Institutionen för Informatik

Phishing - ett säkerhetshot mot Internetbanker

Kandidatuppsats, 10 poäng, Informatik

Framlagd: 2007-01-17
Författare: Kalle Rajala, Tomasz Gidzgier
Handledare: Anders Svensson
Examinator: Erik Wallin

Abstrakt

I takt med den snabba utvecklingen av tjänster på Internet har flera av de ärenden som förr utfördes ansikte mot ansikte hamnat i den virtualiserade världen på Internet. Bankerna har tagit del av denna utveckling och fått de flesta kunder att utföra sina ärenden via deras Internettjänster. Denna möjlighet att utföra sina bankärenden på Internet har inte enbart varit positiv. Phishing är ett problem som dykt upp i samband med den här utvecklingen. Syftet med denna uppsats är att undersöka utifall det finns en medvetenhet hos bankanvändaren gällande Internetbankens säkerhet samt hur användarna hanterar den säkerhetsinformation som banken ger ut. Med hjälp av en enkätundersökning ska medvetenheten bland användare gällande Internetbankens säkerhet kartläggas. En jämförelse görs mellan två svenska banker, Swedbank och Nordea där likheter och skillnader belyses. Resultatet från enkäterna tyder på en riskmedvetenhet bland kunderna från vardera bank. Resultatet visar även att bankerna, speciellt Nordea har lyckats att förmedla sitt budskap till användarna om riskerna. Trots användarnas medvetenhet om riskerna var förtroende bland kunderna för de båda Internetbanker väldigt högt.

Nyckelord: phishing, phishingattack, social engineering, Internetbank, e-postmeddelande, förtroende

Innehållsförteckning

ABSTRAKT ... **2**

INNEHÅLLSFÖRTECKNING ... **3**

FIGURFÖRTECKNING ... **4**

1. INLEDNING ... **5**

1.1 BAKGRUND ... 6
1.2 PROBLEMFORMULERING ... 6
1.3 SYFTE ... 6
1.4 AVGRÄNSNING ... 6
1.5 MÅLGRUPP ... 7
1.6 FRÅGESTÄLLNINGAR ... 7

2. METOD ... **8**

2.1 METODVAL ... 8
2.2 KÄLLGRANSKNING ... 8
2.2.1 Källkritik ... *9*
2.3 ENKÄT ... 10
2.3.1 Enkätens utformning ... *10*
2.3.2 Förberedelse inför enkätundersökningen ... *12*
2.3.3 Urval ... *12*
2.3.4 Enkätens distributionssätt ... *12*
2.4 VALIDITET OCH RELIABILITET ... 12
2.5 EMAIL-KORRESPONDENS ... 13

3. TEORI ... **14**

3.1 SOCIAL ENGINEERING ... 14
3.2 PHISHING ... 15
3.2.1 Phishingsattackens anatomi ... *15*
3.2.2 Säkerhet ... *19*
3.3 FÖRTROENDE ... 20
3.3.1 Vad skapar förtroende? ... *21*

4. BANKENS PRAXIS ... **23**

4.1 NORDEA ... 23
4.2 SWEDBANK ... 24

5. EMPIRI ... **25**

5.1 ENKÄT ... 25
5.2 EMAIL-KORRESPONDENS ... 29

6. ANALYS OCH DISKUSSION ... **32**

7. SLUTSATS ... **38**

7.1 SLUTSATSER ... 38
7.2 KRITISKT GRANSKNING ... 38
7.3 FRAMTIDA FORSKNING ... 39

KÄLLFÖRTECKNING ... **40**

LITTERATUR ... 40
ARTIKLAR ... 40
INTERNETKÄLLOR ... 41

BILAGA 1 ... **43**

BILAGA 2 ... **46**

BILAGA 3 ... **47**

Figurförteckning

Figur 1 Attackens livscykel (Wetzel, 2005, p.47) 16
Figur 2 Exempel på phishing (http://sakerhet.idg.se/2.1070/1.79590) 17
Figur 3, ett exempel på en phishing hemsida (http://sakerhet.idg.se/2.1070/1.79590, omarbetat) 18
Figur 5 Phishingattackernas fördelning på olika sektorer (Symantec Internet Threat Security Report, 2006, p.23) 19
Figur 6 Schema för förtroende mekanism (Foxall et. al, 2005, p.184) 21
Figur 7 Nordeas inloggnings sida (http://app.nordea.se/login/index.html) 23
Figur 8 Swedbanks inloggnings sida (https://internetbank.fsb.se/) 24
Figur 9 Uppsatsens Demografisk Data (Enkät) 25
Figur 10 Genomsnittlig Internetbank användningslängd (Enkät) 26
Figur 11 Svarsfördelning fråga 3 (Enkät) 26
Figur 12 Svarsfördelning fråga 4 (Enkät) 26
Figur 13 Svarsfördelning fråga 5 (Enkät) 26
Figur 14 Svarsfördelning fråga 6 (Enkät) 27
Figur 15 Svarsfördelning fråga 7 (Enkät) 27
Figur 16 Svarsfördelning fråga 8 (Enkät) 27
Figur 17 Svarsfördelning fråga 9 (Enkät) 28
Figur 18 Svarsfördelning fråga 10 (Enkät) 28
Figur 19 Svarsfördelning fråga 11 (Enkät) 28
Figur 20 Svarsfördelning fråga 12 vilka avstod från att använda Internetbank (Enkät) 29
Figur 21 Skälet till avstående (Enkät) 29
Figur 22 Medvetenheten hos respondenterna med fördelningen på respektive Internetbank (Enkät) 32
Figur 23 Respondenternas datorvana med fördelning på respektive Internetbank (Enkät) 33
Figur 24 Hur väl respondenterna läst den säkerhetsinformation som bankerna givit ut med fördelning på respektive Internetbank (Enkät) 34
Figur 25 Respondenternas trygghetskänsla med fördelning på respektive Internetbank (Enkät) 36
Figur 26 Kännedom om begreppet phishing med fördelning på respektive Internetbank (Enkät) 36
Figur 27 Respondenter som avstått från att använda sin Internetbank med fördelning på respektive Internetbank (Enkät) 37

1. Inledning

I detta kapitel presenteras kandidatuppsatsens bakgrund följt av problemformulering samt syfte. Här diskuteras även avgränsningen till kandidatuppsatsen samt målgruppen vilken uppsatsen riktar sig till. Kapitlet avslutas sedan med att uppsatsens frågeställning formuleras.

I takt med den snabba utvecklingen av tjänster på Internet har flera av de ärenden som förr utfördes ansikte mot ansikte hamnat i den virtualiserade världen på Internet. Bankerna har tagit del av denna utveckling och fått de flesta kunder att utföra sina betalärenden via deras Internettjänster (Bankföreningen 2005). Hur pass tillförlitliga är dessa tjänster och vilket ansvar har banken om något skulle gå fel? Idag erbjuder alla de stora bankaktörerna i Sverige ett verifierat utbud av tjänster via deras Internetbank, dessa tjänster är billigare för både kunden och banken (Turban, et al.2004) vilket bidragit till dess popularitet. Bankerna vill upprätthålla tron hos sina kunder att säkerheten är mycket god på deras Internettjänster (Hølle, et al. 2006), men under hösten 2006 uppmärksammades det att Nordeas kunder råkat ut för en phishingattack. Bedragarna lurade åt sig kunduppgifter och kunde därigenom tömma flera kunders bankkonton (Sydsvenskan 2006-11-15). För att kunna upprätthålla god säkerhet måste säkerheten kontinuerligt kritiskt granskas samt utvecklas. Bankerna investerar stora belopp på den tekniska komponentsäkerheten, men har många gånger förbisett den mänskliga aspekten av säkerhet. Enligt en enkätundersökning som publicerades 2005 har 13 % av kunderna i Europa avstått ifrån att använda Internetbanken p.g.a. problemen med identitets stölder (Rombel 2005). Detta är en antydan på att phishing är ett problem som drabbar många Internetbankanvändare. Internetbankanvändandet fortsätter att växa och varje dag tillkommer nya kunder. En del av dessa nytillkomna kunder kommer att lära sig phishing den hårda vägen (Levine 2006). Om ett bedrägeri lyckas, skadas bankens anseende. Förtroende som läggs i bankerna och online transaktioner försvinner och de indirekta kostnader blir till slut mer påtagliga än de direkta kostnaderna (Wetzel 2005).

Få uppsatser inom detta ämnesområde har tidigare skrivits. Tidigare forskning har antagit en forskningsdiskurs som undersöker Internetbankens användargränssnitt i termer av användbarhet (Foxall et al. 2005). Undersökningarna har strävat mot utveckling av hemsidor som ska vara mer användarvänliga. Andra forskningsartiklar har undersökt kundens relation till banken (Johnson & Grayson, 2003). Vilka faktorer det är som bygger förtroende och hur man får kunder att stanna vid en specifik bank. Förtroenderelationen är väldigt viktigt i e-banking eftersom man ställs inför en maskin, ett system som inte har några känslor och inte kan uppfatta det som verbalt sägs (Johnson & Grayson, 2003). Hur ska vi kunna lita på något som vi inte semantiskt kan tolka? Andra forskningsartiklar har belyst ämnet från bankernas synpunkt. Forskningsdiskursen har dock haft en mera ekonomiskt framtoning som bidragit till bankens nytta. Bankerna vill varken verifiera eller dementera incidenter som skett och publicerar ogärna någon statistik om detta (Kane, Bignell 2006)**.**

Användare och deras benägenhet att bli lurade har inte belysts så mycket i Sverige.
Ämnet berörs endast ytligt i dagstidningsartiklar genom klagomål kring bankens bristande säkerhet. Eftersom phishingattacker har blivit allt vanligare i dagens IT-samhälle och är ett växande problem, så är det i allra högsta grad relevant att undersöka användarnas medvetenhet om riskerna. "The lesson is that not matter how strong you build technology solutions to security issues, people can and do give up the keys to the kingdom without thinking about it." (Linda Musthaler, 2006, *How social engineering sinks security, s. 45*).

1.1 Bakgrund

Användandet av bankernas olika Internettjänster har blivit allt vanligare och människor använder de av olika skäl, såsom att betala räkningar, köpa diverse produkter och så vidare. Denna användning är dock inte problemfri och kan innebära vissa risker för användaren. I takt med utvecklingen av komplicerade säkerhetsteknologier har det blivit allt svårare att knäcka den matematiska algoritmen bakom säkerheten. Den tekniska komponentsäkerheten har visat sig på senare tid vara mycket tillförlitlig och det är sällan som säkerheten brister på denna punkt. Allt oftare är det den mänskliga faktorn som brister och det är alltså människan som är den svaga länken (Musthaler 2006). Det är mycket lättare att lura en användare att ge ut sina användaruppgifter till systemet än att hacka sig in i det, bedragaren försöker på så vis komma åt personliga användaruppgifter. Att kunna lura en användare till att ge ut känslig information är exakt vad social engineering grundar sig på. Social engineering har även benämnts som "the practice of tricking" (Hansson, 2006, s.390). Inom social engineering existerar det olika metoder för att uppnå målet med att lura användaren, en av dessa metoder är phishing. Det var en phishingattack som Nordeas bankkunder tidigare i år blivit utsatta för (www.dn.se; Sydsvenskan 2006-11-15). Någon hade försökt att komma åt användarnas känsliga identitetsuppgifter genom att skicka ut ett e-postmeddelande, som innehöll en länk till en fejkad hemsida där användaren ombads att logga in på sitt bankkonto. Utifrån teorin utförs en empirisk undersökning som ska ligga till grund för uppsatsens slutsatser om säkerheten kring bankinloggningen ur ett användarperspektiv.

1.2 Problemformulering

Ett stort problem idag och som ständigt växer är phishing. Phisihing är något som har drabbat många bankkunder världen över. Phishing är ett stort problem då det är kostsamt för både den banken och individen som drabbas. Bankerna fungerar utifrån en förtroenderelation gentemot kunden (Turban, et al.2004; Johnson & Grayson, 2003). Om en attack riktas mot en bank kan detta leda till att bankens rykte försvagas, vilket i sin tur kan skada kundens tilltro till banken (Levine 2006). De phishing attacker som skett under senaste tiden har varit riktade mot Nordeas kunder, och Nordeas säkerhetssystem har därmed fått mycket kritik (Sydsvenskan 2006-11-15). Denna kandidatuppsats kommer att titta närmare på utifall kundernas tilltro gentemot Internetbanker har minskat i samband med den ökade mängden phishingattacker. Uppsatsen kommer även att undersöka vilka åtgärder bankerna vidtar för att informera kunderna om riskerna gällande bankinloggningen på Internet. Det är bankkunderna som använder sig av tjänsten och det är dessa som i första hand blir drabbade om något går fel. Därför anser vi att det är viktigt att utgå ifrån användarperspektiv, det är således användaren som skall svara på frågor kring detta växande problem.

1.3 Syfte

Syftet med denna uppsats är att undersöka utifall det finns en medvetenhet hos bankanvändaren gällande Internetbankens säkerhet samt hur användarna hanterar den säkerhetsinformation som banken ger ut. Med hjälp av en empirisk undersökning ska medvetenheten gällande Internetbankens säkerhet kartläggas.

1.4 Avgränsning

Avsikten med uppsatsen är att undersöka Internetbankens säkerhet vid inloggningsprocessen ur ett användarperspektiv. Den tekniska komponentsäkerheten och dess påverkan utelämnas för att avgränsa uppsatsen något. Vidare avgränsas uppsatsen ytterligare genom att endast

privattjänster på två svenska banker undersöks, nämligen Nordea och SwedBank. Anledning till att endast två banker undersöks är den korta tidsramen för uppsatsen samt att ytterligare inloggningstekniker skulle göra uppsatsen allt för bred. Anledningen till att valet föll på dessa två specifika banker är att Swedbank har det största antalet Internetbankkunder i Sverige samt att Nordea har näst flest Internetbankkunder i Sverige. Ytterligare anledningar till valet av dessa två banker är att de representerar olika inloggningstekniker, men som samtidigt delar samma grundprincip. Nordea tillämpar skrapkort med engångskoder medan Swedbank använder sig av en elektronisk dosa som genererar engångskoder. Tillsammans är Nordea och Swedbanks Internetkunder representanter för större delen av Internetbankkunderna i Sverige (http://www.bankforeningen.se/upload/internetbank_2005.pdf).

1.5 Målgrupp

Denna uppsats riktar sig till informatikstuderande samt systemutvecklare som intresserar sig för säkerhet och vill skapa sig en bredare uppfattning om ämnet. Uppsatsen riktar sig även till andra datorkunniga personer som har ett intresse för säkerhet och vill skapa sig en bredare uppfattning om de olika dimensionera inom säkerhet.

1.6 Frågeställningar

• Hur medvetna är bankanvändarna om riskerna gällande bankinloggningen på Internet?
• Hur förhåller sig bankanvändaren till den säkerhetsinformation banken tillhandahåller?

2. Metod

I detta kapitel beskrivs de metoder som använts för data insamlingen till uppsatsens empiri. Vidare beskrivs metoderna för insamlingen av enkät samt eMail-korrespondens. Innan respektive del presenteras en kort beskrivning av uppsatsens vetenskapliga förhållningssätt.

2.1 Metodval

Utifrån litteratur tillsammans med den empiriska undersökningen analyseras bankernas säkerhetsinformation samt hur användarna förhåller sig till dessa. Detta görs för att få fram vilket ställningstagande användarna har till banksäkerheten samt till den säkerhetsinformation banken ger ut. En enkätundersökning utförs på användarna där resultatet blir en fingervisning kring bankkundernas kunskap om ämnet samt deras riskmedvetenhet. Den empiriska undersökningen består av enkäter samt eMail-korrespondens med SITIC (Sveriges IT Incident Centrum), som är en oberoende organisation som är en del av Post och telestyrelsen.

Enligt Bryman finns det två forskningsmetoder, den kvalitativa och den kvantitativa. Valet av forskningsmetod bör utgå ifrån uppsatsens frågeställning samt den problemformulering som uppsatsen har (Bryman 2002). Det finns en del skillnader mellan det kvalitativa och det kvantitativa förhållningssättet. Den kvalitativa ansatsen har ett mera induktivt synsätt där tyngden läggs på att generera teorier medan kvantitativa har ett deduktivt synsätt på teori och forskning, där tyngden läggs på prövning av befintliga teorier (Bryman 2002).

Tillvägagångssättet som tillämpas i denna uppsats är utav en mera kvantitativ natur, dock med inslag av den kvalitativa. Fördelen med ett kvantitativt angreppssätt är att man kan generalisera undersökningens resultat och dra generella slutsatser (Bryman 1997). Ett kvantitativ förhållningssätt har valts för att det underlättar när man vill kunna kvantifiera resultaten från den empiriska undersökningen. Genom att samla in kvantifierbar data med hjälp av en enkät, har den data sedan kunnat bearbetas och analyseras. Detta har gjorts för att kunna påvisa likheter och skillnader samt för att kunna ge en övergripande bild mellan de olika bankkunder som nämnts tidigare. Dessa likheter och skillnader går sedan att presentera med hjälp av statistiska diagram. Genom att ställa en öppen fråga i slutet av enkäten har även en bit av den kvalitativa tillvägagångssättet fångats in.

I undersökningen används flera olika informationskällor: böcker, akademiska forskningsrapporter och Internetkällor. Ett objektivt ställningstagande eftersträvades gentemot det undersökande fenomenet i den möjligaste mån. Personliga åsikter kan inte åsidosättas och påverkade arbetet samt utvecklingen av undersökningens tillvägagångssättet. Vissa problem kunde anses som triviala och därför antogs en distanserad relation till problemet.

2.2 Källgranskning

I början av uppsatsen fanns en förförståelse om ämnet som baserades på författarnas egna uppfattningar och idéer. Uppfattningar och idéer hade ingen vetenskaplig anknytning utan dessa var genererade utifrån allmäntillgänglig information. När litteraturen granskades ändrades uppsatsens inriktning som därmed blev mera avgränsad och specificerad allt eftersom problemområdet minskande. Med hänsyn till denna avgränsning och förförståelse började insamlingen av litteraturen. Informationen som inte tycktes vara relevant avfärdades och det som belyste problemområdet från olika synvinklar togs med.

2.2.1 Källkritik

Enligt Denscombe (2004) består inte litteraturgranskningen av en rad sammanfattningar av relevant publicerad litteratur utan, målet är att skapa en övergripande bild över hur litteraturen beskriver uppsatsens problemområde. Enligt Bell (1995) ska materialet analyseras utifrån extern och intern kritik. Med extern kritik syftar man till att upptäcka huruvida en källa är äkta eller ej. Intern kritik innebär att källans innehåll utsätts för en rigorös granskning. Artiklarna som använts i uppsatsen har hämtats från Lunds universitets databas ELIN som anses vara en mycket tillförlitlig källa. På följande vis kunde den externa kritiken säkerställas. Eftersom ELIN databasen ger möjlighet att specificera en sökning, kunde en överrensstämmelse med andra artiklar säkerställas. Artiklarna använder begreppen så som phishing och social engineering på ett enhetligt sätt som reflekteras i uppsatsen. De flesta artiklarna fokuserar på banken som en ekonomisk institution vars varumärke kan skadas av en social engineering attack.

En fråga som Bell (1995) ställer är om författaren varit vittne till det denne beskriver d.v.s. arbetar eller forskar personen kring fenomenet eller är detta en utomstående observatör. Artikelförfattarna till artiklarna som använts i uppsatsen är personer med olika bakgrund inom säkerhetsbranschen vilket ökar relevansen. Att relevansen ökar beror på att dessa artikelförfattare är aktiva deltagare på Internet med många års erfarenhet samt arbetar eller forskar inom olika områden på Internet som driver utvecklingen.

Enligt Bell (1995) är en viktig tumregel att de tryckta material som används inte ska vara för gammalt d.v.s. den ska vara tidsenligt till fenomenet. Detta försökte efterföljas vid val av forskningsartiklar, där de flesta artiklar är högst ett par år gamla. Ett medvetet val gjordes att endast använda forskningsartiklar som högst var ett par år gamla, eftersom det fenomen uppsatsen beskriver är ett relativt nytt fenomen.

En annan fråga som man ska ställa är, stödjer andra oberoende källor med det som sägs i artikeln? Eftersom phishing och social engineering begreppen beskrevs på ett likartat sätt i alla de artiklar som använt i uppsatsen, kan det med stor sannolikhet anses att dessa artiklar speglar fenomenet på ett korrekt sätt. Dock skiljer sig artiklarna i den mån att de tar upp fenomenet phishing och social engineering ur olika syvinklar. Detta ses inte som ett hinder eftersom en bredare bild kan skapas av fenomenet och dess implikation inom olika områden. En del av artiklarna belyser problemet ur bankens perspektiv, t.ex. hur mycket pengar banken förlorar på phishingattacker (Sydsvenskan; Levine 2006). Medan andra tar upp den tekniska delen där den matematiska algoritmen bakom inloggningsprocessen belystes (Hølle et al. 2006). En del artiklar belyser hur phishingattacker genomförs och hur dessa attacker i bästa möjliga mån kan förhindras (Wetzel 2005, IT Pro, Berghel 2006).

Några tidigare forskningsrapporter som berörde uppsatsens specifika problemområde kunde inte hittas. Däremot fanns mycket information som berörde problemområdet utifrån andra perspektiv. En forskningsrapport berörde social engineering som ett socialt och vetenskapligt fenomen (Hansson 2006). Andra rapporter tog upp problemet med autentiseringen i e-banking miljö (Bignell 2006). Nästa rapport var en fält studie som utfördes i England av forskarna vid Cardiff University och syftade till att undersöka de faktorer som skapar förtroende i E-banking (Foxall et al. 2005).

De Internetkällor som användes i uppsatsen har genomgått en kritiskgranskning genom att titta på närmare olika faktorer. Faktorer som granskats är t.ex. när hemsidan senast uppdaterades, vem som bidrar till informationen samt vilken anknytning sidan har till andra

företag eller hemsidor. En säkerställande faktor var att se att vilken anknytning sidorna hade till olika företag som sysslar med säkerhet inom den privata- samt företagssfären. Ett stort samarbete mellan olika Internetsidor och säkerhetsföretag hittades. Flera sidor som t.ex. www.esecurelive.com och www.antiphishing.org är sponsrade och stödda av en mängd säkerhetsföretag. Antiphishing's Workgroups hemsida (www.antiphishing.org) har bland annat samarbete med olika länders myndigheter. Detta nationella samarbete mellan olika nationer och deras bekämpning mot incidenter på Internet kunde även bekräftas hos SITIC som är Sveriges IT Incident Centrum. Information hämtades även av ledande leverantörer av säkerhetslösningar för virus och brandväggar: Symantec, McAfee. De olika leverantörer av säkerhetslösningar och organisationer kan vara politisk påverkade i fråga om tillhandahållen information. Det bestämdes att de informationer är ytterst relevanta och ska användas i uppsatsen trots att en viss skevhet i tillhandahållen data påträffades (Symantec Internet Threat Rapport och APWG phishing rapport).

2.3 Enkät

Enkätundersökningen består av strukturerade frågor som respondenterna kan svara på medan de väntar i kön till bankomaten eller efter ett uträttat bankärende. Målet var att få in 60 svar, varav 30 från vardera bank. För att få 30 respondentsvar från vardera bank, delas enkäten ut tills antalet är uppnått för vardera bank. Det medvetna valet till att 30 respondentsvar från vardera bank eftersträvades var att detta ansågs vara tillräckligt för att kunna ge en fingervisning av hur de båda bankernas Internetbankstjänst kunder upplevde säkerheten kring sin bank. En enkätundersökning anses vara en lämplig datainsamlingsmetod ur ett kostnads- och tidsperspektiv. Resultatet av denna enkätundersökning kommer att ge en fingervisning ur ett användarperspektiv. För att nå populationen som består av bankkunder som använder Nordea eller Swedbank, kommer enkäten att utdelas till bankomatkunder vid respektive bankomat och bankkontor. Med bankkunder menas de personer som är 18 år och äldre som använder Nordea eller Swedbank. Anledning till att använda oss av personer som är 18 år och äldre, är att dessa enligt lag kan inneha ett bankkonto och är i juridisk mening ansvariga för sitt handlade. En bred åldersintervall valdes för att inte gå miste om någon relevant data. Populationsantalet kommer att utgöras av antalet insamlade enkäter. Bortfall kan delas in i intern och extern bortfall (Patel & Davidsson, 1991). Internt bortfall menas de bortfall som sker då t.ex. respondenterna inte besvarar alla frågor i enkäten, och därmed påverkar resultatet. Med externt bortfall menas de bortfall som sker t.ex. vid utdelningstillfället, där respondenterna inte vill delta. Externt bortfall kommer givetvis att förekomma, då personer inte vill delta i enkätundersökningen. Att enkäten besvaras anonymt samt att den inte tar många minuter att besvara, hoppas författarna på följande sätt minska bortfallet. Andra bidragande åtgärder för att minska bortfallet är vid utdelningstillfället, eftersom enkäten kommer att delas ut framför respektive bankomat och bankkontor därmed öka sannolikheten att nå populationen och minska bortfallet.

2.3.1 Enkätens utformning

R. Patel & B.Davidsson (1991) har beskrivit olika riktlinjer för att undvika de vanligaste felen vid utformningen av enkäter. När det gäller frågornas formulering bör följande undvikas:

• *Långa frågor*
• *Ledande frågor*
• *Negationer*
• *Dubbelfrågor av typen: Brukar ni stanna hemma på er semester eller brukar ni åka utomlands?*
• *Förutsättande frågor: Har ni slutat dricka alkohol?*

(Patel & Davidsson 1991, s.65)

Vid utformningen av enkäterna har dessa riktlinjer efterföljts i bästa möjliga mån. Ett krav på respondenterna har varit att de ska vara Internetbankkunder i Nordea eller Swedbank. Ett val gjordes att respondenterna skulle svara anonymt på enkäterna av den enkla anledning att personuppgifter inte ansågs påverka resultatet av enkätundersökningen. Anonymiteten anses bidra till ett ökat deltagande bland respondenterna, då de flesta kan uppfatta bankrelaterade frågor som högst personliga (Patel & Davidsson, 1991). Detta eftersom frågor kring banken kan associeras med privatekonomi. Enkätens utformning består av strukturerade frågor för att komma åt strukturen hos användaren och inte processen. Med struktur menas de faktorer som påverkar användarnas trygghetskänsla. Respondenterna får i detta fall samma frågor och svarsalternativ. Den kvantitativa metoden generaliserar på så vis ett samhällsfenomen genom att ge en mera statisk bild. Genom att ta på oss den statiska utgångspunkten kan en regelbundenhet beskrivas som utmärker ett samhälleligt liv, d.v.s. ett mönster kan upptäckas (Bryman 2002, 1997). Genom att använda strukturerade frågor med fasta svarsalternativ på enkäten underlättas hanteringen av resultaten samt att respondenterna slipper då formulera sig och skriva hela meningar.

Enkäten består av 12 frågor (Se Bilaga 1) för att respondenterna på ett smidigt och snabbt sätt ska kunna svara på dessa frågor och inte hinna tappa intresset. Målet har varit att enkäten ska kunna besvaras inom en kort tidsperiod. Enkäten är utformad genom att demografiska frågor ställs i början, för att kunna försöka fånga ett mönster mellan kön, ålder och utbildning i samband med deras riskmedvetenhet. Därefter tillfrågas respondenten vilken bank denne är kund hos, samt hur länge denne har använt sig av Internetbanken. Nästa frågan behandlar respondentens personliga uppfattning om riskerna gällande inloggningen på Internetbanken, där denne kan kryssa i ett av tre alternativ som överrensstämmer bäst med hans/hennes uppfattning. Fråga fyra berör respondentens datorvana där fyra svarsalternativ ges. Svarsalternativen tolkas från de längsta till den hösta användningens utsträckning. Fråga fem och sex behandlar respondentens uppfattning om bankens säkerhetsinformation. Först tillfrågas respondenten om denne har läst säkerhetsinformationen på bankens hemsida. Respondenten ombedes även att ange hur väl insatt han/hon är i säkerhetsinformation samt hur denne ansåg denna är utformad. Fråga sju, åtta och nio berör phishingfenomenet, först frågas respondenten ifall denne mottagit någon e-postmeddelande från sin bank samt ifall han/hon följt anvisningarna i e-postmeddelandet. Fråga nio avslutar med att fråga ifall respondenten känner till någon annan som mottagit ett liknande e-post meddelande, för att kunna få en uppfattning om phishingattacken omfattning. Fråga tio används som kontroll fråga till fråga tre där enkätens påverkan kontrolleras. I de frågor som behandlar respondenternas ställningstagande mot påståendena tillämpas en likertskala. Bara fyra fasta svarsalternativ används utan att ett medelvärde kan väljas, detta medför att respondenterna tvingas att ta ställning. Neutrala svar undviks för att få ut de ytterst relevanta av attityds frågan. Eftersom enkäten inte är ute efter att ta reda ifall respondenten känner till populära termen phishing, utan istället ifall respondenten känner till fenomenet. Genom att fråga respondenten ifall denne avstått att använda sin Internetbank ville en påverkan av phishing påvisas.

2.3.2 Förberedelse inför enkätundersökningen

Vid utformningen av enkäten dyker en viktig fråga upp, ger enkäten den information som den är avsedd för? För att verifiera att frågorna på enkäten skulle fungera så som tänk gjordes ett antal förberedelser innan genomförandet av enkätundersökningen. Genom att följa
Patel & Davidsson (1991) riktlinjer och formulera frågorna på ett tydligt och korrekt sätt kunde många enkla fel undvikas. Därefter testas frågorna på ett antal individer vars uppgift är att betrakta frågorna objektivt. Denna kontroll görs för att se ifall någon av frågorna kan missuppfattas eller på något annat sätt vara otydligt formulerad. Efter genomförandet av denna utomstående kritiska granskning kunde en pilotundersökning av enkäten göras. I pilotundersökningen testades enkäten på ett fåtal personer inom målgruppen för att verifiera ifall enkäten fungerade så som tänkt d.v.s. besvarar den frågorna kring problemområdet.

2.3.3 Urval

Vid en kvantitativ studie är urvalet av respondenter mycket viktigt, detta eftersom urvalet måste vara representativt för den population som undersöks (Bryman 2002). För att undvika ett missrepresentativt urval nämner Bryman ett antal olika metoder för hur ett urval av respondenter kan gå till. I denna uppsats valdes att tillämpa ett bekvämlighets urval. Det blev ett bekvämlighetsurval eftersom de tillfrågade respondenter bestod av personer som var tillgängliga vid bankomater och bankkontor. Ett antagande gjordes att representanterna för populationen skulle befinna sig vid respektive bankomat som därmed skulle öka sannolikheten att nå rätta representanter för vår population. Målgruppen för enkäten är således Internetbankkunder av båda könen, i ålderspannet 18 år och uppåt, och som är kunder hos antingen Swedbank eller Nordea.

2.3.4 Enkätens distributionssätt

Då de respondenter som deltar i enkätundersökningen inte erhåller någon ekonomisk eller någon annan form av kompensation för att deltaga, är det viktigt att ge en motivering till varför de ska deltaga. En motivering kan vara att påpeka till respondenterna att deras bidrag är viktig samt att enkäten inte tar lång till att fylla i (Patel & Davidsson 1991). Viktigt att poängtera i just denna uppsats enkätundersökning är att enkäten besvaras anonymt. Detta tros påverka deltagandet i enkätundersökningen positivt.

För att minska det interna bortfallet med ofullständigt ifyllda enkäter tillfrågas respondenterna om de använder sig av sin Internetbank för att t.ex. betala räkningar. Därmed kommer endast de som använder sig av en Internetbank att besvara enkäten. Eftersom enkäten delas ut framför bankomater och bankkontor samt tack vare att den endast tar några minuter att besvara, så sker insamlingen av enkäterna löpande allt eftersom respondenterna blir klara. Därmed blir det inget bortfall på svarsfrekvensen, vilket annars lätt kan ske om man har t.ex. använder sig av en webb- eller postenkäter, där man är beroende av att respondenterna själva skickar in enkäten med ifyllda svar.

2.4 Validitet och reliabilitet

Reliabilitet säkras genom att mätningen inte utsattes till slumpinflytelser. Mätinstrumentet är en enkät där alla personer tillfrågas på ett likadant sätt. Trost (2001) nämner fyra komponenter som utgör reliabiliteten: kongruens som rör likheter mellan frågor som avser mäta samma sak; precision som hänger samman med hur svaret registreras; objektivitet som har att göra med hur svaren registreras av enkätens utformare och konstans som tar upp tidsaspekten av studien. Kongruens uppnådds genom att frågorna i enkäten endast berörde ett fenomen och täckte de relevanta nyanser av fenomenet. Precisionsaspekten berör enkätens grafiska

utformning. Enkäten är utformad på ett ledande sätt för att ikryssningen av svarsalternativen ska ske på ett logiskt sätt. Objektivitet uppnås genom att alla svar kodas på ett likadant sätt. Eftersom enkäten är utformad på överskådligt sätt lämnar den få möjlighet till feltolkning av svarsalternativen. Det undersökande fenomenet ändras inte under undersökningens gång. Denna studie ska undersöka ett fenomen som inte är styrd av tiden därmed har det ingen betydelse om respondenterna svarar på enkäten på en måndag eller på en fredag, fenomenet kommer fortfarande att existera.

Vid kvantitativa studier ska frågorna och situationen vara så standardiserade som möjligt. Enkäten i denna uppsats är ett instrument genom vilket man standardiserar svaren och omständigheterna. Varje respondent får själv läsa frågorna och de olika svarsalternativen, för att vid någon oklarhet mottaga samma typ av feedback som övriga respondenter, detta för att enkäten skall vara så standardiserad som möjligt. Eftersom frågorna på enkäten är strukturerade med fasta svarsalternativ får respondenterna i detta fall samma frågor och svarsalternativ, därmed är det högst troligt att en annan genomförd enkätundersökning skulle kunna få samma svarsmönster. Genom att använda samma enkät (Se bilaga 1) går det att replikera vår undersökning, och därmed testa reliabiliteten i undersökningen (Bryman 2002).

Med validitet menas att instrumentet ska mäta det den är avsedd att mäta (Trost 2001). Innan enkäten användes i den slutgiltiga formen som presenteras i (Bilaga 1) testades den av utomstående personer för att säkerställa validiteten s.k. pilotundersökning. Validitet och reliabilitet står i förhållande till varandra (Patel & Davidson 1991) vilket innebär att man inte koncentrera sig på en av dem. Utformningsarbetet leddes på sålunda sätt att bägge faktorerna togs med i beräkning.

2.5 eMail-korrespondens

Det visade sig att bankerna var ovilliga att kommentera phishing ärenden. Upprepade försök gjordes att kontakta någon säkerhetsansvarig på vardera banken för att få en kommenterar kring phishing, men utan framgång. Efter några misslyckade försök bestämdes att kontakta en oberoende organisation som bevakar IT trafik i Sverige. Flera författare bl.a. (Hølle et al. 2006) till artiklar som används i uppsatsen påpekar behovet av säkerhetsanalys av någon oberoende organisation.

En telefonkontakt upprättades med SITIC (Sveriges IT Incident Centrum) där det bestämdes att frågorna skulle skickas via e-post och där de sedan kunde vidarebefordras till någon ansvarig som kunde besvara frågorna. E-postmeddelandet bestod av sju strukturerade frågor. Fördelen med intervju via e-post var att ingen intervjuareffekt på de svarande. D.v.s. att intervjuaren som personen påverkade inte respondenten. Intervjun kändes inte heller så påtvingat som det är i enkäternas fall. Ett intrång gjordes i personens vardag men det lämnar större tidsutrymme till svaren. Svartillfället är också mindre stressande och respondenten kan ta tid på sig. Nackdelar med sådana intervjuer är bl.a. annat att respondenten kan kolla igenom alla frågor först och sedan bestämma sig hur svaret blir. Då kanske respondenter undviker att försäga sig om något viktigt. Man vet inte heller vem som besvarar frågorna i verkligheten och man kan inte hjälpa till personen ifall det uppstår något missförstånd.

3. Teori

I detta kapitel förklaras de teorier utifrån vilka arbetet genomförs. Ett vidkommande problem med säkerhet och social engineering är att de finns få vedertagna teorier. Den mesta litteraturen består av branschnormer och rekommendationer vilka man ska följa för att uppnå en tillfredställande grad av säkerhet. Nedan följer en beskrivning av de olika teorier som ligger till grund för denna uppsats.

3.1 Social Engineering

Social engineering har lika många definitioner som författare. Social engineering kan sägas vara en samling metoder för att manipulera människan för att komma åt deras känsliga information. Det är människan som är den svaga länken vid åtkomst av personlig information. Allen (2006) citerar Harl i sin whitepapper där han benämner social engineering som följande: *"…konsten och vetenskapen att få människor till att lyda dina önskemål*" (Författarnas egen översättning, s.4). De flesta aspekter av social engineering är förknippade med stora organisationer där säkerhet och konfidentialitet är en grundläggande byggsten.

För att en social engineering attack ska ske måste en motivation finns hos förövaren som enligt Allen (2006) kan vara något av följande:

- En finansiell intäkt som kan ha olika bakgrunder. T.ex. att någon har skulder och behöver snabbt pengarna. Den potentiella intäkten i phishing är att antingen sälja den drabbade kundens känsliga information, eller använda dennes känsliga information själv genom bedrägeri.
- Egenintresse som t.ex. att man vill ändra sina egna uppgifter i en databas.
- Hämnd som är unik för varje gärningsman.
- Externa påtryckningar då en individ utsätts för påtryckningar från andra.

Enligt Allen (2006) finns en simplifierad modell av social engineering attack som han beskriver som en cykel bestående av fyra faser. Första fasen är insamling av information där förövaren samlar information om den drabbade kunden. Allen beskriver information som t.ex. en lista med anställdas telefonnummer, födelsedatum, företagets arbetsschema etc. Detta kan liknas med den första fasen i en phishingattack vilket presenteras i Figur 1. Andra fasen består av att utveckla en relation med den drabbade kunden. Här skiljer sig phishing och en social engineering attack. I en phishing attack utvecklas inga relationer, den drabbade kunden förblir anonym. När en relation utvecklas måste bedragaren skapa ett förtroende hos den drabbade kunden. Under den tredje fasen av attacken, stjäls information från kunden utan dennes vetskap, genom att bedragaren skickligt lurar kunden till att ge bort den känsliga informationen. Tredje fasen kan även vara början till ett nästa steg av attacken som inbegriper samma cykel. Den sista och fjärde fasen är den verkställande fasen, i vilken den drabbade kunden har utfört det förövaren och därmed är cykeln sluten.

Allen (2006) nämner tolv metoder varav två är relevanta för denna kandidatuppsats. Dessa två är phishing via e-post och phishing attack via hemsida. Dessa två metoder av phishingattacker kombineras ofta genom att kunden får ett e-postmeddelande innehållande en länk till en hemsida. På denna hemsida ombedes kunden att lämna ut sina personliga uppgifter till någon organisation där denne är medlem i. Andra metoder kan t.ex. vara direktkontakt med den drabbade kunden genom att bedragaren t.ex. anger sig för att vara en nyanställd på ett företaget och ber om att låna tidigare anställds inloggningsuppgifter Allen (2006).

Allen (2006) säger att det inte finns något effektivt sätt att helt försvara sig mot en social engineering attack. Det finns alltid en risk att den mänskliga faktorn kommer att påverkas av en social, politisk eller kulturell händelse.

Riskerna går inte att elimineras men de går att minimeras genom att ha kontroll över företagets säkerhet och genom att hålla användarna uppdaterad. Allen (2006) nämner några bra strategier för att motverka phishing attack. Företaget kan t.ex. utbilda sina anställda, klargöra säkerhetspolicyn samt hålla en hög säkerhet på tekniska komponentnivån. Utifall många nya moment implementeras samtidigt kan det uppfattas störande av den anställda och leda till att det uppstår en stor lucka i säkerheten eftersom den ordinära arbetsrutinen som inkluderar säkerhetstänkandet rubbas. Säkerhetsåtgärderna ska inte splittra eller rubba den vanliga arbetsrutinen

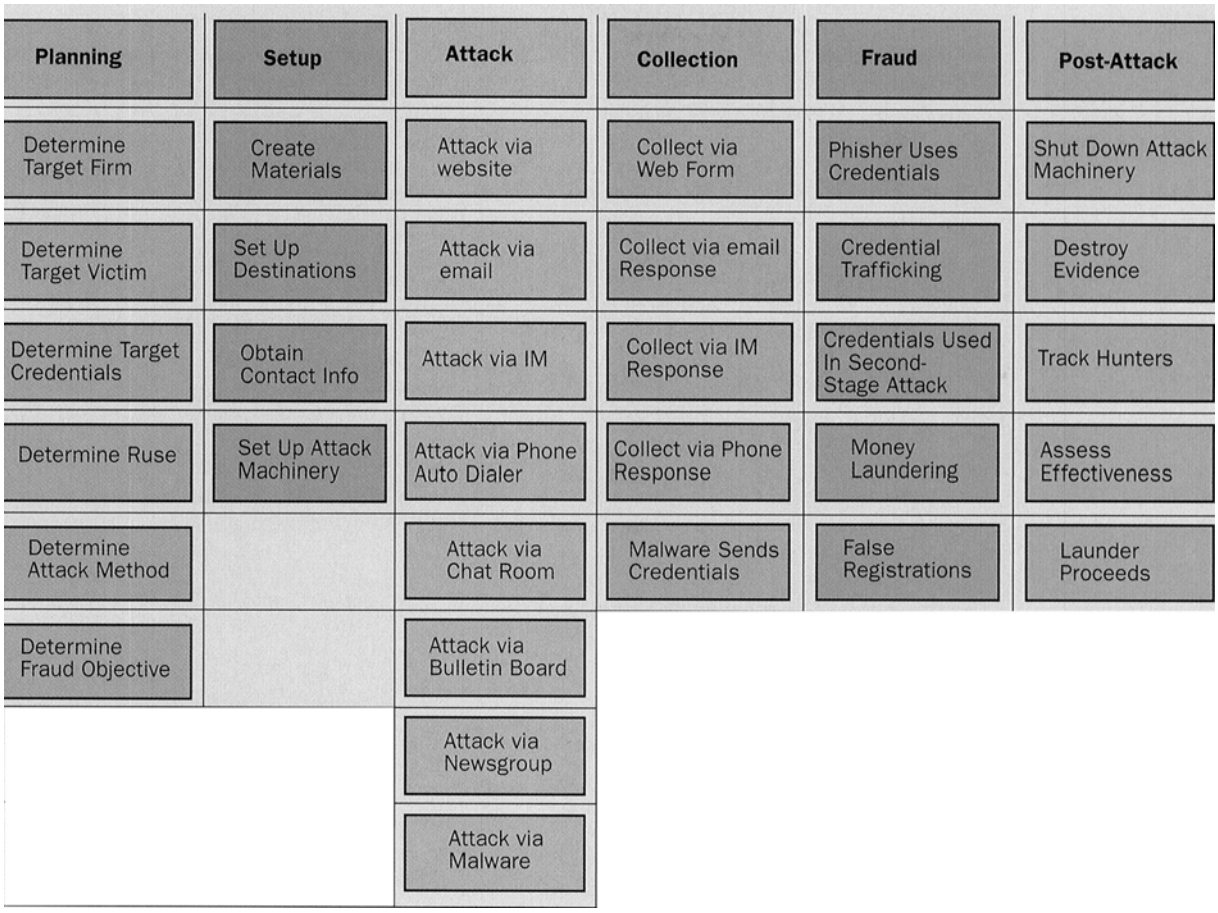
3.2 Phishing

Phishing är en teknisk aspekt ur social engineering där metoden går ut på att lura användaren att ge ut sina uppgifter till bankkonton eller kreditkort, uppgifter såsom lösenord och andra känsliga personuppgifter. I samband med att människor utför allt fler ärenden på Internet har ekonomiska intresset bidragit till att fenomenet phishing drabbar allt fler vanliga människor. Den främsta metoden inom phishing är ett utskick av e-postmeddelande som ser ut att komma från någon bank, kreditkortsbolag eller från något annat stort företag. E-postmeddelandet uppmanar oftast kunden att följa en länk, denna länk innehåller ofta en hemsida som är näst intill autentiskt med företagets egna hemsida, där kunden ombeds att logga in med sina personuppgifter eller koder. Som anledning till det brådskande e-postmeddelandet anges t.ex. vara att banken eller kreditkortsbolaget har förlorat alla uppgifter om kunden och ber därmed kunden att logga in för att undvika att hans/hennes konto blir avslutat (Berghel 2006). Bedragarna skickar ut dessa phishing e-postmeddelande till alla adresser de kan komma åt, i hopp om att någon ska nappa. Taktiken är enkel, bedragarna förlitar sig på kvantiteten av utskickade e-postmeddelanden. D.v.s. av en miljon e-postmeddelanden innehållande en phishingattack kommer någon att nappa (Dhamija et. al 2006).

Det finns ett flertal olika definitioner av phishing som är beroende av hur attacken ser ut. Den gemensamma faktorn för dessa definitioner är att bedragaren vill åt individens känsliga information. Enligt Anti-Phishing Work Group (www.antiphishing.org) kan även phishing förknippas med olika program som stjäl informationen direkt från datorn, t.ex. Trojan Horses, keyloggers osv. I denna kandidatuppsats har det valts att göras en avgränsning endast till phishing attacker visa hemsida i kombination med e-postmeddelandet, därför förklaras dessa termer endast i förbigående. Dock nämns dessa termer för att läsaren ska kunna skapa sig en övergripande bild över vad phishing är.

3.2.1 Phishingsattackens anatomi

Attacken utförs på ett likartad sätt som presenteras i Figur 1. Figur 1 är en taxonomi som presenterades av Financial Services Technology Consortium till att skapa en gemensam terminologi för phishingfenomenet (Wetzel 2005).



Figur 1 Attackens livscykel (Wetzel, 2005, p.47)

Faserna som visas i Figur 1 är detaljerat uppdelade och ska avläsas från vänster till höger, uppifrån och ner. Eftersom phishing är en teknik av social engineering måste en motivation finnas för attacken som enligt (Allen 2006) kan vara följande:

- en finansiell intäkt,
- egenintresse,
- hämnd,
- extern påtryckning.

Kandidatuppsatsen har riktat in sig på den potentiella finansiella intäkten som bedragarna kan lura åt sig. Om inte phishing vore lönsamt skulle ingen syssla med det (Berghel 2006). De två första faserna är planning och setup. Som första steg måste målet bestämmas och därefter vem som ska bli offret. För att en phishingattack ska lyckas, måste den vara utformad på ett listigt sätt. Det är inte konstigt att det dras parallell till vanligt fiske i detta sammanhang. Olika typer av agn används till olika typer av fiskar och vattenområden. För att offret ska nappa på agnen måste den vara utformad på ett korrekt sätt. Berghel (2006) nämner några drag som får agnet att verka verklig:

- den måste se autentisk ut
- måste tillfredsställa den rimliga omgivning, d.v.s. att följa de angivna instruktionerna ska inte verka orimligt
- måste få den tveksamme att avfärda alla misstanker

Som exempel presenteras e-postmeddelandet som många Nordeas kunder fick (Se Figur2).

Figur 2 Exempel på phishing (http://sakerhet.idg.se/2.1070/1.79590)

Något som kan anmärkas på i detta exempel är den dåliga språkkvalitén i e-postmeddelandet som lämnar mycket att önska. Berghel (2006) nämner i sin artikel några exempel på phishingmeddelanden där han graderar varje exempel mellan 0-5 poäng, beroende på hur väl en phishing är utformad. Det första exemplet som Berghel granskar är ett e-postmeddelande som utgav sig att komma från den drabbade kundens bank och även i detta fall visade sig språket vara bristfälligt vilket ledde till att den enbart fick 0.5 poäng ur hans 5-poängs skala. I jämförelsen med e-postmeddelandet som mottogs av en del av Nordeas kunder kunde samma bristfälliga språk påvisas (se Figur 2).

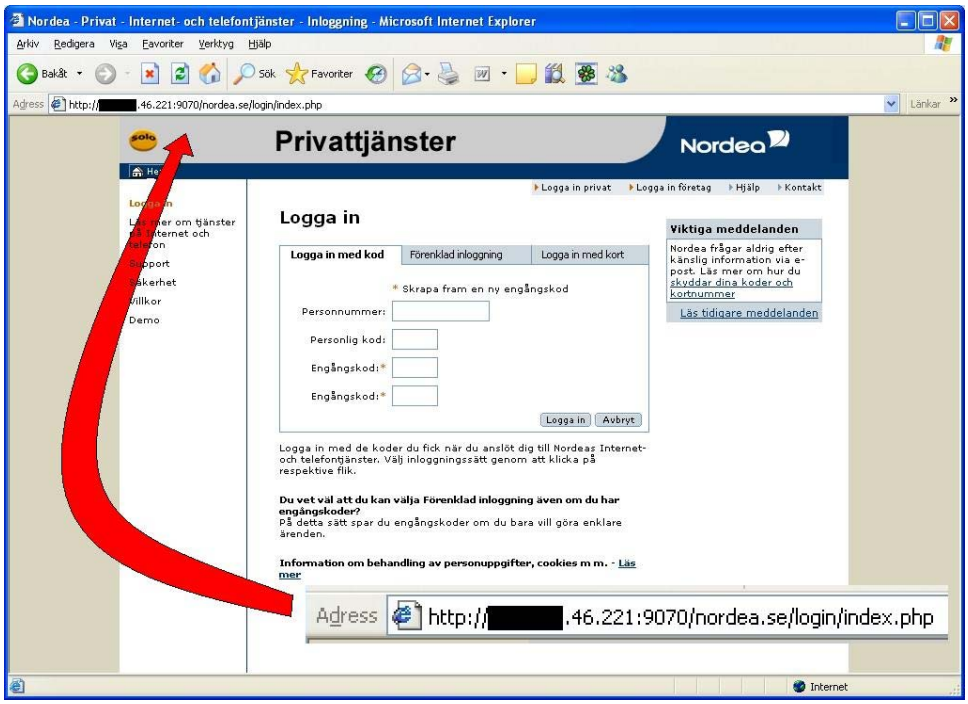
Berghel (2006) ger ingen förklaring till vad olika poäng betyder i hans 5-poängs skala, det är dock bra att ett försök på en skala görs. Genom denna skala kan man kategorisera attackens potentiella fara. Andra skäl till att exemplet från Berghels artikel beskrivs är att flera av de tillfrågade personerna i enkätutdelningen hade reagerat på språket i e-postmeddelanden. Exemplet ovan tyder på att planning fasen är väldigt viktig och e-postmeddelandet måste utformas noga för att få offret att nappa och följa de angivna instruktionerna i e-postmeddelandet.

I setup fasen bestäms målet för attacken. Information samlas in om den drabbade kunden och denna information utformar underlaget till attacken. Bedragaren sätter till sist upp attackens maskineri som i dagens läge har många möjligheter. En attack behöver enbart inte komma från en dator. De flesta bedragarna döljer sig bakom andras IP nummer och använder sig av botnets (Hølle et al. 2006). Botnets är ett nätverk av ofrivilligt kapade datorer som bedragarna har tillgång till och genom vilka de kan starta en phishingattack. Bedragarna kan även stjäla olika domännamn som har en anknytning till den presumtiva banken. Om användaren följer länken i e-postmeddelandet hänvisas denne till en hemsida som härmar den verkliga hemsidan. Allt ser nästintill identiskt ut med originalsidan och för de flesta människor verkar allt vara precis som vanligt. Skillnaden mellan den falska respektive autentiska hemsidan är adressen i adressfältet som visas i exemplet (Se Figur 3). Bedragarna lyckas utifall användaren lämnar ut sina känsliga uppgifter. Det är i attackfasen som bedragarna tar kontakt med den drabbade kunden. När användarna har lämnat ut sina uppgifter sparas dessa hos bedragaren, och därefter hänvisas kunden till den verkliga sidan. I exemplet som visas i figur tre stämmer inte adressen på adressfältet. Den första delen av adressen utgörs av ett IP-nummer där den falska hemsidan befinner sig. Den andra delen av adressfältet är identisk med Nordeas Internet inloggning. Även erfarna användare kan förbise detta att adressen inte

stämmer.

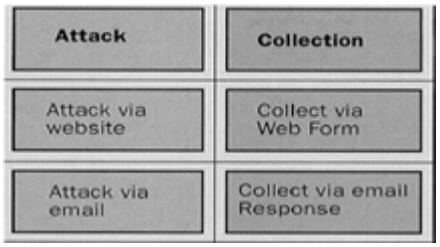
Enligt Boo Ehlin, presschef på Nordea, (Se Bilaga 2) uttalande i Sydsvenskan, ger bedragarna sig på Nordea för att det är den största Internetbanken i Sverige med sina 2,3 miljoner kunder. Eftersom Nordea är störst är givetvis även sannolikheten högre att det falska e-postmeddelandet når fler personer. De e-postmeddelandena som skickades till Nordeas kunder kom från Turkiet (www.idg.se/2.1085/1.79590). De flesta phishingattacker sker från utlandet, som också kunde bekräftas av SITIC (se eMail-korrespondens).

Exemplet med Nordea är bara en av få phishing e-postmeddelande som cirkulerar ute på nätet. Symantec (2006) har uppmärksammat 157 477 unika phishing e-postmeddelanden under första halvåret av 2006. 157 477 delat på 6 månader ger 865 unika phishing e-postmeddelanden per dag.



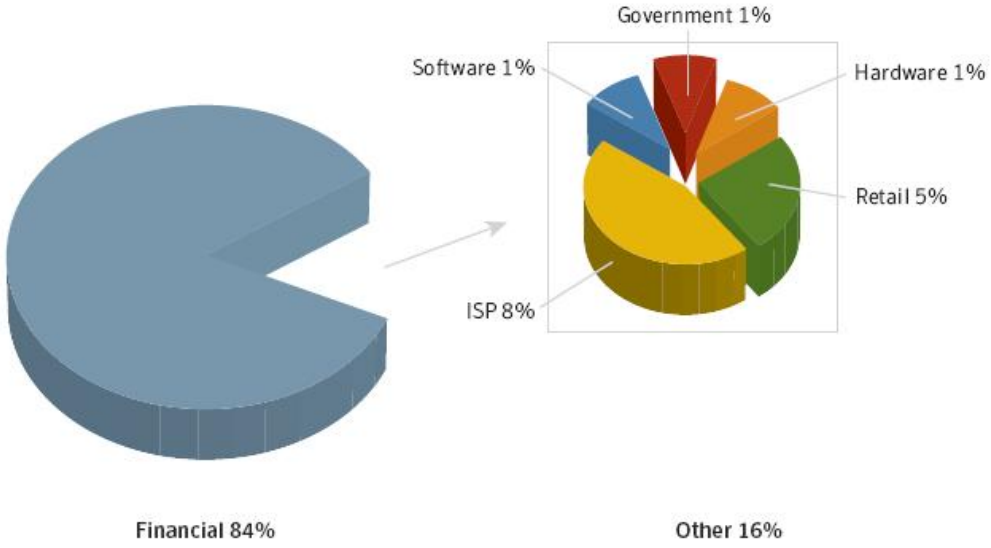
Figur 3, ett exempel på en phishing hemsida (http://sakerhet.idg.se/2.1070/1.79590, omarbetat)

Efter att bedragarna lyckats att samla in de känsliga uppgifterna i collection fasen, som sker via e-postmeddelande eller via ett webb formulär. Så är bedragarna framme vid fraud fasen. Under fraud fasen använder bedragarna den känsliga informationen eller säljer den vidare (Wetzel 2005). Det finns en stor svart marknad för stulna kreditkortsnummer och inloggnings uppgifter på Internet**.** I den sista fasen av attacken uppskattar bedragarna skörden och städar upp efter sig. Figur 4 presenterar visuellt attack- och collection fasen.



Figur 4 Specifik del av attacken
(Wetzel, 2005, p.47, omarbetat)

I de flesta fall är det stora finansiella organisationer som utsätts för phishingattacker. Enligt Symantec (2006) är 84 % av alla attacker riktade mot finansiella organisationer. Symantec är en världsledande leverantör av säkerhetslösningar, deras Internetrapport om säkerhetshot kan dock vara till en viss del överdriven eftersom det kan bidrar till att fler kunder vill ha deras produkter. Denna statistik bekräftas även på andra håll, bland annat hos www.antiphising.org. Statistiken presenteras som ett diagram i Figur 5. Diagrammet är taget ur *Symantecs Internet Threat Security Report*.



Figur 5 Phishingattackernas fördelning på olika sektorer (Symantec Internet Threat Security Report, 2006, p.23)

Det finns många metoder för att motverka phishingattacker. Bland annat finns flera organisationer som försöker motverka phishing genom att uppmärksamma problemet. Ett av dessa företag är Anti Phishing Work Group. Anti Phishing Work Group samarbetar med olika företag i säkerhetsbranschen och har kontakt med olika myndigheter. APWG;s mål är att sprida information om phishing. Symantec har en hemsida www.phishreport.net som samlar in rapporter om nya phishing attentat. I Sverige bedrivs denna verksamhet av SITIC Sveriges IT-Incident Centrum (www.sitic.se) som är en del av Post och Telestyrelsen. SITIC har som mål att sprida information om olika hot som finns på Internet. Att sprida information om phishing anses enligt många författare vara en av de viktigaste och billigaste sätten att motverka phishing (Levine 2006; Allen 2006). För att kontrollera myndigheter och finansiella institutioner krävs det att oberoende organisationer och företag utan egenintresse utför denna kontroll. Bankerna ska utforma säkerhetsinformation på ett begripligt sätt och ska i bästa möjliga mån tillhandahålla denna säkerhetsinformation till sina kunder (Levine 2006).

3.2.2 Säkerhet

Det mänskliga perspektivet inom säkerhet har länge förbisetts. Säkerheten kring inloggningsprocessen på Internetbankens hemsidor är inte enbart beroende av den tekniska säkerheten på komponentnivå utan även den mänskliga faktorn (Musthaler 2006). Givetvis måste den tekniska säkerheten på komponentnivå upprätthållas som garanterar ett antal säkerhetsprinciper. Banken har en hög säkerhetsnivå på sina servrar för att motverka en attack på deras databas. Den höga säkerheten på bankens inloggningsprocess är ingen garanti för att kunden inte kan bli utsatt för ett phishingattentat, eftersom phishing e-postmeddelandet

skickas till kunden. Krav måste även ställas på slutanvändaren d.v.s. Internetbankkunden. David Cole som är director of security product management Symantec *security* nämner i artikeln IT Pro 2005, att det krävs även att användaren har en god Internetsäkerhets hygien (Författarnas översättning p.5). Med god Internetsäkerhets hygien menas sunt förnuft, t.ex. att man inte öppnar e-postmeddelanden där man inte känner till avsändaren, eller ge ut några personliga uppgifter osv. Att kunna balansera och upprätthålla en kombination mellan teknisk säkerhet och säkerhetsmedvetna användare är det som kan minimera riskerna för en phishingattack (Allen 2006).

Ett problem som uppstått i samband med phishingattackerna är att de olika metoderna som används för att autentisera en användare inte varit tillräckliga. Dock är inte detta ett unikt problem för de Internetbanker som har blivit drabbade av phishing. Autentiseringsproblemet är ett generellt problem på Internet i de sammanhang där en användare ombedes att identifiera sig. Att kunna säkerställa användarens identitet till en så hög grad som möjligt är en av grundprinciperna för att minimera riskerna med att en icke auktoriserad person får åtkomst till den känsliga informationen. *”Authentication is a key part of any scheme for preventing unauthorized activity. In a network containing programmable elements, authentication is an essential ingredient for protecting those elements from performing actions illicitly requested by attackers***”** (Schneider, 1999, *Trust in cyberspace, s.56*). Problemet med phishing är det kan vara mycket svåra att upptäcka eftersom phishing är en passiv attack, det vill säga angreppet sker inte vid bankens inloggningsprocess, utan sker passivt via användaren (Bignell 2006). Ett ständigt utvecklingsarbete pågår med att utveckla metoder kring att autentisera en användare. Det pågår en ständig utveckling inom olika metoder för att autentisera en användare. Bland annat utvecklas biometriska tekniker såsom finger avtrycks läsare (Laurence T Levine 2006), dessa nya tekniker kan sedan kombineras med gammal beprövad teknik för att öka säkerheten ytterliggare. Genom att använda fingeravtryckläsare i samband med någon personlig kod, kan säkerheten ökas ytterligare. Dock måste denna teknik vara lätt att använda ur användarens perspektiv likväl som den måste uppfylla kraven på säkerhet (Kane, B. Bignell, 2006). Denna balansgång mellan säkerhet och användarvänlighet är inte lätt att upprätthålla.

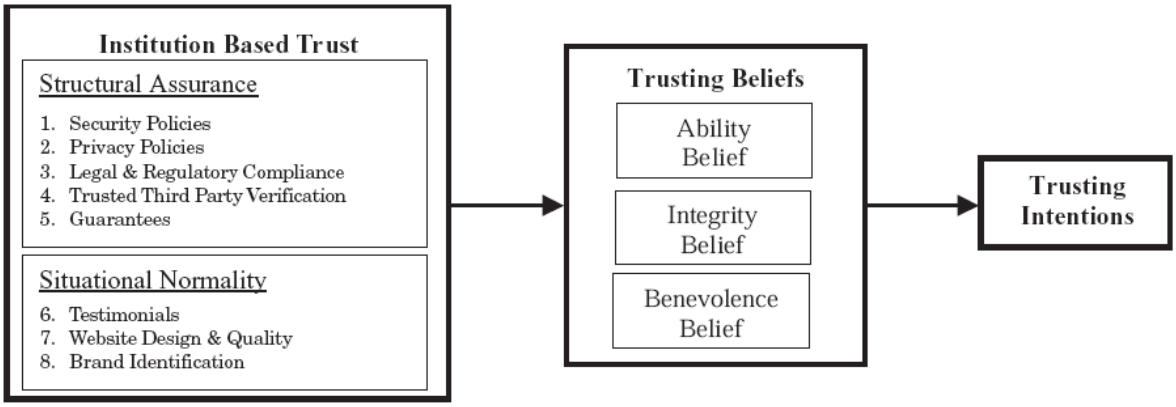
Under december månad 2006 lyckades en 16-årig pojke på Nya Zeeland komma åt ca 45 000 dollar genom Internetbanker. Han gjorde detta genom att sprida ett virus via forum som infekterade totalt 26 personer och han kunde därmed komma åt deras känsliga bankinloggningsinformation. Det inträffade har väckt frågan hur en 16-åring kunnat bedra Internetbankens kunder på stora summor pengar. Flera banker på Nya Zeeland använder inte en tvåfaktors-autentisering av användarna, utan oftast räcket det med ett lösenord för att få åtkomst till Internetbanken, något som tros ha varit en stor bidragande faktor till det lyckade bedrägeriet. Bankerna har dock lovat att ersätta de individer som drabbats (http://www.idg.se/2.1085/1.74862).

3.3 Förtroende

Förtroende skapas på flera dimensioner, där olika faktorer styr användarens benägenhet till att få förtroende för en specifik bank. Användarnas förtroende till e-banking kännetecknas av en distant och opersonlig omgivning eftersom den personliga kontakten med banktjänstemannen saknas (Foxall et. al. 2005). Banker har länge associerats med synonymer till säkerhet och tillit inom den fysiska världen. Dock visar en del forskningsrön att den förknippade associationen inte följt med i utvecklingen av den tekniska plattformen på Internet d.v.s. Internetbanken. I samband med avsaknaden av den personliga kontakten på Internetbanker,

måste nya metoder för att frambringa förtroende hos kunden skapas. Detta eftersom det är den personliga kontakten som varit den förtroendeskapande åtgärden i traditionella bankväsendet (Foxall et. al. 2005).

Enligt (Foxall et. al 2005; Mayer et. al 1995; Rousseau, Sitkin, Burt, Camerer, 1998) definerar förtroende som följande: *”Kundens vilja till att utföra online transaktioner, medan man förväntar sig att banken kommer att uppfylla sin del av avtalet, utan att man har insyn eller kontroll över bankens handlande”* (Författarnas egna översättning s. 183). Denna definition inbegriper två nivåer: första nivån är det traditionella förtroendet gentemot banken som tillhandahåller Internettjänster. Den andra nivån är transaktionens medium dvs. Internet, där transaktionen sker. Den andra nivån inbegriper kundens övertygelse till det förtroende som denne har gentemot Internetbanken. Förtroendet definieras som kundens uppfattningsförmåga, välvilja och integritet gentemot tillhandahållaren av Internettjänsten Foxall et al. (2005) d.v.s. banken.



Figur 6 Schema för förtroende mekanism (Foxall et. al, 2005, p.184)

Att skapa förtroende till transaktionernas medium har försvårats av den omfattade mediebevakning av olika Internetbrott och attacker som bankerna utsatts för. Förtroende är viktig inom globala ekonomiska transaktioner eftersom svårigheterna med att ta lagliga åtgärder vid olika typer av dispyter eller bedrägerier mot bedragarna är komplicerade (Turban et. al 2004). De lagliga åtgärderna försvåras ofta av att bedragarna gör attackerna från utlandet (Berghel 2006) vilket därmed försvårar utredningen. Detta kunde även bekräftas av SITIC vid eMail-korrespondensen.

Johnson & Grayson (2003) delar upp förtroende i två delar, kognitivt förtroende och affektivt förtroende. Kognitivt förtroende är användarens vilja att tro på tjänstens tillhandahållare och dess kompetens och reliabilitet. Det kognitiva förtroendet skapas vid flera lyckade interaktioner med tjänsten tillhandahållare d.v.s. Internetbanken. Affektivt förtroende är mera känslobaserat förtroende. Detta känslobaserade förtroende är beroende av hur mycket tillhandahållaren av tjänsten tar hand om sina kunder d.v.s. att kunden känner att Internetbanken bryr sig om deras problem (Trusting Beliefs i Figur 6).

3.3.1 Vad skapar förtroende?

Institutionellt baserat förtroende är beroende av flera faktorer som påverkas av banken, vilka presenteras i Figur 6. Figuren representerar kundens antaganden angående opersonliga

strukturer och bidragande tillstånd i vilka de känner sig säkra och komfortabla. De flesta kunder tror att Internetbanken är säker eftersom deras bank har sagt det. I realiteten kan deras känsla av trygghet vara falsk (Hølle, et al. 2006).

Institutionellt förtroende kan även ses som förtroende gentemot ett system och dess omgivning (Turban et. al 2004). Inom den strukturella försäkran är det de sociologiska traditioner som styr. Med sociologiska traditioner menas när kunden uppfattar att det är i bankens intresse att allt fungerar. D.v.s. Om Internetbanken inte håller det dem lovat har detta en negativ effekt på bankens förtroende och goda namn. Säkerhetsaspekten har visat sig vara en av de svåraste hindren att överkomma inom användandet av Internetbanker. Bankerna har lagt ut deras säkerhetsföreskrifter på Internet så att kunden kan känna sig säker och för att kunna ta del av information. Privata säkerhetsföreskrifter ger information till kunden vilket ansvar denna har i användandet av Internetbanken. Säkerhetsföreskrifterna informerar även vilka garantier kunden har utifall något skulle gå fel. Något som bidrar till förtroendeskapandet är bland annat hur kunden identifierar varumärket. Associerar kunden varumärket till något positivt bidrar detta till ett ökat förtroende från kunden. Designen och den upplevda kvalitén av Internetbankens hemsida spelar en avgörande roll för kundens upplevelse av banken.

Med institutionellt baserat förtroende skapas övertygelse hos kunden att banken kan uppträda korrekt i en specifik situation. D.v.s. kunden känner att hans/hennes behov möts med god service. Institutionellt baserat förtroende är det som banken skapar genom sitt uppträdande gentemot kunden. Kunden är ingen passiv mottagare av bankens service utan samverkar med den sociala omgivningen, det institutionellt baserade förtroendet skapas genom denna samverkan (Johnson & Grayson, 2003). Denna samverkan bidrar till att aktivt bygga upp en känsla av säkerhet och förtroende hos kunden. Uppbyggnaden av förtroendet är en bilateral relation där både kund och bank påverkar varandra.

När banken har lyckats att skapa ett förtroende hos kunden, kvarstår att kunden ska behålla sin lojalitet gentemot banken. Efraim Turban beskriver i boken *Electronical commerce* att kundlojalitet är, hur villig en kund är att stanna hos ett specifikt företag eller varumärke. Lojala kunder är viktiga för affärsverksamhetens överlevnad, speciellt inom den elektroniska världen. p.g.a. dess positiva effekt på långsiktig vinst (Reichheld & Schefter, 2000). Det kostar företaget fem till åtta gånger mer att värva en ny kund än att behålla en befintlig kund (Turban et. al 2004).

4. Bankens praxis

I detta kapitel presenteras bankernas förtroendeskapande tillvägagångssätt. Bankernas säkerhetsinformation presenteras kort och granskas utifrån en användares perspektiv. All information till detta kapitel är hämtat från respektive banks hemsida, bilderna på inloggningssidorna presenteras för att förtydliga och illustrera för läsaren.

När ett bankkonto öppnas hos Nordea eller Swedbank får kunden i samband med detta tillgång till kontot även via Internet. Hos Nordea erhålls ett skrapkort med engångskoder samt en personlig kod som används i samband med bankens Internetlogin. Medan hos Swedbank erhålls en liten elektronisk dosa som genererar engångskoder samt en personlig kod som används i samband med bankens Internetlogin.

4.1 Nordea

I samband med öppnandet av ett bankkonto erhåller kunden en säkerhetsbroschyr där banken har skrivit ner sina villkor för Internetanvändandet som varje kund ska efterfölja. I dessa villkor finns säkerhetsföreskrifter vilka kunden ombedes att följa. När en inloggning genomförs på Nordeas hemsida (http://app.nordea.se/login/index.html), finns klar och tydlig information om aktuella risker. Information om de aktuella riskerna presenteras som ett viktigt meddelande för bankens kunder på ett iögonfallande sätt, där meddelandets text är skriven med röd text till höger om inloggningsrutan (Se Figur 7). Till vänster om inloggningsrutan finns en lista med länkar där bland annat en länk är säkerhet. Under punkten säkerhet beskrivs de olika säkerhetsaspekterna gällande inloggningen och användandet av Internetbanken. Dessa säkerhetsaspekter är beskrivna på ett lätt och begripligt sätt så att en lekman kan förstå. Foxall et. al (2005) säger att bankens hemsida är en mötesplats mellan kund och bank, där designen och layouten spelar en avgörande roll vid interaktionen, vilket överrensstämmer med punkten Webdeisgn & Quality i Figur 6.

Figur 7 Nordeas inloggnings sida (http://app.nordea.se/login/index.html)

4.2 Swedbank

Inloggningen på Swedbanks hemsida presenteras i Figur 8 (https://internetbank.fsb.se/) resten av Internetadressen återfinns i referenser. Swedbanks hemsida är utformad på ett spartanskt sätt. Säkerhetsinformationen presenteras inte på ett lättillgängligt sätt för kunden. Under bilden finns länken ”Villkor vid användning av våra Internettjänster” denna länk tar kunden till en hemsida där allmänna villkor för Internettjänsten presenteras. Dessa villkor är inte några handfasta tips utan juridiska bestämmelser vid användandet av Internetbanken och dess tjänster. Genom att navigera sig fram följande steg på Swedbanks hemsida kan man komma fram till tips och råd. Startsidan > Våra Internettjänster > Kundtjänst > Information om säkerhet > Säkerhet – Internettjänster > Tips och Råd. Där får kunden tips och råd om vad denne ska tänka på vid användningen av Internetbanken. Ifall inloggningstjänsten inte är tillgängligt mellan vissa tidpunkter, vissas information om avbrottet ovanför inloggningsrutan på hemsidan.

Figur 8 Swedbanks inloggnings sida (https://internetbank.fsb.se/)

Då phishing är ett växande problem och förövarna ständigt utvecklar sina attackmetoder är det svårt för bankerna att hundraprocentigt kunna skydda sig och sina kunder mot dessa attacker. Det finns många olika metoder när det gäller förebyggande åtgärder mot phishing. Det nämns ett antal metoder i teorin där bland annat en metod är upplysa kunderna om de befintliga riskerna. Både Swedbank och Nordea uppfyller villkoret för förebyggande information till kunderna. Tillsammans med bankernas egna säkerhetsinformation uppmanas kunden att ständigt hålla sig uppdaterade. Med detta menas att kunden ska ha ett fungerande antivirusskydd, brandvägg samt att deras dator ska ha de senaste uppdateringar för operativsystemet. Kunderna ska inte heller logga in eller skicka känslig information från några datorer som anses vara mindre säkra. D.v.s. datorer på offentliga platser och datorer som inte har något fullgott virusskydd. I de bägge bankernas säkerhetsinformation framhävas det starkt att banken aldrig skickar ut något e-postmeddelande till sina kunder. Båda bankerna uppmanar sina kunder till ett säkerhetstänkande vid användningen av sin Internetbank vilket överrensstämmer med det metoder som nämnts i teoridelen för förebyggande åtgärder mot phishing. Swedbank nämner bland annat på sin hemsida att ”*Det är banken tillsammans med dig som kund som kan förhindra bedrägerierna. Det spelar därför ingen roll hur bra bankens säkerhetslösning är, om du som kund inte skyddar dina uppgifter*.”

5. Empiri

I detta kapitel presenteras resultaten av enkäten samt eMail-korrespondens med SITIC. Enkäten presenteras fråga för fråga med svarsfrekvensen och en kort kommentar. EMail-korrespondensen med SITIC återges i fullständig form med frågor och svar.

5.1 Enkät

Totalt utdelades 91 enkäter varav 60 utgjorde svar till de två banker till vilka uppsatsen avgränsar sig. En jämn fördelning eftersträvades för att kunna jämföra dessa två bankerna. 30 st enkäter för Swedbank och 30 st för Nordea erhölls. 30 st enkäter för vardera bank erhölls genom att dela ut enkäter tills antalet var uppnått. Bortfallet blev 31 st enkäter vilka utgjordes av andra banker i vilken den största gruppen var SEB. Andra bankerna var även Handelsbanken, Skandiabanken, Sparbanken Finn samt ICA Banken. Uppsatsen avgränsar sig till Nordea och Swedbank eftersom de tillämpar olika säkerhetssystem. Dessutom har Nordea blivit utsatt för phishingattacker. Nordea tillsammans med Swedbank representerar olika inloggningssystem och har tillsammans största antal Internetanvändare i Sverige.

Resultaten presenteras i tabeller med totalt antal svarande respondenter per fråga samt en fördelning mellan respektive bank. Resultatet presenteras som antal svarande personer och inte i procentsats, eftersom intresset av den enskilda individens uppfattning är av vikt. Procentsats kan ge en missvisande bild då enkätundersökningen utgörs av endast 60 respondenter.

Först presenteras undersökningens demografiska data, könsfördelning, ålder, och utbildning. Tanken med de demografiska frågorna var att fånga sambandet mellan ålder, kön och utbildning samt om kombinationen av dessa påverkade riskmedvetenheten. Dessa presenteras som en gemensam grupp bestående av Swedbank och Nordeas kunder. Sedan presenteras resultat fråga för fråga med tillhörande kommentarer.

Demografisk Data					
Kön		**Ålder**		**Utbildning**	
	Antal	Åldersgrupp	Antal		Antal
Man	25	18-25	30	Grundskola	2
Kvinna	35	26-35	14	Gymnasium	9
		36-49	6	Universitet	49
		50-59	10		
		60+	0		
Totalt:	60	**Totalt:**	60	**Totalt:**	60

Figur 9 Uppsatsens Demografisk Data (Enkät)

1. Du är kund hos?
Antal svarande 60

Det totala antalet kunder som svarade på enkäten och som tillhörde vår population var 60 st sammanlagt varav 30 st från Nordea respektive 30 st från Swedbank.

2. Hur länge har du använt dig av Internetbanken?
Antal svarande 60

Totalt medelvärde	Nordea	Swedbank
3.7 år	3.6 år	3.8 år

Figur 10 Genomsnittlig Internetbank användningslängd (Enkät)

Längden av användningen antas påverka medvetenheten och uppskattningsförmågan om riskerna. Det antogs att desto längre man använder Internetbanken desto mer medveten blir man om aktuella risker.

3. Hur medveten anser du dig själv vara om riskerna gällande inloggningen på din Internetbank?
Antal svarande 60

	Totalt	Nordea	Swedbank
Det finns inga risker	0	0	0
Jag litar på banken	33	14	19
Jag håller mig uppdaterad om eventuella risker	27	16	11

Figur 11 Svarsfördelning fråga 3 (Enkät)

För att ta reda på respondenternas riskmedvetenhet om Internetbanken, ställdes denna fråga i början av enkäten för att vid ett senare skede i enkäten kunna jämföra denna med kontrollfrågan. Alternativ ett med ”Det finns inga risker”, tyder på en kund som är helt omedveten om riskerna. Alternativ två tyder på att kunden är delvis medveten om riskerna med litar på banken och dess säkerhetssystem. Sista svarsalternativet tyder på en hög riskmedvetenhet hos kunden.

4. Vilken datorvana har du?
Antal svarande 60

	Totalt	Nordea	Swedbank
Använder dator så lite som möjligt	1	0	1
Använder dator ett par ggr/vecka	4	3	1
Använder dator dagligen på jobbet	25	12	13
Använder dator så mycket som möjligt	30	15	15

Figur 12 Svarsfördelning fråga 4 (Enkät)

Användningsfrekvensen antogs påverka riskmedvetenheten bland kunderna. Eftersom användning i större utsträckning skapar skicklighet hos användaren, antas det att en högre användningsfrekvens leder till en större riskmedvetenhet.

5. Har du läst säkerhetsinformationen på bankens hemsida?
Antal svarande 60

	Totalt	Nordea	Swedbank
Ja, men bara helt kort	22	11	11
Ja, jag tror jag vet vad som gäller	8	5	3
Ja, noga. Jag vet precis vad som gäller.	3	1	2
Ja, jag kollar efter sådant varje gång jag loggar in	5	4	1
Nej *Om Nej, hoppa över nästa fråga*	22	9	13

Figur 13 Svarsfördelning fråga 5 (Enkät)

Frågan ställs för att ta reda på ifall kunden läser säkerhetsinformationen som banken givit ut. Om kunden har läst säkerhetsinformationen anses denne vara medveten om de risker som kan inträffa. Första svarsalternativet tyder på att kunden snabbt har läst igenom information. Andra svarsalternativet tyder på att kunden har läst information och tagit ut de viktigaste punkterna. Tredje svarsalternativ tyder på att kunden är väl medveten om riskerna. Fjärde svarsalternativet tyder på att kunden har ett personligt intresse och har en hög nivå på riskmedvetenheten. Femte och sista svarsalternativet visar att kunden inte har läst säkerhetsinformationen och därmed är omedveten om riskerna.

6. Hur anser du att bankens säkerhetsinformation är utformad?
Antal svarande 38 ,respondenter som hade läst säkerhetsinformationen (se föregående fråga)

	Totalt	Nordea	Swedbank
Dåligt	**1**	**0**	**1**
Tillfredställande	**16**	**9**	**7**
Bra	**18**	**11**	**7**
Utmärkt	**3**	**1**	**2**

Figur 14 Svarsfördelning fråga 6 (Enkät)

Frågan tar upp hur kunden upplever bankens säkerhetsinformation samt om banken har lyckats förmedla säkerhetsinformationen på ett tydligt sätt. En fyrgradig skala används för att ange kundens tillfredsställelse.

7. Har du fått e-post meddelande från din bank?
Antal svarande 60

		Totalt	Nordea	Swedbank
Ja		**13**	**8**	**5**
Nej	*Om Nej Hoppa över nästa fråga*	**47**	**22**	**25**

Figur 15 Svarsfördelning fråga 7 (Enkät)

Genom denna fråga kunde en antydan på en phishingattack plockas fram. En annan anledning till att ställa denna fråga var att respektive bank klargör enkelt och tydligt att inga e-postmeddelanden skickas ut till kunder.

8. Följde du anvisningar i e-post meddelandet?
Antal svarande 13st, respondenter som hade mottagit e-post meddelande från sin bank. (se föregående fråga)

	Totalt	Nordea	Swedbank
Ja	**7**	**3**	**4**
Nej	**6**	**5**	**1**

Figur 16 Svarsfördelning fråga 8 (Enkät)

I kombination med föregående fråga kan en analys göras om phishingattackens utsträckning. Genom att se vilka som inte följde anvisningarna på e-postmeddelandet kan ett statistiskt antagande göras vilket tyder på att respondenten har blivit utsatt för en phishingattack, men lät sig inte luras.

9. Känner du till någon annan som har fått ett liknande e-post meddelande?
Antal svarande 42, antalet respondenter som svarade att de kände någon som hade mottagit..

	Totalt	Nordea	Swedbank
Ja	**7**	**7**	**0**
Nej	**35**	**20**	**15**

Figur 17 Svarsfördelning fråga 9 (Enkät)

Eftersom föregående fråga kan upplevas mycket personlig, ställdes fråga 9 i följd för att belysa att problemet kan vara omfattande. Denna fråga kunde även ge en antydan till oss om problemets utsträckning.

10. Jag känner mig säker när jag loggar in på min Internetbank
Antal svarande 60

	Totalt	Nordea	Swedbank
Instämmer helt	**36**	**14**	**22**
Instämmer delvis	**21**	**14**	**7**
Tar delvis avstånd	**2**	**1**	**1**
Tar helt avstånd	**1**	**1**	**0**

Figur 18 Svarsfördelning fråga 10 (Enkät)

Denna fråga användes som en kontrollfråga till fråga 3. Genom denna fråga kan enkätens eventuella påverkan på respondenten fångas in samt en kombination av dessa två frågor kan ge en säkrare bild av respondentens medvetenhet.

11. En typ av Internetbedrägerier kallas ibland för "Phishing" och innebär att man luras med hjälp av falska Internetsidor. Hur medveten är du om detta tillvägagångssätt?
Antal svarande 60

	Totalt	Nordea	Swedbank
Jag känner inte till det alls	**10**	**4**	**6**
Jag har hört talas om det	**19**	**9**	**10**
Jag vet vad det är, men inte i detalj	**18**	**11**	**7**
Jag är väl informerad och vet precis!	**13**	**6**	**7**

Figur 19 Svarsfördelning fråga 11 (Enkät)

Uppbygganden av denna fråga syftar till att få fram kännedomen om phishing som företeelse och inte som en pop term. Först ges en kort beskrivning som ska få respondenterna att förknippa bedrägerifenomenet med termen phishing. Även om denna beskrivning ges, betyder det inte att kunden känner till termen.

12. Har du vid något tillfälle avstått från att använda din Internetbank?
Antal svarande 60

	Totalt	Nordea	Swedbank
Ja Om *Ja varför, markera ett alternativ nedan*	**13**	**6**	**7**
Nej	**47**	**24**	**23**

Figur 20 Svarsfördelning fråga 12 vilka avstod från att använda Internetbank (Enkät)

Eftersom phishingattacker kunde ha påverkat användarens benägenhet att avstå från att använda sin Internetbank, undersöktes detta påstående med följande fråga. Vid ett jakande svar ombads respondenten att specificera skälet till varför respondenten avstått att använda sin Internetbank.

Antal svarande 13, respondenter som hade vid något tillfälle avstått från att använda sin Internetbank. (Se föregående fråga)

	Totalt	Nordea	Swedbank
Bankens Internetsida fungerade inte vid upprepade gånger	**6**	**3**	**3**
Kände mig osäker på att logga in på Internbanken	**1**	**1**	**0**
Utförde mina ärenden direkt på banken	**2**	**0**	**2**
Annat	**4**	**2**	**2**

Figur 21Skälet till avstående (Enkät)

Anledningen till denna fråga var att få fram om respondenten påverkades av säkerhetsinformationen i den mån att denne har avstått ifrån att använda sin Internetbank. Detta kan även innefatta mediebevakning av bedrägeri försök.

5.2 EMail-korrespondens

Ett e-postmeddelande sändes med frågor efter att ha varit i telefonkontakt med SITIC, där en överenskommelse gjordes att frågorna skulle tas via e-post. Nedan presenteras de frågor som ställdes till SITIC med tillhörande svar med tillhörande kommentar.

Vilka åtgärder görs vid en incidentrapportering av typen phishing?

SITIC: När vi blir varse om ett phishing-försök kan de efterföljande åtgärderna grovt delas in i två kategorier. En del informerande och en del avhjälpande.
Informerande åtgärder innebär exempelvis att vi i tillämpliga fall just informerar om den aktuella händelsen bl.a. via vår webbplats (www.sitic.se och www.pts.se/internetsakerhet) till allmänheten. Den avhjälpande delen kan innebära allt från att vi själva initierar en nedsläckning till att vi förmedlar informationen.

Frågan ställdes för att ta reda vilka konkreta åtgärder SITIC gör vid en phishing incidentrapportering.

På senare tid har det varit mycket tal om phishingattacker i media som har varit riktade mot banker, har någon svensk bank kontaktat er och gjort en incidentrapportering av phishing?

SITIC: Vid phishingattacker har vi kontakt med den berörda banken.

Med hjälp av denna fråga skulle de framgå om svenska banker använder SITIC vid incidentrapportering.

Om t.ex. en bank gör en förfrågan, kan ni utföra analys av deras säkerhetssystem? Om ja, hur utförs denna analys?

SITIC: Nej. Aktiv kontroll av säkerhetssystem är inte del av vårt arbete. Dock hindrar inte det oss från att ge rådgivning på begäran.

Frågan ställdes för att se om SITIC utför några analyser av säkerhetssystem.

Sker de flesta phishingattacker från utlandet?
Finns det någon statistik på detta?

SITIC: Empirisk data tyder på att de flesta attacker har sitt ursprung i utlandet. Någon mer utförlig analys har vi inte genomfört.

Mycket av den litteratur som beskriver phishing nämner att attackerna sker från utlandet, genom denna fråga kunde påståendet bekräftas ifall detta stämde på de phishingattentat som skett i Sverige.

Vilka råd ger ni för att förebygga en phishingattack?
Vad består den data av som ni grundar era förebyggande råd på?

SITIC: Läs mer på:
http://www.pts.se/internetsakerhet/Sidor/sida.asp?Sectionid=1796

Frågan ställdes för att se vilka förebyggande råd SITIC gav för att förhindra phishing. Samt vad SITIC grundade sina förebyggande råd på.

Enligt er, varför har Nordeas kunder blivit utsatta för phishing attacker i större utsträckning än kunder för andra banker?

SITIC: Vi lämnar den analysen åt andra

Nordea har blivit uppmärksammat i media för att ha varit utsatta för phishingattacker. Därför ställdes denna fråga för att kunna verifiera varför Nordea i större utsträckning hade blivit utsatta.

Har ni samarbete med organisationer från utlandet för att bekämpa phishing?
Kan ni kort beskriva hur samarbetet ser ut, samt vilka organisationer ni samarbetar med?

SITIC: Nyckeln till att avstyra phishing-försök är internationella kontakter. Hittills har lejonparten huserande servrar funnit utanför Sverige, så utländsk assistans är nödvändig för en nedsläckning. Ibland kan det handla om direkt kontakt med ISP:er. I andra fall sker kontakten genom respektive lands stats-CERT (Computer Emergency Response Center).

Litteraturen nämner att ett samarbete mellan olika länders organisation kan i bättre mån bekämpa phishing. Därför ställdes frågan för att se om SITIC bedrev ett samarbete organisationer från andra länder.

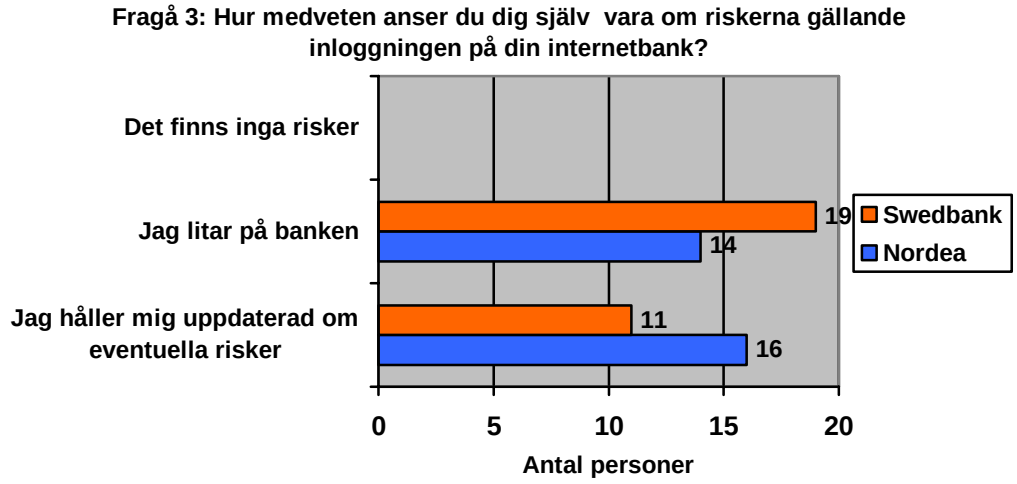
6. Analys och Diskussion

I detta kapitel kommer resultatet från enkätundersökningen att behandlas. En analys och en diskussion kommer att föras kring resultatet, samtidigt som en återkoppling görs till teorin och bankernas praxis. Frågorna kommer att presenteras i den ordning som de är ställda i enkäten. Dock kommer inte alla frågor i enkäten att presenteras som ett enskilt diagram fördelat på vardera bank, då vissa av frågorna knyts samman för att bättre förklara och diskutera resultatet.

Utbildning, kön och ålder antogs från början ha en påverkan på riskmedvetenhen hos användarna, men detta kunde inte bekräftas med resultaten från enkäterna. En bidragande faktor till detta antogs vara att för få enkäter delades ut för att med säkerhet kunna avgöra de demografiska datas påverkan. En stor del av respondenterna har kryssat i att de har någon form av universitetsstudier bakom sig, detta tros bero på att Lund är en universitetsstad. Av de tillfrågade respondenterna hade 49 st kryssat i alternativet med universitet på sin utbildningsnivå. Universitetsutbildningsnivån kunde tolkas på två sätt, antingen helt avklarade studier med en examen eller pågående studier på ett universitet. Hälften av respondenterna var mellan 18 och 25 vilket utgjorde den största åldersgruppen bland respondenterna i enkätundersökningen. Åldersfördelningen hos respondenterna blev mellan 18 och 59 eftersom inga personer över 60 fångades in i enkätundersökningen och därmed täcktes inte hela den tänkta ålderspannen.

En fråga som hos en del respondenter tog lång tid att svara var fråga två som behandlade längden av Internetbanksanvändandet. De respondenter som hade använt sin Internetbank under en längre tid, tyckte att det var svårt att komma ihåg och specificera exakt antal år som de hade använt sig av sin Internetbank.

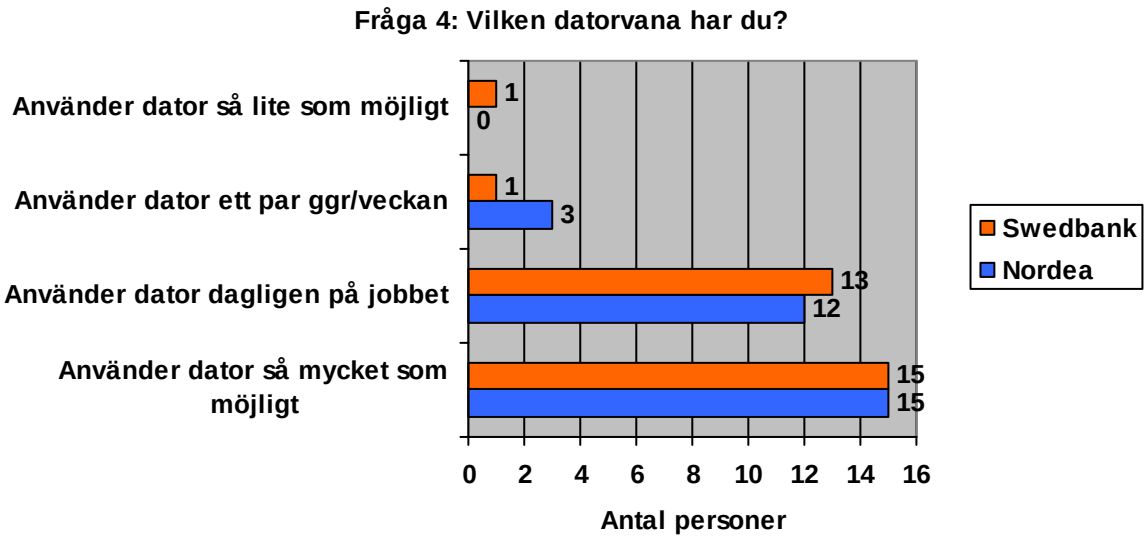
Längden av Internetbanksanvändandet i fråga två i kombination med riskmedvetenhen i fråga tre belyser kundernas tillit till banken. Resultatet från enkäten kunde påvisa att respondenterna inte var helt omedvetna om riskerna eftersom ingen hade kryssat i första svarsalternativet d.v.s. det finns inga risker. Desto längre tid en kund använder en specifik tjänst desto högre blir dennes förtroende till denna tjänst (Johnson & Grayson, 2003). Det förhöjda förtroendet uppstår genom flera lyckade interaktioner sker med tjänstens tillhandahållare d.v.s. Internetbanken (Se Brand Identification i Figur 6).



Figur 22 Medvetenheten hos respondenterna med fördelningen på respektive Internetbank (Enkät)

När resultatet från respektive bank jämfördes framkom det att Swedbanks kunder hade större tilltro till sin Internetbank än Nordeas kunder. Detta skulle kunna bero på att Swedbanks kunder inte blivit utsatta för phishingattacker, vilket lett till att Swedbanks kunder inte har haft någon anledning att misstro sin Internetbank. En stark negativ mediebevakning är en bidragande faktor till ett förminskat förtroende mot Internetbanken (Foxall et al. 2005). Eftersom Nordea har fått en negativ mediebevakning i samband med phishingattackerna, har detta lett till att kunderna blivit mer uppmärksamma på problemet och själva tagit mer ansvar för sin säkerhet. Att själv ta ansvar för sin säkerhet tyder på en större riskmedvetenhet.

När datorvanan förfrågades av respondenterna kunde ingen skillnad påvisas mellan kunderna på vardera bank (Se Fråga 4). Det var nästintill en jämn fördelning mellan bankerna på de två sista svarsalternativen på fråga fyra. Enligt enkätresultatet kan det sägas att Nordeas och Swedbanks kunder hade en likvärdig datorvana. Inget samband kunde påvisas gällande datorvana i kombination med längden av Internetbanksanvändandet i förhållande till riskmedvetenhet. I motsats kunde dock ett mönster påvisas som antydde att riskuppfattningen inte påverkades av datorvanan. Eftersom datorvanan hos bankkunderna var näst intill lika, kan ett påstående göras att kunderna på respektive bank, har samma förutsättningar att ta del av säkerhetsinformationen samt bli medvetna om riskerna. Bankerna förmedlar sin säkerhetsinformation via deras respektive hemsida (Se figur 3 & 4). På bankernas hemsidor finns information om bland annat phishing samt riktlinjer för att upprätthålla en god säkerhetsnivå. I teoridelen beskrivs phishing och där nämns det olika metoder för att i bästa mån motverka ett phishingangrepp, där bland annat en metod är att hålla användarna informerade (Levine 2006). Eftersom datorvanan var näst intill lika bland respondenterna från de båda bankerna kan det antas att de kan bli varse om informationen på ett likartat sätt. En hög grad av datorvana innebär att de kan blir varse om riskerna med phishing från flera olika källor så som ta åt sig information om phishing från andra hemsidor än enbart från bankernas egna hemsidor.

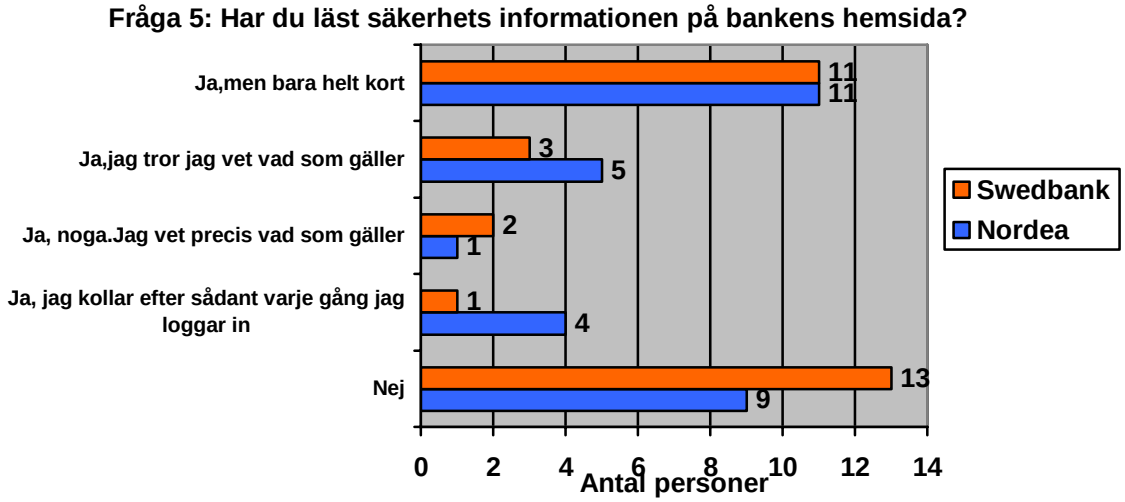


Figur 23 Respondenternas datorvana med fördelning på respektive Internetbank (Enkät)

Fråga fyra tolkades på så vis att de personer som använde datorn så mycket som möjligt hade en hög datorvana, medan de personer som använde datorn så lite som möjligt hade en låg datorvana. Fråga fyra i kombination med fråga tre kunde ge en antydan på respondentens

riskmedvetenhet. De respondenter som använde datorn dagligen på jobbet och angav att denne håller sig uppdaterad om riskerna på fråga tre ansågs vara riskmedvetna. Respondenterna som kryssade i svarsalternativet att de använder datorn så mycket som möjligt på fråga fyra och höll sig uppdaterade om eventuella risker på fråga tre ansågs vara mycket väl insatta och riskmedvetna. Resultatet antydde dock att datorvanan inte påverkade riskmedvetenheten, utan att det är mera egna personliga värderingar som påverkar uppfattningen om riskerna.

En av de viktiga metoderna för att motverka phishingattack är enligt Levine 2006 är att hålla användare informerade. Genom att fråga utifall respondenterna hade läst säkerhetsinformation på bankens hemsida samt hur dem värderade denna säkerhetsinformation fråga sex, kunde en analys göras om bankens förtroendeskapande åtgärder lyckats. Denna förtroendeskapade åtgärd är att hålla användarna informerade d.v.s. har respondenterna läst den säkerhetsinformation som bankerna givit ut, samt hur har respondenterna tagit emot den.



Figur 24 Hur väl respondenterna läst den säkerhetsinformation som bankerna givit ut med fördelning på respektive Internetbank (Enkät)

När en granskning görs på bankernas praxis i hur bankerna lyckats att tillhandahålla säkerhetsinformationen kan tydliga skillnader utläsas. Hos Nordea är säkerhetsinformationen lättillgänglig medan hos Swedbank krävs ett antal steg innan man kommer fram till säkerhetsinformation. Skillnaden på tillhandahållandet av säkerhetsinformation mellan bankerna, tyder på att phishing blivit mer uppmärksammat hos Nordea än hos Swedbank. Resultatet från enkäten kunde påvisa att Nordea lyckats att förmedla sin säkerhetsinformation i större utsträckning till sina kunder än Swedbank. Det var enbart nio personer som inte hade läst säkerhetsinformationen på Nordeas hemsida medan hos Swedbank var motsvarande siffra 13. Här kan även en koppling göras till hemsidans design och utformning. (Instituatinal base trust, webdesign & Quality Se Figur 6). Om informationen på hemsidan lättillägnligt och välutformad når den ut lättare till kunden. På Nordeas hemsida är det svårt att undgå säkerhetsinformationen (Se Figur 7), medan hos Swedbank måste en medveten sökning göras för att nå fram till säkerhetsinformationen. För att ta reda på hur väl säkerhetsinformationen mottogs, tillfrågades de respondenter som hade läst säkerhetsinformationen hur de ansåg att säkerhetsinformationen var utformad. Majoriteten av respondenterna ansåg att utformningen av säkerhetsinformationen var antingen tillfredställande eller bra. Endast en av de 60 respondenter ansåg säkerhetsinformationen vara dåligt utformad, och tre ansåg att den var utmärkt. Generellt sätt tyder resultatet på att de respondenter som hade läst säkerhetsinformation ansåg att den var tillfredställande eller bra.

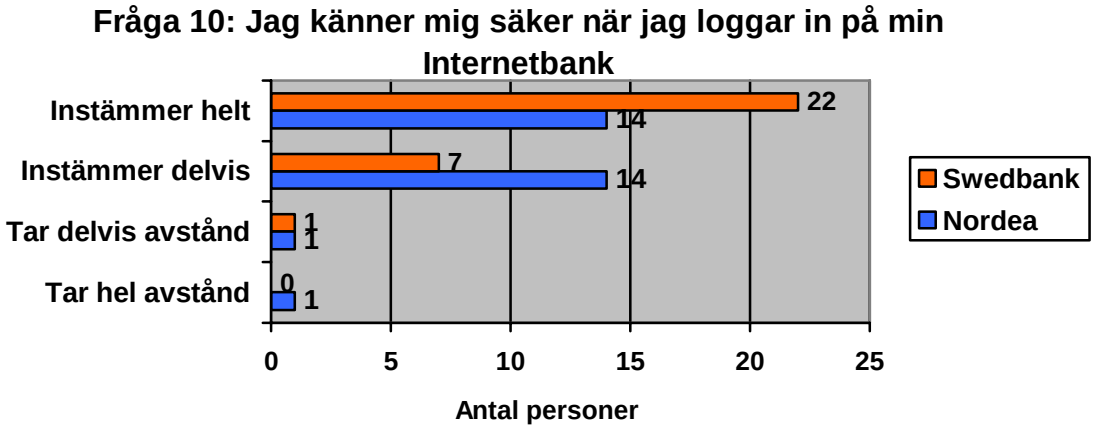
För att ta reda på ifall någon av respondenterna hade blivit utsatta för en phishingattack ställdes frågan utifall respondenterna hade fått något e-postmeddelande från sin bank. Denna fråga hänger samman med följdfrågan ifall de respondenter som hade mottagit ett e-postmeddelande från sin bank hade följt anvisningarna i detta e-postmeddelande. Berghel (2006) ger riktlinjer hur ett phishing e-postmeddelande kan vara utformad för att på bästa sätt öka chanserna att lura mottagaren. Phishing e-postmeddelandet som skickades till en del av Nordeas kunder påvisade stora språkliga brister (se Figur 2). Av den anledning skulle troligen phishing e-postmeddelandet till Nordeas kunder poängsättas med 0.5 eller 1 poäng enligt den skala som Berghel (2006) presenterar sin artikel. Resultatet från följdfrågan tyder på att förövarna hade misslyckats med sitt phishing försök bland de respondenter som deltog i enkätundersökningen. Åtta personer på Nordea och fem personer på Swedbank hade mottagit e-post meddelanden. Av Nordeas åtta kunder som hade mottagit ett e-postmeddelande från sin bank följde endast tre anvisningarna i e-postmeddelandet. Enligt dessa respondenter var detta en följd av en ömsesidig korrespondens med en banktjänsteman från banken. Korrespondens med banktjänsteman via e-post strider emot bankernas egna säkerhetsinformation, då denna säger att banken aldrig skickar ut någon e-postmeddelande till sina kunder. Sex personer följde inte anvisningarna i e-postmeddelandet vilket tyder att det var en phishingattack via e-post, detta kunde även bekräftas av respondenterna.

Resultatet från enkäten bekräftar att kunder hade blivit drabbade av phishing, men även det att de inte lät sig luras. E-föreläsningen på (http://www.esecurelive.com) presenterade ett exempel på en phishingattack. Av två miljoner phishing e-postmeddelanden som skickades ut öppnade 5 % (100 000 st) detta e-postmeddelandet, av dessa 100 000 följde ytterligare 5 % (5 000 st) anvisningarna i e-postmeddelande genom att fylla i de begärda uppgifterna. Flera artiklar stödjer påståendet att upp till 5 % av phishingattentaten lyckas i den mån att användarna tar del av informationen (Dhamija et. al 2006). Kvantiteten av skickade e-postmeddelanden är en stor bidragande faktor till hur väl en attack lyckas. Dock är exemplet ovan bara en exemplifiering av hur lyckad en phishingattack kan vara. Lägger man dessutom till att Symantec rapporterade under första halvåret 2006 om 157 477 unika phishingattacker så kan detta ge en fingervisning om hur stort problemet med phishing är.

För att kunna bilda en uppfattning om phishingattackens utsträckning bland respondenterna, ställdes frågan huruvida respondenterna kände till andra som hade fått liknande e-postmeddelanden från sin bank. Sju st. hos Nordea kände till någon annan som hade mottagit ett liknande e-postmeddelande, medan hos Swedbank var det ingen som kände till någon som hade mottagit ett liknande e-postmeddelande. Resultatet är oroväckande eftersom båda bankerna tydligt klargör att de aldrig skickar ut någon e-postmeddelande till sina kunder där känslig information efterfrågas. På Nordeas inloggningssida står följande ”*Nordea skickar* ***aldrig*** *ut e-post för att fråga efter kodnummer, kreditkortsnummer eller annan känslig information*” (www.nordea.se). Endast 42 respondenter svarade på fråga nio, detta beror på att alla respondenter inte uppfattade att denna fråga skulle besvaras även om man inte personligen hade fått e-postmeddelanden.

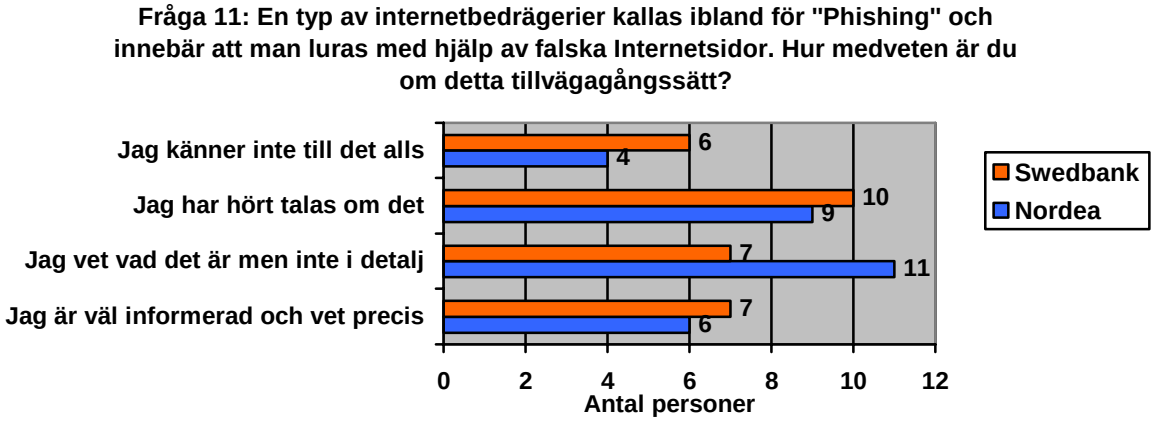
Fråga 10 behandlade respondenternas trygghetskänsla och första tanken vid utformningen av enkäten var att frågan skulle fungera som en kontrollfråga till fråga tre. Denna kontrollfråga skulle belysa enkätens påverkan på respondenternas svar. Det fanns en risk till att tidigare frågor kunde skapa misstro gentemot banken hos respondenterna, men denna koppling kunde dock inte bekräftas i enkätresultatet. Något som istället utmärkte sig var att Swedbanks kunders tycktes känna sig säkrare när de loggar in på sin Internetbank än Nordeas kunder. Detta tyder på att Nordea lyckats upplysa sina kunder bättre om riskerna vid inloggningen till

Internetbanken. Nordeas kunder är mer riskmedvetna och mer uppmärksamma angående säkerheten vid inloggningen hos sin bank. Detta visas genom fördelningen av svaren på fråga 10.



Figur 25 Respondenternas trygghetskänsla med fördelning på respektive Internetbank (Enkät)

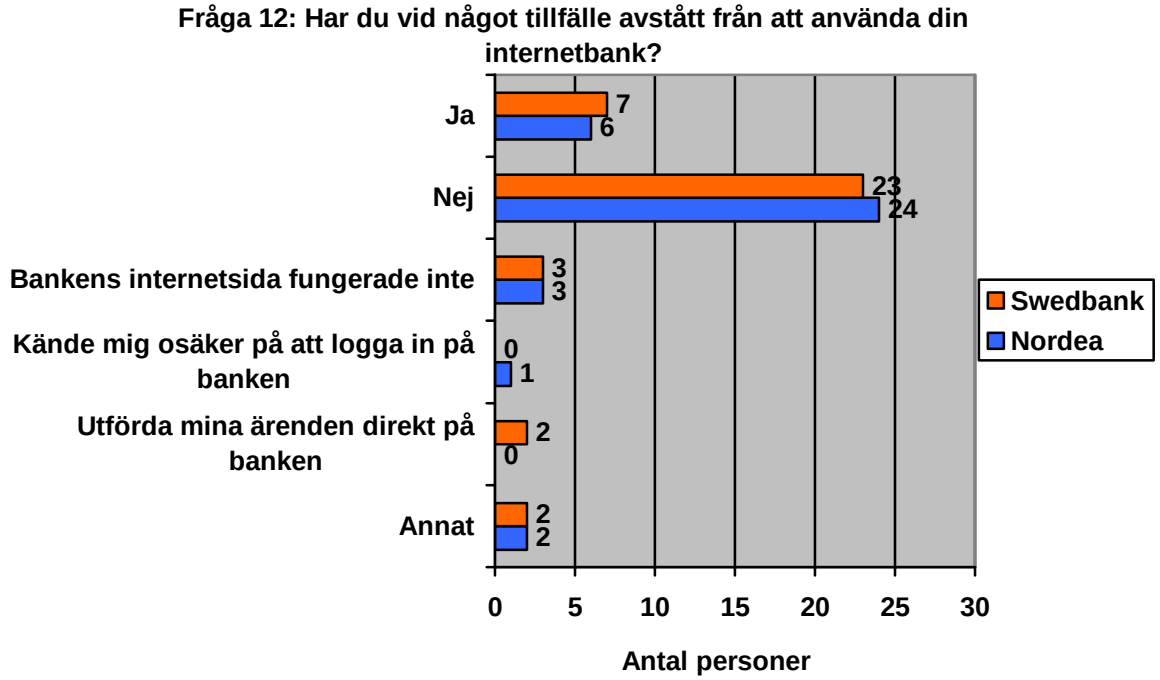
När en jämförelse gjordes mellan de två bankerna visade det sig att Nordeas kunder till större utsträckning visste vad phishing var. En svarsfördelning mellan respektive bank presenteras i Figur 26. Syftet med frågan var att ta reda på hur väl respondenterna har kännedom om termen phishing. Skillnaderna mellan bankerna skulle möjligen ha varit större utifall respondentgrupperna varit större. Enkäten visar inte varifrån respondenterna har fått sin kännedom om termen phishing, tidigare i uppsatsens teoridel nämns flera olika informationskällor där fenomenet phishing nämns. Det finns således inget som kan verifiera att kunderna endast har funnit informationen om phishing på bankernas hemsidor, utan denna kunskap kan även ha erhållits på annat vis. I teoridelen nämns ett antal olika organisationer som arbetar med förebyggandeåtgärder mot phishing. I Sverige bedrivs denna verksamhet av SITIC som är del av Post och Telestyrelsen. På PTS hemsida finns en länk där råd för förebyggande åtgärder ges, alltså hur man i bästa möjliga mån kan motverka en phishing attack. (http://www.pts.se/Nyheter/nyhet.asp?ItemID=3837; http://www.pts.se/internetsakerhet/Nyheter/nyhet.asp?ItemId=327).



Figur 26 Kännedom om begreppet phishing med fördelning på respektive Internetbank (Enkät)

Bankerna fungerar utifrån en förtroenderelation gentemot kunden (Turban, et al.2004). Om detta förtroende minskar av någon anledning, märks detta genom en försvagad trygghetskänsla hos kunderna gentemot banken. För att ta reda på om de senaste

uppmärksammade phishingattackerna hade påverkat kundernas användning av Internetbanken, tillfrågades respondenterna utifall de hade avstått från att använda sin Internetbank vid något tillfälle. Enligt Rombel (2005) hade 13 % av kunderna i Europa avstått från att använda sin Internetbank p.g.a. identitetsstölder bl.a. genom phishing. Detta överrensstämmer med Levine (2006) som säger att bankens anseende skadas om ett bedrägeri lyckas. Nordeas kunder hade blivit utsatta för ett phishingattentat, dock har inte banken lämnat ut några uppgifter om antalet kunder som har blivit drabbade (Sydsvenskan 2006-11-15). Om kunden tappar sitt förtroende gentemot banken och byter, bank kan detta kan bli mycket kostsamt för banken. Enligt Turban (2004) kostar det banken åtta gånger mer att värva en ny kund än att behålla en befintlig kund. Resultatet som erhölls från enkätundersökningens sista fråga var att endast 13 respondenter någon gång hade avstått från att använda sin Internetbank vid något tillfälle. Av dessa 13 personer hade sex personer avstått att använda sin Internetbank vid något tillfälle av den anledning att bankens Internetsida inte fungerade vid upprepade försök. Resultatet visar att endast sju personer av 60 hade avstått från att använda sin Internetbank av andra skäl än att hemsidan inte fungerade. Som andra skäl nämndes bland annat att respondenten hade fått uppmaningen att inte logga in på Internetbanken och att dennes antivirusprogram var inte uppdaterad. Med dessa resultat kan det bekräftas att bankernas säkerhetsinformation når fram till användaren. Både Nordea och Swedbank uppmanar sina kunder att ständigt kontrollera sin säkerhet. På Nordeas hemsida står det följande: *En förutsättning för att din dator ska vara säker att använda på Internet är att du har ett uppdaterat antivirusprogram.*" Och Swedbank säger följande: *För att skydda din dator från skadlig kod och intrångsförsök rekommenderar vi dig att installera både antivirusprogram och någon form av brandvägg. Håll dessa aktiva och uppdaterade.*



Figur 27 Respondenter som avstått från att använda sin Internetbank med fördelning på respektive Internetbank (Enkät)

7. Slutsats

I detta kapitel presenteras slutsatser samt idéer för framtida forskning.

7.1 Slutsatser

Efter genomförd enkätundersökning och gedigna litteraturstudier kunde en analys genomföras där slutsatser kunde bekräfta med de som sagts i teorin. Med hjälp av resultaten från enkätundersökningen kunde slutsatsen dras att kunderna till de undersökta bankerna är medvetna om risker vid använandet av Internetbanken till den grad att de inte förnekar dess existens. Detta kunde konstateras eftersom ingen hade kryssat i svarsalternativet *det finns inga risker* på fråga 3.

Det nämns ett antal metoder i teorin som är till för att förhindra en phishingattack, och en metod är att upplysa kunderna om de befintliga riskerna. Drygt tre fjärdedelar av enkätens respondenter hade läst säkerhetsinformationen på bankernas hemsidor. Några av Nordeas kunder råkade ut hösten 2006 för phishing, vilket även bekräftas av Nordeas presschef Boo Ehlin (Sydsvenskan 2006-11-15). Eftersom Nordea vill behålla sin trovärdighet hos sina kunder, vill de visa kunderna att de är medvetna om problemet med phishing och vidtar åtgärder. Nordeas metod att försöka öka medvetenheten bland sina kunder har lyckats och detta speglades i enkätens resultat.

Swedbank som inte blivit drabbade av phishing, informerar inte kunderna på samma sätt om säkerhet. Enligt enkäten instämde 95 % helt eller delvis på frågan om de kände sig säkra när de loggade in på sin Internetbank, vilket tyder på att bankernas förtroendeskapande åtgärder har lyckats (E. Turban et al 2006), trots att Nordea har fått negativ publicitet i samband med phishingattacker. Endast 10 av de 60 respondenterna var ovetande om vad phishing var för något d.v.s. majoriteten av de tillfrågade respondenterna kände till fenomenet phishing i den utsträckning att det åtminstone hade hört talas om det. Den empiriska data ger en fingervisning om phishingfenomenets stora utsträckning där fem av de 30 tillfrågade kunderna hos Nordea hade mottagit ett phising via e-postmeddelande. Med tanke på att Nordea har ca 1.8 miljoner kunder i Sverige (http://www.bankforeningen.se/upload/internetbank_2005.pdf), kan även denna siffra ge en fingervisning på andelen personer hos Nordea som har mottagit phising e-postmeddelande.

Under tiden som uppsatsen skrevs blev Nordea utsatt för ytterligare en phishingattack (http://www.pts.se/internetsakerhet/Nyheter/nyhet.asp?ItemId=327) (Se bilaga 3). Detta tyder på att uppsatsen belyser ett högaktuellt ämne. Vilket visar att problemet är långt ifrån löst och det är otroligt viktigt att skapa en medvetenhet bland användarna för att i bästa möjliga mån kunna skydda användarna mot phishingattentat.

7.2 Kritiskt granskning

Under uppsatsen fanns det en del begränsningar såsom tids- och ekonomiska begränsningar. Denna uppsats ger endast en fingersvisning på phishing som fenomen d.v.s. undersökningen ger bara en antydan om problemet med phishing och dess utsträckning. Något som observerades vid enkätsummeringen är följderna av att enkäten utdelades i Lund. Att enkäten delades ut i Lund medförde att den största delen av respondenterna höll på med en universitetsutbildning eller hade avlagt en universitetsexamen. Dock gjordes försök att att vidga respondentgrupperna genom att dela ut enkäten vid olika platser på stan, istället för att

endast dela ut enkäten på universitetsområdet, allt för att undvika en alltför homogen svarsgrupp.

Fråga sex behandlade hur respondenten ansåg att bankens säkerhetsinformation var utformad, på frågan svarade de flesta respondenter att den var tillfredsställande eller bra. För att inga otydligheter skulle förekomma mellan vad vardera svarsalternativ avser på fråga sex, så kunde eventuellt svarsalternativen formulerats lite tydligare. En del av respondenterna missade att svara på fråga nio, så endast 42 av 60 besvarade frågan. Uppenbarligen tolkade en del av respondenterna att de inte skull besvara frågan om det inte själva hade mottagit ett e-postmeddelande som ställdes på fråga sju.

7.3 Framtida forskning

Eftersom denna kandidatuppsats är avgränsad till två svenska banker, föreslås det att även andra banker som erbjuder Internettjänster ska undersökas. Undersökningen på de andra bankerna skulle kunna bedrivas på ett likartat sätt denna, med samma enkätfrågor som användes i denna undersökning. Om en mer omfattande studie genomförs på ett flertal individer, vore det intressant och se utifall de demografiska egenskaperna såsom kön, ålder och utbildning påverkar användandet och uppfattningen om riskerna vid inloggningen till Internetbanken.

Eftersom flertalet banker ger möjligheten att använda olika inloggnignstekniker vid inloggning till Internetbanken skulle inloggningstekniker till Internetbanker såsom exempelvis e-legitimation skulle vara intressant att belysa. Ytterligare intressanta undersökningsperspektiv skulle vara att undersöka två banker som använder sig av samma inloggningsteknik, såsom t.ex. den elektroniska dosan som genererar engångskoder och belysa likheter och skillnader mellan bankerna.

Vidare framtida forskning skulle kunna vara mer orienterad mot banken, då bankens hemsida fungerar som en mötesplats mellan bank och kund (Foxall et al. 2005). Svenska bankers hemsidor skulle kunna testas och undersökas på ett likartat sätt som en undersökning som genomförts i England, vilket finns att läsa om i sin helhet i Foxall’s et al. (2005). Undersökningen som genomfördes i England var en fältstudie där potentiella användare ombads utföra vissa specifika uppgifter på bankens hemsida. Kunden skulle sedan registrera sina intryck och uppfattning om banken och dess hemsida.

Källförteckning

Litteratur

Backman, J. (1998). *Rapporter och uppsatser*. Studentlitteratur, Lund.

Bell, J. (1993). *Introduktion till forskningsmetodik*. Studentlitteratur, Lund.

Bryman, A. (1997). *Kvantitet och kvalitet i samhällsvetenskaplig forskning*. Studentlitteratur, Lund.

Bryman, A. (2002). *Samhällsvetenskapliga metoder*. Liber ekonomi, Malmö.

Denscombe, M. (2004). *Forskningens grundregler*. Studentlitteratur, Lund.

Patel, R. & Davidsson, B. (1991). *Forskningsmetodikens grunder*. Studentlitteratur, Lund.

Schneider, F. B. (1999). *Trust in cyberspace.*

Trost, J. (2001). *Enkätboken*. Studentlitteratur, Lund.

Turban, E., King, D., Lee, J., Viehland, D. (2004). Electronical Commerce: *A Managerial Perspective*. Prentice Hall, Special International Edition.

Wallen, G. (1996). *Vetenskapsteori och forskningsmetodik*. 2:a upplagan. Studentlitteratur, Lund.

Artiklar

Allen, M. (2006). *Social Engineering: A means to violate a computer system.* SANS Institute.

Berghel, H. (2006). *Phishing Mongers and Posers.* Communications of the ACM; April 2006/vol 49. No. 4.

Bingell–Baxter, K. (2006). *Authentication in an Internet Banking Environment*; Towards Developing a Strategy for Fraud Detection

Dhamija R, J.D. Tygar, M.Herst (2006). *Why Phishing Works.*

Ericsson, N. (2006, november 15). Nya bedrägeriförsök mot Nordeas kunder. *Sydsvenskan*, s.A21.

Foxall, G.-R., Pallister, J.-G., & Yousafzai, S.-Y. (2005). *Strategies for Building and Communicating Trust in Electronic Banking: A Field Experiment*. Psychology & Marketing, Vol.22(2), 181-201 (Februari 2005).

Hansson, S.-O. (2006). *A note on social engineering and the public perception of technology.*

Hølle, K. J., Moen, V., & Tjøstheim, T.(2006). *Case Study: Online Banking Security.* IEEE Computer Society.

IT Pro p. 5 (2005). *Spike in Phishing and Malware a Danger to IT.*

Johnson, D. & Grayson, K. (2003). *Cognitive and effective trust in service relationships.* Journal of Business Research 58 (2005).

Levine, L.–T. (2006). *Phishing, Pharming and Other Devious Means to Steal Your Good (Brand) Name.* Community Banker; Aug 2006; p. 60.

Musthaler, L. (2006). *How social engineering sinks security*. Network World, Okt 9, 2006; p. 45

Rombel, A. (2005). The *worlds best internet banks 2005.* Global Finance, Dec. 2005, p. 29.

Wetzel, R. (2005). *Tackling phishing.* Business Communications Review, Feb 2005, p.46.

Internetkällor

www.wikipedia.org
http://en.wikipedia.org/wiki/Phishing
Datum 9/11-06

http://www.cissponline.com/index.php?name=News&sid=2&file=article&pageid=2
Datum 9/11 -06

http://www.antiphishing.org/
Datum 9/11-06

http://www.securityfocus.com/infocus/1527
Datum 10/11-06

http://whitepapers.zdnet.com/
Datum 10/11 -06

http://www.idg.se/2.1085/1.74862
Datum 10/11 -06

http://www.idg.se/2.1085/1.79590
Datum 10/11 -06

E-föreläsning
http://www.esecurelive.com/jsp/archiveDetail.jsp?meetingID=414&sectionID=security
Datum 20/11 -06

http://www.dn.se/DNet/jsp/polopoly.jsp?a=582687
Datum 23/11-06

Bankforeningen (2005). *Bank och finansstatistik Fakta om banker i Sverige.*
http://www.bankforeningen.se/upload/bank-och_finansstatistik_2005_004.pdf
Datum 24/11-06

http://www.bankforeningen.se/upload/internetbank_2005.pdf
Datum 24/11-06

http://www.sans.org/reading_room/whitepapers/engineering/529.php?portal=64d6c1b7ecd22626bfd3b74b7cdadefd
Datum 4/12 -06

McAfee (2006) whitepaper, ”Understanding phishing and pharming”
http://www.mcafee.com/us/local_content/white_papers/wp_phishing_pharming.pdf
Datum 4/12 -06

Symantec (2006) ”Internet Security Threat Report”
http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf
Datum 4/12 -06

http://www.idg.se/2.1085/1.88194
Datum 13/12 -06

Nordea
www.nordea.se
http://app.nordea.se/login/index.html
Datum 12/12-06

Swedbank
www.swedbank.se
https://internetbank.fsb.se/SecurityServer/SecurityServer?TDEApplName=TDEApplIdentifiering&_flow_id_=LISTA_IDENTIFIERINGSMETODER_CLIENT&_new_flow_=true&firstReq=true&erendeid=PWrrZq5yzmlcxYgT%2BLFMjtDQ%2B0o6W0JAY2EwZTM4OvjWs%2BU%3D
Datum 12/12-06

Post och Telestyrelsen
http://www.pts.se/internetsakerhet/Nyheter/nyhet.asp?ItemId=327
Datum 13/12 -06

Bilaga 1

Hur är din syn på Internetbanken?

En enkätundersökning rörande Internetbankanvändarnas säkerhet

Kön?		Ålder?	Utbildning
Man	☐	**18-25** ☐ **26-35** ☐	**Grundskola** ☐
Kvinna	☐	**36-49** ☐ **50-59** ☐	**Gymnasium** ☐
		60+ ☐	**Universitet** ☐

1. Du är kund hos?

Swedbank ☐

Nordea ☐

Annan _____

2. Hur länge har du använt dig av Internetbanken?

_____

T.ex. antal år eller månader

3. Hur medveten anser du dig själv vara om riskerna gällande inloggningen på din Internetbank?

Det finns inga risker ☐

Jag litar på banken ☐

Jag håller mig uppdaterad om eventuella risker ☐

4. Vilken datorvana har du?

Använder dator så lite som möjligt ☐

Använder dator ett par ggr/vecka ☐

Använder dator dagligen på jobbet ☐

Använder dator så mycket som möjligt ☐

5. Har du läst säkerhetsinformationen på bankens hemsida?

Ja, men bara helt kort ☐

Ja, jag tror jag vet vad som gäller ☐

Ja, noga jag vet precis vad som gäller. ☐

Ja, jag kollar efter sådant varje gång jag loggar in ☐

Nej *Om Nej, hoppa över nästa fråga* □

6. Hur anser du att bankens säkerhetsinformation är utformad?

Dåligt	**Tillfredställande**	**Bra**	**Utmärkt**
□	□	□	□

7. Har du fått e-post meddelande från din bank?

Ja □

Nej □ *Om Nej Hoppa över nästa fråga*

8. Följde du anvisningar i e-post meddelandet?

Ja □

Nej □

9. Känner du till någon annan som har fått ett liknande e-post meddelande?

Ja □

Nej □

10. Jag känner mig säker när jag loggar in på min Internetbank

Instämmer helt □

Instämmer delvis □

Tar delvis avstånd □

Tar helt avstånd □

11. En typ av Internetbedrägerier kallas ibland för "Phishing" och innebär att man luras med hjälp av falska Internetsidor.
Hur medveten är du om detta tillvägagångssätt?

Jag känner inte till det alls □

Jag har hört talas om det □

Jag vet vad det är, men inte i detalj □

Jag är väl informerad och vet precis! □

12. Har du vid något tillfälle avstått från att använda din Internetbank?

Ja ☐ *Om Ja varför, markera ett alternativ nedan*

Nej ☐

Bankens Internetsida fungerade inte ☐

Kände mig osäker på att logga in på Internbanken ☐

Utförde mina ärenden direkt på banken ☐

Annat *skriv här* _____

Tack för att du har besvarat enkäten och därmed hjälpt oss i vårt kandidatuppsats.
Kalle, Tomas

Bilaga 2

Artikel från Sydsvenskan 15 November 2006

SYDSVENSKAN Onsdag 15 november 2006 **Ekonomi** A21

REDIGERING: KIM OLTHED

Nya bedrägeriförsök mot Nordeas kunder

MALMÖ. Återigen har Nordeas internetbankkunder blivit utsatta för en en så kallad phishingattack, ett försök av bedragare att lura av bankkunderna deras kontonummer och lösenord.

Det senaste bedrägeriförsöket går ut på att lura kunderna att säkerheten på Nordeas internetbank förbättrats och kunden uppmanas klicka på en falsk inloggningssida och där lämna ifrån sig kontonummer och personlig kod.

– Det är samma brev som mejlats ut vid upprepade tillfällen under hösten. Blufförsöket börjar nu bli känt hos våra kunder och för närvarande känner jag inte till någon som drabbats ekonomiskt, säger Nordeas presschef Boo Ehlin.

Men efter tidigare phishingattacker i år har ett hundratal Nordea-kunder blivit av med pengar på sina konton efter att ha lämnat ut kontonummer och personlig kod till bedragarna.

Enligt Nordea har de tillsammans blivit av med 3,5 miljoner kronor.

Nordea lovar att de som drabbats av phishingattackerna ska hållas skadeslösa.

– Vi kompenserar alla som lurats på pengar av de falska mejlen, säger Boo Ehlin.

En av de högsta ersättningarna hittills till en enskild Nordea-kund är 175 000 kronor.

Nordeas internetbankkunder har drabbats värst av phishingattackerna av samtliga svenska banker. Att Nordeas internetbank har sämre säkerhet än konkurrenterna förnekar dock Boo Ehlin.

– De ger sig helt enkelt på den största banken. Vi har 2,3 miljoner internetbankkunder i Sverige och 4,5 miljoner i Norden, säger han.

Men samtidigt uppger Nordea att man ska se över systemet med engångskoder, de skrapkort med koder som kunderna har för att logga in sig på Nordeas internetbank. Datasäkerhetsexperter har dömt ut skrapkorten som osäkra och istället förordat de mer säkra elektroniska dosorna som bland andra SEB och Swedbank använder sig av.

I dagsläget är Nordeas råd till kunderna att omedelbart ta bort mejl som utger sig komma från banken.

– Det finns en enkel regel, befatta er inte med mejl som påstår sig vara från Nordea. Vi skickar inga mejl över huvud taget, vi skickar vanliga brev. Den som fått ett falskt mejl ska ta bort det från datorn och den som öppnat en länk bör köra sitt antivirusprogram, säger Boo Ehlin.

Text: **Niclas Ericson**
niclas.ericson@sydsvenskan.se

FAKTA

Vanligt med falsk e-post

Nätfiske eller phishing (efter engelskans fishing, "fiske") är en olaglig metod för att främst lura innehavare till bankkonton att delge kreditkortsnummer, lösenord eller annan känslig information.

Phishingbedrägeri är oftast ett mejl som ser ut att komma från en banks eller kreditkortföretags supportavdelning. Bedragaren uppger att det uppstått problem med kundens konto, eller motsvarande, och behöver då kontonummer och lösenord för att åtgärda felet.

Phishingutskick skickas ofta till alla mejladresser som bedragaren kan komma över i hopp om att åtminstone ett fåtal ska luras att svara.

En annan form av phishingbedrägeri är när kontantluckan på betalningsautomater förstörs och en kortläsare göms bakom apparatens front som läser av informationen på kreditkortets magnetremsa.

Bilaga 3

Nya phishingattacker, 2006-12-17

"Nordea Banken" <kontakt@nordea.se>
Sent by: User uhaqmkez <uhaqmkez@dsl88-226-15293.ttnet.net.tr>
2006 12-10 17:26

Subject Viktiga nyheter fran var bank
Fornyelser av online-bankskyddssystemet

Om man klickar på länken, hänvisas man till en hemsida som ser ut som Nordeas inloggnings sida, fast om man uppmärksammar adressen då märker man att det är inte den rätta sidan.

http://80.97.77.137:7640/http/app.nordea.se/sitemod/default/portal.aspx/login/pid=2000000/index_php/index.php

De flesta attacker sker från utlandet som också bekräftades av SITIC. Denna gång var det en attack från Turkiet om man kollar avsändarens adress och den fejkade hemsidans adress.