VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Joachim Gunell

INTERNETBEDRÄGERIER – EN UNDERSÖKNING OM KUNSKAP OCH ERFARENHETER

Informationsbehandling
2012

FÖRORD

Detta lärdomsprov har skrivits under sommaren och hösten 2012 i syfte att erhålla tradenomexamen inom utbildningsprogrammet för informationsbehandling vid Vasa yrkeshögskola. Kenneth Norrgård har fungerat som handledare.

Jakobstad 21 december 2012

_____

Joachim Gunell

VASA YRKESHÖGSKOLA

Utbildningsprogrammet för informationsbehandling

ABSTRAKT

Författare	Joachim Gunell
Lärdomsprovets titel	Internetbedrägerier – en undersökning om kunskap och erfarenheter
År	2012
Språk	svenska
Sidantal	38 + 4 bilagor
Handledare	Kenneth Norrgård

Syftet med detta arbete var att göra en undersökning om internetbedrägerier och kunskap samt erfarenheter om dessa för en viss målgrupp. Beroende på tolkningen och resultatet av de svar som har fåtts har en slutledning gjorts.

Detta arbete innehåller redovisningar till olika internetbedrägerier samt en undersökning om målgruppens erfarenheter och kunskap gällande dessa bedrägerier. Problemområdet till varför jag har valt detta som ämne är att det inte har gjorts någon liknande undersökning gällande bedrägerier på internet. Inget liknande finns skrivet om ämnet i Theseus. Ändamålet med undersökningen var att få en helhetsinsyn på målgruppens erfarenheter och kunskaper gällande ämnet.

Resultatet av detta arbete var en slutledning och tillfällig lägesrapport baserat på svaren från frågeformuläret om internetbedrägerier.

Ämnesord	Internet, Bedrägeri, Säkerhet, Surveyundersökning

VAASAN AMMATTIKORKEAKOULU

UNIVERSITY OF APPLIED SCIENCES

Utbildningsprogrammet för informationbehandling

ABSTRACT

Author	Joachim Gunell
Title	Internet frauds - a survey of knowledge and experiences
Year	2012
Language	Swedish
Pages	38 + 4 appendices
Name of Supervisor	Kenneth Norrgård

The aim of this thesis was to do a survey on Internet frauds and knowledge and experiences on these for a specific audience. Depending on the interpretation and the results of the responses that have been received, a conclusion has been made.

This thesis work contains accounts of various Internet scams and a survey of the target group's experience and knowledge regarding these scams. The problem area and the reason why I have chosen this as a topic is that there has been no similar study regarding internet frauds. Nothing like this has been written on the subject in Theseus. The purpose of the survey was to gain an overall insight on the target group's experience and knowledge regarding the topic.

The result of this work was a conclusion and a temporary progress report based on the responses from the questionnaire about internet frauds.

Keywords Internet, Fraud, Security, Survey study

INNEHÅLL

FÖRTECKNING ÖVER FIGURER OCH TABELLER

TERMINOLOGI

Här beskrivs en del ord och uttryck som förekommer i mitt lärdomsprov. Först kommer själva ordet, och därefter ordets betydelse.

En cache är ett tillfälligt dataminne. Information sparas ofta av datorer för att hastigt användas om igen. Det här händer i något som kallas cacheminne. Flera cachetyper existerar. Webbläsare brukar allmänt spara de 500 senast besökta webbsidorna i denna cache. [3]

En DNS är en service vars uppgift är att interpretera en dators namn som t.ex. argo.kib.ki.se till ett siffertal i IP-form som t.ex. 130.237.123.30. I alla domäner existerar åtminstone en dator som funktionerar som en DNS-server. Benämns också som name-servers. [3]

E-mail är en funktion på Internet som används bland användare till att sända meddelanden och skrifter med. [3] Också känt som e-post.

IP står för Internet Protocol och är ett protokoll som används i kommunikativt syfte. Dess uppgift är att skildra adressering och vägval (eng. routing) för informationspaket på Internet. [3]

Keylogger är en tangentbordsregistrerare, en form av malware, mjukvara som noterar varje tangenttryckning, då också lösenord och andra sekretiva uppgifter för att sedan sända dem vidare till någon illvillig individ. [10]

Lösenord, på engelska password, är en speciell följd av alfanumeriska tecken som bör fastställas av användaren innan denne får tillträde in på ett datorsystem. Används för identifiering och behörighetskontroll. [10]

En server är programvara inuti ett datasystem som offererar verksamheter åt program som existerar i övriga datorer. [3]

URL, Uniform Resource Locator, webbadress, är en helhet för adresskoder på Internet. En standardiserad och speciell adress för skrifter på Internet. [10 & 3]

En webbsida är dokument som utges på webben. En webbsida förmår sig att innehålla ren text, bilder, programmeringsbara områden, filmer samt hyperlänkar. Webbsidor som brukas i syfte av att introducera någon eller någonting benämns ofta som hemsidor. [3]

1 INLEDNING

Detta arbete handlar om bedrägerier på internet. Alla har vi väl någon gång hört om dessa bedrägerier och vad de orsakar. Till exempel då en person får sitt lösenord stulet till ett konto denne har på någon webbsida, eller när någon blir bedragen på sin bankkodsnummer. Det faktum att bedrägerierna nu för tiden är allt vanligare än förr och blir bara större och fler till antalet är inte alls bra. När man ser på antalet bedrägerier som har blivit anmälda börjar man nog undra hur det kommer att se ut om några år.

Även om många bedragare blir fasttagna, ökar antalet bedrägerier med varje sekund som går. Anmälningar sker flitigt, det är ändå inte ofta någon låter bli att anmäla en sådan här brottstyp. Jag valde denna rubrik för mitt examensarbete på grund av att det är något som till min kännedom inte har gjorts någon undersökning gällande detta ämne. Samtidigt också för att det på ett sätt är intressant att ta reda på och få veta hur dessa bedragare bär sig åt när de lurar folk, vilka tekniker de använder sig av osv. Syftet med arbetet är att berätta och informera om bedrägerier, men den praktiska uppgiftens syfte är att ge en utvärdering av resultatet av frågeformuläret och målgruppens svar. Beroende på resultaten kan frågan om behovet av en eventuell ny kurs som handlar om internetbedrägerier besvaras positivt eller negativt.

Det andra kapitlet handlar allmänt om bedrägerier, vad som kännetecknar dessa och vilka som drabbas av dem. Några olika typer av bedrägerier redovisas för samt en del bilder som tillhör dessa bedrägerier. Efter det redovisas några olika sätt att skydda sig från bedrägerier samt hur man kan undvika dem.

Den praktiska uppgiften består av ett frågeformulär om bedrägerier som en målgrupp har fått fylla i. Målgruppen för denna undersökning var studerande inom utbildningsprogrammet för informationsbehandling vid Vasa yrkeshögskola. Resultatet av frågeformulärets individuella frågor visas med ett procentdiagram, och antalet personer som deltog i frågeformuläret. Efter det visar jag slutsatsen som drogs på basen av undersökningen och resultatet som den gav.

1.1 Avgränsningar

Ämnen som virus och till viss del spionprogram kommer inte att behandlas. Orsaken till detta är att de inte direkt är bedrägerier, även om de kan vara menade som sådana. Virus är för det mesta ämnade till att sabotera och förstöra datorer med, men det finns undantag på den fronten också.

2 BEDRÄGERIER

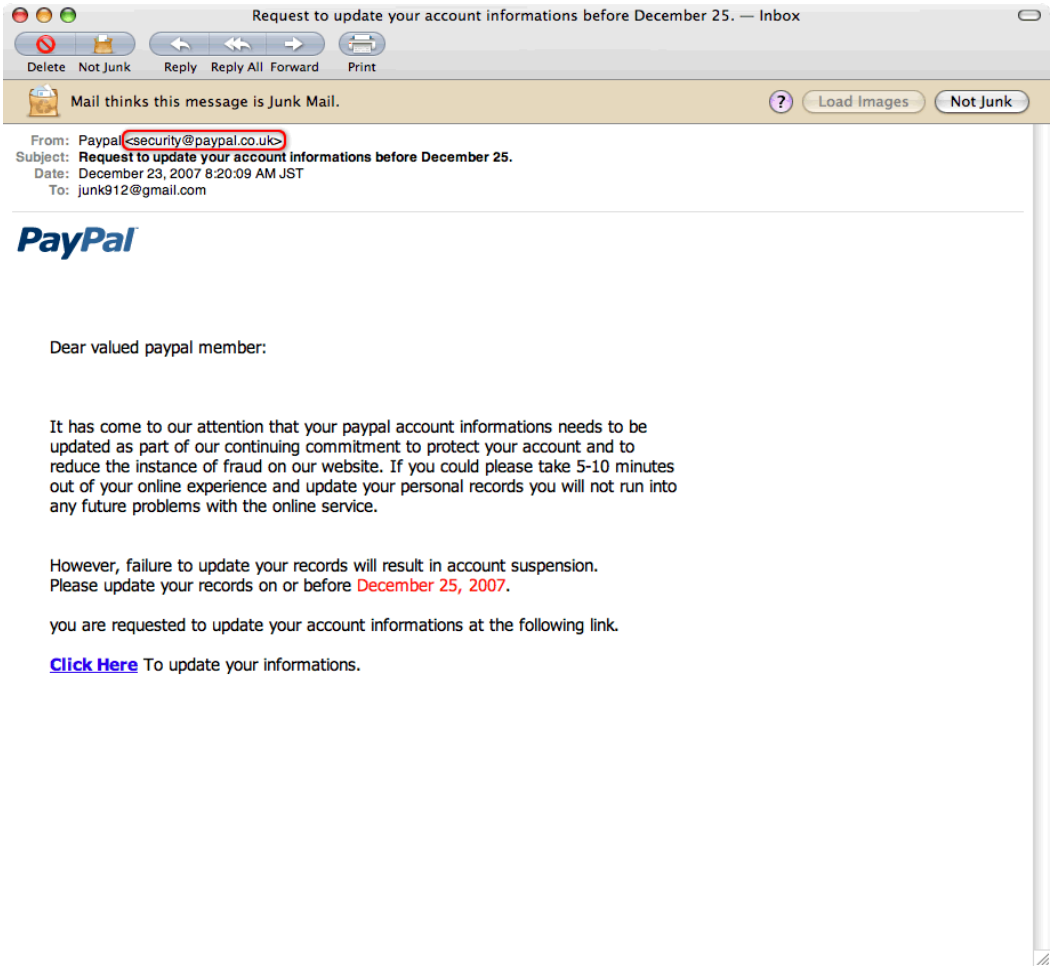
Bedrägerier på internet är ett ganska känt faktum, de händer allt mer och oftare. De som drabbas av bedrägerier kan ganska ofta vara en bred grupp, men t.ex. när det handlar om phishing så är den amerikanska auktions-sidan Ebay's kunder ett stort mål. Även kunder vid olika nätbanker, t.ex inom Finland så brukar Nordea vara ett hett mål för bedragare. För det mesta så kan dock bedragarnas offer vara vem som helst som befinner sig på internet i någon tjänst.

2.1 Phishing

Nätfiske (phishing på engelska) är en typ av bedrägeri som går ut på att lura datoranvändare att avslöja privat information via e-post eller webbsidor. Vanligtvis börjar nätfiske med att du får ett e-postmeddelande som verkar vara från en trovärdig avsändare, till exempel en bank eller en stor e-butik. I meddelandet hänvisas du till en webbsida där du ombeds uppge information som kontonummer och lösenord. Webbsidan är dock falsk och bedragarna använder informationen till att begå olika typer av brott, i ditt namn. [1, s 65]

E-postmeddelandet kan även innehålla ett erbjudande med en länk till en webbplats där du får mer information. När du klickar på länken visas webbplatsen och ett program laddas ner till din dator utan att du märker det. Detta program kan då samla in personlig information som exempelvis användarnamn och lösenord till din Internetbank, och skicka informationen vidare till bedragaren. [1, s 65]

I många e-postprogram och webbläsare finns ett inbyggt nätfiskefilter för att skydda dig som användare. Filtret jämför webbadresserna som du besöker med en lista över webbplatser som rapporterats som legitima. Filtret analyserar även webbplatserna för att se om de har gemensamma egenskaper med nätfiskewebbplatser. Om filtret misstänker att det är en nätfiskewebbplats kommer du att bli varnad, och du kan välja mellan att gå vidare till webbplatsen efter varningen eller att stänga webbsidan. [1, s 65]



Figur 1: *Phishingmail* [12]

Detta är ett exempel på ett phishingmail, förklätt som ett officiellt mail från en bank. Avsändarens avsikt är att lura mottagaren att visa sin information genom att bekräfta och uppdatera kontoinformationnen på fiskarens hemsida. Lägg märke till felstavningen av en del ord i brevet. Även om sidan verkar vara legitim, så länkar den faktiskt till fiskarens hemsida.

Figur 2: *Phishingsida* [6]

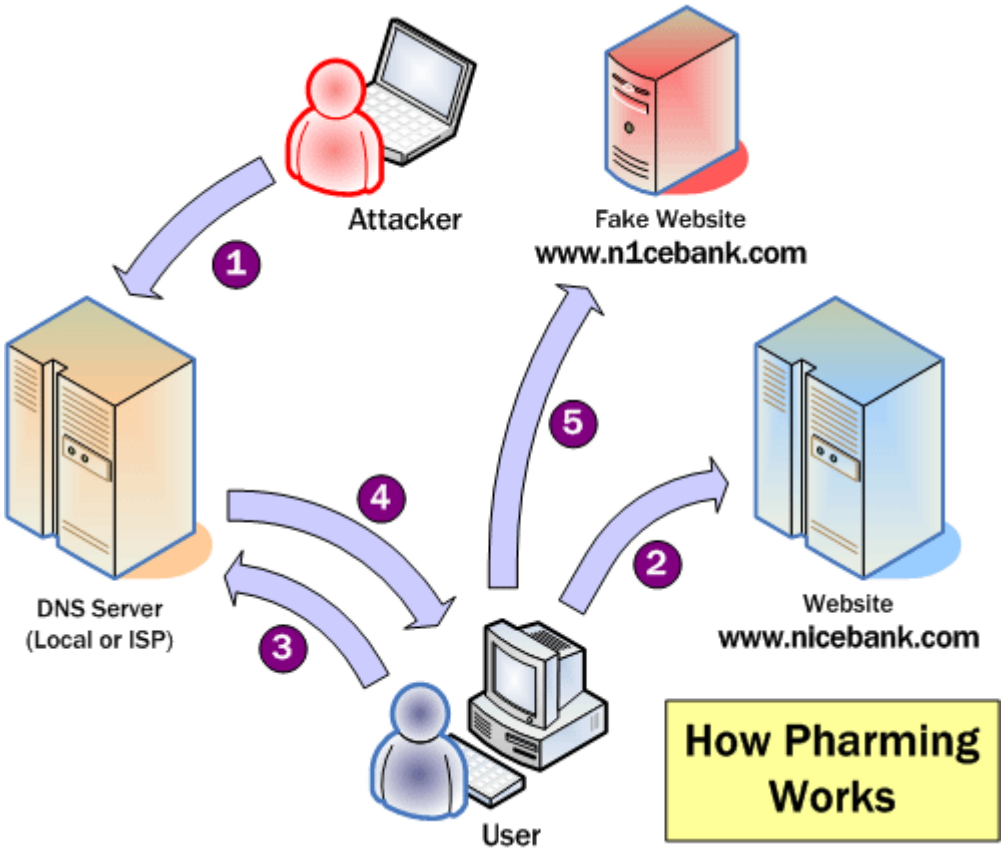
Ännu ett exempel. Denna banksida ser ut att vara legitim, men det är den inte. Kollar man på sidans URL så stämmer den inte alls överrens med den riktiga.

2.2 Pharming

Pharming påminner en hel del om phishing. Dock där phishing endast använder fejkad e-post och hemsidor i syfte av att bedra användaren på dennes personliga uppgifter så är pharming en grad värre. Hela poängen med pharming är att påverka adresservarna på internet så att besökare helt av sig själv skickas till en förfalskad sida. Händelsen kan leda till att fast du har gett en rätt webbadress (till exempel www.swedbank.se) så skickas du till en falsk webbsida som påminner om bankens egna sida. [14]

Attacker i form av pharming brukar inte någon speciell nymodig metod. För det mesta så brukar de den vanliga och kända DNS cache förgiftningen, domän spoofing och kapningstekniker för domäner. Alla dessa har existerat relativt länge. Motiven för att göra dessa attacker har emellertid förändrats. Förut var attackerarna engagerade i att bara besvära tjänster och skapa förtretligheter. Nuförtiden så går allt mera ut på göra ekonomisk vinning istället för att visa vad man kan. Teknika fortsätter att finnas då administratörer och webbplatsägare inte anstränger sig med att skydda och bevaka sina DNS-servrar allteftersom de har placerat summor av miljontals dollar i så kallade applikationsbrandväggar. [11]

Pharming brukar svaga punkter i system för att klara av sin uppgift. De svaga punkterna kan existera i din dator eller i olika stycken av domännamnssystemets (DNS) bland t.ex. Internetleverantörer. Det blir en hel del svårare för dem som ämnar att göra en pharmingattack om du har skydd som t.ex. brandvägg och antivirusprogram på din dator. Man bör komma ihåg att det är viktigt att hålla skydden uppdaterade. Det är på samma vis också för operativsystemet och webbläsaren. Trots all skrämsel kring pharming så är pharmingattacker svåra att utföra och händer på så vis inte lika tätt som phishingattacker. [14]



Figur 3: *Hur Pharming fungerar* [11]

1. Angriparen riktar DNS-tjänsten som används av kunden. Denna server kan vara en DNS-server på det lokala nätverket eller så underhålls DNS-servern av en ISP för alla användare. Angriparen kan med hjälp av diverse tekniker åstadkomma att ändra IP-adressen för "www.nicebank.com" till IP-adressen för en webbserver som omfattar en falsk kopia av nicebank.com. [11]
2. Användaren vill gå till webbplatsen "www.nicebank.com" och skriver in adressen i webbläsaren. [11]
3. Användarens dator frågar DNS-servern efter IP-adressen för "www.nicebank.com". [11]
4. Då DNS-servern tidigare har blivit "förgiftad" av angriparen så ges IP-adressen för den falska webbplatsen tillbaka till användarens dator. [11]

5. Användarens dator blir lurad och tror att det förgiftade svaret som den har fått är den rätta IP-adress till webbplatsen. Användaren har nu blivit lurad att besöka den falska webbplatsen som kontrolleras av angriparen i stället för den äkta www.nicebank.com hemsidan. [11]

Då angriparen har åstadkommit att få användaren att besöka den falska webbplatsen så existerar det flera metoder som kan användas för att få användaren att avslöja hans / hennes meriter eller ge ut personlig information. Pharmingens anseende över nätfiske bevisas av det faktum att ett lyckat försök i förgiftning av DNS-servern möjligen kan brukas för att lura varenda användare i den DNS-tjänsten. Det är mycket mindre ansträngning än vad som krävs inom nätfiske och har därtill bredare effekt. [11]

2.3 Nigeriabrev

Sättet hur nigeriabrev går till på är oftast samma i alla dess typer. Man får ett e-postmeddelande från en individ i Afrika, och denne lovar dig en stor summa pengar i gengäld för hjälp med en tjänst.Dock måste du till först föra över en summa pengar till honom innan du kan ta del av din vinst. Slutligen så ser den som blivit lurad aldrig av några pengar och bedragaren är som försvunnen. Med lite tur så kan du komma ur situationen med endast en liten pengaförlust. Tyvärr så finns det dock människor som har råkat ordentligt illa ut då de har bestämt att möta bedragarna. [13]

Bedragaren har möjlighet att kontakta dig via brev, e-mail eller till och med telefon och påstå sig själv att vara allting från en revisor till en avsatt kunglighet eller politiker. [8]

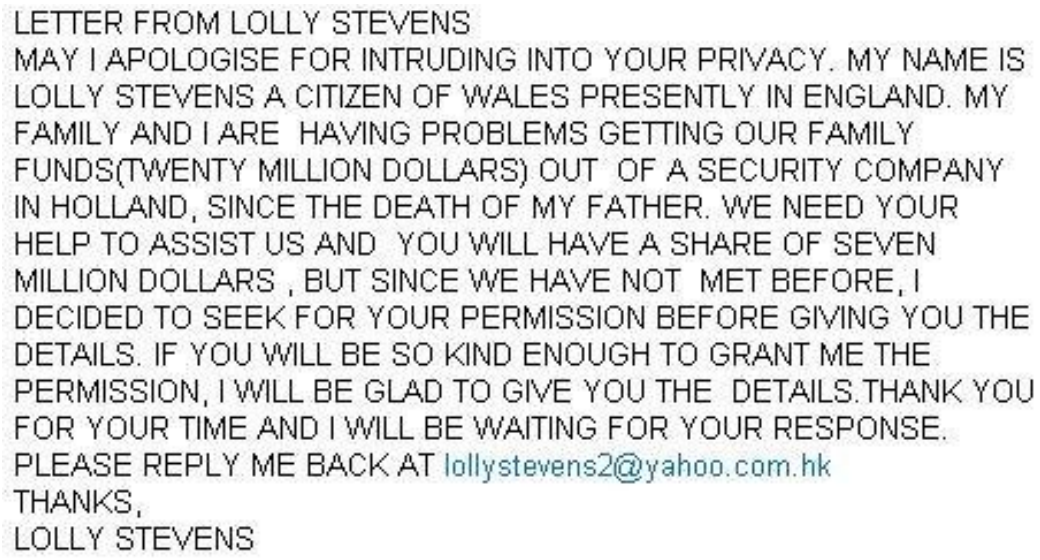
Tidvis så är det en bankanställd som vet av en nyligen avliden rik person som inte innehar några släktingar och erbjuder dig då en del av förmögenheten, (25-30% av 20-30 miljoner dollar), detta i gengäld mot att de får använda sig av ditt bankkonto i syfte av att föra pengarna ut ur landet. [8]

Nigeriabrev, eller bedrägeri 419 som de brukar kallas kan ibland vara skapade på olika sätt men dock så är utgångspunkten ständigt densamma. Innehållen i breven

brukar t.e.x. återge om diktaturen i de länder som avsändarna bor i eller innehålla andra tillsägelser i syfte av att påverka samvetet så att man är överrens med sig själv om att man utför en god gärning och också får en ekonomisk vinst i samband med detta.[13]

Händelser har inträffat då offren har blivit tillsagda att egenhändigt konfrontera bedragarna i deras hemländer för att hämta pengarna, och till följd av detta så har de tagits och hållts som gisslan ända tills att en enorm lösensumma har givits åt bedragarna. Det är även inte ovanligt att mord på människor som har blandat sig i nigerabedrägerier har skett. [13]

Till att börja med så kom den här typen av brev från landet Nigeria, och det var så det fick sitt namn. Nuförtiden så existerar dock avsändare från en hel del andra länder. [13]


LETTER FROM LOLLY STEVENS
MAY I APOLOGISE FOR INTRUDING INTO YOUR PRIVACY. MY NAME IS LOLLY STEVENS A CITIZEN OF WALES PRESENTLY IN ENGLAND. MY FAMILY AND I ARE HAVING PROBLEMS GETTING OUR FAMILY FUNDS(TWENTY MILLION DOLLARS) OUT OF A SECURITY COMPANY IN HOLLAND, SINCE THE DEATH OF MY FATHER. WE NEED YOUR HELP TO ASSIST US AND YOU WILL HAVE A SHARE OF SEVEN MILLION DOLLARS , BUT SINCE WE HAVE NOT MET BEFORE, I DECIDED TO SEEK FOR YOUR PERMISSION BEFORE GIVING YOU THE DETAILS. IF YOU WILL BE SO KIND ENOUGH TO GRANT ME THE PERMISSION, I WILL BE GLAD TO GIVE YOU THE DETAILS.THANK YOU FOR YOUR TIME AND I WILL BE WAITING FOR YOUR RESPONSE.
PLEASE REPLY ME BACK AT lollystevens2@yahoo.com.hk
THANKS,
LOLLY STEVENS

Figur 4: *Nigeria brev* [15]

Ett exempel på ett nigeria brev. I brevet så skriver avsändaren att dennes familj bor i Wales och har problem med att få deras familjefond (20 miljoner dollar) ut från ett säkerhetsföretag i Holland sedan avsändarens fader dog. De behöver din hjälp med att göra detta, och erbjuder att dela med sig 7 miljoner dollar för

besväret. Dock eftersom ni aldrig har träffats så vill denne person ha tillåtelsen så att detaljerna kan skickas.

2.4 Bedrägeri vid handling med kort

När en person handlar med ett bankkort via internet, så lagras informationen om kortet i de flesta nätbutikers databaser. Databaserna i fråga kan hamna ut för intrång, och detta beror oftast på att butikernas säkerhetsskydd inte är tillräckligt bra. Genom dessa intrång kommer bedragare över information om kunders kort. [13]

2.5 Modemkapning

Modemkapning betyder att en person kopplar om ditt modem till ett nytt telefonnummer, med en dyr minutavgift. Kapningen sker genom ett program som utan att du vet om det har blivit nedladdat till datorn. Vanligast är att modemkapningen sker på grund av att en webbsida, annons eller liknande säger åt dig att installera en programvara eller genom ett program som skickas via e-post eller alternativt en chatttjänst. [14]

Har du ett vanligt Internetabonnemang som fungerar på det viset att du ringer upp ett telefonnummer med hjälp av ett modem, så kan du tyvärr råka ut för detta bedrägeri. Använder du däremot det mera moderna och nutida bredbandsmodemet så är du säker. Dock så kan du som har bredband också råka ut för modemkapning OM du utöver ditt bredbandsmodem också har ett vanligt modem inkopplat till telefonjacket, t. ex. i syfte av att förmå dig att skicka fax från din dator. [14]

I slutändan har du en så kallad ”War Dialer” eller ”Porn Dialer” som är installerad och ringer upp dyra betaltjänster, satellitsamtal eller utlandssamtal. [2, s 258]

Du riskerar att ditt modem blir kapat om följande påståenden är uppfyllda:

- Du äger och innehar en dator som kopplas till Internet. [5]
- Din dator kör ett operativsystem från Microsoft (Windows). [5]

- Du äger ett modem som kopplas upp i din dator med hjälp av funktionen Fjärranslutning. [5]

Figur 5: *Misstänkt meddelande/säkerhetsvarning*

Så här kan ett misstänkt meddelande/säkerhetsvarning se ut. De flesta kanske inte tänker så mycket på vad det kan vara för ett meddelande och trycker på knappen ”Ja” nästan automatiskt.

2.6 Identitetsstöld

Identitetsstöld är ett brott där brottslingar härmar individer, oftast för en ekonomisk vinning. Dagens samhälle fungerar på ett sådant sätt att man i princip ofta måste avslöja personliga bitar information om sig själv, till exempel personnummer, en signatur, namn, adress, telefonnummer och även bank-och kreditkortsinformation. Om det är så att en tjuv har förfogande till denna personliga information, kan han eller hon bruka den för att begå bedrägerier i ditt namn. Med hjälp av denna information så kan tjuven göra olika saker som t.ex. ansöka om lån eller nya kontokortskrediter. Efter det kan dessa sedan begära en

ändring av faktureringsadress och tömma ditt befintliga kreditkort utan att du har någon som helst kännedom om det. Det är också möjligt för dem att använda falska checkar och betalkort, eller tillåta elektroniska överföringar i ditt namn, för att tömma ditt bankkonto. [16]

Oftast så är resultatet av en identitetsstöld lika, oavsett hur tjuven lyckas få tag på information. Internet har dock försett människor med nya sätt att stjäla personlig information och att begå bedrägeri på. Tjuvar förmår sig att komma upp till sina mål på flera sätt. Till exempel användning av chattrum på Internet och spridning av trojanska hästar som lämnar keyloggers på din dator för överföring av alla lösenord, användarnamn och kreditkortsnummer som du använder dig av tillbaka till tjuvarna. Flera nutida online företag lagrar även personlig information om kunder på sina webbplatser, och denna information används när en person använder webbplatsen en annan gång. Alla dessa saker innebär andra sätt att få tag på din personliga information. [16]

Identitetsbedrägerier som existerar på internet är ett dilemma samt en svårighet som gör att flera personer tänker både en och två gånger om att göra köp via internet, eller registrering av konton för användning till köpsidor så som t.ex. Paypal. [16]

Identitetsstölder på internet är verkligen ett populärt ämne inom dagens media. Det kan dock vara bra att veta att identitetsstölder på Internet representerar bara en minimal procentandel av alla bedrägerifall som är identitetsstölder. [16]

3 HUR MAN KAN SKYDDA SIG FRÅN BEDRÄGERIER

Att skydda sig från olika bedrägerier är viktigt och ett bra sätt att minska risken för att bli bedragen är att följa vissa riktlinjer och tips. I detta kapitel redovisas diverse riktlinjer och punkter för olika bedrägerier i syfte av att användas som beskyddning mot bedrägerier.

3.1 Phishing

Håll ett öga öppet för e-post som skickas från din bank eller online service, där dom uppmanar dig att besöka sidan och logga in. Du skall komma ihåg att det aldrig finns någon bank som upplyser sina kunder via e-mail att de skall logga in och byta användarnamn eller lösenord. Det är enkelt att förvanska avsändaradresser. Det finns inget sätt att garantera att avsändaren verkligen är den rätta. Använd inte länken som är bifogad i mailet, skriv istället in den länk du kommer ihåg eller använd dig av bokmärkesfunktionen och bokmärket som du har gjort för din online bank. Kontrollera ständigt att ditt system är uppdaterat. [4]

Tänk på att även legitima meddelanden och webbplatser kan fastna i filtret och att nätfiskewebbplatser kan missa filtret. Du måste hela tiden använda ditt eget omdöme. [1, s 65]

En webbsida som är legitim och trygg har en adress som börjar på https. Då du besöker en sådan webbsida bör en låsikon finnas nere i högra hörnet av din webbläsare. Dubbelklickar du på låsikonen så bör ett säkerhetscertifikat visa sig. Om namnet på offentliggöraren inte är namnet på webbsidan, så är det mycket troligt att webbsidan är falsk. Om du är osäker om ett e-mail – ring då det aktuella företaget (banken, internetleverantören m.m.) på deras riktiga telefonnummer och fråga dem om de har kontaktat dig angående dina uppgifter. Är det frågan om nätfiske (phishing), så skicka då vidare meddelandet till adressen för internettjänsteleverantören, t.ex. abuse@hotmail.com om meddelandet härstammar från ett konto hos hotmail. Använd dig av ditt bondförnuft och ställ dig själv frågan varför en äkta bank eller internetleverantör skulle behöva fråga efter dina personliga uppgifter på det sättet. [7]

3.2 Pharming

Att försvara sig bäst mot phishing och pharming bedrägerier är att vara skeptisk till meddelanden som skickas från din bank eller post som efterfrågar din personliga information. Om den webbsida du besöker är en SSL-aktiverad webbplats, se då upp för ett varnings-meddelande fönster. Uppstår ett sådant, så ska du dubbelkolla om den webbplats du är på har gett detta meddelande förut. Kolla om URL är samma som du ämnade att besöka. Meddelandet visas för det mesta då serverns SSL-certifikat inte stämmer överrens med webbadressen och om certifikatet har utgått. Det kan också betyda att det inte är undertecknat av en pålitlig rotcertifikat-myndighet. Installera samt använd anti-spyware verktyg som också kan vaka över phishing attacker. AdAware, Windows Defender, Spybot Search and Destroy är en del anti-spyware verktyg som också innehåller anti-phishing kontroller. Se till att spyware-signaturerna uppdateras till de senaste versionerna. Installera anti-phishing / anti-pharming verktyg för dina webbläsare. Verktygen hjälper att skilja en äkta webbplats från en falsk. Till exempel visar anti-phishing verktyget SpoofStick klart den rätta webbplatsens namn i webbläsaren. Detta är ett effektivt verktyg mot liknande och felskrivna domäner. [11]

Du gör det mycket svårare för de som vill utföra en pharmingattack om du har en brandvägg och ett antivirusprogram installerat på din dator. Att hålla dessa uppdaterade är självklart också viktigt, det samma gäller för operativsystemet och webbläsaren. [14]

3.3 Nigeriabrev

Överlämna inte några bankuppgifter eller övrig personlig information. Bedragarna kan bruka uppgifterna i syfte av att skapa förvanskade dokument, allt för att lura dig att tro att du har fått pengarna, och om du går på detta så brukar det vara enkelt att fortsätta med att lura pengar ifrån dig. [8]

Överlämna aldrig någonsin personlig eller ekonomisk information (till exempel PIN-kod, lösenord, med mera) via e-post eller på hemsidor som är osäkra. [11]

3.4 Bedrägeri vid handling med kort

Det finns ett sätt att inte drabbas av detta bedrägeri, det är att använda bankens tjänst e-kort. Tjänsten ansluts till ditt ordinära bankkort. Med ett e-kort skapas ett speciellt kortnummer för varje köp du utför. Ett e-kort funktionerar endast hos ett inköpsställe och du avgör själv för vilket belopp e-kortet gäller. [13]

3.5 Modemkapning

Ändra inställningen på ditt modem så att det hörs då det slår numret, således har du större chans att märka om modemet kopplar om och ringer ett annat nummer. Modemkapning fungerar endast för de som brukar ett vanligt modem, så att byta till bredbandsmodem är ett simpelt sätt att undvika bedrägeriet. Fråga din teleoperatör vilka tjänster för samtalsspärr de bjuder ut samt se till att förminska möjligheten att t ex koppla upp mot dyra utlandsnummer. Använd en annan variant av webbläsare. Det finns många webbläsare som har bättre försvar än Internet Explorer mot automatiska nedladdningar, såsom Opera och Mozilla Firefox. [5]

3.6 Identitetsstöld

Spara sensitiv information i filer och kataloger som skyddas av lösenord. Bruka dig gärna av lösenordshanterare, som t.ex. Norton Identity Safe i Norton Internet Security och Norton 360, för att skriva i inloggningsinformation automatiskt, utan att bruka dig av tangentbordet. Studera och träna dig på att märka falska emailmeddelanden, webbplatser och andra varningstecken som kan kopplas till nätfiske och pharming. Uträtta bara ekonomiska transaktioner på Internet via trygga webbplatser vars URL-adresser börjar med https: eller som har blivit autentiserade av företag som t.e.x VeriSign Installera en brandvägg, antiviruspogram, skydd mot spionprogram och spam. Alla dessa funktioner existerar i ett programpaket, detta då Norton Internet Security alternativt Norton 360 från Symantec. [9]

4 UNDERSÖKNINGEN

Detta är den empiriska delen av mitt lärdomsprov, och består av en undersökning i form av ett frågeformulär på informationsbehandlingslinjen i Vasa yrkeshögskola. Både de svenska linjerna samt de finska deltog i undersökningen. Motiveringen till varför jag valde just den här typen av praktisk uppgift som empirisk del hittas i underrubriken 4.1. Tanken bakom undersökningen var att skapa en helhetsbild av svaren från frågeformuläret och komma fram till ett resultat som kunde visa tecken på ifall det vore nödvändigt att eventuellt införa en kurs om internetbedrägerier i utbildningsprogrammet för informationsbehandling eller inte baserat på svaren från frågeformuläret.

Eftersom målgruppen var både de svenska och de finska linjerna så använde jag mig av två stycken frågeformulär, ett svenskspråkigt och ett finskspråkigt. Svaren från båda dessa slogs ihop totalt i diagram som redovisas i kapitel 5. Frågeformulärena var aktiva och kunde besvaras från den 14 augusti till den 15 oktober 2012.

Själva undersökningen gjordes med hjälp av programmet e-lomake, och svaren som sparades där behandlades i programmet Microsoft Excel 2010 för att skapa diagram. Svaren redogjordes i kapitel 5 med hjälp av just dessa diagram.

4.1 Tanken bakom undersökningen och mål

Undersökningen i detta lärdomsprov kom till först som en tanke då jag funderade på utvärderingar inom olika saker. Jag tänkte att en utvärdering av Vasa yrkeshögskolas tradenomstuderande då det kom till deras kännedom och erfarenheter av nätbedrägerier vore en lärorik och intressant uppgift. Detta eftersom internetanvändning är ett av de största områden som en framtida tradenomstuderande kommer att arbeta inom, samt för att internetbedrägerier är stort i hela världen just nu plus att det är en viktig sak att ha kunskap om.

En av de allra största orsakerna till varför det verkade som en bra idé inom just denna utbildning var att till min kännedom så har inte något liknande gjorts

tidigare, och det kunde vara bra att ha en tillfällig lägesrapport. Målet med undersökningen var att få en tillfällig lägesrapport och se vad som eventuellt kunde göras med denna information då det är frågan om kurser som handlar om bedrägerier på internet.

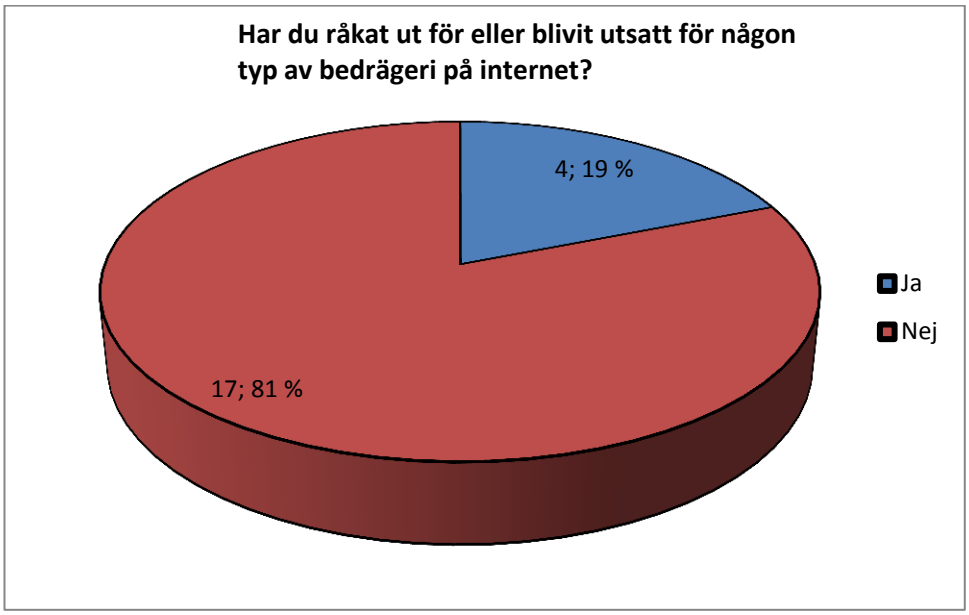
4.2 Frågorna

De frågor som användes i frågeformuläret listas här nedanför.

1. Har du råkat ut för eller blivit utsatt för någon typ av bedrägeri på internet?
2. Känner du någon som har råkat ut för bedrägeri?
3. Om du skulle drabbas av bedrägeri, skulle du anmäla händelsen?
4. Vid näthandel, brukar du kolla butikens/säljarens tillförlitlighet före du handlar?
5. Har du någon gång fått t.ex. ett misstänkt phishing-mail?
6. Tror du att du vet vad du borde göra ifall du råkar ut för bedrägeri?
7. Har ditt antivirusprogram som du använder skydd för nätfiske?
8. Tror du att du med ditt omdöme skulle kunna skilja mellan en legitim webbsida och en fiskesida?
9. Har den e-post-tjänst du använder skydd för bedrägerier som t.ex. phishing?
10. Tycker du att det kunde vara en bra idé att inkludera information om nät-bedrägerier i en redan existerande kurs eller att skapa en helt ny kurs om ämnet?

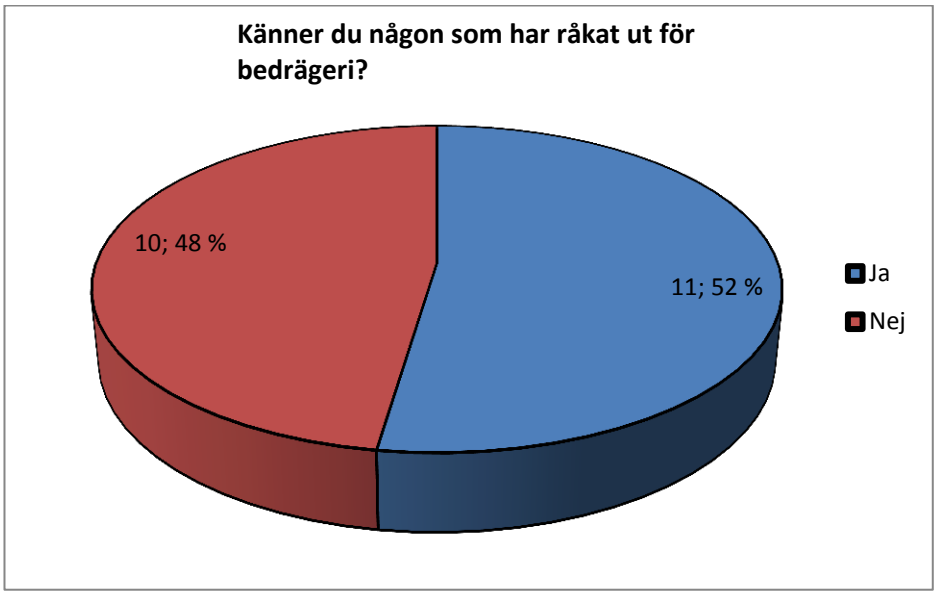
5 RESULTATEN AV UNDERSÖKNINGEN

Resultatet från den första frågan. På grafen nedanför kan man se att 4 personer (19 %) har svarat Ja på frågan, vilket betyder att de har råkat ut för bedrägeri. 17 personer (81%) har svarat Nej, vilket betyder att de inte har råkat ut för bedrägeri.



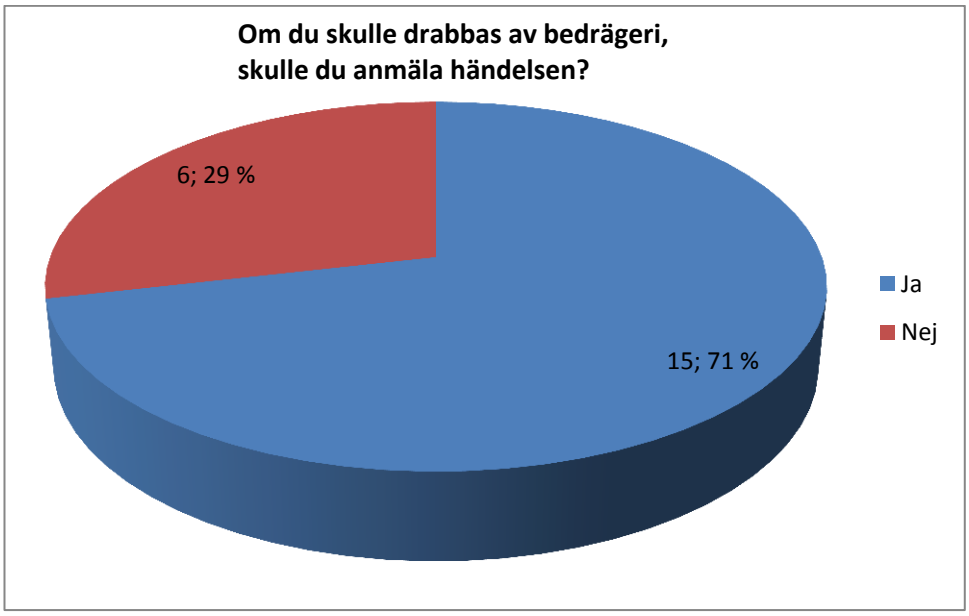
Figur 6: *Ett cirkeldiagram på den första frågan av frågeformuläret*

Resultatet från den andra frågan. På grafen kan man se att 11 personer (52 %) har svarat Ja på frågan, vilket betyder att de känner någon som har råkat ut för bedrägeri. 10 personer (48 %) har svarat Nej, vilket betyder att de inte känner någon som har råkat ut för bedrägeri.



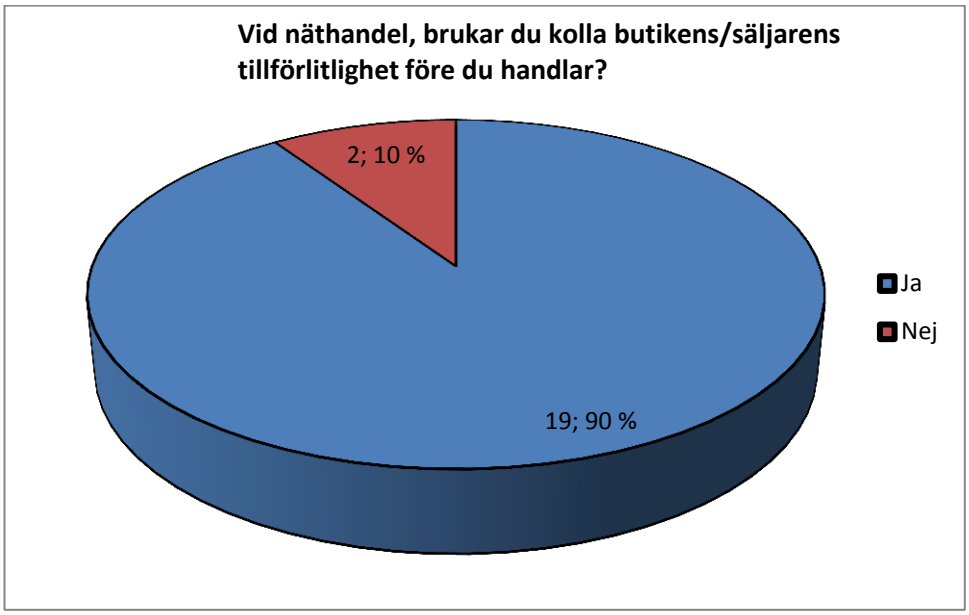
Figur 7: *Ett cirkeldiagram på den andra frågan av frågeformuläret*

Resultatet från den tredje frågan. På grafen nedanför kan man se att 15 personer (71 %) har svarat Ja på frågan, vilket betyder att de skulle anmäla händelsen om de blev bedragna. 6 personer (29 %) har svarat Nej, vilket betyder att de inte skulle anmäla händelsen om de blev bedragna.



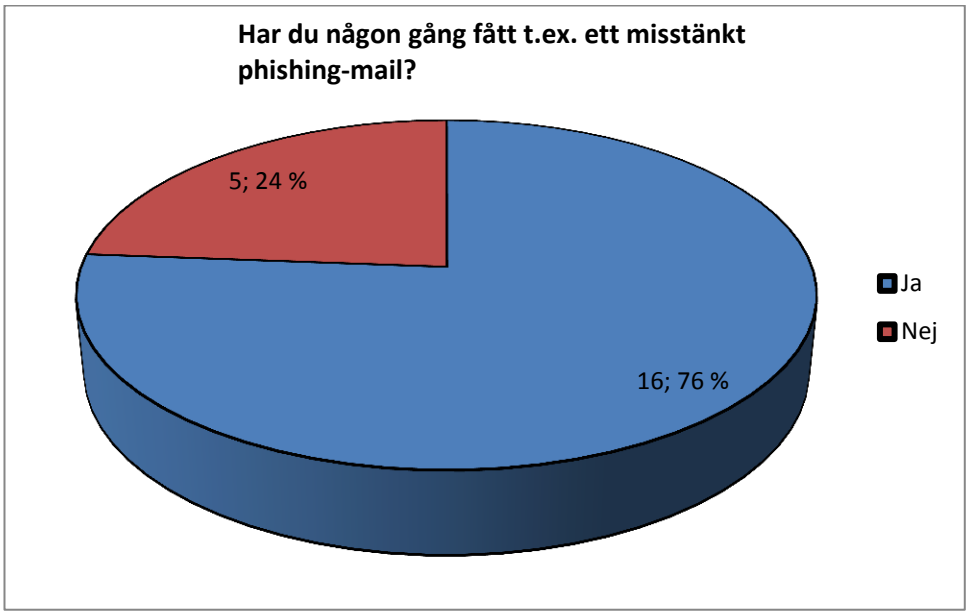
Figur 8: *Ett cirkeldiagram på den tredje frågan av frågeformuläret*

Resultatet från den fjärde frågan. På grafen nedanför kan man se att 19 personer (90 %) har svarat Ja på frågan, vilket betyder att de brukar undersöka butikens/säljarens tillförlitlighet vid näthandel före de handlar. 2 personer (10 %) har svarat Nej, vilket betyder att de inte brukar undersöka butikens/säljarens tillförlitlighet vid näthandel före de handlar.



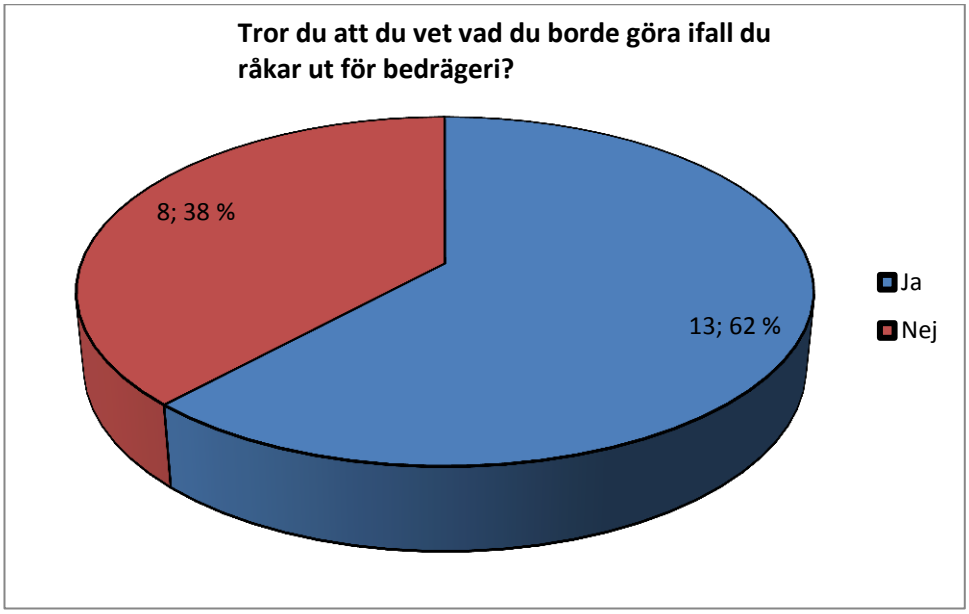
Figur 9: *Ett cirkeldiagram på den fjärde frågan av frågeformuläret*

Resultatet från den femte frågan. På grafen kan man se att 16 personer (76 %) har svarat Ja på frågan, vilket betyder att de någon gång har fått ett misstänkt phishing-mail. 5 personer (24 %) har svarat Nej, vilket betyder att de inte har fått ett misstänkt phishing-mail någon gång.



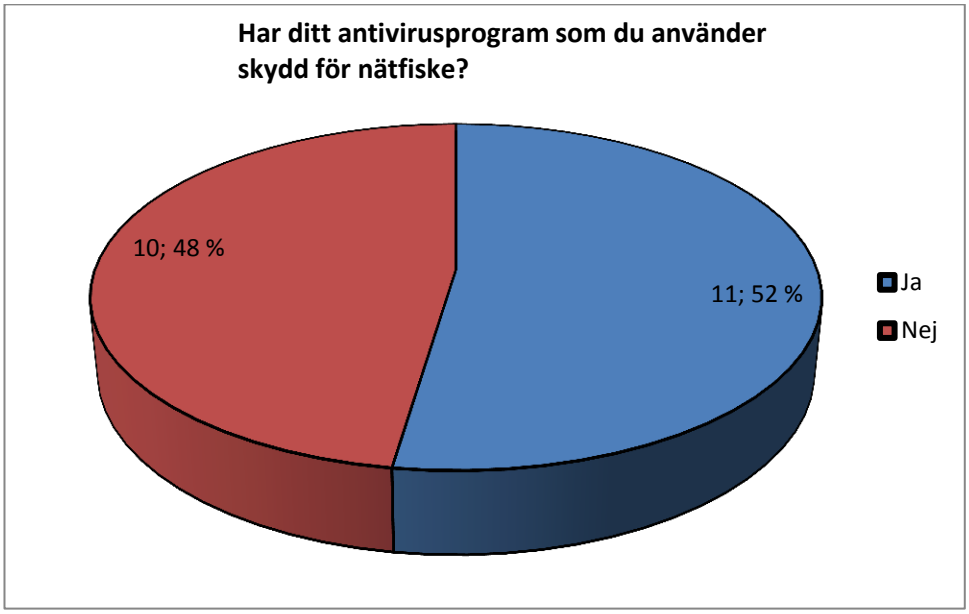
Figur 10: *Ett cirkeldiagram på den femte frågan av frågeformuläret*

Resultatet från den sjätte frågan. På grafen nedanför kan man se att 13 personer (62 %) har svarat Ja på frågan, vilket betyder att de vet vad de borde göra ifall de råkar ut för bedrägeri. 8 personer (38%) har svarat Nej, vilket betyder att de inte vet vad de borde göra ifall de råkar ut för bedrägeri.



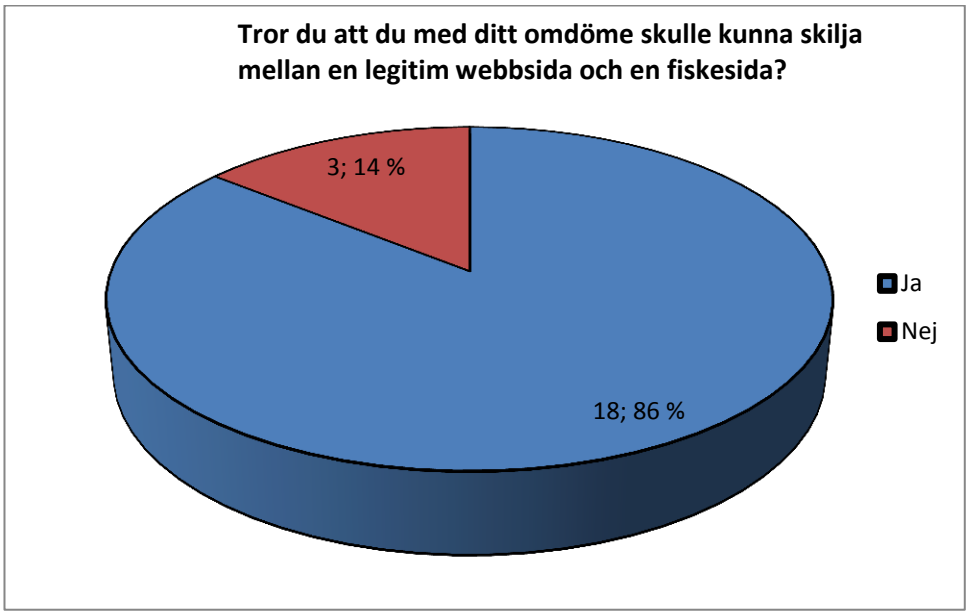
Figur 11: *Ett cirkeldiagram på den sjätte frågan av frågeformuläret*

Resultatet från den sjunde frågan. På grafen nedanför kan man se att 11 personer (52 %) har svarat Ja på frågan, vilket betyder att de använder ett antivirusprogram med skydd för nätfiske. 10 personer (48%) har svarat Nej, vilket betyder att de inte använder ett antivirusprogram med skydd för nätfiske.



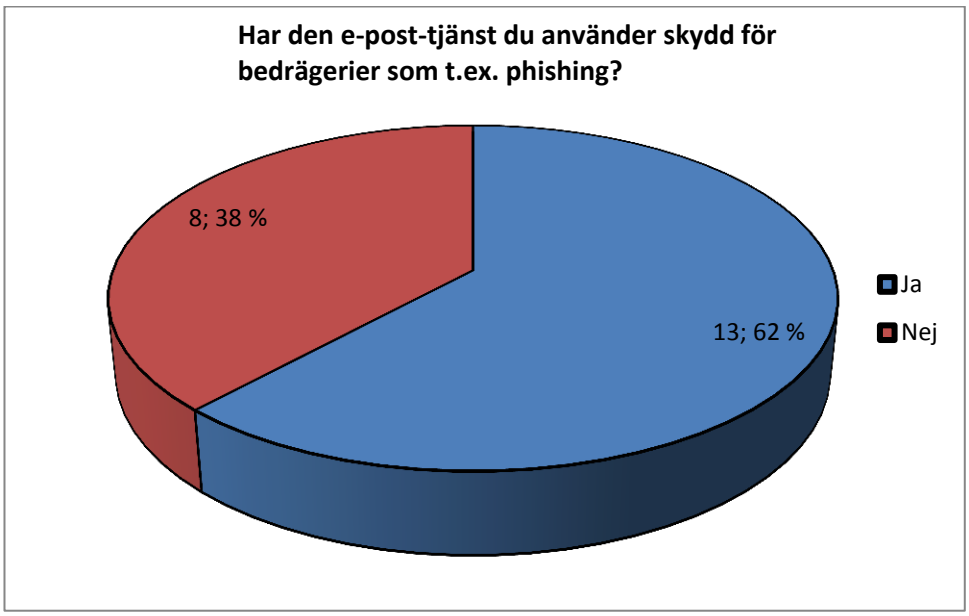
Figur 12: *Ett cirkeldiagram på den sjunde frågan av frågeformuläret*

Resultatet från den åttonde frågan. På grafen kan man se att 18 personer (86 %) har svarat Ja på frågan, vilket betyder att de tror att de med sitt omdöme kunde skilja mellan en legitim webbsida och en fiskesida. 3 personer (14 %) har svarat Nej, vilket betyder att de inte tror att de med sitt omdöme kunde skilja mellan en legitim webbsida och en fiskesida.



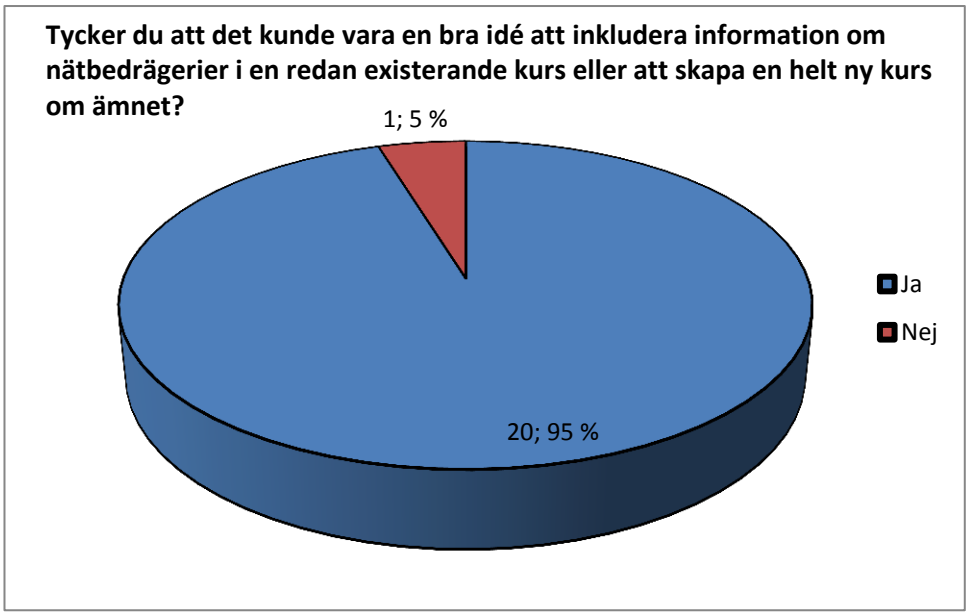
Figur 13: *Ett cirkeldiagram på den åttonde frågan av frågeformuläret*

Resultatet från den nionde frågan. På grafen nedanför kan man se att 13 personer (62 %) har svarat Ja på frågan, vilket betyder att den e-posttjänst som de använder har skydd för bedrägerier som t.ex. phishing. 8 personer (38 %) har svarat Nej, vilket betyder att den e-posttjänst som de använder inte har skydd för bedrägerier som t.ex. phishing.



Figur 14: *Ett cirkeldiagram på den nionde frågan av frågeformuläret*

Resultatet från den tionde och sista frågan. På grafen nedanför kan man se att 20 personer (95 %) har svarat Ja på frågan, vilket betyder att de tycker att det vore en bra idé att inkludera information om nätbedrägerier i en redan existerande kurs eller att skapa en helt ny kurs om ämnet. 1 person (5 %) har svarat Nej, vilket betyder att den personen inte tycker att det vore en bra idé att inkludera information om nätbedrägerier i en redan existerande kurs eller att skapa en helt ny kurs om ämnet.



Figur 15: *Ett cirkeldiagram på den tionde och sista frågan av frågeformuläret*

6 SLUTLEDNING

Det här lärdomsprovet har varit en prövning på de kunskaper som jag besitter angående internetbedrägerier och hur man gör en undersökning beträffande en bestämd målgrupp samt en tolkning av resultaten som gavs av denna undersökning.

Då jag såg på svaren till frågeformuläret så var det relativt lätt att dra en slutsats om allting. 4 personer av 21 råkat ut för någon typ av bedrägeri på internet, medan 17 inte har gjort det. Så största delen har undvikit bedrägerier, och det är en bra sak.

10 personer av 21 känner någon som har råkat ut för bedrägeri, medan 11 personer inte gör det. Här var det jämt mellan svaren men det är slutligen positivt.

15 personer av 21 skulle anmäla händelsen, om de råkade ut för bedrägeri, medan 6 personer inte skulle göra det. Detta verkade som en liten shock, man förväntar ju sig att alla som blir bedragna skulle göra anmälan.

19 personer av 21 brukar undersöka butikens/säljarens tillförlitlighet vid näthandel före handel, medan 2 personer inte brukar göra det. Eftersom detta är en speciellt viktig sak då det gäller näthandel så är det bra att så många personer har svarat positivt på frågan, man kan konstatera att de föredrar att känna sig säkra på denna front förrän de handlar.

16 personer av 21 har någon gång fått ett misstänkt phishing-mail, medan 5 personer inte har fått det. Detta är något som de flesta har fått eller borde ha fått vid någon tidpunkt, så det är inte speciellt shockerande att se att så många har svarat positivt.

13 personer av 21 vet vad de borde göra om de råkade ut för bedrägeri, medan 8 personer inte vet det. Ett rätt så högt svarstal positivt men ändå lite för lågt, man kunde nog ha trott att så gott som alla vet vad de borde göra i en sådan situation.

11 personer av 21 använder ett antivirusprogram med skydd för nätfiske, medan 10 personer inte gör det. De flesta antivirusprogram i dagens läge har skydd för nätfiske, men många gratisversioner av program har inte det, och det brukar oftast vara studerande som använder sådana. Men ungefär hälften positiva svar är väl nog ändå ett bra resultat.

18 personer av 21 tror att de med sitt omdöme kunde skilja en fiskesida från en legitim webbsida, medan 3 personer inte tror att de kunde göra det. Här var det inte någon överraskning alls, de flesta tror att de kan med hjälp av sitt omdöme skilja en fiskesida från en legitim webbsida, och det är positivt på alla vis.

13 personer av 21 använder en e-posttjänst med skydd för olika bedrägerier som t.ex. phishing, medan 8 personer inte gör det. Återigen lite samma som med den sjätte frågan, en smärre överraskning i att inte så många som förväntat använder en e-posttjänst med skydd för olika bedrägerier.

Slutligen så tycker 20 personer av 21 att det kunde vara en bra idé att inkludera information om nätbedrägerier i en redan existerande kurs eller att skapa en helt ny kurs om ämnet, medan 1 person inte tycker det. Här har så gott som alla på klart vad de tycker.

Sammansättningsvis så kan konstateras att de flesta frågor har övertaget på den positiva svarssidan, vilket är bra och roligt att se. En del överraskningar fanns dock och det är väl bara så det är. Eftersom så många svarade positivt på den sista frågan om en eventuell kurs som skulle handla om nätbedrägerier så kan man ju inte göra annat än att tro på resultatställningen, det verkar finnas ett visst intresse. Det kunde vara en bra idé att inkludera information om nätbedrägerier i en redan existerande kurs eller att skapa en helt ny kurs om ämnet.

Målet med lärdomsprovet skulle jag nog säga har uppnåtts. Det enda jag kan komma på i form av ånger är att jag önskade få flera svar på frågeformuläret, i hopp om att möjligen få en mer komplett helhetsbild. Svarsprocenten var något som var i princip omöjligt att få reda på eftersom målgruppen varierar i storlek hela tiden och det finns egentligen inget bestämt antal av personer i målgruppen.

Metoden av att använda ett internetbaserat frågeformulär istället för ett klassiskt med utdelning av frågeformuläret som papper bidrog möjligtvis till detta.

Samarbetet med handledaren har förlöpt bra tycker jag. Även om vi inte har haft allt för många tillfällen att talas vid om lärdomsprovet så har jag fått en klar bild av hur arbetet skulle gå framåt och byggas upp.

Slutligen så skulle jag vilja säga att lärdomsprovet har varit en spännande och mångsidig upplevelse, samt lite av ett test för mig själv. Det var intressant att se alla svar på frågorna och tolka svarställningen. Hela processen med frågeformuläret fungerande som ett test för mig, och det höjer självförtroendet då man vet med sig själv att man har klarat av att göra en sådan uppgift på egen hand.

KÄLLOR

Böcker

[1] Ansell, Eva. 2011. Allmän IT-kunskap. Sverige. Fälth & Hässler.

[2] Mitrovic, Predrag, 2005. Handbok i IT-säkerhet. Sverige. Scandbook.

Elektroniska publikationer

[3] Acc.umu.se, Ordlista, 1997. hänvisat 8.5.2012. Tillgänglig i form av www-dokument: <URL: http://www.acc.umu.se/help/smultron/ordlista.htm>.

[4] Antivirusprogram.se, Phishing, 2005. Hänvisat 14.6.2012. Tillgänglig i form av www-dokument: <URL: http://www.antivirusprogram.se/phishing.php>.

[5] Glocalnet.se, Kundservice, Modemkapning. 2012. Hänvisat 22.6.2012 Tillgänglig i form av www-dokument: <URL: http://kundservice.glocalnet.se/Kundservice/Sakerhetspaket/Modemkapning/>.

[6] Juha Saarinen, Test Driving Internet Explorer 7's phishing filter, bild. 2012. Hänvisat 19.12.2012 Tillgängligt i form av bild på: <URL: http://juha.saarinen.org/661 />.

[7] Konsumenteuropa, E-handelsbedrägeri (phishing/nätfiske) och falska webb-platser, 2011. Hänvisat 14.6.2012. Tillgänglig i form av www-dokument: <URL: http://www.konsumenteuropa.se/sv/Amnesomraden/Bedragerier/Olika-typer-av-bedragerier/Phishing-natfiske-och-falska-webbplatser/>.

[8] Konsumenteuropa, "nigeriabrev", 2011. Hänvisat 14.6.2012. Tillgänglig i form av www-dokument: <URL: http://www.konsumenteuropa.se/sv/Amnesomraden/Bedragerier/Olika-typer-av-bedragerier/Nigeriabrev/ >.

[9] Norton.com, Identitetsstöld: En grundkurs, 2012. Hänvisat 26.6.2012. Tillgänglig i form av www-dokument: <URL: http://se.norton.com/identity-theft-primer/article/>.

[10] Pagina.se, It-ordbok. 2012. Hänvisat 8.5.2012. Tillgänglig i form av www-dokument: <URL: http://itord.pagina.se>.

[11] Palisade.plynt.com, Pharming. 2006. Hänvisat 10.5.2012. Tillgänglig i form av www-dokument: <URL: http://palisade.plynt.com/issues/2006Mar/pharming>.

[12] Search Engine Optimization & Web Hosting Solution, Warning: Phishing Mail Targeted at Paypal Users, bild. 2012. Hänvisat 19.12.2012 Tillgängligt i form av bild på: <URL: http://seo.mhvt.net/blog/?p=163 >.

[13] Spamfighter, Nigeriabrev (bedrägeri 419). 2012. Hänvisat 22.6.2012 Tillgänglig i form av www-dokument: <URL: http://www.spamfighter.com/Lang_SV/FAQ_Nigerian.asp>.

[14] Swedbank.se, bedrägerier på internet. 2012. Hänvisat 8.5.2012 Tillgänglig i form av www-dokument: <URL: http://www.swedbank.se/om-swedbank/sakerhet/bedragerier/index.htm>.

[15] Webometrics Thoughts, Why are nigerian letters so badly written? 2012. Hänvisat 19.12.2012 Tillgänglig i form av bild på: <URL: http://blog.webometrics.org.uk/2008/09/why-are-nigerian-letters-so-badly-written/>.

[17] Webopedia, How to defend yourself against identity theft. 2012. Hänvisat 11.6.2012 Tillgänglig i form av www-dokument: <URL: http://www.webopedia.com/DidYouKnow/Internet/2006/identity_theft.asp>.

BILAGOR

Bilaga 1 – Detaljvy på det svenska frågeformuläret och länk till frågeformuläret

Bilaga 2 – Översikt på det svenska frågeformuläret

Bilaga 3 – Detaljvy på det finska frågeformuläret och länk till frågeformuläret

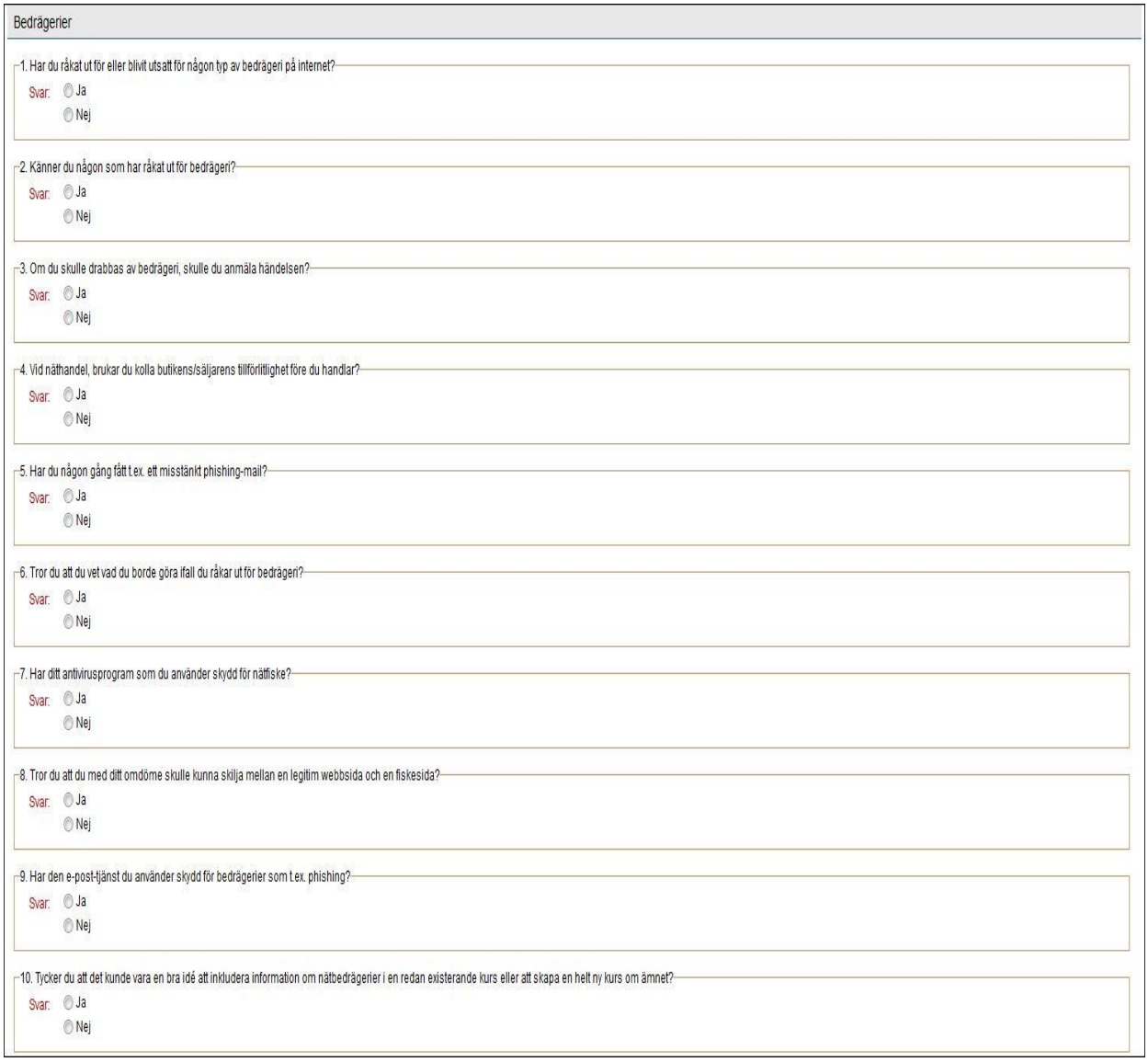
Bilaga 4 – Översikt på det finska frågeformuläret

Bilaga 1 – Detaljvy på det svenska frågeformuläret

lomake3: Frågeformulär om internetbedrägerier	
Blankettens beskrivning	Vänligen besvara denna undersökning om bedrägerier på internet gjord av Joachim Gunell. Ditt svar är viktigt.
Url	https://e-lomake.puv.fi/elomake/lomakkeet/2522/lomake.html
Tillstånd	Tidsinställd [ändra]
Offentlig tid	14.8.2012 kl. 13:00 - 1.10.2012 kl. 23:00
Svar	14 st.

Länk: https://e-lomake.puv.fi/elomake/lomakkeet/2522/lomake.html

Bilaga 2 – Översikt på det svenska frågeformuläret



Bedrägerier

1. Har du råkat ut för eller blivit utsatt för någon typ av bedrägeri på internet?
Svar: Ja / Nej

2. Känner du någon som har råkat ut för bedrägeri?
Svar: Ja / Nej

3. Om du skulle drabbas av bedrägeri, skulle du anmäla händelsen?
Svar: Ja / Nej

4. Vid näthandel, brukar du kolla butikens/säljarens tillförlitlighet före du handlar?
Svar: Ja / Nej

5. Har du någon gång fått t.ex. ett misstänkt phishing-mail?
Svar: Ja / Nej

6. Tror du att du vet vad du borde göra ifall du råkar ut för bedrägeri?
Svar: Ja / Nej

7. Har ditt antivirusprogram som du använder skydd för nätfiske?
Svar: Ja / Nej

8. Tror du att du med ditt omdöme skulle kunna skilja mellan en legitim webbsida och en fiskesida?
Svar: Ja / Nej

9. Har den e-post-tjänst du använder skydd för bedrägerier som t.ex. phishing?
Svar: Ja / Nej

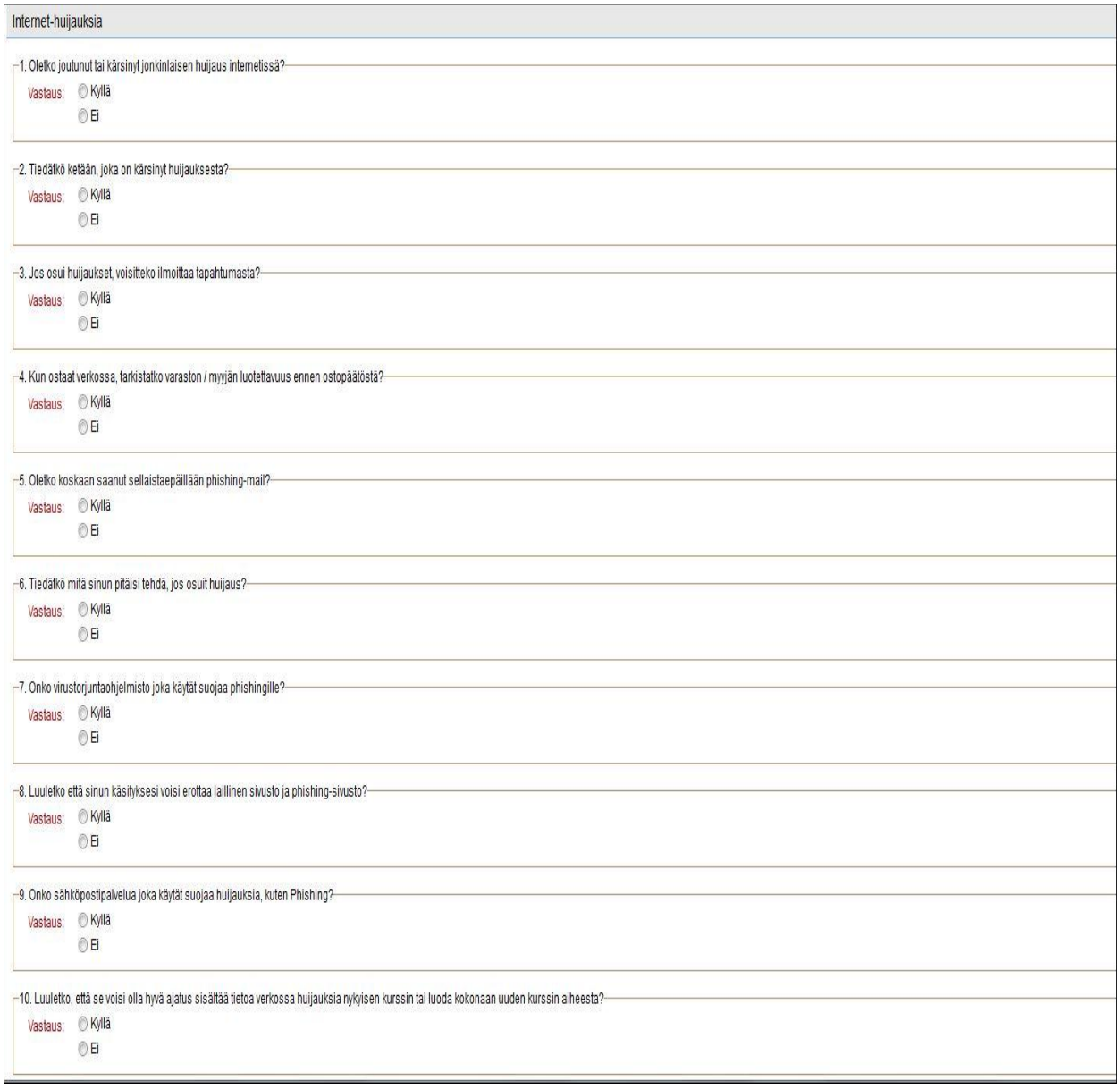
10. Tycker du att det kunde vara en bra idé att inkludera information om nätbedrägerier i en redan existerande kurs eller att skapa en helt ny kurs om ämnet?
Svar: Ja / Nej

Bilaga 3 – Detaljvy på det finska frågeformuläret

lomake4: Kysely Internet-huijauksia	
Blankettens beskrivning	Vastaa tähän kysely internethuijauksia tehnyt Joachim Gunell. Sinun vastaus on tärkeä.
Url	https://e-lomake.puv.fi/elomake/lomakkeet/2524/lomake.html
Tillstånd	Tidsinställd [ändra]
Offentlig tid	14.8.2012 kl. 13:00 - 1.10.2012 kl. 23:00
Svar	7 st.

Länk: https://e-lomake.puv.fi/elomake/lomakkeet/2524/lomake.html

Bilaga 4 – Översikt på det finska frågeformuläret



Internet-huijauksia

1. Oletko joutunut tai kärsinyt jonkinlaisen huijaus internetissä?
Vastaus: Kyllä / Ei

2. Tiedätkö ketään, joka on kärsinyt huijauksesta?
Vastaus: Kyllä / Ei

3. Jos osui huijaukset, voisitteko ilmoittaa tapahtumasta?
Vastaus: Kyllä / Ei

4. Kun ostaat verkossa, tarkistatko varaston / myyjän luotettavuus ennen ostopäätöstä?
Vastaus: Kyllä / Ei

5. Oletko koskaan saanut sellaistaepäillään phishing-mail?
Vastaus: Kyllä / Ei

6. Tiedätkö mitä sinun pitäisi tehdä, jos osuit huijaus?
Vastaus: Kyllä / Ei

7. Onko virustorjuntaohjelmisto joka käytät suojaa phishingille?
Vastaus: Kyllä / Ei

8. Luuletko että sinun käsityksesi voisi erottaa laillinen sivusto ja phishing-sivusto?
Vastaus: Kyllä / Ei

9. Onko sähköpostipalvelua joka käytät suojaa huijauksia, kuten Phishing?
Vastaus: Kyllä / Ei

10. Luuletko, että se voisi olla hyvä ajatus sisältää tietoa verkossa huijauksia nykyisen kurssin tai luoda kokonaan uuden kurssin aiheesta?
Vastaus: Kyllä / Ei