LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

E-legitimationsbedrägerier

Balansgången mellan förtroende och vilseledning

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Sebastian Agnvall
Georg Lavman

Handledare: Benjamin Weaver

Rättande lärare: Magnus Wärja
Paul Pierce

E-legitimationsbedrägerier: Balansgången mellan förtroende och vilseledning

ENGELSK TITEL: E-legitimation fraud: The balance between trust and deception

FÖRFATTARE: Sebastian Agnvall och Georg Lavman

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Odd Steen

FRAMLAGD: maj, 2019

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 71

NYCKELORD: Social Engineering (SE), BankID, e-legitimation, medvetenhet, tillit, åtgärder, Information Security Awareness (ISA), SEADMv2

SAMMANFATTNING (MAX. 200 ORD):
Studien omfattar bedrägerier som utförs via den svenska e-legitimationen BankID. Konceptet social engineering presenteras i denna studie och används som en förklaringsmodell för att kunna utforska huruvida BankID-bedrägerierna faller inom ramen för SE. Vidare diskuteras ett antal mänskliga faktorer som har en påverkan i dessa sammanhang, vilka är målgrupp, medvetenhet och tillit. Genom en intervjustudie ställs det som presenteras i litteraturgenomgången mot respondenternas svar. Respondenterna arbetar inom IT-säkerhetsbranschen och Polismyndigheten, och ger i intervjustudien sin syn på problematiken gällande bedrägerier och BankID. Studien identifierar medvetenhet hos användare som den största bristen i samspelet mellan användaren och teknologin. Avslutningsvis föreslås ett antal förbättringsmöjligheter för att höja säkerhetsnivån och förhindra BankID-bedragarna.

Innehåll

1 Introduktion 1
1.1 Bakgrund 1
1.1.1 Social Engineering 1
1.1.2 BankID 1
1.1.3 Bedrägerier kopplade till BankID 2
1.2 Problemområde 2
1.3 Forskningsfråga/Frågeställning 3
1.4 Syfte 3
1.5 Avgränsning 3
2 Litteraturgenomgång 4
2.1 Social Engineering 4
2.1.1 Förberedelsefasen 4
2.1.2 Attackeringsfasen 6
2.1.3 Postattack-fasen 6
2.2 Social engineering metoder 6
2.2.1 Reverse social engineering 7
2.2.2 Phishing 7
2.2.3 Spear-Phishing 7
2.2.4 Vishing 7
2.3 Information security awareness (ISA) 8
2.4 Tillit och sårbarhet 8
2.4.1 Tillit till teknologier 8
2.4.2 Äldre utgör en sårbar grupp 9
2.5 Social Engineering Attack Detection Model: SEADMv2 10
2.6 Undersökningsramverk 12
3 Metod 14
3.1 Utformning av litteraturstudie 14
3.2 Metodansats 14
3.3 Utformning av intervjufrågor 15
3.4 Urval av intervjuobjekt 15
3.5 Analysmetod 16
3.6 Etik 17
3.7 Reliabilitet och validitet 17
3.8 Metodreflektion 18
4 Empiri och resultatanalys 20

4.1 Social engineering: Faser och metoder 20
4.2 Användare: Medvetenhet och tillit 22
4.3 BankID: Teknisk lösning 25
4.4 Motverka attacker: ISA och SEADMv2 27
5 Diskussion 29
5.1 Social engineering: Faser och metoder 29
5.2 Användare: Medvetenhet och tillit 30
5.3 BankID: Teknisk lösning 31
5.4 Motverka attacker: ISA och SEADMv2 32
6 Resultat och slutsats 34
6.1 Slutsats 34
6.2 Kunskapsbidrag 34
6.3 Vidare forskning 34
Appendix 1 Intervjufrågor 36
Appendix 2 Transkribering Jan Olsson 38
Appendix 3 Transkribering Boris Berberovic 48
Appendix 4 Transkribering Albin Zuccato 58
Referenser 63
Domar 66

Figurer

Figur 1: The anatomy of a Social Engineering attack, (Bhagyavati, 2007, s. 4) 4
Figur 2: Kommentar på Facebook-sida (Swedbank, 2019)..... 5
Figur 3: Kommentar på Facebook-sida (SEB, 2019). 5
Figur 4: Diagram över ett typiskt BankID-bedrägeri (Wollner, 2018). 6
Figur 5: Modell SEADMv2 (Mouton, Leenen & Venter. 2015, s. 217)..... 11
Figur 6: Undersökningsramverk..... 12
Figur 7: Visualisering av ”Administrativ process”. 31

Tabeller

Tabell 1: Litteratursammanställning. 13
Tabell 2. Överblick intervjufrågor och teori. 15
Tabell 3: Respondenter. 16

Förkortningar

Social engineering (SE)

Social engineering detection model version 2 (SEADMv2)

Information Security Awareness (ISA)

Intrusion Detection System (IDS)

Begrepp i denna uppsats

Phishing - Nätfiske, metod för IT-brottslighet där Internetanvändare luras till att lämna ut känslig information som sedan kan användas till bedrägerier, t.ex. att tömma bankkonton på pengar. (Nationalencyklopedin, 2019).

Vishing - Telefonfiske, metod för IT-brottslighet där bedragare lurar personer att via telefon lämna ut känslig information, till exempel bankkoder och lösenord (Nationalencyklopedin, 2019).

Spoofing - Att dölja eller manipulera IP-adress, mailadress eller telefonnummer (Ivaturi & Janczewski, 2011).

Intrusion detection system - Program som upptäcker försök till dataintrång (IDG:s ordlista, 2019).

eiDAS - Alla offentliga verksamheter och deras systemleverantörer med e-tjänster måste kunna erbjuda inloggning med e-legitimation även för europeiska medborgare (Svensk E-IDENTITET, 2019).

E-legitimation - Elektronisk legitimationshandling som används för säker identifiering på internet (Nationalencyklopedin, 2019).

Hackare - Person som använder sina kunskaper till att bryta sig in i datorsystem (Nationalencyklopedin, 2019).

Penetrationstest - Test av datorsystem där sårbarheter eftersöks som en angripare skulle kunna utnyttja (IDG:s ordlista, 2019).

1 Introduktion

1.1 Bakgrund

1.1.1 Social Engineering

Social engineering (SE) kan beskrivas som konsten att utnyttja människans egna brister för att få tillgång till viktig och känslig information (Kaushalya, Randeniya, & Liyanage, 2018), eller som Ian Mann (2008) beskriver; att manipulera människor genom vilseledning för att få ut information, eller få individen att utföra en åtgärd (Mann, 2008, p. 11). Sociala interaktioner används som verktyg av förövare i syfte att utvinna viktig information från det missledda offret, vilket kan vara en specifik individ eller större organisation (Kaushalya et al., 2018). Den största skillnaden mellan SE-attacker jämfört med andra typer av informationssäkerhets-attacker är att vem som helst, oberoende av kunskap eller lön, kan bli attackerad. Av denna anledning är SE-attacker generellt sett svåra att försvara sig mot (Kaushalya et al., 2018). Människor är i sin natur komplexa, vilket innebär att de inte går att säkra på samma sätt som exempelvis en web-server som i sig kan vara komplex, men med rätt expertis är lättare att förstå (Mann, 2008).

Bedragare som använder sig av social engineering utnyttjar kunskaper om mänskliga svagheter för att utveckla nya och mer komplexa typer av attacker (Mann 2008). Dessa attacker används inte enbart för att komma åt ekonomiska tillgångar, utan de används även för att få tillgång till känslig personlig data, samt organisationshemligheter (Kaushalya et al., 2018). Historiskt har utförandet av social engineering inte varit riskfritt, och att lyckas med en attack är ingen garanti. Däremot har internets utveckling möjliggjort för nya typer av attacker att uppstå, dessutom har det även gett bedragare det ultimata skyddet, vilket enligt Mann (2008) är distans och anonymitet från offret.

1.1.2 BankID

Sverige betraktas internationellt ligga i framkant när det kommer till E-legitimation. Redan 2002 lades grunden till BankID av Finansiell ID-Teknik BID AB, ett svenskt bankkonsortium mellan elva svenska storbanker (Finansiell ID-Teknik BID AB, 2019). Det tog däremot flera år innan den funktionalitet som återfinns idag hade utvecklats, detsamma gäller antalet användare som 2016 uppgick till över sju miljoner (Husz, 2018). Idag använder majoriteten av svenskar BankID för att utföra sina bank och myndighetstjänster. På uppdrag av företaget bakom BankID, Finansiell ID-Teknik BID AB genomfördes 2007 en marknadsundersökning genom Synovate som visade att 95% av svenskar känner till e-legitimation (Finansiell ID-Teknik BID AB, 2019).

”BankID är en e-legitimation som gör det möjligt för företag, banker, organisationer och myndigheter att både identifiera och ingå avtal med privatpersoner på Internet.

BankID är en elektronisk ID-handling som är jämförbar med pass, körkort och andra fysiska legitimationshandlingar." - (Finansiell ID-Teknik BID AB, 2019).

Det finns många fördelar med e-legitimation även utanför myndighetstjänster och banker. Inom den privata sektorn finns det många användningsområden som företag i Sverige nyligen börjat utforska. Exempel på detta är inloggningar via fackföreningar, online-casinon och elbolag. Genom att inloggningen till dessa tjänster nu kan göras genom e-legitimation kan användaren på ett tekniskt säkert sätt logga in utan att behöva hålla ordning på olika lösenord.

1.1.3 Bedrägerier kopplade till BankID

BankID har visat sig vara ett användbart hjälpmedel vid identifiering av personer och organisationer. Dessvärre har detta medfört att bedragare har fått tillgång till ett nytt sätt för att lura individer på ekonomiska tillgångar, eller få tillgång till känslig information. Det framgår i ett flertal artiklar (Buvik, 2018; Larsson, 2018) att bedrägerier kopplat till BankID har ökat explosionsartat, bedragarna behöver enbart ha tillgång till en individs namn och personnummer, och kan därefter helt anonymt utge sig för att vara från en bank eller annan myndighet som använder sig av BankID som identifieringsmetod (Larsson, 2018). Äldre individer är överrepresenterade som offer och det finns olika förklaringar till detta som diskuteras vidare nedan i stycke 2.4.2 (BRÅ, 2016).

På BankIDs egna hemsida finns information angående de vanligaste bedrägerierna. Falsk banksupport kategoriseras som en vanligt förekommande bedrägerimetod. Dessutom informerar BankID allmänheten kring hur man som individ kan vara mer vaksam när det kommer till suspekta telefonsamtal (Finansiell ID-Teknik BID AB, 2019). Detta visar på att bedrägerier kopplat till e-legitimation är något som är känt för BankID, och att det är svårt att skydda sig mot (Finansiell ID-Teknik BID AB, 2019).

Malin Wemnell, administrativ chef på BankID, säger i en intervju med "PC För Alla" att de är medvetna om problematiken med bedrägerier, och att de jobbar kontinuerligt för att öka säkerheten. Detta görs enskilt hos BankID men även i samarbeten med utfärdande banker i ett försök att hindra bedrägerier kopplade till applikationen (Wollner, 2018). Wemnell menar att BankID är en säker och uppskattad tjänst. Ingen har tidigare lyckats med att ta sig igenom de tekniska spärrar som applikationen har. Däremot kommer man inte ifrån det faktum att det är användaren själv som släpper in bedragarna och ger dem tillgång till dessa uppgifter (Wollner, 2018; Ekblom, 2018).

1.2 Problemområde

Många nyhetsportaler menar att det för tillfället pågår en bedrägerivåg vilket har resulterat i att miljoner kronor har förflyttats från godtrogna bankkunder till bedragare (Buvik, 2018; Larsson, 2018). BankID är idag en väletablerad tjänst med över 7 miljoner användare bara i Sverige. Omfattande arbete utförs dagligen för att göra applikationen säkrare och på en teknisk nivå håller den mycket hög standard. Trots detta lyckas bedragare genom manipulation och vilseledning utnyttja det faktum att individen är den svaga länken, vilket från BankIDs perspektiv är mycket svårare att förhindra.

1.3 Forskningsfråga/Frågeställning

- Vilka utmaningar står e-legitimationer, såsom BankID, inför vid motverkandet av bedrägerier där den mänskliga faktorn utnyttjas?

1.4 Syfte

Syftet med uppsatsen är att med hjälp av en intervjustudie belysa vilka säkerhetsåtgärder BankID kan införa för att motverka bedrägerier, samt undersöka om dessa bedrägerier går att koppla till social engineering. Respondenterna som deltog i intervjustudien jobbar inom områdena IT-säkerhet och utredning av IT-bedrägerier.

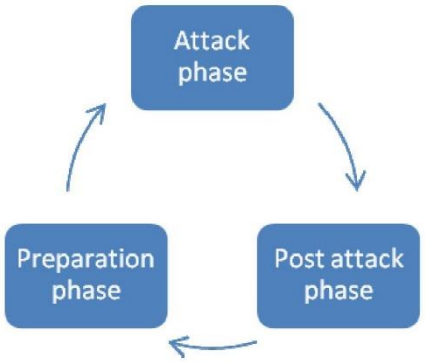
1.5 Avgränsning

Social engineering kommer att beröras för att utforska dess roll i bedrägerier. E-legitimation finns i olika former i flera EU-länder, däremot kommer denna studie enbart beröra den mest populära svenska applikationen för E-legitimation vilket är BankID. Vi har även valt att avgränsa oss till bedrägerier riktade mot privatpersoner och kommer därför inte beröra bedrägerier mot företag och organisationer.

2 Litteraturgenomgång

2.1 Social Engineering

Enligt Krombholz, Hobe, Huber och Weippl (2015) skiljer sig social engineering från traditionell hackning där användandet av tekniska metoder är större. Förövare som använder sig av social engineering riktar sig istället mot individen, och med hjälp av manipulation får de tillgång till känslig och värdefull information (Krombholz et al., 2015). Ivaturi och Janczewski (2011) menar att i ett historiskt perspektiv har stora investeringar i tekniska säkerhetslösningar genomförts i syfte att motverka tekniska attacker. Brandväggar, antivirus och olika typer av intrångsdetekteringssystem (IDS) är exempel på områden där stora investeringar har gjorts, och dessa har visat sig vara effektiva i att motverka tekniska intrång (Ivaturi, & Janczewski, 2011). Detta har resulterat i att bedragare tillsammans med sin tekniska kunskap vänt sig till social engineering för att fokusera mer på mänskliga svagheter. (Ivaturi, & Janczewski, 2011), vilket enligt Manske (2000) är den svagaste punkten i alla säkerhetsarkitekturer. En lyckad SE-attack ger bedragare medlen att kringgå och nollställa tekniska säkerhetsinvesteringar som har kostat uppemot flera miljoner dollar (Manske, 2000).



Figur 1: The anatomy of a Social Engineering attack, (Bhagyavati, 2007, s. 4)

2.1.1 Förberedelsefasen

Inför en SE-attack är informationsinsamling en väsentlig del för att uppnå målet. *"A social engineer needs to plan, prepare, and think about what information he will try to obtain and how he will obtain it."* (Hadnagy, 2011, s. 30). Mer generellt inom SE finns det ett antal olika Linux distributioner, exempelvis Kali (tidigare känt som BackTrack). Dessa Linux-distributioner kommer förinstallerade med mjukvara som exempelvis används för att förenkla hanterandet och navigerandet av den information som finns tillhanda. Linuxdistributionen Kali har över 600 verktyg, många av dessa används framförallt av penetrationstestare men även inom SE. (Offensive Security, 2019)

Informationsinsamlingen görs på flera fronter, bland annat genom användning av sökmotorer och sociala-medier kan bedragaren hitta känslig information som sedan kan användas för att,

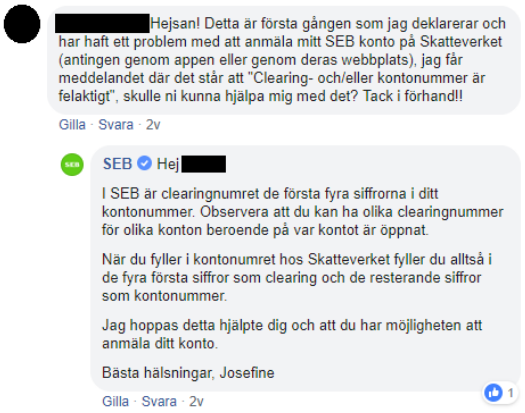
på ett enklare sätt komma åt offret. Generella fakta angående en person eller företag samlas också in, för att man ska kunna bygga en mer komplett profil (Hadnagy, 2011).

- Adress
- Arbetsplats
- Intressen

Listan ovan innehåller tre uppgifter som ofta finns tillgängliga genom användandet av sökmotorer. När informationen är tillhandahållen kan bedragaren exempelvis ringa upp offret och påstå sig jobba hos en underleverantör till offrets arbetsplats. Detta kommer att öka trovärdigheten och således bedragarens chanser (Hadnagy, 2011).

Sökmotorer är kraftfulla verktyg för informationsinsamling. Genom att *Googla* exempelvis "*Site:liveatlund.lu.se filetype:pdf"* får man fram alla PDF-filer som ligger öppet. Detta är en effektiv metod för att hitta telefonnummer och mailadresser. För att identifiera vilken bank någon har kan man besöka bankers Facebook-sidor, där kunder öppet ställer frågor angående bankens tjänster.

Figur 2: Kommentar på Facebook-sida (Swedbank, 2019).



Figur 3: Kommentar på Facebook-sida (SEB, 2019).

Bilderna ovan visar hur två personer ställer frågor till Swedbank och SEB på deras Facebook-sidor.

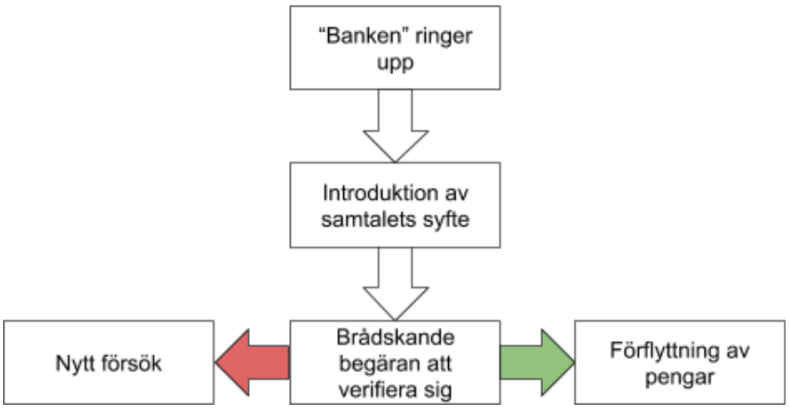
Ur en säkerhetssynpunkt är det oroväckande att folk hjälper bedragarna att identifiera vilken bank de är kunder till. "PC För Alla" belyser problematiken i en artikel kring BankID-bedrägerier, och hur bedragarna som använder sig av vishing ofta uppger sig att komma från banken. (Ekblom, 2018).

"[...] har utsatts för bedrägeri enligt följande. En okänd person har kontaktat henne per telefon och uppgett sig ringa från Nordea. Personen har förmått [...] att signera sitt mobila BankID och på sätt kommit åt hennes konto och därifrån överfört 39 000 kronor." - Mål nr: B 1070–18 (Göteborgs tingsrätt 2018-06-04)

Målsägandens namn har tagits ur citatet för att bevara anonymiteten.

2.1.2 Attackeringsfasen

När informationsinsamlingen är genomförd väljer bedragaren en lämplig metod. Olika typer av SE-metoder beskrivs mer detaljerat i avsnitt 2.2 nedan. Vid BankID bedrägerier har det utifrån rättsfall och mediabevakning framgått att bedragarna mestadels använder sig av *spoofing* och *vishing*, två begrepp vars omfattning kräver en bredare förklaring, se avsnitt 2.2.4. Bedragarna har ett väldigt professionellt tillvägagångssätt där man genom *spoofing* maskerar uppringnings-ID på offrets telefon med bankens namn. Detta ökar trovärdigheten ytterligare (Hadnagy, 2011). "PC För Alla" intervjuade ett offer som blev utsatt enligt metoden ovan (Ekblom, 2018). Där påstod bedragarna att det just nu höll på att ske en transaktion utomlands på offrets konto. För att verifiera sin identitet samt spärra kontot bad bedragarna henne att verifiera sin identitet med hjälp av BankID.



Figur 4: Diagram över ett typiskt BankID-bedrägeri (Wollner, 2018).

2.1.3 Postattack-fasen

För att offret inte skall förstå direkt att denne blivit bedragen är det viktigt att bedragaren fortsätter i sin roll även efter att ha genomfört sin SE-attack. Detta för att ge sig själv tid att kunna slutföra sitt mål, samt fördröja eller förhindra att bli upptäckt (Bhagyavati, 2007).

Enligt artikeln som figur 4 ovan bygger på, ber bedragarna offret att signera med BankID för att beställa hem ett nytt bankkort. Således har offret ingen anledning att misstro någon. Postattackerings-fasen är ännu viktigare utifrån andra fall vi har stött på, där bedragarna laddar ner en egen version av offrets BankID med hjälp av dennes signatur. Bedragarna kan då göra precis vad som helst med offrets bankkonto, fram till dess att offret upptäcker det och kontaktar banken.

2.2 Social engineering metoder

Författarna Krombholz et al. (2015) presenterar i sin artikel *Advanced social engineering attacks* en kategorisering av attacker som är relaterade till SE; fysiska, tekniska, sociala och slutligen socio-tekniska. Fysiska tillvägagångssätt innebär att förövaren utför någon typ av fysisk aktivitet, vilket exempelvis kan vara dumpster diving (Krombholz et al., 2015). Enligt Granger (2001) innebär dumpster diving att förövaren letar igenom en individs eller organisations sopor för att finna information som kan användas mot dem. Tekniska tillvägagångssätt används främst över internet (Krombholz et al., 2015). Internet har medfört

att förövare får distans till offret, och samtidigt kan verka helt anonymt (Mann, 2008). Det sociala tillvägagångssättet är enligt Krombholz et al., (2015) den viktigaste delen vid utförandet av SE attacker. Den sociala aspekten används för att skapa förtroende hos offren för att sedan manipulera dem. Exempel på hur den sociala förmågan används är genom attacker som utförs via telefon (Granger, 2001). Avslutningsvis beskriver Krombholz et al. (2015) det socio-tekniska tillvägagångssättet som en kombination av tekniska och sociala aspekter. Baiting är ett exempel på det socio-tekniska tillvägagångssättet, där bedragarna förlitar sig på nyfikenheten hos människor för att få dem att exempelvis öppna ett mail, exekvera en fil eller koppla in en USB-sticka (Krombholz et al., 2015).

2.2.1 Reverse social engineering

Reverse social engineering är en metod inom SE som tillhör det sociala och socio-tekniska tillvägagångssättet (Krombholz et al., 2015). Huvudsyftet med denna metod är att bedragaren utger sig för att vara någon med makt och auktoritet, vilket ställer den utsatte i en offerposition (Granger, 2001). Enligt Krombholz et al. (2015) är tillit en grundsten, offret blir manipulerad till att tro sig vara i behov av hjälp, och att bedragaren är den som kan lösa problemet. Resultatet blir att offret ger ut känslig information eller utför en handling åt bedragaren (Krombholz et al., 2015). Ett exempel på reverse social engineering är bedrägerier som utförs via telefon där förövaren utger sig för att vara från en bank eller liknande. Offret får veta att man har identifierat misstänksam aktivitet på sitt konto och behöver verifiera med sitt kortnummer och PIN-kod. Dessa bedrägerier är enligt Granger (2001) vanligt förekommande.

2.2.2 Phishing

Jagatic, Johnson, Jakobsson, och Menczer (2007) samt Krombholz et al. (2015) beskriver phishing som att en bedragare maskerar sig för att vara en pålitlig tredjepart genom en elektronisk kanal. Den vanligaste formen av phishing-attacker är massutskick av mail som antingen innehåller en länk med malware, eller leder till ett forum där offren fyller i känsliga uppgifter (Jagati et al., 2007). En stor problematik med att motverka phishing är att dessa typer av attacker kan utföras på en mängd olika kanaler, exempelvis; e-mail, direktmeddelanden, telefon, sociala nätverk och hemsidor (Krombholz et al., 2015).

2.2.3 Spear-Phishing

Spear-phishing är en subkategori av phishing och använder sig av samma typer av kanaler som traditionell phishing. Skillnaden är att förövare som använder sig av spear-phishing har noga valt ut sina offer på förhand (Krombholz et al., 2015). I kombination med detta samlar även bedragarna in väsentlig information kring sina offer. Krombholz et al. (2015) menar på att denna typ av attack är mer tidskrävande, däremot är chansen att lyckas högre om det genomförs på ett korrekt sätt.

2.2.4 Vishing

Namnet vishing härstammar från orden voice och phishing och innebär att förövare använder sig att röstbaserade teknologier, exempelvis över telefon (Yeboah-Boateng & Amanor, 2014). Förövare använder sin sociala förmåga för att låta självsäkra och kunniga när de exempelvis

utger sig för att ringa från en bank. Dessutom använder sig förövare vanligtvis av teknologier som gömmer det verkliga uppringnings-ID, vilket kallas *spoofing*, och maskerar det med bankens uppringnings-ID (Yeboah-Boateng & Amanor, 2014). Att bedragare har denna tekniska kapacitet är enligt Yeboah-Boateng och Amanor (2014) något som offer inte är medvetna om, vilket medför att vishing-attacker har en högre sannolikhet att lyckas.

2.3 Information security awareness (ISA)

Aldawood och Skinner (2018) skriver i sin artikel *Educating and raising awareness on cyber security social engineering: A literature review* att de flesta informationssäkerhetsintrång som sker i dagsläget beror på att den mänskliga faktorn i informationssäkerhet utnyttjas. Detta är möjligt då det finns en brist på förståelse och medvetenhet i anknytning till informationssäkerhet hos individer. Människor går inte att säkra genom tekniska lösningar såsom brandväggar eller antivirusskydd (Mann, 2008), vilket innebär att det är väsentligt att avsätta tid till att lära slutanvändare angående den mänskliga faktorns påverkan i relation till informationssäkerhet (Aldawood & Skinner, 2018).

ISA kan beskrivas som en individs medvetenhet om informationssäkerhet (Bulgurcu, Cavusoglu, & Benbasat, 2010), och är enligt Aldawood och Skinner (2018) en väsentlig del av individers och organisationers informationssäkerhet. I dagsläget besitter individer stora mängder känslig information vilket kan innebära risker om denna information inte hanteras på ett säkert sätt. Det är därför av stor vikt att kontinuerligt träna sin medvetenhet inom informationssäkerhet för att minimera dessa risker (Aldawood & Skinner, 2018). Det finns en mängd studier som visar på att den individuella medvetenheten om informationssäkerhet i relation till social engineering är generellt sett låg. Användandet av e-hälsoapplikationer har under den senaste tiden ökat markant, och är enligt Aldawood & Skinner (2018) ett praktexempel där användare inte är medvetna om de risker som finns vid en informationsläcka. Användarna har inte kunskap angående de tekniker som bedragare använder sig av, eller vilka risker som finns, om informationen skulle hamna i fel händer. Av den anledningen bör åtgärder vidtas för att träna användare angående informationssäkerhet, för att öka säkerheten vid användandet av informationskänsliga applikationer (Aldawood & Skinner, 2018).

2.4 Tillit och sårbarhet

2.4.1 Tillit till teknologier

Att människan känner en tillit till teknologier är något som Lankton, McKnight och Tripp (2015) inte bedömer är förvånande. Dagligen förlitar sig människan på teknologiska skapelser såsom att bilen kommer fungera felfritt när den körs, att alla broar vi kör på kommer hålla, och att orderhanteringssystem sparar dokument åt oss automatiskt. Lankton et al., (2015) hävdar att diskussionen kring tillit till teknologier historiskt sett har varierat. Vissa studier pekar på att tillit till teknologier är obefintlig, medan andra hävdar att motsatsen. Däremot har flera forskare under den senaste tiden börjat erkänna att det finns en mänsklig tillit till vissa teknologier som används (Lankton et al., 2015). Författarna Lankton et al., (2015) kategoriserar teknologier i två olika grupper; 1) teknologier med människoliknande

funktioner, 2) teknologier med systemliknande funktioner. Människoliknande funktioner innefattar system eller program som interagerar med individer genom text, röst eller animationer. Systemliknande funktioner saknar dessa integrerande delar, och är istället byggda för att genomföra en specifik uppgift. Lankton et al., (2015) hävdar att individer har en större chans att skapa tillit till system eller applikationer med människoliknande funktioner.

Detta prövades i en undersökning där ett flertal användare fick använda system med människo- och systemliknande funktioner. Forskarna valde *Facebook* som den teknologi med mer människoliknande funktioner, och *Microsoft Access* som den teknologi med systemliknande funktioner (Lankton et al., 2015). Undersökningen som Lankton et al., (2015) utförde bekräftade deras tes, användare hade en större tillit till teknologier med människoliknande funktioner. Användarna som deltog i studien hade en högre mänsklig tillit till Facebook i och med de mänskliga drag som plattformen innehåller, i form av exempelvis bilder och personliga textmeddelanden.

Det är ofta när pengar blir inblandade som tilliten prövas. Detta var även fallet för näthandeln som i början av 2000-talet fullständigt exploderade. Postnord släpper årligen en rapport om E-handeln i Norden. Den genomsnittliga uppskattade köpesumman per person ökade från *485kr* till *2060kr* under perioden 2008–2018 (Postnord, 2018).

Näthandeln involverade konsumentens finanser och ställde högre krav på tekniskt säkra lösningar. Friedman, Khan Jr, och Howe (2000) skriver i sin artikel *Trust Matters* att *"People trust people, not technology".* Vidare diskuteras även vilka kriterier som måste uppnås för att skapa tillit för sin plattform. Säkerhetscertifiering och revision av externa parter är ett av dessa kriterier (Friedman et al., 2000). *Trustarc* är ett företag som bland annat arbetar med säkerhetsrevision, vid e-handel stöter man ofta på deras TrustE certifiering. Friedman, et al menar att det här kriteriet bidrar till en false sense of security, både för att det är svårt att verifiera att certifieringen är äkta men även då *Trustarc* kritiserats för att ha varit frikostiga med sin säkerhetsstämpel (Friedman et al., 2000).

Eftersom många av de svenska storbankerna gemensamt står bakom BankID bidrar det troligtvis till att applikationen får högre trovärdighet hos användarna. Utöver detta betraktas BankID som tekniskt säker identifieringsplattform.

2.4.2 Äldre utgör en sårbar grupp

Enligt Petra Stenkula (Andersson & Lärka, 2019), chef för polisens utredningsenhet utgör äldre en sårbar grupp för BankID-bedrägerier. Detta bekräftas även om man tittar på mer generella siffror angående telefon- och internetbedrägerier.

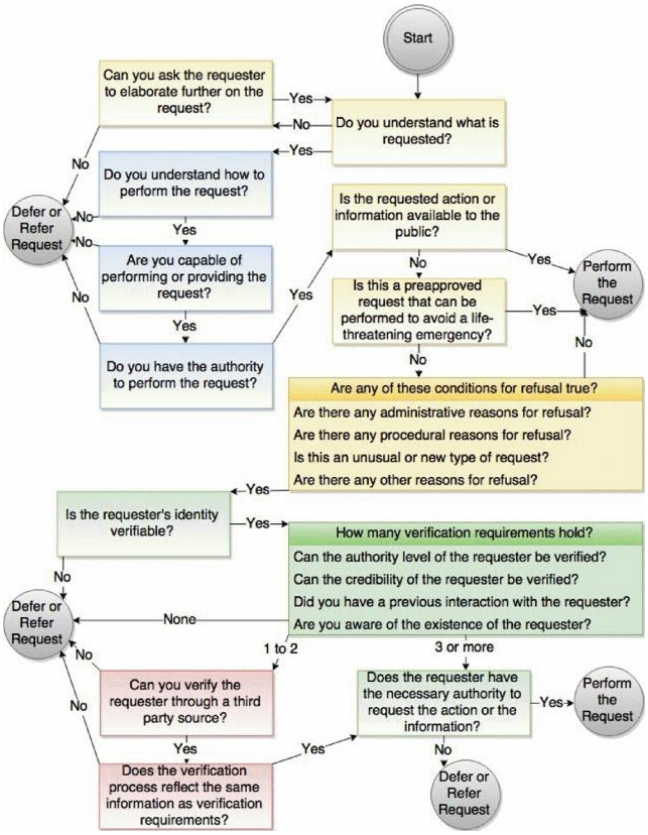
Brottsförebyggande Rådet släppte 2016 en rapport kring bedrägeribrottsligheten i Sverige. BRÅ har granskat bedrägeriärenden från första halvåret 2013 och fastslagit en medianålder hos offer på 54 år för kategorin "Övrigt telefon- eller internetbedrägeri" (BRÅ, 2016) Troligtvis väljer bedragarna att rikta in sig på äldre offer eftersom det bland dem finns en större brist på teknisk kompetens.

2.5 Social Engineering Attack Detection Model: SEADMv2

Författarna Mouton, Leenen och Venter (2015) skapade 2010 modellen SEADM vars syfte var att underlätta identifieringen av SE-attacker i situationer där individer på callcenter blir utsatta. 2015 skapades en reviderad version av modellen (SEADMv2) som går att applicera generellt på alla typer av SE attacker. Tidigare forskning inom detta område handlar mestadels om att utbilda användare i syfte att motverka SE-attacker. SEADMv2-modellen är av den anledningen unik i och med att det ger ett konkret förslag på hur man som individ kan försöka identifiera SE-attacker, oberoende av tidigare utbildning (Mouton et al., 2015).

Modellen använder sig av ett beslutsträd för att bryta ner en förfrågan i mindre beståndsdelar, syftet med detta är att underlätta beslutsfattandet i situationer där en förfrågan genom mail, telefon eller brev inkommer (se figur 5). En förfrågan som kommer in kan exempelvis vara ett försök till att få ut information kring en organisation, eller en lösenordsåterställning (Mouton et al., 2015). Modellen tar upp fyra olika aktörer; förfrågan, mottagaren, den som ger förfrågan och slutligen tredjepart. Dessa aktörer har enligt modellen olika roller i beslutsträdet, de gula rutorna i modellen representerar informationen i själva förfrågan. Mottagaren representeras av de blå rutorna i modellen, och berör individen som hanterar förfrågan och huruvida denna person är kapabel till att genomföra det som efterfrågas. De gröna rutorna berör den som förmedlar förfrågan, vilket kan vara en bedragare, och huruvida den som förmedlar förfrågan går att verifiera. Slutligen representeras tredjepart av de röda rutorna, och beskriver i vilken mån den som ger förfrågan går att identifiera med hjälp av en extern källa (Mouton et al., 2015).

Beroende på hur de olika frågorna besvaras i modellen följer användaren beslutsvägarna genom modellen. Avslutningsvis leder modellen till två olika alternativ; användaren kan avvisa förfrågan eller genomför förfrågan. Förfrågan avvisas i situationer där mottagaren inte kan verifiera att individen som har förmedlat förfrågan har rätt i att få ut informationen. Om det däremot går att bekräfta att den som har förmedlat förfrågan, genomförs åtgärden (Mouton et al., 2015).



Figur 5: Modell SEADMv2 (Mouton, Leenen & Venter. 2015, s. 217)

2.6 Undersökningsramverk

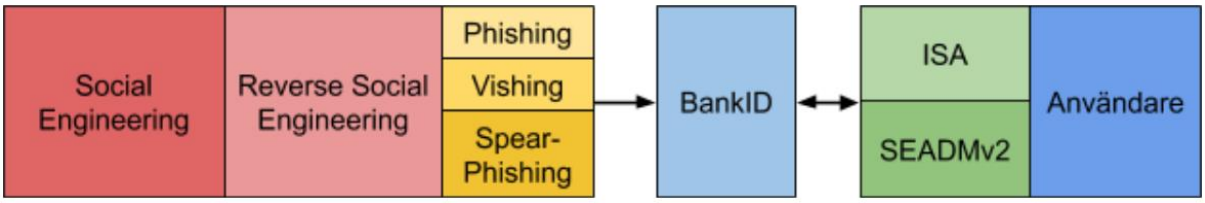
I detta stycke kommer undersökningsramverket presenteras och även visualiseras (se figur 6 nedan) för att påvisa kopplingen mellan litteraturgenomgångens delar.

Ämnet som denna undersökning utgår från är BankID-bedrägerier, hur de kan motverkas och i vilken utsträckning det kan kopplas till social engineering. Av den anledningen har författarna till denna rapport försett läsaren med en övergripande förklaring av social engineering. Vidare förklaras ett antal tillvägagångssätt som bedragare använder sig av.

Mann (2008) beskriver SE som konsten att manipulera människor för att få ut information, eller för att få dem att utföra en åtgärd. Social engineering representeras av den röda rutan i modellen. Inom SE ingår ett flertal hjälpmedel och tillvägagångsätt som representeras i rutorna *reverse social engineering*, *phishing*, *vishing* och *spear-phishing*.

De utsatta individerna representeras av rutan som benämns som användare. Ur de artiklar och rättsfall som presenteras i denna studie framgår det att individer ofta inte är medvetna om att de har utsatts för bedrägeri, vilket visar på att medvetenhet är en betydande faktor i huruvida dessa attacker lyckas eller inte. Av den anledningen har ISA redogjorts, en teori som beskriver i vilken utsträckning medvetenhet inom informationssäkerhetsträning kan skydda individer från SE-attacker (Bulgurcu et al., 2010). Genom kontinuerlig träning kan individer identifiera risker med användandet av vissa applikationer, vilket minskar sannolikheten att bli utsatt (Aldawood & Skinner, 2018).

Utöver ISA har innehållet i modellen SEADMv2 redogjorts och förklarats. Modellen är högaktuell i denna studie då det ger en konkret bild över hur man som individ praktiskt kan gå tillväga vid misstänksamhet. Genom att besvara ett antal frågor guidas användaren genom ett beslutsträd, vilket i slutändan uppmuntrar till att avvisa eller genomföra en förfrågan som kommer från en extern part (Mouton et al., 2015).



Figur 6: Undersökningsramverk.

Nedan kategoriseras källorna baserat på vad de berör.

Tabell 1: Litteratursammanställning.

Tema	**Kategori**	**Faktorer**	**Litteratur**
Informationssäkerhet	Social Engineering	• Faser • Reverse SE • Phishing • Spear-Phishing • Vishing	Mann (2008), Kaushalya et al., (2018), Krombholz et al., (2015), Ivaturi & Janczewski (2011), Hadnagy (2011), Granger (2001), Jagati et al. (2007), Yeboah-Boateng & Amanor (2014)
Informationssäkerhet	Medvetenhet hos användare	• ISA	Aldawood & Skinner (2018)
Informationssäkerhet	Användare	• Tillit	Friedman, et al. (2000), Lankton et al., (2015)
Informationssäkerhet	Motverka attacker	• ISA • SEADMv2	Mouton, Leenen & Venter (2015), Aldawood & Skinner (2018)
Attack-kanal	Applikation	• BankID	Finansiell ID-Teknik BID AB (2019)

3 Metod

3.1 Utformning av litteraturstudie

Litteratur- och informationshantering är enligt Rienecker och Stray Jørgensen (2014) viktiga komponenter i en akademisk text, och hur litteraturen används kommer i sin tur påverka utformandet av själva studien. För att finna relevant litteratur till denna studie har en hybrid av sökmetoderna systematisk sökning och kedjesökning tillämpats. Den systematiska sökmetoden innebär att elektroniska hjälpmedel såsom Google Scholar har använts, och att sökningar gjorts på specifika ämnen eller nyckelord för att hitta litteratur och information (Rienecker & Stray Jørgensen, 2014). Denna metod användes främst i uppstartsfasen av denna studie för att ge en bred överblick i ämnet. Kedjesökningsmetoden har även använts när relevant litteratur för sammanhanget har påträffats (Rienecker & Stray Jørgensen, 2014). Författarna till denna studie har genom referenslistan till artiklar och böcker funnit mer relevant litteratur, som sedan har använts i litteraturgenomgången. För att finna specifik litteratur har sökmotorn Google Scholar använts. Google Scholar ger genom sin funktion antal "citeringar" indikationer på vilka artiklar som är pålitliga. För att få tillgång till dessa texter har databashanteraren LUBsearch använts. Exempel på söktermer som har använts har varit följande; SE, SE methods, SE telephone, SE Attacks, Security awareness, SE detection model, BankID, Bedrägerier BankID, E-ID och E-legitimation.

För att finna relevanta domar som berör bedrägerier kopplade till BankID har databashanteraren Karnov använts. Databasen har möjliggjort för en smidig sökning på begreppen bedrägeri och BankID för att få fram relevanta texter till denna studie.

Vetenskapliga böcker har legat till grund för att förstå SE på ett bredare plan. Vetenskapliga artiklar, nyhetsartiklar, hemsidor samt rättsfall har använts som kompletterande medel för att samla in relevant information kring attacker, offer och applikationen BankID. Rienecker och Stray Jørgensen (2014) menar att artiklar kompletterar böcker på ett bra sätt då dessa oftast är mer aktuella.

3.2 Metodansats

Enligt Rienecker & Stray Jørgensen (2014) finns det två övergripande sätt för att utforma en empirisk undersökning, vilka är kvalitativ eller kvantitativ empiri. Kvantitativ data är den information som kan beskrivas och presenteras genom tal, mängd och storlek. En kvalitativ metod handlar enligt Larsson (1986) mer om att karaktärisera eller gestalta något, och fungerar bra i situationer där man försöker hitta modeller eller beskrivningar som bäst redogör för ett fenomen i ett sammanhang i omvärlden. Då den huvudsakliga forskningsfrågan i denna studie är en explorativ fråga kommer en kvalitativ metod användas. Detta kommer att resultera i en mer omfattande bild över SE i relation till e-legitimationsbedrägerier.

Alvehus (2013) menar att intervjuer är ett kraftfullt verktyg i kvalitativa undersökningar. Man ska däremot använda intervjuer med försiktighet då de kan verka autentiska, men inte alltid stämmer överens med det verkliga sammanhanget. Däremot är det en kraftig metod då det ger en inblick i andra individers verklighetsuppfattning, vilket kan ge tillgång till nya åsikter och tankegångar som bidrar till studien positivt (Alvehus, 2013).

3.3 Utformning av intervjufrågor

Intervjufrågorna som tillämpas i den empiriska undersökningen grundar sig i litteratursammanställningen som har presenterats i tidigare kapitel. Syftet med detta är att ge en tydlig bild av bedrägerier kopplade till BankID. Genom att grunda frågorna i det som har presenterats i litteraturgenomgången anser vi att den empiriska studien berör ett brett spektrum av faktorer som har en påverkan på bedrägerierna. Dessutom kommer detta möjliggöra för en effektiv analys och diskussion då de svar som anges i intervjun kan ställas direkt mot litteratursammanställningen.

I denna studie har intervjuerna varit semistrukturerade, med ett flertal öppna frågor som uppmuntrar till ett bredare samtalsämne. I denna typ av intervju får respondenten större utrymme att styra intervjun, vilket innebär att det är väsentligt att den som håller i intervjun har förmågan att lyssna och ställa motfrågor för att uppmuntra respondenten att vidareutveckla sina svar (Alvehus, 2013). Se appendix 1 för fullständiga intervjufrågor.

Nedan följer en tabell som visar vilka källor som utgör vilka intervjufrågor.

Tabell 2. Överblick intervjufrågor och teori.

Teori	**Författare**	**Intervjufrågor**
Social Engineering Faser metoder	Mann (2008), Kaushalya et al., (2018), Krombholz et al., (2015), Ivaturi & Janczewski (2011), Hadnagy (2011), Granger (2001), Jagati et al. (2007), Yeboah-Boateng & Amanor (2014)	1–3. 7–12.
Användare Medvetenhet Tillit	Aldawood & Skinner (2018), Friedman, et al. (2000), Lankton et al., (2015)	13–17.
BankID	Finansiell ID-Teknik BID AB (2019)	4–6.
Motverka attacker ISA SEADMv2	Mouton et al., (2015), Aldawood & Skinner (2018)	18–21

3.4 Urval av intervjuobjekt

För att kunna besvara den huvudsakliga forskningsfrågan har vi strävat efter att intervjua individer med hög kompetens inom området bedrägerier, såsom anställda på banker som arbetar med frågor som är relaterade till eller med e-legitimation. Då denna studie ska beskriva vad BankID kan göra för att motverka bedrägerier är det av stor vikt att rätt personer med rätt typ av kompetens deltar i intervjustudien. Insikt, kunskap och förståelse kring problematiken anses enligt oss vara väsentliga delar för att få trovärdiga och riktiga svar på intervjufrågorna, vilket också medför bättre resultat när själva forskningsfrågan ska besvaras. Relevanta intervjuobjekt har påträffats genom nyhetsartiklar och intervjuer som är tillgängliga via internet. Efter en övergripande granskning av yrke, titel och roll på organisationer skickades en förfrågan ut till individer som ansågs kunna bidra till denna studie.

Nedan presenteras intervjurespondenterna i tabellform.

Tabell 3: Respondenter.

Respondent	Yrke	Tid	Längd	Plats	Typ
Jan Olsson	Polismyndigheten, Bedrägericentrum	29/4–2019	47 min	Lund	Telefon
Boris Berberovic	Secventia	7/5–2019	55 min	Lund	Google Hangout
Albin Zuccato	ATEA, Nationell affärsområdeschef säkerhet	20/5–2019	34 min	Lund	Telefon

Jan Olsson, som arbetar på Polismyndighetens nationella IT-brottscentrum utreder dagligen bedrägerier i sitt arbete, han har stor insyn tillvägagångssätt och metod. Han har också varit ansiktet utåt för polisen i många nyhetsartiklar relaterade till BankID-bedrägerier.

Boris Berberovic, är grundare till IT-säkerhetsföretaget Secventia och skriver för tillfället ett white-paper angående bedrägerier kopplade främst till bankdosor, men även BankID.

Albin Zuccato, arbetar som nationell affärsområdeschef inom säkerhet på IT-företaget ATEA. Han har en bred kunskap kring tekniska lösningar för att förbättra informationssäkerheten i system.

Vi har haft som avsikt att intervjua individer som arbetar inom banksektorn, exempelvis från BankID eller någon av de utfärdande bankerna. Sju av elva utfärdande banker har blivit tillfrågade att medverka i denna studie, men på grund av sekretess eller resursskäl har samtliga tackat nej. Detsamma gäller för BankID som inte ville medverka. Detta påverkar studien då bankernas perspektiv inte kan presenteras, vilket i vår mening hade genererat ett mer fullständigt svar på forskningsfrågan.

3.5 Analysmetod

Enligt Alvehus (2013) kan en intervju sammanställas genom inspelning och transkribering, eller med minnesanteckningar som utvecklas strax efter intervjun är genomförd. Det finns för- och nackdelar med dessa metoder, då inspelningar kan ses som ett störningsmoment för respondenten, och kan innebära att svaren inte alltid är helt uppriktiga. Att enbart ta anteckningar kan kringgå denna problematik, däremot kan det som sägs ändras på vägen vilket är en risk. Det är vad intervjuaren hör och vill höra som antecknas ner, vilket även kan påverka uppriktigheten (Alvehus, 2013).

I syfte av att säkerställa att de svar som respondenterna ger uppfattas på rätt sätt, och tolkas ord för ord, valde vi att spela in samtliga intervjuer, för att sedan transkribera dem. Detta medför att resultatet blir objektivt presenterande då vi inte påverkar innehållet med våra

förutfattade meningar. Intervjuerna har i största mån transkriberats ord för ord, däremot har mindre korrigeringar gjorts i språket för att generera ett bättre flyt i textform.

Då intervjufrågorna baseras på informationen som presenteras i litteraturgenomgången bidrar det till att analysen får en tydligare struktur. Svaren har kategoriserats under de rubriker som presenteras under *teori* i tabell 2. Genom denna kategorisering kan respondenternas svar ställas direkt mot informationen i litteraturgenomgången för analys och diskussion. För att upprätthålla en tydlig struktur återanvänds samtliga rubriker som återfinns i tabell 2 i resultatanalys- och diskussionskapitlet.

3.6 Etik

Informationssäkerhet är i ett känsligt ämne då det oftast berör känslig information som i fel händer kan missbrukas och kan medföra till att personer råkar illa ut. Detta beskrivs tydligt i litteraturgenomgången där det framgår flera exempel på vad som kan hända när en individ blir utsatt av en SE attack. I studien presenteras exempel på situationer på när individer är oaktsamma på internet, samt rättsfall där individer har utsatts för bedrägerier av den art som presenteras i litteraturgenomgången. Av etiska skäl har vi valt att anonymisera dessa individer och diskuterar enbart kring själva situationen och sammanhanget.

Av forskningsetiska skäl informerades samtliga intervjuobjekt innan intervjuns start angående själva studien i helhet samt själva syftet med deltagandet. Den medverkande fick veta att deltagandet var helt frivilligt, och att intervjun kunde avbrytas när som helst. Med respondentens samtycke spelades även intervjuerna in för att möjliggöra transkribering i efterhand, och en kopia av transkriberingen skickades därefter till respondenten.

3.7 Reliabilitet och validitet

För att säkerställa en hög grad av reliabilitet och validitet har vi ansträngt oss för att vara objektiva i vår informationsinsamling och analys. I frågan om reliabilitet, vilket är att säkerställa att resultaten är konsekventa över tid samt att studien kan genomföras vid ett annat tillfälle med liknande metod (Golafshani, 2003), har tidigare kunskap inom ämnet i största möjliga utsträckning undvikits för att inte färga diskussionen eller resultatet. Genom att grunda den empiriska undersökningen på den omfattande litteraturgenomgången anser vi att studien fått en tydlig röd tråd, och ger läsaren alla medel som är nödvändiga för att följa den tankegång som vi haft under arbetets gång. Då empirin bygger på kvalitativa intervjuer är det nödvändigt att intervjua ett flertal respondenter för att få en tydlig helhetsbild då uppfattningen angående ett särskilt ämne kan skilja sig väsentligt mellan olika individer. På grund av tidsbrist, problematik med avhopp samt att få kontakt med vissa intervjuobjekt har antalet respondenter inte nått upp till det önskade antalet för denna studie. Av den anledningen sjunker dessvärre reliabiliteten då svaren som genererats i den empiriska studien kan skilja sig om samma studie utförs på nytt med andra respondenter.

För att säkerställa en hög grad av validitet i studien har tre subkategorier analyserats under studiens gång; hantverksvaliditet, kommunikativ validitet och pragmatisk validitet (Alvehus, 2013). Hantverksvaliditet innebär att kontinuerligt under arbetets gång ifrågasätter rimligheten i sin analys, vilket applicerats på samtliga delar av studien. Kommunikativ

validitet innebär att det kunskapsspråk som används testas i dialog. Detta har utförts tillsammans med de respondenter som tagit del i studien. Den sista subkategorin pragmatisk validitet innebär att kunskapen blir relevant om den i någon mån kan påverka samhället.

3.8 Metodreflektion

Vi har valt att göra en intervjustudie bestående av personer som har goda kunskaper inom fältet IT-säkerhet samt BankID-bedrägerier. För att få ytterligare förståelse angående hur bedrägerierna går till har vi kombinerat användandet av vetenskapliga texter, rättsfall, intervjuer och nyhetsartiklar. Eftersom alla dessa källor agerar som ett filter mellan offret och förmedlaren av informationen, hade vi kunnat få en fördjupad förståelse om vi hade kommit närmare användaren av systemet tillika brottsoffret. Detta hade exempelvis kunnat göras genom enkätundersökningar eller ett annat urval av intervjuobjekt. Om vi istället valt att göra en enkätstudie hade vi erhållit en större mängd data (respondenter) vilket hade ökat validiteten. Antalet frågor och längden på de intervjuer som vi genomfört påverkar också resultatet. Genomsnittstiden på våra intervjuer var 45 minuter och antalet intervjuer tre. Ovan i tabell 2 ges en överblick över intervjuobjekt. För intervjufrågorna, se appendix 1.

4 Empiri och resultatanalys

4.1 Social engineering: Faser och metoder

Definitionen av SE som denna studie bygger på härstammar från Mann (2008) vilket är; att manipulera människor genom vilseledning för att få ut information, eller få individen att utföra en åtgärd. Som ett inledande steg i den empiriska undersökningen blir samtliga respondenter tillfrågade om de delar samma uppfattning av begreppet SE. Det huvudsakliga syftet med detta är att samtliga parter ska utgå från samma definition. Frågorna 1 till 3 (se appendix 1) berör respondentens uppfattning om SE, samt om de bedrägerier som utförs via BankID kan ses som någon form av SE.

"Ja helt rätt, plattformarna för det kan vara allt från mail eller annat, men det är så jag ser det utan att ha slagit upp det" - (Jan Olsson).

I frågan huruvida metoderna bedragarna använder sig av vid BankID-attacker räknas som en form av SE var intervjuobjekten överens.

"Ja [...] *det är definitivt social engineering. Det är en förädlad form i och med att de använder sig av telefonen för att lura människor. Men absolut Social engineering är ett fundament som ligger bakom de mesta av den vilseledande brottsligheten" - (Jan Olsson).*

"Ja absolut, men jag skulle också betrakta det som en bug [...] *som en brist i systemet" - (Boris Berberovic).*

"Ja man ger sig knappast mot själva algoritmen eller tekniken, utan man ger sig mot den svaga länken, och det är ju människan. Så det är absolut en social engineering attack."- (Albin Zuccato).

Boris Berberovic, grundare till IT-säkerhetsföretaget Secventia, menar att dessa attackmetoder kan ses som en form av SE. Han poängterar dock att det även rör sig om generella brister i applikationen vilket möjliggör att dessa typer av bedrägerier är genomförbara.

Respondenterna blev även tillfrågade om konkreta exempel på när de stöter på social engineering utifrån sin yrkesroll. Jan Olsson, som arbetar på Polismyndighetens nationella IT-brottscentrum kommer i kontakt med alla möjliga typer av bedrägerier på en daglig basis. Enligt honom inkommer årligen ungefär 260 000 anmälningar som berör bedrägerier. Ungefär 200 000 av dem menar Olsson berör just SE. Majoriteten är misslyckade försök till bedrägerier.

"200 000 anmälda fall ute i Sverige som har med social engineering att göra. Men nu höftade jag bara, det kan vara mycket mer" - (Jan Olsson).

Stulna kortuppgifter som säljs vidare, utgör enligt Olsson det största enskilda brottet i Sverige. Eftersom bedragarna genom olika metoder lyckas få tag på stora mängder kontokort, förekommer det en svart marknad av kontokortsinformation på DarkWeb.

"Busarna i sin tur tar dessa kortuppgifter och säljer dessa. Sedan så köper dom (de som köpt kortuppgifterna) saker på internet. Du får fakturan och han får brallorna från Zalando. Och detta är ju också SE, och det är det största enskilda brottet vi har [...]*" - (Jan Olsson).*

Bortsett från de enklaste former av bedrägerier förekommer det också något som Olsson kallar för avancerad SE. Romansbedrägerier är ett exempel. Bedragaren ingår i ett förhållande för att slutligen lura den andra parten på pengar eller egendom. Denna art av bedrägerier har under den senaste tiden ökat, enligt Olsson beror detta främst på internet och alla sociala plattformar som följer med.

"Det ökar så förbannat är för att det finns en så stor social plattform att utgå ifrån och det är ju internet och dess innehåll, facebook eller dating-siter och allt det kan vara. Alla har en dator som är uppkopplad till nätet och antalet plattformar på nätet att använda ökar explosionsartat så ökar självklart också brotten." - (Jan Olsson).

Albin Zuccato, som är affärsområdeschef inom säkerhet på IT-företaget ATEA, stöter också på SE både som privatperson och i sitt dagliga arbete.

"Ja, man kan säga att man är en användare och då är man ju utsatt i alla fall för riktad phishing attack (spear phishing) och såklart i diskussion med kunderna så nämns social engineering attackerna som ett frekvent förekommande beteende." - (Albin Zuccato).

Intervjufrågorna 7 till 10 (se appendix 1) berör tillvägagångssätt och faser inom SE. Utifrån intervjusvaren framgår det att mycket av den information som är nödvändig för bedragaren finns på internet. När det kommer till bedrägerier som görs via BankID behövs namn och personnummer till offret. Olsson ser en problematik i detta, då vi i Sverige har offentlighetsprincipen. Exempelvis personnummer är en offentlig handling, vilken bedragaren kan få ut via flera kanaler på internet.

"I början när man ringde angående BankID när de själva loggade in med offrets personnummer, innan den gjordes visste man vad offret hade för personnummer, och det är ju en offentlig uppgift." - (Jan Olsson).

Detta bekräftar även Berberovic. Han exemplifierar genom att ge ett konkret scenario kring hur denna informationsinsamling kan ske. I Sverige finns det mängder av öppna databaser med generell information om svenska invånare. Genom denna information kan man urskilja vilka invånare som är över 65, samt vilka som har en hög pension. Enligt Berberovic har majoriteten av alla pensionärer konton hos Swedbank eller Nordea, vilket innebär att bedragare kan chansa mellan dessa banker vid vishingbedrägerier.

"Nordea och Swedbank är de största bankerna där du har ett personkonto, och då är det väldigt enkelt att säga, hej jag ringer från Swedbank, så ringer man en annan gång och säger att man ringer från Nordea, det är antingen eller, så har man 50/50 chans att lyckas." - (Boris Berberovic).

Berberovic ger även ett exempel på hur denna typ av informationsinsamling kan försvåras. Han anser att en spårbarhet bör införas, där individer som begär ut offentliga handlingar behöver identifiera sig, i syfte att polisen i efterhand ska kunna urskilja vem som begärt ut dem.

"[...] *när man vill få ut offentliga handlingar, man ska inte få dom anonymt, man ska verifiera sig. I kombination ska det finnas en spårbarhet i detta. Detta ger sedan polisen möjligheten*

att säga; okej, den här personen har blivit utsatt för brott. Vem är det som har tagit ut offentliga handlingar?" - (Boris Berberovic).

Berberovic avslutar denna analys med att diskutera GDPR. Den relativt nya lagen har inte i dagsläget trätt i fullständig kraft, vilket han menar är bidragande till att det fortfarande går att få ut en mängd personlig information. GDPR fastställer att den personliga integriteten är grundläggande, och detta menar Berberovic kan leda till att vissa tjänster som lagrar stora mängder personlig information inte kommer att finnas kvar.

Albin Zuccato menar att bedragare skjuter ganska brett under informationsinsamlingsprocessen, för att kunna filtrera ut individer med en lägre teknisk kompetens. Detta görs via olika typer av kanaler, och Zuccato håller med resterande respondenter i att sociala medier och sökmotorer är verktyg som bedragare kommer långt med. Däremot är Zuccato inte helt övertygad att detta offentlighetsprincipen är avgörande för informationsinsamlingen.

"Nej, phishing förekommer även i andra länder, inte tvär-nej men jag skulle inte säga att det (offentlighetsprincipen) förvärrar eller förenklar saken. Det finns gott om information tillgänglig även utanför offentlighetsprincipen." - (Albin Zuccato).

I frågan om vilka konkreta metoder som bedragare använder sig av vid SE attacker kopplade till BankID är respondenterna eniga i att vishing, är den mest förekommande metoden.

"Det är den absolut bästa vägen till att göra det eftersom man får en fysisk kontakt med offret. Då får man mycket större förtroende, dom som ringer har ofta en ganska stor erfarenhet av företag, eller av den typen av verksamhet där man suttit i ett callcenter. [...] Vishing är mer sofistikerat, det är mer personligt eftersom man får den här kontakten med personen" - (Boris Berberovic).

4.2 Användare: Medvetenhet och tillit

Denna studie berör den mänskliga faktorn i relation till bedrägerier som utförs med hjälp av BankID. Det framgår i litteraturgenomgången att individen är den svaga länken i en teknologisk värld och att säkra upp denna aspekt kan visa sig vara mycket komplicerad. Fråga 8 (se appendix 1) berör vilken målgrupp som är den mest förekommande vid denna typ av bedrägeri, medan intervjufrågorna 13 till 17 (se appendix 1) tar upp användarens roll i bedrägerier som utförs med hjälp av BankID, samt vilka mänskliga faktorer som har en direkt påverkan.

Boris Berberovic anser att äldre individer utgör den största målgruppen som blir utsatta av bedrägerier kopplade till BankID. Detta beror sannolikt på att de inte har introducerats till ett säkert användande av applikationen, samt har en bristande riskmedvetenhet. Det saknas enligt Berberovic en grundläggande misstänksamhet gentemot teknologier. Dessutom är den äldre generationen generellt mer godtrogna, de tenderar att lita på personer som ringer.

Här har dock Zuccato och Olssons en annan uppfattning. Enligt dem beror det på en gammal missuppfattning.

"Det rapporteras en hel del om attackerna mot äldre [...]. Äldre faller offer mer frekvent då tekniken är mer främmande för dom, jag tror det är en omvänd korrelation. Jag tror inte att man singlar ut dom från början utan det handlar mer om selektionsmekanismer." - *(Albin Zuccato).*

"Nä men det där tror jag är en sån där gammal missuppfattning, om vi tänker på hur rovdjur jobbar ute på savannen så fokuserar man ju på de svaga individerna i flocken. Det där har ju satt sig på hjärnan hos intelligenta varelser som ska tjäna pengar på bedrägerier. Och då tror dom att man måste angripa de äldre för de måste vara dom svagaste och mest lättlurade som vi har i samhället, därför finns det en överrepresentation av den personen i målgruppen." - *(Jan Olsson).*

Olsson och Zuccato bekräftar alltså att det finns en överrepresentation hos den äldre generationen, däremot anser de att det beror på att ett gammalt tankesätt. Enligt Olsson löper den yngre generationen lika stor risk att bli utsatta för bedrägerier, men detta är inget bedragare har insett.

Denna studie har diskuterat begreppet ISA, vilket beskriver i vilken mån medvetenhet spelar roll inom ramen för informationssäkerhet. I frågan huruvida medvetenhet hos användarna spelar en direkt roll i SE attacker menar samtliga intervjuobjekt att det absolut har en påverkan.

"*Det är klart som sjutton att det betyder jättemycket. Sedan är det en stor skillnad på att vara medveten och efterleva dom. Jag tror alla är medvetna om att man ska ha säkra lösenord och sådär och att man ska ha ett sånt där lösenordsprogram där man samlar alla lösenord. Men hur många har det egentligen?"* - *(Jan Olsson).*

"Det är den största bristen absolut. De tre stora bristerna är; avsaknad av medvetenhet hos offret, avsaknad av kompetens hos polisen och de utredande myndigheterna, och även brister hos tjänsteleverantören vilket i detta fall är BankID [...] *Det enklaste är att öka medvetenhet hos kunderna. Det är den största bristen om jag rangordnar dom"* - *(Boris Berberovic).*

"Till en otroligt hög grad, man måste gå över en viss gräns. Har man blivit utbildad med någon form av medvetenhetsträning eller snarare om man har någon form av medvetenhet så är jag ganska övertygad att man inte skulle gå på. Det krävs en hel del osäkerhet för att gå på dessa punkter. Det har oftast att göra med man inte har full koll på vad som gäller." - *(Albin Zuccato).*

Detta belyser en problematik med dagens användande av teknologiska lösningar. Det finns oftast en generell medvetenhet om riskerna med användandet av vissa applikationer, och att man ska undvika misstänksamma mail med länkar. Däremot går människor dessvärre fortfarande på SE-relaterade bedrägerier.

"Man ska försöka ha med sig det (medvetenhet), men att vara 100% på det viset klarar inte ens jag av." - *(Jan Olsson).*

Intervjuerna berörde även relationen mellan medvetenheten hos användarna och "success rate" hos bedragarna. Enligt Olsson har polismyndigheten och bankerna jobbat mycket med *awareness* kampanjer för att öka medvetenheten hos användare av monetära applikationer.

"Ja det gör det ju. Tittar vi på vishing, där körde vi jättemycket med awareness kampanjer där vi varna för det här. När vi hade börjat med det såg vi i statistiken att brotten ökade, men

antalet lyckade försök minskade. Och då kan man läsa i dessa anmälningar att "jag hade sett på tv" eller "jag hade hört på radio" att det var någon som stod och tjata om det här." - (Jan Olsson).

Detta visar på att ökad medvetenhet är ett medel för att minska antalet fullföljda försök till bedrägerier kopplade till BankID. Informationskampanjer är enligt Olsson ett konkret exempel på något som han vet fungerar för att minska bedrägerier. Awareness är enligt Olsson nyckeln, däremot poängterar han att det finns forskning som visar på att det enbart är 10% av alla människor som lever efter uppmaningarna.

"Utan jag tror att på awareness absolut, sedan ligger det ett jättestort ansvar på produktägaren. Om jag ska ge ut ett nytt bankkort eller BankID, då ligger ett jättestort ansvar på mig att jag informerar dom som ska ta emot det här, vad det innebär och hur man ska handskas med det, och vilka farorna är. Och detta kommer i alla fall bara räcka en viss bit. Men återigen om man lyckas hindra att 1000 blir brottsoffer är det bättre än att inte hindra någon." - (Jan Olsson).

Albin Zuccato är också övertygad om att det finns en relation mellan medvetenheten hos användarna och "success rate" hos bedragarna, och att produktägaren har ett stort ansvar i att förmedla information angående säker användning av applikationer. Genom att förmedla denna information anser Zuccato att produktägaren kan visa på att online betalning är något fördelaktigt och mycket positivt. Däremot poängterar han att även en tränad användare kan bli lurad då vissa av bedragarna är väldigt skickliga.

Zuccato menar också att det finns ett generellt samhällsproblem som påverkar detta, vilket är *information overflow*. Vid en installation av en applikation är det tänkt att användarvillkor ska läsas, vilket Zuccato menar är något som användare struntar i.

"[...] *information overflow som är en del av vårt moderna samhälle som man framförallt som konsument är utsatt. Det innebär ju att man har inte ork eller möjlighet att ta del av all den informationen som behövs. Inom konsumentskyddslagen har vi identifierat detta och börjat skydda individen bättre och en del typ av lagstiftning kan behövas i det området." - (Albin Zuccato).*

Detta är enligt Zuccato det främsta problemet i att viktig information som är tänkt att höja medvetenheten hos användare missas. Användare har i dagsläget som vana att strunta i att läsa användarvillkor, vilket enligt Zuccato är en brist och resulterar i att varningar förbises.

Tillit är ett begrepp som har diskuterats i denna studie, och det berör här främst tillit till all den teknologi som laddas ner till personliga enheter. Respondenterna har under intervjun blivit tillfrågade om detta och hur de ser på den tillit som finns till olika applikationer.

"Det är ju det som är problemet. Bara för att vi tror oss ha en säker applikation så går vi fria från alla problem. Så är det ju inte utan det är ju hur vi använder applikationen. Och här går den digitala utvecklingen alldeles för fort i relation till vad vi klarar av att följa. [...] *Vi tror alldeles för mycket på applikationen absolut, det är där problemet ligger också" - (Jan Olsson).*

"Absolut, det är något som jag i min roll som säkerhetschef på en stor koncern har haft som ett ganska stort problem." - (Boris Berberovic).

Detta bekräftar även Albin Zuccato. Han menar att det oftast finns ett blint förtroende i sammanhang där användare inte förstår sig på tekniken.

"Den där blinda tilltron den är idiotisk. Den är nog delaktig i en del av problematiken." - (Albin Zuccato).

Vidare blev respondenterna tillfrågade om det finns en extra stor tillit till finansiella applikationer och applikationer som är framtagna i samarbete med banker, såsom BankID. Respondenterna är eniga om det finns en högre tillit till applikationer av denna art. Man menar dock att det finns en skepticism i och med att det berör en individs tillgångar.

"Jag tror att det finns en större tillit men samtidigt, eller hoppas jag på, i och med att det berör ens pengar alltså de finansiella apparna, anser man är viktigare. Och att man då handskas lite mer försiktigt med dem när man använder dem." (Jan Olsson).

Utöver detta poängterar Olsson att det finns en övergripande tillit till allt som finns på internet. Det finns en övertro till digitaliseringprodukter som användare tar del av. Detta visar på problematiken med att tillit inte enbart är applicerbar på finansiella applikationer, utan på samtliga produkter som individer använder.

Berberovic håller med om att det finns en extra tillit till applikationer som har skapats av eller i samarbete med banker. Däremot poängterar han att det existerar en extra skepticism hos yngre, vilket innebär att de förhåller sig generellt mer kritiskt till applikationer som vi laddar ner till på våra mobiltelefoner. Detta gäller dock inte alla unga, och framför allt inte äldre, vilket Berberovic ser som en brist hos själva tjänsteleverantören.

"Så jag tror att det finns väldigt stora brister hos leverantörerna där de inte bedriver någon typ av utbildning till användarna" - (Boris Berberovic).

4.3 BankID: Teknisk lösning

Intervjufrågorna 4 till 6 samt 19 till 21 (se appendix 1) berör respondenternas syn på BankID i sin helhet, samt vilka typer av förbättringar som kan genomföras på applikationen. BankID är vad vi identifierat en tekniskt säker plattform. Detta återspeglas i avsaknaden på fall där den hackats i traditionell mening. Det är istället den mänskliga faktorn hos användarna som utnyttjas.

"Jag håller med det att rent tekniskt "har det blivit hackat?" nä det har det inte och det är inte bekymret heller, det var bara första generationen och det är ju hundra år sedan. Så allt det här är väldigt säkert. Men sedan är det som du är inne på att folk vilseleds så att den används på ett felaktigt sätt." - (Jan Olsson).

"Jag tror att BankID har en ganska hög säkerhetsambitionsnivå och håller nog också ganska godtagbar säkerhet i själv verket. [...] *men jag tror trots allt att den svagaste länken är inte applikationen utan användaren och/eller den miljön den befinner sig i." - (Albin Zuccato).*

Respondenten Boris Berberovic har en mer teknisk bakgrund, i vår intervju tar han upp något som han kallar för en *administrativ process.* Berberovic menar att för att säkra BankID bör man implementera ytterligare tekniska funktioner i applikationen. Om banken vill ringa upp

en kund ska kunden få reda på detta på förhand genom att det dyker upp en notifikation från BankID applikationen.

"Dom borde ju ha lärt sig av sin erfarenhet med dosan att det borde finnas en administrativ, en process dvs om det är någon från banken som ringer" - (Boris Berberovic).

Zuccato instämmer att införandet av en teknisk verifieringslösning där man som kund kan begära att banken identifierar sig är en potentiell lösning för att minska antalet vishing bedrägerier.

"Det skulle vara jättesmidigt om man hittade en verifieringslösning som fungerar åt båda håll, om jag ringer in till min bank så får jag en challenge från dom och då skulle det vara bra om jag kunde ge dom en challenge. "- (Albin Zuccato).

För att förhindra vishingbedrägerier införde BankID ytterligare en säkerhetsfunktion i form av en QR-kod som tvingar användaren att verifiera att det är han som utför handlingen. Detta blir en extra kontroll som kollar att användaren verkligen är den person som sitter framför enheten i fråga där handlingen utförs. Visserligen minskar antalet brott inom den kategorin men bedragarna hittar snabbt sätt att anpassa sig

"Nu har vi ju BankID som användes vid vishing bedrägerier som vi var inne på, det försvann ju i och med att man införde en QR-kod som används när man måste verifiera att du inte bara har mobilen utan att du sitter med datorn, och då försvann ju den typen av bedrägerier, det sjönk med 92%. Man gick ju över till att lura av folk på sina bankdosinloggningskod istället, exakt samma samtal." - (Jan Olsson).

Tekniska lösningar ökar säkerheten och förbättrar BankID men bedragarna hittar kontinuerligt nya metoder och angreppssätt. Många väljer att rikta sin kritik mot bankerna men missar det faktum att vi användare är kravställare i den mån att vi förväntar oss en e-legitimation som tillåter bankärenden från mobiltelefonen. Relationen mellan användarvänlighet och tekniska säkerhetsspärrar är svår.

"Varför ta bort mobila BankID bara för att vi inte kan använda det? Det är ju ingen som vill det, jag vill inte heller det. Jag vill ha BankID så att jag kan göra mina räkningar, jag vill ha det på mobilen och inte på datorn. Det hade naturligtvis kunnat vara mycket säkrare om man skötte allt som rörde banken på en och samma dator, då kan busen ringa hur mycket han vill" - (Jan Olsson).

Berberovic menar att tjänsteleverantören har ett ansvar att utbilda användaren. Vid frågan om hur det ska gå till, föreslår Berberovic att användaren vid installation av BankID ska genomgå en kort, obligatorisk utbildning där man instruerar säkert användande. Den här informationen finns redan tillgänglig på BankIDs hemsida men kan uppfattas vara formulerad på ett krångligt och tråkigt sätt.

"[...] *bankens och BankIDs hemsidor är inte det primära kommunikationsinterfacet mot kund. Det primära interfacet mot kunden är appen, det är inte websidan. Jag loggar aldrig in på BankIDs hemsida. Det är apparna som är det primära interfacet, det är där informationen ska komma." - (Boris Berberovic).*

Vidare menar Berberovic att BankID bör införa notifikationer för att informera användaren exempelvis när det sker suspekt aktivitet från en främmande IP-adress, eller om en ny typ av

bedrägeri uppkommer kan användaren få en notifikation om detta. Hur man väljer att presentera informationen är kritiskt.

"På vilket sätt man gör det på är avgörande för om användaren tar till sig detta eller inte. [...] Man måste göra det på ett grafiskt och intuitivt tilltalande sätt, för att man skall kunna ta till sig detta. [...] *Att språket man använder inte talar bits and bytes. Att man talar språket som tilltalar mottagaren." - (Boris Berberovic).*

Zuccato lyfter svagheten hos telefonen som medel för utförandet av bankärenden. Han förklarar hur man via hemsidan enkelt kan verifiera bankens säkerhetscertifikat men att det finns en avsaknad av liknande lösning vid telefonsamtal.

"Om jag går in på internetbanken så kan jag verifiera deras certifikat så att jag vet iallafall att jag är rätt. Någonting liknande kan man göra genom att pusha ut en notifikationsförfrågan med bankens digitala signatur." - (Albin Zuccato).

4.4 Motverka attacker: ISA och SEADMv2

Frågorna 18 till 21 (se appendix 1) berör hur individer praktiskt kan skydda sig mot bedragare, samt vad BankID med sin applikation kan göra för att motverka bedrägerier. Respondenterna blev som en avslutande del av intervjun tillfrågade om vilka frågor man som utsatt bör ställa i situationer där ett misstänksamt samtal inkommer. Olsson var i denna fråga kritisk till att ställa motfrågor. Han ansåg att det fanns enklare sätt att komma runt detta problem.

"Såhär, är man det minsta osäker på om det är banken som hör av sig eller en myndighet eller skatteverket då ska man motringa, inte ringa det nummer som står i mailet eller i SMSet, man ska ringa bankens på det nummer man själv har eller som man själv slår fram på Google. Sen dubbelcheckar man det verkligen är ni som ringer om det här när man är det minsta osäker. Man ska bli osäker när de vill att du ska ge ifrån dig pengar eller koder eller för att logga in på något sätt." - (Jan Olsson).

Genom att använda denna metod menar Olsson att man kan undvika bedrägeriförsök genom att motringa banken. Man ska aldrig logga in på någon annans begäran. Däremot finns det ett undantag i detta, i vissa situationer när användaren ringer till banken kan man bli ombedd att verifiera sig med sitt BankID, men detta händer enbart om användaren har tagit kontakt med banken först.

Boris Berberovic är även kritisk till att kunna identifiera SE-attacker genom att ställa frågor. Han anser att bedragarna i dessa fall är tränade för att bemöta detta, vilket innebär att de kan manipulera sig ur dessa motfrågor. Berberovic återkommer i denna fråga tillbaka till det kommunikativa interfacet. För att vara helt säker som användare bör banker och BankID, som nämnt tidigare, implementera en funktion som skickar ut notiser till kunder när banken vill kontakta kund, notisen meddelar när samtalet kommer, samt hur banken kommer att verifiera sig. Detta skulle enligt Boris förenkla processen med säker identifiering.

"Det är ju oftast vi som verifierar oss mot banken, men det här måste förändras. Vi behöver få lika mycket tillit med vem vi pratar med på andra sidan, och det här har man inte tänkt på." - (Boris Berberovic).

Detsamma säger Albin Zuccato, i en situation där en individ får en förfrågan kring att utföra en uppgift måste det finnas en kanal för verifiering. Däremot anser han att det i dagsläget inte existerar några bra identifieringsmöjligheter via telefon, vilket är en stor brist.

5 Diskussion

5.1 Social engineering: Faser och metoder

Ivaturi och Janczewski (2011) menar att det historiskt sett har gjorts stora investeringar på den tekniska fronten, med avancerade brandväggar, antivirus och olika typer av intrångsdetekteringssystem (IDS). Samma gäller för BankID som rent teknisk är en mycket säker applikation där ingen har lyckat penetrera de tekniska säkerhetsspärrarna (Wollner, 2018). Detta håller även samtliga respondenter som utgör intervjustudien med om. Olsson poängterar att BankID aldrig har blivit hackat, utan att det är användaren som missleds och använder applikationen på ett felaktigt sätt. Detta bekräftar Manns (2008) påstående angående att människorna i sin natur är komplexa, vilket gör dem extremt svåra att säkra, och detta är dessvärre något som bedragare är medvetna om. Vidare innebär detta även att de bedrägerier som utförs genom att missleda användare till BankID faller inom ramarna för SE; att manipulera människor genom vilseledning för att få ut information, eller att få individen att utföra en åtgärd (Mann, 2008, p. 11).

Informationsinsamling är en väsentlig del inom SE (Hadnagy, 2011). I och med digitaliseringens framfart, samt det konstanta användandet av internet, har denna informationsinsamling blivit avsevärt enklare för bedragare som använder sig av SE. Berberovic, Zuccato och Olsson instämmer med detta och menar att offentlighetsprincipen är till en viss del en bidragande faktor. Personnummer och inkomstdeklarationer är exempel på information som med en enkel sökning på internet eller med ett snabbt telefonsamtal kan hamna i bedragarnas händer. Boris Berberovic tar detta ett steg längre och diskuterar GDPRs inverkan på informationsinsamling. Lagen är för tillfället relativt ny och har inte trätt i fullständig kraft. I ett framtidsperspektiv anser Berberovic att GDPR kan försvåra förberedelsefasen för bedragarna.

I frågan om själva metoderna som används vid bedrägerier kopplade till BankID framgår det i det intervjuresultatet att telefonbaserade bedrägerier är det mest förekommande. I teorin beskrivs denna typ av attack som vishing vilket innebär att förövare använder sig att röstbaserade teknologier, exempelvis telefon (Yeboah-Boateng & Amanor, 2014). Berberovic och Olsson instämmer med detta. Att ringa sina offer visar sig vara en sofistikerad och effektiv metod då bedragaren bygger upp ett förtroende till offret. Bedragare är skickliga i att skapa en tillit till offret genom sin sociala förmåga, för att sedan ställa dem i ett underläge. Detta tillvägagångssätt kan kopplas till det som kallas reverse social engineering (Krombholz et al., 2015). Bedragare som utger sig ringa från banken sätter offret i en beroendeposition, vilket enligt Krombholz et al., (2015) bidrar till att offret upplever en känsla av oro, och i behov av hjälp. Bedragaren blir i denna situation den person som kan hjälpa till med problemet, vilket resulterar i att dessa bedrägerier blir genomförbara.

Sammanfattningsvis har vi utifrån litteraturgenomgången och intervjustudien identifierat kopplingar mellan bedrägerierna och social engineering. Olsson, Zuccato och Berberovic är eniga i att de typer av attacker som görs med hjälp av BankID är en form av SE. Dessutom går det att applicera de delar som har presenterats i teorin med de verkliga exempel som beskrivs.

5.2 Användare: Medvetenhet och tillit

Generellt när det handlar om telefon- eller internetbedrägerier är det den äldre generationen som utgör den mest utsatta målgruppen (Andersson & Lärka, 2019). Detta bekräftas även av Brottsförebyggande rådet som 2016 fastslog att medianåldern hos offer är 54 år för kategorin telefon- eller internetbedrägerier (BRÅ, 2016). Berberovic och Zuccato styrker detta, då de konstaterar att det preliminärt beror på en avsaknad av kunskap om de risker som finns med användandet av diverse applikationer. Olsson bekräftar även att den äldre målgruppen är överrepresenterad i bedrägerier som utförs med hjälp av BankID, däremot anser han att detta grundar sig på en gammal uppfattning. Unga är enligt Olsson en målgrupp som bedragare också hade kunnat vända sig till.

Medvetenhet angående informationssäkerhet har genom den intervjustudien samt teorin visat sig vara en viktig faktor i förhindrandet av bedrägerier. Aldawood och Skinner (2018) menar att de flesta informationssäkerhetsintrång som görs i dagsläget beror på att den mänskliga faktorn utnyttjas. Av denna anledning poängterar Aldawood och Skinner (2018) att det är väsentligt att kontinuerligt arbeta med medvetenhet i syfte att höja informationssäkerheten. ISA är ett begrepp som presenteras i detta sammanhang, vilket beskriver individers och organisationers medvetenhetsnivå angående informationssäkerhet (Aldawood & Skinner, 2018). Individer besitter i dagsläget en mängd känslig information som i fel händer kan missbrukas. Aldawood och Skinner (2018) konstaterar att det finns flera studier som visar på att den individuella medvetenheten hos individer om SE generellt sett är låg, vilket problematiseras. Avslutningsvis skriver författarna att åtgärder bör vidtas för att träna användare i informationssäkerhet. Detta kan ske med applikationer av olika slag (Aldawood & Skinner, 2018).

Intervjurespondenten Jan Olsson betonar att medvetenhet är väldigt viktigt, han menar dock att trots en hög medvetenhet är det inte vanligt att folk efterlever det. Dessutom menar Albin Zuccato att även tränade användare kan råka ut för bedrägerier, då bedragare emellanåt kan vara mycket skickliga. Olsson tar upp exemplet med lösenord, de flesta är medvetna om att det är viktigt att ha säkra lösenord, men färre efterlever det. Berberovic menar att medvetenhet hos offer är den största bristen. De sekundära bristerna menar han är avsaknaden på kompetens hos Polisen och myndigheterna samt brister hos tjänsteleverantören bakom BankID. Han menar att brist på medvetenheten är det som enklast kan förbättras. Detta är ett påstående som styrks av Olsson, som i intervjun ger ett exempel på medvetenhetsträning i form av awareness kampanjer. Efter att ha genomfört ett antal awareness kampanjer noterade Olsson att antalet anmälningar var det samma medan antalet lyckade brott minskade. För att nå ut till en större målgrupp och för att förhindra fler SE-attacker borde BankID och bankerna arbeta mer med push-notifikationer. Som Berberovic framhäver, är det primära kommunikationsinterfacet mot användaren via appen. Därför bör även viktig information kommuniceras den vägen. Exempelvis bör BankID appen notifiera användaren om det pågår ett inloggningsförsök, geografisk position på inloggningsbegäran samt vilken tjänst som används. Användaren kan då på ett enkelt sätt avgöra om det är ett bedrägeriförsök. Berberovic menar också att det är avgörande på vilket sätt man gör detta, språket man använder ska inte vara för komplicerat.

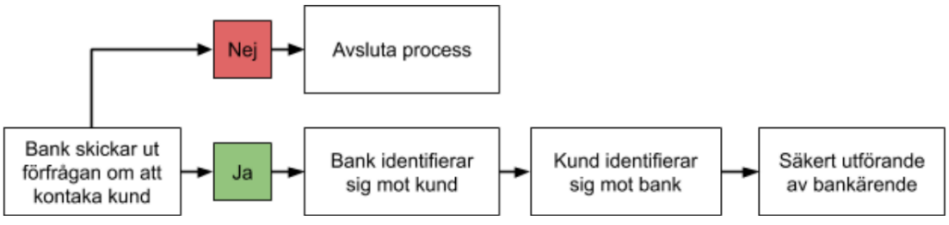
Även om vi troligtvis aldrig kommer att lyckas nå en hundraprocentig medvetandegrad, bör vi fortsätta sträva mot en nollvision. Det är även den enklaste och billigaste faktorn att förbättra på kort sikt enligt samtliga respondenter. Ur intervjustudien har det även uppenbarat sig att det finns skiljaktigheter i frågan kring vilken målgrupp som löper större risk för att bli utsatt. Statistiken från Brottsförebyggande Rådet (2016) visar på att den äldre generationen är

överrepresenterade bland offren, vilket både Olsson, Berberovic och Zuccato bekräftar. Däremot beror detta, enligt Olsson, preliminärt på ett gammalt tankesätt. Unga saknar en källkritisk förmåga vilket även placerar dem i en riskzon. Detta visar på att alla som använder sig av informationskänsliga applikationer bör bli informerade om potentiella risker i samband med dess användning, oberoende av vilken generation de tillhör.

Samtliga respondenter har varit eniga om att det finns en tillit till applikationer som laddas ner till personliga enheter, vilket även bekräftas av Lankton et al., (2015). BankID är i sig en simpel applikation, och faller enligt författarna till denna studie in under kategorin som Lankton et al., (2015) kallar teknologier med systemliknande funktioner, då BankID enbart är byggd för elektronisk identifiering. Det bör enligt teorin därför innebära att det finns en avsaknad av mänsklig tillit till applikationen (Lankton et al., 2015). Däremot finns det en aspekt som påverkar detta, vilket är den mänskliga kontakt som offren får i form av ett telefonsamtal från bedragare. Röstbaserad interaktion med användare kategoriseras enligt Lankton et al., (2015) som en människoliknande funktion, vilket ökar tilliten. Detta kan ses som en kompletterande faktor till varför användare faller offer för BankID-bedrägerierna.

5.3 BankID: Teknisk lösning

BankID har konstant varit tvungna att implementera nya säkerhetsåtgärder för att kunna förhindra bedragarna. Olsson poängterar att införandet av en QR-kod var ett sätt för BankID att säkra applikationen vid bedrägeriförsök till att ladda ner offrets BankID. Tjänsteleverantören försäkrar sig då om att den som beställer BankID är samma person som tar emot det. Detta menar vi är ett steg i rätt riktning, men att man bör ta till en ännu mer drastisk åtgärd. BankID är idag utformat med envägs-verifiering. Respondenterna Boris Berberovic och Albin Zuccato föreslår en säkrare lösning, att möjliggöra för banken att identifiera sig mot kunden. Detta menar Berberovic kan göras genom att förbjuda samtal från banken till kunden, samt i samband med införandet av push-notifikationer som diskuteras ovan i avsnitt 5.2, meddela kunden att banken kommer att kontakta dom, vilken tid detta kommer att ske, samt hur banken kommer att identifiera sig (se figur 7). Genom att identifieringen sker åt båda hållen (tvåvägsverifiering), ökar säkerheten avsevärt. Detta kommer troligtvis inte att eliminera bedrägeriförsök helt och hållet men det försvårar avsevärt för bedragarna. Detta är en del i vad Berberovic kallar för en administrativ process. Banken kan vid misstanke av pågående bedrägeriförsök varna användaren genom en push-notifikation. Samma process kan tillämpas när banken vill kontakta användaren, detta visualiseras i figur 7 nedan.



Figur 7: Visualisering av ”Administrativ process”.

Banken och tjänsteleverantören har även ett ansvar att utbilda användaren, vi har noterat att det på deras hemsidor finns mängder av information angående hur man skall använda tjänsten på ett säkert sätt. Precis som Berberovic menar är det dock appen som är det primära

kommunikationsinterfacet mot kunden, därför bör även säkerhetsutbildning utgå därifrån. Exempelvis skulle BankID kunna sammanställa korta filmer som förklarar hur man på ett säkert sätt kan använda tjänsten, och dessa bör finnas tillgängliga i appen.

Aldawood och Skinner (2018) anser att kunskap om informationssäkerhet på ett generellt plan är bristfällig hos individer, och de poängterar vikten av att kontinuerligt arbeta med utbildning och medvetenhetsträning. Kommunikationsinterfacet är ett konkret exempel på hur tjänsteleverantören, i detta fall BankID eller banken, kan öka den övergripande medvetenheten hos sina användare kring de risker som finns kopplade till användandet av BankID, vilket enligt teorin är ett medel för att minska antalet lyckade SE-attacker.

5.4 Motverka attacker: ISA och SEADMv2

I stycke 5.2 har det fastställts att medvetenhetsträning och information om riskerna är ett tillvägagångssätt för att minska antalet lyckade bedrägeriförsök som görs via BankID. Olsson har praktiskt arbetat med något han kallar awareness-kampanjer vilket har varit framgångsrikt i att förebygga bedrägerier. Boris Berberovic kategoriserar medvetenhet som det främsta problemet när det kommer till bedrägerier som utförs via BankID. Berberovic och Zuccato ger konkreta exempel på förbättringsmöjligheter i form av tekniska lösningar som i hans mening hade gjort BankIDs applikation säkrare.

I syfte för ge konkreta exempel på vad användare till BankID kan ställa för motfrågor i situationer där misstänksamma samtal inkommer har SEADMv2 presenterats i litteraturgenomgången (Mouton et al., 2015). Modellen använder sig av en beslutsträdsliknande arkitektur (se figur 5) som beskriver vad en individ praktiskt ska ställa för typer av motfrågor för att undvika att bli utsatt av bedrägerier. Enligt Mouton et al. (2015) kan denna modell nyttjas i alla SE relaterade attacker som görs via olika kanaler.

I intervjustudien blev samtliga respondenter tillfrågade om vilka typer av motfrågor som en individ kan ställa i situationer där någon uppger sig ringa från bank eller liknande. Enligt Olsson finns det enklare sätt att komma runt detta problem, och ställde sig därför kritiskt till att ställa motfrågor. Olsson anser att användaren i dessa situationer ska lägga på samtalet och motringa på det telefonnummer som finns på bankens hemsida. Genom att använda detta tillvägagångssätt kan man direkt verifiera om det verkligen var banken som ringde. Dessutom belyser Olsson att banken aldrig kommer att ringa och be kunden att verifiera sig med sina personliga koder. Det är enbart när kunden ringer till banken som en verifiering med BankID kan förekomma. Detta är dessvärre en regel som inte nått ut till alla användare, vilket är ett exempel på bristfällig information från tjänsteleverantören.

Även Berberovic ställer sig kritiskt till att ställa motfrågor. Bedragare är i hans mening tränade för att bemöta motfrågor, vilket han anser bidrar till att det är en ineffektiv metod vid bedrägerier som berör BankID. En implementering av ett kommunikativt interface, med en tvåvägs verifikationsprocess där även banken verifierar sig mot kund hade enligt Berberovic och Zuccato förenklat processen genom säker identifiering.

Eftersom SEADMv2 är en generell modell blir vissa delar mindre tillämpliga vid just BankID-bedrägerier. Intervjufrågorna var utformade enligt teorin och respondenterna Olsson, Zuccato och Berberovic visade sig alla vara kritiska till att ställa motfrågor när ett misstänksamt samtal inkommer, därmed minskade relevansen för modellen ytterligare. Vi

menar dock att modellen kan visa sig vara användbar i andra situationer där missledande samtal eller e-mail inkommer till privatpersoner och företag.

6 Resultat och slutsats

6.1 Slutsats

Genom en litteratur- och intervjustudie har författarna till denna rapport diskuterat SE i relation till bedrägerier som utförs med hjälp av BankID. Ett antal faktorer har visat sig spela en stor roll, såsom medvetenhet och tillit. Vidare har förbättringsmöjligheter i form av ökad kommunikation mellan tjänsteleverantör och användare tagits fram.

Den huvudsakliga frågeställningen som är ämnad att besvaras lyder; *Vilka utmaningar står e-legitimationer, såsom BankID, inför vid motverkandet av bedrägerier där den mänskliga faktorn utnyttjas?*

För att besvara frågan har vi diskuterat lösningar som skulle kunna öka medvetenheten samt stärka säkerheten i applikationen ytterligare;

- Direktkommunikation till användaren genom det primära kommunikationsinterfacet
- Tvåsidig verifiering (Användare → Bank samt Bank → Användare)
- Intuitiva och informativa utbildningar som alla användare måste genomföra innan användning av BankID

Det som nämns ovan är exempel på tekniska lösningar som kommer generera en högre medvetenhet hos användare. Medvetenhet är något som samtliga respondenter i intervjustudien har identifierat som en viktig aspekt i frågan om att bibehålla en hög grad av informationssäkerhet.

6.2 Kunskapsbidrag

Studien har delvis haft för avsikt att försöka koppla bedrägerier som utförs med hjälp av BankID till SE. Olika teoretiska delar som berör ämnet social engineering har genom en analys av intervjuresultat gått att koppla till varandra vilket bekräftar att bedrägeriformen är att betrakta som en typ av SE. Vidare har studien presenterat konkreta exempel på lösningar som hade medfört att BankID som applikation kan bli säkrare att använda. Lösningarna berör tekniska åtgärder, samt hur användare tillsammans med medvetenhetsträning kan förminska risken med att bli utsatt för bedrägeri.

6.3 Vidare forskning

Studien har enbart berört det svenska e-legitimationssystemet BankID och de bedrägerier som är kopplade till denna applikation. På grund av avgränsningsskäl har denna studie inte haft resurser till att undersöka om den problematik vi ser i Sverige går att återfinna i andra länder som tillhandahåller sig av någon typ av e-legitimation, vilket enligt författarna till denna studie är ett intressant område att utforska vidare.

Tillit till applikationer som användare laddar ner till sina mobiler har visat sig vara ett problem ur en informationssäkerhetsynpunkt. Respondenterna har i denna studie blivit tillfrågade om det finns en extra tillit till applikationer som är skapade tillsammans med banker, såsom finansiella applikationer. Ingen respondent har haft ett klart svar på om det finns en direkt relation mellan tillit och finansiella applikationer. Av den anledningen anser författarna till denna studie att detta område går att forska vidare.

Appendix 1 Intervjufrågor

Social engineering

1. Definitionsfråga: Utifrån den litteratur vi tagit del av betyder SE att manipulera människor genom vilseledning för att få ut information, eller få individen att utföra en åtgärd (Mann, 2008).
2. Håller du med om att den typ av verksamhet som dessa bedragare arbetar med kan räknas som en typ av SE?
3. I ditt arbete, kan du ge tre exempel på hur bedragare använt sig av SE för att utföra bankbedrägerier (200 000 anmälda brott om året)

BankID (eID)

4. Vi gillar BankID, men utifrån media verkar det finnas uppenbara brister, hur ser du på applikationen i sin helhet?
5. Vad har du utifrån din yrkesroll sett för förändringar av bedrägeritrender inom BankID?
6. Ser du några tekniska brister med BankID som applikation?

Förberedelser, attack & post-attack

7. Vilken typ av förberedelse krävs för att kunna genomföra dessa attacker?
    a. Hur går bedragare praktiskt till väga?
    b. I vilken mån gör bedragare någon typ av "background check" av sina offer?
    c. Från vilka kanaler får de tag på informationen?
8. Är det någon särskild målgrupp som bedragare vänder sig mot?
    a. Varför?
    b. Har denna trend ändrats med tiden?
9. Har du några konkreta exempel på attacker, och vad blev utfallet?

Typer av attacker

10. Vilka metoder använder bedragare för att praktiskt lura individer?
11. Vilka är de mest förekommande i så fall?
12. Har det skett någon särskild utveckling?

Medvetenhet hos användare

13. I vilken mån spelar medvetenheten kring informationssäkerhet hos användaren roll i dessa attacker?
    a. Finns det enligt dig en direkt relation mellan medvetenhet och "success rate"?
    b. Vilka råd skulle du vilja ge till en användare av E-legitimation?

Tillit till teknologi

14. Anser du att det kan finnas en tillit till applikationer som vi laddar ner till våra mobiler?
15. Finns det en särskild tillit till applikationer som är framtagna som ett samarbete med staten och banker?
16. Kan tillit till teknologi vara en faktor att dessa typer av attacker är genomförbara?
17. Kan du ge något exempel på hur vi visar för stor tillit till teknologi

Motverka dessa attacker

18. Hur kan man som privatperson motverka dessa attacker?

   a. Finns det några särskilda metoder eller exempel?
   b. Är medvetenhetsträning svaret?
   c. Vilka typer av frågor bör man ställa för att verifiera att den man pratar med verkligen ringer från exempelvis en bank?

BankID (eID) lösning

19. Ur de iakttagelser vi har gjort har vi insett att det finns mängder med varningar på BankIDs och bankers hemsidor kring dessa attacker, varför når denna information inte ut?
    a. Vad kan BankID göra annorlunda för att varna sina användare på effektivare sätt?
20. Skulle ett extra valideringssteg kunna lösa denna problematik?
    a. Om ja hur skulle detta vara genomförbart?
    b. Skulle detta kunna påverka användarvänligheten i applikationen?
21. September 2018 beslutades det i hela EU att det ska finnas ett gemensamt e-legitimeringssystem (eiDAS). Hur tror du detta kan påverka den kriminella verksamheten på ett geografiskt plan?
    a. Kan samma problematik vi ser i Sverige uppstå i andra medlemsländer? Varför/varför inte?

Appendix 2 Transkribering Jan Olsson

Just social engineering så finns det ju lite olika definitioner som florerar. Vi anser utifrån den litteratur vi har tagit del av att SE betyder att man manipulerar människor genom vilseledning för att få ut information, eller för att få individen att utföra en åtgärd.

Ja helt rätt, plattformarna för det kan vara allt från mail eller annat.

Ja men precis.

Ja men det är så jag ser det utan att ha slagit upp det.

Och håller du med oss i vår ide att just när det handlar om BankID bedrägerier så arbetar många av dessa bedragare med det som skulle kunna kallas SE, att de lägger upp det på ett sådant sätt?

Ja jo det är helt klart det är definitivt social engineering. Det är en förädlad form i och med att de använder sig av telefonen för att lura människor. Men absolut Social engineering är ett fundament som ligger bakom de mesta av den vilseledande brottsligheten, med bedrägerier och andra såsom staten med skattebrott osv.

Ja men precis.

Det är ett väldigt brett vilket gör att det oftast går in i kategorin SE.

Precis, och du arbetar just nu på polisens nationella bedrägericentrum..

Nä,

Det gör du inte?

Nej nej nej, jag jobbar på polisens nationella IT-brottscentrum.

Okej. då har jag missuppfattat det.

Ja jag är processansvarig här för IT-relaterade brott och där ingår bedrägerier. Men det ingår också trojaner, ransomware och annan styggelse.

Okej.

Allt som är komplexa IT-brott och internetrelaterade brott, så att det är lite bredare, lite större och högre i hierarkin helt enkelt.

Ja men okej jag förstår. Och i ditt arbete på polisen har du några exempel på hur bedragare har använt sig av SE för att just komma åt folks pengar, bankuppgifter eller liknande?

Njaa det är väl 200 000 anmälda fall ute i Sverige som har med social engineering att göra. Men nu höftade jag bara det kan vara mycket mer, men om du tittar på allting som det simplaste phishing-mailet som utger för att vara någonting och att du ska klicka dig vidare för

att kontrollera skatteåterbäringen eller att du ska plocka ut en vinst på konsum som de (bedragare) vet med om att du tävlat om. Och när du klickar dig vidare ska du ge ut dina kortuppgifter för att du ska kunna få ut dina pengar. Busarna i sin tur tar dessa kortuppgifter och säljer dessa. Sedan så köper dom (de som köpt kortuppgifterna) saker på internet. Du får fakturan och han får brallorna från Zalando. Och detta är ju också SE, och det är det största enskilda brottet vi har egentligen, det är bara det att det inte anmäls då det är få som går på det, men likafullt så är det så att folk går på det och där så är det. Försöken räknas också som brott. Detta är exempel på den enklaste formen men sedan går det upp till SE andra typer av attacker såsom romansbedrägerier som görs i skriftlig form och detta pågår under en längre tid och det är mycket mer kvalificerade och mer organiserad brottslighetsfrågor bland annat. Sedan tycker jag som är den mest etablerad är att ha en fysisk kontakt, alltså telefonkontakt med offret och lurar offret att göra saker. Där har vi sol och vårar som är ett romansbedrägeri där man lever ihop under en period för att sedan lura ena individen.

Och detta är nästan i sin mest avancerade form kan man säga?

Ja precis och det som blir att det ökar så förbannat är för att det finns en så stor social plattform att utgå ifrån och det är ju internet och dess innehåll, facebook eller dating-siter och allt det kan vara. Alla har en dator som är uppkopplad till nätet och antalet plattformar på nätet att använda ökar explosionsartat så ökar självklart också brotten.

Ja.

Däremot så är det så att när den organiserade brottsligheten ser hur enkelt det är att tjäna fruktansvärt mycket pengar då ger sig dom in i spelet. Vi ska vara glada att det bara ökar med några hundra procent.

Ja precis.

Ja det är ett jätteproblem.
Ja och nu går jag lite off topic men det är verkligen något som vi upplever inte får jättemycket uppmärksamhet heller.

Nä det är lågt prioriterat jämfört med andra brott, såsom våld i hemmet som är mycket värre för individen. Men detta är ett samhällshot och hot mot det monetära-systemet i och med att vi som kunder varken kan använda sig av det som erbjuds. Det är ju bankerna som tillhandahåller oss med det här.

Precis och du nämnde också siffran 200 000 anmälda brott om året…

260 000 anmälda bedrägerier och eftersom de flesta bedrägerierna anmäler någon forma av social engineering, så jag skulle säga att alla dessa 260 000 anmälningarna rör sig om SE. så hur stor den exakta siffran är kan vara 240 000 eller 200 men det vet jag inte, men det är en större mängd i alla fall.

Jag förstår. Tror du att det finns ett mörkertal där också i och med att det kan finnas en skam i att bli lurad?

Ja det är stigmatiseringen som ligger i grunden till det och mörkertalet kan vara enormt stor. Det är få män i min ålder som går till polisen för att de har blivit lurade av en tjej som de

trodde var kär i en som de aldrig har träffat utan bara pratat digitalt där man skickar sina pengar. Det är klart som sjutton att det är ingenting som man anmäler kan man tycka. Man skäms så himla mycket för det man har gjort, och ända till och med vishing-bedrägerier när man ringer och säger att man är från banken vill man inte heller anmäla för att man tycker att man har varit klumpig och naiva för att man har blivit lurad på ett sånt sätt, och det är ju det som är felaktigt, de som gör detta är ju proffs. Vi måste få bort den här stigmatiseringen runt att man har blivit lurad. Mörkertalet är jättestort överallt vilket brott du än tittar på när det gäller SE.

Precis och när vi pratar just BankID, det är väldigt populärt här i Sverige och om man läser vad media skriver om det finns det ju uppenbara brister, inte just i det tekniska men att folk ändå lyckas bli lurade, vad är din syn på BankID applikationen eller e-legitimation i sin helhet?

Jag tycker att bägge delarna är fundamentalt superviktiga att vi har. Jag håller med det att rent tekniskt "har det blivit hackat?" nä det har det inte och det är inte bekymret heller, det var bara första generationen och det är ju hundra år sedan. Så allt det här är väldigt säkert. Men sedan är det som du är inne på att folk vilseleds så att den används på ett felaktigt sätt. Det mest kvalificerade som finns inom säkerhetsbranschen idag är att göra något så svårt att handskas fel med, och det är ingen optimering som är lätt. Nu har vi ju BankID som användes vid vishing bedrägerier som vi var inne på, det försvann ju i och med att man införde en QR-kod som används när man måste verifiera att du inte bara har mobilen utan att du sitter med datorn, och då försvann ju den typen av bedrägerier, det sjönk med 92%. Man gick ju över till att lura av folk på sina bankdosinloggningskod istället, exakt samma samtal. Det är lite svårare för där måste den lurade han måste ju rabbla sin inloggningskod. De tidigare BankID bedrägerierna behövde man inte göra det.

Har du utifrån din yrkesroll sett, det här var ju ett exempel med QR-koden, att det blev en förändring på bedrägerierna?

Det vart ju mycket färre bedrägerier, men jag säger inte att de försvann. QR-koden skyddar bara mot dom mest uppenbara, för den behöver du bara använda när du ska ladda ner nytt BankID eller ska göra en utlandstransaktion transaktion och detta blev konsekvensen av dessa bedrägerier. Man gav ut koder så att man som buse kan ladda ner ett nytt BankID från någons internetbank för att sedan kunna agera, det kan man ju inte numera, och du kan ju inte nu heller vara inne på någons konto och skicka ut pengar utomlands med ett eget nedladdat BankID. Allt annat kan du dock fortfarande göra.

Ja men precis. Du pratade lite angående att det faktiskt inte är någon som faktiskt lyckas hacka sig in på BankID utan det är den mänskliga faktorn som brister, men ser du tekniska brister med BankID som applikation?

Nä, utan man måste hela tiden tänka såhär vad är det vi (kunder) vill ha? Varför ta bort mobila BankID bara för att vi inte kan använda det? Det är ju ingen som vill det, jag vill inte heller det. Jag vill ha BankID så att jag kan göra mina räkningar, jag vill ha det på mobilen och inte på datorn. Det hade naturligtvis kunnat vara mycket säkrare om man skötte allt som rörde banken på en och samma dator, då kan busen ringa hur mycket han vill, men det är inte den lösning som efterfrågas, så det är svårt alltså. Det allra säkraste hade varit att fimpa internet, då hade vi inte haft några brott. Men det vill vi inte heller. Samma med swish-lösningar och sånt, det går fort, det går fort när pengarna försvinner och det blir svårare för någon att stoppa

en transaktion, men det är ju vi (kunden) som vill att det ska gå fort. Så vad ska banken då svara? Det är vi som kunder som efterfrågar det här, så vad ska bankerna svara?

Det är ju väldigt smidigt och om man inte använder det på fel sätt är det ju egentligen en väldigt liten risk.

Ja, men sen är det ju det att jag tror att e-legitimation och BankID då (15:10 jag hör tyvärr inte vad som sägs här) direktiv 2.2.0 som kommer i september som kommer kräva att av handlaren oavsett på nätet eller i fysisk butik att kunna identifiera den som använder kortuppgifter. Inte bara flera kort som är kopplade till konton där stålar går att tjäna utan just den biten. Och då kommer det kanske/förhoppningsvis kräva att e-legitimation verifiering före köp på nätet och då kan man inte längre använda stulna kort. Och då försvinner 105 000 brott där, och det är ju ganska bra.

Ja verkligen, men det här med att man säljer stulna kort, var sker den försäljningen?

Största delen är ju dark-web. Det finns "carding-ID" för öppna google internetdelarna i Sverige, men det kan jag inte rekommendera någon att använda för att de är bedrägliga, alltså att man köper icke-fungerande kort. Men på dark.web kan du köpa hur mycket du vill. Det finns mer kortuppgifter till salu än det finns bedragare som använder korten innan utgångsdatum på dom. Många utav våra (kortuppgifter) är också stulna men vi hinner inte bli brottsoffer innan utgångsdatum är uppnått.

Okej, det där är intressant.

Ja det beror ju på massor av saker, först och främst har vi dessa gigantiska dataintrången där man lyckas stjäla 10 miljoner kontouppgifter i ett svep, till att det finns hundratals svenska företag som använder sig av keyloggers utan att de vet om det, alla på dom sidorna loggar som kunderna knappar in, den den informationen stjäls till en server då, där bedragaren tar emot dem och säljer dem vidare på dark-web, och det här pågår medan vi pratar. Plus alla dom som går på alla dom här phishing mailen.

Ja men precis. Men har du sett några andra förändringar av bedrägeritrender inom just BankID, förutom det du sa om att man la till extra säkerhet (QR-kod)?

Nä, eller det har jag säkert gjort men nu när du ställer frågan kan jag inte komma på något. Nä, utan det började med PPM fonderna, dackefejden för 10 år sedan, där man lyckades plocka 5,5 miljarder. Och då säkrade man ju upp den möjligheten, och sedan kom nästa och nästa, och nu har vi kommit till QR-koden.

Men du sa PPM-fonderna menar du det här med att bluffbolag ringde upp och erbjöd förvaltning av folks PPM?

Ja, men precis och just det här med det tvåkanaliga systemet, att man kan släppa in varandra hur som helst. Men det täppte dom till där då. Det var uppenbart inge bra.

Nä men precis. Jag känner till det där jag gick i gymnasiet då jag tyvärr jobbade på ett sådant företag i en månad.

Ja, och det var ju SE också. Det roliga med SE är att de flesta call-centers som håller på med det är att personalen inte själva vet vad de håller på med. Många av dom tror inte att det är brottsligt, alternativt att de inte tror att det är något märkvärdigt.

Nä precis.

Nä och det är inge bra alls.

Nä verkligen inte, men vilken typ av förberedelse krävs från bedragarna för att kunna genomföra liksom den här typen av attacker vi pratar om? Alltså hur går man praktiskt till väga?

Ja men idag är det jättestökigt, nu handlar det om, om vi nu tänker efter införandet av QR-koden på BankID, nu handlar det att du måste förmå den du talar med att utföra alla handlingar. Vilket inte är helt enkelt. Det är därför man gått över till att försöka förmå dem att försöka ge ut sina bankkontouppgifter, eller bankdoseuppgifter och det är inte nytt. Det största jag har varit med om var 2014 och då kallade vi det för "Facebook-bedrägerier".

Okej då att man skrev till folk direkt på Facebook?

Ja man kapade Facebook-konton och köpte inlogget på darknet och sedan kontaktade man vännerna, och vännerna såg ju på avataren att det här är ju min brorsa som kontaktar mig, det är ju hans foto som dyker upp här på messenger. Och där skrev man "tjena, jag måste pröjsa räkningen med dosa men den är paj, kan jag låna inloggningen till din dosa?" och du som tar emot det där vet ju att det är din bror och då går man med på det. Du vet om att du inte får lämna ut dom (uppgifterna) kanske, men det är ju din brorsa så du lånar ju dom. Och sen är din internetbank tömd. Det där var ju massor och jag följde de där stålarna via Ryssland och fan va de studsade iväg och det var sjukt mycket pengar. Men dom (bedragarna) fick vi tills slut i och för sig.

Okej men en liten följdfråga som vi egentligen inte har med i vårt frågedokument men jag är bara nyfiken, men brukar man lyckas få tillbaka sina pengar i sådana situationer?

Nä, det får man inte, speciellt när vi tänker BankID som var, eller fortfarande är lite grann, där har ju har du ju en chans att få tillbaka det enligt den allmänna reklamationsnämnden, där man tycker att bankerna ska stå för konsekvenserna. Men bankdosa, då lämnar faktiskt du ut dom (uppgifterna) i strid med gällande avtal, och då får du stå för den förlusten själv, de har gjort undantag av emotionella skäl när någon på 99 år inte förstod bättre. Men där är det jättejättesvårt. Och sen det tredje att vi griper någon och skickar tillbaka pengarna, han (bedragaren) har inga pengar kvar. Dom är borta för länge sedan. Det går väldigt fort det här. Och i de fall jag har sett är det uttag på tre olika konton samtidigt som skickas till konto i utlandet, och hur ska en svensk polis då kunna gripa någon i Venezuela?

Ja men precis, det blir väl för stort för svenska myndigheterna att ta hand om?

Ja, bevisningen hinner ju försvinna innan vi vet vad vi ska leta efter. Andra länder svarar inte på våra frågor, och vi går via den internationella åklagarkammaren, och när allt det är gjort då är övervakningsfilmerna överspelade och vi vet inte vem som har tagit emot dom. Och det här utnyttjar ju dom (bedragare) maximalt. När det kommer till vishing har vi gripit 7–8 ligor och

det är delvis varför den typ av brott har gått ner. Och då var det svenskar som låg bakom det, och allting hände i Sverige.

Vi försökte få tag i lite statistik på det här med hur offren brukar se ut, och det fanns ju en, brottsundersökande rådet hade en om bedrägerioffer där man bestämde en medianålder, har du någon...?

Nä, utan om man tittar på vishingen har vi ju 77+ gamla. Men det gäller bara den lilla delen. BRÅs genomgång av det där är det enda som finns när det kommer till bedrägerier i stort.

Ja, i vilken mån gör bedragarna någon typ av "background check" av sina offer?

Ja det gör dom, det beror på vad det är men, i början när man ringde angående BankID när de själva loggade in med offrets personnummer, innan den gjordes visste man vad offret hade för personnummer, och det är ju en offentlig uppgift. Det är en viss strategi. Och sedan när man tittar på kreditbedrägerier, där tittar dom (bedragare) på den som har blivit ID-kapad, för att denne måste ju vara kreditvärdig, så det hade man ju koll på, och det här är ju också offentliga uppgifter. Jag är inte så imponerad av detta men visst har de kartlagt det. Men sen har vi de mer avancerade bedrägerierna där man infiltrerar företag och smittar dem med kod och tar över faktureringsprogrammen och är inne i banker och härjar, då är det en helt annan femma, det är dock inte så många ärenden av den typen.

Precis, och från vilka kanaler, om vi talar mer om brotten som påverkar privatpersoner, från vilka kanaler får man generellt sett tag på informationen? såklart, personnummer är ju offentliga uppgifter som du säger.

Det är det man använder sig utav i största möjliga mån, tittar du på avancerade medel bedrägerier då går du in på företaget. I Sverige är dom så duktiga så man googlar på företaget och tar reda på vad alla heter, mailadresser, telefonnummer till hela styrelsen och ekonomiavdelningen, allt du behöver finns där. Det krävs inte att de måste göra något mer avancerat som man själv kan tycka. Då är SE mycket mycket mer vanligt än någon sorts hacking, att man ringer företaget för att utge sig vara dotterbolagets VD i Frankrike och så skapar man sig ett namn dit, man ringer flera gånger och till slut tror ekonomiavdelningen att den här killen är han från Frankrike, och sedan kommer den "hej, hörredu kan du skicka 30 miljoner till kina för att vi ska göra en affär, men det är lite hemligt så det ska vara diskret".

Om vi går tillbaka till målgruppen för bedragarna, det kan ju låta väldigt självklart men det är samtidigt väldigt svårt att hitta artiklar eller liknande saker om det, men varför tror du att man riktar in sig på äldre?

Nä men det där tror jag är en sån där gammal missuppfattning, om vi tänker på hur rovdjur jobbar ute på savannen så fokuserar man ju på de svaga individerna i flocken. Det där har ju satt sig på hjärnan hos intelligenta varelser som ska tjäna pengar på bedrägerier. Och då tror dom att man måste angripa de äldre för de måste vara dom svagaste och mest lättlurade som vi har i samhället, därför finns det en överrepresentation av den personen i målgruppen. Men jag är definitivt inte säker på att det stämmer, utan jag tror snarare att dom äldre är svårare att lura. Det är dom yngre som är lättare att lura, men det fattar inte bedragarna, därför attackeras äldre och därför ser det ut som att de är mer lättlurade.

Det är en superintressant idé, och vi (Sebastian & Georg) instämmer nog helt på den idén.

Ja och jag hoppas att det är så och att folk tar upp den tråden och slutar angripa våra äldre. Dom tar skada av det här och tappar förtroende för samhället runt omkring dom, och vissa vågar inte gå ut efteråt, och litar inte på någon tillslut.

Ja precis, och tror du att detta kan bero på att vi ungdomar, om vi nu kategoriserar det så, att vi är mindre källkritiska av oss också?

Ja men så är det ju. De yngre bor ju i internet redan när de föds, de äldre ser det här ju som en ny fluga som vi inte litar på alls. Vi vågar knappt trycka på någonting och det tycker jag är skitbra i och för sig. Då laddar de inte ner någon skadlig kod också.

Haha jo precis. Du nämnde lite phishing och vishing och så. Vilka är dom mest populära metoderna som bedragarna använder för att praktiskt lura individer?

Om man ser på den absolut vanligaste är det kortbedrägerier där man köper saker med någon annans kortuppgifter på nätet, det är 105 000 anmälda och det är 40% av alla bedrägerier i sverige och i världen, så det är ju kortbedrägerier. Nummer två är nog kreditbedrägerier där man använder din identitet för att beställa varor, det är 30–40 000 sådana.
Var beställer man dessa varor, är det till en postlåda, eller är det till sin egna adress eller hur fungerar det?

Nä men man beställer det till en annan adress. Tyvärr är det ju så att man kanske är skriven i stockholm men man vill inte skicka hem varan utan man vill istället skicka den till den här adressen. Då skickas det till en annan adress. Och då tar man emot dom där och det kan ske på massor av olika sätt. Sedan förekommer det i viss mån att man beställer till företaget AB och säger att man möts i porten. Sedan förekommer de fortfarande att man adressändrar. Så att det är är liksom inget problem för bedragarna. Hur man än ser på det här, det har kommit en ny lagstiftning kring ID-kort, ID-korten är för dåliga, och sedan är det svårt att begära mer på postens utlämningsställe kanske, jag själv ser inte skillnad på ett äkta och ett falskt, där är det svårt. Utan när man går tillbaka i brottskedjan och på e-handeln där jag beställde mina varor, det är ju där problemet ligger. Idag så har ju bankerna börjat säkra upp sina produkter i viss mån, så det börjar komma på banksidan. Men på e-commerce där har man ju inte koll på sina kunder eller dom som köper saker, som som beställer saker eller köper med stulna kortuppgifter.

Nä precis och dom har väl inget intresse av det heller de vill ju bara sälja sina produkter?

Ja visst, och oftast får de betalt av banken ändå.

Precis. Om man går in lite på medvetenheten hos användarna, i vilken mån spelar medvetenheten inom informationssäkerhet roll i dessa attacker?

Det är klart som sjutton att det betyder jättemycket. Sedan är det en stor skillnad på att vara medveten och efterleva dom. Jag tror alla är medvetna om att man ska ha säkra lösenord och sådär och att man ska ha ett sånt där lösenordsprogram där man samlar alla lösenord. Men hur många har det egentligen? Jag tjatar ju jämt på att man ska ha hänglås på sin brevlåda men det har ju inte själv. Så jag har ju själv tryckt på länkar och hamnat på konstiga sidor. Så människor vet om det men vi efterlever det inte, det är där vi måste bli bättre på att vara källkritiska mot data i överlag, tänka att “det här kanske inte är min bror det här”. Låter det

orimligt då är det nog inte heller helt sant. Man ska försöka ha med sig det, men att vara 100% på det viset klarar inte ens jag av.

Så är det ju. Finns det någon direkt relation mellan den här medvetenheten och success rate hos bedragarna?

Ja det gör det ju. Tittar vi på vishning, där körde vi jättemycket med awareness kampanjer där vi varna för det här. När vi hade börjat med det såg vi i statistiken att brotten ökade, men antalet lyckade försök minskade. Och då kan man läsa i dessa anmälningar att "jag hade sett på tv" eller "jag hade hört på radio" att det var någon som stod och tjata om det här.

Ja så informationskampanjer fungerar alltså?

Ja, men sätta siffror på det där det är svårt.

Jo men det förstår jag.

Men att det fungerar det vet jag.

Och vilka råd skulle du vilja ge till användare av e-legitimation? Vad är de klassiska "följ dom här tipsen" så slipper du bli utsatt?

Minska risken menar du?

Ja precis.

Nummer ett är självklart, lämna aldrig ut inloggningsinformationen till någon som efterfrågar det via mail eller sms eller på annat sätt eller telefon. Man ska inte heller logga in på någon annans begäran oavsett vem det är. Här finns det dock ett pass, när du ringer Nordea då kan du bli ombedd att logga in med ditt BankID men då är det ju du som har sökt upp Nordea. Om Nordea ringer dig, det är då du inte ska logga in, den är ju lite bökig sådär. Och sen är det ju i princip alltid det generella såsom att alltid ha mobilen låst, skriv inte upp inloggningskoder, och tänk på att den korta 6-siffriga koden du har på mobilen på BankID kan du ju förlänga till 10 eller 2 eller 14 siffror, kommer inte riktigt ihåg hur många det var. Men det är också en ide för att göra det lite svårare, detta kanske inte är det första jag tänker på, men det är något jag fick veta att man kunde göra.

Jaha okej, det visste jag faktiskt inte att man kunde göra heller så att…

Nä jag vet inte hur man gör det heller men det var någon som sa det i alla fall.

Och när man kollar lite på tillit till teknologier, anser du att det finns en tillit till applikationer som vi laddar ner till våra mobiler?

Menar du olika applikationer?

Nä alltså generellt sett, alltså att vi människor litar på teknik, lite blint ibland.
Det är ju det som är problemet. Bara för att vi tror oss ha en säker applikation så går vi fria från alla problem. Så är det ju inte utan det är ju hur vi använder applikationen. Och här går den digitala utvecklingen alldeles för fort i relation till vad vi klarar av att följa. Det är jag

knappast ensam med att tycka och säga. Vi tror alldeles för mycket på applikationen absolut, det är där problemet ligger också. Sedan finns det ju appar som vi laddar ner från höger till vänster för att vi tycker de är balla, men de har bara ett syfte och det är att sno dina koder eller ditt levnadssätt för att sälja den informationen vidare.

Jo precis, och tror du att det finns extra mycket tillit till applikationer som är framtagna i samarbete med banker?

Jag tror att det finns en större tillit men samtidigt, eller hoppas jag på, i och med att det berör ens pengar alltså de finansiella apparna, anser man är viktigare. Och att man då handskas lite mer försiktigt med dem när man använder dem. Förhållandena där vet jag inte, det kanske bankerna har kollat på men det tror jag inte för de vill nog inte skryta om det i och med att det är så dåliga siffror. Det är svårt, det ska man egentligen forska lite på.

Ja precis, och har du något annat exempel på hur vi visar för stor tillit till teknologier i övriga sammanhang?

Nä men det är ju hela internetanvändandet och internetanvändandet överlag. Jag har en äldre kille hemma och jag vill nästan slå honom i huvudet för att han inte använder virusskydd, men det tycker inte han var nödvändigt. Alltså vi har någon typ av övertro på digitaliseringsprodukterna, att det skulle säkra upp vår tillvaro mer än på den tiden när man prata med en bankkassörska för att få ut sina pengar och visa sina ID-handlingar. Det där är lite orättvist mot allmänheten också. Bara för att man inte kan hänga med i digitaliseringen, och att det nästan förväntas kunna alla aspekter på ett BankID, att du ska från början veta att såhär kan du inte göra eller att så här fungerar det här, men fasiken kan hänga med i det? Utan produkterna måste vara så pass enkla så att det blir svårt att göra fel i användandet. Agda och jag vi klarar inte av att hålla koll på alla konstiga transaktionsprodukter som finns där ute i samhället och exakt vad som förväntas av dom som användare och vad man inte ska göra med dom.

Tror du att medvetenhetsträning eller upplärning är svaret på detta?

Jag tror att awareness är nyckeln men det finns forskning som visar på att om jag förmedlar till 100 är det 10 som efterlever. Det blir inte 100% ändå. Utan jag tror att på awareness absolut, sedan ligger det ett jättestort ansvar på produktägaren. Om jag ska ge ut ett nytt bankkort eller BankID, då ligger ett jättestort ansvar på mig att jag informerar dom som ska ta emot det här, vad det innebär och hur man ska handskas med det, och vilka farorna är. Och detta kommer i alla fall bara räcka en viss bit. Men återigen om man lyckas hindra att 1000 blir brottsoffer är det bättre än att inte hindra någon.

Ja men precis, och om vi säger att någon ringer upp med ett spoofat telefonnummer så att det ser ut som att det är banken som ringer, vilka typer av frågor bör man ställa för att kunna verifiera att den som ringer verkligen är från banken?

Såhär, är man det minsta osäker på om det är banken som hör av sig eller en myndighet eller skatteverket då ska man motringa, inte ringa det nummer som står i mailet eller i SMSet, man ska ringa bankens på det nummer man själv har eller som man själv slår fram på Google. Sen dubbelcheckar man det verkligen är ni som ringer om det här när man är det minsta osäker. Man ska bli osäker när de vill att du ska ge ifrån dig pengar eller koder eller för att logga in på något sätt.

Ur de iakttagelser vi har gjort har vi insett att det finns ju på BankIDs hemsida så finns det mängder av varningar, och även på bankernas hemsidor. Hur kommer det sig att denna information inte når ut till alla? Att det fortfarande är folk som råkar ut för detta?

Ja och det kommer alltid vara så. Brev fortsätter att fungera där det står att "jag är värd 38 triljarder i diamanter för att jag hade en släkting som heter Karlsson som dött i klamydia". Så går man på detta, ja herregud då är det självklart att det alltid kommer finnas kvar. Men antalet måste bli så få som möjligt. När checkhäftet försvann 1996, 95 var det lika hög grad av bedrägerier som idag, då rörde det sig istället om checkhäften, och det var inte speciellt tekniskt som lösning. Det kommer alltid finnas, man kan bara motarbeta det så mycket som möjligt, och få så många som möjligt att efterleva som 10,3 miljoner invånare.

Och nu i och med eiDAS som innebär att man kommer kunna använda e-legitimationssystem i hela EU, hur tror du att detta kommer påverka den kriminella verksamheten på ett geografiskt plan?

Man befarar ju alltid att det finns en risk att vi ska godkänna alla andra länders legitimationssystem. Är det så att säkerheten är så pass hög som vi önskar överallt, ja då ska det inte vara några problem. Men om något land har en sämre produkt med lägre säkerhet ja då kan det bli läskigt. Det går inte att avgöra idag, i den bästa av världar fungerar allt bra.

Tror du att det finns en risk med att se utländska ligor som försöker angripa den svenska bankmarknaden?

Ja självklart, de är supersnabba. Om de hittar en lucka kommer de utnyttja det.
Vi har haft lite svårt att hitta källor på det men finns det en liknande problematik i andra medlemsländer med just BankID?

Det har jag faktiskt inte tagit mig tid till att kontrollera, jag vet inte. Jag vet att det finns problem med tyska postens e-legitimation, eller de har flera e-legitimation, men den ena var mycket sämre. Men jag tyvärr ingen koll på detta så jag ska inte uttala mig, men det hade varit intressant att veta. Jag tror att Sverige kanske har uppmärksammat det mer än andra länder, eftersom vi rent preventivt är mer aktiva inom myndigheterna och journalistkåren. Vi skriver ju rätt mycket om det här än andra länder. Jag menar att vi har en helt annan kultur, vi hade 260 000 anmälda brott och vi är 10,3 miljoner invånare, i Finland är dom 5 miljoner invånare och dom har 12 000 anmälda brott. De ska ju ha 130 000 om det ska stämma per capita, men de har bara 12 000, resten anmäler inte.

Det är ju väldigt intressant.

Det är ju det. Statistik är ju sådär alltså. Det häftigt och snyggt sådär men man måste fundera på varför siffrorna visar det som dom gör. Det måste ligga något annat bakom förändringarna. Geografiska skillnader påverkar ju också.

Appendix 3 Transkribering Boris Berberovic

Då börjar vi lite med social engineering, utifrån den litteraturen som vi har tagit del av så betyder social engineering; att man manipulerar människor genom vilseledning för att få ut information, eller för att få individen att utföra en åtgärd. Håller du med om den definitionen?

Ja.

Kopplat till BankID bedrägerier, vad vet du om det?

Jag vet att Social engineering, jag har varit i branschen i 20 år, och redan från start har man pratat om social engineering, det vill säga; målmedvetna personer som vill infiltrera ett visst företag eller ett nätverk. Man har ju oftast börjat på den sociala biten, genom att ta sig in fysiskt på företaget på ett eller annat sätt.

Yes.

Genom det interfacet där företaget kommunicerar med sina kunder, eller tillskansa sig på något sätt åtkomst till andra delar av företaget. Jag tror det är egentligen om man möjligheten att "vara där" så är det den enklaste, vad ska man säga, vägarna in. De flesta företag är ju, om man säger, det finns ju företag som har mycket fokus på fysisk säkerhet. Dom företagen ligger oftast efter på dom mjuka delarna, dvs informationssäkerhetsdelen.

Om vi säger traditionellt om såna företag, som oftast har fysiska anläggningar där dom bedriver någon typ av verksamhet som är av allmänt känslig typ, tryckerier exempelvis, som tar fram lotterier. Exempelvis **hör ej** där jag jobbade dom hade stora anläggningar där dom skrev ut tusentals miljoner fakturor, tillverkade sim-kort lotterier osv. Registreringsskyltar [...].

På sådana anläggningar, sådana företag har den fysiska säkerheten varit på ganska hög nivå, och informationssäkerheten halkat efter. Medan exempelvis dom företag som hanterar dom största värden idag, är mer eller mindre digitala. För att dom behandlar tusentals, miljontals, hundramiljonertals personuppgifter av olika typ. Dom företagen har i allmänhet haft dålig koll på fysisk säkerhet, mycket bättre koll på informationssäkerheten. Så att om man nu ska attackera den typen av företag så är det oftast via social engineering.

Om man kollar på exempelvis BankID, det är en väldigt populär applikation i Sverige (ca 8 miljoner användare) Hur ser du på den typ av bedrägerier som sker där, skulle du betrakta det som en typ av social engineering?

Ja absolut, men jag skulle också betrakta det som en bug.

Förlåt vad sa du?

Som en bug, som en brist i systemet. För det här är ingen ny företeelse. BankID var en digital lösning på den här två-faktors autentiseringen har haft sårbarhet sedan 2011 *kan ej höra*

Därför att man gör samma sak egentligen, man ringer och presenterar sig som en banktjänsteman, dom utsatta, dom människor som är mest utsatta är äldre människor, som inte

är så vana vid IT. Kanske yngre också men kanske dom inte har lika mycket medel på sina konton så de är besparade från attackerna.

Ja precis.

Men det är en bug, för man har inte tänkt på risken när man har rullat ut tjänsten. Man borde ha tänkt på den risken eftersom dosorna som fanns innan, man gjorde samma sak med dosorna, att man ringde personen och presenterade sig som banktjänsteman, bad personen skriva in sin kod och då tror personen, "ja men skriv in din kod men berätta inte koden för oss, din kod är hemlig" men vi vill ha.

Svarskoden?

Ja precis

Det är jätteintressant det du säger, det verkar ju finnas rätt så uppenbara brister med BankID applikationen, du som jobbar med IT-säkerhet, finns det några särskilda brister som utlyser sig?

Det är en av de större bristerna, jag skulle exempel säga, jag har inte swish, jag har inte swish eftersom swish läcker personuppgifter. Det räcker att man skriver ett nummer, så ska man initiera en överföring till det numret, swish berättar vem som är ägaren till det numret. Och det är personuppgifter som läcks, det ska inte ske. Man ska som mottagare välja om man vill att det här numret ska ta del av ens egna personliga information

Jag förstår vad du menar, att dom visar vad det finns för koppling mellan ett telefonnummer och en person.

Precis, och som mottagare ska man kunna välja om man vill det eller inte. Om man går tillbaka till BankID, som jag sa till dig innan, det är relativt på det sättet att hanteringen är säker. Det är inte perfekt men det funkar. Dom borde ju ha lärt sig av sin erfarenhet med dosan att det borde finnas en administrativ, en process dvs om det är någon från banken som ringer, för det första jag tror också det är en brist på utbildning, dvs kunden, när man får ett BankID, man måste också få en kort utbildning, kanske tre slides på mobiltelefonen som säger, ringer det någon från banken som gör detta och detta, och dessutom skulle den här utbildningen kunna vara, hur ska man säga?

Obligatorisk?

Obligatorisk men också flexibel, så att varje gång det uppstår nya risker så ska man kunna berätta det till mottagaren. Dessutom så ska man också kunna få de här utbildningarna obligatoriskt på mobiltelefonen, Ok nu vill du använda BankID, du har inte genomfört den här utbildningen, jag menar utbildningen, den kan vara 5 minuter, den kan vara 5 sekunder den kan vara en timme. Man får hitta en balans där, man får se en video, man kan genomföra ett quiz, man kan läsa någon text, man kan ta det på många olika sätt, jag tror att man är rädd för att krydda till det, men samtidigt tar man bort det essentiella i det, dvs att det är inte självklart när man laddar ner BankID hur man ska använda det.

Nä.

Jag fick lära mina föräldrar, som är i 60 års ålder, hur man ska göra. Det är inte alltid intiutivt att man ska "klicka på det här fältet" när man ska signera. Speciellt om man inte ser så bra, som ofta är fallet för äldre personer.

Jag tycker att det är en väldigt intressant del du lyfter, vi instämmer helt i det du säger, dvs att det borde finnas någon obligatorisk utbildning innan man kan använda applikationen. Tror du att det finns någon annan sak man skulle kunna göra från BankIDs håll för att minska antalet bedrägerier?

Det är implementera en administrativ åtkomstprocess, differentiera när kunden identifierar sig, nu finns det olika, vad ska man säga, delvis på bankens sida så skulle man kunna ha bättre igenkänning, AI, för att känna igen bedrägerimönstret.

Ja.

Då skulle man kunna titta på var ligger IP adressen någonstans.

På den som begär inloggningen, kontra den som bekräftar den?

Ja, och då ska det dyka upp på skärmen, en bekräftelse, att nu har du loggat in från den här IP adressen från den här staden, är det du? Det skulle man kunna ha på en initial inloggning. Men jag skulle också lägga in en, någon form av, administrativ process som gör att man kan få support via BankID, Jag menar att det finns en varierande grad av hur mycket man kollar. Jag kan ta ett exempel, båda mina föräldrar har glömt sina koder till dosorna för att de använder BankID, de identifierar sig med fingeravtryck eller med ansikte. När dom skulle falla tillbaka (failover är dosan) så ringde dom, när ena föräldern ringde banken så ställde dom många kontrollfrågor, och då var det Swedbank. Men när dom ringde, när andra föräldern ringde till en filial av Swedbank, vi tror att banken, bara för att Swedbank äger dom att dom har samma system, men det har dom inte.

Nä.

Så ställde dom exempelvis inga kontrollfrågor, dosan räckte för att, för att få…

För att få ett nytt BankID?

Då fick man inga kontrollfrågor, som var har du handlat senast, hur mycket har du på kontot cirka? Osv osv? Och det var ju mina *hör ej*

Jag tror att man definitivt kan förbättra det administrativa interfacet, dvs när banken erbjuder support för appen, man skulle kunna använda video exempelvis för att koppla upp sig på telefonen, sätta på kameran och få människan att verifiera sig, så att man vet vem man pratar med och kan ställa frågor till personen, som varför behöver du detta? Jaha det är någon som ringer dig och behöver din kod, då vet vi att det är bedrägeri på gång

Det är jättebra idéer faktiskt, om man vänder lite på det och kollar utifrån bedragarnas synvinkel, vilken typ av förberedelse krävs för att kunna genomföra såna här attacker?

Vad tror ni själva?

Vi menar ju, ofta är det ju, ett exempel som vi har i vår uppsats är att om man går in på bankernas Facebook sidor, så ser man att folk öppet ställer frågor, till exempel såhär: Jag

behöver hjälp med min pension, och sen, då menar vi att det blir väldigt enkelt för en bedragare att ringa upp den här personen; "Hej jag ringer från banken", och då med hjälp av spoofing få det att se ut som att det är banken som ringer.

Jag skulle ha en helt annan approach, jag skulle titta på, vi har ju fortfarande väldigt mycket öppna databaser på olika invånare i Sverige. Och om jag vill exempelvis lura systemet så vill jag, om jag bor i Stockholm, så vill jag ändå ringa stockholmare, för att om banken har ett AI system som är så pass intelligent, och de blir bättre med tiden, så blir det ändå så att jag kan lura systemet så att jag åtminstone IP-mässigt befinner mig i Stockholm. Sedan hade jag gått in på, om vi säger, ja det räcker med Eniro eller Hitta.se och beställa Ratsit katalogen, det går ju att få digitalt eller fysiskt, jag använder digitala, sen tittar jag på någon, då cementerar jag ut, då kan jag väldigt enkelt cementera ut alla över 65 eller 70 med personnummer, som har ett visst, om vi säger, om dom har en bra pension, om dom har en bra pension, om dom har en bra årlig omsättning för att vara en pensionär, då tror jag att man kan cementera ut dom, sedan kan man relativt enkelt se, hur många är skrivna på den här adressen, för man vill fokusera på dom som är ensamma, för dom får ju ingen hjälp, och dom kan inte fråga någon annan, och tredje alternativet är att anta att dom antingen har Nordea eller Swedbank. Nordea och Swedbank är de största bankerna där du har ett personkonto, och då är det väldigt enkelt att säga, hej jag ringer från Swedbank, så ringer man en annan gång och säger att man ringer från Nordea, det är antingen eller, så har man 50/50 chans att lyckas.

Ja, det där är jätteintressant, I vilken mån tror du att bedragarna gör sådana här background checks, innan de väljer ut sina ringlistor?

Jag tror att de gör det, för det är helt onödigt att bedriva, man slösar, väldigt mycket tid på att genomföra ett framgångsrikt bedrägeri men sedan se att personen har 20 000kr på kontot. Det är mycket bättre att med hjälp av en extern tjänst som Merinfo eller liknande där man faktiskt kan köpa den informationen. Det är väldigt enkelt att hitta målgruppen, säg över 65, jag skulle kanske till och med säga 70–80 och hitta den största omsättningen och fokusera på dom.

Det där är superintressant, du har varit inne och nuddat lite på det där med att man väljer att rikta in sig på äldre? Varför tror du att bedragarna väljer att rikta in sig på äldre?

För att dom är inte utbildade, dom har inte den här misstänksamheten, dom har inte *hör ej*, dom litar fortfarande på den som ringer, dom har en annan typ av förtroende, ofta så har dom en telefonlinje, ringer man via telefonlina så är det ofta något viktigare än när man ringer via mobiltelefon, dom bedragarna som ringer, jag har läst en massa förundersökningar, som jag har laddat ner via flashback till exempel, det kan ni också göra. Dom brukar prata helt perfekt svenska, även om det är en svenskfödd eller utländskt född person, så pratar dom väldigt bra svenska. Dom har redan byggt upp ett manus, som gör att det låter väldigt professionellt, jag tror till och med att de har erfarenheten, utav någon form av telefoni, service, kundtjänst erfarenhet. Jag har hört inspelade samtal med dessa personer, det låter mycket professionellt.

Kan man få ut inspelningarna från förundersökningen? Vet du det?

Jag tror att man kan få vissa saker ut, jag har fått dom via andra vägar.

Det här med att man angriper äldre, statistiken håller helt med om det, BRÅ säger tillexempel att medianåldern för en person som faller offer för en sån här attack är 56, tror du att det här är någonting som har förändrats över tiden eller har man alltid valt att angripa sig på äldre när det gäller finansiella bedrägerier?

Det är självklart att man ska fokusera på de äldre, i den typen av bedrägerier, det finns ju andra orsaker till det också, ni kan ju hitta orsaken i den svenska lagstiftningen. Polisen är inte utbildade för att ta hand om sådana här case, dom hamnar oftast på hyllan, står där länge. Det blir därför väldigt svårt att spåra dom här bedrägerierna. Polisen fokuserar på dom casen där man bedriver våldtäkt, misshandel etc.

Bankerna har också varit väldigt snabba med att ersätta de här personerna, deras förlust, genom försäkringsbolag. Det är ett triangeldrama om vi säger så, det är brister i systemet, brister i kunskap hos kunderna till banken, men också bristen hos polisen, om jag säger svenska domstolsverksamheten.

Om vi pratar lite mer om metoder, såsom vishing och phising. Vilka metoder använder bedragarna för att praktiskt lura individer?

Man skulle kunna säga att dom som gör det, då är det vishing. Det är den absolut bästa vägen till att göra det eftersom man får en fysisk kontakt med offret. Då får man mycket större förtroende, dom som ringer har ofta en ganska stor erfarenhet av företag, eller av den typen av verksamhet där man suttit i ett callcenter. Phising är mer fokuserat på, Vishing fokuserar på ett segmenterat urval av offer medan phising tar stort antal mail-adresser och hoppas på att man får napp på kanske, på åtminstone en promille, eller ännu lägre. Vishing är mer sofistikerat, det är mer personligt eftersom man får den här kontakten med personen.

Jätteintressant, dom fallen som vi har läst om, har det nästan uteslutande handlat om vishing, när det kommer till BankID, har du hört om några andra bedrägerifall? Där man har använt andra metoder, just när det kommer till BankID.

Nej, inte när det kommer till BankID. Då är tillvägagångssättet alltid detsamma. Jag tror att väldigt få personer har BankID på en fil, då ska man fysiskt hacka sig in i den enheten som har den här BankID som en fil. Dom flesta har det på sina mobiltelefoner, Jag tror oavsett att det är samma som det fanns på *hör ej*. Det är exakt samma sak, varför vi har nu den här GDPR lagen det är för att just exponeringen av personer, personlig information. GDPR lagen säger att din personliga integritet är grundläggande, det är en rättighet inom EU. Och dessutom är dina personuppgifter nu bara till lov, du äger dom så länge du lever. Det finns väldigt mycket information man kan få ut, både genom offentlighetsprincipen men också genom andra tjänster, som inte riktigt är reglerade som dom ska. GDPR är en relativt ung lag och det har inte blivit reglerat ännu, så det går ju att få ut en mängd information om olika typer av personer, och sen väldigt snabbt identifiera, flera hundra om inte flera tusen personer som man kan fokusera på.

Ja, nu går jag lite of topic men tror du att vi måste förändra offentlighetsprincipen för att kunna motverka sådanna här attacker i stor utsträckning?

Det tror jag, jag tror att man ska använda… Jag tror att myndigheterna ska kombinera delvis när man vill få ut offentliga handlingar, man ska inte få dom anonymt, man ska verifiera sig. I kombination ska det finnas en spårbarhet i detta. Detta ger sedan polisen möjligheten att säga "okej, den här personen har blivit utsatt för brott. Vem är det som har tagit ut offentliga handlingar?". Om detta kommer, tror jag att de kriminella kommer få ett regressivt beteende och börja fokusera på att ta del utav den information genom att exempelvis; man kan ju köra igenom ett mindre svenskt samhälle där de flesta har en postbox utanför huset. Där kan det finnas ett brev från banken, man tar det brevet och får tillräckligt med information. Men detta blir mycket svårare så att säga. Men spårbarhet, och att ta bort anonyma krav. Nu behöver inte

den personen få veta om det. Ibland kan det vara lite känsligt om du ringer och vill fråga vad din chef har för lön, eller vad din kollega för lön. Men jag tror att starten (kan inte höra sista).

Ja det där är intressant, för jag själv har testat att ringa sådanna här samtal. Jag insåg också att det är väldigt enkelt att få ut vad någon tjänar till exempel.

Ja, och man kan gå till service-kiosken på skatteverket för att ta ut information där och så vidare och så vidare.

Precis, och om vi går in lite på medvetenhet hos användarna, eller vi kallade det för kunder tidigare, bankens kunder, i vilken mån spelar medvetenheten kring informationssäkerhet hos användaren roll i dom här BankID attackerna?

Det är den största bristen absolut. De tre stora bristerna är; avsaknad av medvetenhet hos offret, avsaknad av kompetens hos polisen och de utredande myndigheterna, och även brister hos tjänsteleverantören vilket i detta fall är BankID. Så dom tre. Och då menar bristande som i att det ska finnas på något sätt ett ytterligare steg vid... Om banken får en uppdatering, att det här är något som inte stämmer, kopplad IP-adress är fel, sitter personen någon annanstans ska vi verifiera det. Ska det dyka upp ett nytt system där man identifierar, där banken själv kan få ett larm för att sedan kontakta personen. Ska man kunna identifiera sig med ett foto tillfälligt, som går till bankens SOC security operation center där någon säger att "okej vi avblåser detta för att det inte är den personen". Alltså man kan ju ta olika, man kan ju ringa personen och så vidare och så vidare. Men förbättringar på processen hos tjänsteleverantören. Absolut, jag tror att polisen kommer... Det enklaste är att öka medvetenhet hos kunderna. Det är den största bristen om jag rangordnar dom.

Ja och då blir det här lite av en retorisk fråga men tror du att det finns en direkt relation mellan medvetenhet och success-rate?

Det finns det alltid. Man kan ju ta phishing exemplet, det här har varit väldigt framgångsrikt på massor av företag. Man får ett mail, man klickar på det, man öppnar det, man blir infekterad (av virus). Och företagen har jobbat väldigt mycket med först tekniska åtgärder, men de har insett att de tekniska åtgärderna blir, om vi säger såhär jag berättade på min föreläsning att som här ändrar ju form. Dom här kan vara en länk, kan vara en fil, det kan vara väldigt svårt för de tekniska lösningarna att vara i takt i synk med hur de kriminella utvecklar sina attacker på. Så att det man gjorde istället var att fokusera på från kontrollcentriska åtgärder till människo-fokuserade åtgärder, det vill säga utbildning, medvetande av olika slag. Det har minskat, i alla fall i de organisationer som jag har jobbat på, medvetande metoden, awareness metoden, en kort utbildning krig hur utsatt eller kritisk informationen har fungerat mycket bra.

Ja precis. Och om du fick ge några råd till användare av BankID, vad hade du sagt då för att undvika att du blir bedragen?

Jag skulle kunna säga att, om vi tar mina föräldrar som ett exempel, jag har utbildat dom i detta och sagt att det här förekommer. Bara om ni själva kontaktar banken där ni vet vad ni ringer på för telefonnummer kan ni vara säkra på att mottagaren är rätt. Men om ni inte kan verifiera att dom ringer er och vill hjälpa er, det här har hänt mig personligen ett antal gånger när Microsoft support har ringt mig.

Ja precis med indiska call-centers?

Ja precis, det har hänt mig och det har hänt många andra jag känner, och det är på grund av att Sverige har en stor exponering av sina personuppgifter genom olika typer av databaser och så vidare. Så det är bara för dom att ringa och försöka installera något, exempelvis en klient på ens dator som sedan gör att de tar över den. Och de använder det här för många olika syften. Förut var det väldigt mycket i bitcoin mining och service attacker för att varje hackad dator, speciellt den som var uppkopplad länge, även vad man nu ska säga, vi har ju enheter som är uppkopplade hela tiden under en längre tid som man använder som en router, TV och så vidare som har olika typer av android system, de är värdefulla på det viset.

Precis, men om vi går in lite på tillit till teknologi, anser du att det finns en tillit till de applikationer som vi ladder ner till våra mobiler? Alltså att bara för att det är teknik, att vi inte riktigt analyserar...?

Absolut, det är något som jag i min roll som säkerhetschef på en stor koncern har haft som ett ganska stort problem. Det finns ju väsentliga skillnader mellan appstore och googleplay. anta, hur ska vi kalla det för, antalet misstänkta applikationer, bedrägliga applikationer på google play är mycket större än app store, där apple har mycket starkare och bättre kontroll över applikationer. Och det finns en ganska stor tillit till att det man laddar ner ska göra det den gör, men det finns applikationer som används bland annat för att scanna finansiella tillgångar, men också för att exempelvis skapa fake tinder-konton genom att ta namnet och bilderna ladda upp dom skapa trafik på vissa tjänster som är nya.

Ja precis. Tror du att den här tilliten till teknologi kan vara en faktor till att just den hä typen av attacker är genomförbara? Alltså att många svenskar som inte är teknikvana, laddar ner BankID, och BankID kommer från bankerna och då litar man på denna applikationen och att man tänker att det är en säker applikation.

Mm absolut, det är ju det jag säger, och det är för att om vi säger de yngre personerna de har ju sett detta på ett eller annat sätt, att de har sett hur applikationer inte beter sig korrekt. Man har en mycket högre grad av misstanke bakom, men det är långt från alla. Så jag tror att det finns väldigt stora brister hos leverantörerna där de inte bedriver någon typ av utbildning till användarna, när du laddar ner en så pass viktig applikation såsom en internetbank. Internetbank appar är relativt enkla att jobba med. Men för dom äldre personerna har fortfarande svårt för det här, de kopplar inte det här intuitiva, att det finns en liten fotokamera som man trycker på för att skanna sin faktura exempelvis, och man har inte riktigt fattat det. Det finns ingen utbildning i dom där apparna. De är ju inte så intuitiva, och de blir bara mer komplicerade med tiden. De blir komplexa i och med de funktionaliteter man lägger till. BankID är relativt enkelt men det är fortfarande långt ifrån intuitivt. Exempelvis när man ska signera kommer det upp en sida som man ska läsa igenom och sen klickar man bara någonstans. Det handlar om att behöva gå igenom all text för att kunna klicka vidare. Och då dyker det upp en siffer-modul där du kan knappa in din kod. Det är inte så enkelt. Jag tror inte att man lägger in det för det första; vill man inte kladda till det. För det andra tror jag inte att man tänkt så mycket på det.

Men jag har ytterligare en liten off topic fråga här, tror du att det här har gått lite för snabbt, den här förflyttningen från att gå till bankkontoret till att vi nu kan utföra alla våra bankärenden på mobilen? Alltså att vi har lämnat den här generationen som är född på 40/50/60 talet lite i sticket?

Teknologin kommer alltid gå snabbt och det har alltid gått snabbt. Om vi tittar på förbränningsmotorerna, jag tittade på en presentation från där det år 1901 så var det massor av

hästvagnar och hästar på New Yorks mest trafikerade gata. Medan det 14-15 år efter var det enbart bilar, men bara en häst. Det var hundratals bilar, hundratals taxi, men bara en häst. Det har alltså alltid gått snabbt, och det här är hundra år sedan. Det här kommer hela tiden, nya saker, ny teknologi, nya former av identifieringar som underlättar för oss. Men jag tror att människor inte hänger med. Man får ju höra om alla fördelar "det blir mycket enklare att logga in på banken och betala dina räkningar", men det öppnar ju också upp för risker. Med några knapptryckningar eller ett telefonsamtal kan alla skamma dig på alla dina pengar.

Om man ska vara väldigt pragmatisk, tror du att medvetenhetsträning är lösningen, för att lösa den här frågan på kort sikt.

Jag tror absolut att man ska belysa riskerna, och ta upp det i medierna. Det finns en myndighet i Sverige, som är specifikt framtagen för att hjälpa till med detta, och informera. Det är MSB, myndigheten för samhällsskydd och beredskap, den myndigheten ska ta upp den frågeställningen, utveckla den, och se till att tillsammans med andra myndigheter ge stöd, men först och främst fokusera på att identifiera alla sådana risker gentemot allmänheten, informera och försöka belysa dom. Försöka mitigera dom, men framförallt försöka belysa och informera.

Det vi får veta är bara när något händer, det är ju det som gör nyheter. Vi behöver någon form av, vi behöver 15–20 sekunder inslag på nyheterna, där msb står bakom och informerar.

Som privatperson, om man blir uppringd av någon, det står Swedbank eftersom numret är spoofat, vilka typer av frågor bör man ställa för att verifiera att man verkligen pratar med banken?

Det är svårt att säga, för att du som individ är inte professionell säkerhetskonsult, det är väldigt svårt att säga och dessutom så är de så pass duktiga att dom kan manipulera sig ur dom frågorna. Jag tror att det behövs ett annat system, jag har själv styrt ett sådant whitepaper under några månader, om just bedrägerierna, om först och främst dosorna men även BankID. Jag tror att alla dom behöver ett administrativt interface. När banken kontaktar dig, så ska det komma upp ett interface i appen, där banken verifierar sig mot dig. Det är ju oftast vi som verifierar oss mot banken, men det här måste förändras. Vi behöver få lika mycket tillit med vem vi pratar med på andra sidan, och det här har man inte tänkt på.

Det där är en otroligt bra poäng, det där kommer vi att ta med.

Det är det jag menar med en administrativ process, varje gång du ska få någon form utav stöd, men också vid eventuella upptäckter, incidenter. Jag tror att bankerna skall vara lite mer på tårna, om dom investerar, vilket dom gör, i state of the art AI identifieringssock, de flesta har det. Då tror jag också att BankID måste förbättras genom att implementera support och administrationsfunktionalitet. För banken är vägen in, egentligen inte bara in i banken, utan i våra liv. Vi pratar om Kivra (digital brevlåda), Banken, varje inloggning där du är som medborgare.

Vi har varit inne på det lite förut, men det bidrar till diskussionen. Vi pratade lite om medvetenhet och jag tror att vi kan vara överens om att det är där skon klämmer. Däremot så har vi utifrån våra iakttagelser noterat att det finns mängder med varningar på exempelvis BankIDs och bankernas hemsidor. Varför tror att den här informationen inte når ut?

Vad tror ni själva?

Jag personligen tror att det måste vara obligatoriskt för varje användare, många struntar i att läsa igenom rekommendationer.

I min whitepaper har jag skrivit det såhär; bankens och BankIDs hemsidor är inte det primära kommunikationsinterfacet mot kund. Det primära interfacet mot kunden är appen, det är inte websidan. Jag loggar aldrig in på BankIDs hemsida. Det är apparna som är det primära interfacet, det är där informationen ska komma. Apparna har notificationsmodul, som oftast är påslagen. Det ska vara obligatoriskt påslaget. Jag tycker att man ska rulla ut information den vägen. På vilket sätt man gör det på är avgörande för om användaren tar till sig detta eller inte. Rullar man ut det som en text, om vi ser en väldigt tråkig text. Man måste göra det på ett grafiskt och intuitivt tilltalande sätt, för att man skall kunna ta till sig detta. Sen om man använder video, animation. När jag gjorde implementering av utbildningar på ett stort internationellt företag, som jag var säkerhetschef på. Så var det inte innehållet, vi har ju exempelvis redan en säkerhetspolicy och ett dokument som heter "Acceptable usage of equipment". Vi har inte ens döpt det till IT-equipment, utan det mesta har ju IT inom sig. Det kan ju vara maskiner på arbetsplatsen, om vi säger dom maskiner som hanterar känsliga uppgifter. Våra telefoner, mobiler, det mesta. Där valde vi ett interface, en online utbildning som är mycket mer tilltalande visuellt, som är rolig att hålla på med. Det finns en blandning av animation, video, som är ungefär som en tecknad film.

Det blir lite mer lättsamt för användaren?

Exakt, och språket man använder är superkritiskt. Att språket man använder inte talar bits and bytes. Att man talar språket som tilltalar mottagaren. Det är sådana saker som jag tror saknas helt och hållet. Dom preventiva delarna. Triangeldrama: Preventiva delar är utbildning, reaktiva delar själva utredningen, där har polismyndigheten halkat mycket efter.

Du nämnde ju tidigare det här extra valideringssteget, där banken bekräftar sin identitet gentemot kunden. Hur skulle detta kunna genomföras och hur skulle det påverka användarvänligheten i applikationen?

Jag kallar det för ett administrativt steg, Det är uppdelat i två tillfällen, det första är om banken misstänker ett bedrägligt beteende, det andra är att vi skulle kunna förbjuda banken att ringa sina kunder. Dom ska först via telefonen få en förfrågan från banken, "kan vi ringa, och såhär kommer vi identifiera oss".

Verifiering av båda parter är superkritiskt, i det här fallet jobbar vi bara med det en väg, det är alltid från användaren tillbaka, det tror jag är ett problem.

I september 2018 beslutade man i hela EU att det skall finnas en gemensam infrastruktur för e-legitimationssystem genom eiDAS. Du ska kunna använda varenda medlemslands e-legsystem i andra medlemsländer. Tror du det här kommer att påverka den kriminella verksamheten på ett geografiskt plan?

Jag tror att Sverige ligger i framkant jämfört med andra länder, utan att ha någon jättekoll på andra länders system. Sverige har kommit ganska långt framåt när det gäller e-id och så vidare. EU ska på sikt koppla ihop skattesystem för att förhindra skatteplanering och skattefiffel. Tittar ni idag på text-TV så ser ni att 500 miljarder saknas, för att många företag simulerar att de har betalt en skatt utan att ha gjort det. En av de grundläggande orsakerna bakom GDPR är att skydda sina skatteintäkter. Jag tror inte att enskilda användares

verifiering mot banker är prio nummer ett, om vi säger så. Jag ser att det finns en liten bit att gå där. Jag tror att om vi tar Skandinavien, vi kopierar Danmark och dom kopierar oss.

Danmark låg före oss när det kom till digitala brevlådor, administrativ papperslös kommunikation mot medborgaren. Sedan har Sverige kopierat den här iden. Jag tror att just nu är det varje enskilt land för sig själv men jag tror att på sikt, inom snar framtid, inte 2–3 år men inom snar framtid får vi ett gemensamt EU-baserat system. Men tills dess kommer vi att fortsätta se samma bekymmer. Det är tre parter som behöver ta ansvar; på tjänsteleveranssidan är det BankID, på banksidan och på myndighetsidan. Jag tror inte att man har grävt sig in i djupet, var får bedragarna sin information ifrån. Det kanske också innebär att offentlighetsprincipen blir anpassad eller försvinner helt och hållet.

Vi avslutar där, stort tack för en superintressant intervju. Många nya infallsvinklar som vi inte har tänkt på förut.

Appendix 4 Transkribering Albin Zuccato

Då börjar vi lite med social engineering, utifrån den litteraturen som vi har tagit del av så betyder social engineering; att man manipulerar människor genom vilseledning för att få ut information, eller för att få individen att utföra en åtgärd. Håller du med om den definitionen

Ja, det gör jag nog.

Jag vet inte hur påläst du är på just BankID bedrägerier, men du har säkert läst en och annan nyhetsartikel om det iallafall?

Ja det har jag.

Håller du med om att den typen av bedrägeriverksamhet faller inom ramen för SE?

Ja man ger sig knappast mot själva algoritmen eller tekniken, utan man ger sig mot den svaga länken, och det är ju människan. Så det är absolut en social engineering attack.

Om jag har förstått det rätt så är du affärsområdeschef för säkerhet, eller hur?

Ja, det stämmer bra.

I ditt arbete, har du några exempel på hur du stöter på social engineering?

Ja, man kan säga att man är en användare och då är man ju utsatt i alla fall för riktad phishing attack (spear phishing) och såklart i diskussion med kunderna så nämns social engineering attackerna som ett frekvent förekommande beteende.

Det är något man försöker motverka som säkerhetskonsult?

Ja, det finns olika verktyg, det vanligaste är att man adresserar frågan genom awareness träning, utbildning. Vi har ett antal sådana produkter i vårt erbjudande, Atea har det och min grupp har tidigare på kundens uppmaning sålt sådana lösningar.

Hur ser du på applikationen BankID, utifrån din roll som säkerhetsspecialist? Utifrån media verkar det ju finnas en del brister, vi menar ju som du sa tidigare att det oftast beror på användaren, hur är din syn på detta?

Det finns ett antal tekniska, eller det har rapporterats att det har funnits ett antal tekniska sårbarheter i BankID-applikationen, min position på detta är att det är mjukvara som all annan mjukvara. Det lär därför finnas flera andra sårbarheter men det ligger i naturens sak. Jag tror att BankID har en ganska hög säkerhetsambitionsnivå och håller nog också ganska godtagbar säkerhet i själv verket. Det finns alltid en nivå, och nu har jag inte hört att BankID har utvärderats utifrån en *hör ej* evaluation, eller någon annan evaluation. Det är lite synd kan man tycka, men jag tror trots allt att den svagaste länken är inte applikationen utan användaren och/eller den miljön den befinner sig i. Man kan kapsla en applikation bara så mycket från operativsystemet och dess sårbarheter ärvs naturligt. Då finns den ju på olika operativsystem och jag misstänker att det finns lika mycket exponering därifrån, så det är hela teknikstacken om man vill ifrågasätta den, men jag skulle säga, vad är alternativet?

Precis. Utifrån det vi har läst så är det oftast vishing relaterade attacker som utförs, har du hört talas om några andra BankID-bedrägerier, där man använder sig av andra metoder än just vishing?

Ja, det har rapporterats om Man-In-The-Middle-Attacks mot just BankID, jag vet inte huruvida det har adresserats eller inte. Det fanns någon gång en diskussion om MITM-attackerna.

Ser du några tekniska brister med BankID som applikation mer än att det inte har evaluerats?

Ja det finns säkert ett antal tekniska brister, men jag måste ärligt säga att jag har för lite teknisk insyn i detta för att kunna nämna några.

Jag förstår. Om man kollar lite på själva bedrägerierna, vilken typ av förberedelse krävs för att kunna genomföra exempelvis vishing attackerna? Hur tror du som säkerhetsspecialist att bedragarna går till väga rent praktiskt?

Så dom det berättas om, och det man ser indikationer på. Att man börjar skjuta ganska brett, man gör till och med lite slarv i början, man vill singla ut människor som inte har en hög teknologiförståelse. Man filtrerar ut alla som inte i fortsättning skulle kunna gå på, för det krävs ett antal leads för att kunna göra detta. Man måste ha en viss godtrohet, en viss nivå för att gå på detta. Jag är ganska övertygad att man med flit identifierar ut människor som kanske har lite stavfel, man vill inte ha för utbildade individer som skulle kritiskt fråga, för då behöver man investera för mycket resurser. När man väl har identifierat sådana individer, då läser man upp på den och gör en hel del efterforskning via sociala medier men även andra kanaler för att öka trovärdigheten. Det finns ett antal erkända fenomen för att göra social engineering attacker. Det tillämpas fullt ut.

Tror du att offentlighetsprincipen kan ha en bidragande del i det här?

Nej, phishing förekommer även i andra länder, inte tvär-nej men jag skulle inte säga att det förvärrar eller förenklar saken. Det finns gott om information tillgänglig även utanför offentlighetsprincipen. Jag skulle inte lägga offentlighetsprincipen med i ekvationen. Fördelarna överväger i förhållande till nackdelar om jag ska vara ärlig. Det är iallafall min uppfattning.

Intressant, Du nämnde lite också kring att bedragarna får tag på information via sociala medier, vilka andra kanaler tror du att dom använder sig av för att göra background checks?

Det är oftast fler än en individ, man ger sig nog på olika nivåer på framtida offret för att ta fram information. Enkel Google-sök hjälper, man kan få en hel del information ur arbetsrelationen och hitta och identifiera arbetskompisar. Det är som sagt en liga så man kan göra lite underrättelsearbete för att göra detta, jag tror att det är ganska tydligt kvantifierat, hur mycket arbete du kommer lägga in för att det ska fortsätta vara lönsamt. Jag ser ingen slump i den här processen, den är väl genomarbetad "affärsprocess" från bedragarna.

Du var inne på det lite innan, att man ofta väljer att ge sig på folk som kanske inte har den bästa tekniska bakgrunden, tror du att det finns en särskild målgrupp som bedragarna vänder sig mot?

Det rapporteras en hel del om attackerna mot äldre, men ärligt talat det tror jag inte. Äldre faller offer mer frekvent då tekniken är mer främmande för dom, jag tror det är en omvänd

korrelation. Jag tror inte att man singlar ut dom från början utan det handlar mer om selektionsmekanismer.

Vi har diskuterat just detta i uppsatsen också, att det kan finnas en alternativ förklaring till varför äldre är överrepresenterade.

Min övertygelse är att man skjuter brett, jag tror snarare att det råkar bli så, men jag tror inte att det är riktat i den meningen.

Om man kollar lite mer på typer av attacker, du nämnde tidigare spear-phishing, vi har pratat om vishing. Vilka metoder använder bedragarna om man kollar på dom klassiska SE metoderna?

Jag måste erkänna att jag saknar data, jag avstår från att spekulera.

Om vi kollar lite på awareness, i vilken mån spelar medvetenhet kring informationssäkerhet hos användaren då roll i dom här attackerna?

Till en otroligt hög grad, man måste gå över en viss gräns. Har man blivit utbildad med någon form av medvetenhetsträning eller snarare om man har någon form av medvetenhet så är jag ganska övertygad att man inte skulle gå på. Det krävs en hel del osäkerhet för att gå på dessa punkter. Det har oftast att göra med man inte har full koll på vad som gäller.

Då tror du också att det finns en direkt relation mellan medvetenhet hos användaren och success rate hos bedragarna?

Det är helt övertygad om. Sen kan man alltid råka ut för en mycket skicklig attack, så att säga där man specifikt blir angripen.

Om vi leker med tanken att du jobbar för BankID, vilka råd skulle du ge till användare?

Det vanligaste råd som jag ger exempelvis till min svärmor, om den verkar konstigt, fundera en gång till. I många fall är det, någonting som är lite konstigt och man bör väcka misstroende så fort BankID blir inblandat. Då blir man lite svagare. I mångt och mycket så skulle en liten portion misstroende skulle nog behöva vara där. *Hör ej*

Då är det medvetenhetsträning som är lösningen i mångt och mycket?

Ja, jag vet inte om. Det är en funktion för allmänheten, men att man tar ett ansvar som bank eller finansinstitut att förmedla till kunderna, att online betalning är fördelaktigt och mycket positivt, och det ska du verkligen omfamna kära användare. Så som på vanliga betalningsmetoder, vi kommer inte öppna plånboken och ge 200kr när vi inte förstår riktigt vad dom har gjort för dig.

Precis, tror du att det finns en tillit till teknologin, till applikationer just för att för många är det någonting främmande och nytt?

Jag tror att, ja absolut, det kan jag känna att det är en eventuell förklaring, eller iallafall att det bör betraktas som ett problem. Men om man inte förstår tekniken så har man någonting som ett blint förtroende och en övertro på tekniken. Den är ganska signifikant. Det är kanske vi, om man ska anklaga banken för någonting så har dom underblåst. Det är en positiv konnotation med BankID, där jag skulle säga att vanlig mjukvara lider av samma problem.

Och måste då hanteras med ett annat förtroende, som många andra saker. Den där blinda tilltron den är idiotisk. Den är nog delaktig i en del av problematiken.

Just kopplat till tillit till teknologin, det här är en ganska svår fråga, men har du något exempel på hur vi som användare visar för stor tillit till teknologi generellt?

Oh ja, det finns gott om exempel. Det finns en massa sådana roliga signaturprodukter nu, adobe sign och vad som alla heter nu. Dom känns lite väl luddiga. Om man säger så. Säkerhet måste gå hela vägen och när vi har vissa punkter där det inte finns någon säkerhet eller etablerat korrelation, då blir hela alltet lite svagt. Bara att det finns en adobe sign och det kommer från en mailadress till mig, som identifierar sig i bästa fall med mailadress. Jag skulle säga att den rättsligt bindande karaktären är ganska långsökt. Det är ju krypterat vid överföringen, men när det är addressed på just den servern, även om det bara är en *hör ej*. Där brukar det inte ligga krypterat, just med mail. Ja men min mail kommer in på mailservern och den kommer in krypterat på mailservern just till mig, när man tittar på exchange. Jo, det har ni rätt i men i exchangen som då kontrolleras av en tredje part där ligger det *hör ej* Mail är fortfarande ett mjukt hot även om det är krypterat vid transport.

Vi var inne lite på hur man kan motverka dessa attacker, och då finns det två angreppssätt, vi nämnde medvetenhetsträning innan, som användare, vilka typer av frågor tycker du att man ska ställa om man får ett sånt här samtal, för att kunna verifiera att den som ringer är från banken.

På telefonen finns det inte jättemånga bra identifikationssmöjligheter åt båda håll. Det har ju kompletterats så att man kan ju komma till punkten, hur många känsliga affärer har vi inte tidigare gjort över telefonen, och har vi inte där tänkt på en maximal storlek av affärer som vi vågade göra. Jag skulle säga att det är någon som vill att jag gör någonting förtroenderikt via telefonen så måste man hitta en annan kanal där man kan verifiera identiteten. Det skulle vara jättesmidigt om man hittade en verifieringslösning som fungerar åt båda håll, om jag ringer in till min bank så får jag en challenge från dom och då skulle det vara bra om jag kunde ge dom en challenge.

Det är en potentiell lösning som vi tar upp, att just i BankID applikationen så ska banken verifiera sig genom att skicka en push-notifikation till din applikation?

Ja, precis! Om jag går in på internetbanken så kan jag verifiera deras certifikat så att jag vet iallafall att jag är rätt. Någonting liknande kan man göra genom att pusha ut en notifikationsförfrågan med bankens digitala signatur.

Tror du att man kan lösa det här rent tekniskt utan att påverka användarupplevelsen för mycket?

Det är jag övertygad om att det finns en fullt användbar och tekniskt säker lösning, finns det nu inbyggt? Nej det ser jag inte, men man kommer behöva implementera detta med usability och en design process. Jag ser inte detta som en olösbar situation.

Om vi återgår till medvetenhet, utifrån våra iakttagelser så finns det mängder med varningar på Bankens samt BankIDs hemsidor. Varför tror du att informationen trots detta inte når ut till användarna?

Jag skulle säga, när du installerar mjukvara, hur många användarvillkor har du gått igenom? Och när du signade upp för din bank, har du läst alla dokument du faktiskt accepterade?

Jag tror att vi instämmer helt med dig här, men vi måste ändå ställa frågan…

Om jag försöker formulera mig lite tydligare, information overflow som är en del av vårt moderna samhälle som man framförallt som konsument är utsatt. Det innebär ju att man har inte ork eller möjlighet att ta del av all den informationen som behövs. Inom konsumentskyddslagen har vi identifierat detta och börjat skydda individen bättre och en del typ av lagstiftning kan behövas i det området.

Vi har ett ganska radikalt förslag som vi tar fram, att man skulle förbjuda att banken ringer upp användare, utan att man först har accepterat att ta emot ett samtal genom BankID appen. Exempelvis kan man lösa detta genom att användaren får en notis "banken vill kontakta dig", tror du att det här är genomförbart?

Det är spekulativt, jag vet inte vad jag ska säga. Jag förstår tanken och den är god men jag vet inte om det är praktiskt genomförbart. Det är iallafall värt en diskussion om jag får uttrycka mig så. Jag tänker mig någonting lite smidigare men i tangentens riktning. Jag vet inte om man ska behöva anmäla i förväg om man vill bli uppringd, om man kan göra det överhuvudtaget. Men man bör iallafall bli informerad. Man blandar IT och säkerhet med konsumentskydd och skydd mot reklam och alla dom delarna. Det är tyvärr ofta som säkerhet missbrukas för att pusha en annan agenda också. Det skulle jag tycka vore olyckligt. Den här lösningen har iallafall en del sådana aspekter. Min rekommendation är att ni tar en exekutiv ställning där man gör detta eller inte gör detta. Bankerna vill ju gärna kontakta sina kunder för aktiv marknadsföring. Det är ett mycket hett och omdiskuterat ämne. Varför ger man sig in för att skydda BankID applikationen med detta?

Kan du inte utveckla det lite? Det här med att man använder det som marknadsföring.

Det finns europeisk och amerikansk och på internationell nivå en hel del diskussion, om direktmarknadsföring, och riktad marknadsföring. Det opinionerna går isär från varandra, och många menar att det finns ett betydande intresse för en aktiv direktmarknadsföring. Bankens kontakthavande med sina kunder borde inte blandas ihop med detta, det är min farhåga i den diskussionen. E-commerce directive med flera andra diskuterar detta, jag menar att man ska inte blanda ihop dessa då det är en säkerhetsfråga i allmänhet.

Stort tack för ditt medverkande Albin. Det var alla frågor.

Referenser

Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*(pp. 62-68). IEEE

Alvehus, J. (2013). *Skriva uppsats med kvalitativ metod: en handbok* (1 uppl.). Stockholm: Liber.

Andersson, J., & Lärka, P. (2019) Bedragare lurade äldre på hundratals miljoner. Retrieved April 27, 2019 from https://www.svt.se/nyheter/lokalt/skane/polisen-har-slagit-till-mot-en-bedrageriharva

Bhagyavati, B. (2007). Social Engineering. In *Cyber Warfare and Cyber Terrorism* (pp. 182-190). IGI Global.

Brottsförebyggande Rådet (BRÅ). (2016). *Bedrägeribrottsligheten i Sverige*. Retrieved April 27, 2019 from https://www.bra.se/download/18.358de3051533ffea5ea2ec64/1458044205141/2016_9_Bedr%C3%A4geribrottsligheten_i_Sverige.pdf

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

Buvik, A. (2018). Bedrägerier via bank-id ökar explosionsartat. Retrieved April 10, 2019, from https://www.svt.se/nyheter/lokalt/varmland/bedragerier-via-bank-id-okar-explosionsartat

Ekblom, B. (2018). Så tog bank-id-bedragarna alla Jennys pengar. Retrieved May 16, 2019 from https://pcforalla.idg.se/2.1054/1.691958/bankid-bedragare-scam

Finansiell ID-Teknik BID AB. BankID och säkerhet. (2019). Retrieved April 8, 2019, from https://support.bankid.com/sv/sakerhet/bankid-och-sakerhet

Finansiell ID-Teknik BID AB. Historia. (2019). Retrieved April 8, 2019, from https://www.bankid.com/om-oss/historia

Finansiell ID-Teknik BID AB. Om bankid. (2019). Retrieved April 8, 2019, from https://www.bankid.com/om-bankid/detta-ar-bankid

Friedman, B., Khan Jr, P. H., & Howe, D. C. (2000). Trust online. *Communications of the ACM*, *43*(12), 34-40.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report*, *8*(4), 597-606.

Granger, S. (2001). *Social engineering fundamentals, part I: hacker tactics.* Security Focus.

Hadnagy, C. (2011). *Social engineering: The art of human hacking*. Indianapolis: Wiley Publishing.

Husz, O. (2018). Bank Identity: Banks, ID Cards, and the Emergence of a Financial Identification Society in Sweden. *Enterprise & Society*, *19*(2), 391-429

IDG:s ordlista, Intrusion detection system (IDS). Retrieved May 8, 2019, from https://it-ord.idg.se/ord/intrusion-detection-system/

IDG:s ordlista, penetrationstest. Retrieved May 8, 2019, from https://it-ord.idg.se/ord/penetrationstest/

Ivaturi, K., & Janczewski, L. (2011). A taxonomy for social engineering attacks. In *International Conference on Information Resources Management* (pp. 1-12). Centre for Information Technology, Organizations, and People.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94-100.

Kaushalya, S. A. D. T. P., Randeniya, R. M. R. S. B., & Liyanage, A. D. S. (2018). An Overview of Social Engineering in the Context of Information Security. In 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS) (pp. 1-6). IEEE.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

Lankton, N. K., McKnight, D. H., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association for Information Systems*, *16*(10), 1.

Larsson, P. (2018). Polisen varnar för ny bluff med bank-id. Retrieved April 11, 2019, from https://www.aftonbladet.se/nyheter/a/bKrzQl/polisen-varnar-for-ny-bluff-med-bank-id

Larsson, S. (1986). *Kvalitativ analys-exemplet fenomenografi*. Studentlitteratur.

Mann, I. (2008). Hacking the human: social engineering techniques and security countermeasures. Routledge.

Manske, K. (2000). An introduction to social engineering. *Information systems security*, *9*(5), 1-7.

Mouton, F., Leenen, L., & Venter, H. S. (2015). Social engineering attack detection model: Seadmv2. In *2015 International Conference on Cyberworlds (CW)* (pp. 216-223). IEEE

Nationalencyklopedin, e-legitimation. Retrieved May 8, 2019, from https://www-ne-se.ludwig.lub.lu.se/uppslagsverk/encyklopedi/l%C3%A5ng/e-legitimation

Nationalencyklopedin, hackare. Retrieved May 8, 2019, from https://www-ne-se.ludwig.lub.lu.se/uppslagsverk/encyklopedi/l%C3%A5ng/hackare

Nationalencyklopedin, phishing. Retrieved May 8, 2019, from https://www-ne-se.ludwig.lub.lu.se/uppslagsverk/encyklopedi/lång/phishing

Nationalencyklopedin, vishing. Retrieved May 8, 2019, from https://www-ne-se.ludwig.lub.lu.se/uppslagsverk/encyklopedi/lång/vishing

Offensive Security. (2019). *Our Most Advanced Penetration Testing Distribution, Ever.* Retrieved April 9, 2019, from https://www.kali.org/

Postnord. (2018). *E-handeln i Norden*. Postnord. Retrieved April 27, 2019 from https://www.postnord.se/vara-losningar/e-handel/e-handelsrapporter-och-kundcase/e-handeln-i-norden?aliId=eyJpIjoiaE95bElQdmhqZUJzQ05WZCIsInQiOiJGT2FzMDJXaE82cmtNR3preVZzczdBPT0ifQ%253D%253D

Rienecker, L., & Stray Jørgensen, P. (2014). *Att skriva en bra uppsats* (3 uppl.). Malmö: Liber.

SEB. (2019, 04-11). In *Facebook* [Group page]. Retrieved May 11, 2019 from https://www.facebook.com/sebsverige/

Svensk E-IDENTITET, EIDAS | Med Svensk e-identitet blir anslutningen enkel. Retrieved May 8, 2019, from https://e-identitet.se/tjanster/inloggningsmetoder/eidas/

Swedbank Sverige. (2019, 04-11). In *Facebook* [Group page]. Retrieved May 11, 2019 from https://www.facebook.com/swedbanksverige/

Wollner, A. (2018). Läsarnas värsta skräckhistorier om Bank-ID – lurad på 56 000 kr. Retrieved from https://pcforalla.idg.se/2.1054/1.706477/bank-id-bedragerier

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297-307.

Domar

Hovrätten för västra Sverige Dom 2018-10-12 Mål NR B 3386–18.

Göteborgs tingsrätt Dom 2018-06-04 Mål NR B 1070–18.