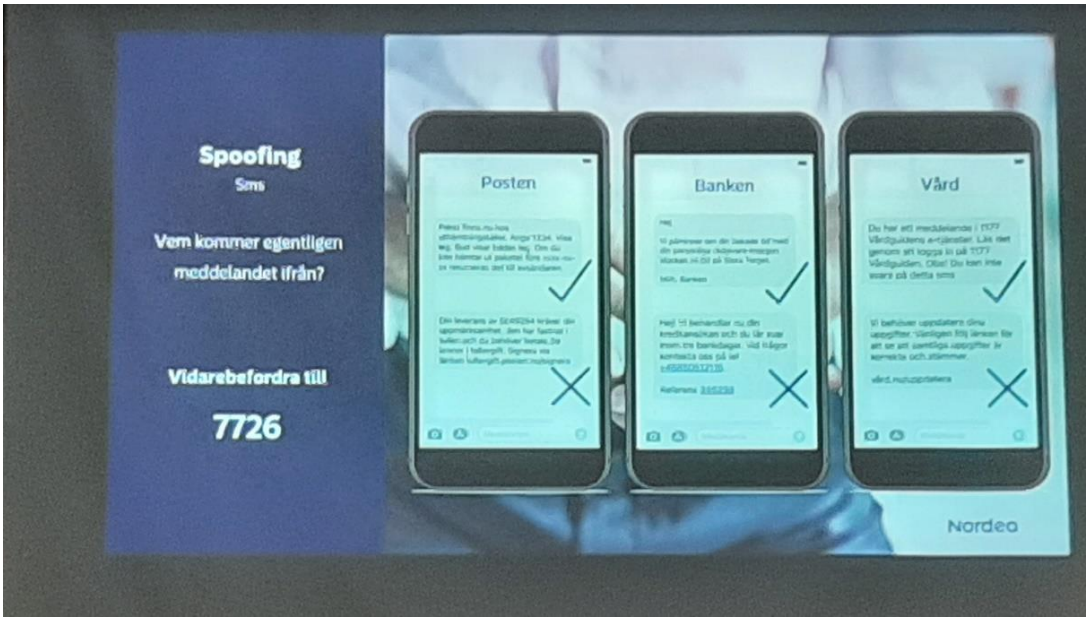


Befogenhetsbedrägerier är en tredje vanlig kategori.

Man använder sig av telefon, s.k. *Vishing* eller av SMS, s.k. *Smishing*.

Man utger sig för att representera en bank eller myndighet och vill ”hjälpa” personen i ett påhittat scenario.

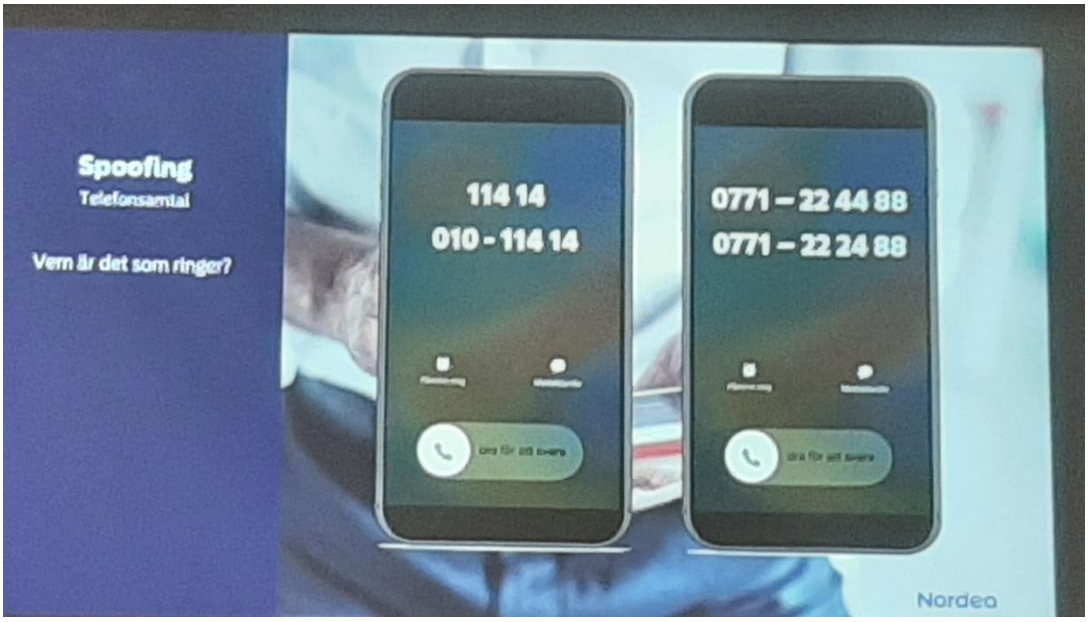
S.k.*fysisk vishing* blir det när någon efter telefonsamtal dyker upp hemma hos personen för att ”ta hand om” värdesaker.



Bedragarna kan också manipulera dig att tro på att meddelandet är äkta genom det som kallas ”*spoofing*”.

De är skickliga på att länka in ett SMS-meddelande i ett pågående legitimt ärende från t.ex. banken.

Svara inte, utan vidarebefordra sådana meddelanden till 7726 för att hjälpa polisen!



Vid telefonsamtal ändrar de en siffra i det riktiga telefonnumret, så att du kommer till dem i stället för banken.

Ändringen är ofta så subtil, så att man inte upptäcker den om man inte är uppmärksam.

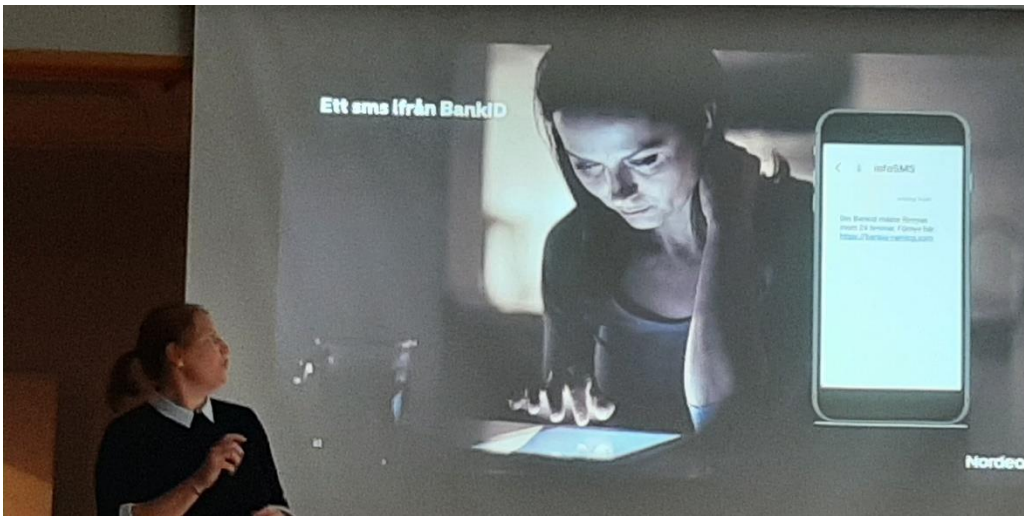
Här är två exempel.

Ett annat sätt att luras är att skicka ett SMS som verkar komma från ett barn eller barnbarn.

”Hej mormor, kan du hjälpa mig?”

”Är det du Lisa?” blir kanske en naturlig fråga.

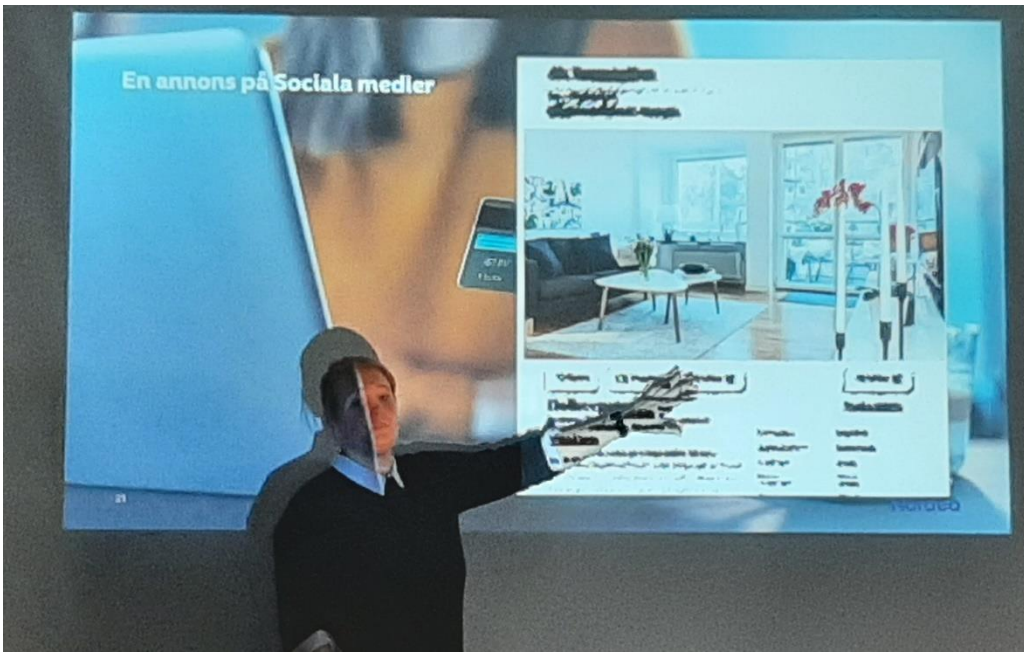
Då har bedragaren lurat in dig i en konversation, som går ut på att få dig att skicka över pengar för något ”behjärtansvärt” ändamål.



Andra bedrägerimetoder:

Man kan få ett SMS som verkar komma från bankID.

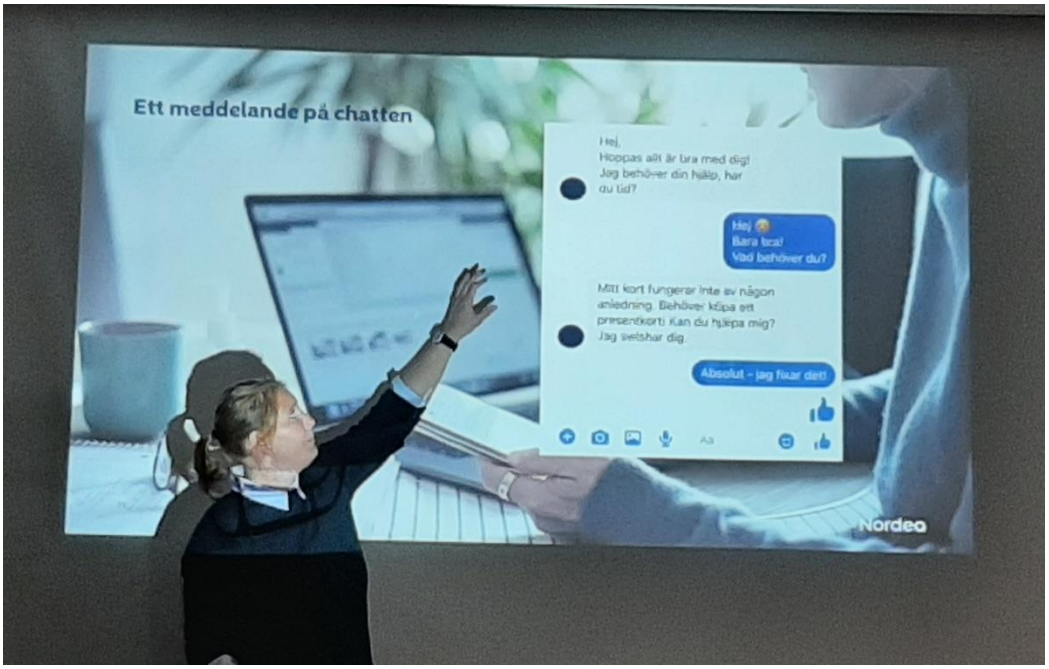
BankID ber dig **aldrig** att logga in, så varning, varning!



Eller man kan se en annons på sociala medier om en lägenhet som kan hyras eller köpas.

Ofta är det riktiga bilder från lägenheter som har funnits på nätet som nu utnyttjas.

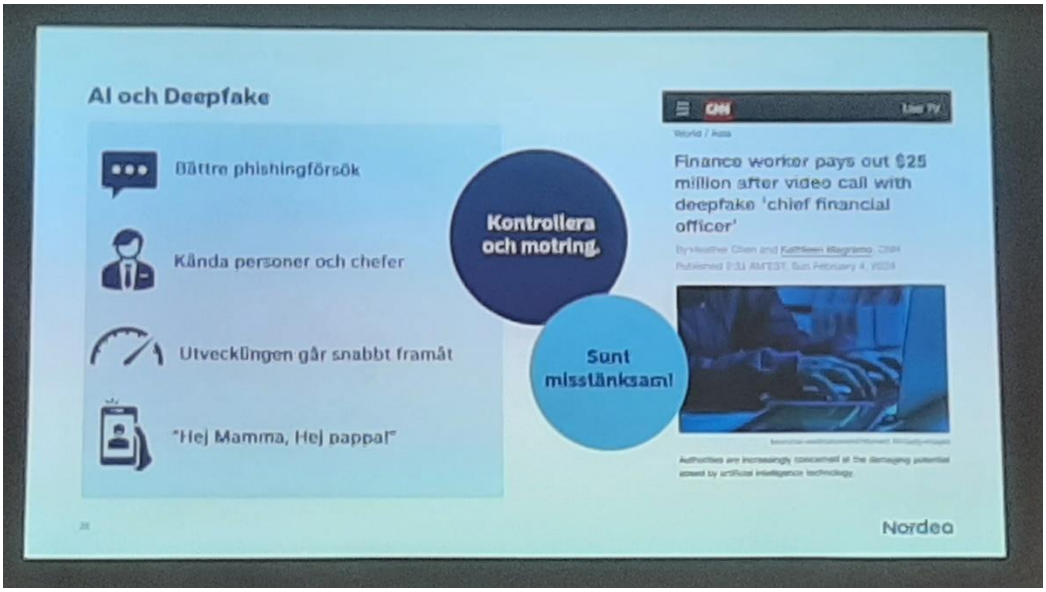
Det behövs bara en ”liten slant” för att du ska komma först i kön...



Även olika chatter används för att få kontakt och luras.

Kolla att du verkligen vet vem som ber dig om hjälp eller pengar.

Amalias budskap kokar ner till detta:
* Var sunt misstänksam!
* Kontrollera och motring!



Tyvärr kommer den nya tekniken med AI (Artificiell Intelligens) och s.k. deepfake, där man kan imitera inte bara utseende utan även röster, att göra det ännu svårare att hålla emot alla bedrägeriförsök.

Men är vi då helt utlämnade till bedragarna?

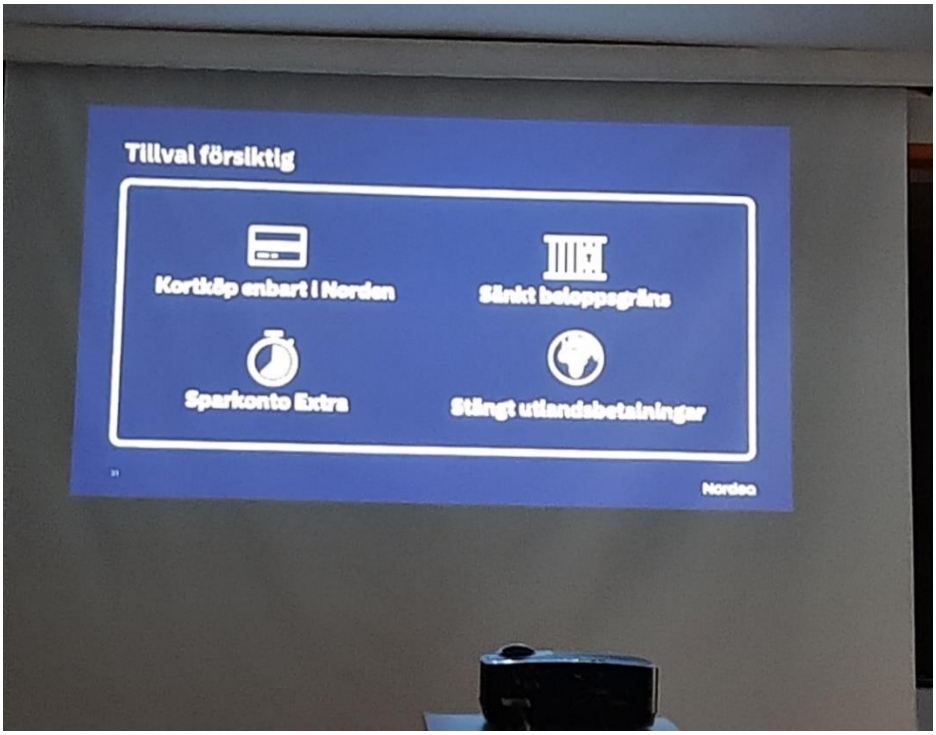
Vad gör bankerna för att skydda våra pengar?

Här pratade Amalia förstås bara för Nordea och vad de gör.

De har vidtagit en del åtgärder för att försvåra för bedragarna som t.ex. *beloppsgränser* för överföringar och *fördröjning* av överföringar.

Dessa åtgärder görs i samråd med bankkunderna.

Så kontakta din bank, om du vill ha någon av dessa spärrar.



Nordea har ett paket kallat *Tillval försiktig,* som innehåller flera av dessa spärråtgärder.

Amalia avrundade med att upprepa några av de kloka råd hon hade givit under den proffsiga och informativa genomgången.

Åhörarna var mycket engagerade och Amalia svarade beredvilligt på frågor.

En av frågorna var: Hur stor chans har man att få tillbaka pengar som man har blivit bedragen på?

Svaret: Det beror på hur aktiv man själv har varit.

Om man själv har loggat in med bankID kan det vara svårt..

Fredrik avslutade med att hänvisa till Nordeas hemsida för mer information: www.nordea.se/säkerhet

Där kan man läsa utförligt om alla de olika typerna av bedrägerier som Amalia berättade om och hur man ska försöka hindra dem.

Fredrik och Amalia avtackades med varma applåder och varsin chokladask för den värdefulla information som vi fick ta del av.

Låt oss hoppas att de har hjälpt till att undvika några bedrägerier bland våra åhörare!