Snacka om brott, avsnitt 49 – en podd från Brå

Bedrägerier mot privatpersoner (Oktober 2023)

Medverkande: Niklas Laninge, VD, Nordic Behaviour Group; Helena Wall, Head of Fraud Intelligence and Awareness, Nordea samt Lina Fjelkegård, projektledare, Brå.
Programledare: Monica Landergård, pressekreterare, Brå.

INLEDANDE CITAT, LINA:
Men just när det kommer till det här som vi pratade om nu bedrägeri genom social manipulation, eftersom det är individer som luras, så är det just sårbarheter kopplade till individen som blir, ja men de blir väldigt centrala. Och det vi såg i vår studie, eller det som lyfts fram där, är särskilt digital ovana och okunskap. Att man kanske inte riktigt har koll på det här med internetbank, BankID och hur det funkar, Swish, som gör att man helt enkelt blir lättare att lura.

MONICA: Bedrägeri är ett av de vanligaste brotten och många privatpersoner luras ofta på stora summor pengar. Med utgångspunkt i en studie som Brå publicerade i september 2023, ska vi bland annat prata om vad bedrägerier är och vilka typer av bedrägerier som är allvarligast, men också vilka sårbarheter som bedragarna utnyttjar. Vi ska diskutera hur bankerna arbetar för att förebygga bedrägerier och vilka utmaningar som kan finnas där. Vi ska också prata om begreppet nudging. Vad är det och hur skulle det kunna användas i det förebyggande arbetet mot bedrägerier? Jag säger hej och välkommen till Helena Wall som representerar banksektorn. Du är Head of Fraud Intelligence and Awareness vid Nordea.

HELENA: Hej!

MONICA: Och Niklas Laninge, du är VD på Nordic Behaviour Group.

NIKLAS: Hej hej!

MONICA: Och vi har också med oss Lina Fjelkegård, projektledare och en av författarna till Brås studie. Hej och välkommen säger jag till dig också, Lina.

LINA: Hej, hej!

MONICA: Och jag som leder samtalet heter Monica Landergård och är pressekreterare på Brå. Men Lina, jag börjar med att vända mig till dig. Kan du ge några exempel på vad bedrägerier kan handla om och vilka typer av bedrägerier som är allvarligast?

LINA: Ja, men jag kan ju börja med att säga att bedrägeri är ett brott som handlar om att en gärningsperson vilseleder eller lurar någon annan för att få ekonomisk vinning. Det är lite förenklat, men det är det det handlar om i grunden. Och som du sa inledningsvis nu Monica, så är det ett väldigt vanligt brott. 2022 hade vi 180 000 anmälda bedrägerier i Sverige och vi har också sett under hela 2000-talet att det är en brottstyp som ökat väldigt kraftigt. Om man tittar på anmälda brott så är kortbedrägerierna det som är allra vanligast, när man lurar någon att göra en, eller man använder någons kort för att genomföra en transaktion. Men om man tittar mer på vad det får för konsekvenser och hur allvarligt det är så är det kanske bedrägerier och social manipulation som man brukar lyfta fram som särskilt.

MONICA: Och vad är det, kan du beskriva social manipulation?

LINA: Mm, det är när bedragaren liksom bygger upp ett förtroende hos brottsoffret och använder det sedan för att lura den här personen att göra någonting. En transaktion eller att lura av den på uppgifter så att bedragaren kan göra en transaktion. Det är till exempel, om jag pratar om romansbedrägerier, där förtroendet handlar om en kärleksrelation eller investeringsbedrägerier, där man får någon att lita på att det här är en väldigt bra investering och satsa massa pengar på något som egentligen kanske inte överhuvudtaget finns. Och det som man hör mycket om i de så kallade telefonbedrägerierna, där en bedragare ringer upp och utger sig för att vara någon annan. En person från en bank eller myndighet och

sedan luras. Det kan vara sms också och få någon att ringa upp till banken och genom det då, ja, men lura någon att göra en transaktion eller lämna ifrån sig uppgifter. Och du frågade också om vad som var vad som var allvarligast. Det kan man säga att det som gör bedrägerier eller bedrägeri genom social manipulation allvarligt är väl också att det är där man verkligen går mot individen och manipulerar individen, så att man kan se utifrån brottsoffrets perspektiv så är det där man verkligen känner att man har blivit lurad. Många brottsoffer här känner sig oerhört dumma att man har låtit sig luras och känner skam. Skäms helt enkelt för det här. Och det är också i den här typen av grejer, som det är ganska stora summor pengar, så att brottsoffren drabbas ganska hårt och ekonomiskt.

MONICA: Vet vi hur många av de som drabbas av bedrägeri som faktiskt anmäler. Har vi någon uppgift om mörkertalet där?

LINA: Nej.

MONICA: Nej.

LINA: Nej, det har vi inte. Sen kan man ju anta att just bedrägeri genom social manipulation, eftersom det är en typ där man kanske skäms mer, att mörkertalet är större där. Men samtidigt så är det större summor, vilket ju annars brukar leda till en ökad anmälningsbenägenhet. Men vi har inte tittat på det i den här studien.

MONICA: Nej. Det här med sårbarheter hos privatpersonerna. Vad kan du berätta om det? Vilka sårbarheter är det som bedragarna främst utnyttjar?

LINA: Ja, men just när det kommer till det här som vi pratar om nu, bedrägeri genom social manipulation, så eftersom det är individer som luras, så är det just sårbarheter kopplade till individen som blir, ja men de blir väldigt centrala. Det vi såg i vår studie, eller det som lyfts fram där, är särskilt digital ovana och okunskap. Att man kanske inte riktigt har koll på det här med internetbank, BankID och hur det funkar, Swish som gör att man helt enkelt blir, blir lättare att lura. En sak som är tydlig också är det här med stress, hur bedragarna använder stress och oro som ett verktyg när de när

de luras. Att man kanske säger att " ja men det pågår misstänkta transaktioner på ditt konto" och ringer upp. "Och nu är det bråttom, du måste göra någonting, annars kommer du bli av med alla dina pengar. Oj,oj hur ska det gå? Vi måste göra någonting nu!". Och sen så just den här bedragaren som erbjuder då, som också kommer med lösningen - jag kan hjälpa dig. Och på det sättet bygger upp ett förtroende. Och när det här potentiella brottsoffret blir väldigt stressad så är man ju mindre benägen att agera rationellt och tänka igenom vad man ska göra. Så man blir helt enkelt mer lättlurad. Och personer som också har inte helt vana vid det digitala och internetbanker blir ju mer känsliga just för den här stressen också.

MONICA: Det är ju främst äldre vad jag förstår, eller hur?

LINA: Ja, men just den här typen av bedrägerier är ju särskilt äldre och det verkar som att bedragare väljer äldre brottsoffer just för att man tänker att de är mer sårbara. Men sen har vi också med det som vi kallar för strukturella eller tekniska sårbarheter. Där finns det olika saker som bedragarna kan använda för att liksom bli mer tillförlitliga i sin manipulering. Att man kan manipulera vilket telefonnummer som visas hos mottagaren, det som kallas för spoofing. Så att det kan se ut, ja men som ett annat nummer som gör att det potentiella brottsoffret redan på något sätt har blivit lurad innan man ens har lyft luren eller öppnat smset. Vem det är man tror att det är.

MONICA: Så det kan se ut som att det är min son som smsar mig till exempel?

LINA: Ja, det kan det vara. Men det kan också vara till exempel en myndighet eller något företag som man har förtroende för eller är kund hos, som gör att man blir mer lättare att luras. Och sen så är det, en omständighet som är viktig också är ju just den digitala betal- och bankmarknaden som någonstans möjliggör enkla och snabba transaktioner. Det blir ju en omständighet i samhället som bedragarna kan utnyttja.

MONICA: I den här rapporten, som du är projektledare för, så vet jag att den innehåller många förslag på olika åtgärder. Flera av åtgärderna handlar

om att tekniken behöver bli säkrare, till exempel. Och här har ju bankerna en viktig roll. Kan du berätta lite mer om det?

LINA: Ja, men det är ju lite kopplat till den här sårbarheten just med att det är snabba och enkla transaktioner som kan göras. Vi tror att, att bankerna skulle kunna bli bättre i sin övervakning av transaktioner. Bankerna har en övervakning av transaktioner idag. Men att bli bättre på att stoppa misstänkta transaktioner och kanske i större utsträckning basera det på vad individer brukar göra, hur de transaktionsmönster som man har, var, att identifiera när det avviker. Ja, men jag får min lön den 25:e, jag brukar betala räkningarna av de här mottagarna och att kanske ha system som bättre flaggar upp när det sker någonting misstänkt, något avvikande och stoppa det. Och kanske då att det ska krävas någon särskild kontroll eller så för att kunna släppa igenom de transaktionerna. Vi pratar också om, eller skriver också om, att det skulle kunna vara att man skulle kunna jobba mer med valfria begränsningar så att kunder som känner sig osäkra och vill vara tryggare eller ha en säkrare, vara säkrare helt enkelt i sina ekonomiska eller sina bankärenden väljer själva att ta, nej men jag vill aldrig göra en transaktion över den här summan. Att man då kan välja att det ska vara en fördröjning om man vill göra en större transaktion så att man måste godkänna igen nästa dag eller att man måste föranmäla innan, eller kanske en tredje part också måste gå in och godkänna eller en kombination av sådana olika lösningar.

MONICA: Det kräver också en väldig medvetenhet, tänker jag, av kunden?

LINA: Absolut. Då behöver man få information att det här finns. Så det skulle ju vara ett ansvar i så fall för bankerna också att rekommendera den typen av lösningar. Till de kunder som kanske är riskgrupper eller som själva känner sig osäkra. Men syftet skulle då vara just att, att när en person faktiskt blir lurad av en bedragare, att bankerna ska hjälpa till att gå in och stoppa sådana transaktioner som man har blivit lurad att göra.

MONICA: Då vänder jag mig till dig, Helena. Nu har Lina pratat lite om bankerna och vad bankerna gör och så där. Du, jag nämnde din titel inledningsvis, jag

tror nästan att du får lite kort berätta vad det innebär - Head of Fraud Intelligence och Awareness, vid Nordea. Vad gör du och ditt team där?

HELENA: Ja, alltså man kan säga så här att det är som två delar. Jag har åtta experter specialister, två i varje land, så vi har en i Norge, Danmark, Finland och Sverige. Intelligence-biten går i korthet ut på att vi som har den rollen i teamet är väldigt mycket ute i de olika nätverk och samverkansforum som finns inom vår bransch. Betyder att vi träffar andra banker och andra relevanta aktörer, utbyter information om trender som vi ser speciella modus operandi eller tillvägagångssätt, helt enkelt, som bedragarna använder. Så plockar vi hem den informationen, analyserar den, ser om det är någonting som vi måste omedelbart åtgärda eller information som vi behöver sprida rent internt. Sen tar vi också den här nya kunskapen och omvänder den till awareness och det är egentligen att skapa utbildningsmaterial kan man säga, som används mot kunder, olika typer av kundgrupper men också inåt mot våra medarbetare så att de som till exempel sitter i första ledet och möter kund också är uppdaterade på det senaste. Så det blir som ett litet ekosystem där vi både hämtar in och delar information. Men också skapar awareness content helt enkelt som kan användas. Så skulle man kunna sammanfatta det ungefär.

MONICA: Det är ju viktigt att de som möter kunden, har den dialogen, vet om vad som händer då.

HELENA: Absolut, absolut. Vårt ansvar är både det externa ut mot våra kunder och internt mot våra medarbetare.

MONICA: Men du, kan du ge några exempel på hur bankvärlden generellt, för jag vet ju att ni har mycket samarbete med övriga banker, hur arbetar ni för att förebygga bedrägerier? Det är ett enormt problem.

HELENA: Alltså, det finns ju. Om man ska tala om bankvärlden och förebyggande så blir det, man kan ju säga att vi samverkar så mycket som vi får. Och det är en av utmaningarna att det finns gränser för hur mycket vi får samverka, hur mycket vi får dela. Och där jobbar vi också tillsammans under bankföreningens parasoll, men också på andra sätt för att påverka

lagstiftning till exempel och aktörer, så att reglerna på sikt kan förändras så att vi får bli mer effektiva. Nu kan vi byta med andra banker saker som vi ser har blivit ett problem. Vi kan också dela med oss av om någon annan bank har kommit på en smart lösning som stoppade det. Sådana saker kan vi göra, men det blir ju på en övergripande nivå. Sen en annan sak som bankerna gör förstås för att förebygga är ju de olika tekniska lösningarna som man har och de ser olika ut hos olika banker, så där kan jag bara prata för min egen bank egentligen. Och jag menar, det handlar ju om att skruva i system i monitorering som du Lina nämnde. Och skapa innehåll, så. Vi har säkerhetslösningar som idag är ganska gemensamma mellan bankerna. Vi har till exempel BankID, alla banker erbjuder, alla ger inte ut BankID, men du kan använda BankID för att logga in var som helst och även runt BankID finns det samverkan. Runt Swish finns det också samverkan, så det är på flera nivåer som en lök med olika lager helt enkelt.

MONICA: Men du nämnde att det finns begränsningar, men vad är det ni, om du kan ge exempel på vad är de ni skulle vilja göra som inte går idag?

HELENA: Absolut, just nu så både från bankernas håll och i samverkan med polis, med polis har vi en samverkansform där vi försöker hitta exakt vilken typ av utökad informationsdelning skulle vi behöva. Så där finns det begränsningar och vi skulle konkret vilja kunna till exempel utbyta målvaktskonton. Snabbt. Här handlar det om att vara snabb för att någon som upplåter sitt konto för att ta emot bedrägliga pengar, det är färskvara. Men om vi till exempel får reda på, på grund av ett försök till bedrägeri eller genomför, då får vi ju en målvakt. Då skulle vi vilja kunna dela den jättesnabbt med alla andra banker.

MONICA: Och det kan ni inte idag?

HELENA: Det får vi inte göra.

MONICA: Nej.

HELENA: Vi kan byta information med en part. Så om vår kund blir drabbad, pengarna går till en kund på SE-banken eller vad som helst, då får vi byta den informationen just kopplat till den transaktionen. Men vi får inte göra det generellt, vilket skulle vara oerhört effektivt. För jag menar skickar du, när du begår ett bedrägeri så vill du skicka pengarna vidare och om inte det går så blir det väldigt svårt att använda den kanalen över huvud taget. Så det är en sådan väldigt konkret sak. Och de här behoven och förslagen har även vi tillsammans med Bankföreningen fört fram nu till de som kan eventuellt fatta beslut om att justera det här.

MONICA: Ser du någon lösning eller någon ljusning där?

HELENA: Alltså, ja, man får ju hoppas, man får fortsätta envist och framhålla att det behövs.

MONICA: Det förekommer ju mycket i media nu om kriminella nätverk och barn och unga som rekryteras in. Och just det du nämnde med målvakter är ju ett väldigt vanligt sätt att utnyttja de här barnen, så kan man komma åt det så är ju mycket vunnet.

HELENA: Jo, men just att unga används som målvakter. Det är ett stort problem. Och där gör vi, var och en av bankerna gör olika webbinar, insatser, vi är aktiva i sociala medier för att nå fram till dem, vilka konsekvenserna kan bli. Och idag så är det ju faktiskt så att du kan, om du medverkar och blir målvakt och det blir tydligt, så kan det få konsekvensen att du inte får ha ett BankID, på ett helt år, i någon bank. Det är en ganska kraftfull konsekvens som man kanske inte skulle vilja få om man var medveten om det på ett annat sätt.

LINA: Barnen kan ju också, eller målvakter blir också återbetalningsskyldiga om man har medverkat i brott som man inte medveten om. Man kanske inte är medveten om att, att man bidrar till ett ganska allvarligt brott när man tar emot pengar och skickar pengar vidare. Men eftersom man har hanterat de här pengarna så har man också ett ansvar att betala tillbaka. Och det kan ju bli jätteallvarliga konsekvenser för unga människor.

MONICA: Ja, det är otroligt viktigt att informera de unga om det.

HELENA: Vi försöker ju vara i den mån vi så mycket som vi kan, finnas där ungdomar finns i skolor och sånt, och hålla olika dragningar för dem på deras villkor för att de ska förstå vilka risker de tar. Ofta kan det vara så, en del är väldigt medvetna om att de gör något brottsligt, men många är inte särskilt medvetna om vad man får och inte får göra. En målvakt kan också vara ett offer för ett romansbedrägeri i första ledet och sen bli utnyttjad en gång till. Så det finns ju verkligen skillnad på målvakter och målvakter.

MONICA: Men generellt då, vilka utmaningar ser du från bankers håll att förebygga och komma åt bedrägerier mot privatpersoner?

HELENA: Nej men en av, den största utmaningen med målgruppen äldre människor är att de är svårast att nå. Det är över huvud taget väldigt svårt att nå ut med information, men det är ändå den vägen vi måste gå på något sätt. Där har vi tillsammans med alla andra banker faktiskt gjort någonting helt fantastiskt som aldrig hänt förut och skapat en gemensam sådan här awareness kampanj som heter “Svårlurad” som har ett väldigt stort genomslag där vi använder kanaler som vi aldrig tidigare använt. Det är både TV och det är stora affischer på stan, i tidningar och i sociala medier. Men här var det ju viktigt att inte bara vara i sociala medier för där är inte målgruppen i första hand. Så därför har vi gått mycket på tv och press också. Och det är helt fantastiskt. Men en annan utmaning är att banksystem låter sig inte ändras och justeras så snabbt som bedragarna kan ändra sitt angreppssätt. Det är alltid en utmaning att hinna vara tillräckligt snabb för att göra de justeringar som finns.

MONICA: Har ni sett något genomslag på den här? Jag har också sett den här kampanjen “Svårlurad", väldigt bra. Men har ni sett något genomslag på den eller någon effekt?

HELENA: Ja, det beror på vad du menar. Det är väldigt svårt att se de bedrägerier som inte genomfördes på grund av att…

MONICA: Såklart.

HELENA: …att någon. Men jag menar jag kan ju i alla fall se om jag tittar in i vilka anmälningar vi får in. Så finns det ju ganska många fall där de faktiskt säger att ”nej, men när jag förstod vad det var jag la på luren”. Det är ett väldigt centralt budskap och då blir man väldigt glad för då har man åtminstone räddat den personen, så. Men vi hoppas väldigt mycket att den ska inte bara nå målgruppen äldre utan även bli, jag brukar kalla det awareness through delegation helt enkelt. vi vill ju att anhöriga till äldre eller grannar till äldre, vänner till äldre, hjälper till att sprida budskapet så att man når så långt som möjligt.

LINA: När vi har pratat om just den här typen av kampanjer i vår studie, det finns ju många olika typer med olika innehåll, så är det ju just en sådan bit att få en snackis att det sprider sig att man pratar med varandra, både om vad man ska göra för att skydda sig, men också kanske vad man har varit med om och delar sina erfarenheter och inte skäms utan berättar. Att det blir en sån, ja men att det är där man kanske faktiskt kan förvänta sig en riktig effekt att det sprids och inte då samma risk heller att det blir den här skammen för att man hör om andra som har varit med om samma sak. Och att det kanske mer också blir den här praktiska förberedelsen att “jaha, men vad hände med dig? Hur gjorde du då? Ja men jag ska tänka på det här…” att det kommer närmare och att man verkligen förbereder sig mer praktiskt och blir mer motståndskraftig.

MONICA: Ja, nu har vi pratat lite grann om förebyggande arbete, informationskampanjer och vad bankerna gör och så vidare och vad som kom fram i Brås rapport. Men jag tänkte vi skulle fråga dig Niklas, du jobbar ju med nudging. Du får nästan förklara vad det är?

NIKLAS: Ja, men jag och mina kollegor vi brukar säga att vi jobbar med problemlösning och ett av verktygen vi jobbar med är ju nudging som är ett begrepp som populariserades här i Sverige, kanske någon gång på början av tiotalet. Och från början så kom det upp genom att folk som forskar inom beteendevetenskap tittade på möjliga alternativ till att

förändra beteenden, framför allt i offentlig sektor. Och där har man ju de traditionella policy-verktygen är ju väldigt mycket det ni pratar om: awareness och information, lagar och förbud, skatter. Och någonstans där 2008 så var det två akademiker som också rådgör, ja men diverse presidenter i USA och premiärministrar i Storbritannien, som sa att om vi tittar på hur människor faktiskt fungerar så skulle det kunna vara så att ett komplement till de här strategierna som vi använder, alltså information för att det är väldigt verkningslöst i regel när det kommer till beteendeförändring. Lagar och förbud och skatter för att det är jättesvårt att få igenom. Det är väldigt svårt att få igenom. Så tittar de på ja men vi kan det här vi kallar för nudging, alltså att förändra beslutsmiljöerna, att göra det som många säger lite lättare att göra rätt. Och det här är ju egentligen, alltså jag jobbar med mycket stora matbutikskedjor och det här är ju sådan psykologi som de alltid använt. Jag jobbar också mycket med digitala teknikbolag och de skulle vi kalla det för användarvänlighet. Men kärnan är väl ändå någonstans att det är ju ett sätt att tillämpa beteendevetenskaplig forskning för att förändra lite de ytorna där vi fattar beslut i syfte att på ett lite förutsägbart sätt öka ett visst beteende, utan att för den delen förbjuda vissa beteenden eller bestraffa dem ekonomiskt. Så om vi pratar om till exempel sanktioner eller moms skatter som ska upp eller ner, då är det inte nudging. När vi pratar om försäljning av varor som folk kanske egentligen inte behöver, då är det inte nudging. Det är kreativ användning av beteendevetenskap. Men nudging ska ändå ligga i mottagarens intresse. Och när vi använder det och pratar om att förbjuda saker, då är det inte nudging heller, utan det är de här små förändringarna i när man fattar beslutet. Som ibland finns jättemånga exempel där det får stor effekt. Men om man tittar på de metaanalyser som finns, mest nudging forskning har handlat om hållbarhet, och då ser man kanske att, ja men i snitt så kanske en liten nudge, alltså man förändrar miljön där man fattar beslut, kanske påverkar beteenden tre till fem procent. Att man ser en ökning av önskade beteenden. Det finns många härliga studier som pekar på dubbelsiffriga,

men man ska ändå vara rätt ödmjuk inför att de saker vi pratar om nu, alltså social manipulation, ganska svårt att nudga bort.

MONICA: Mm, men vad tror du, skulle nudging kunna användas mot bedrägerier? Och på vilket sätt i så fall?

NIKLAS: Nej men jag skulle nog, jag skulle nog tänka att det är ju i grund och botten ett beteendeproblem som vi vill att människor inte ska göra vissa saker och istället till exempel lägga på luren. Eller när man pratar om det här med att man sprider ordet om en kampanj, det är också ett beteende. Så jag tänker att det som det här perspektivet kan bidra med är ju väldigt mycket bara så här ja men bryta ner saker i konkreta beteenden. Alltså bryta ner utmaningar kring vare sig det telefonbedrägeri eller kortbedrägerier och börja prata om vad det är vi vill att folk ska göra istället. Och kanske också hur mäter vi det? För det är ju i regel organisationer jättedåliga på. Alltså man är oftast awareness och information, då blir man ju lite hänvisad till, lite svårare mått som kanske inte säger någonting om hur folk beter sig. Men om man tittar på hur stora plattformar i USA till exempel använder beteendevetenskap så är man ju väldigt duktig på att titta på att, ja men addera friktion kring oönskade beteenden, alltifrån spridning av missinformation. Jag tycker vi var inne på det lite mer så här, ja men dela kortuppgifter, hjälpa folk att sätta upp spärrar. Det kom väl en sådan liten policy när Bolund var finansmarknadsminister kring Klarna, tror jag att det var. Att när det just kom till det här med att ta saker på faktura eller inte, att förvalet skulle vara att betala med pengar man har här och nu. Sedan kringgick ju Klarna det på ett jättekreativt sätt på typ två timmar. Men det är väl ändå lite mer åt det hållet, addera friktion. Tycker det är jättekul med många kortleverantörer som har notiser nu när det dras, ett jättekreativt grepp. Alltså Mobilt BankID att man har gått över till att man scannar QR-koder. Den typen av saker, stora köp och säljplattformar när det dyker upp ett telefonnummer då får man ändå en liten varning som säger “okej tar man dialogen om den här köpprocessen utanför plattformen så för det med sig risker”. Och att man kan skicka meddelande inom till exempel Blocket

istället för via krypterade appar som WhatsApp. Jag skulle säga att kärnan för att råda bot på den här typen av problem inte är att informera bort problemet, utan det är verkligen att bygga de här infrastruktur-förändringarna som gör det lätt per default om man säger så, beter sig mer, mer säkert. Sen är det lättare sagt än gjort. Det är ju mycket, väldigt mycket av sådana här köp- och säljbeteenden till exempel som görs på internationella plattformar. Då behövs det väl någon EU-standard och så banksamarbeten som går att göra eller som inte går att göra på grund av regleringar. Men det är där kärnan är, skulle jag säga.

LINA: Man pratar ju mycket tycker jag också om den här konflikten mellan att det ska vara enkelt att köpa och handla och göra. Vi vill att allt ska gå smidigt, både att göra banktransaktioner och betala och köpa och att det kan stå i motsats till den här friktionen som du pratar om Niklas, så att det ska vara lite svårt.

NIKLAS: Nej men precis. Det är väl mer av en personlig preferens, men jag tycker så här, det kanske har kommit till peak friktionsfri betalning nu, alltså att det kanske är… Jag ser ett hål i marknaden i att det kanske är en aktör som skulle kunna ta positionen "säker betalning" för det upplever jag att det inte är så många som trycker på utan det är fortfarande då "smooth payment" och "one click" och såna saker. Det här är ju bara början på vad som kommer hända.

LINA: Det är på något sätt det som, eller som vi lyfter i rapporten att vi ser att man önskar att bankerna också kunde se det som en möjlighet att marknadsföra sig som de säkra bankerna genom att ha sådana här valbara tjänster eller produkter där man kan på ett enkelt sätt sätta begränsningar. I likhet med det jag pratade om förut, att det blir ett sätt att konkurrera på marknaden för att vara den säkraste banken om man är orolig för att utsättas för bedrägerier.

NIKLAS: Jag tror att det skulle kräva en nischaktör som ni sedan sväljer. Ni har ju tusen och en saker att tänka på. Så det, jag ser verkligen att det skulle

kunna dyka upp någon sådan alltså Volvo för transaktioner, Volvo-säkerhet över hela världen eller vad det nu skulle kunna vara.

HELENA: Men det ironiska i det hela tycker jag lite grann är att våra, om man tittar på de nordiska bankerna och säkerhetslösningar och om man tittar på intrång och sånt där - vi är toksäkra. Det är därför vi har så mycket att bedrägerierna går just mot privatpersoner eller mot människan istället som, som är den osäkra faktorn. Och även när vi har infört, för det som du efterlyser Lina, och det här med friktion, det finns på plats. Man kan redan göra vissa justeringar själv. Problemet är lite grann att de här bedragarna får de utsatta att kringgå det här själva som att, om vi går tillbaka någon tid så var det väldigt populärt att försöka få ut ett BankID från offret och ha det i sin kontroll. Nu finns det så mycket säkerhet och larm och grejer kring när ett BankID ges ut felaktigt, så då har man istället gått över till att försöka få offret att utföra alla transaktionerna själv och då blir det väldigt, då kan det vara väldigt, väldigt svårt att identifiera det om det är normalt eller inte normalt. Till exempel om man plötsligt skickar en massa eller små betalningar via SMS till någon som har försökt lura en, eller via swish menar jag, förlåt. Då kan det se väldigt likt ut ditt vanliga beteende och det är fullkomligt omöjligt att se. Så där har vi en utmaning att man kringgår, även det offret kringgår med väldigt duktigt, måste jag säga, människor som kanske annars säger "jag men jag förstår inte hur det här funkar" men de kan uppenbarligen kringgå säkerhetsrutiner, för att de känner sig så fullkomligt övertygade om att det de gör är bra.

MONICA: Ja, visst är det så.

HELENA: Höja överföringsgränser och sådana saker. Ta bort spärrar. Det är en stor utmaning.

LINA: Man behöver ju hitta sätt som gör det möjligt att ta bort dem, men inte att i stunden av en bedragare ta bort dem.

HELENA: Precis, ja men precis.

NIKLAS: Jag saknar verkligen en, alltså något som vi alltid gör i våra projekt, oavsett om det handlar om mat eller kollektivtrafik, alltså beteendekartläggning där man försöker systematisera alla aktörer. Och jag gissar att en sådan om man skulle ha en sådan så är banken en överlägsen, det är den aktören som har flest touchpoints med de beteendena som vi vill minska i det här sammanhanget. Men betalaktörerna, kortaktörerna, alltså var och varannan e-handel drivs av Shopify nu och, det är i och för sig ett kanadensiskt bolag, så det måste man se till dem. Det skulle vara väldigt intressant att se landskapet… Tycker det kan bli lätt att man fastnar så här att bankerna ska göra mer av ditten och datten och givet regleringar och så vidare så kanske man fastnar i lite så här awareness, awareness training och det vill jag verkligen att alla som lyssnar ska veta att de studier jag sett kring awareness, oavsett om det är cybersäkerhet eller mångfald och inkludering eller hållbarhet eller hälsa, awareness har sällan kausal effekt på beteenden man vill förändra. Så är det bara. Utan det är de här infrastruktur-förändringarna. Då måste vi hitta systemet som man ska verka i. Då kanske det vore kul att föra ett samtal om vilka de andra systemen som måste ta ansvar och som man kan samverka med, som inte är banker. Det blir lätt att vi hamnar där.

MONICA: Vad tror du Helena, vilka system skulle det kunna vara? Pratar ni någonting om det?

HELENA: Alltså jag vet inte riktigt vad du menar när du säger system, men det finns ju aktörer på marknaden som på något sätt går under radarn men som ändå är verktyg i. Och det är till exempel teleoperatörerna. Där har vi ju också försökt att dels få en dialog med teleoperatörer. Men det kommer ju också tecken från omvärlden att det kommer att ställas även krav på teleoperatörer, att till exempel ha kontroller för att undvika spoofing, till exempel. I Finland har ju deras myndighet för telekommunikation infört ett krav på alla tele, teleoperatörer att de måste garantera att telefonnummer inte är spoofat. Då talar vi både sms och uppringt. Det skulle jag gärna se här också.

NIKLAS: Ja men det är precis…

HELENA: För de har möjligheten att göra det. Och vi är ofta i dialog med dem eftersom vi ser det som pågår, då har det väl i stor utsträckning varit nej men det där kan inte vi göra någonting åt. Men det är klart man kan. Man måste bara ha rätt incitament.

LINA: Det pågår ju ett samarbete också mellan teleoperatörer, telekområdgivarna och Post- och telestyrelsen i Sverige när man tittar på lite liknande lösningar som man har i Finland. Jag tror att man till en början kommer man, ja men jag tror att det närmar sig en lösning där det framförallt är fasta telefonnummer då som visas. Det kommer från utlandet, men det visas fasta svenska telefonnummer att det ska kunna stoppas. Men det behöver man också titta vidare just på sms för det är precis som du säger det ett… Det används ju mycket och bedragarna hittar hela tiden något, något litet kryphål, blir lite säkrare så hittar man nya sätt, så man behöver hela tiden liksom.

HELENA: Ja men precis.

LINA: Men det är ändå på gång även i Sverige just med det här med spoofingen.

NIKLAS: Det var ju någonting kul i när jag läste den här rapporten som vi pratar om, som ja, som gjorde mig väldigt glad. Det var ju ändå på temat information. Jag minns inte exakt sägningen Lina, men det var någonting i stil med den information som ges måste bli mer målgruppsanpassad eller mer skräddarsydd utifrån mottagaren och de risker som han eller hon står inför och de beteendena. För det, det kan jag sakna lite i att det blir lite av en sån här hagelsvärmssituation i de här informationskampanjen är i regel, att bli inte lurad. Men jag minns inte exakt hur du skrev det, men det gjorde mig som sagt väldigt glad, just att det kom mer till att, om jag tolkar det rätt?

LINA: Jo,jo.

NIKLAS: Anpassa råden utifrån som ung så är det, alltså det här vi pratar om med målvakten var superintressant. Det hade jag ingen aning om att det var,

alltså det kändes helt främmande för mig som 36-åring och då ska ju inte jag nås av det råden. Jag behöver ju inte, jag behöver faktiskt inte lära mig om hur man undviker att bli målvakt.

LINA: Du är inte riskgruppen, nej.

NIKLAS: Jag är inte riskgruppen. Men problemet är ju när man har lite svårt att anpassa sina råd. Det blir ju lätt ett brus och om jag stöter på en irrelevant rekommendation, då finns det ganska stor risk att jag slår dövörat till för att avfärda allt som oavsett om det är banken eller om det är Brå som har kommit med det. Så det där känner jag mig väldigt nyfiken på att se hur ni kommer att jobba med.

LINA: Jo, men det där behöver vara relevant. Det är både, det är både innehållet som behöver vara relevant just för den målgruppen och sen också formatet. Att det är information som framställs på ett sätt som man verkligen kan ta det till sig. Men de här grupperna som är allra svårast att nå, då kanske man får jobba genom anhöriga också, precis som du är inne på, Helena, tänker jag. Men sen när vi har pratat lite med äldre också och där lyfter man fram just behovet av att praktiskt förbereda sig. Att liksom ha en strof färdig, det här ska jag säga när någon ringer och kanske ha ett rollspel. En övning där man lyfter på luren och så här "nej" och lägga på. För att när man hamnar i den här stressade situationen så är det lättare att, det är lättare att ta till sig det man har övat på, för det är lättare att agera på än det som man bara vet i huvudet. "Ja, just det jag ska lägga på luren". Man behöver ha gjort det någon gång på något sätt för att klara av att göra det just i den stressade situationen.

MONICA: Det är nog bra, öva rollspel. Men vi ska knyta ihop säcken lite. Jag tänkte bara avslutningsvis fråga er här vilka åtgärder tror ni är viktigast för att förebygga bedrägerier så att färre utsätts och drabbas?

LINA: Får jag börja? haha.

MONICA: Mm, det får du haha.

LINA: Nej men jag vill, det är lite också återknyta till det som vi pratade om med det här systemet och, för det vi lyfte fram i rapporten är att man behöver se till hela händelsekedjan för bedrägerier, både till det bedragarna gör när de förbereder det kanske vi pratar om att man kartlägger och vet, väljer ut brottsoffer, kanske publicera annonser på sociala medier, ta reda på information för att kunna vara manipulativ i samtalet. Och det här med spoofing och sen vidare till hur genomföra transaktionen och hur det går till, vad skulle man kunna göra där. Och sen det här hantering av brottsvinster, att föra dem vidare till målvakt är att man behöver just se till hela händelsekedjan, alla sårbarheter och täppa igen överallt.

MONICA: Någon annan som?

NIKLAS: Den lilla åtgärden haha.

LINA: Ja precis den viktigaste. Allt! Ja förlåt.

NIKLAS: Nej men alltså, jag tänker så här en kort skulle vara mer kring tvåstegs autenticering, alltså, när det är, så som vi gör med inlogg. Att verkligen att man, man behöver godkänna saker, eller som du var inne på i början att det finns ett litet lagg mellan beslutet och en transaktion att den är utförd. Men sen skulle jag ha en lite längre och det är att man kan inspireras lite av industrin och byggbranschen. För där har man börjat arbeta med något som heter beteendebaserad säkerhet, alltså ifrån att man länge pratar om nu måste vi informera våra arbetare i industrin om hur man undviker arbetsplatsolyckor. Så har man beteendeutbildade skyddsombud numera. Oavsett om det är gruvor eller en tunnelbana som byggs så går det runt psykologer eller beteendevetare och faktiskt förändrar miljöerna. Jag tycker ändå att det perspektivet, för, alltså, det har vi gjort sedan länge när det kommer till köp. Det arbetar psykologer på Uber, på Tiktok, på Snapchat. De jobbar inte så mycket med säkerhet utan de jobbar mer med köp. Och det är väl helt okej. Men jag hade gärna sett att samma våg kommer in i den här typen av säkerhetsfrågor.

MONICA: Helena, har du någon?

HELENA: Nej, men jag tror att det är viktigt att lite det som du nämnde Lina om att se hela kedjan. Det tycker jag faktiskt att vi tillsammans gör. Sen kan man göra ännu mera förstås. Så samverkan och viss justering av regelverk skulle verkligen behövas, så att vi alla kan bli bättre på att agera snabbt och effektivt. Sen tror jag också att det här, som också nämnts, att ha större möjligheter till individanpassade inställningar och tjänster och sånt där det är också vägen framåt. Vi har redan börjat med det vad det gäller just våra äldre kunder. Men det kan ju göras mer. Men det blir fortfarande lika svårt kanske att nå de här målgrupperna med den informationen att de här möjligheterna finns. Så att jag tror på det, mera flexibilitet i vad man kan göra och inte kan göra, eller hur och när? Samt fortsatt samverkan tror jag.

MONICA: Du har lyssnat på ett avsnitt av Brås podd Snacka om brott. Idag har vi pratat om bedrägerier mot privatpersoner och olika metoder och arbetssätt för att förebygga utsattheten för bedrägerier. Jag vill tacka Helena Wall från Nordea. Niklas Laninge från Nordic Behavior Group och Lina Fjelkegård från Brå som har bidragit med värdefulla kunskaper och nya insikter när det gäller arbetet mot bedrägerier. Jag som ledde samtalet heter Monica Landergård och är pressekreterare på Brå. Tack för att du har lyssnat.